(ISC)² Official Study Guide

CISSP

CISSP

官方学习指南（第7版）

CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide, Seventh Edition

James Michael Stewart
[美] Mike Chapple 著
Darril Gibson
唐俊飞 译
北京汇哲信安科技有限公司 审稿

100%涵盖2015年CISSP CIB考点：

- 访问控制
- 应用开发安全
- 业务持续性计划
- 灾难恢复计划
- 密码学

清华大学出版社

目　录

第 1 章

通过原则和策略的安全治理

本章中覆盖的 CISSP 考试大纲包含：

安全和风险管理(例如安全、风险、合规性、法律、法规、业务连续性)

- A. 理解和应用机密性、完整性和可用性的概念
- B. 应用安全治理原则，通过：
  - B.1 安全功能与战略、目标、使命和愿景的一致(例如商业案例、预算和资源)
  - B.2 组织的流程(例如并购、剥离和治理委员会)
  - B.3 安全角色和职责
  - B.4 控制架构
  - B.5 应尽关注
  - B.6 应尽职责
- F. 开发和实现文档化的安全策略、标准、程序和指南
- J. 理解和应用威胁建模
  - J.1 识别威胁(例如竞争对手、供应商、雇员和值得信赖的伙伴)
  - J.2 确定和用图表示潜在攻击(例如社会工程学、欺骗)
  - J.3 执行降低分析
  - J.4 修复威胁的技术和流程(例如软件架构和操作)
- K. 把安全风险考虑到收购策略和实践中
  - K.1 硬件、软件和服务
  - K.2 第三方评估和监控(例如现场评估、文件传递和审查、流程/策略审查)
  - K.3 最小化安全需求
  - K.4 服务级别需求

对于 CISSP 认证考试，在通用知识体(Common body of Knowledge，CBK)的安全和风险管理知识域中有许多安全解决方案的基本要素要处理。这些基本要素包括安全机制的设计、执行和管理。这个知识域的另外一些要素在第 2 章“人员安全和风险管理概念”、第 3 章“业务连续性计划”和第 4 章“法律、法规和合规性”中讨论。请务必检查所有这些章节中针对这一知识域主题的全部观点。

1.1 理解和应用机密性、完整性和可用性的概念

安全管理概念与原则是安全策略和解决方案部署中的固有元素。它们既定义了安全环境所需的基本参数，也定义了策略设计人员和系统实现人员为创建安全解决方案所必须达到的目的和目标。透彻地理解这些内容，对现实生活中的安全专业人士以及 CISSP 考生来说是非常重要的。

安全的主要目的和目标被包含在 CIA 三元组(见图 1.1)中。CIA 三元组是三条主要安全原则的名字，这三条安全原则是：

- 机密性(Confidentiality)
- 完整性(Integrity)
- 可用性(Availability)

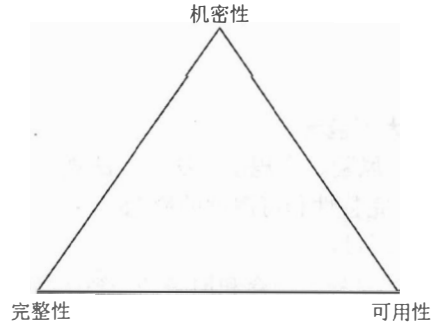


图 1.1 CIA 三元组

对安全控制进行评估时，通常关注是否涉及这些核心的信息安全原则。总的来说，完整的安全解决方案应当充分地涉及所有这些原则。对脆弱性和风险的评估也是基于它们对一个或更多个 CIA 三元组原则的威胁程度。因此，熟悉这些原则，并使用它们作为评判安全相关问题的指导原则，是一个不错的主意。

这三条原则被认为是安全领域内最重要的原则。然而，每条原则对一个特定的组织究竟有多重要，主要取决于组织的安全目标和需求以及安全性所受到的威胁程度。

1.1.1 机密性

CIA 三元组的第一条原则是机密性。如果安全机制提供机密性，那么它就为限制未授权主体不能访问数据、客体或资源提供了高级别保证。如果存在对机密性的威胁，那么就有可能发生未授权的泄漏。

通常，在网络上维护机密性时，数据在存储、处理和传输过程中必须受到保护，从而不会出现未授权的访问、使用或暴露。数据、资源和客体的每一种状态都需要唯一的和特殊的安全控制，以便维持机密性。

针对破坏机密性的攻击有很多，这些攻击包括捕获网络通信、窃取密码文件、社会工程学、端口扫描、肩窥、偷听和嗅探攻击等。

对机密性的破坏不限于直接针对机密性的攻击。许多未授权的敏感或机密信息泄露都是由于人为错误、疏忽或失职造成的。造成机密性遭到破坏的事件包括：没能对传输数据进行适当的加密；在传输数据之前，没能对远程系统进行充分的身份认证；一直打开不安全的接入点；访问恶意代码

导致打开后门；传真的误传，在打印机上遗失文件，甚至在显示器上显示数据时，从访问终端离开。如果终端用户或系统管理员的行为不当，或者安全策略存在疏漏以及安全控制配置不正确，那么机密性也会受到破坏。

许多对策有助于保障机密性，抵御潜在威胁。这些措施包括加密、网络流量填充、严格的访问控制、严格的认证程序、数据分类和广泛的人员培训。

机密性和完整性相互依赖。客体如果缺乏完整性，机密性就无法被维护。机密性的其他概念、条件和特征包括：

敏感性　敏感性是指信息的品质，如果这种信息被披露，就可能会造成伤害或损坏。维护敏感信息的机密性有助于预防伤害或损坏。

自主性　自主性是一种决策行为，操作员可以凭这种权利影响或控制信息的披露，以便将伤害或损坏降到最低。

关键性　信息的关键级别是对其关键性的评测。关键级别越高，越需要保持信息的机密性。高级别的关键性对一个组织的运营和功能是必不可少的。

隐蔽性　隐蔽是一种隐蔽或防止披露的行为。隐蔽通常被视为覆盖、混淆或干扰的一种手段。

保密性　保密是一种保守秘密或防止信息泄露的行为。

隐私性　隐私是指要保持信息处于机密状态，这些可能是个人识别信息，或是如果泄露就可能对某人造成伤害、尴尬或丢人的信息。

隐藏性　隐藏就是把信息存储到一个偏僻的位置。这个位置还可以附加严格的访问控制。隐藏有助于实施机密性保护。

隔离性　隔离是指把特定信息与其他信息分隔开来的行为。隔离可以用来防止信息混杂或信息泄露。

每个组织都需要对他们希望实现的机密性进行细微差别的评估。用于实现一种形式机密性的工具和技术可能不支持或不允许用于其他的形式。

1.1.2　完整性

CIA 三元组的第二条安全原则是完整性。为了维护完整性，客体必须保持自身的正确性，并且只能由被授权的主体进行有意修改。如果安全机制提供了完整性，那么它就对数据、客体和资源提供了保持原有受保护状态和不被修改的高级别保证，这也包括当客体在存储、传输或处理过程中发生的变更。因此，维护完整性意味着客体本身不会被改变，并且管理和操纵客体的操作系统与程序实体不会受到安全威胁。

我们可以从下列三个方面查看完整性：

- 应该禁止未授权的主体执行修改操作。
- 应该禁止经过授权的主体执行未授权的修改操作，例如失误。
- 客体应当内外保持一致，这样它们的数据才能正确并真实地反映现实情况，并且与任何子客体、同等客体或父客体的关系都是有效的、一致的和可检验的。

为了在系统上维护完整性，必须对数据、客体和资源的访问进行适当控制。此外，应当使用活动日志记录，从而保证只有经过授权的用户才能够访问他们各自的资源。在存储、传输和处理过程中维护和确认客体完整性时，需要各种各样的控制和监督措施。

针对破坏完整性的攻击有很多。这些攻击包括：病毒、逻辑炸弹、未授权访问、编码和应用程序中的错误、恶意修改、有企图的替换以及系统后门。

与机密性一样，对完整性的破坏不限于有意攻击。许多对敏感信息的未授权修改实际是由于人为错误、疏忽或失职造成的。导致完整性被破坏的事件包括：意外地删除文件；输入无效数据；更改配置，例如命令、代码和脚本中包含的错误；引入病毒以及执行恶意代码(例如，特洛伊木马)。任何用户(包括管理员)的不当行为都可能破坏完整性，安全策略的疏漏或安全控制的配置不正确也可能导致类似事情的发生。

有许多措施可以确保完整性不会受到可能的威胁。这些措施包括：严格的访问控制、严密的身份认证过程、入侵检测系统、对客体/数据进行加密、散列总和认证(详见第 6 章“密码学与对称加密算法”)、接口限制、输入/功能检验以及广泛的人员培训。

完整性依赖于机密性。缺乏机密性，也就无法维护完整性。完整性的其他概念、条件和特征包括：准确性、真实性、可靠性、合法性、不可否认性、可问责性、可信任性、完整性以及可理解性。

1.1.3 可用性

CIA 三元组的第三条安全原则是可用性，可用性指的是经过授权的主体被及时准许和不间断地访问客体。如果安全机制提供了可用性，那么它就提供了经过授权的主体能够访问数据、客体和资源的高级别保证。可用性包括有效地不间断地访问客体和阻止拒绝服务(Denial-of-Service，DoS)攻击。可用性还意味着支持基础结构(包括网络服务、通信和访问控制机制)的正常运作，并允许经过授权的用户获得被授权的访问。

为了在系统中维护可用性，必须进行适当的控制，从而确保被授权的访问和可接受的性能等级、快速处理中断、提供冗余度、维持可靠的备份以及避免数据丢失或破坏。

针对可用性的威胁有很多。这些威胁包括：设备故障、软件错误，以及环境问题(如高温、静电、洪水、断电等)。针对可用性的其他攻击形式还包括 DoS 攻击、客体损坏和通信中断。

与机密性和完整性一样，对可用性的破坏不限于有意攻击。许多对敏感信息的未授权修改实际是由于人为错误、疏忽或失职造成的。导致可用性被破坏的事件包括：意外地删除文件；硬件或软件组件的过度使用；私下分配资源；贴错标签或不正确的客体分类。任何用户(包括管理员)的不当行为都可能破坏可用性，安全策略的疏漏或安全控制的配置不正确也可能导致类似事情的发生。

有许多措施可以确保可用性不会受到可能的威胁。这些措施包括：正确设计中间传输系统、有效地使用访问控制、对性能和网络通信进行监控、使用防火墙和路由器阻止 DoS 攻击、为关键系统实现冗余以及维护和测试备份系统。大多数安全策略，以及业务连续性计划(Business Continuity Planning，BCP)，都集中使用各种级别的访问/存储/安全(即磁盘、服务器或站点)来容错，达到消除单点故障的目标，从而维护关键系统的可用性。

可用性依赖于完整性和机密性。缺乏完整性和机密性，就无法维护可用性。与可用性有关的其他概念、条件和特征包括：使用性、可访问性和时效性。

真实场景

CIA 优先级

每个组织机构都有自己独特的安全需求。就 CISSP 考试而言，大多数安全概念只是被笼统地讨论，但是在现实生活中，普通概念和最优方法不适用于具体的安全工作。管理团队和安全团队必须一起工作，从而确定组织的各种安全要求的优先顺序。这项工作包括制定预算费用计划、分派技术与时间，以及集中 IT 人员和安全职员的工作成果。这些活动的一个主要方面是确定组织各种安全要求的优先顺序。了解各种原则或资产的重要程度，能够指导安全观点的形成以及安全解决方案的最终部署。通常，开始建立优先顺序是一项艰巨的任务。面对这样的挑战，可行的解决方案是首先确定机密性、完整性和可用性这三条主要安全原则的优先顺序。对于为组织机构设计内容全面的安全解决方案来说，确定最重要的元素是绝对必要的。由此建立的模式能够复制来自设计、体系结构、部署以及维护方面的概念。

你是否知道自己组织中 CIA 三元组组件的优先顺序？如果不知道，那么请尝试找出优先顺序。

让我们看一个对 CIA 优先顺序概念的有趣归纳：在许多情况下，军队和政府机构倾向于机密性的优先顺序高于完整性和可用性，而私人公司则倾向于可用性的优先顺序高于机密性和完整性。尽管这种优先顺序更关注于某条安全原则，但并不说明可以忽视或不恰当地应对优先顺序排在第 2 位和第 3 位的安全原则。

1.1.4　其他安全概念

除了 CIA 三元组以外，在设计安全策略和部署安全解决方案时，还需要考虑其他很多与安全有关的概念和原则。这一节主要讨论身份标识、身份认证、授权、审计、可问责性(见图 1.2)，以及不可否认性。

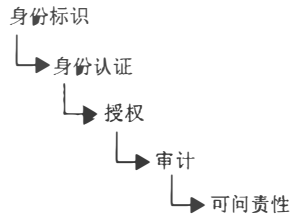


图 1.2　AAA 服务的 5 个要素

1. 身份标识

身份标识是一个过程，在这个过程中，主体会表明身份，并且开启可问责性。主体必须向系统提供身份，从而启动身份认证、授权和可问责性的过程。提供身份的方式可以是：键入用户名、刷智能卡、挥动接近设备、说出一条短语，或将脸、手或手指置于照相机或扫描设备前。提供 ID 号的过程也是身份标识过程。如果没有提供身份，那么系统就没有办法将身份认证因素与主体关联在一起。

一旦主体通过身份标识(也就是识别和验证了主体的身份)，此身份就对主体今后的行为负责。IT 系统根据身份而非主体本身进行跟踪活动。计算机无法区分不同的人，但是却知道不同用户的账户

是有区别的。主体的身份通常被标记为或被视为公共信息。然而，简单地声明身份并不意味着访问或授权。在获得授权访问受控资源之前，身份必须被证明或验证。这个过程称为身份认证。

2. 身份认证

认证或测试所声明身份合法性的过程就是身份认证。身份认证要求来自主体的附加信息必须完全对应于被表明的身份。身份认证的最常见形式是使用密码(包括密码的变化形式 PIN 和密码短语)。通过与合法身份(也就是用户账户)数据库中的一种或多种因素进行比较，身份认证能够认证主体的身份。用于认证身份的身份认证因素通常被标记为或被视为私有信息。主体和系统维护身份认证因素隐蔽性的能力直接反映了该系统的安全级别。如果非法获得和使用目标用户身份认证因素的过程相对容易，那么身份认证系统就不安全。如果这个过程相对困难，那么身份认证系统就相当安全。

身份标识和身份认证总是作为一个过程中的两个步骤被一起使用。提供身份是第一个步骤，提供身份认证因素则是第二个步骤。如果不执行上述两个步骤，那么主体就不能获得对系统的访问权限。就安全性而言，缺少其中任何一个步骤都是没用的。

主体能够提供多种身份认证类型(例如，“你知道什么”、“你拥有什么”等)。每种身份认证技术或因素都具有自己独特的优点和弱点。因此，根据每种身份认证技术或因素以及部署的环境来确定是否适用，从而评价每种机制是十分重要的(第13章“管理身份与认证”中详细讨论了身份认证的内容)。

3. 授权

一旦主体通过了身份认证，其访问还必须经过授权。授权的过程确保被请求的活动或客体访问，可以获得通过身份认证和指派的权利和特权。在大多数情况下，系统会评估一个访问控制表，这个表会对主体、客体和预计的活动进行比较。如果允许进行指定的操作，那么主体就获得了授权；反之，主体就没有获得授权。

需要记住的是，虽然主体通过了身份标识和身份认证，但是并不意味着在受控环境内被授权执行任何操作或访问所有资源。主体登录某个网络(也就是说，提供了身份标识和通过了身份认证)，但是仍然可能被阻止访问文件或进行打印(也就是说，未授权执行这些活动)。大多数网络用户只是被授权在指定的一组资源上执行数量有限的一些操作。身份标识和身份认证是访问控制的“全有”或“全无”。对于环境中的每个客体，在“全有”与“全无”之间，授权具有非常大的变化。例如，用户也许能够读取某个文件，但是不能删除这个文件；用户也许能够打印文档，但是不能更改打印队列；用户也许能够登录到系统中，但是无法访问任何资源。通常，对授权的定义使用了访问控制模型中的一个概念，例如 DAC、MAC 或 RBAC(参看第 14 章“控制和监控访问”)。

AAA 服务

你可能听过 AAA 服务的概念。这三个 A 是 Authentication(认证)、Authorization(授权)和 Accounting(可问责性，有时是 Auditing，意思是审计)的英文缩写。然而，有点让人不明白的是，虽然这是三个英文单词的缩写，但实际上它指的是 5 个元素：身份识别、身份认证、授权、审计和可问责性。因此，第一个和第三个 A 实际上代表了两个概念而非一个概念。这 5 个元素代表了下面的安全性流程：

识别 当试图访问受保护区域或系统时声明身份

认证 证明身份

授权　允许和拒绝对特定身份进行资源和客体的访问

审计　记录与系统和主体相关的事件和活动日志

可问责(又名可问责性)　审核日志文件，检查符合与违反行为以便主体可为自己的行为负责

虽然 AAA 常用于身份认证系统，但其实 AAA 是所有安全形式的一个基础概念。如果一个安全机制缺少这 5 个元素中的任何一个，这个机制就是不完整的。

4. 审计

审计或监控是程序化方式，通过这种方式，主体在系统中经过身份认证的行为是可问责的。审计也是对系统中未授权的或异常的活动进行检测的过程。审计不仅会记录主体及其客体的活动，而且还会记录维护操作环境和安全机制的核心系统功能的活动。通过将系统事件记录写入日志而创建的审计跟踪，可以用于评估系统的健康状况和性能。系统崩溃可能表明存在程序错误、驱动器错误或入侵企图。记录系统崩溃起因的事件日志常常被用于发现系统出现故障的原因。日志文件为重建事件、入侵和系统故障的历史提供了审计跟踪。我们需要通过审计来检测主体的恶意行为、入侵企图和系统故障以及重构事件，为起诉提供证据、生成问题报告和分析结果。审计通常是操作系统、大多数应用程序和服务的内在特性。因此，配置系统功能来记录特定类型事件的相关信息非常简单。

5. 可问责性

只有在支持可问责性时，才能够正确实施组织的安全策略。换句话说，只有在主体的活动可问责时，才能够保持安全性。有效的可问责性依赖于检验主体身份以及跟踪其活动的能力。通过审计、授权、身份认证与身份标识这些安全服务和机制，将联机身份的活动与某个人联系在一起，就可以建立可问责性。因此，人员的可问责性最终依赖于身份认证过程的强度。如果没有强大的身份认证过程，那么在发生不可接受的活动时，我们就无法确定与特定用户账户相关联的人员就是实际控制该用户账户的实体。

为了获得切实可行的可问责性，在法律上你必须能够支持自己的安全性。如果不能在法律上支持自己的安全努力，那么就不太可能问责与某个用户账户相关联人员的活动。只使用密码进行身份认证，这显然值得怀疑。密码是最不安全的身份认证形式，针对这种形式的不同攻击方式有数十种之多。不过，如果使用多因素身份认证(例如，组合使用密码、智能卡和指纹扫描)，那么其他人几乎不可能通过攻击身份认证过程来假冒特定用户账户的关联人员。

法律上的可防御安全性

安全的要点是：防止坏的事情发生，同时支持好的事情出现。发生坏的事情时，组织常常希望通过法律的实施和法律系统的援助来得到补偿。为了获得法律赔偿，就必须证明存在罪行或者嫌疑人实施了犯罪，以及自己已尽力阻止罪行的实施，只有这样才能从法律上防御保护组织的安全性。如果无法使法庭相信日志文件是准确的，以及只有主体才会实施特定的罪行，那么就无法获得法律赔偿。最终，这就需要一个完整的安全解决方案，这个方案应当使用难以破解的身份认证技术、稳固的授权机制以及完美的审计系统。此外，还必须提供下列证明：组织机构遵守了所有适用的法律和规则；公告了适当的警告和通知；逻辑和物理安全性没有受到其他危害；以及电子证据没有其他可能的合理解释。你要面对这个相当具有挑战性的标准。如果不打算在法律上的可防御安全性的设计和实施方面做出努力，那么尝试低于标准的安全性的要点是什么呢？

6. 不可否认性

不可否认性确保活动或事件的主体无法否认所发生的事件。不可否认性能够防止主体宣称自己没有发送消息、没有执行过某项活动或者不是某个事件的起因。身份标识、身份认证、授权、可问责性和审计使不可否认性成为可能。通过使用数字证书、会话标识符、事务日志以及其他很多传输和访问控制机制，我们能够建立不可否认性。如果没有在系统中构建或正确实施不可否认性，那么就无法认证特定实体是否执行了某种动作。不可否认性是可问责性不可缺少的部分。如果嫌疑人能够否认指控，那么他的行为就无法被问责。

1.1.5 保护机制

理解和启用机密性、完整性和可用性概念的另一方面是保护机制的概念，保护机制是安全控制的常见特性。并非所有的安全控制都必须具有这些机制，但是许多控制通过使用这些机制提供对机密性、完整性和可用性的保护。这些机制包括：使用多层次或多级别的访问、利用抽象、数据隐藏以及使用加密。

1. 分层

分层只是简单地使用连续的多重控制，也被称为深层防御。没有一种特定的控制方法能保护并对抗所有可能存在的威胁。使用多层次的解决方案允许引入多种不同的控制方法来应对随时出现的各种威胁。当分层设计安全解决方案时，大多数的威胁都会被消除、缓解或阻挡。

使用连续分层法而不是并行分层法，这一概念非常重要。通过连续方式执行安全限制意味着使用线性的方式依次执行。只有通过一系列配置，才能由每个安全控制对攻击进行扫描、评估或缓解。单个安全控制方法的失败不会使整个解决方案失效。如果安全控制是以并行方式执行的，某个威胁就可能穿过单个检查点，从而无法消除该威胁特殊的恶意活动。

连续配置方法虽然范围很窄，但是层次很深；并行配置方法虽然范围很宽，但是层次很浅。并行系统在分布式计算应用程序中非常有用，但是在安全领域内，并行机制往往不是一种有用的概念。

考虑一下通往建筑物的物理入口。并行安排出入口的方法被用于购物商场，商场周边的许多地方都设置了出入口。连续设置出入口的方式很可能用于银行或机场。这种场合只提供单一的入口，并且此入口实际上是为了获得进入建筑物活动区域而必须按顺序通过的几个关口或检查点。

分层还包括网络由多个独立实体组成的概念，每个实体都有自己独特的安全控制方法与脆弱性。在有效的安全解决方案中，所有构成单个安全防线的网络系统之间存在协同作用，从而共同筑起一道安全防线。使用独立的安全系统会导致生成分层的安全解决方案。

2. 抽象

抽象是为提高效率而使用的。相似的元素被放入组、类别或角色(被整体性授予安全控制、限制或权限)中。因此，当为客体分类或为主体分配角色时，就需要使用抽象的概念。抽象的概念还包括客体和主体类型的定义或客体本身的定义(也就是用于为实体类别定义模板的数据结构)。抽象用于定义客体可以包含的数据类型、可以在这个客体上执行的或由该客体执行的功能类型以及这个客体具有的功能。抽象使你能够为按类型或功能分类的客体组分配安全控制方法，并抽象简化了安全措施。

3. 数据隐藏

顾名思义，数据隐藏通过将数据置于主体不可访问或无法看到的存储空间，从而防止主体发现或访问数据。不让未授权的访问者访问数据库是数据隐藏的一种形式，同样，限制分类级别较低的主体访问级别较高的数据也属于这种情况，阻止应用程序直接访问硬件也是数据隐藏的一种形式。在安全控制和程序设计中，数据隐藏通常是一个关键要素。

4. 加密

加密是对计划外的接收者隐藏通信数据的含义或意图的一门艺术和学科。加密可以具有很多形式，并且能够被应用于所有的电子通信类型，包括文本、音频和视频文件以及应用程序本身。加密技术是安全控制中一个非常重要的要素，尤其系统之间的数据传输更是如此。加密的强度各种各样，每种强度的设计都针对一种特定的用途或目的。第 6 章“密码学与对称加密算法”和第 7 章“PKI 和密码学应用”中详细讨论了加密技术。

1.2　应用安全治理原则

安全治理是实践行为的集合，这些实践都与支持、定义和指导组织的安全工作相关。安全治理与组织和 IT 治理密切相关，而且经常交织在一起。这三种治理的目标一般是相同或相关的。例如，治理的共同目标就是确保组织能持续且能随时间的推移不断扩大。因此，治理的共同目标就是维持业务流程，同时努力实现增长和弹性。

由于立法和法规遵从性的需要，一些治理要求会被强加于机构，还有其他一些强加的治理要求可能是由于行业指导方针或许可证所要求的。所有的治理形式，包括安全治理，都必须不时地经受评估和认证。可能由于政府的规定或行业最佳实践，都会对组织有各种审计和认证要求。治理合规问题常常因行业和国家的不同而不同。由于机构扩张和不断去适应全球市场，治理问题变得越来越复杂。再加上各国法律不同以及实际的冲突，这个问题也就更加棘手。组织整体上应该有方向、有指导、有工具、有足够的监督能力和管理能力，如此才能应对威胁和风险，并注重消除故障以及将潜在的损失或损坏降到最低。

如你所知，安全治理的各项定义往往是严标准、高要求。最终，安全治理是要实施安全的解决方案和管理方法，而这两个方面紧密相连。安全治理直接监督和参与各级安全。安全不是并且也不应该只被视为属于 IT 事务。相反，安全影响着组织的方方面面。它不是仅靠 IT 人员自己就可以解决的事情。安全是商业运行问题，是组织流程，而不只是 IT 怪才在幕后所谋之事。使用安全治理这个术语就是为了强调这一点，这意味着安全是需要整个组织同时进行管理和控制的，而不只是在 IT 部门。

1.2.1　安全功能战略、目标、任务和愿景的一致

安全管理计划能确保安全策略的适当创建、实现和实施。安全管理计划将安全功能与组织的战略、目标、任务和愿景相结合，这包括根据商业论证、预算限制或稀缺资源设计和实现安全性。为了对做出决定或采取某种形式行动的必要性进行定义，商业论证通常会记录参数或说明立场。制定商业论证就是要说明具体的商业需求，以改变现有业务或选择实现商业目标的方法。商业论证的制

定通常能证明启动了一个新的项目，尤其是与安全相关的项目。同样重要的是，要考虑能够分配的预算有多少，这些预算用于以商业需求为基础的安全防范项目。做好安全防护往往成本很高，但这却是长期可靠经营的重要因素。对大多数机构而言，资金和资源，比如人、技术和空间，都是有限的。由于有这样的资源限制，因此需要努力实现利益最大化。

解决安全管理计划编制的最有效方法是采用自上而下的方式。上层、高层或管理部门负责启动和定义组织的安全策略。安全策略为组织中较低级别的人员指出了方向。中层管理部门的职责是在安全策略的指导下制定标准、基准、指导方针和程序。接着，操作管理者或安全专家负责实现在安全管理文档中规定的配置要求。最后，最终用户必须遵守组织制定的所有安全策略。

注意：

与自上而下方式相反的是自下而上。在采用自下而上方式的环境中，IT 人员在没有来自高层管理部门指示时直接进行安全判断。组织极少使用自下而上的方式，在 IT 行业中，这种方式被认为存在问题。

安全管理部门(而不是 IT 人员)负责更高层的管理，并且考虑的是业务运营问题，而不是 IT 管理问题。安全管理团队或部门负责组织内的安全性，应当独立于其他所有部门。信息安全团队应当由指定的首席安全官(Chief Security Officer，CSO)领导，CSO 必须直接向高级管理者报告。为 CSO 及其团队赋予组织特有分级结构之外的自主权，这不仅能够改善整个组织之间的安全管理，而且有助于避免部门交叉和内部权力斗争问题。

安全管理计划编制的元素包括：定义安全角色；规定如何管理安全性、谁负责安全性以及如何测试安全性的效力；开发安全策略；执行风险分析；以及要求对员工进行安全教育。这些职责要经过管理计划开发的指导。

如果缺少一个关键因素(得到高级管理者的批准)，那么再好的安全计划也是无用的。缺少高级管理者的批准和委托，安全策略就无法取得成功。策略开发团队负责对高级管理部门进行充分的教育，从而使其理解即使采取安全策略所规定的安全措施之后也仍然存在的风险、义务和暴露。开发和实现安全策略能够证明高级管理者对安全性问题进行了适度关注并尽责。如果某个公司没有对安全性进行适度关注并尽责，那么管理者就对疏忽负有责任，并且应当为资产损失和财务损失担责。

安全管理计划编制团队应该开发下列三种计划(如图1.3所示)：

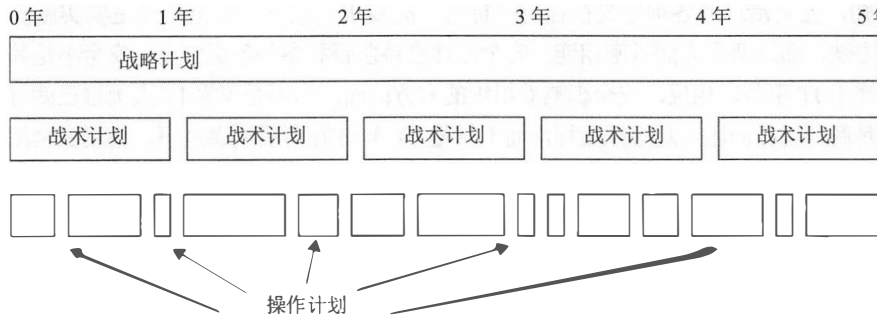


图 1.3　战略计划、战术计划和操作计划的时间线比较

战略计划　战略计划是一个相当稳定的长期计划，它定义了组织的目标，也有助于理解安全功能与组织的安全目标、愿景和使命方面的一致性。如果战略计划每年都被维护和更新，那么大约可

以使用 5 年时间。战略计划还可以作为计划编制的基准。未来的长期目标和愿景在战略计划中将被讨论。战略计划还应当包含风险评估。

战术计划　战术计划是一个中期计划，它被开发用于提供实现战略计划所提出目标的详细细节。战术计划通常一年有效，并且往往规定和调度实现组织目标所必需的任务。战术计划的一些示例包括：项目计划、采购计划、雇佣计划、预算计划、维护计划、支持计划以及系统开发计划。

操作计划　操作计划是一个短期计划，它是基于战略计划和战术计划制定的非常周详的计划。操作计划只在很短的时间内有效或有用。为了服从战术计划，操作计划必须经常被更新(如每个月或每个季度都进行更新)。操作计划是十分周详的计划，它清楚地说明了如何完成组织机构的各种目标。操作计划包括：资源分配、预算要求、人员分配、进度安排以及循序渐进或实现措施。操作计划包括实现如何服从组织安全策略的详细措施细节。操作计划的示例包括：培训计划、系统部署计划和产品设计计划。

维护安全性是一个持续的过程。虽然安全管理计划编制的活动可能具有一个明确的起始点，但是其任务和工作永远不可能完全实现或完成。有效的安全计划重点关注特定的和可完成的目标、预计变化和潜在问题，并且作为整个组织决策的基础。安全文档记录应当是具体的、定义完善的和清晰表述的。为了使安全计划有效，就必须开发、维护和实际应用安全计划。

1.2.2　组织流程

安全治理需要照顾到组织的方方面面，包括收购、剥离和治理委员会等组织流程。收购兼并会增加机构的风险等级，这些风险包括不适当的信息披露、数据丢失、故障或未达到足够的投资回报率(Return On Investment，ROI)。除了收购兼并中的典型商业和财务方面，有效的安全监督和强化审查往往也是降低损失可能性的必要措施，比如在转型期。

同样，剥离、任何形式的资产减少或员工减少都会使阶段内的风险等级变高，从而也需要提高集中安全治理的必要性。需要对资产进行无害处理以防止数据泄漏。应该删除和销毁存储介质，因为介质净化处理技术不能完全保证可以防止数据残留被恢复。需要对不再负责相关事宜的员工进行事后审查，这个过程通常被称为离职面谈。这个过程也通常涉及审查所有的保密协议和其他具有约束力的合同或协议，这些文件需在他们离职后依然有效。

通常，安全治理由治理委员会或至少是董事会进行管理。这群人应是有影响力的专家，他们的主要任务是监督和指导确保组织安全与操作的行为。由于安全是一项复杂的任务，很多组织由于太大无法从个人视角理解这个问题。最可靠的策略是集齐一组专家共同为实现可靠安全治理这一目标而努力。

加强安全治理的两个必要额外组织流程的实例是变更控制/变更管理和数据分类。

1. 变更控制/变更管理

安全管理中的另外一个重要方面是对变更进行控制或管理。安全环境的改变可能引入会导致新脆弱性出现的漏洞、重叠、客体丢失和疏漏。面对变更，维持安全性的唯一方法是系统地管理变更，这往往涉及对安全控制和机制相关的活动，进行广泛的计划编制、测试、日志记录、审计和监控。然后对环境变化进行记录，确定变更的作用者，无论这些作用者是主体、客体、程序、通信路径还是网络本身。

变更管理的目标是确保任何变更都不能降低或危及安全性。变更管理还负责能够将任何变更都

回滚到先前的安全状态。变更管理可以在任何系统上实现(不考虑安全级别)。变更管理要求系统遵守信息技术安全评估标准(Information Technology Security Evaluation and Criteria，ITSEC)的 B2、B3 和 A1 分类。最终，通过避免对已实现的安全性带来无意识的、间接的或连带性的降低现象，变更管理能够改善环境的安全性。尽管变更管理的一个重要目标是防止安全性被不期望地降低，但其主要用途是：详细记录和审计所有变更，从而能够通过管理进行详细的检查。

变更管理应该用于监督系统每个方面发生的变更，包括硬件配置、操作系统和应用软件的变更。变更管理应该被包含在设计、开发、测试、评估、实现、分发、演变、发展、持续操作以及修改中。变更管理不仅需要每个组件和配置的详细目录，而且还需要为每个系统组件(从硬件到软件，以及从配置设置到安全特性)收集和维护完整的文档。

配置或变更管理的变更控制过程具有以下几个目标或要求：

- 以受监控的和有序的方式实现变更。变更总是处在控制之下。
- 包含正式的测试过程，这种过程用于确认变更产生的预期结果。
- 所有的变更都可以撤消(也被称为回退或回滚计划/流程)。在变更发生前向用户发出通知，以避免降低生产率。
- 对变更的影响应进行系统分析。
- 变更对能力、功能和性能产生的负面效应最小化。
- 变更由变更审批委员会(Change Approval Board，CAB)审阅和批准。

并行运行是变更管理过程的一个示例，在这种新系统部署测试中，新系统和旧系统并行运行。每个主要的或重要的用户进程在所有系统上同时执行，从而确保新系统支持老系统所支持或提供的所有必需的业务功能性。

2. 数据分类

数据分类是根据数据的秘密性、敏感性或机密性需求来保护数据的主要方式。在设计和实现安全系统时，因为某些数据项需要更高的安全性，所以对所有数据采取同样的处理方法是低效率的。用较低安全级别来保护所有数据，意味着敏感数据很容易被访问。用较高安全级别保护所有数据，成本太高且对未分类的非关键数据访问限制太多。数据分类用于确定需要分配多少工作量、资金和资源去保护数据以及控制对数据的访问。数据分类或归类，是根据相似，性组织项、对象和主题到组、类别和集合中的过程。这些相似性可能包括价值、成本、灵敏度、风险、脆弱性、权力、特权、损失或损害的可能水平以及“需知”原则。

数据分类方案的主要目的是：根据重要性和敏感性给数据分配标签，对数据安全保护过程进行规范化和层次化。数据分类用于为数据存储、处理和传输提供安全机制，此外还可以确定如何从系统中删除数据和销毁数据。

使用数据分类方案具有下列优点：

- 能够证明组织致力于保护宝贵的资源和资产。
- 能够有助于确定对组织最关键的或最有价值的资产。
- 为安全机制的选择提供安全保证。
- 常常是遵守规范或法律约束所必需的。
- 帮助定义访问级别、授权使用类型，以及对不再有价值的资源进行解除分类和/或对于销毁操作所需的参数。
- 在数据生命周期管理中，对于确定数据的存储(保留)时长、使用和销毁是有帮助的。

数据分类标准取决于执行分类的组织。不过，从通用或标准化分类系统中可以找到很多一般性原则：

- 数据的有用性。
- 数据的时效性。
- 数据的价值或成本。
- 数据的成熟度或年龄。
- 数据的生存期(或何时过期)。
- 与人员的关联。
- 数据泄露的损失评估(也就是数据泄露会对组织有何影响)。
- 数据修改的损失评估(也就是修改数据会对组织有何影响)。
- 数据的国家安全性含义。
- 对数据的已授权访问(也就是谁可以访问数据)。
- 对数据的访问限制(也就是谁对数据的访问受到限制)。
- 数据的维护和监控(也就是谁应该维护并监控数据)。
- 数据的存储。

使用适用于组织的标准、评估数据以及适当地分配数据分类标签。在某些情况下，数据分类标签被添加到数据对象中。在其他情况下，通过把数据放入存储机制或放在安全保护机制之后就可以分配数据分类标签。

为了实现分类方案，必须完成下列 7 个主要的步骤或阶段：

(1) 确定管理人员并定义他们的职责。

(2) 指定如何对信息进行分类和标记的评估标准。

(3) 为每个资源进行分类和添加标签(所有者主导这个步骤，但是必须有监督人员进行检查)。

(4) 记录发现的分类策略的所有例外，并且将这些例外集成到评估标准中。

(5) 选择应用于每个分类级别的安全控制，从而提供必要的保护级别。

(6) 指定解除资源分类的过程以及将资源的保管权转移给外部实体的过程。

(7) 创建一份整个组织范围内都知晓的计划，从而指导所有人员对分类系统的使用。

在设计分类系统和记录使用过程时，往往会忽视解除分类。一旦某个资产不再需要当前分配的分类或敏感性级别保护，就需要解除分类。换句话说，如果资产是新的，它会被分配一个比当前级别更低的敏感性标签。在资产不能根据需要被解除分类时，安全资源就会被浪费，并且更高敏感性级别的价值和保护会被降低。

两种通用的分类方案是政府/军方分类(见图 1.4)和商业/私营部门分类。政府/军方分类具有 5 个级别(以下按从高到低列出)：

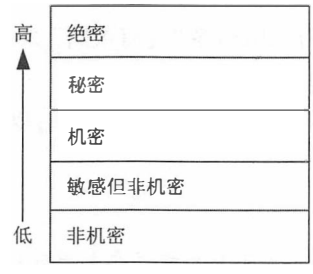


图 1.4　政府/军队分类的级别

绝密(top secret) 最高的分类级别。未授权而泄露绝密数据将会有灾难性的后果，并导致对国家安全的毁灭性破坏。

秘密(secret) 用于具有受限特性的数据。未授权而泄露秘密数据将会有严重后果，并导致对国家安全的重大破坏。

机密(confidential) 用于具有机密特性的数据。未授权而泄露机密数据将会有重大后果，并导致对国家安全的严重破坏。这个分类级别被用于处在“秘密”级别和“敏感但非机密”级别之间的所有数据。

非机密(unclassified) 最低的分类级别。用于既不敏感，也不必分类的数据。非机密数据的泄露既不会危及机密性，也不会造成任何明显的损坏。

提示：

采用首字母记忆法可以按照从低到高的安全顺序轻易地记住政府或军方分类方案的 5 个级别：U.S.Can Stop Terrorism(美国能够制止恐怖主义)。你会看到：从左至右的 5 个大写字母分别表示从低到高的 5 个指定分类级别(或者说图 1.4 中自下而上地列出 5 个级别项)。

机密级别、秘密级别和绝密级别统称为分类的级别。通常，对未授权的个人泄露真实的数据分类是一种数据侵权行为。因此，术语“分类的”通常用于指示敏感但非机密级别以上的被分级的数据。所有分类的数据都免受信息自由法案以及其他很多法律与规章的限制。美国军队的分类方案与数据的敏感度关系最密切，而且关注于对机密性的保护(也就是防止泄漏)。根据危害机密性事件的破坏程度，可以粗略地定义每个分类级别或标签。绝密级别的数据泄漏会对国家安全造成毁灭性破坏，而非机密级别的数据泄漏则不会对国家安全或地方安全造成任何严重破坏。

商业/私营部门的分类系统通常相差很大，因为他们的特点就是不会坚守一个标准或法规。CISSP 考试侧重于 4 种常见或可能的商业分类级别(图 1.5 显示了从最高到最低的级别)：

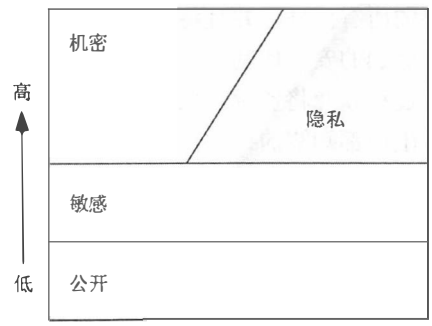


图 1.5 商业/私营部门分类的级别

机密 最高的分类级别，用于极端敏感的和只能内部使用的数据。如果机密数据被泄露，那么会对公司产生重大的负面影响。有时也用标签“专有数据”来替代标签“机密信息”。如果专有数据被泄露，将会对组织的竞争力产生灾难性后果。

隐私 用于具有隐私性或个人特性以及只供内部使用的数据。如果隐私性数据被泄漏，那么会对公司或个人产生重大的负面影响。

注意：

商业/私营部门分类方案中的机密和隐私性数据要求大致相同的安全保护级别。这两个标签的实际差异是：机密数据被用于公司数据，而隐私性数据则被用于与个人有关的数据(例如医疗数据)。

敏感　用于分类级别高于公开数据的数据。如果敏感数据被泄漏，那么会对公司产生负面影响。

公开　最低的分类级别，用于不属于任何一种较高分类级别的所有数据。这种数据的泄漏不会对组织造成严重的负面影响。

数据分类还要考虑的一个相关因素就是所有权。所有权是对个人或群体职责的正式指定。所有权可以明确区分操作系统中的哪些文件或其他类型客体被分配给一个所有者。通常，一个所有者对其拥有的客体具有完整的功能和权限。所有权通常归属于操作系统内功能最强大的账户，比如 Windows 系统中的管理员或 Unix 和 Linux 系统中的 root 用户。在大多数情况下，主体在创建新客体时，该客体的所有者是默认的。但有些环境的安全策略要求在创建新对象时，必须对从最终用户到管理员或管理用户的所有权进行正式变更。在这种情况下，管理员账户可以直接获取新客体的所有权。

除了正规的 IT 结构，其他结构的客体的所有权通常都不明显。公司文档可以为设施、商业任务、流程、资产等定义所有者。然而，这样的文档编制在现实世界中并不总能够“执行”。文件客体的所有权是由操作系统和文件系统执行的，其中物理客体、无形资产或机构概念(如研发部门或项目)的所有权只能进行书面定义，所以容易遭到破坏。必须对物理世界中的所有权实施额外的安全治理，如此才能达到加强效果。

1.2.3　安全角色和责任

安全角色是指个人在组织内部的整个安全实现和管理方案中所扮演的角色。因为并不总是明确的或静态的，所以安全角色在工作描述中不是必须被规定的。熟悉安全角色将对在组织内部建立通信和支持结构很有帮助，这种结构能够支持安全策略的部署和执行。接下来，我们将按照在安全环境中出现的逻辑顺序介绍 6 种安全角色：

高级管理者　组织所有者(高层管理者)的角色被分配给最终负责组织机构安全维护和最关心保护资产的人。高层管理者必须对所有策略问题签字。事实上，所有活动在被执行之前，都必须得到高层管理者的认可和签字。如果没有高层管理者的授权和支持，那么就不存在有效的安全策略。高层管理者对安全策略的认同表明承认在组织机构内部实现的安全性的所有权。高层管理者对安全解决方案的总体成败负有责任，并且负责对组织机构建立安全性予以适度关注并尽职尽责。

虽然高层管理者对安全负有最终责任，但他们实际上很少去实现安全解决方案。在大多数情况下，相应的责任会被委派给组织内部的安全专家。

安全专家　安全专家、信息安全官或计算机应急响应团队(Computer Incident Response Team，CIRT)的角色被分配给受过培训和经验丰富的网络工程师、系统工程师和安全工程师，他们对落实高层管理部门下达的指示负责。安全专家的职责是保证安全性，包括制定和实现安全策略。安全专家的角色可以被标记为 IS/IT 职能角色。安全专家的角色通常由负责设计和实现安全解决方案的团队担任，安全解决方案则是根据已批准的安全策略制定的。安全专家不是决策制定者，他们只是实现者。所有的决策都必须由高层管理者制定。

数据所有者　数据所有者的角色被分配给在安全解决方案中为了放置和保护信息而负责对信息进行分类的人。通常，数据所有者是层次较高的、最终负责数据保护的管理者。然而，数据所有者一般会将实际管理数据的任务委派给数据管理员。

数据管理员　数据管理员的角色被分配给负责实施安全策略和上层管理者规定的保护任务的用户。数据管理员通过执行所有必要的措施为数据提供适当的 CIA 三元组(机密性、完整性和可用性)

保护，并完成上层管理者委派的要求和责任。这些必要的措施包括：完成和测试数据备份、确认数据的完整性、部署安全解决方案以及根据分类管理数据存储。

用户 用户(最终用户或操作者)的角色被分配给具有安全系统访问权限的任何人。用户的访问权限与他们的工作任务联系在一起并且受到限制，所以他们只具有工作职务所要求的能保证完成任务所需的权力(也就是最小特权原则)。用户负责了解组织的安全策略，并遵守规定的操作过程，在已定义的安全参数内进行操作，以便维护安全策略。

审计人员 另一个角色是审计人员。审计人员负责测试和认证安全策略是否被正确实现以及衍生的安全解决方案是否合适。审计人员的角色可以被分配给安全专家或受过培训的用户。审计人员要完成遵守情况报告和有效性报告，高层管理者会审查这些报告。通过这些报告发现的问题，会由高层管理者转换成下达给安全专家或数据管理员的新指示。不过，因为审计人员需要将用户或操作者在环境中的工作作为审计和监控的活动来源，所以审计人员被列为最后一个角色。

所有这些角色在安全环境中都起着重要的作用。对于确定义务和责任以及确定分级管理和任务委派方案，这些角色都非常有用。

1.2.4 控制架构

为组织起草安全性立场通常会涉及很多事情，不只是写下几条远大的理想。在多数情况下，制定可靠的安全策略会涉及很多规划。许多读者可能认识到这个看似荒谬的概念，即召开会议为未来制定计划。事实证明，为安全制定计划必须从规划计划开始，然后规划标准和合规，最后再进行实际的计划开发和设计。跳过这些“规划计划”中的任何一步都可能使计划在开始之前就发生偏移。

安全计划步骤中最重要的一步，也是第一步，就是考虑组织想要的安全解决方案的整体控制框架或结构。可以从几个与安全性相关的概念基础设施中进行选择；而 CISSP 考试覆盖的一个方面是信息及相关技术控制目标(Control Objectives for Information and Related Technology，COBIT)。COBIT 记录了一整套优秀的 IT 安全实践，这些是由国际信息系统审计协会(Information System Audit and Control Association，ISACA)起草的。COBIT 规定了安全控制的目标和要求，鼓励将 IT 的理想安全目标映射到商业目标中。COBIT 5 的基础是企业 IT 治理和管理的 5 条关键原则：原则 1：满足利益相关者的需求；原则 2：对企业做到端到端的覆盖；原则 3：使用单一的集成框架；原则 4：使用整合处理法；原则 5：把治理从管理中分离出来。COBIT 不仅可用于计划组织的 IT 安全，也可以作为组织审计师的指导方针。

幸运的是，这一考试只是参考了COBIT的大体内容，不需要了解很多详细内容。但是如果对这个概念有兴趣，可访问ISACA网站(www.isaca.org)，或者如果想有个总体概览，可阅读维基百科对COBIT条目的解释。IT安全还有很多其他的标准和指导方针，包括《开源安全测试方法手册》(OSSTMM)、ISO/IEC 27002(取代了ISO 17799)和信息技术基础设施库(ITIL，更多信息可参见www.itlibrary.org)。

1.2.5 应尽关注和应尽职责

为什么规划安全计划如此重要？一个原因就是，这是应尽关注和应尽职责的要求。应尽关注是通过合理的关注保护组织利益。应尽职责是不断实践能够维持应尽关注成果的活动。例如，应尽关注会开发规范化的安全结构，这个结构会包含安全策略、标准、基线、指导方针和程序；而应尽职

责是继续将这个安全结构应用到机构的 IT 基础设施中。操作性安全需要组织内各责任方都能够对应尽关注和应尽职责保持持续不断的维护。

当今的商业环境，必须要谨慎。做到应尽关注与应尽职责是唯一能够证明损失发生不是因为疏忽的方法。高管必须做到应尽关注和应尽职责才能在出现损失时减少他们的过失和责任。

1.3　开发和文档化安全策略、标准、指导方针和程序

对于大多数的组织来说，维护安全性是业务发展的重要组成部分。如果安全受到严重危害，那么许多组织就无法正常运作。为了减少出现安全故障的可能性，已经在一定程度上规范了实现安全性的过程。这种规范化过程大大减少了为 IT 基础架构设计和实现安全解决方案中的混乱和复杂性(开发和实现文档化的安全策略、标准、指导方针和程序能产生坚实可靠的安全基础设施。安全解决方案的规范化采取了文档的分级组织形式，每个级别都关注信息和问题中的一个特定类型或类别。

1.3.1　安全策略

规范化的最高层次被称为安全策略。安全策略是一个文档，这个文档定义了组织所需的安全范围，并且讨论了需要保护的资产以及安全解决方案为提供必要保护而应当涉及的范围。安全策略概述或归纳了组织的安全需求，定义了主要的安全目标，并且概述了组织的安全架构。安全策略还确定了数据处理的主要功能领域，并且澄清和定义了所有相关的术语。安全策略应当清楚地定义为什么安全性很重要以及哪些资产是有价值的。它是实现安全性的战略计划。安全策略应当广泛地概括出用于保护组织切身利益的安全目标和原则。文档讨论了安全性对于日常营业每个方面的重要性以及高层职员对实现安全措施予以支持的重要性。安全策略被用于分配职责、定义角色、指定审计要求、概述实施过程、指明遵循要求以及定义可接受的风险级别。这个文档通常用于证明高层管理部门为保护不遭受入侵、攻击和灾难予以应有的关注。安全策略是强制性的。

许多组织都采用多种类型的安全策略来定义或概括它们整体的安全策略。组织安全策略的重点集中在与组织所有方面的相关问题上。特定问题的安全策略集中在特定的网络服务、部门、功能或有别于组织整体的其他方面。特定系统的安全策略关注个别系统或系统类型，并且规定了被认可的硬件和软件，概述了锁定系统的方法，甚至委托防火墙或其他特定的安全控制。

除了这些针对特定部分的安全策略类型以外，还有三种综合的安全策略类别；规章式的策略、建议式的策略和信息式的策略。只要行业或法律标准适用于你的组织，那么就需要规章式的策略(regulatory policy)。这种策略讨论了必须遵守的规章制度，并概略说明了用于让人们遵守规章制度的安全措施。建议式的策略(advisory policy)讨论可接受的行为和活动，并且定义违背安全性的后果。这种策略解释了高层管理部门对组织内部安全和遵守规定的期望。大多数安全策略都是建议性的。信息式的策略(informative policy)被设计用于提供特定主体的相关信息或知识，例如公司目标、任务声明或者组织如何与合作伙伴和客户进行交流。信息式的策略提供了与整个策略特定元素相关的支持、研究或背景信息。

从安全策略可以引出完整安全解决方案所需的其他很多文档或子元素。策略是广泛的概述，而标准、基准、指导方针和程序包括了更加特定的、详细的与实际安全解决方案有关的信息。标准处于安全策略的下一个层次。

安全策略与个体

作为一条经验法则，安全策略(以及标准、指南和程序)应当不针对特定的个体。安全策略并不为某个人分配任务和职责，而是为特定的角色定义任务和职责。这个角色可能具有行政管理控制或人员管理职责。因此，安全策略会定义安全基础架构内不同角色必须执行的操作，而不会定义哪些人负责做哪些事情。随后，这些已定义的角色作为工作描述或指定的工作任务被分配给个人。

可接受的使用策略

可接受的使用策略是一个常规生成的文档，它属于整个安全文档记录基础架构的一部分。可接受的使用策略被特别设计用于分配组织内的安全角色以及确保职责与这些角色相联系。此策略定义了可接受的性能级别以及对行为和动作的期望。不遵循该策略会导致工作行动警告、惩罚或解聘。

1.3.2 安全标准、基准及指南

一旦设定了主要的安全策略，就可以在这些策略的指导下拟定剩余的安全文档。标准为硬件、软件、技术和安全控制方法的统一使用定义了强制性要求。标准提供了操作过程，在这个过程中，整个组织内部统一实现技术和措施。标准是战术文档，定义了达到安全策略指定的目标和总体方向的步骤或方法。

下一个层次是基准。基准定义了安全性的最低级别，组织中的所有系统都必须达到基准要求。没有达到基准的所有系统都应该被排除在生产系统之外，直至这些系统被提升达到基准要求为止。基准建立了通用的安全状态基础，所有附加的和更严格的安全措施可以被建立在这个基础之上。基准通常是系统特定的，并且往往指的是行业或政府标准，例如可信任计算机系统评估标准(TCSEC)、信息技术安全评估和标准(ITSEC)以及 NIST(美国国家标准技术研究院)标准。

指南是规范化安全策略结构的下一个元素。指南提供了如何实现标准和基准的建议，并且能够作为安全专家和用户的操作指南。指南具有灵活性，因此为了适合每种特定的系统或条件，它们可以被定制，并且能够在新措施的创建过程中使用。指南说明了应当部署哪些安全机制，而不是规定特定的产品或控制以及详细的配置设置。指南概述了一套方法(包括行动建议)，但并非强制性的。

1.3.3 安全程序

程序是规范化安全策略结构的最后一个要素。程序是详细的、按部就班的指导文档，它描述了实现特定安全机制、控制或解决方案所需的确切行动。程序可以讨论整个系统的部署操作或者关注单个产品或方面，例如部署防火墙或更新病毒定义。大多数情况下，程序仅限于具体的系统和软件。随着系统硬件和软件的发展，程序必须被不断更新。程序的目的是确保业务流程的完整性。如果通过某个详细的程序能够达到所有目的，那么所有活动都应当遵循策略、标准和指导方针。程序有助于在所有系统之间确保安全性的标准化。

通常，策略、标准、基准、指导方针和程序只是在顾问或审计人员的敦促下，作为事后产生的想法进行发展。如果这些文档没有被使用和更新，那么安全环境的管理就无法将它们作为指南使用。如果没有这些文档提供的计划编制、设计、结构和监督，就无法维持环境的安全，也无法代表已经

尽责并给予适度的关注。

此外，开发一个包含上述所有元素方面的文档是一种惯用做法。事实上，我们应该避免这种做法。这些结构中的每一个都必须作为独立的实体存在，其原因在于每种结构执行不同的特殊功能。在规范化结构的顶层(也就是安全策略)，因为只包含全面的、一般性的观点和目标，所以文档较少。在规范化结构的较低层(也就是指南和程序)有比较多的文档，因为它们包含数量有限的系统、网络、部门和区域的特定详细信息。

将这些文档作为独立的实体保存，具有以下一些好处：

- 不是所有的用户都需要知道所有安全分类层次中的安全标准、基准、指导方针和程序。
- 当发生变化时，可以较为方便地只更新和重新分配受影响的资源，而不用更新整个策略以及在整个组织机构中进行重新分配。

拟定整个安全策略及所有支持性文档是一个令人畏惧的任务。许多组织只是致力于定义基本的安全参数，较少详细说明日常活动的每个方面。不过在理论上，详细和完整的安全策略以针对性的、有效的和特定的方式支持现实生活中的安全性。如果安全策略文档相当完整，就可以用于指导决策、培训新用户、回应问题以及预测未来的发展趋势。安全策略不应当是一种事后的考虑或想法，而应当是建立组织的一个关键部分。

对包含完整安全策略的文档的理解还有一些其他视角。图 1.6 展示了这些组件的依赖关系：策略、标准、指南和程序。安全策略是有组织的安全文档的总体结构的基础。然后，标准基于策略并受规章制度的管辖。指南从中衍生而来。最后，程序基于结构的三个基本层。使用倒金字塔来表示每个文档的体积或大小。完整安全策略中的程序通常都要比任何单个元素中的程序要多得多。相比较而言，指南要比策略少，标准也比策略少，并且通常整体或全组织范围内的安全策略甚至也更少。

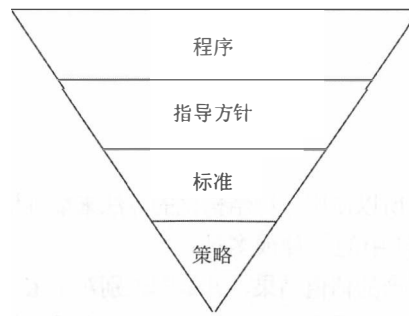


图 1.6　完全策略组件的比较关系

1.4　理解和应用威胁建模

威胁建模是潜在威胁被识别、分类和分析的安全流程。威胁建模在设计和开发过程中可以作为一种积极主动的措施执行，而产品一旦被部署，就会被作为一种被动式措施。在这两种情况下，流程会识别潜在危害、发生的概率、问题优先级以及消除或减少威胁的手段。

威胁建模并不意味着是一个单独的事件。相反，组织在系统设计流程早期就开始威胁建模并在整个系统周期内一直持续是很常见的。例如，微软使用安全开发生命周期(Security Development Lifecycle，SDL)流程在产品的每个开发阶段考虑和实现安全。这支撑了这句箴言：“设计安全、默认安全、部署和沟通安全”(也称为 SD3 + C)。这一流程有两个目标：

- 减少安全相关的设计和编码缺陷的数量
- 降低剩余缺陷的严重程度

换句话说，试图减少漏洞，降低任何存在缺陷的影响。总的结果是减少风险。

威胁建模的主动式方法发生于系统开发的早期阶段，特别是在初始设计和规范建立阶段。这种类型的威胁建模也被称为防御方式。这种方式基于编码和制作流程中对威胁的预测和特定防御中的设计，而不是依靠部署后的更新和补丁。大多数情况下，集成安全解决方案更符合成本效益，比后面硬塞的方案更成功。遗憾的是，并不是所有的威胁都可以在设计阶段预测出来，所以仍然需要被动式的威胁建模来解决不可预见的问题。

威胁建模的被动式方法发生在产品被创建和部署之后。此部署可以在测试或实验室环境中，或是指被部署到一般市场上。这种类型的威胁建模也被称为对抗方式。这种威胁建模的技术是道德黑客攻击、渗透测试、代码审查和模糊测试背后的核心概念。尽管这些流程通常有助于发现需要解决缺陷和威胁，但遗憾的是，它们需要额外的编码努力来增加到新对策中。从长远来看，回到设计阶段可能会产生更好的产品，但从头开始是非常昂贵的，并会造成产品发布时间的极大延迟。因此，捷径是在部署后精心制作需要增加到产品中的更新或补丁。这样的结果就是，可能在牺牲了功能性和用户友好性的前提下，也未带来更有效的安全改进(相比主动式威胁建模来说)。

注意：

模糊测试是一项专门的动态测试技术，它向软件提供了许多不同类型的输入，来强调其局限性并发现先前未被发现的缺陷。模糊测试软件向软件提供无效输入，可能是随机生成，也可能是专门制作以触发已知的软件漏洞。然后，模糊测试者会监控应用程序的性能，观察软件崩溃、缓冲区溢出或其他不良和/或不可预知的结果。可参考第 15 章“安全评估和测试”以查看更多有关模糊测试的内容。

1.4.1 识别威胁

可能的威胁几乎是无限的，所以使用一种结构化的方法来准确地识别相关威胁是很重要的。例如，一些组织使用以下三种方法中的一种或多种：

关注资产 这种方法使用资产的估值结果，并试图识别对于宝贵资产的威胁。例如，可以评估一个特定的资产，以确定其是否容易受到攻击。如果资产寄存着数据，则可以评估访问控制来识别能够绕过身份认证或授权机制的威胁。

关注攻击 一些组织能够识别潜在的攻击者，并能够基于攻击者的目标识别他们所代表的威胁。例如，政府往往能够识别潜在的攻击者，并识别攻击者想要达到的目标。然后他们可以使用这种知识来识别并保护他们的相关资产。这种方法面临的一个挑战是，可能会出现以往未被视为一种威胁的新攻击者。

关注软件 如果一个组织开发了一个软件，则可能会考虑针对软件的潜在威胁。尽管几年前组织一般不自己开发软件，但如今这已非常常见。具体地说，大多数组织都有网络存在，许多都创建了自己的网页。精美的网页带来更多的流量，但他们也需要更复杂的编程，并会受到更多的威胁。

如果威胁被确定为攻击者(而不是自然威胁)，那么威胁建模尝试确定攻击者可能会试图达到什么目的。有些攻击者可能想禁用系统，而其他攻击者可能想要窃取数据。一旦确认了这种威胁，就会基于目标或动机对他们进行分类。此外，将威胁和漏洞进行并列，来识别可能通过利用漏洞给组

织带来重大风险的常见威胁。威胁建模的一个终极目标就是优先处理针对组织宝贵资产的潜在威胁。

当试图对威胁进行盘点并分类时，使用指南或参考通常是有用的。微软开发了一个称为 STRIDE 的威胁分类方案。STRIDE 的使用经常与对应用程序或操作系统威胁的评估相关。然而，它也可以用于其他情境。STRIDE 是以下几个单词的首字母缩写：

- 电子欺骗(Spoofing)——通过使用伪造身份获得对目标系统访问的攻击行为。电子欺骗可以用于 IP 地址、MAC 地址、用户名、系统名称、无线网络名称、电子邮件地址以及许多其他类型的逻辑标识。当攻击者将自己伪装成一个合法或授权的实体时，他们往往能够绕过针对未授权访问的过滤器和封锁。一旦电子欺骗攻击让攻击者成功访问目标系统，后续的滥用、数据盗窃或特权提升攻击就都可以发起。
- 篡改(Tampering)——任何对数据进行未授权的更改或操纵的行为，不管是传输中的数据还是被存储的数据。使用篡改来伪造通信或改变静态信息。这种攻击是对完整性和可用性的侵害。
- 否认(Repudiation)——用户或攻击者否认执行了一个动作或行为的能力。通常攻击者会否认攻击，以便保持合理的推诿，从而不为自己的行为负责。否认攻击也可能会导致无辜的第三方因安全违规而受到指责。
- 信息披露(Information disclosure)——将私人、机密或受控信息揭露、传播给外部或未授权实体的行为。这可能包括客户身份信息、财务信息或自营业务操作细节。信息披露可以利用系统设计和实现错误，如未能删除调试代码、留下示例应用程序和账户、未对客户端可见内容的编程注释(如 HTML 文档中的注释)进行净化或将过于详细的错误消息暴露给用户。
- 拒绝服务(DoS)——指攻击试图阻止对资源的授权使用。这可以通过缺陷开发、连接重载或流量泛滥实现。DoS 攻击并不一定会导致对资源的完全中断；而是会减少吞吐量或造成延迟，以阻碍对资源的有效利用。尽管大多数 DoS 攻击都是暂时的，只在攻击者进行袭击时存在，但还是存在一些永久性的 DoS 攻击。永久 DoS 攻击可能涉及对数据集的破坏、使用恶意软件对软件进行替换，或强迫可以被打断或安装错误固件的固件 flash 操作。这些 DoS 攻击将造成系统的永久受损，使其不能使用简单的重启或通过等待攻击者结束而恢复正常操作。要从永久 DoS 攻击中恢复过来，将需要进行完整的系统修复和备份恢复。
- 权限提升(Elevation of privilege)——此攻击是指有限的用户账号被转换成拥有更大特权、权力和访问权的账户。这可能会通过盗窃或开发高级账户(如管理员或 root 账户)凭证来实现。有的系统或应用程序还可能会为原本有限的账户临时或永久授予额外权力。

STRIDE 虽然通常被专门用于应对应用程序威胁，但也适用于其他情况，比如网络威胁和主机威胁。其他的攻击可能会比网络和主机问题更具体，比如网络嗅探和劫持、恶意软件和主机的任意代码执行，但是 STRIDE 的 6 个威胁概念使用相当广泛。

一般来说，威胁建模中 STRIDE 和其他工具的目的是考虑被危害问题的范围，并关注攻击的目标或结果。试图识别每一个特定的攻击方法和技术是不可能完成的任务，因为新的攻击正在不断开发中。虽然攻击的目标或目的仅能粗略地进行分类和分组，但它们是保持相对稳定的。

警惕个人威胁

竞争通常是企业成长的一个关键部分，但过头的对抗性竞争会增加个人的威胁等级。除了黑客和心怀不满的雇员，对手、承包商、员工甚至是信赖的合作伙伴都可能由于关系的恶化而对组织形成威胁。

- 不要相信顾问或承包商对组织的忠诚度会如同长期员工一样。承包商和顾问实际上就是雇佣兵，谁出价高就为谁工作。也不要把员工的忠诚视为理所应当。员工如果对他们的工作环境感到不满或觉得他们受到了不公平待遇，就有可能试图报复。有经济困难的员工可能会有不道德行为和违法活动，他们为了自己的利益可能会对组织构成威胁。
- 可信的合作伙伴仅仅是值得信赖的伙伴，前提是你们各自的利益对彼此合作是友好的。如果最后的合作关系恶化或变得敌对，那么先前的伙伴可能会采取行动，对组织构成威胁。

组织的潜在威胁多种多样。公司面临的威胁可能来自自然环境、技术以及人。大多数组织在预防威胁上会关注自然灾害和 IT 攻击，但需要注意来自个人的潜在威胁同样重要。一定要事先想好企业活动、决策和交互行为带来的最好和最坏的可能结果。识别威胁是设计防御、减少故障、降低危害和避免损失的第一步。

1.4.2 确定和用图表示潜在攻击

一旦明白开发的项目或部署的基础设施可能面临的威胁，那么下一步是进行威胁建模，确定可能发生的潜在攻击概念。通常通过创建事务中的元素图表、数据流指向和特权边界来完成(见图 1.7)。

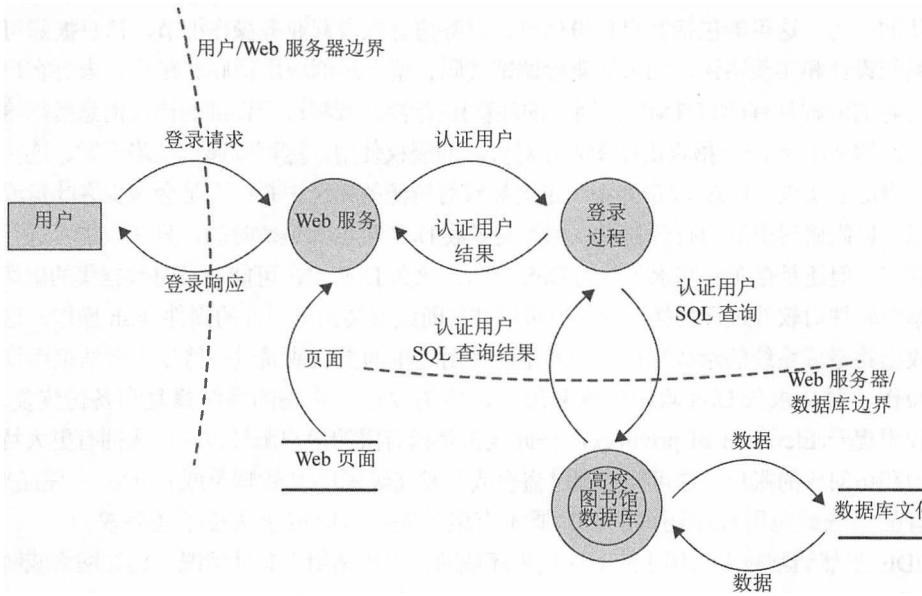


图 1.7 揭示威胁问题的图表实例

这些数据流图通过可视化表示，能更好地帮助理解资源和数据流动的关系。图表流程也被称为制作架构图。创建图表有助于详述商业任务、开发流程或工作活动中每个元素的功能和目的细节。一定要包括执行具体任务或操作的用户、处理器、应用程序、数据存储和所有其他的基本要素，这一点十分重要。该图表是一种高度概括，不是对编码逻辑的详细评估。然而，如果系统更复杂，则需要创建多个图表，关注不同的焦点且把细节进行不同程度的放大。

完成图表的创建后，要识别出图表中涉及的所有技术，包括操作系统、应用程序(基于网络服务和客户端)和协议。需要具体到使用的版本号和更新/补丁级别。

接着，识别可能对图表中每个元素发起的攻击。记住，要考虑到各种形式的攻击，包括逻辑/

技术、物理层面和社会层面的工具。例如，一定要包括电子欺骗、篡改和社交工程学。这个过程能很快帮助你进入威胁建模的下一阶段：执行降低分析。

1.4.3　执行降低分析

威胁建模的下一步是执行降低分析。执行降低分析是为了分解应用程序、系统或环境。这个任务的目的是更好地理解产品逻辑及其与外部的交互元素。不管是应用程序、系统还是整个环境，都需要被分成更小的容器或隔间。如果关注的是软件、电脑或操作系统，这些可能是子程序、模块或客体；如果关注的是系统或网络，这些可能是协议；如果关注的是企业的整个基础设施，这些可能是部门、任务和网络。应该对识别出的每个子元素进行评估，以便理解输入、处理、安全性、数据管理、存储和输出。

在这个分解流程中，必须了解 5 个关键概念：

- **信任边界**　信任或安全等级发生改变的位置。
- **数据流路径**　数据在两个位置之间的流动。
- **输入点**　接收外部输入的位置。
- **特权操作**　需要比标准用户账户或流程有更大特权的任何活动，通常需要进行系统修改或改变安全性。
- **安全立场和方法细节**　安全策略、安全基础和安全假设的声明。

把系统分解成各个组成部分能更容易识别每个元素的必要组件，同时也能注意到漏洞和攻击点。越能准确理解程序、系统或环境的运作方式，就越容易识别威胁。

1.4.4　优先级和响应

因为威胁要通过威胁建模进行识别，所以需要规定额外活动来完善整个流程。下一步是记录归档全部威胁。在文档编制中，应该对威胁的手段、目标和后果进行定义。要考虑实施某项开发可能需要的技术，以及列明潜在的对策和保障措施。

编制文档后，要对威胁进行排序或定级。可以利用各种技术完成这个过程，如使用概率×潜在损失的排名、高/中/低评级或 DREAD 系统。

概率×潜在损失的排名技术能产生一个代表风险严重性的编号，编号是从 1 到 100，100 代表可能发生的最严重的风险。概率和潜在损失的初始值可以在数字 1 到 10 之间指定，1 是最低，10 是最高。这些排名从某种层面看可以是武断或主观的，但因为同一个人或同一支团队会将编号分配给自己的组织，所以仍然应该在相对准确的偏差基础上准确估值。

高/中/低的评级流程更加简单。每个威胁都会被标注为这三种优先级标签中的一种。那些有高优先级标签的威胁需要立即解决。那些有中优先级标签的威胁最终也要解决，但无须立即采取行动。那些有低优先级标签的威胁可能需要解决，但如果解决这类威胁与整个项目相比需要付出很多的努力或费用，是否解决它们是可选的。

设计 DREAD 评级系统是为了提供灵活的评级解决方案，其基于对每种威胁的 5 个主要问题的回答：

- 潜在破坏——如果威胁成真，可能造成的损失有多严重？
- 再现性——攻击者重现这一漏洞有多复杂？

- 可利用性——实施攻击有多难?
- 受影响用户——有多少用户可能受到攻击的影响(按百分比)?
- 可发现性——攻击者发现弱点会有多难?

通过询问这些以及潜在的额外自定义问题，并对这些回答标注 H/M/L 或 3/2/1 值，就可以建立一张详细的威胁优先级表。

一旦设置了威胁的优先级，就需要确定对这些威胁的响应。应根据解决威胁的技术以及流程的成本和效率，对这些技术和流程进行考察权衡。反应选项应包括调整软件架构、改变操作和流程以及实现防御和检测组件。

1.5 把安全风险考虑到收购策略和实践中

将网络安全风险管理与收购策略和实践进行综合，是确保组织安全策略成功强健的一种手段，而不管机构的规模是什么样的。如果在没有考虑安全性的情况下贸然购买，那么所购买的这些产品的固有风险将在整个部署过程中一直存在。将收购元素的固有威胁最小化能减少安全管理成本，并且有可能减少安全违规。

选择带有弹性集成安全性的硬件、软件和服务往往比选择那些没有安全基础的产品和解决方案更贵一些。然而，这些额外的初始费用与满足不良设计产品安全需求的费用相比，通常更具成本效益。因此当考量收购成本时，很重要的一点是要考虑产品在整个部署周期内所有权的总花费，而不是只考虑初期购买和实施费用。

收购涉及的不只是软硬件，还包括外包、供应商承包和顾问咨询等。当与外部实体协同工作时，综合安全评估同确保产品设计考虑了安全因素一样重要。

许多情况下可能需要进行不间断的安全监测、管理和评估。可能会是行业的最佳实践或规章。组织内部可以进行这样的评估和监测，也可以由外部审计师进行。当有第三方参与评估和监控服务时，要记住，外部实体需要在他们的业务操作中体现出安全性意识。如果外部组织无法在安全的基础上管理他们自己的内部操作，那他们又将如何为你提供可靠安全的管理功能呢?

在为了安全整合而对第三方进行评估时，应考虑以下流程：

现场评估 访问该组织的网址，与其成员进行交谈并观察他们的操作习惯。

公文交换和审核 调查交换数据和文档的方式以及他们执行评估和审核的正式流程。

流程/策略审核 要求提供他们的安全策略、流程/程序、审查事件和响应文档的副本。

对所有的收购设立最低限度的安全需求。这些应该以现有的安全策略为模板。对新的硬件、软件或服务的安全要求，应该达到或超过现有基础设施的安全性。在处理外部服务时，一定要审查所有的 SLA(Service-Level Agreement，服务层级协议)，确保承包服务中有关于安全的规定。这可能包括根据特定需求定制服务层面的要求。这里有一些关于收购安全的不错资源：

- 通过收购提高网络安全和弹性。*Final Report of the Department of Defense and General Services Administration*(www.gsa.gov/portal/getMediaData?mediaId=185371)。
- NIST *Special Publication 800-64 Revision 2*：*Security Considerations in the System Development Life Cycle*(http://csrc.nist.gov/publications/nistpubs/800- 64-Rev2/SP800-64-Revision2.pdf)。

1.6　本章小结

安全治理、管理概念与原则是安全策略和解决方案部署中的固有元素。它们不仅定义了安全环境所需的基本参数，也定义了策略设计人员和系统实现人员为创建安全解决方案所必须达到的目的和目标。

安全性的主要目标和目的包含在 CIA 三元组中：机密性、完整性和可用性。这三条原则被认为是安全领域内最重要的原则。然而，每条原则对一个特定的组织究竟有多重要，主要取决于组织的安全目标和需求以及安全性所受到的威胁程度。

CIA 三元组的第一条原则是机密性，也就是客体不能暴露给未授权主体的原则。安全机制提供了机密性，也就为限制未授权主体不能访问数据、客体或资源提供了高级别保证。如果存在对机密性的威胁，那么就有可能发生未授权的泄漏。

CIA 三元组的第二条原则是完整性，也就是客体保持自身的正确性和只能由已授权主体进行有意识修改的原则。如果安全机制提供了完整性，也就对数据、客体和资源提供了保持原有受保护状态并不被修改的高级别保证，这包括当客体在存储、传输或处理过程中发生的变更。维护完整性意味着客体本身不会被改变，并且管理和操纵客体的操作系统与程序实体不会受到安全威胁。

CIA 三元组的第三条原则是可用性，也就是经过授权的主体被及时准许和不间断地访问客体的原则。如果安全机制提供了可用性，也就提供了经过授权的主体能够访问数据、客体和资源的高级别保证。可用性包括有效地、不间断地访问客体和阻止拒绝服务攻击。可用性还意味着支持基础设施的正常运作，并允许经过授权的用户获得被授权的访问权。

除了 CIA 三元组以外，在设计安全策略和部署安全解决方案时，还需要考虑其他很多与安全有关的概念和原则，包括隐私性、身份标识、身份认证、授权、可问责性、不可否认性和审计。

安全解决方案的概念和原则的其他方面是保护机制的元素：分层、抽象、数据隐藏以及加密。这些元素是安全控制的常见特性。并非所有的安全控制都必须具有这些元素，但是许多控制通过使用这些机制提供对机密性、完整性和可用性的保护。

安全角色决定谁对组织机构的资产安全负有责任。担任高管角色的人对任何资产损失最终负责和承担义务，并且对安全策略进行定义。安全专家负责实现安全策略，用户负责遵守安全策略。担任数据所有者角色的人负责对信息进行分类，数据管理员负责维护安全环境和备份数据。审计人员负责确认安全环境是否能恰当地保护资产。

规范化的安全策略结构由策略、标准、基准、指导方针和程序组成。这些独立的文档是在任何环境中设计和实现安全的必要元素。

安全管理实践中的一个重要方面是对变更的控制或管理。安全环境的改变很可能引入会导致新脆弱性出现的漏洞、重叠、客体丢失和疏漏。面对变更，能维持安全性的唯一方法是要系统地管理变化，这往往涉及对与安全控制和机制相关的活动进行广泛的日志记录、审计和监控。最终得到的数据随后用于确定变更的作用者，无论这些作用者是客体、主体、程序、通信路径还是网络本身。

数据分类是根据数据的秘密性、敏感性或机密性需求来保护数据的主要方式。在设计和实现安全系统时，因为某些数据项需要更高的安全性，所以对所有的数据采取同样的处理方法是低效率的。在较低的安全级别保护所有的数据，意味着敏感数据很容易被访问到。在较高的安全级别保护所有的数据，成本太高且对未分类的非关键数据的访问限制太多。数据分类用于确定需要分配多少工作量、资金和资源去保护数据以及控制对数据的访问。

安全管理计划的一个重要方面是实施适当的安全策略。为确保有效，安全管理方法必须是自上而下的。启用和定义安全策略的责任属于组织上层或高管人员。安全策略是为组织下层人员提供方向的。中层管理人员负责把安全政策充实为具体标准、基准、指导方针和步骤。对安全管理文件中预定的参数进行配置是运营经理或安全专家的责任。最后，最终用户的责任是要遵循组织的所有安全策略。

安全管理计划编制的元素包括：定义安全角色；开发安全策略；执行风险分析；以及要求对员工进行安全教育。这些职责要经过管理计划开发的指导。安全管理团队应当开发战略计划、战术计划和操作计划。

威胁建模是一种安全流程，能识别、分类和分析潜在威胁。威胁建模在设计开发阶段可作为一种提前措施来执行，或在产品被部署后作为一种被动性措施来执行。在这两种情况下，这个安全流程能识别潜在危害、发生概率、优先级问题以及消除或减少威胁的手段。

将网络安全风险管理与收购策略和实践进行综合，是确保组织安全策略成功和完善的一种手段，而不管组织的规模是什么样的。如果在没有考虑安全性的情况下贸然购买，所购买的这些产品的固有风险将在其整个部署过程中一直存在。

1.7 考试要点

理解 CIA 三元组的元素：机密性、完整性和可用性。机密性是客体不能暴露给未授权主体的原则。了解这条原则为什么重要、支持该原则的机制、针对该原则的攻击以及有效的对策。完整性是客体保持自身的正确性以及只能由已授权主体进行有意识修改的原则。了解这条原则为什么重要、支持该原则的机制、针对该原则的攻击以及有效的对策。可用性是经过授权的主体被及时准许和不被打断地访问客体的原则。了解这条原则为什么重要、支持该原则的机制、针对该原则的攻击以及有效的对策。

能够解释身份标识是如何工作的。身份标识是一个过程，在这个过程中，主体会表明身份，并且开始提供可问责性。主体必须向系统提供身份，从而启动身份认证、授权和可问责的过程。

理解身份认证的过程。认证或测试所声明身份合法性的过程就是身份认证。身份认证要求来自主体的附加信息必须完全对应于被表明的身份。

了解如何在安全计划中实现授权。一旦主体通过了身份认证，其访问还必须经过授权。授权的过程确保请求的活动或客体访问，可能获得了为通过身份认证的身份而指派的权利和特权。

理解安全治理。安全治理是关于组织支持、定义和指导安全工作的实践集合。

能够解释审计过程。审计或监控是程序化方式，通过这种方式，主体在系统中经过身份认证的行为是可问责的。审计也是对系统中未经授权的或异常的活动进行检测的过程。我们需要通过审计来检测主体的恶意行为、入侵企图和系统故障以及重构事件，为起诉提供证据、生成问题报告和分析结果。

理解可问责性的重要性。只有在支持可问责性时，组织的安全策略才能够被正确实施。换句话说，只有在主体的活动可问责时，才能够保持安全性。有效的可问责性依赖于检验主体身份以及跟踪其活动的能力。

能够解释不可否认性。不可否认性确保活动或事件的主体无法否认所发生的事件。不可否认性能够防止主体宣称自己没有发送消息、没有执行过某项活动或者不是某个事件的起因。

理解安全管理计划编制。安全管理基于三种类型的计划：战略计划、战术计划和操作计划。战略计划是长期计划，并且是相当稳定的，用于定义组织机构的目的、任务和目标。战术计划是中期计划，用来提供更加详细的实现战略计划所提出目标的计划。操作计划是短期计划，是基于战略和战术计划的非常周详的计划。

了解规范化安全策略结构的元素。为了生成全面的安全计划，需要适当地遵守下列要求：安全策略、标准、基准、指导方针和程序。这些文档清楚地描述了安全需求并反映了责任方的适度关注。

理解重要的安全角色。主要的安全角色有高层管理者、组织机构所有者、上层管理者、安全专家、用户、数据所有者、数据管理员以及审计人员。通过构建安全角色的层次，就可以全面限制风险。

了解如何实现安全意识培训。在真正的培训开始之前，必须为用户建立树立为公认实体的安全意识。一旦树立了安全意识，培训或教育员工执行工作任务和遵守安全策略就可以开始了。所有的新员工都需要进行培训，这样他们才能够遵守安全策略中规定的所有标准、指导方针和程序。教育是一项更细致的工作，学生/用户需要学习比他们完成工作任务实际所需知识多得多的知识。教育往往与用户参加认证考试或寻求职务晋升相关联。

了解分层如何简化安全。分层是串联使用多个控制层次。使用多层次解决方案，使用许多控制去防范威胁。

能够解释抽象的概念。抽象用于将相似的元素放入组、类别或角色(被整体性授予安全控制、限制或权限)中，抽象提高了实施安全计划的效率。

理解数据隐藏。顾名思义，数据隐藏防止主体发现或访问数据。在安全控制和程序设计中，数据隐藏通常是一个关键要素。

理解对加密的需求。加密是对计划外的接收者隐藏通信数据的含义或意图的一种艺术和学科。加密可以具有很多形式，并且能够用于所有的电子通信类型，包括文本、音频和视频文件以及应用程序本身。加密技术是安全控制中一个非常重要的元素，尤其系统之间的数据传输更是如此。

能够解释更改控制和更改管理的概念。安全环境的改变很可能引入会导致新脆弱性出现的漏洞、重叠、客体丢失和疏漏。面对更改，维持安全性的唯一方法是系统地管理更改。

了解为什么和如何进行数据分类。数据分类旨在简化给客体组(而不是单独客体)分配安全控制的过程。两种通用的分类方案是政府/军方分类和商业/私营部门分类。了解政府/军方分类中的 5 个级别和商业/私营部门分类中的 4 个级别。

理解解除分类的重要性。一旦某个资产不再需要当前分配的分类或敏感性级别保护，就需要解除分类。

了解 COBIT 的基础知识。信息及相关技术控制目标(COBIT)是一种安全概念基础架构，用于组织公司的复杂安全解决方案。

了解威胁建模的基础知识。威胁建模是一种安全流程，能识别、分类和分析潜在威胁。威胁建模在设计开发阶段可作为一种提前措施来执行，或在产品被部署后作为一种被动性措施来执行。关键概念包括资产/攻击者/软件、STRIDE、图形表示、约简/分解和 DREAD。

了解安全并购的必要性。将网络安全风险管理与收购策略和实践进行综合是确保组织的安全策略成功强健的一种手段，而不管组织的规模是什么样的。如果在没有考虑安全性的情况下贸然购买，所购买的这些产品的固有风险将在其整个部署过程中一直存在。

1.8 书面实验室

1. 讨论和描述 CIA 三元组。
2. 为了能够问责与特定用户账户相关联人员的活动，具体有哪些需求？
3. 描述变更控制管理的优点。
4. 实现分类方案的 7 个主要步骤是什么？
5. 指出(ISC)^2 为 CISSP 定义的 6 种主要安全角色。
6. 完整的组织安全策略的 4 个组成部分及其基本目的是什么？

1.9 复习题

1. 下列哪一项包含安全性的主要目标和目的？
   A. 网络的外围边界
   B. CIA 三元组
   C. 一个独立的系统
   D. 互联网
2. 脆弱性和风险是基于它们对下列哪一项的威胁评估？
   A. 一条或多条 CIA 三元组原则
   B. 数据有效性
   C. 应尽关注
   D. 责任范围
3. 下列哪一项在 CIA 三元组原则中用于说明授权主体被及时授予和不间断地访问对象？
   A. 识别
   B. 可用性
   C. 加密
   D. 分层
4. 下列哪一项不被视为违反保密性？
   A. 窃取密码
   B. 窃听
   C. 硬件破坏
   D. 社会工程学
5. 下列哪一项是不正确的？
   A. 保密性的违反包括人为错误。
   B. 保密性的违反包括管理监督。
   C. 保密性的违反仅限于直接故意攻击。
   D. 当传输未正确加密时保密性违反可能发生。
6. STRIDE 通常与用于评估针对应用程序或操作系统的威胁有关。以下哪一项不是 STRIDE 的元素？
   A. 欺骗

B. 权限提升
C. 否认
D. 披露

7. 如果一个安全机制提供可用性，也就提供了高级别保证，该授权对象可以 _____ 数据、对象和资源。

A. 控制
B. 审计
C. 访问
D. 否认

8. _____指的是保持信息的机密性，防止一旦泄露，个人身份可能造成伤害、尴尬或丢人。

A. 隐居
B. 隐蔽
C. 隐私
D. 临界

9. 对于所有个人的影响，除了下面哪一项以外都需要注意？

A. 制约个人电子邮件
B. 记录电话交谈
C. 收集关于上网习惯的信息
D. 用于保留电子邮件的备份机制

10. 数据分类管理的什么元素可以覆盖所有其他访问控制的形式？

A. 分类
B. 物理访问
C. 监管者职责
D. 取得所有权

11. 什么确保了活动或事件的主体不能否认发生过的事件？

A. CIA 三元组
B. 抽象
C. 不可否认性
D. 哈希总数

12. 以下哪一项相对于分层安全是最重要和独特的概念？

A. 多层
B. 系列
C. 并行
D. 过滤

13. 下列哪一项不被认为是数据隐藏的例子？

A. 防止对象的授权阅读者删除该对象
B. 阻止未经授权的访问者访问数据库
C. 限制较低级别的主体访问较高级别的数据
D. 阻止应用程序直接访问硬件

14. 变更管理的主要目标是什么？
   A. 维护文档
   B. 保持用户得到变更通知
   C. 允许失败变更的回滚
   D. 防止安全危害
15. 数据分类方案的主要目标是什么？
   A. 控制授权主体访问对象
   B. 为了形式化和根据重要性和敏感性分配标签以分层保护数据的过程
   C. 为审计可问责性建立交易跟踪
   D. 为操作访问控制以提供最有效的手段来授予或限制功能
16. 在分类数据时，下列哪一项通常是不考虑的特征？
   A. 价值
   B. 物体的大小
   C. 使用寿命
   D. 国家安全的影响
17. 两种常见的数据分类方案是哪些？
   A. 军事和私营部门
   B. 个人和政府
   C. 私营部门和非限制性行业
   D. 分类和未分类
18. 下列哪一项是机密数据的最低军事数据分类？
   A. 敏感
   B. 机密
   C. 专有
   D. 隐私
19. 下列商业/私营部门的哪一个数据分类用来控制组织内的个人信息？
   A. 机密
   B. 隐私
   C. 敏感
   D. 专有
20. 数据分类都用于关注安全控制，除了以下哪一个？
   A. 存储
   B. 处理
   C. 分层
   D. 转移

第 2 章

人员安全和风险管理概念

本章中覆盖的 CISSP 考试大纲包含：

安全和风险管理(例如安全、风险、合规性、法律、法规、业务连续性)

- H. 促进人员安全策略
  - H.1 筛选候选人(例如背景检测、教育核查)
  - H.2 雇佣协议和策略
  - H.3 解雇员工的流程
  - H.4 供货商、顾问和承包商控制
  - H.5 合规性
  - H.6 隐私
- I. 理解和应用风险管理的概念
  - I.1 识别威胁和脆弱性
  - I.2 风险评估/分析(定性、定量、混合)
  - I.3 风险分配/接受(例如系统授权)
  - I.4 措施选择
  - I.5 实施
  - I.6 控制类型(阻止、检测、纠正等)
  - I.7 控制评估
  - I.8 监控和测量
  - I.9 资产评估
  - I.10 报告
  - I.11 持续改进
  - I.12 风险框架
- L. 建立和管理信息安全教育、培训和意识
  - L.1 适合组织需要的水平的安全意识、培训和教育
  - L.2 定期的内容相关审查

安全评估与测试(设计、执行和分析安全测试)

- C.5 培训和意识

在 CISSP 认证考试中，通用知识体系(CBK)的安全和风险管理领域涉及许多安全解决方案的基本元素。其中，安全机制的设计、执行以及管理都是必不可少的基本元素。

安全和风险管理领域的附加元素在如下许多章都有讨论：第 1 章，“通过原则和策略的安全治理”；第 3 章，“业务连续性计划”；以及第 4 章，“法律、法规和合规性”。请一定复习这些章，以便能够从一个完整的角度来讨论安全和风险管理领域的相关话题。

由于硬件和软件控制的复杂性和重要性，在整个安全计划编制中，针对员工的安全管理往往会被忽略。本章从确定安全雇佣过程和工作描述到开发员工基础架构，从人的角度探讨了安全性。此外，员工的培训、管理和解雇过程被视为创建安全环境的一个不可或缺的部分。最后，我们将介绍如何评估和管理安全风险。

2.1 促进人员安全策略

在任何安全解决方案中，人都是最薄弱的环节。无论部署怎样的物理或逻辑控制，人总能发现避免受到控制、回避或消除控制以及禁用控制的方法。因此，在为自己所处的环境设计和部署安全解决方案时，要将用户的人性因素考虑进去，这一点非常重要。

在开发安全解决方案的所有阶段，都会产生与人有关的论点、问题和折中方案。这是因为人贯穿了任何解决方案的整个开发、部署和持续管理过程。因此，我们必须评估用户、设计人员、编程人员、开发人员、经理以及实现人员在这个过程中的作用。

雇佣新的职员通常涉及几个明确的步骤：创建工作描述、设置工作分类、筛选候选人、雇佣和培训最适合这项工作的人。如果没有工作描述，就不能形成应该雇佣何种类型人员的统一意见。因此，在定义与即将被雇佣人员有关的安全需求时，创建工作描述是第一步。因为有对人员特殊技能和经验的要求，所以组织应该增加人手。组织内部对任何职位的工作描述，都应该确定相关的安全问题。必须考虑到一些相关事宜，例如，是否需要这个职位处理敏感资料或访问分类的信息。实际上，工作描述定义了为了完成工作任务而需要为员工分配的角色。工作描述应该对职位所要求的访问安全网络的类型和范围进行定义。一旦确定了这些问题，为工作描述分配的安全类别就相当标准了。

提示：工作描述的重要性

对于实现和支持安全解决方案来说，工作描述十分重要。然而，许多组织要么忽略工作描述，要么工作描述陈旧和脱离实际。看看能否找到自己的工作描述。有这样的工作描述吗？如果有的话，那么最近一次更新是什么时候？工作描述能否反映所做的工作？工作描述是否说明了履行特定工作职责所需的安全访问类型？有些组织必须精巧地设计工作描述以符合 SOC-2，而其他符合 ISO27001 要求的工作描述需要按年度审查。

如下所示，在构建工作描述方面的重要元素包括职责分离、工作职责和岗位轮换：

职责分离 职责分离属于安全概念，是指把关键的、重要的和敏感的工作任务分配给若干不同的管理员或高级执行者(见图 2.1)。这样做能阻止任何一个人具备破坏或削弱重要安全机制的能力。可以将职责分离视为对管理员的最小特权原则的应用。职责分离也能够防止共谋，共谋指的是负面

活动由两人或多人共同完成，其意图往往是伪造、偷窃或间谍行为。

管理任务	数据库管理	防火墙管理	用户账户管理	文件管理	网络管理
指派管理员	管理员 1	管理员 2	管理员 3 & 4	管理员 5	管理员 6 & 7

图 2.1　关于 5 个管理任务和 7 个管理员职责分离的例子

工作职责　工作职责是要求员工在常规的基础上执行的特定工作任务。根据他们的职责，员工需要访问各种不同的对象、资源和服务。在安全的网络上，用户必须被授予访问与其工作任务有关元素的权限。为了保持最大的安全性，应该按照最小特权原则分配访问权限。最小特权原则规定：在安全环境中，应该授予用户完成工作任务或工作职责所必需的最小访问权限。这条原则的实际应用要求对所有资源和功能进行低级别的粒度访问控制。

岗位轮换　岗位轮换是一种简单的方法，组织通过让员工在不同的工作岗位间轮换职位来提高整体安全性(见图 2.2)。岗位轮换有两个作用。首先，它提供了一种知识冗余类型。当许多员工中的每一位都有能力胜任所要求的若干工作岗位时，如果因为疾病或其他事件导致一位或多位员工在较长的时间内无法工作，那么组织遭受严重停工或生产效率降低的可能性就较小。

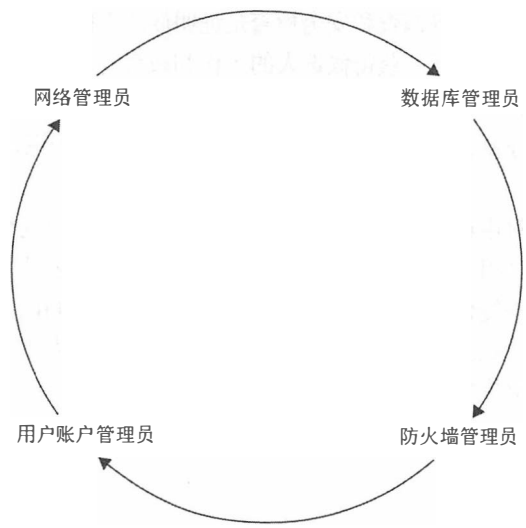


图 2.2　管理职位间岗位轮换的例子

其次，人员流动可以减少伪造、数据更改、偷窃、阴谋破坏和信息滥用的风险。员工在一个特定岗位工作的时间越长，就越有可能为他们分配额外的工作任务，从而扩展了他们的特权和访问权限。由于个人逐渐熟悉了自己的工作任务，因此很可能为了个人利益或恶意报复而滥用特权。如果某位员工误用或滥用特权，那么就很容易被另一位了解该工作岗位和工作职责的员工发现。因此，

岗位轮换也提供了一种同级审计形式，并且能够防止共谋。

交叉训练

交叉训练通常被作为工作轮换的另一种方法进行探讨。在这两种情况下，员工都可以了解到多个工作岗位的职责。然而，在交叉训练中仅要求员工履行其他工作岗位的职责；员工并不是定期地轮换工作岗位。在找不到合适员工的情况下，交叉训练能够利用现有的人才填补职位空缺，是一种应急预案。

当几个人一起共同犯罪时，这被称为共谋。由于将职责分离、限制工作职责和提供岗位轮换组合在一起，因此导致共谋被发现的风险性更高，这使得同谋愿意参加非法活动或滥用职权的可能性降低。共谋和特权滥用可以通过严格的权限监控得以减少，例如管理员、备份操作员、用户管理人员以及其他人员。

工作描述不能只在雇佣过程中使用，还应当在组织的整个生命周期中被维护。只有通过详细的工作描述，才能将员工应该担负的责任与他实际上所担负的责任做比较。这个管理性任务必须确保工作描述的重叠性尽可能小，并且一位员工的职责与另一位员工的职责没有出现偏移或侵占的情况。同样，经理应该对权限分配进行审计，从而确保员工只能获得完成工作任务所需的访问权限。

2.1.1 筛选候选人

为特定的职位筛选候选人时，是以工作描述中定义的敏感程度和分类级别为基础的。特定职位的敏感程度和分类级别依赖于该职位的员工无意或有意违反安全性所造成的危害程度。因此，筛选员工的全过程应当反映如何满足职位的安全性要求。

对于职位的安全性来说，背景调查和安全检查是证明候选人能够胜任工作、具备工作资格和值得信赖的必要因素。背景调查包括：获得候选人的工作和教育历史记录；检查证明材料；与候选人的同事、邻居和朋友进行会面；向公安局和政府机关调查候选人的拘捕或违法活动记录；通过指纹、驾驶执照和出生证明来认证身份；以及进行面试。此外还可以采用测谎仪、药检、性格测试/评估等形式。

对于许多组织而言，对申请人进行在线背景调查和社交网络账户复审已经成为一种标准惯例。如果一个潜在的员工向这些组织的图片分享网站、社交网络档案或公共即时信息服务平台发送不适当的材料，他们就没有那些提供相称材料的求职者更受青睐。当我们以文档、图片或视频的形式记录材料，并发布在网上时，我们的这些行为在公众的视野中就会成为永久不断的。通过查看一个人的网络身份，我们可以很快收集到这个人的态度、智力、忠诚、常识、勤奋、诚实、尊重、坚定性、遵守社会准则以及企业文化等方面的大致情况。

2.1.2 雇佣协议和策略

雇佣新员工时，应该签署雇佣协议。协议文档概略说明了组织的规则和限制、安全策略、可接受的使用和行为准则、详细的工作描述、破坏活动及其后果、要求员工胜任工作所需的时间。其中，很多条目都是独立的文档。这种情况下，雇佣协议用来确认所雇佣的候选人已经阅读并了解了与他们所期望工作职位相关联的文档。

除了雇佣协议以外，还必须确定其他与安全相关的文档。一个通用的文档是保密协议(NonDisclosure Agreement，NDA)。NDA 用来保护组织的机密信息不会被以前的员工泄漏。当员工签署 NDA 时，他们同意不对组织外的任何人泄露被定义为机密级的信息。违反了 NDA 的行为常常会遭到严厉的处罚。

真实场景

NCA：同样具有限制作用的 NDA 的孪生协议

NDA 通常与竞业禁止协议(NonCompete Agreement，NCA)同时存在。竞业禁止协议试图阻止格外了解组织秘密的员工加入另一个存在竞争关系的组织，从而使第二个组织不能受益于该员工所了解的秘密。NCA 还用于防止员工因为高薪或其他诱惑而跳槽到其他的公司。通常，NCA 具有时间限制，例如半年、一年甚至三年。NCA 的目标是：通常保持人力资源为自己的利益服务(而不是反戈一击)，从而准许原来的公司维持自己的竞争优势。

许多公司都要求新雇佣的员工签署 NCA。然而，在法庭上完全实现 NCA 的效力是极为困难的。法庭认可员工为了保障自己和家庭的生活，允许使用所具备的技能和知识谋取工作的情况。如果 NCA 妨碍员工获得适当的收入，那么法庭通常会认为 NCA 无效，或者阻止协议的约定结果成为现实。

即使 NCA 在法庭上并非总是可强制实施，但是这并不意味着原来的公司无法获得利益：

- 首先，由于违反 NCA 导致的诉讼威胁，常常足以阻止员工在新公司工作时违反秘密条款。
- 其次，如果员工确实违反了 NCA 的条款，那么即使由于法庭限制无法实现特别定义的约定结果，法庭审理的漫长时间和耗费的精力(更不必说花费的金钱)也足以让人望而生畏了。

在被雇佣时，你是否签署了 NCA？如果签署了 NCA，那么你是否了解各种条款以及违反 NCA 的潜在后果？

在员工的整个雇佣期内，经理应当定期审计每一位员工的工作描述、工作任务和特权等。随着时间的推移，工作任务和特权通常会发生偏差，这会导致一些任务被忽略，而其他一些任务又被多次重复执行。偏差还会导致违反安全性的行为。定期审查每一种工作描述中定义的界限与实际界限的关系，有助于保持安全破坏程度的最小化。

这个审查过程的关键部分是强制性休假。在许多安全环境中，一到两个星期的强制性休假被用于审计和认证员工的工作任务和特权。此时，这位员工暂时离开自己的工作环境，另一名员工接替其工作。通过这种做法，往往很容易发现滥用、伪造或疏忽行为。

2.1.3　解雇员工的流程

需要解雇某位员工时，必须解决很多问题。在解雇过程中，安全部门和 HR 之间的紧密关系对于维护控制和最小化风险是很重要的。对于维护安全环境来说，解雇过程或策略是必要的，即使是面对一位必须离开组织的、心怀不满的员工也同样如此。被解雇员工的反应大相径庭，包括从平静、理解接收到反应强烈乃至破坏性的狂怒。必须设计和实施合理的解雇过程，以便减少不愉快事件的发生。

处理解雇员工事宜时，应该采取不公开的和尊重人的方式。然而，这并非意味着不应当采取防

范措施。终止合同时应该至少有一位证人在场，证人最好是高层经理和/或安保人员。一旦员工被告知离职，他们应该被立刻护送离开，并且不允许通过任何理由返回办公地点。员工在被解雇离开之前，组织特有的所有身份证件、访问权限或员工安全标志以及门卡、钥匙和出入证都应该被收回(见图 2.3)。通常，解雇员工的最佳时间是员工轮班结束时。在一周的早期和中期解雇员工可以让这个前雇员有时间去申请失业和/或在周末前开始寻找新的就业机会。同时，换班时解雇员工可以让员工以一种更加自然的方式告别其他员工，这样可以减少压力。

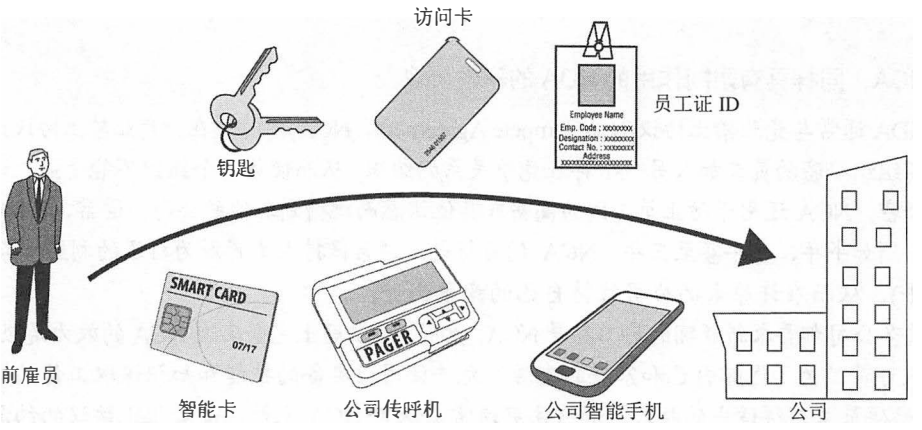


图 2.3　前雇员必须归还所有公司资产

如果有可能，那么应该进行一次离职面谈。然而，这种做法通常依赖于员工面对解雇和其他因素时的心理状态。如果离职面谈无法在解雇时立刻进行，那么应该越快越好。离职面谈的主要目的是：根据前雇员签署的雇佣协议、保密协议和其他安全相关文档来审查责任和约束条件。

以下列出了应该尽快处理的其他事宜：

- 确认员工已归还放在交通工具或家中的组织配发的装置或供应品。
- 删除或禁用员工的网络用户账号。
- 通知人力资源部门支付最后的薪水，把未使用的休假换成工资，终止所有的福利待遇。
- 安排安全部门的人员陪同被解雇的员工在工作场所收拾他们的个人物品。
- 通知所有安全人员以及监控出入口的其他人员，确保被解雇的员工只能在安全人员护送下再次进入工作场所。

大多数情况下，应该在通知员工被解雇的同时或之前就禁止或删除此员工对系统的访问权限。如果被解雇的员工仍然能够访问机密数据，或者通过访问权限去修改、损坏数据和服务，那么更需如此。如果没能对被解雇员工的行为进行限制，就会给组织留下广泛的脆弱性，包括对物理财产和逻辑数据的窃取和破坏。

真实场景

解雇：不仅仅是解雇通知书

解雇员工是一个复杂的过程。将解雇通知书直接放入员工邮箱的做法已经行不通了。在大多数以 IT 为中心的组织中，终止工作合同可能使员工或公司处于被危害或导致危害的风险之中。因此，我们需要精心设计面谈过程。

然而，只有面谈过程是不够的。毫无疑问，每次解雇都应该恰当地进行会谈。遗憾的是，历史上存在许多没有进行离职面谈的实例。你甚至可能听说过一些由匆忙的面谈过程导致的惨痛后果，常见的示例包括在实际通知员工之前执行下列所有操作(因而对要解雇的员工进行事先警告):

- IT 部门要求返回笔记本电脑。
- 禁用网络账户。
- 阻止某人的 PIN 或智能卡被用于进入工作场所。
- 废除某个停车证。
- 分发公司的重组图表。
- 在狭小的工作空间内安置一名新员工。
- 准许将解雇信息泄漏给中介。

不用说，为了使离职面谈和安全解雇过程能够正常运作，就必须在正确的时间(也就是离职面谈的开始时间)按照正确的顺序实施这些过程，例如以下的例子:

- 告知其他人，他们已被解除工作。
- 要求收回所有的访问徽章、钥匙和公司设备。
- 禁止此人电子访问组织的各个方面。
- 提醒此人关于 NDA 的责任。
- 护送此人离开建筑物。

2.1.4　供应商、顾问和承包商控制

利用供应商、顾问以及承包商控制来确定这个主要组织外部的不同实体、个人或组织的绩效水平、期望值高低、薪酬水平以及影响程度。通常情况下，在服务级别协议(Service-Level Agreement，SLA)的文件或策略中会对这些控制进行明确规定。

利用 SLA 确保组织向其内部和(或)外部客户提供的各种服务，能够维持在服务提供商和供应商双方达成一致的适当服务水平上，这种方式越来越受欢迎。将 SLA 适当应用于任何数据电路、应用程序、信息处理系统、数据库或其他对组织持续生存能力至关重要的部分，是一种明智之举。在使用任何类型的第三方服务提供商时，SLA 尤为重要，这其中包括云服务。如下是在 SLA 中处理的常见问题:

- 系统运行时间(作为总体运行时间的百分比)
- 最长连续停机时间(以秒或分钟等计算)
- 最大负载
- 平均负载
- 诊断任务
- 故障转移时间(如果冗余处于适当位置)

SLA 通常还包括财务和其他合同补救措施。如果这份协议得不到维护，那么这些补救措施将开始生效。例如，如果一条关键回路出现故障的时间长达 15 分钟以上，那么服务提供商可能同意免除这条回路一周的所有费用。

SLA 以及供应商、顾问和承包商控制是降低风险和回避风险的一个重要部分。通过明确地定义外部单位的期望值和处罚，所涉及的每个人都应知道他们所期待的是什么，以及万一达不到期望值会出现什么样的后果。利用外部提供商来提供许多商业功能或服务，价格可能非常划算，但是潜在

的风险也会随着攻击面的扩展和漏洞范围的扩大而增大。除了确保优质适时的服务和合理的价格外，SLA 还应包括一个重点，就是保护和完善安全机制。

2.1.5 合规性

合规是符合或遵守规则、策略、法规、标准或要求的行为。合规性对安全治理来说是一个重要的问题。在人员层面，合规性涉及的是员工个体是否遵守公司策略以及是否按照定义的程序来执行他们的工作任务。许多组织依靠员工的合规性来保证高质量、一致性、效率和节约成本。如果员工不坚持合规性，组织的利润、市场份额、公认度和声誉可能就会受损。员工需要接受培训，以便知道他们需要做什么；只有这样，如果出现违规或缺乏合规，才可能追究他们的责任。

2.1.6 隐私

隐私是一个难以定义的概念。通常，在很多环境中使用这个术语时并没有进行定量或定性。下面列出了一些对隐私性的可能定义：

- 主动防止对个人可确认的信息(也就是与某人或某个组织直接联系的数据点)的未授权访问。
- 防止对被视为个人的或秘密的信息进行未授权的访问。
- 防止未被同意或知晓的观察、监控或检查行为。

注意：

在讨论隐私性时经常出现的一个概念是个人身份信息(Personally Identifiable Information，PII)。*PII 是可以很容易地和/或明显地追溯到源头的人或涉及人的任何数据项。电话号码、电子邮件地址、邮寄地址、社会保障号和名字都是* PII。*MAC 地址、IP 地址、操作系统类型、最喜欢的度假地点、高中吉祥物的名字等一般不是* PII。

在 IT 领域内解决隐私性问题时，通常需要在个人权限和组织的权力或活动之间达到平衡。某些人认为，个人有权控制是否能收集他们的信息以及如何处置这些信息。其他人则认为，在公共场合执行的任何活动(例如，在互联网上执行的大多数活动或者在公司设备上执行的活动)，可以在不必通知或得到被监视人授权的情况下而被监控，而且只要组织认为合适或值得，通过监控收集的信息就可以用于任何目的。

保护个人免于遭受不希望的监控、产品直销以及不暴露个人隐私性或秘密资料的努力，被认为是值得的。然而另一方面，一些组织宣称通过人口统计学研究、收集信息和关注市场能够改进业务模式、减少广告浪费以及节省所有人的支出。

有许多关于隐私性立法和合规性的问题。许多美国法案中都有关于隐私的要求，如《健康保险流通与责任法案》(HIPAA)、2002 年的《萨班斯-奥克斯利法案》(SOX)和《金融服务现代化法案》以及欧盟指令 95/46/EC(又名数据保护指令)和合同要求《支付卡行业数据安全标准》(PCI DSS)。重要的是，要理解你所在的组织需要遵从的所有政府规定，并保证合规性，尤其是在隐私保护的地区。

无论个人或组织对网上个人隐私性问题的态度如何，都必须在组织的安全策略中被确定。隐私性不仅是外部访问者对提供的联机信息进行访问的问题，而且也是客户、员工、供应商和承包商的问题。如果要收集与个人或公司相关的任何类型信息，那么必须解决隐私性问题。

大多数情况下，特别是当隐私性被破坏或受到限制时，必须通知个人和公司，否则可能面对法

律上的纠纷。当允许或限制个人使用电子邮件、保留电子邮件、记录电话谈话、收集有关网上冲浪或消费习惯时，同样必须解决隐私性问题。

2.2　安全治理

安全治理是与支持、定义和指导组织安全工作相关的实践集合。安全治理经常与企业和 IT 治理密切相关，并交织在一起。这三种治理议程的目标常常相互关联或者都是相同的。例如，组织治理的一个共同目标是确保组织将继续存在并随着时间的推移成长或扩大。因此，三种治理形式的目标都是维持业务流程，同时努力追求增长和弹性。

第三方治理是可能由法律、法规、行业标准、合同义务或许可要求规定的监督制度。实际的治理方法可能有所不同，但通常包括外部人员或审计人员。这些审计人员可能会由管理组织指定，也可能是目标组织雇佣的顾问。

第三方治理的另一个方面是将安全监督应用到组织所依赖的第三方。许多组织选择将他们业务的各个方面外包出去。外包业务可能会包括保安、维修、技术支持和会计服务。第三方需要遵从主要组织的安全立场。否则，他们就会对主要组织带来额外的风险和漏洞。

第三方治理重点认证对所述安全目标、要求、法规和合同义务的合规性。现场评估可以为在某个位置使用的安全机制提供第一手信息。那些在现场执行的评估或审计需要遵循审计协议(如 COBIT)，并有一个特定的要求检查表来进行调查。

在审计和评估过程中，目标和管理组织都应当参与全面和开放的文档交换和审查。组织需要知道必须遵守的要求的全部细节。组织应向管理组织提交安全策略和自我评估报告。这种开放的文档交换确保各方在所有问题上达成一致，减少了未知需求或不切实际的期望的机会。文档交换不以文件或电子文件的传输而结束，相反，它通向文档审查的过程。

文档审查是阅读交换材料并利用标准和期望对其进行检验的过程。文档审查通常会在现场检查开始前执行。如果交换文档是充分的、符合预期的(或至少满足要求)，那么现场审查就能够专注于对所述文档的遵守。然而，如果文档不完整、不准确或不够，现场审核可能就要被推迟，直到对文档进行了更新和修正。这一步很重要，因为如果文档不合规，很有可能位置也不合规。

在许多情况下，尤其是与政府或军事机构或承包商有关时，未能提供足够的文档来满足第三方治理的需求可能会导致授权操作(ATO)的损失或无效。完整和充分的文档通常可以维持现有 ATO 或提供临时的 ATO(TATO)。然而，一旦 ATO 丢失或撤消，那么要重建 ATO，就必须有显示完全合规的完整的文档审查和现场审查。

文档审查的一部分是对业务流程和组织策略的逻辑和实际调查。这一审查确保声明和实施的业务任务以及系统和方法是实用、高效和成本有效的，最重要的是(至少在有关安全治理方面)，它们可以通过减少漏洞以及避免、减少或缓解风险来支持安全目标。风险管理、风险评估和风险解决都是在执行流程/策略评估中涉及的方法和技术。

2.3　理解和应用风险管理概念

安全性的目的是在维护经过授权的访问时，防止数据的丢失或泄露。可能发生造成数据损坏、毁坏或泄露的事情被称为风险。了解风险管理的概念不仅是 CISSP 考试的重点，也是建立充分的安

全状态、适当的安全治理和应尽关注、应尽职责的法律证明的根本。

因此，管理风险是维护安全环境的一个元素。风险管理是一个详细的过程，包括识别可能造成数据损坏或泄漏的因素，根据数据的价值与对策的成本来评估这些因素，以及为了减轻或降低风险而实现有成本效益的解决方案。风险管理的整个过程被用来制定和实施信息安全策略。这些策略的目标是减少风险和支持组织的使命。

风险管理的主要目的是要将风险降低到一个可以接受的级别。究竟要达到哪一个级别，这主要取决于组织、其资产的价值、预算的多少以及其他许多因素。某个组织认为可接受的风险对于另一个组织来说可能是完全不合理的、过高的风险级别。设计并实现一个完全没有风险的环境是不可能的，但是，显著地减少可能出现的风险还是可能的，而且往往只需付出要很少的努力。

IT 基础架构中的风险并不只涉及计算机。事实上，许多风险来自于非计算机。当为组织进行风险评估时，考虑到所有可能存在的风险是十分重要的。如果不能正确地评估和响应所有的风险形式，那么公司的安全性就是脆弱的。需要记住的是，IT 安全性(通常被称为逻辑或技术安全性)只针对逻辑或技术攻击提供保护。为了保护 IT 安全性不遭受物理攻击，就必须建立物理保护措施。

达到风险管理主要目标的过程被称为风险分析。风险分析包括：分析环境中的风险，评估每种风险发生的可能性和造成的损失，评估各种风险对策的成本，以及生成安全措施的成本/效益报告并呈交给上级管理者。除了这些针对风险的活动以外，风险管理还要求对组织内部的所有资产进行估算、评估和分配。如果没有恰当的资产评估，就不可能划分资产的优先级和比较风险可能造成的损失。

2.3.1 风险术语

风险管理引用了大量的术语，你必须清楚地理解这些术语(尤其是 CISSP 考试所要求的术语)。本节定义和讨论所有与风险相关的重要术语：

资产 资产是指环境中应该加以保护的任何事物，是用于商业过程和任务中的任何东西，可以是计算机文件、网络服务、系统资源、进程、程序、产品、IT 基础设施、数据库、硬件设备、家具、产品秘方/配方、人员、软件和设施等。如果组织认为自己控制之下的某种资源有价值并需要保护，那么这种资源就被标记为可以进行风险管理和风险分析。资产出现损失或泄漏会危及整体的安全性，造成生产效率的降低、利润的减少、额外支出的增加、组织停工以及造成许多无形的不良后果。

资产估值 资产估值指的是根据实际的成本和非货币性支出为资产分配的货币价值，其中包括开发、维护、管理、宣传、支持、维修和替换资产的成本，还包括许多难以计算的价值，例如，公众信心、行业支持、生产效率的提升、知识产权以及所有者权益。资产估值将在本章稍后部分进行详细讨论。

威胁 任何可能发生的、为组织或某种特定资产带来所不希望的或不想要结果的事情都被称为威胁。威胁是指会造成资产损失、破坏、变更、丢失或泄漏的任何行为或非行为，或者是指阻碍访问或阻止资产维护的行为。威胁可大可小，并会造成或大或小的后果。它们可能是有企图的或意外的，可能源自人、组织、硬件、网络、结构或自然界。威胁主体会有企图地利用脆弱性。威胁主体通常是人，不过也可能是程序、硬件或系统。威胁事件是脆弱性的意外利用。威胁事件包括火灾、地震、水灾、系统故障和人为错误(一般是因为缺少培训或疏忽)和断电。

脆弱性 资产中的弱点或防护措施/对策的缺乏被称为脆弱性。

换句话说，脆弱性就是 IT 基础设施或组织其他方面的缺陷、漏洞、疏忽、错误、局限性、过失

或敏感之处。如果脆弱性被他人加以利用，那么就有可能造成资产的破坏或损失。

暴露　暴露是指由于威胁而容易造成资产损失，脆弱性会被或将被威胁主体或威胁事件加以利用的可能性是存在的。暴露并不意味着实施的威胁(造成损失的事件)实际发生(暴露给已实施的威胁称为经历的暴露)，而仅仅是指如果存在脆弱性并且威胁可以利用脆弱性，那么就有可能发生威胁事件或出现潜在的暴露。

风险　风险是某种威胁利用脆弱性并导致资产损害的可能性，是对可能性、概率或偶然性的评估。可能性越大，威胁事件就越可能发生，风险就越大。暴露的每个实例都是一种风险。用书面公式表示的话，风险可以被定义为：风险 = 威胁*脆弱性

因此，减少威胁主体或脆弱性将直接降低风险发生的几率。

当风险发生时，威胁主体或威胁事件已经利用了脆弱性并导致一种或多种资产的损害或泄漏。安全的整体目标是：通过消除脆弱性和阻止威胁主体和威胁事件危及资产安全，从而避免风险变成现实。作为一种风险管理工具，防护措施能够实现安全性。

防护措施　防护措施或对策是指能消除脆弱性或对付一种或多种特定威胁的任何方法。防护措施可以是：安装软件补丁程序、修改配置、雇请保安人员、改变 IT 基础设施、更改流程、改善安全策略、更有效地培训员工、电气化的周边防护、安装照明设备等。防护措施可以是通过消除或减少组织内任何位置的威胁或脆弱性来降低风险的任何行为或产品。防护措施是削弱或消除风险的唯一方法。防护措施或对策不必是购买新产品，记住这一点十分重要。重新配置现有的元素，甚至从安全基础设施中去除某些元素，都是有效的防护措施。

攻击　攻击指的是威胁主体对脆弱性的利用。换句话说，攻击是任何有意利用组织安全基础设施的脆弱性并导致资产的损害、损失或泄漏的企图。攻击还可以被视为违反或未遵守组织安全策略的任何行为。

破坏　破坏是指发生安全机制被威胁主体绕过或阻挠的事情。当破坏与攻击结合时，就会发生渗透或入侵事件。渗透指的是威胁主体通过避开安全控制获得访问组织基础设施的权力并且能够直接危及资产安全的情况。

如图 2.4 所示，资产、威胁、脆弱性、暴露、风险和防护措施是相互关联的。威胁利用脆弱性，脆弱性导致暴露。暴露就是风险，风险又被防护措施减轻。防护措施保护被威胁危及安全的资产。

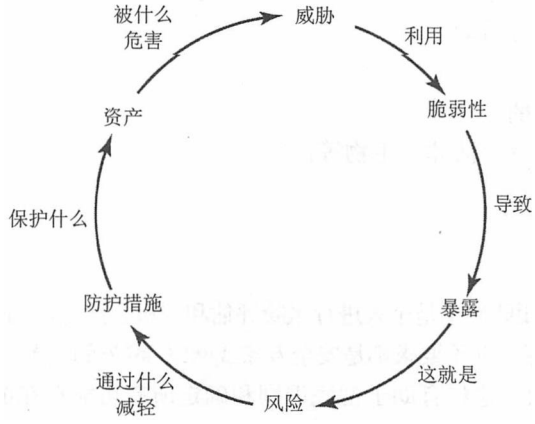


图 2.4　风险的元素

2.3.2 识别威胁和脆弱性

风险管理的一个基本部分就是对威胁进行标识并检查，这涉及创建详尽的组织中认定资产可能存在的所有威胁列表。列表应该包括威胁主体和威胁事件。威胁可能来自任何地方，记住这一点十分重要。对 IT 的威胁并不只限制在 IT 源。当编制威胁列表时，需要考虑以下各项：

- 病毒
- 级联错误(一系列逐步上升的错误)和相关性错误(由于依赖的事件或事物不存在而引起)
- 已授权用户的犯罪行为
- 运动现象(振动、炸裂声等)
- 有企图的攻击
- 重组
- 已授权的用户疾病或传染病
- 黑客
- 不满的员工
- 用户错误
- 自然灾害(地震、水灾、火灾、火山爆发、飓风、龙卷风、海啸等)
- 物理损坏(碎裂、抛射、线缆被切断等)
- 数据、资源或服务的误用
- 对数据分类或安全策略的改变或危害
- 政府、党派或军队的入侵或限制
- 处理错误、缓冲区溢出
- 滥用个人特权
- 温度失控
- 能量异常(静电噪音、EM 脉冲、无线电频率、电源损耗、电涌等)
- 数据丢失
- 信息战争
- 破产或改变/中断业务活动
- 编码/编程错误
- 入侵(物理的或逻辑的)
- 环境因素(存在天然气、液体、生物等)
- 设备故障
- 物理盗窃
- 社会工程学

大多数情况下，应该是团队而不是个人进行风险评估和分析。此外，团队成员应该来自组织内部的不同部门。通常，团队成员并不要求都是安全专家或网络/系统管理员。团队成员的多样性是以组织的人口统计学为基础的，这将有助于彻底识别和确定所有可能存在的威胁和风险。

委托顾问评估风险

风险评估是一个极为难懂、烦琐、复杂和漫长的过程。通常，由于风险的大小、范围或责任，现有的员工无法适当地进行风险分析，因此许多组织委派风险管理顾问来完成这项工作。这提供了极高的专业知识级别，不会使员工的工作停顿下来，并且被证明是评估现实风险的最可靠措施。但是，即使风险管理顾问并不只是在书面进行风险评估和分析，他们通常也仍会使用复杂和昂贵的风险评估软件。这种软件能够简化整个任务、提供更可靠的结果以及生成保险公司、董事会等可接受的标准化报告。

2.3.3　风险评估/分析

风险管理/分析主要是上层管理者的事情。上层管理者负责通过定义工作的范围和目标，启动和支持风险分析和评估。执行风险分析的实际过程经常被委派给安全专家或评估团队。然而，所有的风险评估、结果、决策和成果必须得到上层管理者的理解和批准，并作为提供谨慎的适当关注的元素。

所有的 IT 系统都存在风险。现实中不存在能够完全消除所有风险的方法。但是，上层管理者必须决定哪些风险是可以接受的，哪些风险是不可以接受的。决定哪些风险可以接受时，要求详细的、复杂的资产与风险评估。

一旦完成威胁列表的编制，就必须对每种威胁及相关的风险逐一地进行评估。目前有两种风险评估方法：定量的风险分析和定性的风险分析。定量的风险分析把真实的货币价值分配给损失的资产。定性的风险分析把主观的和无形的价值分配给损失的资产。对于完整的风险分析来说，这两种方法都是必要的。大多数环境中同时使用混合的风险评估方法，以获得他们的安全考虑的平衡观点。

1. 定量的风险分析

用定量的方法能推导出具体的概率百分比，这意味着定量的分析方法会创建一个报告，该报告用货币形式表明风险的级别、潜在的损失、对策的成本以及防护措施的成本。理解这个报告相当容易，尤其对于了解电子表格和预算报告的人来说更是如此。定量分析可以被视为对风险进行定量分配的行为，换句话说，就是用货币形式表示每个资产和威胁。然而，纯粹的定量分析是不可能的，不是所有的分析元素和方面都是可以被量化的，这是因为某些元素和方面是定性的、主观的或无形的。

定量风险分析的过程开始于资产估值和威胁标识，下一步则是评估每种风险的可能性和发生频率。然后，使用这些信息，计算各种不同的价值函数，这些函数被用于评估防护措施。

下面列出了定量的风险分析的 6 个主要步骤或阶段(见图 2.5)：

(1) 列出资产清单和分配资产价值(Asset Value 或 AV，在本章后面的“资产估值”部分详细介绍，资产价值是一个详细特征)。

(2) 研究每项资产，生成每个资产所有可能威胁的列表。针对列出的每个威胁，计算暴露因子(Exposure Factor，EF)和单一损失期望(Single Loss Expectancy，SLE)。

(3) 执行威胁分析，计算每种风险在一年内发生的可能性，也就是年发生比率(Annualized Rate of Occurrence，ARO)。

(4) 通过计算年度损失期望(Annualized Lost Expectancy，ALE)，得到每个威胁可能的总损失。

(5) 研究每个威胁的对策，然后基于应用的对策，计算 ARO 和 ALE 的变化。

(6) 针对每个资产的每个威胁的每个对策执行成本/效益分析。选择对每个威胁最适用的对策。

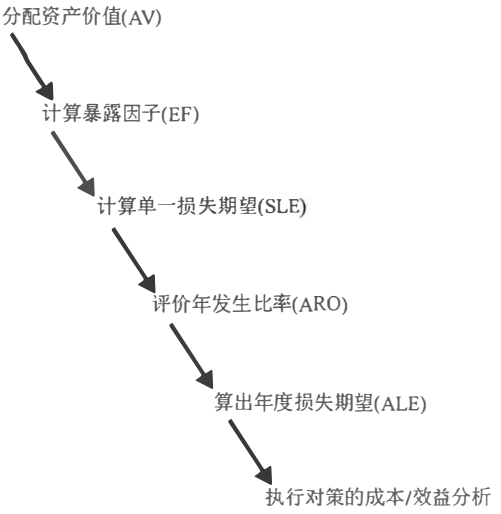


图 2.5　定量的风险分析的 6 个主要元素

某些价值函数与定量的风险分析相关联，其中包括暴露因子、单一损失期望、年发生比率和年度损失期望。

暴露因子　暴露因子(EF)代表组织的某种特定资产被已实施的风险损坏所造成损失的百分比。EF 还称为潜在损失。大多数情况下，已实施的风险不会造成资产的全部损失。EF 简单地表示在发生单个风险时全部资产价值损失的预计值。EF 通常较小(对于容易被替换的资产，例如硬件)，但也可以很大(对于不能替换的或专用的资产，例如产品设计或客户数据库)。EF 被表示为百分数。

单一损失期望　计算单一损失期望(SLE)时需要使用 EF。单一损失期望(SLE)是与针对特定资产的单个已实施风险相关联的成本。如果某个资产被特定威胁损害，SLE 计算对组织造成的确切损失。

计算 SLE 时，可以使用公式：

SLE =资产价值(AV) *暴露因子(EF)

或简化为：

SLE=AV*EF

SLE 用美元表示。例如，如果资产的价值是 200 000 美元，并且针对特定威胁的 EF 为 45%，那么这个资产的威胁的 SLE 就是 90 000 美元。

年发生比率　年发生比率(ARO)指的是特定威胁或风险在一年内将会发生(也就是成为现实)的预计频率。ARO 的范围为数值 0.0(表示威胁或风险永远不会发生)到一个非常大的数(表示威胁或风险经常发生)。ARO 的计算可能非常复杂，可以从历史记录、统计分析或猜测数据中推导出来。ARO 的计算也被称为概率测定。通过将单个威胁发生的概率与引起威胁的用户个数相乘，就可以计算出几个威胁或风险的 ARO。例如，塔尔萨发生地震的 ARO 可能是 0.00 001，然而在塔尔萨市某个办公室中存在电子邮件病毒的 ARO 可能是 10 000 000。

年度损失期望　年度损失期望(ALE) 指的是针对某种特定的资产，所有已实施的威胁每年可能造成的损失成本。计算 ALE 时可以使用公式：

ALE = 单一损失期望(SLE)*年发生比率(ARO)

或简化为：

ALE = SLE * ARO

例如，如果资产的 SLE 是 90 000 美元，并且某一特定威胁(如全部断电)的 ARO 是 0.5，那么 ALE 是 45 000 美元。另一方面，如果特定威胁的 ARO 是 15(如用户账号受到安全威胁)，那么 ALE 是 1 350 000 美元。

为每个资产和每种威胁/风险计算 EF、SLE、ARO 和 ALE 的工作量是惊人的。幸运的是，定量风险评估软件工具使这个烦琐的过程得到了简化和自动化。这些工具用来产生资产估值的详细目录，然后使用预先定义的 ARO 和一些定制的选项(如行业、地理位置、IT 组件等)生成风险分析报告。下面是经常涉及的计算：

计算使用防护措施时的年度损失期望　除了确定防护措施的年度成本之外，还必须计算实现防护措施时资产的 ALE。这需要防护措施特定的新的 EF 和 ARO。大多数情况下，即使应用了防护措施，某个资产的 EF 也仍然是相同的。EF 是风险成为现实时造成的损失大小。换句话说，如果防护措施失败，那么资产会受到多少损害？考虑一下这样的情况：如果身穿防弹衣，但是子弹却穿过防弹衣打中你的心脏，那么你仍然会遭受和未穿防弹衣一样的伤害。因此，如果防护措施失败，那么资产的损失往往与没有防护措施时是相同的。不过，某些防护措施即使在不能完全阻止攻击的情况下也仍然能够减少造成的损坏。例如，尽管火灾仍然可能发生，并且防水设施可能会被火灾破坏，还有来自喷洒头的水灾破坏，但这些总的损坏可能是小于整个建筑物被烧毁。

即使 EF 不变，防护措施也会对 ARO 做出修改。事实上，防护措施的目的是减少 ARO。换句话说，防护措施应该减少攻击对资产造成成功损害的次数。在所有可能的防护措施中，最好是将 ARO 减少为零。尽管有一些完美的防护措施，但大多数并不是完美的。因此，许多防护措施都有应用型 ARO，比非防护措施的 ARO 更小(你希望更小一些)，但通常不为零。有了新的 ARO(可能会有新的 EF)，应用防护措施的新 ALE 就会被计算出来。防护措施前的 ALE 和防护措施后的 ALE 被计算出来之后，要进行成本效益分析还需要一个值。这个额外的值就是防护措施的年度成本。

计算防护措施成本　针对每个特定的风险，必须在成本/效益的基础上评估一种或多种防护措施或对策。为了执行这个评估，首先必须为每种威胁编制防护措施列表，随后必须为每种防护措施分配部署价值。事实上，必须针对受保护资产的价值度量防护措施的部署价值或成本。因此，受保护资产的价值决定了保护机制的最大支出。安全措施应当是有成本效益的，因此保护某个资产的成本(包括现金或资源)超过该资产在组织内的价值并非明智之举。如果防护措施的成本超过资产的价值(也就是风险的成本)，那么就只能接受风险。

计算对策的价值时会涉及下列很多因素：

- 购置、开发和许可证的成本
- 实现和定制的成本
- 年度运营、维护和管理等的成本
- 年度维修和升级的成本
- 生产率的提高或降低
- 环境的改变
- 测试和评估的成本

一旦知道了防护措施的潜在成本，就有可能评估将防护措施应用于基础设施的收益。正如前面提到的，防护措施的年度成本不应该超过预计的年度资产损失成本。

计算防护措施成本/效益 成本/效益计算是此过程中最后进行的计算，用于确定某个防护措施是否能够通过较低成本真正改善安全性。为了确定防护措施的支出是否合理，可以使用下面这个公式：

使用防护措施前的 ALE-使用防护措施后的 ALE-防护措施的年度成本(ACS)=公司防护措施的价值

如果结果是负数，那么这个防护措施就不值得选择。如果结果是正数，那么这个结果值就是组织部署防护措施之后每年节省下来的钱。

采取防护措施之后每年节省或损失的钱不应该是评估防护措施时唯一需要考虑的因素。法律责任和谨慎的适度关注也是应该被考虑的问题。在某些情况下，因为部署防护措施而损失一些资金，比起承担资产暴露或损失的法律责任风险更为明智。

回顾一下，执行某个防护措施的成本/效益分析时，必须计算下列三个元素：

- 针对某个资产与威胁组合不采取对策的 ALE
- 针对某个资产与威胁组合采取对策的 ALE
- 防护措施的年度成本(ACS)

借助上述元素，最后能够获得针对特定资产的特定风险使用特定防护措施的成本/效益公式：

(采取对策前的 ALE - 采取对策后的 ALE) - ACS

甚至还可以写成更简单的形式：

(ALE1 - ALE2) - ACS

从成本/效益公式得到最大结果值的防护措施就是针对特定资产与威胁组合部署的最经济措施。

表 2.1 阐明了与定量的风险分析相关联的各种公式。

表 2.1 定量的风险分析公式

概念	公式
暴露因子(EF)	%
单一损失期望(SLE)	SLE = AV * EF
年发生比率(ARO)	# /年
年度损失期望(ALE)	ALE = SLE * ARO 或 ALE = AV * EF * ARO
防护措施的年度成本(ACS)	$ /年
防护措施的价值或收益	(ALE1 - ALE2) - ACS

天啊，这么多数学运算！

是的，定量的风险分析涉及许多数学运算。幸运的是，考试中的数学问题只可能涉及基本乘法。在 CISSP 考试中，你最有可能被问到综合了定义、应用和概念的问题。这意味着你需要知道等式/公式和值的定义、它们的含义、它们为什么重要以及如何被用于帮助组织。你至少需要知道 AV、EF、SLE、ARO、ALE 的概念以及成本/效益公式。

通过定量的风险评估过程中使用的所有计算得到的最终值，用于区分优先顺序和进行选择，了解这一点十分重要。最终值本身并不真正反映现实生活中由于安全破坏导致的损失或成本。因为在定量的风险评估过程中要求猜测、统计分析和概率预测，所以这是显而易见的。

一旦计算了针对影响特定资产的每种风险的每个防护措施的成本/效益，随后就必须对这些值进行整理分类。在大多数情况下，成本/效益值最大的就是针对特定资产的特定风险的最佳防护措施。但是与现实生活中的所有事情一样，这只是决策过程的一部分。尽管成本/效益是非常重要的因素，并且往往是主要的指导因素，但是并非数据的唯一因素。其他因素包括：实际成本、安全预算与现有系统的兼容性、IT 职员的技能/知识水平、产品的可用性、政治问题、合作关系、市场趋势、流行趋势、市场推广、合同和偏爱。作为高级管理部门的人员甚至 IT 职员，应当负责通过获取或使用可用的数据和信息来为组织确定最佳的安全决策。

大多数企业的预算都是有限的。因此，安全管理中一个至关重要的部分就是在有限的成本下获得最安全的保障。然而，要想对安全性方面实施有效的管理，就必须先对预算、效益和性能指标，以及安全控制的每个必要资源进行评估。只有在经过彻底评估之后，才能确定哪种安全控制是必不可少的也是有益的。当然，这不仅仅就其安全性而言，往往也是你的底线所在。

2. 定性的风险分析

定性的风险分析更多是根据场景而不是根据计算。这种方式不是为可能发生的损失分配准确的货币值，而是按程度将威胁分成等级，从而评估其风险、成本和影响。由于不可能进行纯粹的定量风险评估，因此定量分析的结果平衡是必要的。进行定性的风险分析的过程涉及判断、直觉和经验。在进行定性的风险分析时，可以使用很多技术，如下所示：

- 自由讨论
- Delphi 技术
- 情节串联图板
- 焦点组
- 调查
- 问卷
- 核对清单
- 一对一的会议
- 面谈

决定使用哪一种机制要根据组织的文化氛围和所涉及风险与资产的类型。比较通用的做法是：几种方法同时使用，并且在提交给上层管理者的最后的风险分析报告中比较和对照各种方法的结果。

场景

所有这些机制的基本过程都涉及场景的创建。场景是对单个主要威胁的书面描述。描述的重心集中在威胁是如何产生的及其对组织、IT 基础设施和特定的资产会产生什么影响。通常，场景描述被限制在一页纸以内，从而便于管理。对于每个场景来说，有一种或多种防护措施可以完全或部分应对场景中所描述的主要威胁。然后，分析的参与者分配场景的威胁级别、可能的损失以及每种防护措施的优点。分配威胁级别既可以非常简单，例如，使用高、中、低或数值 l 到 10 来表示，也可以用详细的文章来反映。最后，来自所有参与者的反馈会被编制成报告，并且被提交给上层管理者。至于参考评级和级别的例子，请参考 NIST SP 800-30 中的表 3-6 和表 3-7：http://csrc.nist.gov/

publications/nistpubs/800-30/sp800-30.pdf。

由于参与者的数量和多样性在评估时不断增加，因此定性的风险分析的有效性和真实性也被提高了。只要有可能，参与者中应该包括组织体系内每个层次的一人或多人，范围从上层管理者到终端用户。参与者中还应包括来自各个主要部门、办公室或分支机构的人员。

Delphi 技术

Delphi 技术也许是这个列表中不能被立刻识别和理解的唯一一种机制。Delphi 技术只是一个简单的匿名反馈和响应过程，它的主要目的是从所有参与者中得到真实的和未受影响的反馈。参与者通常被集中在一间会议室里，对于每个要获得反馈意见的请求，每个参与者都会在纸上以匿名方式写下自己的回答。得到的结果被总结和提交给风险分析小组进行评估。这个过程重复进行，直到达成一致意见。

定量的和定性的风险分析机制都能提供有用的结果。不过，每种技术都包括评估相同财产和风险的独特方法。谨慎的适度关注要求同时使用这两种方法。表 2.2 描述了这两种方法的优缺点。

表 2.2　定量的风险分析和定性的风险分析的比较

特征	定性的风险分析	定量的风险分析
是否使用复杂的函数	否	是
是否使用成本/效益分析	否	是
是否得到具体的值	否	是
是否要求猜测	是	否
是否支持自动化	否	是
是否需要大量的信息	否	是
是否客观	否	是
是否使用主要意见	是	否
是否要求付出很多时间和努力	否	是
能否提供有用的和有意义的结果	是	是

2.3.4　风险分配/接受

风险分析的结果包括：

- 所有资产的完整且详细的评估。
- 所有威胁和风险、发生概率以及一旦发生的损失范围的详细列表。
- 针对特定威胁的并且标识出有效性与 ALE 的防护措施和对策列表。
- 每种防护措施的成本/效益分析。

对于管理层制定出的、有根据的且明智的有关实现防护措施和修改安全策略的决定来说，这些信息至关重要。

一旦完成风险分析，管理层就必须处理每种特定的风险。对于风险有下列 4 种可能的反应：

- 降低风险
- 转让风险
- 接受风险

- 拒绝风险

你需要知道以下 4 种可能反馈的内容：

风险消减　降低风险或风险消减是一种消除脆弱性或阻止威胁的防护措施的实施。选取最划算或性价比最好的防御措施是风险管理的一部分，但不是风险评估的元素。事实上，对策选择是一项风险评价后或风险分析后进行的活动。降低风险的另一个潜在变化是规避风险。风险通过消除风险的原因是可以避免的。一个简单的例子是从服务器上删除 FTP 协议，以避免 FTP 攻击，以及更大的例子就是转移到内陆地区，以避免飓风带来的风险。

风险转让　风险转让或转移风险是把风险带来的损失转嫁给另外一个实体或组织。购买保险和外包就是转让或转移风险的常见形式。

风险接受　风险接受或接受风险是管理层对可能采用的防护措施进行成本/效益分析评估，并且确定对策的成本远远超过风险可能造成的损失的成本。接受风险还意味着管理层已经同意接受风险发生所造成的结果和损失。大多数情况下，接受风险要求清楚说明影响的书面陈述，书面陈述通常采用“书面签名”的方式说明为什么不实施防护措施、谁对做出的决定负责以及谁对可能发生的风险损失负责。组织是否接受风险的决定依据于对风险的容忍程度。风险容忍度是组织忍受发生风险所造成损失的能力，这也是所说的风险容忍和风险偏好。

风险拒绝　最后，但也是令人无法接受的对风险的反应称为拒绝风险或忽略风险。否认风险的存在以及希望风险永远不会发生，这都未做到适度关注，不是正确的谨慎对待风险的反应。

一旦实现了对策，继续存在的风险就被称为剩余风险。剩余风险是由针对特定资产的任何威胁组成的，高层管理部门选择不对这些资产实施防护措施。换句话说，剩余风险是管理层选择接受而非去缓解的风险。在大多数情况下，剩余风险的存在表明成本/效益分析说明可采用的防护措施不划算。

总风险指的是在没有实现防护措施的情况下，组织将要面对的风险数量。计算总风险的公式是：

威胁*脆弱性*资产价值=总风险

(注意：这里的*不是乘法，只是起到联合的功能；这不是一个数学公式。)总风险和剩余风险之间的差值被称为控制间隙(controls gap)。控制间隙是指通过实现防护措施被减少的风险数量。计算剩余风险的公式是：

总风险-控制间隙=剩余风险

与一般风险管理一样，处理风险不是一个一次性的过程。相反，安全性必须不断维护和再确定。事实上，随着时间的推移，重复地进行风险评估和分析过程已经成为评估安全计划完整性和有效性的一个机制。此外，它还有助于定位系统缺陷并及时发现改变的区域。因为随着时间的变化，安全性也在不断变化，所以定期重新评估对于维护系统安全性至关重要。

2.3.5　对策的选择和评估

在风险管理范围内选择对策主要依赖于成本/效益分析结果。不过，当评估安全控制的价值和相关度时，还应当考虑下面列出的其他一些因素：

- 对策的成本应当小于资产的价值。
- 对策的成本应当小于措施的效益。

- 应用对策的结果应当使犯罪者进行攻击的成本大于通过攻击获得的效益。
- 对策应当为真实的和识别出的问题提供解决方案(并不只是因为它们是可用的、被宣传的或听起来很不错而实施对策)。
- 对策的效益应当不依赖于其秘密状态。这意味着“隐藏式保全”不是切实可行的对策，任何切实可行的对策都能够承受公开的曝光和监视。
- 对策的效益应当是可测试的和可认证的。
- 对策应当在所有用户、系统、协议之间提供一致和统一的保护。
- 对策应当与减少级联故障无关联或基本无关联。
- 在最初进行部署和配置之后，对策应当仅需最低限度的人为干预。
- 对策应当是防止篡改的。
- 只有拥有相应权限的操作员才拥有对策的覆盖访问权限。
- 对策应当提供故障安全(fail-safe)和/或故障保护(fail-secure)选项。

请记住，安全应该被设计用来支持和保障业务任务和功能。因此，对策和防护措施需要根据业务任务的上下文进行评估。

2.3.6 实施

安全控制、对策和防护措施可以通过行政管理性、逻辑/技术性或物理性控制来实现。这三类安全机制应该以纵深防御的方式来实现，以提供最大化利益(见图2.6)。

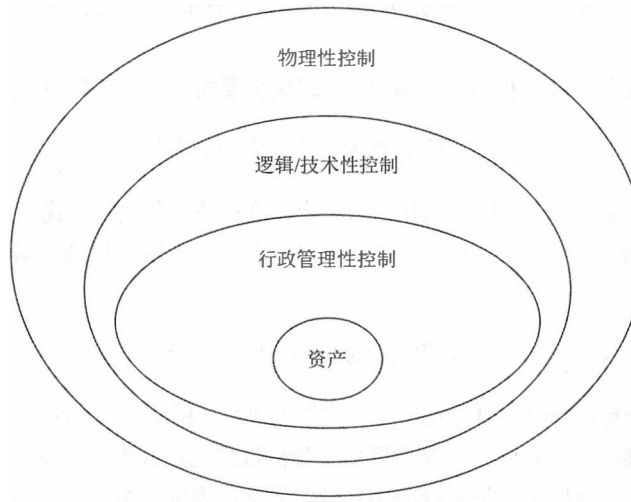


图 2.6 深度防御实施中的安全控制分类

1. 技术性控制

技术性访问和逻辑访问作为硬件或软件机制，既可以用于管理对资源和系统的访问，也可以提供对这些资源和系统的保护。顾名思义，采用的方式是技术。逻辑性或技术性访问控制的示例包括认证方法(例如用户名、密码、智能卡和生物识别)、加密、受限接口、访问控制列表、协议、防火墙、路由器、入侵检测系统(Intrusion Detection System，IDS)以及阈值级别。

2. 行政管理性控制

行政管理性访问控制是依照组织的安全策略和其他规范或需求而定义的策略与过程。它们有时被称为管理控制。这些控制主要关注两个方面：人员与业务经营方式。行政管理性访问控制的示例包括策略、过程、雇佣准则、背景调查、数据分类和标签、安全意识和培训效果、休假记录、报告和回顾、工作监督、人员控制以及测试。

3. 物理性控制

作为部署的物理屏障，物理性访问控制可以防止对系统或设施某部分的直接访问。物理性访问控制的示例包括保安、围墙、移动探测器、闭锁的门、密封窗、灯光、线缆保护、笔记本电脑锁、磁条卡、看门狗、摄像机、陷阱以及报警器。

2.3.7　控制的类型

术语“访问控制”指的是一种广泛的控制，可以执行的任务诸如确保只有授权用户可以登录，并防止未授权用户获得资源。访问控制规避了各种各样信息的安全风险。

不论何时，只要有可能，希望防止任何类型的安全问题或事件的发生。当然，一些意想不到的事件总会发生，并不是每次都能阻止。一旦事件发生，你会希望尽快检测到这个事件。如果发现，你会希望做出纠正。

当阅读控制说明时，你会注意到有些举例所列的控制不止出现在一种访问控制类型中。比如，围绕在建筑四周的防护栏(或以周长进行定义的设备)可以成为预防性控制，因为它们从本身物理结构上阻止了进入建筑场地的可能。然而，这也是一种制止性控制，因为对那些企图进入场地的人也起到了制止作用。

1. 威慑

部署威慑性访问控制是为了吓阻出现违反安全策略的情况。威慑性和预防性控制比较类似，但是威慑性控制取决于某人的决定并不阻止某个动作。相反，预防性控制实际上阻止一个活动。威慑性访问控制的示例包括策略、安全意识培训、锁、围墙、安全标识、保安、陷阱、安全摄像机。

2. 预防

部署预防性访问控制是为了阻止不受欢迎的或未授权活动的发生。预防性访问控制的示例包括围墙、锁、生物识别、陷阱、灯光、警报系统、责任分离、工作轮换、数据分类、渗透测试、访问控制方法、加密、审计、使用安全摄像机或闭路电视、智能卡、回叫、安全策略、安全意识培训、反病毒软件、防火墙和入侵防御系统(IPS)。

3. 检测

部署检测性访问控制是为了发现不受欢迎的或未授权的活动。通常，检测性访问控制并不实时进行，而是在活动出现后运行。检测性访问控制的示例包括保安、移动探测器、记录和检查安全摄像机或闭路电视捕获的事件、工作轮换、强制休假、审计跟踪、蜜罐或蜜网、IDS、违规报告、对用户的监管和检查、事故调查。

4. 补偿

部署补偿性访问控制是为了向其他现有的访问控制提供各种选项，从而帮助增强和支持安全策略。补偿性访问控制还可以包括一些其他控制，这些控制用于替代必要的或被破坏的控制。例如，一个组织策略可以指示所有的 PII 必须加密。审查发现，预防性访问控制在数据库中加密所有 PII 数据，但 PII 通过网络传输以明文形式发送。可以添加补偿性访问控制来保护传输中的数据。

5. 纠正

部署纠正性访问控制是为了在发生不受欢迎的或未授权的操作后，将系统还原至正常的状态。试图纠正发生安全事件造成的任何问题。纠正性访问控制通常较为简单，例如终止恶意行为或重启系统。其中还包括病毒解决方案，可以删除或隔离病毒并具有备份和恢复计划，以确保丢失的数据可以被恢复，活跃的 ID 可以修复系统环境并停止攻击程序。安全策略被入侵后，访问控制可以用来修复或恢复资源、功能和能力。

6. 恢复

恢复性访问控制与纠正性访问控制相比，恢复性访问控制响应访问违规的性能更高级、更复杂。恢复性访问控制的示例包括备份和还原、容错驱动系统、系统镜像、服务器群集、反病毒软件以及虚拟机影像。

7. 指令

部署指令性访问控制是为了指示、限制或控制主体的活动，从而强制或鼓励主体遵从安全策略。指令性访问控制的示例包括安全策略需求或标准、张贴通告、疏散路线出口标志、监控、监督、工作任务过程。

2.3.8 监控和测量

安全控制提供的益处应该是可以监测和度量的。如果安全控制提供的益处不可以被量化、评估或比较，那么这种控制实际上并没有提供任何安全性。安全控制应该可以提供本地或内部监控，有时也可能需要外部监控。在做初步的对策选择时，应该考虑到这一问题。

衡量一个对策的有效性并不是在进行绝对的价值度量。许多对策提供了一定程度上的改善而不是具体的关于防止破坏和阻挠攻击的数量。通常来说，要想度量对策的成功或失败，在安全措施执行前后对事件进行监测和记录是十分必要的。只有当知道起始点(正常点或初始风险水平)时，益处才能准确衡量出来。成本/效益公式中有一部分也考虑到了对策的监测与度量。安全控制在一定程度上增强了安全性，但这并不意味着获得的利益就是划算的。需要明白的是，安全性的显著提高证明了新的对策部署是物有所值的。

2.3.9 资产评估

风险分析的一个重要步骤是评估企业的资产价值。如果资产没有价值可言，那么也就没有必要为其提供保护。风险分析的一个主要目标就是确保部署的安全防护措施是符合成本效益原则的。花

费 100 000 美元来保护一项价值只有 1000 美元的资产是毫无意义的。资产价值直接影响并引导了保障和安全保护的水平。作为一项规则，安全防护措施的年度成本不应超过预期的资产损失年度成本。

当评估资产成本时，需要考虑到许多方面。资产估值的目的是给资产分配具体的货币价值，包括有形和无形价值。确定资产的精确价值通常是很困难的或不可能的，尽管如此，具体的价值必须被确定(注意，定性与定量的风险分析可以说明这个问题)。不合适地为资产分配价值会造成不能适当地保护资产或无法在财政上支持防护措施。下面列出了对有形资产和无形资产的估值有所帮助的一些问题：

- 购置成本
- 开发成本
- 经营或管理成本
- 维护或保养成本
- 获得资产的成本
- 保护或维持资产的成本
- 所有者和用户的价值
- 竞争者的价值
- 知识产权或资产的价值
- 市场评估(可维持的价格)
- 产品换代成本
- 生产率提升或下降
- 资产存在和损失的运营成本
- 资产损失责任
- 用处

为组织分配或确定资产的价值可以满足很多要求。资产估值可以作为通过部署防护措施，从而实现资产保护的成本/效益分析的基础，可以作为选择或评估防护措施和对策的方法，能够为保险目的提供资产价值并为组织确定总净值，有助于高层管理部门正确了解组织内部的风险。了解资产价值还能帮助人员避免疏忽，进行适当的关注，并激励他们服从法律要求、行业规章以及内部的安全策略。风险分析的最后一项关键任务就是风险报告。风险报告包括制作风险报告书并将其呈现给利益相关方。对许多企业来说，风险报告只是作为内部的一个参考，而其他的一些企业可能会规定必须由第三方或公众来报告他们的风险结果。

风险报告对于整个组织应该是准确及时且全面的，能清晰和准确地支持决策的制定和定期更新。

2.3.10　持续改进

风险评估可以为高层管理人员提供细致的分析，以帮助其决定哪些风险应该规避，哪些应该被转移，以及哪些应该被接受。其结果就是根据成本效益原则，在预期资产损失成本和应对威胁以及漏洞的安全措施部署成本之间进行比较。风险分析可以识别风险、量化威胁的影响，并有助于安全预算，还有助于将企业的目标和宗旨与安全策略的需求和目标整合在一起。风险分析/风险评估是对“时间点”的度量。威胁和漏洞在不断变化，因此，风险评估需要定期进行，以确保系统安全性得以持续改进。

安全性总是在不断变化。因此，随着时间的推移，任何已经实现的安全解决方案都需要更新和

更改。如果不是由选定的对策提供连续的完善路径，那么应该将其替换为可以为安全性提供灵活改进的对策。

2.3.11 风险框架

风险框架是关于如何评估风险、解决风险和监管风险的指南或诀窍。CISSP 考试中所提到的关于风险框架的主要案例由美国国家标准技术研究所(NIST)在 800-37 专业出版物中做出了定义(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf)。我们鼓励大家阅读整本出版物，以下为该出版物中关于 CISSP 的一些内容节选。

节选

该出版物提出了一些将风险管理系统(Risk Management Framework，RMF)应用于美国联邦信息系统的方法。风险管理系统包括 6 步：安全分类、安全控制的选择、安全控制的实现、安全控制的评估、信息系统的授权和安全控制的监管。风险管理系统通过实施强劲且持续不断的监管过程，促进实时风险管理概念和不间断的信息系统授权概念的提升，同时可向高层领导者提供必要的信息，帮助其在组织信息系统方面做出基于风险且划算的决定，以支持其核心任务和商业功能。另外，风险管理系统将信息安全与公司系统结构以及系统开发生命周期相结合，通过风险管理(功能)将信息系统层面的风险管理过程与组织层面的风险管理过程相联系，为部署在组织信息系统中并使用这些系统的安全控制建立责任和问责一体化制度。风险管理系统有以下特点：

- 通过实施强劲且持续不断的监管过程促进实时风险管理概念和不间断的信息系统授权概念的提升。
- 鼓励通过自动化操作，向高层领导者提供必要的信息以帮助他们在组织信息系统方面做出基于风险且划算的决定，以支持他们的核心任务和商业功能。
- 将信息安全与公司系统结构以及系统开发生命周期相结合。
- 强调选择、实施、评估、安全控制的监管以及信息系统的授权。
- 通过风险管理(功能)将信息系统层面的风险管理过程与组织层面的风险管理过程相联系。

为部署在组织信息系统中并使用这些系统的安全控制建立责任和问责一体化制度。风险管理系统的步骤包括(详见图 2.7)：

分类 对信息系统和基于影响分析做过处理、存储和传输的系统信息进行分类。

选择 基于安全分类选择该系统安全控制的初始化基线集；根据风险和当地情况的组织评估调整和补充安全控制基线。

实施 实施安全控制并描述如何在信息系统和操作环境中部署控制。

评估 使用恰当的评估步骤评估安全系统，确定一个范围，在此范围内可以保证控制的正确实施、按计划运行且达到系统安全要求的预期效果。

授权 基于对组织操作以及信息系统操作涉及的资金、个人、其他组织和国家风险的确定而授权信息系统操作，并确定风险是可接受的。

监控 不间断地监控信息系统中的安全控制，包括评估控制的有效性、记录系统变化或操作环境的变化、进行相关变化的安全影响分析以及向特定组织报告系统的安全状态。

[源自 NIST SP 800-37]

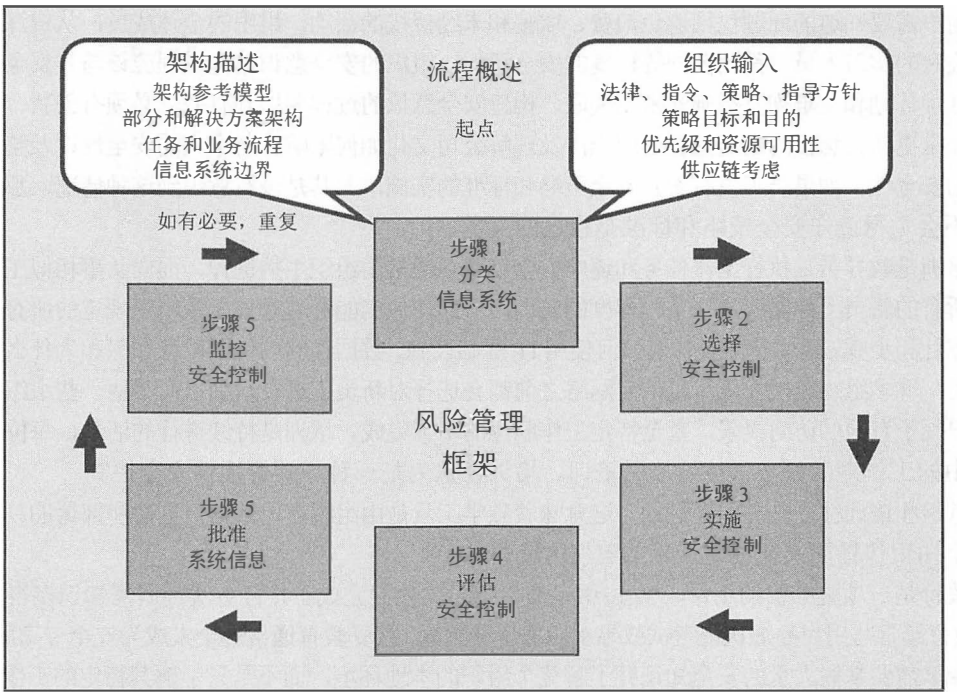


图 2.7　风险管理框架的 6 个步骤

美国国家标准技术研究所(NIST)的出版物中有更多关于风险管理系统的细节描述；请阅读该文献以便全面理解风险框架。

尽管 CISSP 考试主要关注的是 NIST 的风险管理框架(RMF)，但你也应该了解现实生活中使用的其他风险管理框架的类型。请考虑可操作的关键威胁、资产和脆弱点评估(OCTAVE)，信息风险要素分析(FAIR)和威胁代理风险评估(TARA)。如果想要获取更多信息，请阅读以下文章：www.csoonline.com/article/2125140/metrics-budgets/it-risk-assessment-frameworks--real-world-experience.html。了解目前的公认框架并选择适合企业要求和风格的框架。

2.4　建立和管理信息安全教育、培训和意识

安全解决方案的成功实现要求改变用户的行为方式。这些变化主要从改变常规的工作方式一直到遵守安全策略中规定的标准、指南和程序。行为的改变包括部分用户开展一定程度的学习工作。为了开发教育、培训和意识，所有相关项目的知识转移必须清楚地识别和加以程序演示、曝光、协同和实施方案制定。

实际的安全培训的先决条件是意识。培养安全意识的目标是要将安全放到首位并让用户认识到这一点。意识在整个组织机构之间建立了通用的安全理解基线或基础。通过课堂式的练习以及实际的工作环境都能培养出安全意识。许多工具都可以被用于培养安全意识，例如海报、通知、时事通讯文章、屏幕保护程序、T 恤衫、经理振奋人心的讲话、告示、演讲、鼠标垫、办公用品、备忘录以及传统的由教师引导的培训课程。

安全意识关注于与安全有关的重要或基础的话题和问题。所有人员应充分认识到他们的安全责任和义务。他们应该接受培训，知道什么该做，什么不该做。

用户需要知道的问题包括避免浪费、欺骗和未经授权的活动。组织的全体成员，从资深的管理者到临时的实习人员，都需要同等程度的安全意识。组织的安全意识培养过程应该与其安全策略、事件处理计划和灾难恢复措施紧密相关联。构建安全意识的过程要做到有效，必须有创新、有创造力和经常更新。意识的构建过程还应当涉及理解公司文化如何影响针对个人的安全性以及整个组织机构的安全性。如果员工没有看到安全策略和标准的实施，尤其是没有意识到这种情况，那么他们可能不会觉得遵守安全策略和标准是自己的义务。

培训是教导员工执行工作任务和遵守安全策略。通常由组织主持进行，面向从事相似工作的人群。所有的新员工都需要进行某种程度的培训，从而使他们能够遵守安全策略中规定的所有标准、指导方针和步骤。新用户需要知道如何使用 IT 基础设施、数据存储的位置以及如何和为什么要对资源分类。许多组织在授权新员工访问网络之前都会选择对新员工进行培训，而其他一些组织则会为新用户授予有限的访问权限，直至特定工作职位的培训完成。培训是持续进行的活动，每位员工在组织中的工作期间都必须持续接受培训。培训被认为是一种行政管理性安全控制。

意识和培训往往是内部提供的，这意味着教学工具是由组织在内部自己创建和部署的。不过，下一个知识传播层次往往是从外部第三方获得的。

教育是一项更细致的工作，学生/用户需要学习比他们完成工作任务实际所需知识多得多的知识。教育最常与用户参加认证考试或寻求职务晋升关联。接受教育通常是个人成为安全专家的要求。安全专家需要掌握大量的安全知识并了解整个组织的本地环境，而不是只了解其特定的工作任务。

对机构内的意识、培训和教育要求适时地进行评估，且应遵循一定的周期。培训工作应该根据工作发展及时更新和调整。另外，应该采用新颖大胆的思维方法，保持内容与时俱进。如果不对内容相关性进行周期性审核，内容会变得陈旧，员工可能会倾向于自我修补指导方针和步骤。有必要成立安全治理团队和安全规则，提供培训和教育以促进这些规则的实施。

2.5 管理安全功能

为管理安全功能，公司必须采纳恰当且充分的安全治理。实施风险评估以确保安全策略是管理安全功能最显著直接的实例。

安全必须符合成本效益原则。由于公司预算有限，因此必须合理分配其资金。此外，公司预算需要包括专门用于安全管理和处理其他商业任务和流程的费用，而不只是包括员工酬劳、保险费、退休费等。安全性应该足以抵挡对公司的传统或标准威胁，其花费不应该比其需要保护的资产还多。参考前面章节提到的“了解和应用风险管理概念”，如果保护措施的花费比资产价值本身还高，就不是有效的解决方案。

安全必须可度量。可度量的安全意味着安全机制功能的多个方面能提供明确收益，且可以记录和分析一个或多个度量。同性能度量相似，安全度量是与安全特性相关的性能、功能、操作、行动等的测量。当实施对策或防护措施时，安全度量应减少意外事件的发生或探测出更多的尝试。否则，就不能称安全机制提供了预期的效益。测量和评估安全度量的行为是评估安全项目完整性和有效性的实践，应该包括评测常见的安全指导方针和追踪控制的成功案例。追踪和评估安全度量是确保安全治理有效的一部分。然而，需要指出的是，如果选择的安全度量不正确，则会导致重大问题。例如，选择监管或评测安保人员无法控制的事物或选择基于外部驱动的事物。

安全机制本身和安全治理过程都会消耗资源。很明显，安全机制应消耗尽可能少的资源，尽可

能低地影响生产率或系统吞吐量。然而，所有硬件、软件对策以及用户需要遵守的各项政策、程序都会造成资源消耗。在选择、部署和协调对策之前和之后意识到并评估资源消耗是安全治理和管理安全功能的重要部分。

安全管理功能包括信息安全策略的开发和执行。CISSP 考试及本书的大部分内容关注的都是信息安全策略开发和执行的各个方面。

2.6　本章小结

在任何安全解决方案中，人都是最薄弱的环节。无论部署怎样的物理或逻辑控制，人总能发现避免受到控制、回避或消除控制以及禁止控制的方法。因此，在为自己所处的环境设计和部署安全解决方案时，要将用户的因素考虑进去，这一点非常重要。安全的人员雇佣、角色、策略、标准、指导方针、措施、风险管理、意识培训以及管理计划编制等方面都有助于保护资产。使用这些安全结构能够对人为的风险提供某些保护。

安全的人员雇佣需要详细的工作描述。工作描述被用于作为选择候选人和根据职位进行正确评估。通过工作描述维持安全性，这包括职责分离、工作职责和岗位轮换。

为了保护组织和现在的员工，需要有解雇策略。终止合同的过程应该包括：有证人在场、归还公司的财产、禁止访问网络、进行离职面谈以及由人员护送离开公司。

第三方治理是可能由法律、法规、行业标准或许可要求规定的监督制度。实际的治理方法可能有所不同，但通常包括外部人员或审计人员。这些审计人员可能会由管理机构指定，也可能是目标机构雇佣的顾问。

确定、评估、防止或减少风险的过程被称为风险管理。风险管理的主要目的是要将风险降低到可以接受的级别。究竟要达到哪个级别，主要取决于组织、资产价值、预算多少。尽管设计和部署完全没有风险的环境是不可能的，但是，付出很少的努力显著地减少可能出现的风险还是可能的。风险分析是达到风险管理目标的过程，这个过程包括：分析环境中存在的风险，评估每种风险发生的可能性和造成的损失，评估每个风险的不同对策的成本，以及生成安全措施的成本/效益报告并呈交给上层管理者。

安全解决方案的成功实现要求改变用户的行为方式。这些变化主要从改变常规的工作方式一直到遵守安全策略中规定的标准、指导方针和步骤。行为的改变包括部分用户开展一定程度的学习工作。三种被公认的学习层次是：意识、培训和教育。

2.7　考试要点

知道隐私如何被放入 IT 安全领域。知道隐私的多重含义/定义，为什么保护它是非常重要的，以及围绕隐私尤其是在工作环境中的隐私的各种问题。

能够讨论安全的第三方治理。第三方治理的监督制度可以根据法律、法规、行业标准或许可要求进行强制执行。

能够定义整体的风险管理。风险管理的过程如下：识别可能造成数据损坏或泄漏的因素、根据数据的价值与对策的成本来评估这些因素，以及实现能够减轻或降低风险的有成本效益的解决方案。

通过执行风险管理，就能够为降低整体风险奠定基础。

理解风险分析及涉及的要素。执行风险分析能够为上层管理者提供详细、必要的依据，从而使其决定哪些风险应当被削弱、哪些风险应当被转移以及哪些风险应当被接受。为了全面评估风险和随后采取恰当的防范措施，就必须分析下列要素：资产、资产估值、威胁、脆弱性、暴露、风险、已发生的风险、防护措施、对策、攻击和突破。

知道如何评估威胁。威胁可能有很多来源，包括 IT、人和自然界。以团队的形式评估风险以便提供范围最广的视角。通过从各个角度全面地评估风险，就可以减少系统的脆弱性。

理解定量的风险分析。定量的风险分析关注硬性指标和百分比。全部使用定量分析是不可能的，因为风险的某些方面是无形的。定量的风险分析过程涉及：资产估值和威胁识别，接着确定威胁发生的潜在频率和损失，结果是防护措施的成本/效益分析。

能够解释暴露因子(EF)的概念。暴露因子是定量风险分析的一个元素，表示组织的某种特定资产被已发生的风险损坏后造成损失的百分比。通过计算暴露因子，能够较好地实现风险管理策略。

了解单一损失期望(SLE)并知道如何计算。SLE是定量风险分析的一个元素，表示与针对特定资产的单个已发生风险相关联的成本。计算SLE时，可以使用公式：SLE=资产价值(AV)*暴露因子(EF)。

理解年发生比率(ARO)。ARO 是定量风险分析的一个元素，指的是特定威胁或风险在一年内将会发生(也就是成为现实)的预计频率。理解 ARO 能够进一步计算风险和采取适当的防范措施。

了解年度损失期望(ALE)并知道如何计算。ALE 是定量风险分析的一个元素，指的是针对某种特定的资产，所有已实施的威胁每年可能造成的损失成本。计算 ALE 时可以使用公式：ALE=单一损失期望(SLE)*年发生比率(ARO)。

了解评估防护措施的公式。除了确定防护措施每年的成本外，还必须计算实现措施后资产的 ALE。为此，可以使用下面这个公式：实现防护措施前的 ALE−实现防护措施后的 ALE−每年的防护措施成本=公司防护措施的价值，即(ALE1 − ALE2) − ACS。

理解定性的风险分析。定性的风险分析更多是根据场景而不是根据计算。这种方式不是为可能发生的损失分配准确的货币价值，而是按程度将威胁分成等级，从而评估其风险、成本和影响。这些分析结果可以帮助那些负责制定风险管理策略的人。

理解 Delphi 技术。Delphi 技术只是一个简单的匿名反馈和响应过程，这个过程被用于达成一致意见。达成的一致意见为责任方提供了正确评估风险和实施解决方案的机会。

了解处理风险的选项。降低风险或风险缓解是防护措施和对策的实现。风险转让或转移风险是把风险带来的损失成本转移给另一个实体或组织。购买保险就是转让或转移风险的一种常见形式。接受风险是因为管理层对可能采用的防护措施进行了成本/效益分析上的评估，并且确定对策的成本远远超过风险可能造成的损失的成本，还意味着管理层已经同意接受风险发生所造成的结果和损失。

能够解释总风险、剩余风险和控制间隙。总风险指的是在没有实现防护措施的情况下，组织将要面对的风险数量。计算总风险的公式是：威胁*脆弱性*资产价值=总风险。剩余风险是管理层选择接受而不是缓解的风险。总风险和剩余风险之间的差值被称为控制间隙，控制间隙是指通过实现防护措施被减少的风险数量。计算剩余风险的公式是：总风险−控制间隙=剩余风险。

理解控制类型。“访问控制”这一术语指的是一系列执行以下任务的控制=确保只有授权用户能够登录而未授权用户不能访问资源。控制类型包括预防、测探、校正、警报、恢复、指令和补偿控制。按执行方式控制可分为：行政管理性控制、逻辑性控制或物理性控制。

理解雇佣新员工的安全含义。为了制定合适的安全计划，必须具有工作描述、工作分类、工作任务、工作职责、阻止共谋、候选人筛选、背景调查、安全许可、雇佣协议和竞业禁止协议的标准。

通过部署这些机制，确保新雇佣的人员意识到要求的安全标准，从而保护组织的资产。

能够解释职责分离。职责分离属于安全概念，指的是将关键的、重要的和敏感的工作任务分配给不同的人。通过分离责任这种方式，就可以确保任何人不可能危及系统安全。

理解最小特权原则。最小特权原则表明，在安全环境中，用户应该被授予完成要求的工作任务或工作职责所必需的最少访问权限。通过限制用户只能访问完成工作任务所要求的那些资源，就能限制敏感信息的脆弱性。

了解岗位轮换和强制性休假是必要的。岗位轮换有两个作用：提供了一种知识冗余类型；人员流动可以减少伪造、数据更改、偷窃、阴谋破坏和信息滥用的风险。一到两个星期的强制性休假被用于审计和认证员工的工作任务和权限。这种做法往往比较容易发现滥用、欺诈或疏忽行为。

理解供应商控制、顾问控制和承包商控制。利用供应商控制、顾问控制以及承包商控制来确定这个主要组织外部的不同实体、个人或机构的绩效水平、期望值高低、薪酬水平以及影响程度。通常情况下，服务水平协议(SLA)的文件或政策中会对这些控制进行明确规定。

能够解释适当的解雇策略。解雇策略定义了解雇员工的过程，应当包括：始终有一位证人在场，禁止员工访问网络，进行离职面谈，护送员工离开办公室，交回安全标志和门卡，返还公司的财产。

了解如何实现安全意识培训。在真正的培训开始之前，必须让用户树立主人翁的安全意识。一旦树立了安全意识，培训或教育员工执行工作任务和遵守安全策略就可以开始了。所有的新员工都需要进行培训，这样他们才能够遵守安全策略中规定的所有标准、指导方针和步骤。教育是一项更细致的工作，学生/用户需要学习比他们完成工作任务实际所需知识多得多的知识。教育往往与用户参加认证考试或寻求职务晋升相关联。

理解如何管理安全功能。为了实现管理安全功能，组织必须采取恰当且充分的安全治理。执行风险评估以驱动安全政策的施行是最明显、最直接的安全功能管理例子。同时这也和预算、度量、资源以及信息安全策略以及评估安全系统的完整性及有效性息息相关。

了解风险管理框架的 6 个步骤。风险管理框架的 6 个步骤分别是：分类、选择、实施、评估、授权和监控。

2.8　书面实验室

1. 指出 6 种用于保证人员安全的行政管理性控制。
2. 定量的风险分析中使用的基础公式有哪些？
3. 描述用于达成在定性的风险评估过程中匿名共识的过程或技术？
4. 讨论进行平衡的风险评估需求。什么是可以使用的技术，为什么这是必要的？

2.9　复习题

1. 以下哪一项是任何安全解决方案中最薄弱的元素？
   A. 软件产品
   B. 互联网连接
   C. 安全策略

D. 人

2. 当试图雇佣新员工时，首先要做什么？

A. 创建工作描述

B. 设置职位分类

C. 审查候选人

D. 要求简历

3. 以下哪一项是离职面谈的主要目的？

A. 返还离职员工的个人物品。

B. 审查保密协议。

C. 评估离职员工的表现。

D. 取消离职员工的网络访问账户

4. 当员工被解雇时，接下来应该做什么？

A. 在他们被正式解雇前几个小时通知员工。

B. 一旦他们被通知解雇，就禁用员工的网络访问权。

C. 发送一封广播的电子邮件通知大家，某个员工将被解雇。

D. 等到你和雇员是楼里唯一剩下的人时宣布解雇。

5. 如果一个组织与外部实体签订合同，提供关键业务功能或服务，例如账户或技术支持。用于确保这些实体能够提供充分的安全性的流程被称为什么？

A. 资产识别

B. 第三方管理

C. 离职审查

D. 定性分析

6. _____的一部分是业务流程和组织策略的逻辑和实际调查。这个过程/策略审查确保定期的和执行的业务任务、系统和方法是可行、有效的，并且具有成本效益，但最重要的是(至少相对于安全治理)，他们通过减少脆弱性和避免、减少或缓解风险来支持安全性。

A. 混合评估

B. 风险规避过程

C. 对策选择

D. 文档审查

7. 以下哪一项不是正确的？

A. IT 安全只能针对逻辑性或技术性的攻击提供保护。

B. 实现风险管理目标的过程被称为风险分析。

C. 对于 IT 基础设施的风险是以所有计算机为基础的。

D. 资产是在业务流程或任务中使用的任何东西。

8. 下列哪一项不是风险分析过程中的元素？

A. 为风险分析环境。

B. 为防护措施创建成本/收益报告并提交给上层管理者。

C. 选择适当的防护措施并实施它们。

D. 评估每个威胁事件，及其发生和造成损害的成本和可能性。

9. 在风险分析中，下列哪一项一般不会被认为是资产？
   A. 开发过程
   B. IT 基础设施
   C. 专有的系统资源
   D. 用户的个人文件
10. 以下哪一项表示偶然的或有意的漏洞利用？
   A. 威胁事件
   B. 风险
   C. 威胁代理
   D. 破坏
11. 当没有或缺乏防护措施和对策时，会存在什么？
   A. 脆弱性
   B. 暴露
   C. 风险
   D. 渗透
12. 下列哪一项不是有效的风险定义？
   A. 几率、可能性或机会的评估
   B. 移除脆弱性或防止一个(或多个)特定攻击发生的任何事情
   C. 风险=威胁*脆弱性
   D. 每个暴露实例
13. 当评估防护措施时，在大多数情况下应遵循什么规则？
   A. 资产年度损失期望成本不应该超过年度的保护成本。
   B. 防护措施的年度成本应该等于资产价值。
   C. 防护措施的年度成本不应该超过资产的年度损失期望。
   D. 防护措施的年度成本不应该超过安全预算的 10%。
14. 单一损失期望是怎样计算的？
   A. 威胁+脆弱性
   B. 资产价值*暴露因子
   C. 年发生比率*脆弱性
   D. 年发生比率*资产价值*暴露因子
15. 一家公司的防护措施的价值怎样计算？
   A. 使用防护措施前的 ALE–使用防护措施后的 ALE–防护措施的年度成本
   B. 防护前 ALE*防护措施的 ARO
   C. 执行防护后 ALE+年度防护价值– 控制间隙
   D. 总风险–控制间隙
16. 什么安全控制直接关注于防止共谋？
   A. 最小特权原则
   B. 工作描述
   C. 职责分离
   D. 定量的风险分析

17. 什么样的流程或事件通常是由组织主持，针对具有相似工作职能的员工群体？

A. 教育

B. 意识

C. 培训

D. 解雇

18. 以下哪一项没有具体或直接关系到组织的安全功能管理？

A. 员工工作满意度

B. 度量

C. 信息安全策略

D. 预算

19. 由于缺少灭火器，你意识到一场火灾的威胁和脆弱性，然后开始执行风险分析。基于这些信息，下列哪些是可能的风险？

A. 病毒感染

B. 设备损坏

C. 系统故障

D. 未授权地访问机密信息

20. 通过特定的威胁/脆弱性/风险关系，已经执行了基本的定量风险分析。选择一个可能的对策。当再次计算时，下列哪个因素会变化？

A. 暴露因子

B. 单一损失期望

D. 资产价值

D. 年发生比率

第 3 章

业务连续性计划

本章中覆盖的 CISSP 考试大纲包含：

安全和风险管理(例如，安全、风险、合规性、法律、法规、业务连续性)

- G. 理解业务连续性需求
  - G.1 开发和文档化项目范围和计划
  - G.2 引导业务影响分析

安全运营(例如基本概念、调查、事件管理、灾难恢复)

- N. 参与业务连续性规划和演习

不管我们的愿望有多么美好，总会有这样或那样的灾难袭击每个组织。无论是像飓风或地震那样的自然灾害，还是像建筑火灾或水管爆裂那样的人为灾难，每个组织都会遇到真正威胁运营甚至生存的事件。

完善的组织拥有合适的计划和措施，从而帮助它们降低灾难对业务持续运营的影响，以及快速恢复正常运营。由于认识到针对业务连续性和灾难恢复计划的重要性，$(ISC)^2$ 在 CISSP 考试的 GBK 体系中包括了这两个过程。这些基本主题的知识将会帮助你准备考试，并且还能帮助你的组织为意外突发事件做好准备。

在本章中，我们探索业务连续性背后的概念。在第 18 章“灾难恢复计划”中将继续我们的讨论，并且深入讨论如果业务连续性控制失败后的具体操作，以及组织需要在灾难发生之后其操作能够恢复并再次运行。

3.1 业务连续性计划

业务连续性计划(Business Continuity Planning，BCP)涉及对组织各种过程的风险评估，还有在发生风险的情况下为了使风险对组织的影响降至最小程度而制定的各种策略、计划和措施。BCP 被用于在出现应急事件时维护业务的连续运作。BCP 计划编制人员的目标是实现策略、措施和过程的组合，从而使潜在的破坏性事件对业务的影响尽可能小。

BCP 关注于在基础设施功能和资源减少或受限的情况下维持业务操作。只要维持组织执行关键

工作任务的能力的连续性，BCP 就能够被用于管理和还原系统环境。如果这种连续性受到破坏，那么业务过程就会停止，并且组织进入灾难模式；此时，系统将采用灾难恢复计划(Disaster Recovery Planning，DRP)。

提示：

BCP 和 DRP 首先考虑的往往是人。这两种计划主要关心的是使人不受到伤害，然后再解决 IT 恢复和还原问题。

业务连续性计划与灾难恢复计划对比

你应当理解业务连续性计划和灾难恢复计划之间的差异。记住此差异的一个简单方式是 BCP 首先被应用，如果 BCP 努力失败，那么就会应用 DRP 步骤。以一个位于水坝下游的数据中心为例。BCP 努力可能涉及对水坝进行预防性维护并加固数据中心，以便抵御洪水。

即使付出最大的努力，你的业务连续性努力仍然可能失败。水坝的压力可能超出其承受的水平而出现溃堤，导致整个地区遭受洪灾。在洪水等级过高时，数据中心可能无法通过加固应对如此高的水位，以至于数据中心遭受洪灾和业务操作中断。此时，业务连续性计划所做的努力失败，我们就应当启用灾难恢复计划。

我们将在第 18 章中讨论灾难恢复计划。上述努力的最终目标是尽可能快速地还原主数据中心的业务操作。

BCP 的整体目标是在紧急情况下提供快速、沉着和有效的响应，从而增强公司立即从破坏性事件中恢复过来的能力。$(ISC)^2$ 定义的 BCP 过程包括以下 4 个主要步骤：

(1) 项目范围和计划编制

(2) 业务影响评估

(3) 连续性计划

(4) 批准和实现

本章接下来将详细讨论每个阶段，最后一部分则会介绍在编写组织的业务连续性计划时，应该认真考虑的一些关键要素。

3.2 项目范围与计划

与任何正式的业务过程一样，开发强大的业务连续性计划需要使用经过认证的一套方法。下面是这种要求的具体内容：

- 业务组织从危机计划编制的角度进行结构化分析。
- 在高层管理人员准许的情况下，建立 BCP 团队。
- 评估参与业务连续性活动的可用资源。
- 管理组织对灾难性事件做出反应的法律和法规方面的分析。

你所使用的实际过程依赖于具体组织及其业务的规模和性质。实际上，业务连续性项目的计划编制不存在“一刀切”的指南。你应当与组织内的项目计划编制专业人员进行协商并确定企业文化内的最佳运作方式。

3.2.1　业务组织分析

对于负责 BCP 计划编制的人员，首要职责之一就是进行业务组织分析，从而确定参与业务连续性计划编制过程的所有相关部门和人员。分析时需要考虑包括下面的一些领域：

- 负责为用户提供核心服务业务的运营部门。
- 重要的支持服务部门，如 IT 部门、设备维护部门和其他负责对支持运营部门的系统进行检修的团队。
- 高层行政管理人员和对于组织继续生存来说非常重要的关键个人。

基于两方面原因，这个确定过程很关键。首先，确定过程为确定 BCP 团队(参见下一节)的潜在成员提供了所需的根据；其次，为 BCP 过程的其余部分提供了基础。

通常，业务组织分析由个别团队完成，他们是 BCP 工作的先头部队。这些人一般会使用分析出的结果，来帮助进行 BCP 团队其他成员的选择工作，这是可以接受的。当 BCP 团队召集会议时，对分析结果进行彻底审查，应该是分配给团队全部成员的第一项任务之一。这个步骤非常关键，因为个人最初进行的分析可能会忽略某些重要的业务功能，这些功能是代表组织其他部分的 BCP 团队成员所了解的。如果团队继续他们的工作而不对结构分析进行修正，那么整个 BCP 过程会受到负面影响，并导致所制定的计划不能完整说明组织如何作为整体，在紧急状况下作出响应。

提示：

组织的每个位置都应当具有自己的不同计划，以便满足该位置的独特需求。单个计划应当不能覆盖多个位置。

3.2.2　BCP 团队的选择

在许多组织中，IT 和/或安全部门被指定对业务连续性计划负有专门的责任。运营部门和其他支持部门在计划编制过程中没有发言权，甚至都不知道它的存在，直至灾难发生或即将来临。这是一个致命的缺陷！独立开发业务连续性计划可能会从两方面导致灾难。首先，计划本身没有将那些只负责日常业务运作的人的能力情况纳入考虑范围；其次，这会使有关计划的操作性说明要素“处在黑暗之中”，直至必须开始实施。这种情况会降低操作要素与计划条款保持一致并有效实施的可能性，而且否定了组织针对计划的结构化培训和测试程序所取得的成绩。

为了防止这些事件对 BCP 过程造成不利的影响，负责此项工作的人在选择 BCP 团队时应当特别谨慎。这个团队中应该至少包括下列人员：

- 来自组织的负责业务所提供核心服务的每个部门代表。
- 经过组织结构分析所确认的重要支持部门代表。
- BCP 所涉及领域内的具有技术专长的 IT 代表。
- 了解 BCP 过程的安全代表。
- 熟悉公司法律、法规和契约责任的法律代表。
- 来自高层管理部门的代表。

选择一支有效 BCP 团队的技巧

选择你的 BCP 团队时要非常小心!你需要在选择代表不同观点的人和创建一支具有展示个人差异的团队之间做到平衡。你的目标是应当尽可能建立一支人才多样化并仍然保持关系协调的团队。

考虑适合组织的技术、财务和政治环境的 BCP 团队成员需要花费一定的时间。BCP 团队应当包括哪些人呢?

前面提到的每一类人都为 BCP 过程带来了不同的视角,并且都具有个人的偏好。例如,来自每个运营部门的代表通常会认为他们的部门对于组织的持续生存来说是最重要的。虽然这些见解最初看来会引起分歧,但在 BCP 过程中应该接受它们并以有效的方式进行管理。如果使用得当,这些偏向作为不同部门代表的倡议将会在最终的 BCP 计划中达到某种程度的平衡。另一方面,如果没有合适的领导人员,那么这些偏向可能转变为具有破坏性的争斗,BCP 过程将偏离正确的方向,并且会伤害整个组织。

高层管理人员和 BCP

在不同的组织机构内,BCP 过程中的高层管理人员的角色变化范围很广,企业内部的文化、高层人员对该计划的兴趣以及企业运作所处的法律和法规环境对这也有影响。高层管理人员所扮演的重要角色通常包括设置优先级和裁决、提供人员和经济资源以及解决服务关键性相关的争端。

本书的一位作者最近完成了与某个大型非营利机构的 BCP 协商约定。在会晤初期,他有机会与该机构的行政副总裁坐在一起讨论共同工作的目标。在会晤期间,他对这位作者提出这样的问题:“为了完成约定,我需要做些什么?”

他一定已经预计到会得到敷衍的回应,因为在这位作者回答时他立即说道:“哦,事实上……”随后,这位作者开始向他解释他的主动参与对于其成功来说至关重要。

但在编制业务连续性计划时,作为 BCP 团队的领导,必须尽可能在高级行政管理层找到并获得一个积极的角色。这就把 BCP 过程的重要性传达给整个组织,并提高那些把编写 BCP 计划认为是浪费时间而应将这些时间用在运营活动上的人的积极性。此外,法律和法规也可能会要求那些高层管理者的积极参与。如果你为一家从事公共贸易的公司工作,那么你可能希望提醒行政管理人员在灾难发生导致公司业务瘫痪时查找公司领导和主管的个人责任,并查找在他们的应急计划中有没有实施尽职(due diligence)的措施。

你还可能必须使管理层相信 BCP 和 DRP 开销应当不是随意的花费。管理层对组织的股东和董事会负有受信责任,受信责任要求管理层至少确保采取了适当、充分的 BCP 措施。

在这个 BCP 会晤实例中,组织的行政副总裁认识到其支持的重要性并同意参与 BCP 团队。副总裁向所有员工发送了一封电子邮件,这封邮件介绍了 BCP 工作进展并表明了自己对该工作的全力支持。此外,他还参加了几次高级计划编制会谈,而且在全组织范围的某次会议上提到了 BCP 工作。

3.2.3 资源要求

在团队确认业务组织结构分析之后,他们就应当转向 BCP 工作中所要求的资源评估,这涉及下列三个完全不同的 BCP 阶段所需的资源:

BCP 开发:BCP 团队需要某些资源来实施 BCP 过程的 4 个要素(项目范围和计划编制、业务影响评估、连续性计划、批准和实现)。此 BCP 阶段消耗的资源很可能是 BCP 团队成员和要求帮助计

划开发的支持员工所付出的人力。

BCP 测试、培训和维护：BCP 的测试、培训和维护阶段会要求一些硬件和软件支持，但是不管怎样，这个阶段的主要支持工作都将涉及活动中部分员工所付出的人力。

BCP 实现：当灾难来袭且 BCP 团队认为有必要全面实现业务连续性计划时，就需要大量的资源。这包含大量的人力(即使不是全部，BCP 也仍然很可能成为组织的主力)和对“硬”资源的利用。出于这个原因，团队正确并果断地使用其 BCP 实现能力是很重要的。

一个有效的业务连续性计划需要耗费公司大量的资源，资源的范围从购买和部署冗余的计算设施直至团队成员拟制计划草稿所需的铅笔和纸张。然而，正如前面所提到的那样，BCP 过程中消耗的最重要的资源之一是人力。许多安全专家忽略了计算所耗费人力资源的重要性。不过，你完全可以放心，高层管理者是不会忘记人力资源消耗的。企业领导能够敏锐地意识到有关时间消耗方面的活动对组织生产率的影响，以及在工资、津贴和机会损失方面实际的人力成本。当你向高层管理人员要求时间时，所涉及的这些方面会变得特别重要。

你应当意识到，负责资源使用管理的领导会把你的 BCP 提案放在“放大镜”下审查，而你应当通过具有条理性和逻辑性的 BCP 业务案例论据为计划的必要性说明做好准备。

真实场景

解释 BCP 的好处

在最近的一次会谈中，本书的一位作者有机会与来自美国某中等城市的一位卫生系统的首席信息安全官(Chief Information Security Officer，CISO)共同讨论业务连续性计划。这位 CISO 对 BCP 的看法令人震惊，他的机构没有实施正式的 BCP 过程，并且他自信万一发生灾难，“凭直觉”的方式仍然能够保证运营的良好。

这种“凭直觉”的理由是拒绝为 BCP 投入资源的一个最为常见的论点。在许多组织中，业务往往能够幸存，在发生灾难时主要领导者会组织救灾的想法非常普遍。如果遇到这样的反对理由，那么你可能应当向管理层指出业务中断每天导致的损失(直接损失和丧失机会的非直接损失)，随后请求他们考虑“凭直觉”恢复可能需要的时间，并且与有序的、有计划的操作连续性进行比较。

3.2.4　法律和法规要求

许多行业可能会发现他们要受到联邦政府、州和地方法律或法规的限制，这些限制要求他们实现不同程度的 BCP。我们在本章中已经讨论了一个例子，即公共贸易公司的领导和主管在他们的业务连续性职责中，对尽职具有不可推卸的责任。在其他环境中，法律和法规的要求(以及出现失败的后果)可能会更严格。在灾难事件发生时，紧急情况服务(例如，警察、救火和紧急医疗工作)负责社会团体能够维持继续运营。事实上，在出现紧急情况、公共安全受到威胁时，紧急情况服务变得越来越重要。如果由于他们的原因导致无法可靠地实现 BCP，那么会造成生命和/或财产的损失并降低政府在群众心中的威信。

许多国家、金融机构(例如，银行、经纪公司)和公司在处理数据时，会受到政府和国际银行与证券制度的严格控制，这些制度帮助他们持续运作和确保国家经济的生命力。当药品生产商必须在发生灾难之后在非最佳环境中生产药品时，他们会被要求必须向政府管理者证明药品的纯度。各行

各业中还有很多其他的例子，各种法律和法规都对紧急情况下的持续运营提出了要求。

即使不受到这些因素中任何一项的约束，也要对用户要求，承担实施有效 BCP 措施的契约责任。如果合同中包括某种服务级别约定(SLA)，那么就会在发生灾难导致用户服务中断时，发现自己违反了这些合同条款。许多用户可能会表示理解并希望继续使用你的产品或服务，但是他们自己的业务要求可能会迫使他们终止合同，去寻找新的供应商。

另一方面，发展完善的、文档化的业务连续性计划能够帮助组织从现有的客户那里赢得更多的新用户和其他业务。如果能够向用户展示出在发生灾难事件时，公司具有恰当的完善措施来保证用户服务的持续发展，那么他们就会对你的公司充满信心并且很可能首选你成为供应商。这样你将处于一个有利的位置！

从所有这些方面总结出一个结论，即在 BCP 过程中，将组织的法律顾问添加进来是非常重要的。法律顾问非常熟悉应用于组织的各种法律、法规和契约责任，在保证组织持续生存从而给包括员工、股东、供应商和用户在内的各方带来利益的同时，他们能够帮助团队实现满足这些要求的计划。

警告：

有关计算系统、商业惯例和灾难管理的法律经常改变，并且在不同的管辖区域差别很大，因此一定要让你的律师全程参与整个 BCP 过程，包括测试和维护阶段。如果只是把他们限制在计划实现前的审查阶段，那么你将无法意识到法律和法规的变化会对公司的职责产生怎样的影响。

3.3 业务影响评估

一旦你的 BCP 团队完成了准备创建业务连续性计划的 4 个阶段，那么就会进入工作的核心部分：业务影响评估(Business Impact Assessment，BIA)。BIA 确定了能够决定组织持续发展的资源，以及对这些资源的威胁，并且还评估每种威胁实际出现的可能性以及出现的威胁对业务的影响。BIA 的结果提供了一些用于量化的度量，这些度量有助于你确定在组织面对各种本地、区域和全球风险时投入业务连续性资源的优先顺序。

业务计划者在进行决策时会使用两种不同的分析类型，认识到这一点非常重要。决策类型如下：

定量决策：定量决策涉及使用数字和公式做出决定。这种数据类型通常以美元表示各种与业务相关的选项。

定性决策：定性决策考虑的是非数值因素，例如情感、投资者/顾客的信心、员工的稳定性以及其他感兴趣的事务。这种数据类型通常以优先级类别(例如，高、中、低)表示。

提示：

在 BCP 过程中，定量分析和定性分析都扮演了重要的角色。不过，绝大多数人都会倾向于只使用其中一种分析方式。当选择 BCP 团队的成员时，应当试图在倾向不同策略的人之间达到平衡。这种做法使我们能够开发完善的 BCP，并且最后对整个组织也是大有好处的。

本章从定量分析和定性分析的观点出发阐述 BIA 过程。无论如何，对于 BCP 团队来说，使用数字并执行定量评估是十分诱人的，毕竟定性评估更为复杂。但是，BCP 团队对影响 BCP 过程的因素进行定性分析非常重要。例如，如果你的业务高度依赖于某些非常重要的客户，那么为了长期拥有这些客户，管理团队可能愿意忍受可观的短期经济损失。BCP 团队必须在一起仔细进行定性分

析(最好有高级管理人员参与)，从而找出使所有利益相关方都满意的综合处理方法。

3.3.1　确定优先级

BCP 团队的第一个 BIA 任务是确定业务优先级。根据具体业务的范围，在出现灾难时，某些活动对于日常操作来说非常必要。优先级确认或关键性优先级涉及创建业务流程的综合列表，并且按照重要性排序。虽然这个任务似乎有些令人畏惧，但是事实上并非如此。

将确定优先级过程的工作量划分给团队成员的一个主要方法是：指定每个参与者都创建一个优先级列表，这个列表涉及该参与者所负责部门的业务功能。当整个 BCP 团队开会讨论时，团队成员会使用这些优先级列表为整个组织创建一个优先级主列表。

这个过程有助于从定性的角度确定业务优先级。前面曾经提到过同时开展定性和定量 BIA 的尝试。为了开始定量评估，BCP 团队应当在一起讨论和拟制一份组织资产清单，并且以货币形式为每种资产分配资产价值(AV)。这些数字被用在剩余的 BIA 步骤中，从而能够开发基于财务的 BIA。

BCP 团队必须为每个业务功能开发的另一个量化度量是最大允许中断时间(Maximum Tolerable Downtime，MTD)，有时也称为最大容忍中断时间(Maximum Tolerable Outage，MTO)。MTD 指的是某个业务功能出现故障但是不会对业务产生无法弥补的损害所允许的最大时间长度。在进行 BCP 与 DRP 计划编制时，MTD 提供了重要的信息。

对于每一个业务功能，这就引出另一个度量标准，这个标准就是恢复时间目标(Recovery Time Objective，RTO)。这是一个当中断事件发生时，你认为可以实际恢复功能的时间量。一旦定义了恢复目标，就可以设计和计划必要的步骤去完成任务。

BCP 过程的目标是确保 RTO 小于 MTD，这就使得一个功能从来没有在最大容忍中断时间下不可用。

3.3.2　风险识别

接下来的 BIA 阶段是识别组织所面临的风险。在组织特有的这个列表中，某些风险一下子就会被想到，而确定其他模糊的风险则需要 BCP 团队成员做一番努力。

风险具有两种形式：自然风险与人为风险。下面列出了某些引发自然风险的事件：

- 暴风/飓风/龙卷风/暴风雪
- 地震
- 泥石流/雪崩
- 火山爆发

人为风险则包括下列事件：

- 恐怖活动/战争/平民骚乱
- 盗窃/故意毁坏
- 火灾/爆炸
- 长时间断电
- 建筑物坍塌
- 运输故障

需要记住的是，上面的列表并未包含所有风险。上面给出的仅仅是一些许多组织会面对的风险。

你可能希望以这些风险为出发点，但是要完整地列出组织所面临的风险，则需要 BCP 团队所有成员的共同努力。

BIA 过程的风险识别部分实际上是纯粹的定性分析。在这个阶段，BCP 团队应当不关心每种风险实际发生的可能性，也不必关心发生风险对业务继续运作的影响破坏程度。这种分析的结果有助于对 BIA 剩余任务的定性和定量分析。

业务影响评估和云服务

当进行业务影响评估时，别忘记考虑在任何云供应商中运行的组织依赖的账户。根据云服务的性质，供应商自己的业务连续性安排可能也会对组织的业务运营产生重要影响。

考虑一下，例如，一家将电子邮件和日程安排外包给一家第三方软件即服务(Software-as-a-Service，SaaS)提供商的公司。与供应商签订的合同包括供应商的 SLA 细节吗？在灾难事件中有恢复运营承诺吗？

同时也应该记得，当选择一家云服务商时，合同通常也没有足够的应尽职责。应该去核实他们提交的合同中承诺的控制措施。尽管对你来说不太可能实地考察供应商设施来核实他们的控制措施的执行情况，但也可以退而求其次——派一个人去！

现在，在去挑选一名代表和预订航班前，你会意识到供应商的许多客户可能也会问同样的问题。出于这个原因，供应商可能早就雇用了一个独立的审计师事务所来对他们的控制工作进行评估。他们能做出这次评估的结论，以服务组织控制(Service Organization Control，SOC)报告的形式给你使用。

记住 SOC 报告有三个不同版本，其中最简单的是 SOC-1 报告，它仅仅涵盖财务报告的内部控制。如果想核查安全、隐私和可用性方面的控制，需要去审查 SOC-2 或 SOC-3 报告。美国会计师协会(American Institute of Certified Public Accountant，AICPA)设立并且维持围绕这些报告的标准，保持来自不同会计事务所的审计师意见一致。

3.3.3 可能性评估

在前面的步骤中，BCP 团队拟制了一个综合列表，这个列表列出了威胁组织的各种事件。你可能已经意识到：列表中的某些事件更容易发生。例如，对于南加州的业务来说，地震的风险大大高于火山爆发的风险；而在夏威夷，情况正好相反。

为了说明差异，业务影响评估的下一个阶段是确定每种风险发生的可能性。考虑到计算的一致性，可能性评估通常采用年发生比率(ARO)表示，ARO 反映了业务每年预期遭受特定灾难的次数。

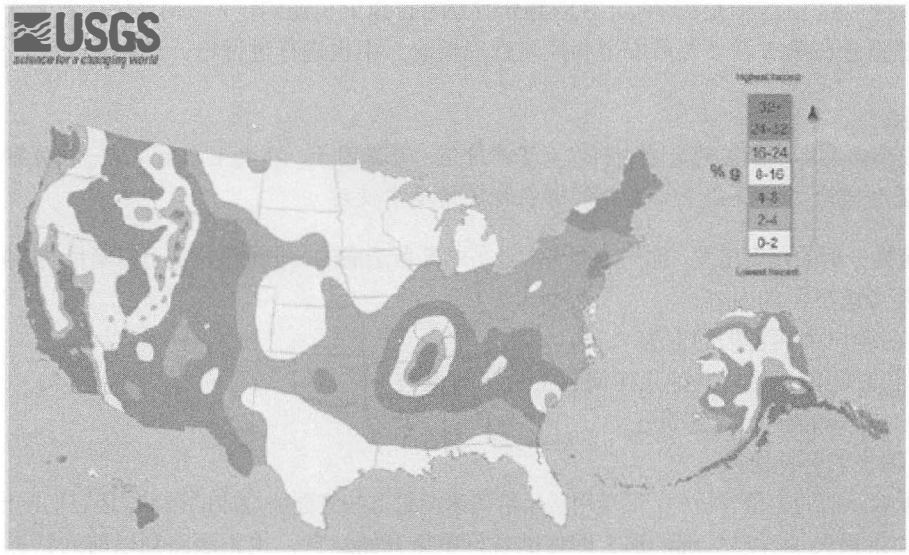
BCP 团队必须一起为先前识别的每种风险确定 ARO，这些数字应当基于公司的历史、团队成员的专业经验以及专家(如气象学家、地震学家、防火专家和需要的其他顾问)的建议。

提示：

除了在本章确认的政府资源以外，保险公司开发大型风险信息存储库作为他们的保险统计过程的一部分。你可以从他们那里获得这些信息来帮助你的 BCP 活动。毕竟，在预防对你的业务破坏方面，你们有共同的利益。

在许多情况下，你可能发现某些风险的可能性评估完全由专家提供。例如，美国地质勘探局(U.S. Geological Survey，USGS)绘制了如图 3.1 所示的地震危险图，这幅图说明了美国不同地域的地震 ARO。类似地，美国联邦应急管理署(Federal Emergency Management Agency，FEMA)相应地详细绘

制了全美各地洪灾图。总之，这些资源在网上都可以找到，它们为组织执行业务影响评估提供了丰富的信息。



(Source: U.S. Geological Survey)

图 3.1　美国各地地震危险图

3.3.4　影响评估

顾名思义，影响评估是业务影响评估的一个关键部分。在这个阶段，你需要分析识别的风险与可能性评估期间收集的数据，并且尝试确定如果每种风险发生会对业务产生什么影响。

从定量的观点出发，业务影响涉及三个特定的度量：暴露因子、单一损失期望和年度损失期望。这些度量中的每一个值都是针对 BIA 前几个阶段中评估的每种特定风险/资产组合计算的。

暴露因子(EF)是指风险对资产造成损失的程度，以资产价值的百分比来表示。例如，如果 BCP 团队向防火专家咨询并确定建筑物发生火灾会造成 70%的建筑物被毁坏，那么建筑物火灾的暴露因子就是 70%。

单一损失期望(SLE)是指每次风险发生后预计造成的货币损失，可以使用下面的公式计算 SLE：

$$SLE = AV * EF$$

继续前面的例子，如果建筑物价值 500 000 美元，单一损失期望就是 500 000 美元的 70%，即 350 000 美元。我们可以将这个数字解释为：建筑物内的一次火灾预计会造成 350 000 美元的损失。

年度损失期望(ALE)是指一年内由于风险引起资产损失而预计对公司造成的货币损失。你已经拥有执行这个计算所需的所有数据。SLE 是每次风险发生后预计造成的损失成本，ARO(根据可能性分析得到)是灾难预计在一年内的发生次数。通过将这两个数简单相乘就可以计算 ALE：

$$ALE = SLE * ARO$$

再一次回到前面的建筑物示例。如果防火专家预计建筑物每 30 年才发生一次火灾，那么 ARO 就是 1/30 或 0.03。ALE 则是 350 000 美元 SLE 的 3%，即 11 667 美元。可以将这个数字解释为：由

于建筑物火灾，公司每年预计损失 11 667 美元。

显而易见，火灾不会每年都发生，这个数字表示的是 30 年间发生火灾的平均损失。它对于预算没有什么特别的用途，但是在给特定风险划分所分配的 BCP 资源的优先级时能够体现无法衡量的价值。这些概念在第 2 章“人员安全和风险管理概念”中也进行过讨论。

提示：

一定要熟悉本章涵盖的定量分析以及资产价值、暴露因子、年发生比率、单一损失期望和年度损失期望的概念。了解各个公式并能够在特定情境中使用。

从定性分析的角度出发，你一定要考虑业务中断所造成的、非货币价值可以衡量的影响。例如，你可能要考虑下面的内容：

- 在客户中间丧失的信誉
- 长时间停工后，其他工作岗位上员工的流失
- 对公众的社会/道德责任
- 消极的公共影响

在影响评估的定量分析中，很难用货币价值来衡量这些方面所造成的影响，但它们同样很重要。毕竟，如果损失了客户基础，那么即使准备好重新开始运营，也无法回到以前的状态。

3.3.5 资源优先级划分

BIA 的最后一个步骤是划分针对各种不同风险所分配的业务连续性资源的优先级，这些风险已在 BIA 前面的任务中进行了确定和评估。从定量的角度来看，这个过程相对简单。只需要生成一个 BIA 过程期间分析过的所有风险的列表，然后按照影响评估阶段计算出来的年度损失期望的降序进行分类，这样就生成了应当解决的风险优先级列表。从列表的顶部选择愿意(而且能够)同时处理的足够多的条目，然后下移。如果确定准备处理一个已有条目，则另添一个条目。最后，我们将达到这样一种程度：风险列表容量已满(不太可能)或者所有可用的资源已耗尽(很有可能)。

前面部分已经强调了定性分析的重要性。在 BIA 的前几个阶段，虽然某些方面有所重复，但是我们仍然将定量分析和定性分析作为独立的主要功能来看待。现在是时候合并两个优先级列表了，这可是一个技巧。你必须与 BCP 团队和代表高级管理层的人员坐在一起，从而将这两个列表合并成一个优先级列表。

定性分析可以证明提高或降低风险的优先级是否正确，这些风险在定量列表中存在并已按照 ALE 进行分类。例如，如果你经营一家防火公司，那么优先级排在第一位的是在主要业务地点采取防火措施，虽然地震会造成更多的实际损失，但不会将其放在首位。如果一家防火公司受到火灾的破坏，将很难挽回该公司在商界的声誉，并最终会导致公司倒闭，因此要调整提高相应的优先级。

3.4 连续性计划

BCP 过程的前两个阶段(项目范围和计划编制、业务影响评估)主要确定 BCP 过程如何工作并确定必须防止其出现中断的业务资产的优先顺序。BCP 开发的下一个阶段是连续性计划编制，这个阶段专注于连续性策略的开发和实现，从而最小化已发生风险可能对被保护资产的影响。

在这一节中，你将学习连续性计划涉及的下列子任务：

- 策略开发
- 预备和处理
- 计划批准
- 计划实现
- 培训和教育

3.4.1　策略开发

连续性计划的策略开发阶段为业务影响评估和 BCP 开发的连续性计划阶段之间架起了桥梁。BCP 团队现在必须采用由定量和定性资源优先级确定工作产生的事项优先列表，并且确定业务连续性计划会处理哪些风险。对于所有意外事件的全面处理，需要实现维护每个或所有可能的风险的零故障时间的预备和处理。基于显而易见的原因，实现这样一个综合策略简直就是不可能的事情。

BCP 团队应当回顾一下 BIA 前期建立的 MTD 评估时间，并且确定哪些风险被认为是可接受的，哪些必须采取 BCP 连续性措施加以缓解。有些决定是明显的，如在埃及发生对操作设备的暴风雪袭击风险是可以忽略的，并且将被作为可接受的风险；新德里雨季的风险非常严重，因此 BCP 措施必须缓解这个风险。

提示：

需要记住的是，对待风险可能有 4 种反应：减轻、指派、接受和拒绝。根据不同的条件，每种反应都可能是可接受的。

一旦 BCP 团队决定需要缓解的风险和每种缓解任务将被交付的资源级别，他们便准备进入连续性计划的预备和处理阶段。

3.4.2　预备和处理

连续性计划的预备和处理阶段是整个业务连续性方案的重要部分。在这个任务中，BCP 团队设计了具体的过程和机制，将在策略开发阶段缓解被认为不可接受的风险。下列三种资产类型必须通过 BCP 预备和处理进行保护：人、建筑物/设备以及基础设施。在接下来的三个小节中，我们将探讨一些可以用于保护这些类型的技术。

1. 人

首先，必须确保组织内部的人在紧急事件发生前、发生期间和发生后都是安全的。一旦达到这些目标，就必须准许员工在尽可能正常的条件下处理他们的 BCP 和操作任务。

警告：

不要忽视这样的事实：人其实是最有价值的资产。在几乎所有业务中，人的安全必须始终优先于公司的商业目标。务必确保业务连续性计划为员工、客户、供应商和其他可能受到影响的个人提供恰当的防备措施。

必须为人们提供他们完成所分配任务而需要的所有资源。同时，如果环境要求人们在工作时间外加班，那么就必须为他们安排住宿和食品。任何要求这些预备措施的连续性计划都应该包括对 BCP 团队在面对灾难事件时的详细指导。为经营和支持团队长久地提供足够多的预备储备，这些储备应该放在易接近的地方。计划中应当指出定期轮换这些储备，以防损坏。

2. 建筑物/设备

许多业务为了完成其关键性操化，要求使用专门的设备。这些设备可能包括标准的办公设备、制造车间、操作中心、仓库、配送或物流中心，以及维修或维护站。在执行 BIA 时，你会确定在公司的连续运营能力中扮演重要角色的那些设备。连续性计划应该说明每种关键设备的下列两个方面：

强化预备措施 BCP 应当对要采取的机制和过程进行概述，这些机制和过程可以被用于保护现有的设施能够抵御策略开发阶段定义的风险。这可能会包括一些步骤，这些步骤既可能像修补漏屋顶一样简单，也可能像安装飓风遮蔽物和防火墙一样复杂。

预备场所 在不可能强化设施抵御风险时，BCP 应该确定业务活动可以立即恢复的预备场所(或为所有受影响的关键性业务功能提供的时间至少要低于最大可容忍故障时间)。在第 18 章“灾难恢复计划”中，将介绍几种在这种状态下可能有用的设施。

3. 基础设施

每种业务的关键性处理过程都要依赖某些类型的基础设施。对于许多业务来说，基础设施的关键部分是通信的 IT 主干和处理订单、管理供应链、管理用户交互和执行其他业务功能的计算机系统。这个主干包括很多服务器、工作站和各站点之间的关键通信链接。BCP 必须说明如何保护这些系统，从而抵御策略开发阶段所确定的风险。与建筑物和设备一样，提供保护的方法主要有下列两种：

强化系统 可以通过引入保护性措施来为系统抵御风险，这些措施包括计算机防火抑制系统和不间断电源。

预备系统 业务功能也可以通过引入的冗余性得到保护(依赖于不同设备的冗余构件，或是完全冗余的系统或通信链接)。

这些相同的原则应用于任何基础设施组件，从而为关键性业务处理提供服务，这些基础设施组件包括运输系统、输电网、银行业和财务系统、供水管道等。

3.4.3 计划批准和实现

一旦 BCP 团队完成了 BCP 文档的设计阶段，那么就该申请获得高级管理层的批准了。如果你很幸运地在计划的开发阶段就有资深管理人员介入，那么获得批准应当是相当简单的过程。另一方面，如果你是第一次向管理人员提交 BCP 文档，那么你应当准备为计划目标和具体预备措施进行详细的解释。

提示：

资深管理人员的批准和参与是整个 BCP 工作成功的关键。

如果可能，那么应当尝试获得公司最高领导(如首席执行官、董事长、总裁或类似的业务领导)对计划的批准。这个步骤证明了计划对整个组织的重要性，并且显示了业务领导对业务连续性的承诺。像这样的个人签名还加深了对其他资深经理的影响和计划的可信性，否则他们将会把计划作为

必要的但却琐碎的 IT 事务丢在一边。

3.4.4　计划实现

一旦得到高级管理层的批准，就应当推动并开始实现你的计划。BCP 团队应该共同开发一个实现计划，这个计划利用特定的资源，从而尽可能迅速地在给出修改范围和组织环境的情况下取得所声明的过程和预备措施的目标。

在完全部署所有这些资源之后，BCP 团队应当监督恰当的 BCP 维护程序，以便确保计划能够响应业务需求的发展。

3.4.5　培训和教育

培训和教育是 BCP 实现中的一项重要内容。计划中(直接或间接)涉及的所有人都应当接受某些与整个计划和个人职责相关的培训。

组织中的每个人都应当接受至少一份计划综述简报，从而使他们具有信心，相信业务领导已经考虑到连续性业务的可能风险，并且制定了计划来缓解对组织的影响。

具有直接的 BCP 职责的人们应当受到培训，对其具体的 BCP 任务进行评估，确保在灾难发生时他们能够有效地完成其任务。此外，至少应当为每个 BCP 任务培训一名候补人员，以便确保在人员受伤或危机时刻人员不能到位时的冗余性。

3.5　BCP 文档化

文档化是业务连续性计划过程中的关键步骤。将 BCP 方法记录到纸上可以提供下列重要优点：

- 确保所有 BCP 人员都有一个连续性的书面文档，在紧急事件发生时，甚至在资深 BCP 团队成员不在现场指导时可以作为参考。
- 提供了 BCP 过程的历史记录，这对于将来人员试图理解不同过程的内因并对计划进行必要的修改是有用的。
- 促使团队成员将他们的想法记录到纸上，这个过程常常有助于确定计划中的缺陷。将计划记录到纸上还可以向不属于 BCP 团队的人分发简报，从而进行“理智的分析”。

接下来，我们将探讨书面的业务连续性计划中的一些重要组成部分。

3.5.1　连续性计划的目标

首先，计划应当描述 BCP 团队和高级管理层提出的连续性计划的目标。这些目标应当在第一次 BCP 团队会议上或会议之前决定，并且很可能在 BCP 的生命周期内保持不变。

BCP 的最常见目标十分简单：确保在紧急事件发生时业务的连续性操作。为了满足组织的需求，其他目标也可能被放入文档的这部分内容。例如，可以设置这样的目标：客户呼叫中心的连续停机时间不能超过 15 分钟，或者备份服务器能够处理一小时全速工作 75%的处理负载。

3.5.2 重要性声明

重要性声明反映了 BCP 对于组织继续生存能力的关键程度。这份文档通常采取向组织的员工发送信件的形式，声明为什么要将重要的资源放到 BCP 开发过程中，并且要求所有人员在 BCP 实现阶段进行协作。

这就是高管参与 BCP 的重要性。如果可以在这封信上签署 CEO 或类似级别领导的名字，那么这个计划本身将在整个组织内实现改变时产生极大的影响。如果是一名较低级别管理者的签字，那么在试图对组织中由其直接领导的部门之外的其他部门进行操作时可能会受到阻碍。

3.5.3 优先级声明

优先级声明是业务影响评估的优先级确定阶段的直接产物，它仅仅涉及按优先次序列出的被认为对连续业务操作具有关键作用的功能。当列出这些优先级后，你还应当包括一个声明，指出它们作为 BCP 过程的一部分进行开发，并且反映在紧急事件中这些功能对连续性业务操作的重要性。否则，优先级的这个列表可能被用在无计划的目标中，并且导致竞争组织之间的争斗，进而对业务连续性计划造成破坏。

3.5.4 组织职责的声明

组织职责的声明也来自于高管，并且可能并入与重要性声明相同的文档内。它基本上反映了“业务连续性是所有人的职责”这一观点。组织职责的声明重申了组织对业务连续性计划的承诺，并且通知组织的员工、供应商和分支机构，要求他们每个人都做他们能够协助 BCP 过程的所有工作。

3.5.5 紧急程度和时限的声明

紧急程度和时限的声明表述了实现 BCP 的关键性，并且概述了由 BCP 团队决定的并由上层管理者同意的实现时间表。声明的措辞将依赖于由组织的领导层为 BCP 过程分配的实际的紧急程度。如果声明自身包括在优先级声明和组织职责声明的同一文档中，那么时间表应该作为一份单独的文档。否则，时间表和这个声明可能会被放入同一文档。

3.5.6 风险评估

BCP 文档的风险评估部分实质上重述了业务影响评估中进行的决策制定过程。它应该包括对 BIA 过程中所有风险的讨论以及评估这些风险时执行的定性和定量分析。对于定量分析来说，应当包括实际的 AV、EF、ARO、SLE 和 ALE 数值。对于定性分析来说，风险分析背后的考虑过程应当提供给阅读者。值得注意的是，风险评估内容必须进行定期更新，因为它反映了某个时间点的评估。

3.5.7　可接受的风险/风险缓解

BCP 文档中可接受的风险/风险缓解部分包含 BCP 过程的策略开发部分的结果。它应该覆盖风险分析部分确定的所有风险，并且概述一个或两个考虑过程(如下所示)：

- 对于那些被认为可接受的风险，应当概述风险被认为可接受的原因，以及未来可能导致值得重新考虑这个决定的事件。
- 对于那些被认为不可接受的风险，应当概述风险缓解的预备措施和用来减少威胁组织持续生存能力的风险过程。

警告：

在事情变得简单之前说一句“我们接受这个风险”是极其简单的，但很难看到一个困难的风险缓解的挑战。业务连续性规划人员应该抵制上述这些陈述并且要求业务管理者要一份他们决定接受风险的正式文件。如果审计人员稍后仔细阅读你的业务连续性计划，他们将肯定会查阅在 BCP 过程中做出的任何风险接受决定的正式工件。

3.5.8　重大记录计划

BCP 文档还应当概述组织的重大记录计划。这份文档阐述了关键业务记录将要存放的地方和对这些记录建立和存储副本的过程。

执行重大记录计划最大的挑战之一，通常首要的是识别重大记录。在许多组织从纸质转换为数字工作流时，他们常常丢失了围绕创建和维护正式文件结构的精确性。重大记录可能现在分布在各种 IT 系统和云服务中。一些可能会存储在团队可访问的中央服务器上，然而其他可能位于数字仓库中，并分配给一个员工。

假如混乱的事务状态听起来像是你的现状，你可能希望通过识别对业务真正重要的重大记录，来开始你的重大记录计划。和领导一起坐下来并且提问：“如果我们现在需要从一个全新的位置开始重建我们的组织，并且不访问我们的任何计算机和文件，你们会需要哪些记录？”通过这个方式的提问，迫使团队将真实的重建操作流程可视化，他们将跟随自己内心的步骤，产生一份有关组织的重大记录清单。这份清单也会随着人们想起其他重要信息源而有所发展，所以你应该考虑用多次会议来完成它。

一旦已经识别出组织认为重大的记录，下个任务就很艰难了：找出它们！对于在重大记录清单中识别的每条记录，你应该能够标识出存储的位置。一旦你完成了这个任务，接下来就可以使用这个重大记录清单，去报告剩下的业务连续性计划工作情况。

3.5.9　响应紧急事件的指导原则

紧急事件响应指导原则概述了组织和个人对于紧急事件立即响应的职责。此文档为首先发现紧急事件的员工提供了激活未自动激活的 BCP 预备措施的步骤，这些指导原则应当包括下列内容：

- 立即响应规程(安全性规程、防火规程、通知恰当的紧急事件代理机构等)
- 事件通知清单(主管、BCP 团队成员等)
- 在等待 BCP 团队集中时采取的二级响应规程

你的指导方针应该被所有人接受，当一次危机事件来临时，第一个站出来的人有可能就在这群人中间。任何时候破坏罢工，时间都是宝贵的。降低业务连续性进程的速度可能会导致业务运营出现非预期中断。

3.5.10 维护

BCP 文档和计划本身必须是实际使用中的文档。每个组织都会遇到几乎持续的变化，这种动态特性也确保了业务连续性要求随之发生变化。BCP 团队不应该在计划开发完成后被解散，而是应当定期接触并讨论计划、复审计划测试的结果，以确保能够继续满足组织的要求。

显而易见，计划的较小变更不要求整个 BCP 开发过程重新开始，只需要通过 BCP 团队的非正式会议达成一致意见。然而，需要记住的是，组织任务或资源的剧烈变更可能要求重新开始 BCP。

在更新 BCP 的任何时候，必须进行良好的版本控制。所有旧的 BCP 版本都应该进行物理销毁，并且被最新版本代替，这样就不会产生对 BCP 正确实现的混淆。将 BCP 组件包含在工作描述中以便确保 BCP 保持更新和正确实施是很好的习惯。员工的工作描述中包含 BCP 职责也会使其成为绩效审查过程考虑的对象。

3.5.11 测试和演习

BCP 文档还应当概述一个正式的测试计划，以确保计划是最新的，并且所有人员都接受了充分培训，从而在实际的灾难事件发生时能够履行他们的职责。测试过程实际上与用于灾难恢复的计划非常类似，因此我们将在第 18 章中讨论具体的测试类型。

3.6 本章小结

每个依赖技术资源作为生存基础的组织都应该拥有一个综合的业务连续性计划，以便确保组织在发生无法预知的紧急事件时具有持续的生存能力。很多重要的概念支撑着可靠的业务连续性计划(BCP)，其中包括项目范围和计划编制、业务影响评估、连续性计划、批准和实现。

每个组织都必须具备计划和规程来帮助缓解灾难对于连续运营的影响，并且加速恢复正常运营。为了确定业务所面临的需要缓解的风险，必须从定量和定性的角度实施业务影响评估。必须采取恰当的步骤开发组织的连续性策略，并且了解在经受未来的灾难时要做什么。

最后，必须建立用于确保计划能够有效传递至现有或未来 BCP 团队成员的文档。这样的文档必须包括连续性计划指导原则。这个业务连续性计划必须包含重要性、优先级、组织职责、紧急程度和时限的声明；还应当包含风险评估、接受和缓解、重大记录计划、紧急事件响应指导原则以及维护和测试的计划。

第 18 章将讨论如何制定下一步的计划，即开发并实现灾难恢复计划。灾难恢复计划在业务连续性计划中止时开始。当中断业务的紧急事件发生时，尽管 BCP 采取了措施，但是灾难恢复计划仍然要指导必要的恢复工作，以便尽可能快地恢复到正常的业务运营状态。

3.7　考试要点

理解业务连续性计划编制过程的 4 个步骤。业务连续性计划涉及 4 个不同的阶段：项目范围和计划编制、业务影响评估、连续性计划、批准和实现。每个任务都为整体目标服务，从而确保业务在发生紧急事件时不会中断并持续运营。

描述如何执行业务结构分析。在业务结构分析中，负责领导 BCP 过程的人确定哪些部门和个人会参与业务连续性计划。这种分析被用作 BCP 团队选择的基础，并且在 BCP 团队确认后被用于指导 BCP 开发的后续阶段。

列出业务连续性计划团队的必要成员。BCP 团队至少应当包括下列人员：每个运营和支持部门的代表；IT 部门的技术专家；具有 BCP 技能的安全人员；熟悉公司法律、规章、契约责任的法律代表；以及高管代表。其他团队成员取决于组织的结构和特性。

了解业务连续性计划编制者面对的法律和规章要求。业务领导必须尽职，以确保股东的利益在灾难事件发生时得到保护。美国的一些行业还必须服从美国联邦、州和当地的法规，这些法规要求特殊的 BCP 规程。很多业务在灾难发生之前和之后都具有客户必须满足的合约义务。

解释业务影响评估过程的步骤。业务影响评估过程的 5 个步骤包括优先级确定、风险确定、可能性评估、影响评估和资源优先级划分。

描述连续性策略的开发过程。在策略开发阶段，BCP 团队确定哪些风险要进行缓解。在预备和处理阶段，将会对实际缓解风险的机制和规程进行设计。计划必须随后得到高管的批准并且加以实现。人员还必须接受其在 BCP 过程中所处角色的培训。

解释为组织机构的业务连续性计划进行全部文档化的重要性。将计划记录下来，以便在灾难发生时为计划的实施提供规程上的书面记录。这避免了“在我脑子里”的综合症，从而确保在紧急事件中有序地实施计划。

3.8　书面实验室

1. 为什么 BCP 团队包括法律代表是重要的？
2. 针对 BCP 的“凭直觉”论点错在哪里？
3. 定量和定性风险评估之间有何差异？
4. BCP 培训计划中应当包含哪些关键组件？
5. BCP 过程具有哪 4 个主要步骤？

3.9　复习题

1. 对于那些对业务连续性计划开发负责的人来说，第一步应该执行什么？
   A. 团队选择
   B. 业务组织分析
   C. 资源需求分析
   D. 法律和合规性评估

2. 一旦 BCP 团队选定，放在团队议程首要位置的是什么？

A. 业务影响评估

B. 业务组织评估

C. 资源需求评估

D. 法律和合规性评估

3. 在组织持续生存方面，为确保适当的措施用于减少灾难影响，以下哪一项描述了企业管理人员和总监的责任？

A. 企业责任

B. 灾难需求

C. 应尽关注

D. 持续经营责任

4. 在 BCP 阶段，BCP 过程消耗的主要资源将是什么？

A. 硬件

B. 软件

C. 处理时间

D. 人员

5. 在业务影响评估的优先级识别阶段，什么测量单位用于资产价值量化？

A. 货币

B. 效用

C. 重要性

D. 时间

6. 下列哪一项 BIA 条款标识了一个特定风险每年预计损失的货币量？

A. ARO

B. SLE

C. ALE

D. EF

7. 什么 BIA 度量值被用于表示一个业务功能的最长中断时间，但这个中断没有对组织产生不可弥补的损害？

A. SLE

B. EF

C. MTD

D. ARO

8. 你担心雪崩这个风险会威胁到你的 300 万美金运输设施。基于业内意见，你确定每年雪崩有 5%的几率发生。专家提醒你，雪崩会彻底摧毁你的建筑物，并迫使你在同一块土地上重建。这 300 万美金的设施中 90%的价值是大楼，另外 10%是土地本身。雪崩对于你的运输设施的单一损失期望是多少？

A. 300 万美金

B. 270 万美金

C. 27 万美金

D. 13.5 万美金

9. 在问题 8 提到的场景中，年度损失预期是多少？

A. 300 万美金

B. 270 万美金

C. 27 万美金

D. 13.5 万美金

10. 你担心飓风会对设在南佛罗里达州的公司总部造成风险。这个建筑物本身价值1500万美金。在咨询了国家气象服务部门后，你确定飓风在一年之中袭击的可能性有 10%。你雇佣了一支由建筑师和工程师组成的团队，确定了一般的飓风会摧毁约 50%的建筑物。年度损失期望(ALE)是多少？

A. 75 万美金

B. 150 万美金

C. 750 万美金

D. 1500 万美金

11. 以下哪个 BCP 任务连接业务影响评估和连续性规划阶段？

A. 资源优先级

B. 可能性评估

C. 策略开发

D. 条款和流程

12. 当设计连续性计划条款和流程时，首先应该保护哪个资源？

A. 厂房

B. 基础设施

C. 金融

D. 人

13. 在业务影响评估过程中，下列哪个观点不适合定量测量？

A. 厂房的损失

B. 车辆的损坏

C. 负面宣传

D. 断电

14. Lighter Than Air 公司预计如果龙卷风袭击了它的飞机业务设施，就会损失 1000 万美金。假设龙卷风袭击设施每 100 年会发生一次。那么在这个场景下单一损失期望是多少？

A. 0.01

B. 1000 万美金

C. 10 万美金

D. 0.10

15. 根据问题 14 提到的场景，年度损失期望是多少？

A. 0.01

B. 1000 万美金

C. 10 万美金

D. 0.10

16. 在哪个业务连续性计划任务中，会设计流程和机制以减少 BCP 团队认定的不可接受的风险？

A. 策略阶段
B. 业务影响评估
C. 条款和流程
D. 资源优先级

17. 安装冗余通信链路，这是利用了什么类型的缓解条款？

A. 加固系统
B. 定义系统
C. 减轻系统
D. 更换系统

18. 如果灾难中断了业务的正常运行，什么类型的计划概述了相关处理流程？

A. 业务连续性计划
B. 业务影响评估
C. 灾难恢复计划
D. 脆弱性评估

19. 用于为单个风险场景计算单一损失期望的公式是什么？

A. SLE = AV × EF
B. SLE = RO × EF
C. SLE = AV × ARO
D. SLE = EF × ARO

20. 对于下面列出的人员，一份重要的业务连续性计划声明会对谁提供最佳承诺？

A. 业务运营副总裁
B. 首席信息官
C. 首席执行官
D. 业务连续性经理

第 4 章

法律、法规和合规性

本章中覆盖的 CISSP 考试大纲包含：

安全和风险管理(例如，安全、风险、合规性、法律、法规、业务连续性)

- C. 合规性
  - C.1 法律和法规遵从
  - C.2 隐私需求遵从
- D. 理解全球范围内涉及信息安全的法律和法规问题
  - D.1 计算机犯罪
  - D.2 许可和知识产权(例如，版权、商标、数字版权管理)
  - D.3 进口/出口控制
  - D.4 跨境数据流
  - D.5 隐私
  - D.6 数据破坏

在早期的计算机安全中，信息安全专业人士更多地依靠个人的力量来保护他们的系统免受攻击，而没有得到刑事和民事司法系统的帮助。当信息安全专业人士寻求执法机构的帮助时，工作繁忙的执法机构却不情愿这样做，其原因在于他们对于涉及计算机的行为哪些属于犯罪，没有一点儿基本概念。政府的立法机构并没有对计算机犯罪的问题进行说明，而执法分支机构认为他们没有法定的授权或义务来追查这些问题。

幸运的是，我们的法律系统和执法人员已经走过了二十几年漫长的道路。全世界的政府立法机关至少已经尝试解决计算机犯罪的问题。许多执法机构已经有了全职的、受过良好安全培训的计算机犯罪调查人员，以便帮助那些需要了解这方面情况却又不知道向谁咨询的人。

在本章中，我们将讨论有关处理计算机安全问题的各种法律类型，并且我们还将研究有关计算机犯罪、隐私、知识产权和多个相关话题的法律问题。我们还将介绍基本的调查技术，其中包括请求执法部门援助的利弊。

4.1 法律的分类

在我们的法律系统中有三种主要的法律类别发挥着作用。每一种法律都涵盖了许多不同的环境，并且在不同的类别下对于违法的处罚方式也不相同。接下来，你将学习刑法、民法和行政法如何相互作用，进而形成司法系统的复杂网络。

4.1.1 刑法

刑法形成了法律体系的基石，维护着我们所处社会的和平和安全。许多高等法院的法官都关心刑法的问题，这些也是警察和其他执法机构所关心的问题。刑法包含针对某些行为的禁令，如谋杀、伤害、抢劫、纵火和类似的犯罪行为。对违反刑法的处罚有一个范围，包括强制性劳教、以罚金形式的货币处罚(或多或少)、以监狱判决形式剥夺公民自由权。

真实场景

警察是精明的！

本书其中一位作者的好友是地方警察部门的技术犯罪调查人员，他经常接手计算机滥用的案子，这些案子涉及危险的电子邮件和 Web 站点帖子。

最近，这名调查人员谈起一起通过电子邮件向当地中学发出的炸弹威胁案。罪犯向学校校长发送了一封威胁性邮件，信中宣称炸弹将在下午 1 点爆炸，同时警告校长撤离学校。这位好友在上午 11 点接到报警，此时他只有两个小时时间来调查罪行和建议校长采用最佳的一系列动作。

这位调查人员立刻紧急传唤网络服务供应商，并且跟踪到威胁邮件来自学校图书馆的某台计算机。在中午 12 点 15 分，调查人员向嫌疑人出示了表明其当时在图书馆内的监控录像以及最终表明其发送了邮件的审计日志。该学生很快承认发出这个威胁只是企图将放学时间提前两个小时。他的解释是“我不相信有人能够发现真相”。

然而事实表明，这位学生的想法是错的。

目前有许多刑法都是为了通过打击计算机犯罪保护社会安全。在本章稍后的几节中，你将学习到美国的一些法律，如计算机欺诈和滥用法案(Computer Fraud and Abuse Act)、电子通信隐私法案(Electronic Communications Privacy Act)、阻止盗用和伪装身份法案(Identity Theft and Assumption Deterrence Act)，以及这些法律如何对严重计算机犯罪予以刑事处罚。通过法院系统为过去被认为无害的冒犯法律的行为裁定漫长的刑期，拥有技术专长的检察官能够与执法机构一起狠狠地打击“地下黑客”。

在美国，政府中各个级别的立法机构通过选举代表建立刑法。在联邦一级，众议院和参议院为了使刑法法案变成法律，法案必须获得多数议员通过(在大多数情况下)。一旦通过，这些法律便成为联邦法律，并在联邦政府具有管辖权的案件中生效(主要包括州间贸易的案件、跨越州边界的案件或者违反联邦政府本身法律的案件)。如果不能应用联邦一级的司法权，那么州的主管当局将使用类似方式由州立法机构通过的法律处理这些案件。

所有联邦和州的法律都必须遵守美国宪法，它是规定美国政府系统如何工作的文档。所有的法

律都要受到地方法院的司法审查，有向美国最高法院请求上诉的权利。如果法院发现某个法律是违反宪法的，那么就有权力驳回该法律并认定其无效。

需要记住的是，刑法是非常严肃的。如果发现自己卷入刑事当局的案件中并成为计算机犯罪的证人、被告或受害者，那么建议向熟悉刑法系统和了解计算机犯罪问题的律师寻求帮助。在如此复杂的系统中，采取“独自应对”的态度是不明智的。

4.1.2　民法

民法形成了法律体系的大部分。它们用于维护社会秩序，并管理不属于犯罪行为但需要一位公正的仲裁者来解决的个人之间和组织之间的问题。由民法进行判决的问题类型的例子包括：合同纠纷、不动产交易、雇佣问题、财产/遗嘱规程。民法还被用于创建政府框架，行政机构使用这个体系架构来履行自己的职责。这些法律为政府活动提供了预算，并且安排管理机构授权允许行政机构创建行政法(参见下一节)。

制定民法的方式与刑法相同。在成为法令之前，它们必须通过立法程序，并且受到相同宪法的限制和司法审查过程。在联邦级别，刑法和民法都被收录在美国法典(United States Code，USC)中。

民法和刑法的主要差异在于它们执行的方式。通常，执法当局不会卷入超出采取必要的措施以恢复正常秩序的刑法问题。在刑事诉讼方面，政府通过执法调查员和检察官对被指控犯罪的人采取措施。在民事问题中，它的职责是让那些受到冤枉的人得到法律建议，并提起民事诉讼对付那些应对他们的冤情负责的人。政府(除非是原告或被告)在纠纷或争论的过程中不站在任何一方的立场。在民事纠纷中，政府唯一的作用是提供审理民事诉讼的法官、陪审团和法院设施，并在管理司法系统与法律一致方面扮演行政角色。

与刑法一样，如果认为需要提起民事诉讼或提起的民事诉讼是针对你的，那么最好获得法律帮助。虽然民法中没有关押措施，但是败诉的一方可能面临严厉的经济处罚。我们从每晚播报的新闻中就能发现身边发生的例子，包括起诉烟草公司、大公司和富人赔偿数百万美元的案例。每天都会发生这样的事情。

4.1.3　行政法

政府的行政机构要求众多的机构对保证政府功能的有效性担负广泛的责任。这些机构的责任是遵守并执行立法机构制定的刑法和民法。但是，正如很容易想象到的那样，刑法和民法制定的规则和措施不可能在任何可能的情况下都被遵守。因此，执行机构有制定行政法的回旋余地，从而以政策、规章和制度的方式管理机构的日常运作。行政法涉及的话题可能是小事，如联邦机构购买办公电话的手续，也可以是更重大的问题，如用于执行在国会中通过的法律的移民政策。行政法被颁布在美国联邦法规中，通常被称为 CFR(Code of Federal Regulations)。

虽然行政法不需要立法机构的法案来获得法律的效力，但是必须遵守所有已存在的民法和刑法。政府机构不能执行与立法机关通过的现行法律直接相矛盾的规章制度。此外，行政法(和政府机关的活动)也必须遵守美国宪法并接受司法审查。

为了理解合规要求和程序，必须充分熟悉法律的复杂性。从行政法到民法再到刑法(一些国家甚至有宗教法)，操纵监管环境是一项艰巨的任务。CISSP 考试重点在于法律、法规、调查和合规的概述，因为它们对组织安全工作有影响。然而，你的责任是向专业人员(如律师)寻求帮助，从而指导

和支持从事的维护法律以及法律所支持的安全工作。

4.2 法律

下面我们将讨论许多与信息技术有关的法律。根据需要，这些讨论都是以美国为中心的，CISSP 考试会涉及这些内容。我们还将介绍几种立场鲜明的外国法律，如欧盟的数据隐私法案。不过，如果你所在的环境涉及外国的司法权限，那么就应该请本地的法律顾问来指导你了解他们的法律系统。

警告：

每一位信息安全方面的专业人士都应该对涉及信息技术的法律有一个基本了解。然而，应该学习的重要一课是知道何时向法律专家咨询。如果你认为自己正处在法律的“灰色区域”，那么最好寻求专家的建议。

4.2.1 计算机犯罪

被立法者确定的第一起计算机安全问题是那些涉及计算机犯罪的事件。早期的计算机犯罪诉讼依据传统的刑法，许多案件都被拒绝受理，这是由于法官认为：如果将传统的法律应用到这种现代类型的犯罪中，那么扩展的范围太广。为此，立法者通过了特殊的法令，法令中对计算机犯罪进行了定义，并为各种罪行设置了具体的处罚措施。接下来，我们将介绍其中的几种法令。

提示：

本章中讨论的美国法律是联邦法律。几乎每个州都针对计算机安全问题制定了一些立法形式。由于互联网在全球的延伸，大多数计算机犯罪都跨越了州的边界，因此落在了联邦司法权限之内并在联邦法院系统中进行诉讼。不过，在某些环境中，州法律可能比联邦法律更具有限制性，并且处罚更严厉。

1. 计算机诈骗和滥用法案

美国国会在 1984 年首先制定了计算机欺诈和滥用法案(CFAA)，并且通过一些修正后，直到今天仍然在执行。这条法律经过精心编写，专门用于跨越州边界的计算机犯罪，避免违反州的权力和践踏宪法。法案的主要条款主要针对下列这些罪行：

- 没有经过授权或超出了权限范围而访问联邦系统中的机密信息或财务信息。
- 没有经过授权而访问只能由联邦政府使用的计算机。
- 使用联邦计算机进行欺诈活动(除了欺诈的唯一目标是要使用计算机本身)。
- 对联邦计算机系统造成恶意损失超过 1000 美元的行为。
- 修改计算机中的医疗记录，从而影响或可能影响个人的检查、诊断、治疗或医疗看护。
- 非法买卖计算机密码，如果非法买卖行为影响了州间的贸易或涉及联邦的计算机系统。

计算机欺诈和滥用法案在 1986 年经过了修正，法案的作用范围也有所改变。除了处理敏感信息的联邦计算机之外，法案中还包括了所有的涉及联邦利益的计算机，这样就拓展了法案的范围，如下所示：

- 由美国政府专门使用的所有计算机。

- 由金融机构专门使用的所有计算机。
- 当犯罪活动妨碍了政府或机构使用系统的能力时，由政府或金融机构专门使用的计算机。
- 不处在同一个州的被用于犯罪活动的所有计算机的组合。

提示：

准备 CISSP 考试时，需要保证能够简要描述本节所讨论的每个法律的目的。

2. CFAA 修正案(1994 年)

在 1994 年，美国国会认识到自从 CFAA 于 1986 年最后一次修正以来，计算机安全的面貌已经发生了彻底的变化，于是对该法案进行了许多次大范围的修改。总的来说，这些变化被称为计算机滥用修正法案，其中包括下面这些条款：

- 宣布那些可能造成计算机系统损害的、生成任何类型恶意代码的行为是不合法的。
- 修改了 CFAA，包含了所有被用于州间贸易的计算机，而不只是包含用于联邦利益的计算机系统。
- 允许关押罪犯，不管他们是否造成了实际的损坏。
- 为计算机犯罪的受害者提供了提起民事诉讼的法律权力，对受到的损失可以申请获得减轻和补偿。

2015 年，奥巴马总统提议对计算机犯罪和滥用法案进行重大修改，计划把计算机犯罪放入反诈骗腐败组织集团犯罪法(RICO)条款范围中，用于打击有组织的犯罪。截至本书印刷时，那个提案仍然悬而未决。

3. 计算机安全法案(1987 年)

CFAA 在 1986 年修正之后包括了范围广泛的计算机系统，美国国会将注意力转向了内部，并且调查了当前联邦政府系统中计算机安全的状况。美国国会成员对他们看到的情况很不满意，进而制定了计算机安全法案(CSA，1987 年)，为所有的联邦机构设置了安全要求基准。在引入 CSA 时，美国国会详细规定了法案的 4 个主要目的，如下所示：

- 授予美国国家标准技术研究所(NIST)开发联邦计算机系统标准和准则的职责，包括负责为联邦计算机系统开发标准和准则。在适当时使用美国国家安全局(NSA)的技术性建议和援助(包括工作产品)。
- 颁布这些标准和准则。
- 要求包含敏感信息的联邦计算机系统的所有操作人员制定安全计划。
- 要求包含敏感信息的联邦计算机系统所涉及的所有管理、使用和操作人员强制性参加定期培训。

这条法案中宣布的许多要求经过很多年形成了美国联邦计算机安全策略的基础，而且还将计算机安全的责任分摊给两个联邦机构。原来美国国家安全局(NSA)对所有的计算机安全问题都有权限，现在只保留了对机密系统的权限。美国国家标准技术研究所(NIST)获得了负责保护其他所有联邦政府系统的权利。NIST 发布的专业出版物 800 系列与联邦政府的计算机安全相关。这些对于安全从业者是有用的，并且可以免费从网站上获得：http://csrc.nist.gov/publications/PubsSPs.html。

4. 美国联邦判决指导方针

1991 年发布的美国联邦判决指导方针提供了处罚指导方针，从而帮助联邦法官解释说明计算机犯罪的相关法律。如下所示，这些指导方针的三个条款对信息安全团体产生了持久的影响：

- 指导方针使审慎者规则成为书面形式，这种规则要求高级行政长官个人负责确保平常的适度关注，审慎的个人会经历相同的情况。这条在财政责任领域中开发的规则现在也被应用于信息安全领域。
- 通过证明使用适度关注来履行自己的信息安全责任，指导方针允许组织和行政长官遭受最小的违法处罚。
- 指导方针概述了三个为疏忽提供证据的责任。首先，被控疏忽的人员必须具有法律上认可的责任。其次，被控人员必须未遵守公认的标准。最后，疏忽行为和随后的受损之间必须存在因果关系。

5. 美国国家信息基础设施保护法案(1996 年)

1996 年，美国国会还通过了对计算机诈骗和滥用法案的一系列修正案，从而进一步扩展了其提供的保护范围，其中包括了下面这些新覆盖的领域：

- 放宽了法案的范围，除了用于州间贸易的计算机系统，还包括用于国际贸易的计算机系统。
- 扩展了对国家基础设施(除了计算系统外还有铁路、燃气管道、电网和通信线路)的类似保护。
- 对于故意的或不计后果的造成国家基础设施重要部分损坏的行为，作为重罪处理。

6. 文书精简法案(1995 年)

文书精简法案(1995 年)要求机构在请求大多数类型的公共信息之前，必须获得美国行政管理和预算局(Office of Management and Budget，OMB)的批准。信息收集包括表格、会谈、记录保存要求以及其他各种行为。2000 年的政府信息安全改革法案(Government Information Security Reform Act，GISRA)对文书精简法案进行了修正。

7. 政府信息安全改革法案(2000 年)

2000 年的美国政府信息安全改革法案(GISRA)修正了美国法典，从而实施了额外的信息安全策略和措施。在该法案的文本中，美国国会为建立 GISRA 设置了下列 5 个基本目标：

- 提供内容全面的体制，从而建立和确保控制那些支持联邦工作和资产的信息资源的有效性。
- 认识到联邦计算环境高度网络化的特点，其中包括联邦政府协同工作能力的需要以及改善的安全管理措施的实现，从而保证协同工作的能力不会受到负面影响。
- 提供有效的政府范围内的管理以及监督与安全风险相关的信息，包括贯穿所有市民、国家安全和执法社区的信息安全工作。
- 为保护联邦信息和信息系统安全所需的最小控制措施提供开发和维护。
- 为联邦机构信息安全程序的监督措施的改进提供机制。

GISRA 的条款继续要求美国国家标准技术研究所和美国国家安全局负有安全监督的责任，二者分别负责非机密的和机密的信息处理系统。然而，GISRA 将维护政府信息和信息系统的安全性和完整性的担子放在了个别机构领导者的肩上。

GISRA 还创建了一种新的计算机系统类别。关键任务系统满足下面的标准之一：

- 被其他法律条款定义为国家安全系统。
- 由为机密信息而建立的措施保护。
- 对所处理的信息发生丢失、误用、泄露或未经授权的访问，或者对所处理的信息的任何修改都会对机构的任务产生不良影响。

GISRA 为美国国防部长和中央情报首长的关键任务系统提供了具体的评估和审计权限。这是一种尝试，从而保证所有的政府机构，甚至是那些日常工作中不处理国家机密安全信息的机构，在对机构持续运转方面绝对重要的系统上实施充分的安全控制措施。

注意：

在过去的 10 年里，美国国会没有通过任何新的关于计算机犯罪的重大事项，但是有股力量在最近推动制定新的法律。值得注意的失败事例包括：2012 年的网络安全法案和 2013 年的网络情报共享和保护法案。

尽管这些条例没有通过成为法律，但是很有可能推动继续颁布新的网络犯罪法律，并且新的规定正在冉冉升起。

8. 美国联邦信息安全管理法案

在 2002 年通过的美国联邦信息安全管理法案(Federal Information Security Management Act，FISMA)要求联邦机构实施一个信息安全项目，这个项目要覆盖机构部门的运营。FISMA 同样也要求政府部门，包括承包商在内的活动在安全管理项目内。美国国家标准技术研究所(NIST)负责开发 FISMA 实施指南，概括了下面的关于一个有效信息安全项目的要素：

- 定期评估风险，包括可能由未授权的访问、使用、信息披露、破坏、修改，或由信息破坏和支撑着组织运营的系统以及组织的资产导致的伤害，将它们降低到最小。
- 基于风险评估的策略和程序，在成本效益原则下把信息安全风险降低到一个可接受的级别，以及确保信息安全贯穿于组织每个信息系统的整个生命周期中。
- 下级计划为网络、设施、信息系统或信息系统群体提供恰当的信息安全。
- 通过安全意识培训去告知每个人(包括承包商和其他支撑着组织运营和资产的信息系统用户)，信息安全风险关系到他们的活动和责任，要遵守为了降低这些风险由组织设计的策略和程序。
- 定期测试和评估信息安全策略、程序、实践和安全控制的有效性，执行频率取决于风险，但每年至少一次。
- 规划、实施、评估和记录补救措施的过程，去解决信息安全策略、程序和组织实践中任何不足的地方。
- 制定对信息安全事件检测、报告和响应的流程。
- 制定计划和程序来确保支撑着组织运营和资产的信息系统的持续运行。

FISMA 给联邦机构和政府承包商带来了很大责任，联邦机构和政府承包商必须开发和维护他们在 FISMA 合规方面的大量资料。

4.2.2　知识产权

在全球经济中，美国的角色正在从产品的制造商转变为服务的供应商。这个趋势也在世界大部

分的工业化国家中体现出来。随着向服务供应商的转变，知识产权在许多公司中担任着越来越重要的角色。实际上对于许多大的跨国公司，最有价值的资产只是我们已经逐渐认识到的品牌名字和公司名称，如 Dell、Proctor & Gamble 和 Merck，他们是产品信誉的保证。出版公司、电影制片人和艺术家依靠他们富有创造力的思想赢得生存。许多产品是依靠秘密处方或生产技术得以发展，例如，可口可乐公司富有传奇色彩的饮料秘密处方或者 Colonel 公司秘密的香草和香料的混合产品。

这些无形的资产被总称为知识产权，并且存在一整部保护所有者权利的法律。毕竟，如果一家音乐商店只购买每位艺术家光盘的复制品，并为所有的客户刻录复制的光盘，这样做就太不公平了，这是剥夺艺术家的劳动成果。接下来，我们将介绍与 4 种主要知识产权类型(版权、商标权、专利权和商业秘密)相关的法律，并且还将讨论这些概念如何与信息安全专家相关联。许多国家以不同的方式保护(或不予以保护)这些权力，但是基本的概念在世界各地大体相同。

1. 版权和数字千禧年版权法案

版权法保护“原创作品”的创作者，防止创作者的作品遭到未经授权的复制。目前有下列 8 种主要的作品类别受到版权保护：

- 文学作品
- 音乐作品
- 戏剧作品
- 哑剧和舞蹈作品
- 绘画、图形和雕刻作品
- 电影和其他音像作品
- 声音录音
- 建筑作品

软件版权属于文学作品这一类。然而，注意到下面这一点很重要：版权法只保护计算机软件中内在的表达方式，也就是实际的源代码，不保护软件背后的思想或过程。目前还有一些问题是，关于版权是否可以被延伸到包括软件包的图形用户界面的“外观”。法院判决对于这类问题已经给出了两种看法，如果卷入了这类问题，那么应该向知识产权方面的资深律师进行咨询，以便确定当前的立法状态和相关的法律案例。

目前有一个正规的过程可以获得版权，将受到保护的作品连同注册费用一起送到美国国会图书馆。有关这个过程的更多信息，请访问网站 www.copyright.gov。然而，注意到下面这一点很重要：正式登记版权不是实施版权的先决条件。实际上，法律规定作品的创作者从作品产生出来起就立即自动享有版权。如果能在法院证明你就是作品的创作者(也可能是发行者)，那么你就会受到版权法的保护。正式注册只是让政府承认他们在具体的日期收到了你的作品。

版权的所有权总是属于作品的创作者。这个政策的特例是：作品是租用的。员工在日常工作期间生产出的作品被认为是“租用的”。例如，当某位员工在公司的公共关系部门写了一篇新闻稿时，该新闻稿就被认为是租用的。当作为书面合同的一部分声明作品是租用时，那么这件作品也被认为是租用的。

目前的版权法提供了一个相当长的保护时间。有一位或多位创作者的作品，被保护的时间是直到最后一位创作者死后 70 年。租用的作品和匿名作品被保护的时间是以下两项中时间较短者：从第一次发表日期起的 95 年，或从创作日期起的 120 年。

在 1998 年，美国国会认识到迅速变化的数字技术正在延伸至现行的版权法。为了迎接这个挑战，

他们制定了引起广泛讨论的数字千禧年版权法案(Digital Millennium Copyright Act，DMCA)。DMCA 还被用于使美国的版权法符合世界知识产权组织(World Intellectual Property Organization，WIPO)条约中的两个条款。

DMCA 的第一个主要条款是阻止那些挫败版权保护机制的企图，这些保护机制由版权所有者用于受保护的作品。这个条款被设计用于保护阻止复制数字介质的机制，如 CD 和 DVD。DMCA 对重复罪行规定了高达 100 万美元和 10 年监禁的处罚。非营利性机构(如图书馆和学校)被从这个条款中免除。

DMCA 还限制了当网络服务提供商的线路被罪犯用来违反版权法时应当承担的责任。DMCA 认识到，ISP 的法律地位与电话公司“普通运营商”的地位类似，并且对于他们的用户的暂时性行为不承担责任。为了符合免除条件的资格，服务提供商的活动必须符合下列各项要求(直接引用于 1998 年 12 月美国版权办公室摘要，数字千禧年版权法案)：

- 传输必须由提供商之外的某个人发起。
- 传输、路由、连接准备或复制必须由自动化的技术过程执行，而不是由服务提供商进行选择。
- 服务提供商不能决定数据的接收者。
- 任何中间的复制品除了预期的接收者以外，不能让任何人访问，并且保留的时间不能超过合理的需要时间。
- 不能修改所传输数据的内容。

DMCA 还免除了服务提供商有关系统缓存、搜索引擎和个人用户在网络上存储信息的活动。然而，在这些情况中，服务提供商必须采取迅速的行动，在接到侵权通知之时删除受版权保护的内容。

美国国会在 DMCA 中还包括了这样的条款，允许备份计算机软件和维护、测试或需要复制软件的日常活动。这些条款只应用于经过许可的在特定计算机上使用的软件，用法要符合许可证协议，并且这些复制品在不再需要允许的活动时必须被立刻删除。

最后，DMCA 清楚地说明了版权法原则在新兴的 Web 广播领域中的应用。所谓 Web 广播，即通过互联网以广播形式，将音频和/或视频内容传送给接收者。这种技术通常被称为流式音频或流式视频。DMCA 声明，这些使用被认为是“合法的非预定传输”。这个领域的法律仍然在发展之中，因此，如果计划参与这种类型的活动，那么应该咨询一位律师，以确定符合当前的法律要求。

提示：

留意《反假冒贸易协议》的发展，它提出了一个关于国际知识产权执法保护的框架。自 2015 年 2 月起，该条约就在等待欧盟成员国、美国和其他 5 个国家的批准。

2. 商标

版权法被用来保护创造性的作品，对于商标也有保护。商标是单词、口号和标志语，被用于标识某家公司及其产品或服务。例如，一家公司可能获得了自己的销售说明书的版权，从而保证竞争对手不能复制其销售材料。同一家公司还可能寻求获得商标保护，从而保护公司名称以及提供给客户的特殊产品和服务的名称。

保护商标的主要目的是在保护个人和组织的知识产权时避免市场发生混乱。与版权的保护一样，为了获得法律的保护，商标不需要正式注册。如果在公众活动期间使用了商标，那么你会自动受到相关商标法的保护，并可以使用™符号来表示出想要保护作为商标的单词或口号。如果想让别人正

式承认商标，那么可以在美国专利和商标局(United States Patent and Trademark Office，USPTO)进行注册。这一过程通常需要律师对已存在的商标尽职尽责地做一次全面搜索，以排除注册时的障碍。整个注册过程从开始到完成可能需要一年多的时间。一旦收到来自 USPTO 的注册证书，就可以使用®符号来表示标记是已注册的商标。

商标注册的一个主要好处是：可以注册一个想要使用的商标，但不必是已经使用的商标。这种类型的应用被称为“使用意向(intent to use)”，并且从提供文档的申请之日起保护商标权(假定在特定期限内将商标真正投入商用)。如果选择不向 PTO 注册商标，那么保护从第一次使用商标时开始。

在美国，接受商标应用主要有下列两个要求：

- 该商标不能与其他商标类似，以免造成混淆。这需要在律师尽职搜索期间予以确定。在该商标的开放接受反对意见期间，其他公司可以对应用的商标提出质疑。
- 该商标不应该对所提供的产品和服务加以描述。例如，“Mike’s Software Company”就不是一个好的商标候选名称，因为它描述了该公司生产的产品。如果 USPTO 认为该商标具有描述性，就可能拒绝它的应用。

在美国，商标准许的初始期是 10 年，年限到了可以再连续不受限制地使用 10 年。

3. 专利权

专利权是保护发明者的知识产权。他们提供 20 年的保护，在这期间发明者具有独家使用发明的权力(无论是直接使用还是通过许可协议)。在专利专用期结束时，该发明在公共领域允许任何人使用。

专利权有下列三个主要的要求：

- 该发明必须是新的。只有在发明是原始创意时，才能申请专利。
- 该发明必须是有用的。它必须能够实际工作并完成某种类型的任务。
- 该发明不能是显而易见的。例如，你不能为你的主意(即使用喝水的杯子收集一杯雨水)而获得专利权。然而，你可以设计一个特殊的杯子，能优化收集到的雨水，并且将蒸发量减到最少，这个解决方案就可以获得专利。

在技术领域中，专利权已经被长期用于保护硬件设备和制造过程。在这些方面存在丰富的发明者的先例。最近被发布出来的专利涉及软件程序和类似的机制，但是仍由陪审团公开这些专利是否在法庭上进行审查。

4. 商业秘密

很多公司都有知识产权，这对于他们的业务绝对关键，并且如果泄露给竞争对手和/或公开，那么就会导致相当大的损害。换句话说，这也就是商业秘密。之前我们曾提到这种公众文化信息类型的两个例子，可口可乐公司的秘方和肯德基公司的“香草和香料的混合秘密”。其他的例子还有很多，制造公司可能希望保持某种生产过程的秘密，这个秘密只有少数重要员工完全理解，或者统计分析公司可能希望对为内部使用而开发的先进模型进行保护。

前面讨论的版权和专利这两种知识产权工具可能被用于保护这种信息类型，但是却具有下列两个主要缺点：

- 提出版权或专利应用申请时，要求公开地透露你的工作或发明的细节。这自动去除了产权的“秘密”特性，并且可能由于去除了产品的神秘或者允许不择手段的竞争对手违反国际知识产权法拷贝你的产权而对公司造成伤害。

- 版权和专利都提供有限时间的保护。一旦合法保护过期，那么其他公司就可以随意使用你的工作成果(并且他们拥有在申请过程中公开透露的所有细节)。

官方关于商业秘密的处理过程实际上没有那么多，就它们的本质而言，不必向任何人登记，而是自己保持秘密。为了保持秘密，必须对企业实施适当的控制，确保只有经授权的需要了解这些秘密的人才可以访问这些秘密。还必须确保任何具有这类访问能力的人遵守不泄漏协议(NonDisclosure Agreement，NDA)以防止与他人共享，并且对违背协议的行为进行处罚。向律师咨询一下，确保协议能够持续法律准许的最长时间。此外，必须采取措施来证明你的价值，并保护你的知识产权。如果不这样做，可能会导致商业秘密保护的损失。

商业秘密保护是保护计算机软件的一种最好方法。正如前面所讨论的，专利法没有为计算机软件产品提供适当的保护。版权法只保护源代码的实际正文，并且没有禁止其他人以不同的形式重写代码并达到相同的目标。如果将源代码作为商业秘密，那么首先需要不要使它落在竞争者的手中。这是像 Microsoft 这样的大型软件开发公司用于保护知识产权核心基础的技术。

经济间谍法案(1996 年)

商业秘密常常是大公司的制胜法宝，美国政府在国会颁布经济间谍法案(1996 年)时认识到保护这种知识产权类型的重要性。这项法律有下列两个主要规定：

- 任何被发现带有为外国政府或机构获利的意图而从美国公司窃取商业秘密的人可以被处以高达 50 万美元的罚款和长达 15 年的监禁。
- 任何被发现在其他情况中窃取商业秘密的人可以处以高达 25 万美元的罚款和长达 10 年的监禁。

经济间谍法案的条款给予商业秘密拥有者知识产权权利的真正保护。这项法律的强制实施要求公司采取适当的步骤，确保其商业机密受到良好保护，并且不会意外地放到公共区域。

5. 许可证

安全专家还应当熟悉软件许可证颁发协议的相关法律问题。许可证具有下列 4 种类型：

- 合同许可证协议在软件商和用户之间采用书面的合同概述双方的责任。这些协议常见于高价的和/或特别专用的软件包。
- 收缩性薄膜包装的许可证协议是写在软件包装外面的协议。由于常常规定撕开封装软件包的收缩薄膜包装就承认了合同条款，因而得名。
- 单击包装许可证协议比收缩性薄膜包装协议更普遍。在这种协议类型中，合同条款或者写在软件包装盒外，或者包括在软件文档中。在安装过程中，你被要求单击一个按钮，表示已经阅读了协议条款并且同意遵守这些条款。这为协议的认同过程增添了积极的认可，确保使用者在安装之前知道协议的存在。
- 云服务许可协议让单击协议走向了极端。大部分云服务不需要任何形式的书面协议，而是在屏幕上简单闪现法律条款供检阅。在一些情况下，它们也许简单地为用户提供一个到法律条款的链接，以及一个确认已经阅读并同意条款的确认框。对于兴奋地访问一个新服务的大部分用户，他们不阅读协议就简单单击通过，这可能无意中使他们的整个组织负有法律责任的条款和条件。

统一计算机信息处理法案

统一计算机信息处理法案(Uniform Computer Information Transactions Act，UCITA)是被所有 50 个州都采纳的美国联邦法律，它提供了计算机相关业务处理行为的共同架构。UCITA 包括对软件许可证颁发的规定。UCITA 条款对先前可疑的收缩性薄膜包装许可证和单击包装许可证颁发行为提供了法律援助，从而将它们变为有法律约束力的合同。UCITA 还要求生产制造者为软件用户提供选择，用户可以在完成安装过程之前拒绝许可证协议的条款，并且能够收到软件订购价格的全额退款。

提示：

两个重要的行业团体提供了关于软件许可证颁发的指导和强制操作。可以从他们的网站上获得更多的信息。商业软件联盟的网站是 www.bsa.org。

4.2.3 进口/出口

美国联邦政府认识到，驱动互联网和电子商务发展的、非常类似的计算机和加密技术，还可能成为军用的强大工具。因此，在冷战期间，美国政府出台了一套复杂的规定，以便控制向其他国家出口敏感的硬件和软件产品。规定包括新技术、知识产权和个人身份信息的跨境数据流管理。

直到最近，除了一些选择的盟国之外，向美国以外国家或地区出口强大能力的计算机还是很难的事情。对于加密软件的出口控制甚至更严，实质上向美国以外国家或地区出口加密技术是不可能的。最近美国联邦策略的一些改变已经放松了这些限制，从而提供更加开放的商业环境。

1. 计算机出口控制

当前，美国公司可能将高性能的计算机系统出口到事实上没有受到美国政府事先许可的一些国家。如果某些国家被美国商务部的工业和安全局认为，它们构成核扩散问题、支持恐怖主义或与此相关，那么对这些国家来说这条“规则”就是例外的。

注意：

可以从美国商务部的网站www.bis.doc.gov找到这些国家的完整列表和他们相应的计算机出口等级。

2. 加密产品出口控制

美国商务部的工业和安全局对向美国以外的国家出口加密产品建立了又一个规定。在前面的规定中，事实上即使向美国以外的国家出口相对低等级的加密技术也是不可能的。这使得美国的软件制造商与没有这些限制的外国公司相比，具有很大的竞争劣势。在经过软件企业的长期游说之后，美国总统指示美国商务部修订其规定，以促进美国安全软件业的成长。

现在的规定定义了安全软件的零售种类和大规模市场销售。现在这些规则准许公司提交这些产品，由美国商务部进行复审，但是复审将不会超过 30 天，在复审成功地完成后，这些公司就可以自由地出口这些产品。

4.2.4　隐私

在美国，隐私权已经成为多年来争论的热门问题。争论的主要问题是宪法的权利法案没有明确规定隐私权。然而，很多法院都已经支持这个权力，并且像美国公民自由协会(American Civil Liberties Union，ACLU)这样的组织也在积极地追求这个权力。

欧洲人同样一直在关注他们的隐私。实际上，像瑞士这样的国家由于其保护财务秘密的能力已为世界所知。在本节的后面部分，我们将研究新的欧盟数据隐私法如何影响这些公司和互联网用户。

1. 美国隐私法

虽然隐私没有宪法的保障，但还是有数量众多的美国联邦法律(很多都是最近几年颁布的)被用于保护政府维护的隐私信息，这些信息有关公民以及私营机构中的重要部门，如财务、教育和卫生机构。接下来，我们将对这些联邦法律中的许多法律进行研究。

第四修正案　隐私权的基础是美国宪法的第四修正案，内容如下所示：

人们保护其人身、房屋、证件和财物不受无理搜查和没收的权利不应当被违反，并且这些违反行为不应得到授权批准，但是那些可能性很大的原因、受到誓词或证词支持的、特别描述的需要搜查的地方和需要被逮捕或扣押的人或物品除外。

这个修正案的直接解释防止了美国政府机构在缺乏授权批准和可能性很大的原因的情况下对私有财产进行搜查。一些美国法院已经扩展了其对第四修正案的解释，包括针对窃听和侵犯其他隐私的防护。

隐私法案(1974 年)　美国的隐私法案(1974 年)可能是对美国联邦政府处理公民个人私有信息的方法进行限制的最重大的隐私立法，它严格地限制了美国联邦政府机构在没有事先得到当事人书面同意的情况下向他人或其他机构泄漏隐私信息的能力。这个法案还规定了一些例外，涉及人口普查、执法、国家档案、健康和安全以及法院判决。

隐私法案要求政府机构只维护那些对于管理其业务必要的记录，并且在政府的合法职能不再需要时销毁这些记录。它为个人对这些政府维护的记录进行访问并要求修正不正确的记录规定了正式的程序。

电子通信隐私法案(1986 年)　电子通信隐私法案(Electronic Communication Privacy Act，ECPA)使得对个人电子隐私的侵犯成为犯罪行为。这个法案更新了联邦窃听法案，以便应用于非法的电子(也就是计算机)通信侦听或者对于以电子形式存储的数据的有意和未授权访问。ECPA 禁止侦听或泄漏电子通信，并且定义了公开电子通信的合法情况。该法案对电子邮件和语音邮件通信的监视提供了防护，并且防止这些服务的提供商对这些内容进行未授权的公开。

ECPA 最著名的规定是使得对蜂窝电话通信的监听成为非法。实际上，这种监听会被处以最高 500 美元的罚款和最高 5 年的监禁。

执法通信协助法案(1994年)　执法通信协助法案(Communication Assistance for Law Enforcement Act，CALEA)是对1986年的电子通信隐私法案的修正。CALEA 要求：无论采用怎样的技术，所有通信运营商都需要允许持有适当法院判决的执法人员进行窃听。

经济和专有信息保护法案(1996年)　经济和专有信息保护法案将财产的定义扩展为包括经济信息，从而可以将窃取这类信息的行为视作针对行业或公司的间谍行为。这个法案修改了盗窃的法律定义，从而使这种行为不再受到物理约束。

健康保险流通与责任法案(1996 年) 1996 年，美国国会通过了健康保险流通与责任法案(Health Insurance Portability and Accountability Act，HIPAA)，这使得管理健康保险和健康保护组织(Health Maintenance Organization，HMO)的法律发生了许多变化。在 HIPAA 的条款中，隐私和安全法规要求医院、医师、保险公司和其他处理或存储个人医疗隐私信息的组织采取严格的安全措施。

HIPAA 还明确地定义了个人在医疗记录方面的权利，并且要求保存医疗记录的组织书面表明这些权利。

注意：

HIPAA 隐私和安全法规很复杂。你应当熟悉这个法案的广义意图。如果你在卫生保健行业工作，那么就应当考虑花费时间对这个法律规定进行深入研究。

2009 关于经济和临床健康的卫生信息技术法案 在 2009 年，美国国会通过了“关于经济和临床健康的卫生信息技术法案(Health Infomation Technology for Economic and Clinical Health，HITECH)”来修订 HIPAA。这条法律更新了许多 HIPAA 的隐私和安全需求，并于 2013 年通过 HIPAA Omnibus Rule 实施。

被新法规强制变化的其中之一就是在法律对待商业伙伴(Business Associate，BA)的方式上，处理被保护的健康信息(Protected Health Information，PHI)的组织机构代表了 HIPAA 覆盖的实体。覆盖实体和一个 BA 之间的任何关系必须被书面合同管理，这个合同被称为业务联合协议。

HITECH 也引入了新的数据泄露通告需求。在 HITECH 违约通知规则下，经历了数据泄露的 HIPAA 覆盖实体必须通知受影响的个人，当泄露影响超过 500 人时，必须通知卫生和人力服务部的部长和媒体。

数据泄露通知法

HITECH 的数据泄露通知规则的独特之处在于，它是一个由联邦法律授权的影响个人的通告。在超出医疗记录的要求范围之外，数据泄露通知的要求在各州是不相同的。

在 2002 年，加利福尼亚州通过了 SB 1386 并且成为第一个公开已知或疑似违反个人身份信息的州，这包括与下面信息有关联的个人名字的未加密副本：

- 社会保险号
- 驾照号码
- 身份证号码
- 信用卡或借记卡号码
- 银行账户与安全代码、存取码或口令等能够允许访问账户的信息
- 病历
- 医疗保险信息

在 SB 1386 颁布后的几年间，许多(并非所有)另外的州通过了相似的法令，这些法令都是从加利福尼亚州的数据泄露通知法修订过来的。截至 2015 年，只有阿拉巴马州、新墨西哥州和南达科他州还没有数据泄露通知法。

注意：

对于各州的数据泄露通知法的完整列表，请参阅 www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx。

儿童联机隐私保护法案(1998 年)　2000 年 4 月，儿童联机隐私保护法案(Children's Online Privacy Protection Act，COPPA)中的规定成为美国本土的法律。COPPA 对关心孩子或有意收集孩子的信息的网站提出了一系列要求：

- 网站必须发送隐私通知，清楚地说明他们所收集信息的类型和用途，包括是否有一些信息会泄漏给第三方。隐私通知还必须包括网站工作者的联系信息。
- 必须向父母提供机会，复查任何从他们的孩子那里收集到的信息，并且可以从网站的记录中永久地删除这些信息。
- 如果孩子的年龄小于 13 岁，那么在收集信息前，父母必须对有关孩子信息的收集做出可证实的允许。法律中存在一些例外，准许 Web 站点只是为了获得父母允许收集最少的信息。

Gramm-Leach-Bliley 法案(1999 年)　直到 Gramm-Leach-Bliley Act(GLBA)法案于 1999 年成为法律，在商业机构之间才形成了严格的政府屏障。银行、保险公司和贷款提供商受到对他们所能提供的服务和相互共享的信息的严格限制。GLBA 稍微放松了涉及每个组织所能提供的服务的规定。当美国国会通过了这条法案后，它意识到这扩大了具有深远隐私意义的范围。基于这点考虑，该法案包括了许多限制，对可能在相同公司的子公司之间交换的信息类型进行了限制，并且要求从 2001 年 7 月 1 日开始金融机构对所有用户提供书面的隐私策略。

美国爱国者法案(2001 年)　美国国会对 2001 年 9 月 11 日发生在纽约市和华盛顿哥伦比亚特区的 9•11 恐怖袭击做出了直接反应：通过了提供拦截和阻止恐怖行为所需的适当工具来团结和巩固美国(USA PATRIOT)法案。美国爱国者法案大大扩大了执法机构和情报机构跨多个领域的力量，包括对电子通信的监视。

美国爱国者法案提出的一个主要改变涉及政府机构获取窃听授权的方法。以前，策略只能一次获取一条线路的授权(在证实这条线路被受到监控的某人使用后)。美国爱国者法案规定准许官方获得对个人的一揽子授权，并且随后根据这项单一授权监视此人的所有通信。

另一个主要的改变是政府处理网络服务提供商(ISP)的方式。根据美国爱国者法案中的条款，ISP 可以自愿地向政府提供大范围的信息。美国爱国者法案还准许政府通过使用传唤获取用户活动的详细信息(与窃听相反)。

最后，美国爱国者法案修正了计算机欺诈和滥用法案(是另一组修正案)，从而对犯罪行为处以更严厉的处罚。美国爱国者法案规定了最长 20 年的监禁条款，并再一次扩大了 CFAA 的范围。

子女教育权利和隐私法案　子女教育权利和隐私法案(Family Educational Rights and Privacy Act，FERPA)是另一种特殊的隐私法案，它影响所有接受美国联邦政府资助的教育机构(绝大多数学校)。这个法案赋予 18 岁以上的学生和未成年学生父母的确定的隐私权。具体的 FERPA 保护包括下列内容：

- 父母/学生具有检查由教育机构保存的此学生教育记录的权利。
- 父母/学生具有要求改正他们认为不正确的记录的权利，具有在记录中包括声明争辩任何没有被改正的内容的权利。
- 学校不能不经书面许可而发放学生记录的个人信息，某些特定的情况除外。

身份偷窃和冒用阻止法案(1998 年)　1998 年，美国总统签署了身份偷窃和冒用阻止法案，从而使之成为法律。在过去，只有身份偷窃的合法受害人才是受侵害的债权人。这个法案使得身份偷窃成为对被偷窃身份的个人犯罪行为，并且规定了对任何违反此法律的人处以严厉的犯罪处罚(长达 15 年的监禁条款和/或 250 000 美元的罚款)。

真实场景

工作间内的隐私

本书的一位作者最近与在办公室工作的亲戚进行了一次饶有兴趣的谈话。在家庭的圣诞聚会上，这位亲戚偶然提到在网上读过的一则故事，它讲述了本地某家公司的几位员工由于滥用互联网权限而遭解雇。这位亲戚非常震惊，并且无法相信公司会侵犯员工的隐私权。

正如本章前面所述，美国法院系统长时间以来一直支持传统的隐私权作为基本合法权利的扩展。然而法院一直主张，此权利的一个重要因素是隐私只应当在具有“合理的隐私要求”时受到保护。例如，如果你向某人发送一封密封在信封中的信，那么你有理由期望它在邮寄途中不会被拆开阅读，这就是合理的隐私要求。另一方面，如果通过明信片发送信息，那么你已经知道在信件到达对方之前会有一人或多人看到信件的内容，因此此时没有合理的隐私要求。

最近的法院裁决已经发现员工在工作间内使用店员自己的通信设备时没有合理的隐私要求。如果使用雇主的计算机、互联网连接、电话或其他通信设备发送消息，那么雇主可能会将其作为常规的商业程序进行监视。

也就是说，如果正在计划监视员工的通信，那么就应当采取合理的预防措施，确保没有默许的隐私要求。下面列出了一些可供考虑的常见措施：

- 在雇佣合同的条款中声明员工在使用公司设备时没有隐私要求。
- 在公司可接受的应用和隐私策略中的类似书面声明。
- 登录界面警示所有的通信都受到监视。
- 用计算机和电话上的警示标记警示监控。

与本章中讨论的很多问题一样，在采取通信监控措施之前向律师进行咨询是一种明智的做法。

2. 欧盟隐私法

1995 年 10 月 24 日，欧盟(European Union，EU)议会通过了描绘隐私措施的概括指令，也就是必须采取措施保护信息系统中处理的个人数据。这个指令在 3 年后(1998 年 10 月)生效。指令要求所有个人数据的处理都要满足下列标准中的某一条：

- 同意
- 合同
- 法律义务
- 数据主体的主要利益
- 数据所有者和数据主体之间利益的平衡

如下所示，指令还描述了有关数据被持有和/或处理的个人的重要权利：

- 访问数据的权利
- 知道数据源的权利
- 改正错误数据的权利
- 拒绝在某些情况下处理数据的权利
- 这些权利被违反时应当采取的合法行为

甚至欧洲以外的组织，根据跨境数据流的要求，必须考虑这些规则的适用性。为防止欧盟公民

的个人信息从欧盟泄露出去，这些发送的数据必须确保是受到保护的。在欧洲从事商业活动的美国公司可以根据欧盟和美国之间的谈判获得保护，该谈判准许美国商务部证明业务遵守规定，并且为他们提供“安全避难所”，以免于受到起诉。

为了符合安全避难所规定，在欧洲进行商业活动的美国公司必须满足下列 7 项处理个人信息的要求：

- **通知**　他们必须通知个人收集了什么信息，以及信息将如何使用。
- **选择**　如果信息将被用于其他目的或与第三方共享，那么他们必须准许个人决定退出。对于涉及敏感的信息，必须采取决定参加的策略。
- **向前传递**　企业只可能与其他遵守安全避难所原则的企业共享数据。
- **访问**　个人必须被授权访问任何包含其个人信息的数据。
- **安全**　必须采取适当的机制保护数据，以防止丢失、滥用和未授权的公开。
- **数据完整性**　企业必须采取措施，确保他们所维护信息的可靠性。
- **实施**　企业必须为个人提供争论解决办法，向管理机构提供证明，表明遵守安全避难所规定。

注意：

有关适用于美国公司的安全避难所的更多信息，读者可以查询美国商务部的安全避难所网站 http://export.gov/safeharbor。

4.3　合规性

在过去的 10 年间，信息安全管理的监管环境变得越来越复杂。组织可能会发现自己受到广泛的各种各样的法律约束(其中很多在本章早些时候提到过)，以及来自监管机构或合同义务的强制合规。

真实场景

支付卡行业数据安全标准

支付卡行业数据安全标准(Payment Card Industry Data Security Standard，PCI DSS)是一个非法律但有合同义务的优秀合规要求的典范。PCI DSS 管理信用卡信息的安全，并且有一个商业合同条款，在接受信用卡信息的业务与处理业务交易的银行之间强制执行。

PCI DSS 有 12 个主要要求：

1) 安装和维护防火墙配置来保护持卡人数据。
2) 不要使用供应商提供的系统默认密码和其他安全参数。
3) 保护存储的持卡人数据。
4) 在开放的公共网络下要加密持卡人的传输数据。
5) 防止所有系统受恶意软件入侵，并定期更新杀毒软件或程序。
6) 开发和维护安全系统和应用程序。
7) 根据业务须知，限制对持卡人数据的访问。
8) 访问系统组件要经过标识和认证。

9) 限制对持卡人数据的物理访问。

10) 跟踪和监视所有对网络资源和持卡人数据的访问。

11) 定期测试安全系统和程序。

12) 坚持对所有人宣传信息安全的策略。

这些要求中的每一个在完整的PCI DSS标准中都有详细阐述，可以在 www.pcisecuritystandards.org/ 上找到。

组织在面对和处理许多的交叉和有时相互矛盾的合规需求时，需要仔细计划。许多组织雇佣全职的 IT 合规人员负责跟踪合规环境，监督控制以确保持续合规，促进合规性审核，并满足该组织的合规性报告责任。

警告：

非商业组织在行为上和商业组织一样会存储、处理或传输信用卡信息，但也必须符合 PCI DSS 标准。例如，要求适用于共享主机的供应商，必须保护持卡人数据环境。

组织可能会经受合规性审计，要么通过标准内部或外部审计机构，要么通过监管或其代理。例如，组织的财务审计人员也许主导 IT 控制审计，这种审计被设计用于确保组织金融系统的信息安全控制满足萨班斯-奥克斯利法案的要求。一些合规，例如 PCI DSS，可能要求组织雇佣被认可的独立审计师来证明控制，并直接向监管部门提供报告。

除了正式的审计，组织必须经常把合规遵从报告发送给内部或外部的股东。例如，组织的董事会(或者，更多是董事会的审计委员会)可能需要定期的合规义务和状况的报告。类似地，PCI DSS 非强制地要求组织主导一个正式的第三方审计，从而完成和提交一份自我评估报告，罗列出他们的合规状态。

4.4 合同与采购

使用云服务和其他外部供应商来存储、处理和传输敏感信息的用户逐渐增加，这导致一些组织在他们的合同签订和采购过程中，实施安全审查和控制成为一个新的关注点。安全专家应该主导对供应商部署的安全控制措施进行审查，这包括最初的供应商选择和评估流程，以及作为供应商持续管理过程的一部分。

供应商管理审查中覆盖的一些问题包括：

- 什么类型的敏感信息应该由供应商存储、处理或发送？
- 在部署保护组织信息时有什么样的控制措施？
- 组织的信息如何与其他客户的信息分开？
- 如果加密是一种值得信赖的安全控制措施，那么我们要用什么样的加密算法和密钥长度？密钥管理如何进行？
- 供应商执行了什么类型的安全审计？客户访问这些审计必须做什么？
- 供应商是否依赖于任何其他第三方来存储、处理或传输数据？如何处理扩展到第三方与安全有关的合同条款？
- 数据存储、处理和传输发生在什么地方？如果客户或供应商在国外，会有什么影响？

- 供应商的事件响应流程是什么？什么时候将会通知客户存在潜在安全泄露？
- 在确保客户数据的持续完整性和可用性方面有什么条款？

上面也许只是你关注的一些简要清单。需要裁剪组织专门关注的安全审查范围、供应商提供的服务类型以及与他们共享的信息。

4.5　本章小结

计算机安全必然需要合法团体的高度介入。在本章中，你已经学习了管理安全问题(如计算机犯罪、知识产权、数据隐私和软件许可证颁发)的大量法律。

有三大类法律影响到信息安全专家。刑法概述了规则和对公信度重大违反的制裁。民法为我们提供了一个商业处理的框架。政府机构使用行政法来颁布日常条例，解释现有法律。

管理信息安全活动的法律是多种多样的，并且覆盖了所有的三大类别。一些法律，例如，电子通信隐私法案和数字千禧年版权法案是刑法，违反可能导致刑事罚款或监禁。其他法律，如商标和专利法，是管理商业交易的民法。最后，许多政府机关颁布的行政法，如 HIPAA 安全规则，它们影响着特定行业和数据类型。

信息安全专家应该了解他们的特定行业和商业活动的合规需求。遵守这些要求是一个很复杂的任务，并应分配给一个或多个合规专员，去监控法律中的变化、商业环境中的变化以及这两个领域交集中的变化。

简单地担心自己的安全性和合规性也是不够的。随着越来越多地采用云计算，许多组织现在与那些作为服务提供商的供应商分享敏感信息和个人数据。安全专家必须采取措施，以确保供应商处理数据时像公司自己处理数据一样仔细，并且符合任何适合的合规性要求。

4.6　考试要点

了解刑法、民法和行政法之间的差别。刑法保护社会免遭那些违反我们信奉的基本原则的行为。违反刑法的行为是由美国联邦和州政府进行起诉的。民法提供了个人和组织之间的商业交易体制。违反民法的行为被提交法院并由受到影响的双方进行辩论。行政法是由政府机构使用的，目的是为了有效地执行日常事务。

能够解释用来保护社会免遭计算机犯罪影响的主要法律的基本条款。计算机诈骗和滥用法案(修正案)保护政府或州间贸易使用的计算机不被滥用。计算机安全法案概括了政府为了保护自己的系统免遭攻击而必须采取的措施。政府信息安全改革法案进一步发展了美国联邦政府信息安全程序。

了解版权、商标、专利权和商业秘密之间的差别。版权保护创作者的原创作品，如书籍、文章、诗和歌曲。商标是名称、口号和徽标，用于标识公司、产品或服务。专利权为新发明的创作者提供保护。商业秘密法律保护公司的运营机密。

能够解释数字千禧年版权法案(1998 年)的基本条款。数字千禧年版权法案禁止绕过针对数字介质的复制保护机制，并限制网络服务提供商对于其用户行为的责任。

了解经济间谍法案(1996 年)的基本规定。经济间谍法案对任何被发现偷盗商业秘密的人进行处罚。在盗窃者知道这些信息将为外国政府获利时，他会被处以严厉的处罚。

理解不同类型的软件许可证协议。合同许可证协议是软件商和用户之间采用的书面协议。收缩性薄膜包装协议写在软件包装上，并且在用户打开包装时生效。单击包装协议包括在包装中，但是需要用户在软件安装过程中接受这些条款。

解释关于软件许可证颁发的统一计算机信息处理法案。统一计算机信息处理法案提供了由美国联邦和州政府强制执行的收缩性薄膜包装和单击包装协议的架构。

理解一个经历数据破坏的组织的通告要求。加利福尼亚州颁布的 SB 1386 是第一个在全州范围内要求通告个人信息被泄漏到当事人的法律。美国目前除了三个州以外的其他州都最终审议通过了相似的法律。目前，只有当涉及 HIPPA 覆盖的实体破坏了它们保护的健康信息时，联邦法律才要求需要通知个人。

理解在美国和欧盟管理个人信息隐私的主要法律。美国有很多影响政府对信息的使用以及控制涉及敏感信息的具体行业(如金融服务公司和卫生健康组织)对信息使用的隐私法律。欧盟对数据隐私有着更加广泛的法令，以管理个人信息的使用和交换。

了解法庭上可接纳的证据的基本要求。要被接纳，证据就必须与本案发生的事实相关，事实必须对本案是必要的，并且证据必须有法定资格或是合法收集的。

了解怎么把安全整合到采购和供应商管理流程中。被许多组织大量使用的云服务，就要求更加注意在供应商选择过程中，以及作为供应商持续管理的一部分，引导信息安全控制的审查。

4.7 书面实验室

1. 在欧盟的数据隐私法令下，什么关键因素保障了个人权利？
2. 在考虑外包信息存储、处理和传输时，什么应该是组织应该去问的一些常见问题？
3. 为了向员工通知系统监视，雇主采取的常见措施是什么？

4.8 复习题

1. 对于病毒、密码和其他类型的破坏计算机系统的恶意代码的编写者，下列哪个刑法是第一个去执行惩罚的？
   A. 计算机安全法案
   B. 国家基础设施保护法案
   C. 计算机欺诈和滥用法案
   D. 电子传输隐私法案
2. 哪条法律首先要求美国联邦的相关计算机系统操作者接受计算机安全问题的定期培训？
   A. 计算机安全法案
   B. 国家基础设施保护法案
   C. 计算机欺诈和滥用法案
   D. 电子通信隐私法案
3. 什么类型的法律并不要求国会的法案在联邦一级执行，而是由行政部门以法规、政策和程序的形式颁布？

A. 刑法
B. 普通法
C. 民法
D. 行政法

4. 哪个联邦政府机构有安全责任确保政府计算机系统没有用于处理敏感和/或分类信息？
A. 美国国家安全局
B. 联邦调查局
C. 国家标准和技术协会
D. 联邦情报局

5. 什么是计算机系统最广泛的类别，这个类别受计算机欺诈和滥用方案(修正案)保护？
A. 政府所属系统
B. 联邦相关系统
C. 用于洲际贸易的系统
D. 美国境内系统

6. 在设置对获得政府部门授权的监管部门搜查私人住宅和设施的权利限制方面，什么法律保护了公民的隐私权？
A. 隐私法案
B. 第四修正案
C. 第二修正案
D. Gramm-Leach-Bliley 法案

7. Matthew 最近编写了一个创新的算法去解决一个数学问题，并且他希望与全世界分享。但是，在技术杂志上发布软件代码之前，他想获得一些知识产权方面的保护。下列哪个保护最适合他？
A. 版权
B. 商标
C. 专利
D. 商业秘密

8. Mary 是一家制造企业 Acme Widgets 的联合创始人。与合伙人 Joe 一起，她开发了一个特种油，能显著提高小部件的生产过程。为了保证配方的机密性，Mary 和 Joe 计划在其他工人离开后，由他们自己在厂房里大量生产这种油。他们想尽可能保护这个配方。下列哪个知识产权保护最适合他们？
A. 版权
B. 商标
C. 专利
D. 商业秘密

9. Richard 近期为计划即将开始使用的新产品起了一个不错的名字。他与律师商量并填写相应的申请去保护他的产品名字，但是仍未从政府收到关于他的申请的回应。他想立即开始使用名字。他应该使用什么样的符号来表明他的产品名字处于受保护的状态？
A. ©
B. ®
C. ™

D. †

10. 什么法律禁止政府机构泄露个人提交给政府保护环境下的信息？

A. 隐私法案

B. 电子通信隐私法案

C. 健康保险流通与责任法案

D. Gramm-Leach-Bliley 法案

11. 软件行业使用什么法律来正式地派发大量许可，并试着标准化从一个州到另一个州的使用？

A. 计算机安全法案

B. 统一计算机信息处理法案

C. 数字千禧年版权法案

D. Gramm-Leach-Bliley 法案

12. 儿童联机隐私保护法案被设计用来保护在互联网上使用的儿童隐私。在企业可以从他们那里收集未经父母同意的个人身份信息之前，孩子的最小年龄是几岁？

A. 13

B. 14

C. 15

D. 16

13. 为了获得数字千禧年版权法案的短暂活动条款的保护，下列哪些是互联网服务提供商不用满足的需求？

A. 服务提供商和消息的发起者必须处于不同的状态。

B. 传输、路由、连接的提供或复制必须由一个没有通过服务提供商选择的材料的自动化技术过程来进行。

C. 任何中间副本一般不得让预期外的任何收件人访问，并且不得保留超过合理必要的时间。

D. 传输必须由除供应商以外的人发起。

14. 以下哪一个法律不是为了保护消费者和网民的隐私权？

A. 健康保险易流通与责任法案

B. 阻止盗用和伪装身份法案

C. 美国爱国者法案

D. Gramm-Leach-Bliley 法案

15. 以下哪一项许可协议类型不需要用户在执行之前确认他们已经阅读了协议？

A. 标准许可协议

B. 拆封协议

C. 单击许可协议

D. 口头协议

16. 什么行业受 Gramm-Leach-Bliley 方案中的条款影响最直接？

A. 卫生保健

B. 银行

C. 执法

D. 防护承包商

17. 在美国专利保护期是多长？

A. 提交申请日开始 14 年

B. 专利获得日开始 14 年

C. 提交申请日开始 20 年

D. 专利获得日开始 20 年

18. 在处理关于欧盟数据隐私法令下的个人信息时，以下哪一项不是有效的法律依据？

A. 合同

B. 法律义务

C. 市场需求

D. 赞成

19. 涉及信用卡信息处理时，要符合什么合规义务？

A. SOX

B. HIPAA

C. PCI DSS

D. FERPA

20. 什么法案更新了健康保险流通与责任法案(HIPAA)中的隐私和安全需求？

A. HITECH

B. CALEA

C. CFAA

D. CCCA

第 5 章

保护资产的安全

本章中覆盖的 CISSP 考试大纲包含：

A. 对信息及支持资产进行分类(如敏感性、关键性)

B. 确定及维护所有权(如数据所有者、系统所有者、业务/任务所有者)

C. 保护隐私

- C.1 数据所有者
- C.2 数据处理者
- C.3 数据剩磁
- C.4 收集限制

D. 确保适当地保留资产(如介质、硬件、人员)

E. 确定数据安全控制(如静态数据、传输过程中的数据)

- E.1 基准线
- E.2 审视和定制
- E.3 标准选择
- E.4 密码学

F. 建立处理需求(敏感信息的标记、贴签、存储、破坏)

资产安全领域着重于在信息的整个生命周期中收集、处理和保护信息。在这一领域的主要步骤是根据对组织的价值来分类信息。

所有后续行动都根据分类的不同而不同。例如，高级机密数据要求有严格的安全控制。相比之下，非机密数据需要的安全控制则更少。

5.1 对资产进行分类和标记

资产安全的第一步是对资产进行分类和标记。组织通常包括安全策略中的分类定义。然后人员根据安全策略的要求对资产进行标记。在这种情况下，资产包括敏感数据、用于处理数据的硬件以及用来保存数据的介质。

5.1.1 定义敏感数据

敏感数据指所有不公开或未分类的信息，可能包括组织需要保护的机密、专有信息，或因数据对组织的价值或组织为遵守现行法律、法规而保护的任何其他类型的数据。

1. 个人身份信息

个人身份信息(PII)是指任何可以识别个人的信息。美国国家标准技术研究所(NIST)的专业出版物 800-122 提供了更正式的定义：

任何有关个人的信息，包括：

- 任何可以用来区分或跟踪个人身份的信息，如姓名、社会保障号、出生日期和出生地、母亲的娘家姓或生物学记录。
- 任何其他个人相关信息，如医疗、教育、金融和就业信息。

关键是组织有责任保护 PII。这包括 PII 相关的员工和客户。许多法律要求，如果数据泄露导致 PII 的破坏，组织应通知个人。

提示：

对个人身份信息(PII)的保护对世界各地(特别是北美和欧盟)的规则、规定和立法提出了保密要求。NIST SP 800-122《保护个人身份信息(PII)机密性指南》对于如何保护 PII 提供了更多信息。可以从 NIST 专业出版物(800 系列)下载页面获取此文件：http://csrc.nist.gov/publications/PubsSPs.html。

2. 受保护的健康信息

受保护的健康信息(PHI)是任何与个人健康有关的信息。在美国，健康保险流通与责任法案(HIPAA)授权保护 PHI。HIPAA 提供了更加正式的 PHI 定义：

健康信息是指口头或以任何形式记录或存放在介质中的任何信息：

- 由卫生保健提供商、健康计划、卫生行政部门、雇主、人寿保险公司、学校或大学、医疗清算公司创建或接收。
- 与任何个人过去、现在或将来身体或精神健康或状态相关、与向个人提供医疗保健相关或与向个人提供医疗保健而进行的过去、现在或未来支付有关。

有些人认为只有医生和医院等医疗保健提供商需要保护 PHI。然而，HIPAA 对 PHI 的定义要广泛得多。任何提供或补充医疗策略的雇主都会收集和处理 PHI。这对于提供或补充医疗策略的组织来说是很常见的，所以 HIPAA 适用于美国大部分的组织。

3. 专有数据

专有数据指的是任何帮助组织保持竞争优势的数据。可以是开发的软件代码、产品的技术计划、内部流程、知识产权或商业秘密。如果竞争对手能够访问私有数据，就可能会严重影响组织的主要任务。

虽然版权、专利和商业秘密法律为专有数据提供了一定程度的保护，但这并不总是足够的。许多罪犯不重视版权、专利和法律。同样，国外组织也窃取了大量的专有数据。

作为一个例子，信息安全公司 Mandiant 在 2013 年发布了一份报告，一支他们命名为 APT1 的团体，在国外进行操作。Mandiant 将相当数量的数据盗窃归结于这种高级持续威胁(Advanced

Persistent Threat，APT)。他们观察了受到 APT1 危害的 141 家公司，跨越 20 个主要行业。在一个实例中，他们观察到，APT1 在 10 个月的时间内窃取了 6.5TB 的压缩后的知识产权数据。

注意：

2014 年，美国网络安全公司 FireEye 以大约 10 亿美元的价格收购 Mandiant。

5.1.2　定义分类

组织通常会在安全策略或在单独的数据策略中包括数据分类。数据分类识别的是数据对于组织的价值，并对数据的机密性和完整性保护至关重要。策略确定了组织内使用的分类标签，还确定了数据所有者如何确定合适的分类以及人员应如何根据分类保护数据。

例如，政府数据分类包括绝密、保密、机密和非机密。高于非机密级别的所有信息都属于敏感数据，但很显然，它们的价值不同。美国政府对这些分类提供了明确的定义。当你阅读时，注意每个定义的措辞都是相近的，除了一些关键词不同。绝密使用的短语是“特别严重的损害”，保密使用的短语是“严重损害”，机密使用的术语是“损害”。

绝密　绝密标签适用于这样的信息，“未授权披露通常可能会对国家安全带来可以由原分类组织识别或描述的特别严重的损害。”

保密　保密标签适用于这样的信息，“未授权披露通常可能会对国家安全带来可以由原分类组织识别或描述的严重损害。”

机密　机密标签适用于这样的信息，“未授权披露通常可能会对国家安全带来可以由原分类组织识别或描述的损害。”

非机密　非机密信息指不符合上述绝密、保密、机密标签描述的任何信息。在美国，非机密信息任何人都可用，尽管通常要求个人使用信息自由法案(Freedom Of Information Act，FOIA)中确定的程序来申请这些信息。

分类组织是将原分类适用于敏感数据并规定谁能这么做的严格规则的实体。例如，美国总统、副总统和部门负责人在美国可以分类数据。另外，担任这些职务的个人可以委托他人对数据进行分类。

提示：

虽然分类的重点通常是数据，但这些分类也适用于硬件，这包括任何处理或保存这些数据的计算系统或介质。

非政府组织很少需要基于对国家安全的潜在危害对数据进行分类。然而，管理层会担心对组织的潜在损害。例如，如果攻击者访问组织的数据，潜在的负面影响是什么？换句话说，组织并不仅仅考虑数据的敏感性，还会考虑数据的关键性。他们在描述绝密、保密、机密数据时也会使用美国政府采用的相同短语，即“特别严重的损害”、“严重的损害”和“损害”。

一些非政府组织使用标签，比如分类 3、分类 2、分类 1、分类 0。其他组织使用更有意义的标签，比如机密(或专用)、私有、敏感和公开。图 5.1 展示了这些不同分类之间的关系，左边是政府分类，右边是非政府(或民用)分类。正如政府可以基于数据泄露的潜在负面影响来定义数据，组织也可以使用类似的描述。

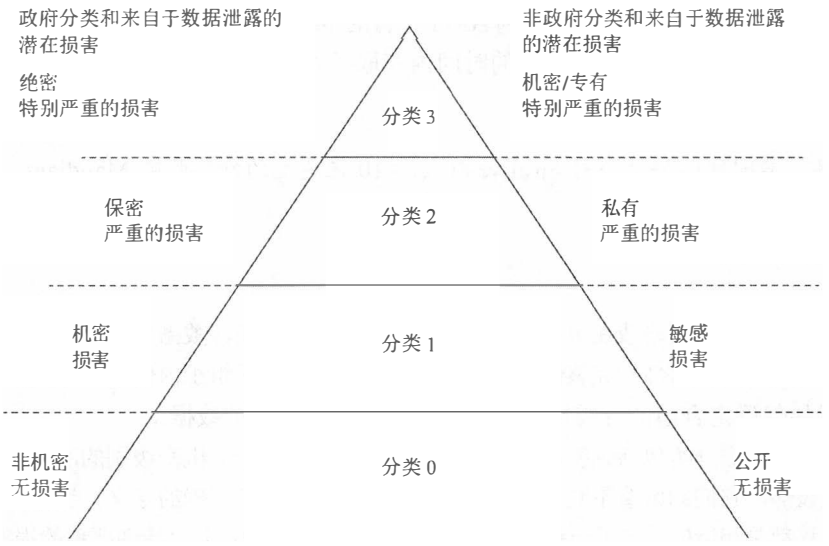


图 5.1 数据分类

对于政府分类来说，在标识数据对组织的相对价值方面，绝密代表最高等级，对于如图 5.1 所示的组织来说，机密代表最高分类。然而，重要的是要记住，组织可以使用任何他们想用的标签。当使用图 5.1 中的标签时，敏感信息是指所有非机密等级以上(当使用政府分类时)或非公开(当使用民用分类时)的信息。以下部分讲述的是非政府分类的意义。

索尼攻击

你可能还记得 2014 年 11 月和 12 月对索尼公司的攻击。Mandiant 公司的创始人 Kevin Mandia 表示："这种攻击的范围不同于我们过去应对的任何攻击，因为其目的是破坏财产并将机密信息向公众发布。最重要的是，这是由一个有组织的团体执行的无与伦比的、精心策划的犯罪。"

攻击者获得超过 100TB 的数据，包括未发布电影的完整版本、薪资信息和内部电子邮件。其中一些数据比其他数据对组织更有价值。当你阅读非政府数据分类的定义时，考虑其对索尼公司带来损害的严重性以及此类数据的适当分类。注意，任何人对数据的分类标签都可能与索尼公司数据所有者的分类不同。这里没有对错。然而，攻击确实为我们提供了一些现实的例子。

机密或专有 机密或专有标签指的是最高水平的分类数据。在这种情况下，数据泄露会对组织使命造成特别严重的损害。索尼攻击后，攻击者发布了几个电影的未发布版本。它们迅速出现在文件共享网站上，安全专家估计人们对这些电影进行了多达 100 万次下载。因为有了盗版电影，当索尼最终发布这些电影时，许多人也就不用看了。这直接影响到他们的盈亏底线。电影是专有的，组织可能会认为这是非常严重的损害。回想起来，他们可以选择将电影作为机密或专有信息，并使用最强的访问控制来保护它们。

私有 私有标签指的是数据应为组织私有，但不符合保密或专有数据的定义。在这种情况下，数据泄露会对组织使命造成严重损害。索尼攻击后，攻击者发布了索尼公司 30 000 多名员工的薪资信息，包括 17 位高管数百万美元的薪水。当这些细节出来后，员工开始将他们的薪水和这 17 位高管进行比较，可以打赌这肯定造成了内部问题。索尼公司可能认为这是严重的损坏，现在回想起来，可能会选择将这种类型的数据标注为私有标签。

敏感 敏感数据类似于机密数据。在这种情况下，数据泄露会导致对组织使命的损害。索尼攻

击发生后，攻击者发布了一份被解雇或终止合同的所有员工的电子表格。其中包括终止的原因和每个员工终止合同的成本。他们还发布了几封电子邮件，包括尴尬的评论。例如，一个制作人将一名电影明星说成“稍有才华的被宠坏的小孩”，一些电子邮件还包括许多人视为无情的种族言论的内容。这些都是尴尬的，还可能会对组织造成损害。回想起来，他们可以选择将这种类型的数据标注为敏感信息并适当地保护。

公开　公开数据类似于未分类数据，包括发布在网站上、宣传册中或任何其他公共来源的信息。尽管组织不保护公开数据的机密性，但仍需采取措施保护其完整性。例如，任何人都可以查看发布在网站上的公共数据。然而，组织不想让攻击者修改这些数据，因此需要措施来保护它们。

提示：

虽然 CISSP 考试大纲(CIB)指出任何没有公开或未分类的数据为敏感信息，但一些组织仍使用敏感作为标签。换句话说，和 CISSP 考试中的意思相比，“敏感信息”一词在组织中的意思可能会不同。对于考试来说，只要记住“敏感信息”是指任何未公开或分类的信息。

不要求民间组织使用任何特定的分类标签。然而，重要的是要以某种方式分类数据，并确保人员理解分类。不管组织使用什么标签，都仍然有义务保护敏感信息。

对数据进行分类后，组织需要基于分类采取额外的措施来进行管理。对敏感信息未经授权的访问可能导致对组织的重大损害。然而，基本的安全措施，如根据分类正确标记、处理、存储和破坏数据，有助于防止损失。

5.1.3　定义数据安全要求

在定义了数据分类后，对数据的安全要求进行定义也很重要。比如，组织应该采取什么步骤保护邮件的安全性？

组织至少应该对比较敏感的邮件进行标记和加密。加密是将明文转换为密文，从而增加阅读的难度。采用强大的加密方法，例如，拥有 256 位加密密钥的高级加密标准(AES 256)，使未被授权者能够阅读加密文章的可能性几乎为零。表 5.1 表明组织可能会对邮件实施的安全要求。

表 5.1　保护电子邮件数据安全

分类	对电子邮件的安全需求
机密	电子邮件和附件必须用 AES 256 加密
	电子邮件和附件除了被浏览时要一直保持被加密
	电子邮件只能在组织内发送给收件人
	电子邮件只能被收件人打开和浏览(被发送邮件不能被打开)
	附件能被打开和浏览，但不能保存
	电子邮件的内容不能被拷贝和粘贴到其他文档中
	电子邮件不能被打印
隐私	电子邮件和附件必须用 AES 256 加密
	电子邮件和附件除了被浏览时要一直保持被加密
	电子邮件只能在组织内发送给收件人
敏感	电子邮件和附件必须用 AES 256 加密
公开	电子邮件和附件能够以明文形式发送

注意：

表 5.1 所列的要求仅仅用作举例。任何组织都可以使用这些要求，也可以定义适合组织自身的其他要求。

虽然满足表 5.1 的所有要求也是可能的，但是各个组织可能会要求施行其他的解决方案。例如，Boldon James 销售的一些产品就可以让各组织自动完成这些任务。使用者在发送电子邮件之前，可以为邮件贴上相关的标签(如保密、私有、敏感及公开)。之后的数据丢失防护(Data Loss Prevention，DLP)服务器可以检测到这些邮件的标签，并且对它们实施相应的保护。

表 5.1 列出了组织希望对邮件实施的一些可能性要求，但是各个组织的要求可能不止于此。各个组织想要保护的任何类型数据都需要进行类似的安全定义。例如，组织可以对存储在服务器上的数据、存储在办公场所内外的备份数据以及专有数据(例如，未发行的全部电影数据)进行安全性要求的定义。

5.1.4 理解数据状态

在数据静止、传输以及使用过程中，保护数据的安全性是非常重要的。静态数据是指存储在介质(例如，硬盘、USB 闪存盘、存储区域网(SAN)和备份磁带)上的数据。传输数据(有时称为动态数据)是指那些通过网络传送的数据，包括通过有线或无线在内网上传输的数据以及在公共网络(如互联网)上传输的数据。使用中的数据是指在临时存储区中正在被应用程序使用的数据。

保护数据机密性的最好方法是使用强大的加密协议，这一点将在本章的后面进行讨论。此外，强大的身份验证和授权控制能有效阻止未经授权的访问。

比如，用于检索电商交易中信用卡数据的 Web 应用程序。这种信用卡数据存储在一台单独的数据库服务器中，并且在静态、动态以及使用时都会得到保护。

数据库管理员会采取措施对存储在数据库服务器上的敏感数据(静态数据)进行加密。例如，他们会对存储敏感数据(如信用卡数据)的列进行加密操作。而且，他们还会施行身份认证和授权控制，以防止未经授权的实体访问数据库。

当 Web 应用程序从 Web 服务器上发送数据请求时，数据库服务器会验证 Web 应用程序是否已获得检索数据的授权。如果情况属实，数据库服务器就会发送数据。然而，这需要几个步骤来完成。例如，数据库管理系统首先要检索和解密数据，并将其转变为 Web 应用程序可读取的格式。接着，数据库服务器在传送之前使用传输加密法则对数据进行加密，这确保了数据在传输过程中的安全性。

Web 应用程序服务器对收到的加密数据进行解密，然后传输给 Web 应用程序。在授权传输时，Web 应用程序会把数据存储在临时缓冲区中。当 Web 应用程序不再需要这些数据时，该程序会采取措施来清除内存缓冲区，确保所有敏感数据从内存中彻底清除。

5.1.5 管理敏感数据

管理敏感数据的一个主要目标是防止数据泄露。数据泄露会使任何一个未被授权的实体查看或访问敏感数据。如果看新闻，你可能会经常听到有关数据泄露的事件。比如在 2014 年，索尼数据泄露事件就是当时的头版头条。即使从没听过小规模的数据泄露事件，但这些也是经常发生的，每周平均会有 15 次关于数据泄露事件的报道。接下来，我们将明确各组织内部人员在查询数据时应当遵

循的几个基本步骤，以降低数据泄露的可能性。

注意：

身份盗窃资源中心(Identity Theft Resource Center，ITRC)通常会对数据泄露进行追踪。该中心通过他们的网站(www.idtheftcenter.org/)发布相关报道供人们自由浏览。2014 年，他们追踪了 783 件数据泄露事件，公开了 8500 多万条记录，核算下来，大约每周会发生 15 起数据泄露事件，并且每年的数据泄露事件呈上升趋势。

1. 标记敏感数据

对敏感数据进行标记(通常称为贴签)能确保用户可以轻松识别任何数据的分类级别。标记或标签提供的最重要信息就是关于数据的分类。例如，绝密标记能让看到的人明白该信息属于最高机密级别。在了解数据价值后，用户很有可能在分类的基础上采取适当措施进一步控制和保护这些信息。标记包括物理的和电子的标记和标签。

物理标签能指出存储在介质或处理系统上的数据的安全性分类。例如，如果备份磁带包含机密数据，该磁带就会被贴上物理标签以明确告知使用者其含有机密数据。同样，如果一台计算机有机密信息，该计算机将会被贴上标签以指示其含有最高机密级别的数据。一台计算机通常可用来处理保密、私密和绝密数据，因此，对处理最高机密数据的计算机应该做出标记。物理标签会一直保留在系统或介质上。

提示：

许多组织用带颜色编码的硬盘来辅助标记工作。例如，一些组织大量购买红色的 USB 闪存盘，员工只能用该盘复制机密数据。技术安全控制中心用通用唯一识别符(UUID)来识别这些闪存盘，进而执行安全策略。DLP 系统能阻止用户将数据拷贝到其他 USB 设备上，并且能确保当用户将数据复制到其他这样的设备时，数据会被加密。

标记也包括使用数字水印或标签。一种简单方法是将数据归类成文档中的标题和脚注，或将其嵌入作为水印。这种方法的好处是在打印输出时，这些标记也会显示出来。即使文档打印出来包含了标题和脚注，很多组织也还会要求使用者将打印出来的敏感数据文档用含有标签和封面的文件夹进行装订，从而更加明确这些数据的分类。不只文件能用标题，很多备份磁带也可以包含标题信息，并且还可以在标题中添加分类信息。

标题、脚注和水印的另一个好处是，DLP 系统可以识别包含敏感信息的文档并施行适当的安全控制。一些 DLP 系统在检测到这些文档被归类后，会把元数据标记附到其中。通过这些标签可以洞察这些文档的内容并帮助 DLP 系统更加妥善地处理文档。

同样，一些组织设定他们的计算机必须使用特定的桌面背景。例如，用于处理专用数据的计算机系统可能会用黑色的桌面背景，以及白色的“专用”二字和橙色宽边框。桌面背景上也可能会有声明，如“这台电脑处理专用数据”，警示使用者有责任保护这些数据的安全性。

在许多安全环境中，人们也会对非机密介质和设备进行标记，如此可预防在敏感信息未被标记时发生遗漏失误。例如，如果存储有敏感数据的备份磁带没有被标记，用户可能会认为上面只包含了非机密数据。但是，如果组织对非保密数据也进行了标记，用户使用时就可能会多考虑一下。

各个组织通常会明确介质降级的程序。例如，如果备份磁带含有机密信息，管理员可能希望将其降级为非机密备份磁带。各个组织还会对可信的程序进行鉴别，并对磁带中的所有可用数据进行

清除处理。在管理员将磁带中的数据清除后，他们就可以执行降级操作并重新替换标签。

然而，许多组织都禁止介质降级。例如，数据政策可能会禁止对存储有绝密数据的备份磁带进行降级。相反，该政策也可能会授权系统在磁带生命周期结束时将其销毁。同样，系统几乎是不可能降级的。换句话说，如果一个系统曾经处理过绝密数据，它几乎是不可以降级的，也不可能被重新标记为非机密系统。

注意：

如果介质或系统需要降级为较不敏感的数据分类，就必须通过适当程序来净化其中的数据，相关内容会在本章后面的“销毁敏感数据”一节中讲到。然而，与净化数据重新使用相比而言，直接购买新的介质或设备往往显得更便捷、更安全。许多组织都采用禁止任何介质或系统降级的策略。

2. 管理敏感数据

管理敏感数据是指在介质的整个生命周期内确保传送过程的安全。人们依据数据的价值和分类对其进行不同的管理，正如你所期望的，高级机密信息需要更强大的保护。尽管上面说到的这些都是常识，但人们还是会在这方面犯错。很多时候，人们习惯于处理敏感信息，但对于保护这些信息却不关心。

例如，2011 年 4 月，英国国防部错误地公布了有关核潜艇的保密信息和其他一些机密信息，作为对信息自由请求的回应。他们通过图像编辑软件将机密信息标黑并进行了重新编辑。然而，任何想试图复制数据的人都能够复制整篇文档，包括标黑的数据。

有一个普遍的现象就是，人们很少在意对备份磁带的控制。备份磁带应该与备份数据一样受到同级别的保护。换句话说，如果机密信息存储在备份磁带中，备份磁带就应该被视为机密信息保护起来。然而，很多例子表明人们并没有遵循这一准则。2011 年，一家政府的承包商，国际科学应用公司(SAIC)并没有对备份磁带进行控制，而这些磁带包含 490 万名患者的 PII 和 PHI 数据。即使是低于 HIPAA 数据分类的 PHI 数据，也需要得到具体措施的保护，但显然 SAIC 并没有对其实施保护。

要想确保人们了解如何处理敏感数据，那么策略和程序都必须到位。最先要做的就是，确保系统和介质都已经被合理标记。第 17 章“事件预防和响应”将讨论记录、监控和审计的重要性。这些控制是为了确保在重大损失发生前，机密数据得到了应有的妥善处理。如果损失确实发生了，调查员会使用审计线索来发现到底在什么地方出错了。任何一起因没有恰当地处理数据而发生的突发事件，都应及时展开调查并采取措施以防止类似事件的再次发生。

3. 存储敏感数据

敏感数据应存储在受保护且没有任何损失的介质中。最有效的保护办法就是加密。在撰写本书时，AES 256 提供了强大的数据加密方法，并且许多应用都可以通过 AES 256 对数据进行加密。此外，许多操作系统内置了同时对文件级和磁盘级别数据进行加密的功能。

如果敏感数据存储在物理介质上，如便携式硬盘或备份磁带，那么人们应遵循基本的物理安全做法，以防止因盗窃而损失数据。这些做法包括将数据存储在保险箱、保险库或安全室内，也包括另外的一些物理控制。例如，服务器机房应包括物理安全措施，以防止未经授权的实体访问数据，所以将便携式介质存放在服务器带锁的柜子内能有力地保障数据安全。

此外，也应该采取环境控制来保护介质的数据安全。这些做法包括温度和湿度控制，如安装加热、通风和空调(HVAC)等系统。

这里有一点终端用户经常忘记：任何敏感数据的价值都大于存储介质的价值。换句话说，买高质量的存储介质是物超所值的，尤其是当数据要被保存很长一段时间的情况下，例如备份磁带。同样，购买内置加密程序的高品质 USB 闪存也是值得的。一些 USB 闪存内置了需要使用指纹的身份验证装置，这就为数据安全提供了额外保护。

注意：

加密敏感数据为数据安全提供了一层额外保护，并且也应当把静态数据考虑在内。如果数据做了加密，那么即使存储被盗，攻击者也很难获取数据。

4. 销毁敏感数据

当组织不再需要这些敏感数据时，就应当将其销毁。适当的破坏可以确保这些数据不会落入投机者的手中，从而防止未经授权的数据泄露。与低级数据相比，高级机密数据需要不同的销毁步骤。组织的安全策略或数据策略中应当根据数据分类原则来定义销毁数据的方法。例如，组织可能要求完全销毁存储高级机密数据的介质，但允许人员使用软件工具来覆盖较低级别的数据文件。

数据剩磁(data remanence)是指数据仍然作为剩余磁道上的数据保留在硬盘驱动器上。利用系统工具来删除数据，通常会使许多信息残留在介质中，很多工具可以很容易地取消删除。即使使用复杂的工具来覆盖介质，原始数据的痕迹可能仍然会存在，并保存在不易察觉的磁盘区域。这类似于，如果相同的数据经过长时间显示后，会在电视或计算机显示器上显示出重像。取证专家和攻击者可以使用工具来恢复这些数据，即使介质已被覆盖。

删除数据剩磁的一种方法是使用消磁工具。消磁工具能产生强大的磁场区域，并将磁介质(传统的硬盘、磁带和软盘驱动器)中的磁场区域重新排列。强大的消磁工具能够有效地重写这些磁场区域并且消除数据剩磁。然而，这种方法仅在磁介质上有效。

相反，固态硬盘(Solid State Drives，SSD)使用的是集成电路，而不是旋转盘片的磁盘。正因为如此，固态硬盘没有数据剩磁并且去磁也不会删除数据。然而，即便使用其他方法从固态硬盘中删除数据，数据剩磁也依然存在。在一篇题为“在闪存固态硬盘中可靠地删除数据”的论文中(www.usenix.org/legacy/event/fast11/tech/full_papers/wei.pdf)，作者发现，就单个文件来说，传统的净化方法没有一个有效。一些固态硬盘包含内置的擦除命令来净化整个磁盘，但遗憾的是，对来自不同制造商的一些固态硬盘不起作用。基于这些风险，最好的净化方法就是销毁固态硬盘。美国国家安全局(NSA)要求使用经批准的粉碎机来破坏固态硬盘。批准的粉碎机可以粉碎尺寸为 2 毫米或更小的固态硬盘。安全工程设备(Security Engineered Machinery，SEM)出售许多销毁信息和消除数据的设备，其中包括许多由美国国家安全局批准的设备。

警告：

执行任何类型的消除、清除、净化过程时都要小心。人为操作的设备或工具可能无法正常执行这些任务，并且可能无法完全从介质上删除数据。软件可能是有缺陷的，磁体可以有错误，这都有使用不当之时。在进行了净化处理之后，始终要验证是否达到预期效果。

下面的列表包括一些与销毁数据相关的常见术语：

擦除　擦除介质上的数据就是对文件、文件的选择或整个介质执行删除操作。在大多数情况下，删除或清除程序只是删除了目录或与目录相链接的数据。实际的数据还在驱动器中。随着新文件写入介质，系统最终将重写删除的数据，但是这取决于驱动器的大小、还有多少剩余空间以及其他影

响因素，数据可能几个月都不会被完全重写。任何人都可以使用复原工具来恢复这些数据。

消除 消除或重写是使介质可以重新使用的一个准备过程，这个过程可以确保消除的数据不会通过传统的工具恢复。当介质上的数据被消除时，非机密数据被写在介质上的所有可寻位置。一种方法是在整个介质中写入单个字符或特定的位模式。另一种更常用的方法就是在整个介质中写入单个字符，将这个字符填充到整个介质中，最后用一个随机位来结束。这种方法就是在 3 个单独的磁道中不断重复，如图 5.2 所示。虽然这听起来好像原始数据永远丢失了，但是有时可以通过一些复杂的实验或取证技术来获取到原始数据。此外，这种消除技术对于一些类型的数据存储介质并不适用。例如，硬盘驱动器中的多余区域、标记为“坏的”区域以及许多现代 SSD 并不总是会消除干净，仍可能有数据保留。

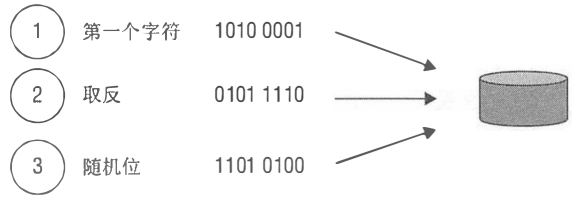


图 5.2 消除硬盘驱动器

清除 清除是比消除更强烈的一种形式，是指在安全性较差的环境中使介质达到可再次使用的准备过程，确保原始数据使用任何已知方法都不会恢复。清除过程是将消除过程多次重复，并结合其他方法，如去磁法来完全清除数据。即使清除过程会除去所有残留的数据，但这种方法并不总是可靠的。例如，美国政府不会考虑采用任何的清除方法来清除绝密数据。标记为绝密数据的介质将始终保留最高机密，直到被摧毁。

解除分类 解除分类是指在非机密情况下对介质或系统进行清除，以使其能够再次使用的准备过程。可以使用清除来为解除分类做准备，但是在安全性较低的情况下，为确保安全解除分类介质而做出的努力比花钱买新介质的成本更高。此外，尽管用任何已知的方法都不能恢复清除的数据，但是似乎还有可以使用的方法。为了规避风险，许多企业选择不解除分类任何介质。

净化 净化是指从系统或介质中删除数据，确保数据不会以任何形式恢复。当一台计算机被处置时，净化包括确保所有的非易失性存储器已被删除或被破坏，系统在任何驱动器中都不含CD/DVD光盘，且内部硬盘(硬盘驱动器和 SSD)已被净化、删除和/或销毁。净化指的是破坏介质或使用一种可靠的方法将机密数据从介质上清除，但不破坏介质。

消磁 消磁工具会建立一个强大的磁场区域，从而以消磁的方法擦除介质上的数据。技术人员通常使用消磁的方法将磁带上的数据清除，从而使其回到最初状态。硬盘也可以消磁，但是我们不建议那样做。硬盘消磁通常会破坏访问数据的电路。但是，并不确定硬盘上的数据是否被完全清除。可能会有人在干净空间中启动驱动并在不同的驱动上安装盘片来读取数据。消磁不会对 CD、DVD 或 SSD 造成影响。

销毁 销毁是介质生命周期的最后阶段，也是清除介质数据的最安全方法。当销毁介质时，一定要确保其不能再使用或修复，并且数据不能从被破坏的介质上提取。销毁方法包括焚烧、破碎、粉碎、解体，并使用腐蚀性或酸性化学物质溶解。有些组织将高级机密的磁盘驱动器盘片取下，并单独销毁它们。

注意：

当企业捐赠或出售二手电脑设备时，他们通常会清除并销毁设备中的敏感数据，而不是试图清

除这些存储设备。这降低了清除过程中数据可能不会完全清除的风险，从而造成机密数据泄露的损失。

5. 保留资产

保留要求适用于数据或记录、含有敏感数据的介质和系统，以及接触敏感数据的人员。记录保留和介质保留是资产保留的最重要元素。

记录保留指的是，在需要信息时保留和维护重要的信息，在不需要时破坏信息。组织的安全策略或数据策略通常会确定出保留时间表。一些法律、法规规定了组织应该保留数据的时间长度，如 3 年、7 年甚至是无限期的。然而，即使没有外部要求，组织也应该确定数据保留的时间。

作为一个例子，许多组织需要保留所有审计日志三年或更长时间。这使得组织能够重建过去安全事故的细节。当组织没有保留策略时，管理员可以在管理层提出期望之前就删除有价值的数据或企图无限期地保持数据。数据保留的时间越长，在介质、存储位置和保护人员方面的成本就越高。

大部分硬件都有更新周期，可能每 3 至 5 年就被取代。硬件保留主要是指将硬件保留到其被正确净化。

人员保留在这种情况下是指人员受雇于组织时获得的知识。组织在招聘新的人员时签订保密协议(NDA)是很常见的。NDA 可以保证员工在离职后不会和他人共享私有数据。

真实场景

保留策略可以减少责任

如果保存数据的时间比需要的时间长，可能会带来不必要的法律问题。例如，飞机制造商波音公司曾经成为一次集体诉讼的目标。申请人律师得知波音公司有一个仓库，里面有 14 000 份电子邮件的备份磁带，他们要求相关的磁带。并不是所有的磁带都与诉讼相关，但波音公司必须首先恢复这 14 000 个磁带，并在移交之前检查其中的内容。最终诉讼成本达到 9250 万美元，分析师推测，如果 14 000 个磁带不存在，就不会是这样的结果。

这是一个极端的例子，但不是唯一的一个。这些事件促使许多公司实施积极的电子邮件保留策略。电子邮件策略中要求删除超过 6 个月邮件的并不少见。这些策略通常使用自动化工具来实现，工具会查询旧的邮件并删除，而不需要任何用户或管理员干预。

提起诉讼后，一家公司删除潜在证据就是不合法的。然而，如果保留策略规定具体的时间后删除数据，那么在任何诉讼被提出之前删除这些数据就是合法的。这种做法不仅防止浪费存储不必要数据的资源，还通过查看旧数据对浪费资源提供了一层额外的法律保护。

5.1.6　应用密码学保护机密文件

保护数据机密性的一个主要方法就是加密。第 6 章“密码学与对称加密算法”以及第 7 章“PKI 和密码学应用”从更深层次介绍了加密算法。然而，我们很有必要指出用于静态数据和传输中数据的算法之间的差异。

开始时，加密将明文数据转换成杂乱的密码文本。如果文件是明文格式，每个人都能读取。然而，当我们使用强大的加密算法时，几乎不可能读取杂乱的密码文本。

1. 应用对称加密保护数据

对称加密在加密和解密数据时应用同样的密钥。换言之，如果一个算法加密数据的密钥是 123，那么解密时的密钥也是 123。对称算法对于不同的数据不会使用同样的密钥。例如，如果将一个数据集的加密密钥设为 123，解码下一个数据集的密钥就可能是 456。在这里重要的是，用 123 作为密钥的加密文件只能用同样的密钥 123 来解密。在实际操作中，密钥长度会更长。例如，AES 使用的密钥长度为 128 位或 192 位，AES 256 使用的密钥长度为 256 位。

下面的列表定义了一些最常用于对称加密的算法，尽管这些算法中的大部分都应用于加解密静态数据，有些也应用于传输加密算法。我们会在下一部分进行讨论。此外，这绝对不是加密算法的完整列表，第 6 章囊括了大多数算法。

高级加密标准算法 高级加密标准算法(AES)是众多算法中最受欢迎的对称加密算法。2001 年，美国国家标准技术研究所将它选为标准算法，用以替代旧的数据加密标准算法(DES)。从那时起，开发者一直稳定地将高级加密标准算法编入许多其他算法和协议中。例如，BitLocker(一个带有可信平台模块的完整硬盘加密应用)使用了高级加密标准算法。微软加密文件系统将高级加密标准算法应用于文件及文件夹加密。高级加密标准支持的密钥长度为 128 位、192 位和 256 位。美国政府已经同意应用高级加密标准算法来保护绝对机密资料。较长的密钥长度会增加安全系数，使得未授权的人员难以解密数据。

三重数据加密标准算法 开发者开发了三重数据加密标准算法(3DES)，用以替代数据加密标准算法(DES)。初始实现使用 56 位密钥，但是新的算法实现了使用 112 位或 168 位密钥。密钥越长，安全等级越高。微软 OneNote 和系统中心配置管理器使用 3DES 来保护特定内容和口令。

Blowfish 信息安全专家布鲁斯 • 施奈尔开发的 Blowfish 可以作为数据加密标准的可选择项。Blowfish 可用的密钥长度为 32 位至 448 位，是一个强大的加密协议。Linux 系统使用 bcrypt 来加密密码，而 bcrypt 这款跨平台文件加密工具就是基于 Blowfish 的。bcrypt 添加了额外的 128 位密钥作为 salt 值来阻止彩虹表攻击(rainbow table attack)。

2. 应用传输加密保护数据

传输加密算法在传播之前加密数据，对传输过程中的数据进行保护。通过网络发送未加密数据的最主要风险就是嗅探攻击。攻击者可以使用嗅探器或协议分析器在网络上捕捉流量。嗅探器允许攻击者读取所有以明文发送的数据。然而，如果数据用很强的加密协议加密，攻击者则不能读取。

例如，网络浏览器使用 HTTPS 来加密电子商务交易，这可以防止攻击者捕捉数据以及使用信用卡信息累积费用。相比较而言，超文本传输协议以明文传输数据。

几乎所有 HTTPS 传输都使用 TLS(Transport Layer Security)作为基本加密协议。加密套接字协议层(Secure Sockets Layer，SSL)是 TLS 的先导。美国网景公司在 1995 年开发并发布了 SSL。随后，互联网工程任务组(IETF)发布了 TLS 作为 SSL 的替代品。2014 年，谷歌公司发现 SSL 易受 POODLE 攻击。结果是，许多组织都在他们的应用中禁用了 SSL。

很多组织通常会授权远程访问解决方案，如虚拟专用网(VPN)允许在家办公或出差的员工使用组织的网络。VPN 能够在诸如互联网的公共网络上流动，所以加密是非常重要的。虚拟专用网使用的加密协议有 TLS 和网际协议安全(Internet Protocol security，IPsec)。

网际协议安全通常和第二层通道通信协议(Layer 2 Tunneling Protocol，L2TP)结合来使用虚拟专用网。L2TP 在明文中传输数据，但是 L2TP 或 IPsec 在数据传输过程中使用通道模式来保护数据，

并通过互联网加密和发送数据。IPsec 包括一个认证报头(Authentication Header，AH)，该认证报头提供了鉴定和完整性，同时，封装安全载荷(Encapsulating Security Payload，ESP)提供保密性。

对于在互联网上传播数据之前给机密数据加密，它也同样适用。IPsec 和 SSH 通常都用来在互联网传输数据的过程中保护数据。SSH 是一个强大的加密协议，包括其他协议，如安全复制(Secure Copy，SCP)和安全文件传输协议(Secure File Transfer Protocol，SFTP)。SCP 和 SFTP 都是安全协议，它们用来通过网络传输加密文件。一些协议，如文件传送协议(FTP)在明文中传输数据，这些协议不适合在网络中传输机密数据。

许多管理者在管理远程服务器时，用 SSH 代替远程登录协议(Telnet)。由于 Telnet 会在明文中通过网络发送数据，因此不应该使用远程登录协议。连接到远程服务器时，管理者需要登录服务器，因此远程登录也需要通过网络以明文形式发送他们的认证信息。然而，SSH 会给所有数据加密，包括管理者的认证信息。

注意：

Telnet 必须用于连接远程服务器，管理者通常会使用 VPN 在隧道内给远程登录数据加密。

5.2　定义数据角色

组织内的许多人都会管理、处理和使用数据，基于角色他们有不同的要求。不同的文件涉及的这些角色也略有不同。有些在 CISSP 考试大纲(CIB)中使用的信息与一些 NIST 文件中的术语是匹配的，并且一些术语符合与欧盟数据保护法相关的避风港项目。适当时我们会列举这些信息来源，以便你可以深度学习这些信息。

5.2.1　数据所有者

数据所有者是数据的最终责任人。所有者通常是首席执行官、总裁或部门主管。数据所有者定义数据类别，确保给数据贴上合适标签。他们也要确保基于分类和组织的安全策略要求足够安全。如果数据所有者在制定和执行安全策略的过程中没有尽职去保护和维持机密数据，那么他们有义务承担过失责任。

NIST SP 800-18 概括了信息所有者的以下责任，也可以理解为同样是数据所有者的责任：

- 制定规则，以便用于主体的数据或信息的适当使用及保护(行为规则)。
- 为信息系统所有者提供输入，要考虑到信息所在地的信息系统的安全要求和安全控制。
- 决定谁有权访问信息系统，拥有何种特权或准入权。
- 协助对信息所在地的普通安全控制进行定义和评估。

注意：

NIST SP 800-18 经常使用短语“行为规则”，它和可接受使用策略(Acceptable Usage Policy，AUP)高度一致。两者都要概括责任和个体的预期行为，以及陈述和规则或可接受使用策略不一致的后果。此外，我们要求个体定期告知他们已经读取、理解并且同意规则或可接受使用策略。许多组织都把这些信息放到网上，允许使用者告知他们已经理解并同意遵守(使用在线电子数字签名)。

5.2.2 系统所有者

系统所有者是拥有含机密数据的系统的人。NISTSP 800-18 概括了系统所有者的以下责任：

- 开发和信息所有者、系统管理者、功能终端使用者相一致的系统安全计划。
- 维持系统安全计划并确保系统依照已经同意的安全要求进行部署和运行。
- 确保系统使用者和支持人员受到适当的安全培训，如行为规则说明(或是 AUP)。
- 当发生重大变化时，更新系统安全计划。
- 协助定义、执行和评估通用安全控制。

系统所有者通常和数据所有者是同一个人，但是有时候也可能是不同的人，如不同的部门主管。举例来说，考虑一下一台和后端数据库服务器相互作用并用于电子商务的网络服务器。软件开发部门可能会为数据库和数据库服务器进行数据库开发或数据库管理，但是信息技术部门负责维护网络服务器。在这种情况下，软件开发部门主管就是数据库服务器的系统所有者，信息技术部门主管就是 Web 服务器的系统所有者。然而，更普遍的是一个人(如一个部门主管)来控制两个服务器，那么这个人就同时是两个系统的系统所有者。

系统所有者负责确保在系统中运行的数据的安全性，这包括定义系统运行的最高级数据。系统所有者要确保精确标记系统，同时也需要适当的安全控制来保护数据。系统所有者和数据所有者通过交流来确保在系统静止时、在系统之间传输时以及在系统应用运行使用时能够保护数据。

5.2.3 业务/任务所有者

业务/任务所有者在不同的组织中角色也不同。NISTSP 800-18 指的是业务/任务所有者作为项目经理或信息系统所有者。同样，业务/任务所有者的责任可以和系统所有者的责任有重叠或相同。

业务所有者拥有的程序可能是由其他实体管理的系统。举例来说，销售部门可能是业务所有者，但是信息技术部门和软件开发部门可能是系统所有者，原因是系统会应用于销售过程中。想象一下，销售部门使用电子商务网站和网站入口访问后端数据库服务器，将注意力集中于线上销售。在之前的例子中，信息技术部门将网络服务器管理为自己的系统所有者，软件开发部门将数据库服务器管理为自己的系统所有者。销售部门即使不拥有这些系统，也确实拥有商业程序，这些程序通过使用这些系统产生销售额。

在业务中，业务所有者负责确保系统能够给组织提供价值。这是显而易见的。然而，信息技术部门有时会过度热情，执行安全控制，而不考虑业务的影响或其任务。

许多业务的潜在竞争区域是成本中心和利润中心的对比。信息技术部门不能产生收益。相反，成本中心会产生成本。相比较而言，经营方作为利润中心产生收益。由信息技术部门产生的成本会消耗由经营方产生的利润。此外，许多由信息技术部门执行的安全控制会减少符合安全要求的系统的可用性。如果把这些放在一起考虑，就能看到经营方有时候会将信息技术部门视为花钱并减少收益的部门，同时使得业务更难产生收益。

组织通常执行信息技术管理方法，如信息及相关技术的控制目标(COBIT)。这些方法帮助业务所有者和任务所有者根据业务或任务需求平衡安全控制要求。

5.2.4　数据处理者

一般来说，数据处理者是用来加工数据的任意系统。然而，在欧盟的数据保护条文中，数据处理者有更确切的定义。欧盟数据保护法将数据处理者定义为“一个自然人或法人，他拥有个人资料，仅代表数据控制者的利益”。在该条文中，数据控制者是一个控制数据过程的人或实体。

举例来说，一家收集员工个人信息用来制定工资单的公司就是数据控制者。如果他们将此信息发送给第三方公司来制作工资单，那么工资单制作公司就是数据处理者。在这个例子中，在数据控制者的角色中，工资单制作公司(数据处理者)除使用数据进行工资单制作之外，不能将数据用作他用。

欧盟数据保护法(法令95/46/EC)限制将数据传输至欧盟以外的国家。这些国家必须符合特定要求，要求显示他们达到数据保护的足够级别。美国贸易部执行安全港项目，它是一个控制机制，包括一系列避风港法则。目标是防止未授权的信息泄露，由数据处理者处理数据，以及在数据处理者和数据控制者之间进行传输。如果他们同意遵守7项法规和条款15中描述的要求，并且经常提问，美国公司可以自愿选择进入项目。这些法规中有很多法律措辞，解释如下：

- 通知：任何组织都必须告知个人关于收集及使用数据的目的。
- 选择：任何组织必须为个人提供可选择的机会。
- 向前传输：组织只有在遵守通知及选择规则的基础上才能向其他组织传输资料。
- 安全性：组织必须采取合理预防措施来保护数据。
- 数据完整性：除组织在注意规则及使用者选择的可选规则中的目的之外，组织不得将信息用作他用。此外，组织应该采取措施确保数据可信。
- 访问：个人必须可以使用组织持有的关于他们的个人信息。在个人信息不准确的情况下，个人也能够更正、修改或删除信息。
- 执行：组织必须执行机制来确保和这些原则一致。

注意：

美国贸易部将安全港的很多信息放在一个网站上：www.export.gov/safeharbor/。可以通过搜索安全港法规和安全港常见问题来浏览他们的网站、浏览规则的全文以及常见问题列表。

5.2.5　管理员

数据管理员负责将数据以合适的方式授予人员。他们不一定必须拥有全部管理者权限和特权，但是他们可以分配权限。管理员分配权限时需要基于最低权限准则和须知，只有在工作有需要时才会授予使用者。管理员通常会使用基于角色的访问控制模型来分配权限。换句话说，他们将用户账号添加至群组，然后授予群组权限。当用户不再需要访问数据时，管理员就将他们的账户从群组中移除。第 13 章“管理身份与认证”进一步介绍了基于角色的访问控制模型。

5.2.6　保管者

数据所有者经常将每天的任务委任给保管者。通过以适当方式保存和保护数据，保管者协助保护数据的安全性和完整性。例如，保管者会根据备份策略确保数据备份。如果管理员在数据上有配置的审计，保管者也同样会保存这些记录。

在实际中，信息技术部门的人员或者系统安全管理员通常会成为保管者。他们可能是负责分配权限的相同管理员。

5.2.7 用户

用户就是任何通过计算系统获取数据并完成工作任务的人。用户只能获取他们需要用来完成工作任务的数据。也可以把用户想象成员工或最终用户。

5.3 保护隐私

组织有义务保护他们收集和保存的数据。对于保护 PII 和 PHI 数据而言，更是如此(本章开始部分讨论过)。很多法律规章都要求保护隐私数据，组织有义务去学习他们适用于哪些法律和规章。此外，组织需要确保他们的行为符合这些法律规章。

很多法律要求组织披露他们收集到的数据、收集数据的原因以及准备怎样使用这些信息。此外，这些法律禁止组织以正当使用信息之外的方法使用这些信息。例如，如果组织声明正在收集邮箱地址进而与顾客交流购买议题，那么组织不应该将这些邮件地址卖给第三方。

组织在他们的网站上使用在线隐私策略是很普遍的事情。一些实体要求严格按照隐私法办事，包括美国(健康保险流通与责任法案隐私法则)、加利福尼亚州(加利福尼亚在线隐私保护法令 2003)、加拿大(个人信息保护和电子文件法令)以及欧盟的数据保护法。

注意：

欧盟起草了通用数据保护条例(General Data Protection Regulation，GDPR)来替代欧盟数据保护条例。各组织计划的时间线是于 2015 年和 2016 年选取各项要求，于 2017 年和 2018 年执行各项要求。

如果这些法律在司法中得以执行，那么各组织就必须履行这些要求。例如，加利福尼亚在线隐私保护法令(COPA)要求对于任何商业网站或在线服务组织收集的加利福尼亚居民的个人信息，都要求严格的保护策略。实际上，这种策略适用于世界上任何收集个人信息的网站。原因是，如果网站在互联网上可以登录，那么任何加利福尼亚居民都可以登录该网站。很多人认为 COPA 是美国最严格的法律，那些遵守加利福尼亚法律要求的美国组织一般说来也会遵守其他地方的法律。然而，任何组织都有义务来决定自己适用于哪种法律并且要遵守该种法律。

在保护隐私时，组织通常会使用一些不同的安全控制。选择适当的安全控制是一项令人生畏的任务，尤其是对于那些新成立的组织而言。然而，使用安全基准线以及定义相关标准让这项任务变得更简单。

5.3.1 使用安全基线

基线提供了一个起点，确保最低安全标准。各组织使用的一条普通的基线就是镜像。在第 16 章“管理安全运营”中深入讨论了配置管理中的镜像。作为介绍，管理者配置了一个带有预期设定的单一系统，捕捉其镜像，然后将该镜像配置到其他系统中。这就确保了所有系统都配置成相似的

安全状态。

将系统设置成安全状态之后，审计程序要周期性地检查系统，以确保他们维持在安全状态。举例来说，微软组策略可以周期性地检查系统，调整设定以和基准线相匹配。

NIST SP 800-53 讨论了作为安全控制列表的安全控制基准线。它强调，单一的安全控制不能适用于所有情况，但是任何组织都可以选择一组基准线安全控制，并且根据需求做出调整。SP 800-53 的附录 D 概括了 4 组优先安全控制，各组织可以执行以保证基本安全。这些准则向各组织展示了他们应该首先执行什么、其次执行什么和最后执行什么。

例如，表5.2是在访问控制家族中安全控制的一部分清单。美国国家标准技术研究所指派了这些控制的编号和名称，并且提供了推荐的优先控制。P-1 代表优先级最高，P-2代表优先级居中，P-3 代表优先级最后。NIST SP 800-53说明所有这些控制在附录 F 中都有深入说明。

表 5.2　安全控制基准线

控制编号	控制名称	优先级
AC-1	访问控制策略和程序	P-1
AC-2	账户管理	P-1
AT-2	安全意识培训	P-1
AC-5	职责分离	P-1
AC-6	最小特权	P-1
AC-7	失败的登录尝试	P-2
AC-10	协同会话控制	P-3

需要指出的是，许多标志为 P-1 的项目都是基本安全实践。访问控制策略和程序确保用户有特定的身份(如用户姓名)，并且由鉴定程序证明他们的身份。根据用户身份(利用鉴定程序证明)，管理者授予用户基础资源的权利。类似的，任何准备参加 CISSP 考试的人都不应该对执行基本安全规则感到奇怪，如职责分离和最小特权原则。当然，仅仅因为它们是基本的安全实践，也不意味着各组织就会执行。遗憾的是，很多组织还没有发现或执行这些基本规则。

5.3.2　审视和定制

审视是指评估基线安全控制，然后只选择那些适用于想保护的 IT 系统的控制。例如，如果一个系统不允许任何两人在同一时间登录，就不需要应用并发会话控制。

定制是指修改基线内的安全控制列表，使其与组织的使命相适应。例如，组织可能决定一组基线控制完全适用于处在他们主要位置的电脑，但有些控制在远程办公位置可能不适当或不可行。在这种情况下，组织可以选择补偿安全控制来调整基线到远程位置。

5.3.3　选择标准

在选择基线内的安全控制时，组织需要确保控制符合某些外部安全标准。外部元素通常定义了对组织的强制性要求。例如，支付卡行业数据安全标准(PCI DSS)定义了企业在处理主要信用卡的过程中必须遵循的要求。同样，想在欧盟国家之间传输数据的组织必须遵守安全港中的原则标准。

显然，并不是所有组织都必须遵守这些标准。不处理信用卡交易的组织不需要遵守 PCI DSS。同样，不在欧盟国家之间传输数据的组织也不需要遵守安全港中的原则标准。鉴于此，组织需要确定适用的标准，并确保他们选择的安全控制遵守这些标准。

5.4 本章小结

资产安全关注的是在信息的整个生命周期中收集、处理和保护信息，包括在计算系统中存储、处理或传输的敏感信息。敏感信息是任何组织列为私有的信息，可以包括多个层次的分类。

这个过程中的一个关键步骤是在安全策略或数据策略中定义分类标签。政府可以使用绝密、保密、机密和非机密这样的标签。非政府组织可以使用他们选择的任何标签。关键是，他们要在安全策略或数据策略中定义标签。数据所有者(通常是高级管理人员)提供数据定义。

组织采取具体措施来标记、处理、存储并破坏敏感信息，这些措施有助于防止由于未经授权的披露而失去保密。此外，组织通常会为记录保留定义特定的规则，确保必要的数据是可用的。数据保留策略也减少了长时间保存数据带来的责任。

保护数据机密性的一种关键方法是加密。对称加密协议(比如 AES)可以加密静态数据(存储在介质上的数据)。传输加密协议保护传输过程中的数据，方法是在传输之前对其进行加密。

人员在处理数据时可以满足许多不同的角色。数据所有者最终负责分类、标识和保护数据。系统所有者负责处理数据的系统。业务和任务所有者拥有流程，并确保系统对组织的价值。数据处理者通常是为组织处理数据的第三方实体。管理员基于数据所有者提供的指导方针授权访问数据。保管人被委托负责日常正确存储和保护数据。用户(通常称为最终用户)访问系统上的数据。

欧盟数据保护法规定保护隐私数据。数据控制者可以雇佣第三方来处理数据，在这种情况下，第三方为数据处理者。数据处理者有责任对数据进行保密，并且不会将其用于任何由数据控制者指定的目的以外的任何其他目的。安全港项目包括组织同意遵守的 7 条原则，这样他们也就能够遵守欧盟数据保护法的要求。

安全基线提供了一套安全控制，组织可以将其作为安全起点来实施。一些出版物(如 NIST SP 800-53)会识别安全控制基线。然而，这些基线不会完全适用于所有的组织。相反，组织使用审视和定制技术来识别在其基线中实施的安全控制。此外，组织确保他们会实施外部标准规定的适用于他们组织的安全控制。

5.5 考试要点

理解数据分类的重要性。数据所有者负责定义数据分类，确保系统和数据被正确标记。此外，数据所有者定义保护不同分类的数据的需求，比如对静态数据和传输中的敏感数据进行加密。数据分类通常在安全策略或数据策略中定义。

知道 PII 和 PHI。个人身份信息(PII)是任何可以识别个人的信息。受保护的健康信息(PHI)是指任何与特定个人的健康有关的信息。许多法律、法规都规定保护 PII 和 PHI。

知道如何处理敏感信息。敏感信息是指所有类型的机密信息，正确地管理它们可以帮助防止由于未经授权的披露而失去保密。适当的管理包括标志、处理、存储和破坏敏感信息。组织经常漏掉

标记的两个区域是充分保护承载敏感信息的备份介质以及在介质和设备生命周期结束时对其进行净化。

理解记录保留。记录保留策略确保在需要数据时，将数据保存在可用状态，在不需要数据时将其破坏。许多法律、法规都规定数据要在特定的时间内进行保存，但是没有正式的规定，因此组织会在策略中指定保留时间。审计跟踪数据需要保持足够长的时间来重建过去的事件，但是组织必须确定他们想要调查多久之前的数据。许多组织当前的趋势是通过对电子邮件实施短期保留策略来减少法律责任。

知道不同角色之间的区别。数据所有者负责分类、标记和保护数据。系统所有者负责处理数据的系统。业务和任务所有者拥有流程，并确保系统对组织的价值。数据处理者通常是为组织处理数据的第三方实体。管理员基于数据所有者提供的指导方针授权访问数据。用户在执行工作任务的过程中访问数据。保管者负责日常存储和保护数据。

了解 7 条安全港原则。欧盟数据保护法规定保护隐私数据。第三方同意遵守 7 条安全港原则，以确保它们遵守欧盟数据保护法。7 条原则是通知、选择、向前传输、安全性、数据完整性、访问和执行。

了解安全控制基线。安全控制基线提供一份组织可以用作基线的控制清单，并不是所有的基线适用于所有的组织。然而，组织可以应用审视和定制技术来选择满足自身需求的基线。

5.6　书面实验室

1. 描述 PII 和 PHI。
2. 描述净化 SSD 的最好方法。
3. 指出组织为数据实施的 4 个分类等级。
4. 列出安全港项目中的 7 条原则。

5.7　复习题

1. 下面哪一项指的是分类过程的主要目的？
   A. 定义保护敏感数据的要求
   B. 定义备份数据的要求
   C. 定义存储数据的要求
   D. 定义传输数据的要求
2. 在确定数据分类时，以下哪一项是最重要的考虑因素？
   A. 处理系统
   B. 价值
   C. 存储介质
   D. 可访问性
3. 以下哪个答案不属于敏感数据？
   A. 个人身份信息(PII)

B. 受保护的健康信息(PHI)
C. 专有数据
D. 发布在网站上的数据

4. 标记介质的最重要方面是什么？
A. 日期标签
B. 内容描述
C. 电子标签
D. 分类

5. 在将分类介质再次用到不太安全的环境中之前，管理员通常会怎样做？
A. 擦除
B. 消除
C. 清除
D. 重写

6. 以下哪个描述正确表述了净化方法的问题？
A. 没有移除数据的方法，保证了未授权人员不能检索数据。
B. 即使已被完全焚烧的介质也会提供可推断出的数据。
C. 人员可能会不适当地执行净化步骤。
D. 存储的数据被物理销毁介质。

7. 以下哪个选项是摧毁固态硬盘上数据的最可靠方法？
A. 擦除
B. 去磁
C. 删除
D. 清除

8. 以下哪个选项是删除 DVD 上数据的最安全方法？
A. 格式化
B. 删除
C. 销毁
D. 去磁

9. 以下哪一项不会擦除数据？
A. 消除
B. 清除
C. 重写
D. 剩磁

10. 以下哪一项基于 Blowfish 并能保护免受彩虹表袭击？
A. 3DES
B. AES
C. bcrypt
D. SCP

11. 管理员会用以下哪一项来安全连接远程服务器以进行管理？
A. Telnet

B. 安全文件传输协议(SFTP)
C. 安全拷贝(SCP)
D. 安全外壳(SSH)

12. 以下哪一项是保管者通常会执行的任务？
A. 访问数据
B. 分类数据
C. 分配数据权限
D. 备份数据

13. 以下哪个数据角色最可能有权授予用户对数据的访问权？
A. 管理员
B. 保管者
C. 所有者
D. 用户

14. 以下哪一项是对数据所有者确立的“行为规则”的最好定义？
A. 确保用户只被授予对他们所需东西的访问权。
B. 决定对系统有访问权的人。
C. 识别对数据的恰当使用和保护。
D. 对系统实施安全控制。

15. 在欧盟数据保护法的背景下，以下哪一个是数据处理者？
A. 代表数据控制者处理个人数据的实体
B. 控制数据处理的实体
C. 处理数据的计算系统
D. 处理数据的网络

16. 通知、选择、向前传输及访问原则最适用的是？
A. 保密
B. 识别
C. 保留
D. 分类

17. 组织正在实施安全控制的预选基线，但发现不是所有的控制都适用。他们应该做些什么呢？
A. 不管怎样，实施所有控制
B. 确定另一条基线
C. 重新创建一条基线
D. 根据他们的需求定制基线

在回答问题 18 至 20 时请参考下面的场景：一个组织有一个数据中心，24 小时全天处理高级敏感信息。数据中心包括电子邮件服务器，管理员会清理超过 6 个月的电子邮件，以遵守组织的安全策略。对数据中心的访问是受控制的，所有处理敏感信息的系统都进行了标记。管理员定期备份在数据中心处理的数据。他们在现场保留一份备份，并把没有标记的备份发送到公司的一个仓库。仓库工人按日期整理介质，他们有过去 20 年的备份。员工白天在仓库工作，晚上和周末在离开前会将仓库锁闭。最近，仓库发生了盗窃，丢失了所有的离线备份磁带。之后，他们数据的副本，包括几年前的敏感电子邮件，开始出现在互联网网站上，因此组织的内部敏感数据被公开。

18. 在下面的选项中，哪一项可以在不牺牲安全性的情况下阻止此丢失事件的发生？
    A. 标记场地外保存的介质
    B. 不要把数据存储在场地外
    C. 将场地外的备份全部摧毁
    D. 使用安全的场地外存储设备
19. 以下哪个管理员行为可以阻止此事件的发生？
    A. 在把磁带送到仓库之前对它们进行标记
    B. 在磁带上备份数据之前清理磁带
    C. 在磁带上备份数据之前对磁带进行去磁
    D. 将磁带加入资产管理数据库
20. 在以下选项中，关于备份介质不遵守哪一项策略？
    A. 介质销毁
    B. 记录保留
    C. 配置管理
    D. 版本控制

第 6 章

密码学与对称加密算法

本章中覆盖的 CISSP 考试大纲包含：

安全工程

- I. 应用加密学
  - I.1 密码学生命周期(例如，密码学的局限性、算法/协议的管理)
  - I.2 密码学的种类(对称密码学、非对称密码学、椭圆曲线密码学)
  - I.7 不可否认性
  - I.8 完整性(哈希和撒盐)

密码学为数据的处理、存储和通信过程提供附加的安全级别。近年来，数学家和计算机科学家开发了一系列日益复杂的算法，这些算法被设计用于确保机密性、完整性、身份认证和不可否认性。在密码学家花费大量时间开发强加密算法的同时，黑客们和政府同样投入了可观的资源来破解这些密码学算法。这产生了密码学领域的“军备竞赛”，并且导致如今使用的极其精密的算法的不断发展。本章将研究密码学的历史、基本的密码学通信和私钥密码系统的基本原理。下一章将通过研究公钥密码系统和攻击者用于击败密码学的各种技术来继续对密码学的讨论。

6.1 密码学历史上的里程碑

自从有了人类，人们设计了各种不同的书写通信方法，这些方法从古人类写在岩洞墙壁上的象形文字，一直延伸到塞满了用现代英语写成的含全部信息的百科全书光盘。伴随着人类通信的发展，为了对那些局外人隐藏通信的真正含义，保密的方法应运而生。古人类社会使有复杂的秘密符号系统代表战争中安全的地方。现代文明社会使用多种代码和密码促进个人和组织之间的私人通信。在下面的内容中，你将看到现代密码学的发展和一些著名的暗中拦截和破译加密通信的尝试。

6.1.1 凯撒密码

已知最早的一种密码系统是朱利叶斯•凯撒在征服欧洲时，在罗马与西塞罗通信时使用的密码

系统。凯撒在传递信息时知道会有很多风险：送信人可能就是敌人的间谍，或者可能在通过敌方兵力部署区域的途中遭到伏击。出于这些原因，他开发了一种密码学系统，现在我们称之为凯撒密码。这个系统自身相当简单。为了对消息进行加密，可以简单地将字母表中的每个字母都替换为其后的第三个字母。例如，字母A被替换为D，而字母B则替换为E。如果在这个过程中到达了字母表的结尾，那么可以简单地返回到字母表的开始，这样字母X就替换为A，字母Y替换为B，字母Z则替换为C。因此，凯撒密码也被称为ROT3(或Rotate 3)密码。凯撒密码是单一字母的替代置换密码，也被称C3密码。

注意：

虽然凯撒密码使用 3 位的移位，但是其他根据用户所需而使用同样方式并移动任意数量字符的算法也称为凯撒密码。例如，ROT12 就是将字母 A 变为 M，将字母 B 变为 N，并以此类推。

下面给出了一个凯撒密码的实际例子。第一行是原始句子，第二行则显示了在使用凯撒密码加密后的句子：

THE DIE HAS BEEN CAST

WKH GLH KDV EHHQ FDVW

要解密这条消息，只需要简单地将每个字母都替换为前面的第三个字母。

警告：

尽管凯撒密码易于使用，但是也很容易被破解。凯撒密码很容易遭受频率分析攻击。你可能知道，英语中常见的字母是E、T、A、O、N、R、I、S和H。攻击者要破解凯撒型密码，只需通过查找加密文本中最常见的字母，然后尝试替换为英语中常见的字母，就能够确定加密模式。

6.1.2 美国内战

从凯撒时代到美国建国初期的漫长岁月里，科学家和数学家做出了巨大的成就，从而超越了古代文明所使用的早期密码。在美国内战期间，由于北部联邦和南部联邦的支持者都通过窃听对方的电报线路来刺探情报，因此双方对前线的安全通信都使用了相对先进的密码系统。这些系统使用词汇替代和置换(详细内容参看“密码”部分)的复杂组合，从而试图破坏敌人的破译企图。在内战中广泛使用的另一个系统是由军医 Albert J. Myer 开发的一系列标记符号。

注意：

关于本章诸多讨论项目的图片，可以在 www.nsa.gov/about/cryptologic_heritage/museum 这个网址看到。

6.1.3 Ultra 与 Enigma

美国人并不是唯一在追求超级编码制造机方面投入大量资源的人。在第二次世界大战之前，德国军事产业复合体为了官方使用而改造了一种名为 Enigma 的商业编码机。这台机器使用一系列 3 到 6 个转子实现了一种极复杂的替换密码。使用同时代的技术对加密消息进行破译的唯一可行方法是使用类似的机器，这些机器应当具有与传输设备使用的相同转子设置。德国人认识到保护这些设

备的重要性，这使得同盟国极难获得一台这样的设备。

同盟国军方开始了一项代号为 Ultra 的绝密工作，其目的是对 Enigma 编码进行攻击。最终，当波兰军方成功地复原了一台 Enigma 原型机并且与英国和美国的密码术专家共享了他们的成果时，他们的努力得到了回报。同盟国在 1940 年成功地破解了 Enigma 编码，历史学家相信这次成功为最终战胜轴心国起到了重要的作用。

日本人在第二次世界大战期间使用了类似的一台机器，被称为 Japanese Purple Machine。美国人对这个密码系统的攻击效果显著，导致日本人的密码在战争结束前就已被破解。美国人从日本人的发报机所使用的消息规范格式中获得了帮助，这些规范格式导致多条消息中存在大量类似文本，从而使密码分析工作变得容易了许多。

6.2　密码学基础

任何学科的研究工作都必须从对其所依赖的基本原则的讨论开始。下面的内容从几个方面对密码学基础进行了讨论：密码学的目标、密码学技术的基本概念、密码系统使用的主要数学原理。

6.2.1　密码学的目标

安全从业人员利用密码系统达到下列 4 个基本目标：机密性、完整性、身份认证和不可否认性。实现每个目标都需要满足很多设计需求，并且不是所有的加密系统都要达到所有 4 个目标。接下来，我们将对每个目标进行详细研究，并且对达到目标所需的必要技术进行简要说明。

1. 机密性

机密性确保数据在存储中(例如，存储在磁盘上)或在传输中(例如，在两方或多方之间传递)保持秘密状态。这可能是密码系统提到的最广泛目标，即促进个体和组织之间的通信保密。强制实施机密性的密码系统主要有两种类型：对称密钥密码系统使密码系统中的所有用户都能够使用一个共享的密钥，公钥密码系统使系统中的每个用户都能够使用公钥和私钥的单独组合。这两个概念将在本章稍后的“现代密码学”部分进行探讨。

提示：

保护静态数据和传输中数据的概念往往也包含在 CISSP 考试范围中。你也应该知道传输中的数据通常被称为“线缆上的数据”，指的是承载数据通信的网络电缆。

当开发以提供保密为目的的加密系统时，你必须考虑两种不同类型的数据：

- 静态数据或存储数据，是指数据保存在固定和等待接入的位置。静态数据的例子包括存储在硬盘、磁带备份、云存储服务、USB 设备和其他存储介质上的数据。
- 运动中的数据或线缆上的数据，是指在两个系统之间通过网络传输的数据。运动中的数据可能在企业网络、无线网络或公共互联网上进行传输。

运动中的数据和静态数据会构成不同类型的机密性风险，但是可以通过加密对其进行保护。例如，运动中的数据容易受到窃听攻击，而静态数据更容易受到物理设备被盗窃的风险。

2. 完整性

完整性确保数据在传输的过程中不会被修改。如果采用了适当的完整性机制，那么消息的接收者可以确定接收到的消息与发送出的消息完全相同。简单来说，完整性检查能确保存储的数据在创建和被访问期间不会遭受篡改。这样做可以防止所有形式的修改：第三方企图插入错误信息的有意修改以及因传输过程中的错误导致的无意修改。

消息完整性通过使用在传输消息时创建的数字签名消息摘要来强制实施。消息的接收者简单地对消息摘要和签名的有效性进行验证，确保消息未在传输过程中修改。公共和私钥密码系统都能够强制实施完整性。在第 7 章的“数字签名”一节中将对这个概念进行详细讨论。使用哈希加密算法来保护文件完整性将在第 21 章“恶意代码和应用攻击”中进行阐述。

3. 身份认证

身份认证对声明的系统用户身份进行验证，并且是密码系统的主要功能。例如，假设 Alice 希望与 Bob 建立通信会话，并且他们都参与到一个共享的保密通信系统。Alice 可能使用挑战/响应身份认证技术确保 Bob 名副其实。

图 6.1 显示了挑战/响应协议在实际操作中是如何运行的。在这个示例中，由 Alice 和 Bob 使用的共享秘密代码很简单：每个词汇的字母都被简单地颠倒次序。Bob 首先与 Alice 联系，并且标识自己的身份。Alice 随后向 Bob 发出挑战信息，要求他使用只有 Alice 和 Bob 知道的秘密代码对一小段消息进行加密。Bob 将加密后的消息回应给 Alice。在 Alice 验证这段加密消息的正确性之后，她相信 Bob 确实位于连接的另一端。

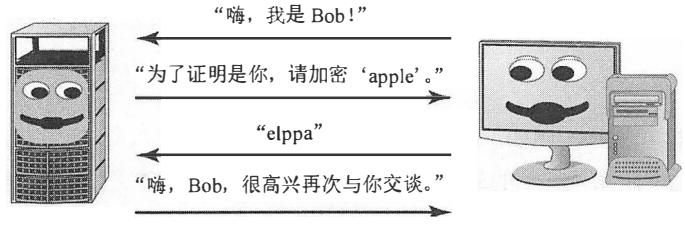


图 6.1　挑战/响应身份认证协议

4. 不可否认性

不可否认性为接收者提供了担保，保证消息确实来自发送者而不是来自伪装成发送者的人。不可否认性能够防止发送者宣称原先从未发送过信息(也被称为否认消息)。秘密密钥(或对称密钥)密码系统(如简单的替代密码)并不提供对不可否认性的保证。如果 Jim 和 Bob 都参与了某个密钥通信系统，那么他们就能够使用他们的共享密钥生成相同的加密消息。只有公钥(或非对称密钥)密码系统才提供不可否认性，第 7 章将对这个问题进行更详细的讨论。

6.2.2　密码学概念

与任何科学一样，在研究密码学之前，你必须熟悉某些术语。下面会介绍一些用于描述编码和密码的关键术语。消息在成为编码形式之前，被称为明文消息，并且在描述加密函数时使用字母 P

表示。消息的发送者使用密码学算法将明文消息加密为密文消息，并且使用字母 C 表示。消息通过一些物理的或电子的方式被传送给接收者。接收者随后使用预先确定的算法对密文消息进行解密，从而得到明文形式的消息(关于这个过程的详细解释，请参看本章后面的图 6.3)。

所有密码学算法都依赖密钥来维护其安全性。在很大程度上，密钥只不过是一个数字。密钥往往是一个非常大的二进制数，不过仍然是一个数字。每种算法都具有一个特定的密钥空间。密钥空间是一段值的范围，此范围内的值可作为密钥算法的有效密钥。密钥空间由其位的长度定义。位的长度只不过是密钥中的比特数或位数(0s 和 1s)。密钥空间的范围为：从所有位全部为 0 到所有位全部为 1。如果采用另一种方式表示，那么密钥空间的范围为 0 到 2n，其中 n 是密钥的位的长度。因此，128 位密钥的值可以从 0 到 2^{128}(大约为 $3.40282367*10^{38}$，这是一个相当大的数字)。保护密钥的安全是非常重要的。事实上，从密码学获得的所有安全性就只能依赖于保证秘密使用密钥的能力。

Kerchoff 原则

所有密码学都基于算法的思想。算法通常是一组数学规则，这组规则规定如何进行加密和解密过程。大多数算法都遵循 Kerchoff 原则，这条原则使算法已知和公开，并且允许任何人检查和测试算法。说的明确一些，Kerchoff 原则(也被称为 Kerchoff 假设)就是算法应当公开，但是所有密钥都应当保密。这条原则可归纳为“敌人知道了这个体系”。

许多密码学家都遵循这条原则，但是并非所有人都如此。事实上，一些人坚持相反的观点，他们坚信算法和密钥都保密能够维护更佳的整体安全性。Kerchoff 原则的支持者反驳这种相反的做法包含“隐藏式保全”习惯，并且相信公开算法能够产生更大的活力，能够更容易地暴露更多的弱点，从而使人们能够放弃不够强壮的算法，并且可以更快地采用适合的算法。

正如你将在本章和下一章中学到的那样，不同类型的算法要求不同类型的密钥。在私钥(或秘密密钥)密码系统中，所有参与者都使用单个共享的密钥。在公钥密码系统中，每个参与者都具有自己的密钥对。密钥有时被称为密码变量。

创建和实现秘密编码和密码的技术被称为密码术，与之对应的技术是密码分析学——对解码和解密方法进行的学习研究。通常，密码术与密码分析学一起被称为密码学。编码或密码在硬件和软件上的具体实现被称为密码系统。美国联邦信息处理标准 140-2(FIPS140-2)的“密码模块的安全需求”为美国联邦政府使用的密码模块定义了硬件和软件需求。

提示：

在继续学习本章和下一章的内容之前，必须确保理解这些术语的含义。对于理解接下来要介绍的密码学算法的技术细节来说，理解这些术语是必不可少的。

6.2.3　密码学的数学原理

由于密码学存在数学基础，因此它与大多数计算机科学学科没有什么区别。为了全面理解密码学，必须首先理解二进制数学的基本知识以及用于操作二进制数值的逻辑操作。下面将对最基本的一些概念进行简要介绍，这些概念是你应该熟悉的内容。

1. 二进制数学

二进制数学定义了一些形成所有计算机神经系统的比特和字节所使用的规则。你非常熟悉十进

制系统。十进制系统是一个以 10 为基础的系统，其中每一位都是从 0 到 9 的整数，并且每一位都是 10 的倍数。我们所依赖的这个十进制系统很可能具有生物学起源——人类有 10 根手指用来计数。

提示：

二进制数学一开始可能会很混乱，但是我们值得花时间来学习各种逻辑运算是如何工作。更重要的是，为了真正理解密码学算法的内在工作原理，你需要理解这些概念。

类似的，计算机依赖的二进制系统起源于电。在电流中，只有两种可能的状态：开(代表存在电流)和关(代表没有电流)。电子设备执行的所有计算都必须利用这些术语来表达，这就出现了现代电子学中对二进制的使用。总的来说，计算机科学家将开的状况称为真，将关的状况称为假。

2. 逻辑运算

密码学的二进制数学使用多种逻辑函数来操纵数据。接下来我们将对这些逻辑运算进行简要介绍。

AND

AND 运算(用符号∧表示)可以检查两个值是否都为真。下面的这张真值表说明了 AND 函数的所有 4 种可能的结果。需要记住的是，AND 函数只有两个输入变量。在二进制数学中，每个变量都只有两种可能的值，因而为 AND 函数准备了 4 种可能的输入。正是这种有限的可能性才使得计算机在硬件上实施逻辑函数变得非常容易。在下面的真值表中可以看到，只有一组输入组合(其中两个输入值都为真)的输出值能够为真值：

X	Y	X ∧ Y
0	0	0
0	1	0
1	0	0
1	1	1

逻辑运算常常在整个二进制代码的基础上执行，而不是在单一的数值基础上执行。让我们来看一看下面的例子：

```
   X:   0 1 1 0 1 1 0 0
   Y:   1 0 1 0 0 1 1 1

--------------------------
X ∧ Y:   0 0 1 0 0 1 0 0
```

可以看到，AND 函数通过比较每一列上 X 和 Y 的值进行计算。只有在 X 和 Y 的值都为真的列上，结果才为真。

OR

OR 运算(用符号∨来表示)可以检查是否至少有一个输入值为真。下面的真值表中列出了 OR 函数的所有可能的值。可以看到，只有在两个输入值都为假时，OR 函数的结果才会返回假：

X	Y	X ∨ Y
0	0	0
0	1	1
1	0	1
1	1	1

我们可以利用与上面相同的例子，如果 X 和 Y 执行 OR 运算而不是 AND 运算，输出内容如下所示：

```
    X:   0 1 1 0 1 1 0 0
    Y:   1 0 1 0 0 1 1 1
-------------------------
X ∨ Y:   1 1 1 0 1 1 1 1
```

NOT

NOT 运算(用符号~或!来表示)简单地将输入值取反。这个函数每次只对一个变量进行操作。下面是 NOT 函数的真值表：

X	~X
0	1
1	0

在下面的例子中，我们对前面示例中的 X 值进行 NOT 运算：

```
 X:     0 1 1 0 1 1 0 0
-------------------------
~X:     1 0 0 1 0 0 1 1
```

XOR

本章要研究的最后一个逻辑函数可能在密码学应用中最为重要且最常用，这就是异或(XOR)操作。在数学文献中，也被称为 XOR 函数，并且通常用符号⊕表示。只有在一个输入值为真时，XOR 函数的结果才为真。如果两个输入值都为假或都为真，那么 XOR 函数的结果为假。下面是 XOR 运算的真值表：

X	Y	X ⊕ Y
0	0	0
0	1	1
1	0	1
1	1	0

在下面的示例中，可以看到当 X 和 Y 进行 XOR 运算时的情况：

```
   X:   0 1 1 0 1 1 0 0
   Y:   1 0 1 0 0 1 1 1

--------------------------
X ⊕ Y:   1 1 0 0 1 0 1 1
```

3. 模函数

在密码学领域，模函数极为重要。回想一下我们最初学习除法时的情形。在那时，你并不熟悉小数，每次在进行除法操作时都会得出余数。计算机本来也不理解小数系统，并且这些余数在计算机执行很多数学运算时起到了至关重要的作用。模函数十分简单，也就是在完成除法运算后得到余数。

提示：

对于密码学来说，模函数就如同逻辑运算一样重要。应该确保对其功能非常熟悉，并且可以执行一些简单的模运算。

在等式中，模函数通常由缩写词 mod 来表示，不过有时也会用%运算符来表示。下面给出了几个模运算的输入和输出示例：

```
 8 mod 6 = 2
 6 mod 8 = 6
10 mod 3 = 1
10 mod 2 = 0
32 mod 8 = 0
```

我们将在第 7 章探讨 RSA 公钥算法(以其发明者 Rivest、Shamir、Adleman 命名)时再次介绍这种运算。

4. 单向函数

单向函数是一种数学运算，它可以通过所有可能的输入值组合得出结果，但是反向得出输入值却是不可能的。公钥密码系统都建立在单向函数的基础上。但实际上，人们从未证明过任何指定的已知函数确实是单向的。密码员依赖于他们认定的单向函数，但是理论上它们可能会被将来的密码分析人员破解。

这里举一个例子。试想你有一个三个数相乘的函数。如果限制输入值是一位数字，那么通过查看数值结果反向设计这个函数并确定可能的输入值是相当简单的。例如，通过 1、3 和 5 这三个输入值可以得到结果 15。然而，假设限制输入值为 5 位的素数。通过计算机或计算器获得结果还是很简单的，但是反向推算就不是那么简单了。你能算出 10 718 488 075 259 是哪三个素数得出的结果吗？不是那么简单，对吗？(这三个数是 17 093、22 441 和 27 943)。实际上 5 位的素数共有 8 363 个，因此利用计算机或穷举攻击算法可能会破解这个问题，但口算是无法得出结果的，这一点是肯定的！

5. 随机数

密码学往往通过在加密过程中添加随机性来获得强度。实现这个目标的一种方法是使用随机数。随机数是随机数字发生器，起到了数学函数中占位符变量的作用。执行数学函数时，占位符会被替换为在处理时刻生成的随机数。每次使用数学函数时，随机数都会产生一个独特的数字。随机数的一个更为人接受的示例是初始向量(Initialization Vector，IV)，这是一个与分组长度相同的随机比特串，并且与原始消息相异或。在每次使用相同密钥加密相同的消息时，IV 都被用于创建独特的密文。

6. 零知识证明

密码学的一个优点是建立了这样的机制：在不向第三方揭示事实本身的情况下向第三方证明对事实的了解。这种机制通常涉及密码和其他秘密的身份认证。

零知识证明的经典示例涉及两个人：Peggy 和 Victor。Peggy 知道环形洞穴内部暗门的密码，如图 6.2 所示。Victor 愿意从 Peggy 那里购买密码，但是在付款之前希望 Peggy 证明她确实知道密码。因为担心得不到酬金，所以 Peggy 也不愿意先将密码告诉 Victor。零知识证明就能够解决这个左右为难的问题。

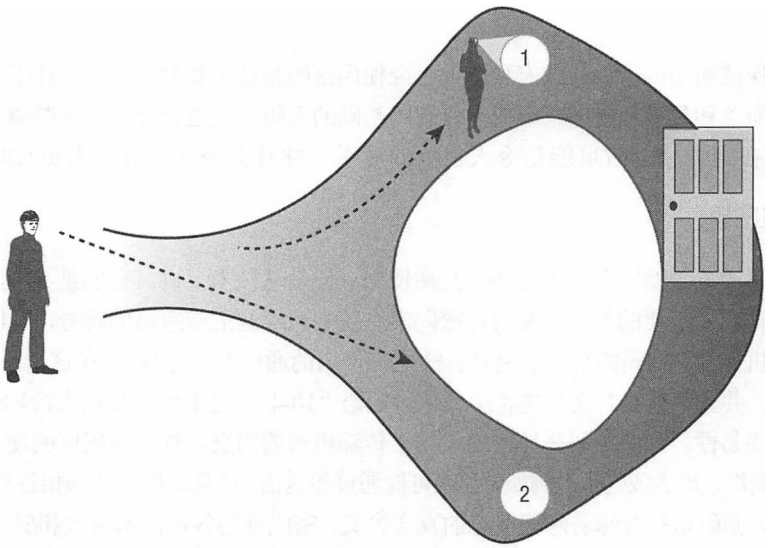


图 6.2　魔法门

Victor 可以站在洞穴的入口，并且目送 Peggy 进入洞穴。Peggy 随后到达暗门，并且使用密码打开暗门。她穿过暗门，最后通过路径 2 返回洞穴入口。Victor 看到 Peggy 从路径 1 进入洞穴，然后通过路径 2 返回，这就证明她肯定知道打开暗门的密码。

7. 分割知识

如果执行某个操作所需的信息或权限在多个用户之间分配时，任何一个人都没有足够的权限来危害环境的安全性。单个解决方案中包含的这种职责分离和两人控制被称为分割知识。分割知识的最佳示例就是密钥托管的概念。通过使用密钥托管，密码密钥、数字签名甚至数字证书，可以被存储在或备份在一种被称为密钥托管数据库的特殊数据库中。如果用户的密钥丢失或损坏，那么可以从备份中抽取出相应的密钥。然而，如果只存在一个密钥托管恢复代理，那么就有机会伪

造和滥用这种权限。“M of N 控制”要求：在总数为 N 的代理中，最少需要 M 个代理一起工作才能完成安全性很高的任务。因此，“3 of 8 控制”要求 8 个人(被分配了密钥托管恢复代理的工作任务)中的 3 个人一起完成工作，才能从密钥托管数据库中取出单个密钥(本例说明了 M 始终小于等于 N)。

8. 工作函数

通过使用工作函数或工作因数，从成本和/或时间方面来度量所有努力，就可以度量密码学系统的强度。通常，针对加密系统执行完全穷举攻击所需的时间和努力，就是工作函数所表示的内容。密码系统提供的安全性和保护与工作函数/因数的值成正比。工作函数的大小应当与受保护资产的相对值匹配。工作函数只需稍大于受保护资产的时间值。换句话说，所有安全性(包括密码学)都应当是有效益的和有效率的。保护某个资产所花费的成本不能超过这个资产自身的价值，但是一定要保证提供足够的保护。因此，如果信息由于时间的推移而失去价值，那么工作函数的大小只需确保在数据失去价值前提供保护即可。

6.2.4 密码

许多关心保持通信机密性的政府和个人已经使用密码系统很长时间了。在接下来的内容中，我们将对密码的概念和几种常见的、形成现代密码基础的密码类型进行介绍。这些概念看起来只是基础知识，但是在组合使用时可能是令人畏惧的对手，并且会令密码分析人员长时间无法破解。

1. 编码与密码

人们常常将词汇“编码”和“密码”互换使用，但是从技术上讲，它们是不能互换的。在这两个概念之间，存在很重要的差异。编码是密码学系统中表示词汇或短语的符号，有时是秘密的，但是不一定提供机密性。编码的常见示例是执法机构使用的通信“10 系统”。在这个系统中，语句“我收到你的信息，并且理解其含义”被表示成编码短语“10-4”。这个编码是众人皆知的，但是它确实提供了通信的简易性。一些编码是秘密的。为了传输机密的消息，这些编码可能使用数学函数或密码字典来表示词汇、短语或句子。例如，间谍可能通过传送语句“鹰着陆了”来报告敌人飞机的来袭。

另一方面，密码总是意味着隐藏消息的真实含义。密码使用各种技术修改和/或重新排列消息中的字符或比特，从而实现机密性。在比特(也就是二进制编码的单个位)、字符(也就是 ASCII 码消息的单个字符)或分组(也就是一条消息的固定长度分段，通常用比特数表示)的基础上，密码将消息从明文转换为密文。接下来将介绍几种目前常用的密码。

提示：

记住编码和密码之间差异的一种简单方法是：编码针对词汇和短语，而密码则针对单独的字符和比特。

2. 换位密码

换位密码使用某种加密算法重新排列明文消息中的字母，从而形成密文消息。解密算法只需反演加密转换过程就可以得到原始消息。

在本章前面的图 6.1 所示的挑战/响应协议示例中，一个简单的换位密码被用于简单地调换消息中的字母，从而使 apple 变成 elppa。换位密码可能会比这个示例复杂得多。例如，可以使用一个密钥来执行柱状换位(columnar transposition)。在该例中，我们试图利用密钥 attacker 对信息“The fighters will strike the enemy bases at noon”进行加密。首先，我们要取出密钥的字母，并且依照字母顺序进行编号。第一个字母 A 的值为 1，第二个字母 A 的值为 2，下一个字母按顺序是 C，编号为 3，依此类推。结果就是下面这个顺序：

```
A T T A C K E R
1 7 8 2 3 5 4 6
```

接下来，消息中的字母按顺序写在密钥字母的下面：

```
A T T A C K E R
1 7 8 2 3 5 4 6
T H E F I G H T
E R S W I L L S
T R I K E T H E
E N E M Y B A S
E S A T N O O N
```

最后，发送者通过向下读取每一列对消息进行加密，这些列的顺序依据第一步中分配的数字读取。这个过程便产生了如下所示的密文：

```
T E T E E F W K M T I I E Y N H L H A O G L T B O T S E S N H R R N S E S I E A
```

在另一端，接收者利用密文和相同的密钥重建这个 8 列矩阵，随后按行读取得到明文消息。

3. 替代密码

替代密码使用加密算法将明文消息中的每一个字符或比特都替换为不同的字符。在本章开始时讨论的凯撒密码就是替代密码的一个很好的例子。现在我们已经学习了密码学的一些数学知识，所以将从另外的方面研究凯撒密码。前面曾经介绍过，我们简单地将消息中的每个字母都替换为其右侧第三个字母，从而生成密文。然而，在到达字母表的末端并且用光了字母时，我们碰到了问题。通过绕回到字母表的开头就可以解决这个问题，这样明文字符 Z 变成了密文字符 C。

通过将每个字母转换成与之对等的十进制值(即 A 等于 0，Z 等于 25)，就可以采用数学关系来表示 ROT3 密码。随后，通过将每个明文字母加 3 就能够确定密文。利用“密码学的数学原理”一节中的模函数可以将回绕过程考虑在内。凯撒密码最终的加密函数如下所示：

```
C = (P + 3) mod 26
```

对应的解密函数如下所示：

```
P = (C - 3) mod 26
```

与换位密码一样，有很多替代密码比本章提供的示例更复杂。多字母替代密码在相同的消息中使用多个字母表来阻碍解密操作。多字母替代密码的一个著名示例是 Vigenere 密码。Vigenere 密码使用如下所示的单个加密/解密图表：

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

可以看到，这个图表只是重复书写(26 次)的字母表，每一列的首字母都是前一列首字母的下一个字母。Vigenere 系统需要使用一个密钥。例如，密钥可以为 secret。随后，可以执行下列加密过程：

(1) 写下明文及密钥。

(2) 根据需要重复密钥，从而建立一行与明文长度相同的文本。

(3) 将每个字母位置都从明文转换为密文。

a. 定位以第一个明文字符(a)开头的列。

b. 随后，定位以第一个密钥字符(s)开头的行。

c. 最后，定位所找出行列的交叉点，并且写下交叉点的字母，这就是相应的密文字母。

(4) 重复步骤(1)至(3)，对明文的所有字母进行加密。

明文:	a t t a c k a t d a w n
密钥:	s e c r e t s e c r e t
密文:	s x v r g d s x f r a g

虽然多字母替代能够防范直接的频率分析，但是容易遭受二阶形式的频率分析(也被称为周期分析攻击，这种攻击基于密钥的重复使用进行频率检查)。

4. 一次性填充

一次性填充是一种极为强大的替代密码。一次性填充对明文消息的每个字母都使用一个不同的字母表。它们可以通过下面的加密函数来表示，其中 K 是以 C 表示的字母的加密密钥：

```
C = (P + K) mod 26
```

通常，一次性填充被记为插入函数的一个很长的数字序列。

注意：

一次性填充也被称为 Vernam 密码，这种密码以 AT&T Bell 实验室的发明者 Gilbert Sandford Vernam 的名字命名。

一次性填充的巨大好处是：如果运用得当，它是一个不可破解的加密方案。由于不存在重复的字母替代模式，这使得密码分析工作徒劳无益。然而，为了确保算法的完整性，必须满足下列几个要求；

- 加密密钥必须随机生成。使用一个短语或书中的一段话会引入密码分析人员破译这个编码的可能性。
- 一次性填充必须进行物理保护，以防泄露。如果敌人具有这个一次性填充的副本，那么他们就可以轻易地破译加密的消息。

注意：

可以考虑一下这一点：凯撒密码、Vigenère 密码和一次性填充密码听起来非常相似。它们确实如此，不同之处只是密钥的长度。凯撒切换密码用的是一位的长度，Vigenère 密码用的是更长的长度(通常是一个词或一句话)，一次性填充密码用的就是消息本身。

- 每个一次性填充必须只使用一次。如果填充被重复使用，那么密码分析人员可以比较多个使用相同填充的加密消息中的相似之处，并有可能确定使用的密钥值。
- 密钥必须至少与被加密的消息一样长，这是因为每个密钥元素都只对消息中的一个字符进行编码。

提示：

这些一次性填充的安全性要求是所有网络安全从业人员都要掌握的基本知识。人们时常试图实现一次性填充密码系统，但却无法达到其中的一个或多个基本要求。了解整个 Soviet 编码系统是如何由于在这方面的粗心大意而被破解的例子。

如果这些要求中的任意一个没有被满足，那么一次性填充难以破解的本质特性就会立即消失。实际上，美国谍报工作的一个主要成功之处是由于密码分析人员破解了依赖使用一次性填充的绝密的Soviet密码系统。在这个代号为VENONA的计划中，Soviet在填充中所使用的密钥值的生成模式被发现了。这个模式的存在违反了一次性填充密码系统的第一个要求：密钥必须随机生成，不使用任何重复的模式。整个VENONA项目直到最近才被公开，并且在美国国家安全局的Web站点www.nsa.gov/about/_files/cryptologic_heritage/publications/coldwar/venona_story.pdf上可以看到相关的信息。

一次性填充一直被用于保护极其敏感的通信，不能被广泛使用的主要障碍是很难生成，以及分发和保护所需的冗长密钥。由于密钥的长度问题，一次性填充在实际中只可用于短消息。

5. 滚动密钥密码

密码学的许多脆弱性都涉及密钥的有限长度。前面刚介绍过，通过在加密和解密期间为每个密码转换使用不同的字母表，一次性填充避免了这些脆弱性。然而，因为要求填充的物理交换，所以一次性填充难以实现。

对于这个难题，一个常见的解决方案是使用滚动密钥密码，也被称为书籍密码。在这种密码中，加密密钥与消息本身一样长，并且往往从一般的书籍中选取。例如，发送者和接收者可以预先约定使用 *Moby Dick* 中某一章节从第三段开始的文本作为密钥。双方只是使用足够多的连续字符以便执行加密和解密操作。

让我们来看一个例子。假设希望使用刚才描述的密钥加密消息“Richard will deliver the secret package to Matthew at the bus station tomorrow”。这条消息的长度为 66 个字符，因此需要使用滚动密钥的前 66 个字符：“With much interest I sat watching him. Savage though he was, and hideously marred”。随后，任何算法都可以使用这个密钥来加密明文消息。以模 26 加法为例，这种算法会将每个字母都转换为相应的十进制数，然后将明文与密钥相加，最后执行模 26 运算得到密文。如果指定字母 A 对应值 0、字母 Z 对应值 25，那么对消息的前两个词汇进行加密后得到的密文如下所示：

明文	R	I	C	H	A	R	D	W	L	L
密钥	W	I	T	H	M	U	C	H	N	T
数字明文	17	8	2	7	0	17	3	22	11	11
数字密钥	22	8	19	7	12	20	2	7	13	19
数字密文	13	16	21	14	12	11	5	3	24	4
密文	N	Q	V	O	M	L	F	D	Y	E

当接收方接收到密文时，他们会使用相同的密钥，从密文中减去密钥，执行模 26 运算，最后将得到的明文结果转换回字母表字符。

6. 分组密码

分组密码按消息的“组块”或分组进行操作，并且对整个消息分组同时应用加密算法。换位密码就是分组密码的一个例子。在挑战/响应算法中使用的简单算法，是取出完整的词汇并且逆向排列字母。更加复杂的柱状换位密码对整条消息(或一段消息)进行操作，并且使用换位算法和保密密钥对消息进行加密。大多数现代加密算法都实现了某些类型的分组密码。

7. 流密码

流密码对消息(或数据流)中的每个字符或每一位进行操作，每次只处理一个字符/一位。凯撒密码就是流密码的一个例子。一次性填充也是一种流密码，这是因为该算法对明文信息中的每个字符独立进行操作。流密码也可以作为一种分组密码使用。在此类情况下，某个缓冲区被填满实时数据，随后这些数据作为分组进行加密并传送给接收方。

8. 混淆与扩散

密码学算法依靠两种基本的操作来隐藏明文信息：混淆与扩散。混淆出现在明文和密钥的关系十分复杂时，此时攻击者不能通过继续修改明文和分析产生的密文来确定密钥。扩散出现在明文的改变导致多种变化时，这些变化被扩散到整个密文中。

思考一下，例如一个算法，首先执行一种复杂的替换，然后使用换位去重新排列替换后的字符。在这个例子中，替换引入了混淆，换位引入了扩散。

6.3　现代密码学

为了实现密码学的机密性、完整性、身份认证和不可否认性目标，现代密码系统利用计算复杂的算法和长密钥。接下来的内容将介绍密码学在数据安全领域中的作用，并且研究目前常用的三种算法类型：对称加密算法、非对称加密算法和散列算法。

6.3.1　密钥

在密码学的早期，其中一条主导原则就是“通过隐匿实现安全”。密码学家们认为保护加密算法安全的最好办法就是对外人隐藏算法的细节。旧的密码系统要求通信双方保持对信息加密和解密所使用算法的安全性，并且不对第三方泄露。算法的任何泄露都可能导致对手对整个系统的破坏。

现代密码系统并不依赖于其算法的安全性。事实上，大多数密码系统的算法在附带的文献和互联网上都能够找到，并且可以公开查阅。通过向公众开放审查，实际上也改善了算法的安全性。计算机安全机构对于算法的广泛分析，允许从业人员发现并纠正潜在的安全脆弱性，并且确保他们用于保护通信的算法尽可能安全。

现代密码系统不依赖于保密的算法，而是依赖于具体的用户或用户组专用的一个或多个密钥。在对换位密码的讨论中曾经提到过，柱状换位中使用的密钥被用于指导加密和解密操作。用于实现柱状换位的算法非常有名，在本书中刚刚进行了详细介绍。然而，只要选择了外人猜不出的密钥，柱状换位就可以被用于双方的安全通信。只要密钥的安全性得到维护，那么就不必担心第三方会知

道算法的细节。

注意：

不过需要注意的是，柱状换位存在几个固有的弱点，这使得它容易受到密码分析人员的攻击，因此对于现代安全通信来说是一种不恰当的应用技术。

在本章前面对一次性填充的讨论中，你知道了一次性填充算法的强度来自于使用极长的密钥这个事实。实际上，对于这个算法来说，密钥至少要与消息本身的长度相等。大多数现代密码系统并不使用那么长的密钥，但是在确定密码系统的强度和加密无法通过密码分析技术破解的可能性中，密钥的长度仍是一个极为重要的因素。

计算能力的快速增长，使得能够在密码学工作中使用日益变长的密钥。然而，密码分析人员试图破解你所使用的算法时，也能够使用相同的计算能力。因此，使用足够长的、超出对手破解能力的密钥，对于击败同时期密码分析人员的工作是非常重要的。此外，如果希望数据直到将来的某个时候仍然无法被密码分析人员破解，那么在数据保持安全的整个时间段里，必须努力使用超出分析能力增长速度的密钥。

几十年前，在数据加密标准(DES)建立时，56 位的密钥被认为足以维持任何数据的安全性。然而，由于在密码分析技术和超级计算能力方面的进步，现在人们已经广泛认识到 56 位的 DES 算法已不再安全。现代密码学系统使用至少 128 位的密钥对数据进行保护。记住，密钥的长度直接和加密系统的功能性相关，密钥长度越长，就越难破解加密系统。

6.3.2 对称密钥算法

对称密钥算法依赖于一个“共享的秘密”加密密钥，该密钥会被分发给所有参与通信的成员。所有通信成员都使用这个密钥进行消息的加密和解密，因此发送者和接收者都拥有共享密钥的副本。通信两端会使用相同的密钥加密和解密消息。当使用很长的密钥时，对称加密难以被破解。对称密钥算法主要被用于执行批量加密，并且只为安全服务提供机密性。对称密钥密码学也被称为秘密密钥密码学和私有密钥密码学。图 6.3 说明了对称密钥的加密和解密过程。

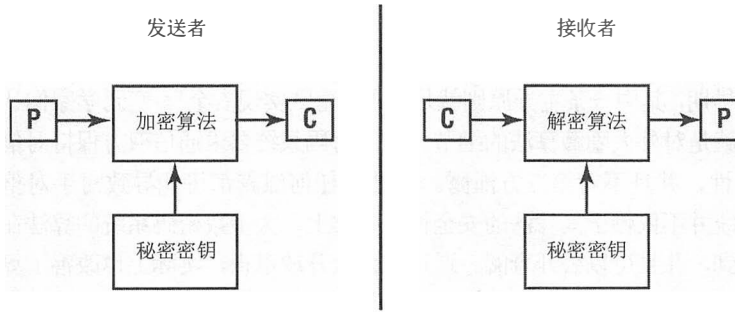


图 6.3 对称密钥密码学

注意：

术语“私有密钥”的使用比较复杂，其原因在于它是具有两种不同含义的三个不同术语中的一部分。术语“私钥”指的始终是公钥密码学(也就是非对称密钥密码学)密钥对中的私钥。不过，私有密钥密码学和共享私钥指的都是对称密码术。词汇“私有”的含义被延伸为两个人共享要保守的

秘密，而不是原有的真实含义：只有一个人知道要保守的秘密。在学习过程中，一定不要混淆这些术语。

对称密钥密码学具有下列几个弱点：

密钥分发是一个主要问题。在使用对称密钥协议建立通信之前，通信参与者必须具备一种安全交换密钥的方法。如果没有可用的安全电子通道，那么往往必须使用离线的密钥分发方法(已不属于交换)。

对称密钥密码学并未实现不可否认性。由于任意通信方都可以利用共享的密钥对消息进行加密和解密，因此无法分辨指定消息的来源。

这种算法不可扩展。对于大的用户组来说，使用对称密钥密码进行通信非常困难。只有在每个可能的用户组合共享私有密钥时，组中个人之间的安全专有通信才能实现。

密钥必须经常更新。每当有成员离开用户组时，所有涉及这个成员的密钥都必须被抛弃。

对称密钥密码学的主要强度在于能够以极快的速度进行操作。对称密钥算法的速度很快，通常是非对称密钥算法的 1000 倍到 10 000 倍之间。鉴于其数学特性，对称密钥密码学还可以在硬件上实现，这为更高速度的运行创造了机会。

本章稍后的“对称密码”部分将详细介绍目前使用的一些主要密钥算法。

6.3.3　非对称密钥算法

非对称密钥算法也被称为公钥算法，它为对称密钥加密的弱点提供了解决方案。在这个系统中，每个用户都有两个密钥：一个在所有用户之间共享的公钥，以及另一个只有用户自己知道并保管的私钥。但是让人意想不到的是：相对立的和相关的密钥必须被先后应用于加密和解密。换句话说，如果使用公钥加密消息，那么只有相关的私钥能够进行解密，反之亦然。

图 6.4 说明了公钥密码系统中加密和解密消息所使用的算法。考虑一下这个例子：如果 Alice 希望使用公钥密码学向 Bob 发送消息，她首先生成这条消息，随后使用 Bob 的公钥对消息进行加密。对这个密文进行解密的唯一可能办法是使用 Bob 的私钥，并且唯一有权使用这个密钥的用户就是 Bob。因此，Alice 在加密消息后，甚至不能对这条消息进行解密。如果 Bob 希望向 Alice 发出回应消息，他会使用 Alice 的公钥对回应消息进行加密，Alice 随后可以使用她自己的私钥对消息进行解密，从而读取这些消息。

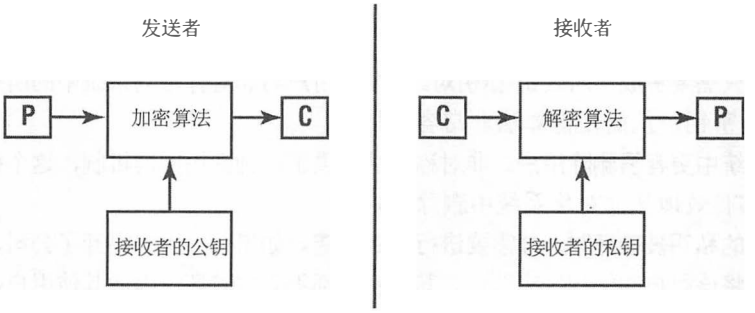


图 6.4　非对称密钥密码学

真实场景

密钥需求

最近，本书的一位作者在授课时，一位学生希望了解与对称加密算法相关联的可扩展性问题示例。对称密码系统要求每对潜在的通信者都具有一个共享的私有密钥，这一事实使得对称加密算法不可扩展。使用对称密码学的 n 个通信方之间实现完全连接所需的密钥总数可以用下面的公式表示:

$$\text{密钥的数量}=\frac{n^{*}(n-1)}{2}$$

在现实情况下，这个数字似乎还可以接受(对于小系统来说)，但是请仔细查看表 6.1。显而易见，参与者越多，对称密码系统就越难满足相应的密钥数量需求。

表 6.1 密钥数量与参与者数量的关系

参与者数量	需要的对称密钥数量	需要的非对称密钥数量
2	1	4
3	3	6
4	6	8
5	10	10
10	45	20
100	4950	200
1000	499 500	2000
10 000	49 995 000	20 000

非对称密钥算法还提供对数字签名技术的支持。本质上，如果 Bob 希望使其他用户确信带有其签名的消息是由 Bob 本人发送的，那么首先要使用散列算法(在下一节中你将看到更多散列算法)创建一个消息摘要。Bob 随后使用其私钥对消息摘要进行加密。所有希望验证这个签名的用户只需要利用 Bob 的公钥对消息摘要进行解密，然后验证解密的消息摘要是正确的。这个过程将在第 7 章中进行详细阐述。

下面列出了非对称密钥密码学的主要优点：

增加新用户只需要生成一对公钥-私钥对。这个新用户与非对称密码系统中的所有用户通信时都使用这对相同的密钥，从而使得算法非常容易扩展。

从非对称系统中更容易删除用户。非对称算法提供了一种密钥撤消机制，这个机制准许密钥被取消，从而能够有效地从非对称系统中删除用户。

只有在用户的私钥被破坏时，才需要进行密钥重建。如果某位用户离开了公司，那么系统管理员只需要简单地将该用户的密钥作废即可。其他密钥都不会被破坏，因此其他用户都不需要进行密钥重建。

非对称密钥加密提供了完整性、身份认证和不可否认性。如果某位用户没有与其他个体共享其私钥，那么具有该用户签名的消息就是正确无误的，并且具有特定的来源，在以后的任何时刻都不能被否认。

密钥分发是一个简单的过程。希望加入非对称密码系统的用户，只需要使他们的公钥对于所有与他们进行通信的人来说可用就可以了。目前尚无办法从公钥导出私钥。

不需要预先存在通信链接。两个个体可以从通信一开始就进行安全的通信。非对称密码学并不要求预先存在能够提供安全数据交换机制的关系。

公钥密码学的主要弱点是运算速度慢。因此，很多需要安全传输大量数据的应用程序会使用公钥密码学建立连接，然后交换对称密钥。会话任务的剩余部分随后采用对称密码学开始运作。表 6.2 比较了对称和非对称密码学系统。仔细查看这个表可以发现，一种系统中的弱点恰好与另一种系统中的优点互补。

表 6.2　对称和非对称密码学系统的比较

对称密码学系统	非对称密码学系统
单个共享的密钥	密钥对
带外交换	带内交换
不可扩展	可扩展
快速	慢速
批量加密	小块数据分组、数字签名、数字封装、数字证书
机密性	完整性、机密性、身份认证、不可否认性

注意：

第 7 章提供了现代公钥加密算法的技术细节及一些应用。

6.3.4　散列算法

在上一节中，你学习了公钥密码系统在与消息摘要一起使用时可以提供数字签名的能力。消息摘要概述了经过散列算法处理的消息内容(与文件的校验和不同)。如果可能的话，从理想的散列函数中派生出消息是非常困难的，并且两条消息生成相同散列值的可能性几乎是不存在的。

下面列出了目前常用的一些散列算法：

- 消息摘要 2(MD2)
- 消息摘要 5(MD5)
- 安全散列算法(SHA-0、SHA-1 和 SHA-2)
- 基于散列的消息身份认证代码(Hashed Message Authentication Code，HMAC)

第 7 章“PKI 和密码学应用”提供了这些当代的散列算法的细节，并且解释了如何使用它们提供数字签名能力，此能力可以帮助我们实现密码学的完整性和不可否认性目标。

6.4　对称密码

你已经学习了对称密钥密码、非对称密钥密码以及散列函数内在的基本概念。在下面的内容中，我们将深入讨论下列几种常见的对称密码系统：数据加密标准(DES)、三重数据加密算法(3DES)、

国际数据加密算法(IDEA)、Blowfish、Skipjack 以及高级加密标准(AES)。

6.4.1 数据加密标准

美国政府在 1977 年公布了数据加密标准(DES)，并且将之作为向所有政府通信而提议的标准密码系统。由于该算法中的缺陷，密码学界和政府不再认为 DES 是安全的。大家普遍相信情报机构已经能轻易破解 DES 加密的信息。DES 在 2001 年 12 月被高级加密标准取代。了解 DES 仍然是重要的，因为它是构成三重 DES(3DES)的基础，该加密算法将在下一节进行阐述。

DES 是一个 64 位的分组密码，具有 5 种操作模式：电子代码本(Electronic CodeBook，ECB)模式、密码分组链接(Cipher Block Chaining，CBC)模式、密码回馈(Cipher FeedBack，CFB)模式以及输出回馈(Output FeedBack，OFB)模式和计数(CounTeR，CTR)模式。这些模式将在接下来的内容中进行阐述。所有 DES 模式每次处理 64 位的明文，并且生成一个 64 位的密文分组。DES 使用的密钥长度为 56 位。

DES 利用长序列的异或(XOR)操作生成密文。每个加密/解密操作都要重复 16 次这个过程，每次重复通常被称为“一轮”加密，因此 DES 要执行 16 轮加密。

注意：

正如所提到的那样，DES 使用一个 56 位的密钥来进行加密和解密操作。然而，某些文献可能会说 DES 使用一个 64 位的密钥。这并不矛盾，其中具有完美的逻辑解释。DES 规范确实有使用 64 位密钥的说法。然而在这 64 位中，实际上只有 56 位包含密钥信息，其余 8 位包含奇偶信息，从而确保 56 位密钥是正确的。然而，这些奇偶位事实上很少使用，只需要牢牢记住这 56 位数字。

1. 电子代码本模式

电子代码本(ECB)模式是最容易了解的模式，但安全性最差。这个算法每次处理一个 64 位分组，它简单地使用所选择的密钥对这个分组进行加密。这意味着如果算法多次遇到相同的分组，那么将产生完全相同的加密分组。如果敌人正在对通信进行偷听，那么就可以简单地建立起所有可能加密值的“代码本”。在收集到足够多的分组后，就可以使用密码分析技术对一些分组进行解密并破解加密方式。

除了最短传输之外，这个脆弱性使得通过 ECB 模式进行传输并不现实。在日常使用中，ECB 只被用于交换少量数据，例如，启动其他 DES 模式的密钥和参数以及数据库中的单元。

2. 密码分组链接模式

在密码分组链接(CBC)模式中，未加密文本的每个分组在使用 DES 算法加密之前，都与前一密文分组进行异或操作。解密过程简单地将密文解密，并且反向执行异或操作。CBC 创建了一个 IV，并且将这个 IV 与消息的第一个分组相异或，从而每次操作都生成独特的输出。IV 必须被发送给接收方，我们既可以将 IV 以明文形式置于完整的密文之前，也可以使用与消息所用的相同的密钥通过 ECB 加密模式保护它。在使用 CBC 模式时，需要考虑的一个重要问题是错误传播，也就是如果一个分组在传输中被破坏，那么这个分组将无法解密，并且下一个分组也是如此。

3. 密码回馈模式

密码回馈(CFB)模式是流密码形式的 CBC。换句话说，CFB 针对实时生成的数据进行操作。不过，CFB 并不将消息分为若干分组，而是使用相同分组大小的内存缓冲区。在缓冲区被填满时，对数据进行加密并发送给接收方。接着，系统等待下一个缓冲区被新生成的数据填满，然后继续进行加密和传输。除了将先前存在的数据变化为实时数据，CFB 的操作方式与 CBC一样，也使用了 IV 和链接。

4. 输出回馈模式

在输出回馈(OFB)模式中，DES 的操作样式几乎与在 CFB 模式中的操作样式完全相同。不过，DES 并不将明文分组与前一个密文分组的加密版本相异或，而是将明文与某个种子值相异或。对于第一个被加密的分组来说，初始向量被用于创建种子值。通过对先前的种子值运行 DES 算法，就可以派生出之后的种子值。OFB 模式的主要优点是不存在链接功能，并且传输错误不会通过传播影响之后分组的解密。

5. 计数模式

在计数(CTR)模式中运行的 DES 使用的流密码，类似于在 CFB 和 OFB 模式中使用的流密码。不过，这种模式并不根据前一个种子值的结果为每个加密/解密操作创建种子值，而是使用一个简单的、每次操作后都增加的计数。与 OFB 模式一样，CTR 模式中也不传播错误。

提示：

CTR 模式允许将一个加密或解密操作分解为多个独立的步骤，这使得该模式特别适用于并行计算。

6.4.2　三重数据加密算法(3DES)

正如前面几节中提到的那样，面对现代密码分析技术和超级计算能力，数据加密标准的 56 位密钥被认为已不再适用。然而，DES 的修改版本三重数据加密算法(3DES)能够使用相同的算法实现更安全的加密。

3DES 具有 4 种版本。第 1 种版本只是使用三个不同的密钥(K_1、K_2 和 K_3)对明文加密三次。它被称为 DES-EEE3 模式(三个 E 表示存在三个加密操作，而数字 3 表示使用三个不同的密钥)，这种模式可以利用下面的符号来表示，其中 E(K, P)表示使用密钥 K 加密明文 P：

$$E(K_1,E(K_2,E(K_3,P)))$$

DES-EEE3 具有的密钥的有效长度为 168 位。

第 2 种 3DES 版本 DES-EDE3 也使用三个密钥，但是将第二个加密操作替换为解密操作，如下所示：

$$E(K_1,D(K_2,E(K_3,P)))$$

第 3 种 3DES 版本 DES-EEE2 只使用两个密钥 K_1 和 K_2，如下所示：

$E(K_1,E(K_2,E(K_1,P)))$

第 4 种 3DES 版本 DES-EDE2 也使用两个密钥，但是在中间使用一个解密操作，如下所示：

$E(K_1,D(K_2,E(K_1,P)))$

第 3 种和第 4 种 3DES 版本具有的密钥的有效长度都为 112 位。

注意：

从技术上讲，3DES 具有第 5 种形式 DES-EDE1，这种形式只使用一个密钥。不过，这种形式导致与标准 DES 相同的算法(和强度)，并且只是为了向后兼容而提供。

由于若干密码研究人员提出了这样的理论：一种形式比其他三种形式更安全，因此这 4 种 3DES 已经经过了多年发展。然而，目前人们相信所有模式一样安全。

提示：

请花费一些时间理解 3DES 的各种变化形式。使用纸笔进行运算，确保理解每种变化形式如何使用两个或三个密钥达到强度更高的加密效果。

注意：

这个讨论自然会引出一个问题：如果使用双重 DES(Double DES，2DES)，会有怎样的效果？在第 7 章中你会看到，人们尝试过 2DES，但是在证明存在攻击使得 2DES 并不比标准 DES 安全时，很快就放弃了这种算法。

6.4.3 国际数据加密算法(IDEA)

国际数据加密算法(IDEA)的分组密码是针对 DES 算法的密钥长度不够而开发的。与 DES一样，IDEA 对 64 位的明文/密文分组进行操作。然而，国际数据加密算法采用 128 位的密钥进行操作。这个密钥随后在一系列操作中被分解成 52 个 16 位的子密钥。这些子密钥接着使用异或和模运算的组合对输入的文本进行操作，从而生成输入消息的加密/解密版本。IDEA 能够在 DES 使用的 4 种模式(ECB、CBC、CFB 和 OFB)中工作。

警告：

所有与密钥长度、分组大小和加密轮数有关的内容可能看起来特别枯燥。但是，这些内容是非常重要的，因此一定要确信在参加考试之前复习这些内容。

IDEA 算法的专利权属于它们的瑞士开发人员。但是，开发人员向期望使用 IDEA 作为非商业用途的人授予了无限制许可。在 Phil Zimmerman 的流行的可靠隐私(Pretty Good Privacy，PGP)安全电子邮件包中，发现了 IDEA 的一种流行实现。第 7 章将对 PGP 进行更详细的介绍。

6.4.4 Blowfish

Bruce Schneier 的 Blowfish 分组密码是 DES 和 IDEA 的另一种选择。与它的这些前辈们一样，Blowfish 对 64 位文本分组进行操作。然而，Blowfish 扩展了 IDEA 的密钥强度，甚至准许使用变长密钥，范围从相对不安全的 32 位到相当难破解的 448 位。很显然，较长的密钥将导致加密/解密时

间的相应增加。不过，计时试验已经表明，Blowfish 是比 IDEA 和 DES 更快的算法。Schneier 先生没有对 Blowfish 进行许可限制，人们可以自由使用该密码。Blowfish 加密被内嵌到许多商业软件产品和操作系统中，此外还存在许多可以被软件开发人员使用的 Blowfish 库。

6.4.5　Skipjack

Skipjack 算法由美国政府在联邦信息处理标准(Federal Information Processing Standard，FIPS)185，即托管加密标准证书(Escrowed Encryption Standard，EES)中批准使用。与许多分组密码一样，Skipjack 对 64 位的文本分组进行操作。这种算法使用一个 80 位的密钥，并且支持 DES 支持的相同 4 种操作模式。美国政府很快接受了 Skipjack，并且提供支持 Clipper 和 Capstone 高速加密芯片的密码学程序，这些芯片是为重要商业应用而设计的。

然而，Skipjack 有一个额外的麻烦，即支持加密密钥的托管。美国国家标准和技术协会(NIST)和财政部这两个政府机构都持有重建 Skipjack 密钥所需的一部分信息。当法律执行机构获得合法授权后，他们将联系这两个机构获得密钥的部分信息，并且可以对参与成员之间的通信进行解密。

Skipjack和Clipper芯片还没有被密码学团体普通接受，这是因为它的托管程序由美国政府控制。

Rivest 密码 5(Rivest Cipher 5，RC5)

Rivest 密码 5 或 RC5 是 RSA 数据安全公司拥有专利的对称算法。RC5 是一种分组大小可变的(32 位、64 位或 128 位)分组密码，使用的密钥长度在 0 位到 2048 位之间。

6.4.6　高级加密标准(AES)

2000 年 10 月，美国国家标准和技术协会(NIST)宣布 Rijndael(发音为“rhine-doll”)分组密码已经被选中成为 DES 的替代标准。在同年的 12 月，美国商务部长批准了 FIPS 197，它要求使用 AES/Rijndael 对所有敏感但未被美国政府分类的数据进行加密。

AES 密码准许使用三种密钥强度：128 位、192 位和 256 位。AES 最初的规范支持 128 位分组的处理，但是 Rijndael 超出了这个规范，它准许密码学家使用与密钥长度相等的分组大小。如下所示，加密的轮数依赖于所选的密钥长度：

- 128 位密钥需要 10 轮加密。
- 192 位密钥需要 12 轮加密。
- 256 位密钥需要 14 轮加密。

Twofish 算法

由Bruce Schneier(也是Blowfish的创建者)开发的Twofish算法是AES的另一种选择。与Rijndael一样，Twofish也是一种分组密码。这种算法处理 128 位的数据分组，并且能够使用长度最大为 256 位的密钥。

Twofish 利用了其他算法所没有的两种技术：

- 预白噪声化(prewhitening)涉及在第一轮加密前将明文与一个单独的子密钥进行异或。
- 后白噪声化(postwhitening)在第 16 轮加密后进行相似的操作。

AES 只是你需要熟悉的众多对称加密算法之一。表 6.3 列出了某些常见且著名的对称加密算法

及其分组大小和密钥大小。

表 6.3 对称加密算法记忆表

算法名	分组大小(单位为位)	密钥大小(单位为位)
数据加密标准(DES)	64	56
三重 DES(3DES)	64	112 或 168
高级加密标准(AES)	128	128、192、256
Rijndael	可变	128、192、256
Twofish	128	1-256
Blowfish(通常在 SSH 中使用)	64	32-448
IDEA(在 PGP 中使用)	64	128
基于 RSA 的 Rivest 密码 5(RC5)	32、64、128	0-2040
基于 RSA 的 Rivest 密码 4(RC4)	流式	128
基于 RSA 的 Rivest 密码 2(RC2)	64	128
Skipjack	64	80

6.4.7 对称密钥管理

由于加密密钥中包含的信息对于密码系统而言是至关重要的，因此密码系统的管理员和用户必须采取特殊的措施以保护密钥材料的安全。这些安全措施被统称为密钥管理实践。它们包含密钥的生成、分发、存储、销毁、恢复和托管。

1. 创建和分发对称密码

正如前面提到的，对称加密算法内在的一个主要问题是操作算法所需密钥的安全分发。在下面的内容中，将对下列三个主要的用于安全交换密钥的方法进行分析：离线分发、公钥加密和 Diffie-Hellman 密钥交换算法。

离线分发 在技术方面最简单的方法涉及密钥材料的物理交换。一方向另一方提供包含密钥的一张纸或一份存储介质。在很多硬件加密设备中，密钥材料以电子设备的形式存在，这类似于插入到加密设备中的真实的钥匙。然而，这些方法都具有各自固有的缺陷。如果通过电子邮件发送密钥材料，那么密钥材料就可能被截获。电话可能会被窃听。包含密钥的纸张则可能被无意丢进废纸篓或丢失。

公钥加密 许多通信人员希望在没有密钥分发之争的情况下获得密钥加密的速度优势。因此，许多人使用公钥加密来建立初始的通信链接。一旦链接成功建立，并且双方对相互的身份都感到满意，那么他们就会在安全的公钥链接上交换密钥。随后，通信双方从基于公钥算法的通信进入基于秘密密钥算法的通信，并且能够享受快速的处理过程。一般而言，与公钥加密相比，私有密钥加密的速度快数千倍。

Diffie-Hellman 算法 某些情况下，无论是公钥加密还是离线分发，都是不充分的。双方可能需要相互通信，但是他们没有物理手段交换密钥材料，并且没有适当的公钥基础设施来促进秘密密钥的交换。在这样的情况下，像 Diffie-Hellman 这样的密钥交换算法被证明是极为有用的机制。

提示：

安全 RPC(S-RPC)利用 Diffie-Hellman 算法进行密钥交换。

关于 Diffie-Hellman 算法

当 Diff-Hellman 算法与 1976 年发布时，对于当时的密码学科学是一次大的进步。当然，它目前仍在使用，该算法的工作过程如下：

(1) 通信双方(我们称他们为Richard和Sue)约定两个大数p(一个质数)和g(一个整数)，其中1<g<p。

(2) Richard 选择一个随机的大整数 r，并且执行下面的计算：$R = g^r \bmod p$

(3) Sue 选择一个随机的大整数 s，并且执行下面的计算：$S = g^s \bmod p$

(4) Richard 将 R 发给 Sue，并且 Sue 将 S 发给 Richard。

(5) Richard 随后执行下面的计算：$K = S^r \bmod p$

(6) Sue 随后执行下面的计算：$K = R^s \bmod p$

此时，Richard 和 Sue 都得到相同的值 K，并且可以在双方的通信中将之用于私有密钥通信。

2. 存储和销毁对称密钥

在对称密钥加密中，另一个主要的挑战是在密码系统中使用的密钥必须进行安全保管。以下给出了存储加密密钥的最佳实践：

- 永远不要将加密密钥存储在存放加密数据的同一个系统中，这将使攻击者更容易进行攻击！
- 对于敏感的密钥，可以考虑两个不同的人分别持有密钥的一半。他们必须合在一起才能构成完整的密钥。这是众所周知的知识分割原则(已在本章前面提到)。

当知道密钥的用户离开组织或不再被允许访问通过密钥包含的材料时，密钥必须更改，同时使用该密钥进行加密的所有材料必须用新的密钥进行重新加密。销毁一个密钥并将一个用户从对称密码系统中移除是困难的，这也是组织转而使用非对称算法的一个重要原因。这部分内容将在第 7 章中进行讲述。

3. 密钥托管

密码学是一种强大的工具。与大多数工具一样，密码学可以被用于实现许多有益的目的，但是也可能被恶意使用。为了应对密码学技术的爆炸性增长，各国政府纷纷考虑实现密钥托管系统。这样的系统允许政府在有限的情况下(例如，法院判决)从中央存储设备获得特定通信所使用的密钥。

在过去 10 年中，人们提议通过下列两种主要途径进行密钥托管：

公平密码系统　在这种托管方法中，通信中使用的私有密钥被分为两个或多个部分，这些部分都被交给独立的第三方。每个部分本身都是无用的，但是通过重新组合可以获得私有密钥。政府获得法律授权访问特定的密钥时，需要向所有第三方提供法院的证据，随后才能重新组装这个私有密钥。

托管加密标准　这种托管方法向政府提供解密密文的技术手段。这个标准是本章前面讨论的 Skipjack 算法的基础。

政府管理者几乎不可能克服不可避免的法律和隐私障碍来广泛实现密钥托管。虽然技术上没有问题，但是一般民众不可能接受政府对个人生活的潜在介入。

6.4.8 密码生命周期

除了一次一密，所有的密码系统都有一个有限的生命周期。摩尔定律经常被用来描述计算能力的进步趋势，它指出微处理器的性能将每两年翻一番。这意味着，最终处理器将达到简单猜测用于通信加密密钥所需的处理能力。

安全专家在选择一个加密算法和相应的管理控制措施时必须考虑密码的生命周期以确保算法、协议和选择的密钥长度足以保存密码系统的完整性，以确保能够用于保护所需时间内信息的完整性和安全性。安全专家可以使用以下算法和协议管理控制：

- 确定组织内可以接受和使用的加密算法(例如，AES、3DES 和 RSA)。
- 基于传输信息的敏感性确定每个算法可接受使用的密钥长度。
- 列出可以使用的安全传输协议(如 SSL 和 TLS)。

举例来说，如果设计的密码系统用来保护计划下周执行的商业计划，就无须担心处理器可能从目前到今后 10 年内可以破解它们这种理论上的风险。从另一方面看，如果要保护那种可能用于建造核弹的机密信息，那就十分肯定仍需要在今后 10 年里一直维护这个机密。

6.5 本章小结

为了开发出更加安全的密码系统和战胜这些系统的高级密码分析技术，密码专家和密码分析专家始终处于一场从未结束的竞赛之中。

密码学的历史可以追溯到凯撒的年代，并且已经被持续研究了很多年。在这一章中，你学习了密码学领域的一些基本概念，对密码学专业人员使用的术语有了基本的了解，并且分析了密码学早期使用的一些编码和密码。

本章还分析了对称密钥密码学(通信双方使用相同的密钥)和非对称密钥密码学(每个通信方都有一对公钥和私钥)的相似和不同之处。

我们接下来分析了当前可提供的对称算法和他们的强度及弱点。我们通过了解密码的生命周期和算法/协议治理在企业安全中的作用结束了本章的讨论。

下一章将展开讨论当代的公钥密码算法，此外还将对一些常见的用于击败这两种类型密码系统的密码分析技术进行分析。

6.6 考试要点

理解机密性、完整性和不可否认性在密码系统中扮演的角色。机密性是密码学的一个主要目标，它确保信息不对未授权的个人泄漏，并且准许加密信息以在开放的网络中自由传输。对称和非对称密码系统都能够保证机密性。完整性为消息的接收方提供了消息在发送者建立和接收者接收到的时间范围内没有被(有意或无意)修改的保证。对称和非对称密码系统都能够保证完整性。不可否认性提供了不可否认的证据，从而证明消息的发送者确实是这个消息的作者。它防止发送者否认他们发送了原始信息。

了解如何使用密码系统达到身份认证的目标。身份认证提供了对用户身份的保证。使用身份认

证的一种可能方案是挑战/响应协议，其中的远程用户被要求使用只有通信双方知道的密钥对消息进行加密。对称和非对称的密码系统都可以实现身份认证。

熟悉密码学的基本术语。当发送者希望向接收者传送一份私有消息时，发送者会取出明文(未加密的)消息，并且使用某种算法和某个密钥对明文消息进行加密，从而生成发送给接收者的密文消息。接收者随后使用相似的算法和密钥对密文进行解密，并且重建原始的明文消息以供查看。

理解编码和密码之间的区别，并且能够解释密码的基本类型。编码是对词汇或短语操作的符号密码学系统，有时是隐秘的，但是并不能永远提供机密性。不过，密码永远意味着对消息的真实含义进行隐藏。了解下列密码类型的工作方式：换位密码、替代密码(包括一次性填充)、流密码以及分组密码。

了解成功应用一次性填充的要求。要获得成功的一次性填充，密钥必须随机生成，并且不使用任何已知的模式。密钥必须至少和被加密的消息一样长。填充必须防止物理泄露，并且每个填充在被丢弃前必须只使用一次。

理解零知识证明的概念。零知识证明是一个通信概念。正如数字签名和数字证书一样，零知识证明交换特定类型的信息，但是不传输实际的数据。

理解知识分割。分割知识意味着执行某个操作所需的知识或权限在多个用户之间分配，这样可以确保任何一个人都没有足够的权限来危害环境的安全性。“M of N 控制”是分割知识的一个示例。

理解工作函数(工作因数)。工作函数或工作因数通过度量解密消息所需的成本和/或时间，来度量密码学系统的强度。通常，针对加密系统执行完全穷举攻击所需的时间和努力就是工作函数所表示的内容。密码系统提供的安全性和保护与工作函数/因数的值成正比。

理解密钥安全性的重要性。密码学密钥为密码系统提供秘密性的必要组件。现代密码系统使用至少 128 位的密钥来提供足够的安全性。通常，人们都赞同数据加密标准(DES)56 位密钥的长度已无法提供足够的安全性。

了解对称和非对称密钥系统之间的差异。对称密钥密码系统(或密钥密码系统)依赖于一个共享密钥的使用。它们的速度远远快于非对称算法，但是缺乏对可扩展性、简单密钥分发和不可否认性的支持。非对称密码系统对双方之间的通信使用公共/私钥对，但是要比对称算法的操作速度慢得多。

能够解释数据加密标准(DES)和三重 DES(3DES)的基本操作模式。数据加密标准具有 4 种操作模式：电子代码本(ECB)模式、密码分组链接(CBC)模式、密码回馈(CFB)模式和输出回馈(OFB)模式。ECB 模式被认为是最不安全的，并且只用于短消息。3DES 使用 DES 的三次迭代，利用两或三个不同的密钥，从而将密钥的有效强度各自增加到 112 位或 168 位。

了解高级加密标准(AES)。高级加密标准使用 Rijndael 算法，并且是美国政府安全交换敏感但非分类数据的标准。AES 使用 128、192 和 256 位的密钥和固定 128 位大小的分组达到比旧的 DES 算法高得多的安全性。

6.7　书面实验室

1. 阻碍广泛采用一次性填充密码系统来确保数据机密性的主要障碍是什么？

2. 使用密钥为 SECURE 的柱状换位密码，对消息“I will pass the CISSP exam and become certified next month”进行加密。

3. 使用凯撒 ROT3 替换密码，对消息“F R Q J U D W X O D W L R Q V B R X J R W LW”进行

解密。

6.8 复习题

1. 4 位的密钥空间存在多少个密钥?

   A. 4

   B. 8

   C. 16

   D. 128

2. John 近期收到一封来自 Bill 的电子邮件。需要满足什么密码学目标，才能让 John 相信 Bill 是这封邮件的发送者?

   A. 不可否认性

   B. 机密性

   C. 可用性

   D. 完整性

3. 数据加密标准(DES)密码系统中使用的密钥长度是多少?

   A. 56 位

   B. 128 位

   C. 192 位

   D. 256 位

4. 什么类型的加密方式，依赖于不断变化消息中字符的位置去实现机密性?

   A. 流加密

   B. 换位加密

   C. 块加密

   D. 替换加密

5. 下列哪一个不是高级加密标准 Rijndael 算法可能的密钥长度?

   A. 56 位

   B. 128 位

   C. 192 位

   D. 256 位

6. 秘密密钥加密系统不能实现下列哪一项?

   A. 不可否认性

   B. 机密性

   C. 可用性

   D. 密钥分发

7. 如果配置正确，已知唯一的牢不可破的加密系统是什么?

   A. 换位密码

   B. 替代密码

   C. 高级加密标准

D. 一次性填充

8. 数学函数 16 模 3 的输出值是多少？

A. 0

B. 1

C. 3

D. 5

9. 在 20 世纪 40 年代，一队来自美国的密码破译专家成功破解了基于一次一密的被称为 VENONA 的项目。该项目破坏了什么规则，导致引起这个事件？

A. 密钥值必须随机。

B. 密钥值必须和信息一样长。

C. 密钥值必须仅能被用一次

D. 密钥值必须防止物理泄露

10. 以下密码类型中，哪一项对大块的消息而不是单个字符或位的消息进行操作？

A. 流加密

B. 凯撒加密

C. 块加密

D. ROT3 加密

11. 为了通过使用对称加密算法对双向通信进行保护，需要的加密密钥的最小数目是多少？

A. 1

B. 2

C. 3

D. 4

12. Dave 正在开发一个需要多人才能取回密钥的密钥托管系统，但并不依靠每个参与者到现场。他正在使用什么类型的技术？

A. 分割知识

B. M of N 控制

C. 工作函数

D. 零知识证明

13. 下面哪种数据加密标准(DES)操作模式能被用于大量信息，确保在加密/解密过程中不会因为一个早期的错误而破坏整个通信？

A. 密码分组链接(CBC)

B. 电子代码本(ECB)

C. 密码回馈(CFB)

D. 输出回馈(OFB)

14. 许多加密算法依赖于分解大素数乘积的难题。它们依靠的这个问题的特点是什么？

A. 包含扩散

B. 包含混淆

C. 包含单向函数

D. 遵照 Kerchoff 原则

15. 全面实现有 10 人参与的对称算法需要多少个密钥?

A. 10

B. 20

C. 45

D. 100

16. 高级加密标准使用的分块大小是多少?

A. 32 位

B. 64 位

C. 128 位

D. 可变

17. 什么样的攻击，使得凯撒密码几乎无法使用?

A. 中间人攻击

B. 托管攻击

C. 频率分析攻击

D. 换位攻击

18. 什么类型的密码系统经常利用一个通道，借助一本著名的书来加密密钥?

A. Vernam 加密

B. 轮换密钥加密

C. Skipjack 加密

D. Twofish 加密

19. 哪个入围的 AES 利用了预白噪声化和后白噪声化技术?

A. Rijndael

B. Twofish

C. Blowfish

D. Skipjack

20. 全面实现有 10 人参与的非对称算法需要多少个密钥?

A. 10

B. 20

C. 45

D. 100

第 7 章

PKI 和密码学应用

本章中覆盖的 CISSP 考试大纲包含：

安全工程学

- I. 密码学应用
  - I.2 密码学类型(例如，对称密码学、非对称密码学、椭圆曲线密码学)
  - I.3 公钥基础设施(PKI)
  - I.4 密钥管理实践
  - I.5 数字签名
  - I.6 数字版权管理
  - I.7 不可否认性
  - I.8 完整性(哈希和撒盐)
  - I.9 密码分析攻击方法(例如，暴力破解、仅知密文、已知明文)

第 6 章“密码学与对称密钥算法”中介绍了基本的密码学概念，并且探索了多种私钥密码系统。这些对称密码系统虽然提供了快速、安全的通信方式，但是也引入了在以前无关的各方之间进行密钥交换时所面临的实际挑战。

本章将探讨非对称(或公钥)密码学和公钥基础设施(PKI)领域，这个领域支持世界范围内各方之间的安全通信，并且这些通信方在通信之前不必彼此认识。非对称算法提供方便的密钥交换机制并可扩展到非常大的用户数量，而这些都是使用对称密码算法所要面临的挑战。

本章还将研究几种密码学在安全电子邮件、Web 通信、电子商务、数字版权管理和网络连接方面的实际应用情况。最后，本章介绍怀有恶意的个人可能使用的威胁较弱密码系统的多种攻击方法。

7.1 非对称密码学

在第 6 章的“现代密码学”一节中介绍了私有密钥(对称)和公钥(非对称)密码学背后的基本原则。你已经学习过对称密钥的密码系统要求通信双方都具有相同且共享的秘密密钥，从而产生了安全密钥分发的问题。你还学过为了克服这个难题，非对称密码系统使用了公钥和私钥对，从而促进在无须支出复杂密钥分发系统的开销的情况下，进行安全通信。这些系统的安全性取决于反向使用单向

函数的难度。

在下面的几节中，我们将会更详细讨论公钥密码学的概念，并介绍当今使用较多的三种公钥密码系统：RSA、El Gamal 和椭圆曲线密码系统(Elliptic Curve Cryptosystem，ECC)。

7.1.1 公钥与私钥

第 6 章曾经介绍过，公钥密码系统依赖于为每个密码系统用户分配的一对密钥。每个用户都同时维护一个公钥和一个私钥。顾名思义，对于想与公钥密码系统用户通信的任何人来说，都可以从该用户那里自由获得公钥。第三方拥有的公钥不会将任何脆弱性引入密码系统。另一方面，私钥只供专人使用，这种密钥从不与其他密码系统用户共享。

公钥密码系统用户之间的正常通信相当简单。图 7.1 说明了一般过程。

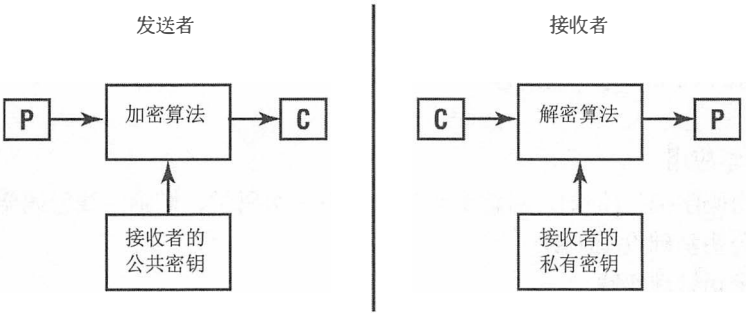


图 7.1 非对称密钥密码学

可以看到，这个过程并不需要共享私钥。发送者用接收者的公钥加密明文消息(P)，从而产生密文消息(C)。当接收者打开密文消息时，他们使用自己的私钥解密密文，重新生成最初的明文消息。

一旦发送者用接收者的公钥加密了消息，那么在不知道接收者的私钥(用于生成消息的公钥/私钥对的另一半)的情况下，没有用户(包括发送者)能够解密这些信息。这就是公钥密码学的优点，即可以使用不安全的通信通道自由共享公钥，并在以前并不认识的用户之间创建安全的通信信道。

你曾学过公钥密码学具有较高程度的计算复杂性。为了产生同等加密强度的密码系统，公钥系统中使用的密钥长度必须比私钥系统中使用的密钥长度更长。

7.1.2 RSA

最著名的公钥密码系统以其创造者命名。1977 年，Ronald Rivest、Adi Shamir 和 Leonard Adleman 提出了 RSA 公钥算法，这种算法成为今天在全世界范围仍在使用的标准。他们为这个算法申请了专利并成立了一家商业公司(RSA 安全公司)，该公司开发使用其安全技术的主流产品。今天，RSA 算法已经构成许多知名安全基础设施(例如，Microsoft、Nokia 和 Cisco 公司的相应产品)的安全构架。

RSA 算法依赖于大质数在因数分解时固有的计算难度。密码系统的每个用户都使用下列步骤描述的算法产生一对公钥和私钥：

(1) 选择两个大的质数(每个质数大约 200 位)，用 p 和 q 来表示。

(2) 计算出这两个质数的乘积，即 n = p * q。

(3) 选择一个满足下列两项要求的数字 e：

a. e 小于 n。

b. e 和(n−1)(q−1)互质，也就是说，除了 1 以外，这两个数没有共同的因数。

(4) 找到一个数 d，使得(ed − 1) mod (p − 1)(q − 1) = 0。

(5) 把 e 和 n 作为公钥分发给所有的密码系统用户，将 d 作为私钥并保持其秘密性。

如果 Alice 想把一条加密的消息发送给 Bob，那么她会使用如下所示的公式将明文(P)加密为密文(C)，其中密钥产生过程中生成的 e 是 Bob 的公钥，n 是 p 和 q 的乘积：

$$C = P^e \bmod n$$

当 Bob 收到消息时，他会运用下面这个公式得到明文消息：

$$P = C^d \bmod n$$

Merkle-Hellman 背包算法

另一种早期的非对称算法 Merkle-Hellman 背包算法在 RSA 公开一年后被开发出来。与 RSA一样，这种算法也基于执行因式分解操作的难度，但是它依赖于被称为超增序列的集合论组件，而不是依赖于大质数。在 1984 年被破解时，Merkle-Hellman 背包算法曾被证明是不安全的。

密钥长度的重要性

密码系统中密钥的长度也许是最重要的安全参数，它可以根据安全管理员的判断自由设定。了解加密算法的能力并选择能够提供适当保护程度的密钥长度是十分重要的。通过权衡击败给定密钥长度的难度(测量击败密码系统所需的处理时间)与数据的重要程度做出决定。

一般而言，数据越重要，保护数据的密钥加密强度就应该越强。数据的时间性也是重要的考虑因素。必须考虑到计算能力的迅速增长，著名的摩尔定律指出，大约每隔 18 个月计算机的计算能力就会翻一番。如果使用现在的计算机，需要花费一年的处理时间来破解代码，那么按照摩尔定律，使用三年后同时代的技术，这种尝试只需三个月时间。如果希望数据在三年后的敏感程度仍然不变，就应该选择比较长的加密密钥，从而在今后保持较好的安全性。

根据所使用密码系统的不同，各种密钥长度的加密强度有很大差异。有三种非对称密码系统的密钥长度能提供相同的保护程度，如表 7.1 所示：

表 7.1　三种非对称密码系统的密钥长度

密码系统	密钥长度
RSA	1088 位
DSA	1024 位
椭圆曲线密码系统	160 位

7.1.3　El Gamal

在第6章中，你已经学习了 Diffie-Hellman 算法如何使用大的整数和模数算法来帮助在不安全的通信信道上安全交换秘密密钥。1985年，T. El Gamal 博士发表了一篇文章，文中介绍了 Diffie-Hellman 密钥交换算法背后的数学原理如何被扩展用于支持整个密码系统中的消息加密和解密。

在发布时，El Gamal 算法优于 RSA 算法的一个主要方面是：它是公开发布的。El Gamal 博士没有申请 Diffie-Hellman 算法的扩展专利权，并且它的使用是免费的，不像商业化的已取得专利的 RSA 技术(在 2000 年，RSA 公布其算法到公共领域)。

然而，El Gamal 算法也有一个主要缺点，即用此算法加密的任何消息的长度都加倍了。当加密长信息或数据并且要在带宽较窄的通信线路上传输时，这会表现出难以克服的困难。

7.1.4 椭圆曲线密码系统(ECC)

也是在 1985 年，两位数学家 Neil Koblitz(来自华盛顿大学)和 Victor Miller(来自 IBM)独立地提出了运用椭圆曲线密码系统(ECC)理论来开发安全的密码系统。

注意：

椭圆曲线密码系统背后的数学概念是相当复杂的，并且也超出了本书的讨论范围。但是，在准备 CISSP 考试时，应当大致熟悉椭圆曲线算法及其潜在的应用情况。如果有兴趣学习椭圆曲线密码系统的数学知识，可以参考 www.certicom.com/index.php/ecc-tutorial 上的优秀指南。

使用下面这个方程式可以定义任何椭圆曲线：

$$y^2 = x^3 + ax + b$$

在这个方程式中，x、y、a 和 b 都是实数。每个椭圆曲线都有一个对应的椭圆曲线组，这个椭圆曲线组由椭圆曲线上的点和位于无穷大处的点 O 组成。在同一个椭圆曲线组中的两个点(P 和 Q)可以用椭圆曲线的加法算法加在一起。这个运算非常简单，如下所示：

$$P + Q$$

这个问题可以被扩展以涉及乘法。假设 Q 是 P 的倍数，如下所示：

$$Q = xP$$

计算机科学家和数学家相信，即使在 P 和 Q 已知的情况下，找到像 x 这样的数也是极其困难的。这个难题被称为椭圆曲线的离散对数问题，也是形成椭圆曲线密码学的基础。人们一般认为，解决这个问题比解决 RSA 密码系统依赖的质数因数分解问题和 Diffie-Hellman 与 El Gamal 应用的标准离散对数问题还要困难。前面的“密钥长度的重要性”通过具体数据阐述了这个问题，也就是 1088 位的 RSA 密钥的加密强度相当于 160 位的椭圆曲线密码系统密钥的加密强度。

7.2 散列函数

在本章的后面部分，你将了解密码系统如何通过实现数字签名来证明某条消息来自于密码系统的一位特定用户，并且保证此消息在双方传输的过程中没有被修改。在完全理解这个概念之前，我们必须先解释一下散列函数的概念。本节我们将研究散列函数的基础知识，并讨论现代数字签名算法中常用的几种散列函数。

散列函数具有一个非常简单的用途，那就是它们接收一条可能会很长的消息，然后根据消息内容生成唯一的输出值。该值通常被称为消息摘要。消息摘要可以由消息的发送者产生，并连同完整的消息一起传送给接收者，这其中有两个原因：

首先，接收者能够使用相同的散列函数对完整的消息进行重新计算，得出消息摘要。然后，接收者将计算得出的消息摘要与传送过来的消息摘要进行比较，从而确保始发者发送的消息与接收者收到的是同一条消息。如果两个消息摘要不匹配，那么就表明消息在传送的过程中因为某种原因被修改过。

其次，消息摘要可以被用于实现数字签名算法。这个概念将在本章稍后的“数字签名”部分中进行介绍。

注意：

术语“消息摘要”可以与其他多种同义词互换使用，这些同义词包括散列、散列值、散列总数、CRC、指纹、校验和、数字 ID。

大多数情况下，消息摘要为 128 位或更长。不过，某个单位值可以被用于执行奇偶校验功能，低位或单位校验值被用于提供单独的验证点。大多数情况下，消息摘要越长，完整性验证就越可靠。

按照 RSA 安全公司的标准，对密码学散列函数有下列 5 个基本要求：

- 输入值可以是任意长度。
- 输出值具有固定的长度。
- 散列函数在计算任何输入值时要相对容易。
- 散列函数是单向的(意味着在提供输出值时确定输入值是极其困难的)。单向函数及其在密码学中的用途在第 6 章中曾经介绍过。
- 散列函数是不会发生冲突的(意味着找到产生相同散列值的两条消息是极其困难的)。

接下来，我们将介绍 4 种常见的散列算法：SHA、MD2、MD4 和 MD5 。本章稍后部分还将对 HMAC 进行讨论。

提示：

散列算法有很多，CISSP 考试只涉及其中几种算法。除了 SHA、MD2、MD4、MD5 和 HMAC 之外，你还应当了解变长散列(Hash of Variable Length，HAVAL)。HAVAL 是 MD5 的修改版，这种算法使用 1024 位的分组，并且产生 128、160、192、224 和 256 位的散列值。

7.2.1　SHA

安全散列算法(SHA)及随后衍生的 SHA-1 和 SHA-2 算法是由美国国家标准和技术协会(NIST)开发的政府标准的散列函数，并在正式的政府出版物——安全散列标准(Secure Hash Standard，SHS)中进行了说明，此标准也被称为联邦信息处理标准(FIPS)180。

SHA-1 表面上可以接受任意长度的输入数据(事实上，在此算法中输入值的长度的上限大约是 2 097 152TB)，并且生成一个 160 位的消息摘要。SHA-1 算法处理 512 位的消息分组。因此，如果消息的长度不是 512 的倍数，那么 SHA 算法就会用附加的数据填充消息，直至长度达到 512 的下一个最高倍数。

近年来的密码分析攻击已证明 SHA-1 算法中存在缺陷，这导致 SHA-2 算法的出现，SHA-2 具有下列 4 种变体：

- SHA-256 处理 512 位的分组大小，生成一个 256 位的消息摘要。
- SHA-224 处理 512 位的分组大小，使用删减版本的 SHA-256 散列算法生成一个 224 位的消息摘要。
- SHA-512 处理 1024 位的分组大小，生成一个 512 位的消息摘要。
- SHA-384 处理 1024 位的分组大小，使用删减版本的 SHA-512 散列算法生成一个 384 位的消息摘要。

提示：

虽然看似没那么重要，但还是要花时间记住本章讨论的每种散列算法生成的信息摘要的大小。

密码机构通常将 SHA-2 算法视为安全的，但是这种算法在理论上存在与 SHA-1 算法相同的缺陷。在 2012 年，美国联邦政府宣布选择 Keccak 算法作为 SHA-3 标准。然而，SHA-3 标准仍是草案的形式并且一些技术细节仍然需要完成。观察家认为，一旦 NIST 定型 SHA-3，SHA-2 仍将是 NIST 安全散列标准(SHS)的一部分，直到有人证明对 SHA-2 的有效实际攻击。

7.2.2 MD2

MD2 散列算法由 Ronald Rivest(也就是 Rivest、Shamir 和 Adleman 中的同一人)于 1989 年开发，是为 8 位处理器提供的一种安全散列函数。MD2 对消息进行填充，从而使消息的长度成为 16 字节的倍数。然后，该算法会计算出一个 16 字节的校验和，并添加到消息的结尾处。最后，通过使用完整的原始消息与添加的校验和共同生成 128 位的消息摘要。

存在针对 MD2 算法的密码分析式攻击，尤其是 Nathalie Rogier 和 Pascal Chauvaud 发现，如果校验和在消息摘要计算之前没有被添加到消息中，那么就有可能发生冲突。之后，Frederic Mueller 证明 MD2 不是一种单向函数。因此，这种算法已不再使用。

7.2.3 MD4

1990 年，Rivest 增强了其信息摘要的算法，进而支持 32 位的处理器并提高了安全级别。这种高级的算法被称为 MD4。这个增强算法先对消息进行填充，确保消息的长度比 512 比特的倍数短 64 比特。例如，一条 16 比特的消息会用 432 比特的附加数据进行填充，使之达到 448 比特，这条消息的长度是比 512 比特的倍数短 64 比特。

随后，MD4 算法对 512 位的消息分组进行处理，经过三轮计算，最后的输出结果是一条 128 比特的消息摘要。

提示：

MD2、MD4 和 MD5 算法不再被承认是合适的散列函数。不过，CISSP 考试中仍然可能涉及这些算法的细节问题。

几位数学家已经公开发表了书面文档，证明 MD4 算法完整版本的缺点以及不正确实现的 MD4 版本。特别地，Hans Dobbertin 在 1996 年发表了一篇论文，概述了如何使用现代个人计算机在不到一分钟的时间内找到针对 MD4 消息摘要的冲突。因此，MD4 已经不再被认为是一种安全的散列算法，如有可能，应当尽量避免使用这种算法。

7.2.4　MD5

1991 年，Rivest 发布了其消息摘要算法的下一个版本，也就是 MD5。这个算法还是处理 512 位的消息分组，但是使用 4 轮明显不同的计算生成与 MD2 和 MD4 算法一样长度的消息摘要(128 位)。MD5 与 MD4 具有同样的填充要求，即消息长度必须比 512 位的倍数短 64 位。

MD5 实现了额外的安全特性，显著降低了消息摘要的生成速度。遗憾的是，近来的密码分析攻击已经证明 MD5 协议会产生冲突，这表明它不是一种单向函数。特别地，Aijen Lenstra 和其他一些人在 2005 年证明了使用不同的公钥能够创建两个具有相同 MD5 散列的数字证书。

表 7.2 列出了知名的散列函数及其生成散列值的长度。请记住这张表。

表 7.2　散列算法记忆表

算法名称	哈希值的长度(单位为位)
HAVAL——一种 MD5 变种	128、160、192、224 和 256
HMAC	可变
MD2	128
MD4	128
MD5	128
SHA-1	160
SHA-224	224
SHA-256	256
SHA-384	384
SHA-512	512

7.3　数字签名

一旦选择足够安全的散列算法，那么就能够使用其实现数字签名系统。数字签名基础结构具有两个明显的目标：

- 数字化的签名消息可以向接收方保证：消息确实来自己声明的发送者，并且实施了不可否认性(也就是说，排除了发送者之后声称消息是伪造的情况)。
- 数字化的签名消息可以向接收方保证：消息在发送方和接收方之间进行传输的过程中不会被改变。这种方法确保消息不会受到恶意的修改(第三方想要修改消息的含义)以及无意识的修改(由通信过程中的故障造成，如电磁干扰)。

数字签名算法的基础是本章已经介绍过的两个重要概念：公钥密码学和散列函数。

如果 Alice 想要数字化签名一条发送给 Bob 的消息，那么她会执行下列动作：

(1) Alice 使用一种足够安全的散列算法(如 SHA-512)生成原始明文消息的消息摘要。

(2) 然后，Alice 使用她的私钥只对消息摘要进行加密。加密的消息摘要便是数字签名。

(3) Alice 将签名的消息摘要添加到明文消息中。

(4) Alice 将完成添加的消息传送给 Bob。

当 Bob 接收到数字化签名的消息时，他会逆向完成如下过程：

(1) Bob 使用 Alice 的公钥解密数字签名。

(2) Bob 使用相同的散列函数，生成从 Alice 那里接收到的完整明文消息的消息摘要。

(3) 然后，Bob 将从 Alice 那里接收到的已解密的消息摘要与自己计算得到的消息摘要进行比较。如果两个消息摘要匹配，那么 Bob 就能够确认接收到的消息是由 Alice 发送的。如果这两个消息摘要不匹配，那么这条消息有可能不是 Alice 发送的，也有可能在传输过程中被修改了。

注意：

数字签名不仅仅用于消息，软件供应商经常使用数字签名技术对从互联网上下载的编码分发(例如，applet 和软件补丁)进行身份认证。

需要注意的是，数字签名过程本身并不提供任何隐私保护。数字签名只是确保满足加密目标中的完整性和不可否认性。然而，如果 Alice 想保证发送给 Bob 的消息的隐私性，那么她就要在消息生成的过程中增加额外的步骤。在将已签名的消息摘要添加到明文消息中以后，Alice 可以用 Bob 的公钥加密整条消息。当 Bob 接收到消息时，他会用自己的私钥在上述所列的步骤之前对消息进行解密。

7.3.1 HMAC

HMAC 算法实现了部分的数字签名功能，即保证了消息在传输过程中的完整性，但是不提供不可否认性。

真实场景

应当使用哪一种密钥？

如果对公钥密码学不是很熟悉，那么就会对针对各种不同的应用情况选择适当的密钥感到相当困惑。加密、解密、消息签名和签名验证都使用具有不同密钥输入值的相同算法。下面列出的一些简单规则能够帮助读者在准备 CISSP 考试时记住这些概念：

- 如果想要加密消息，那么就使用发送者的公钥。
- 如果想要解密发送给你的消息，那么就使用自己的私钥。
- 如果想要数字化签名发送给其他人的消息，那么就使用自己的私钥。
- 如果想要验证由其他人发送过来的消息中的签名，那么就使用发送者的公钥。

这 4 条规则是公钥密码学和数字签名的核心原则。只要对每一条规则都有了深刻的理解，就有了一个良好的开端。

通过使用一个共享的密钥，HMAC 可以与任何标准的消息摘要生成算法(如 SHA-2)组合在一起。因此，只有知道此密钥的通信双方能够产生或验证数字签名。如果接收方解密消息摘要，但是无法将这个消息摘要与明文消息产生的消息摘要进行成功比较，那么就说明这条消息在传输过程中被更改了。

因为HMAC依赖于一个共享的密钥，所以它无法提供任何的不可否认性功能(正如前面提到的)。然而，与下面将要介绍的数字签名标准相比，HMAC 以一种更加有效的方式进行操作，并且可能更适合于使用对称密码学的应用。简而言之，在不使用加密的消息摘要算法与基于公钥密码学的采用计算方式的昂贵数字签名算法之间，HMAC 能够起到折中的作用。

7.3.2　数字签名标准

在美国联邦信息处理标准(FIPS)186-4 中，美国国家标准和技术协会指定了联邦政府可以使用的数字签名算法，该标准也被称为数字签名标准(DSS)。这个文档指定美国联邦政府批准的所有数字签名算法都必须使用 SHA-2 散列函数。

DSS 还指定了可以被用于支持数字签名基础结构的加密算法。目前存在下面三种经过批准的标准加密算法：

- 数字签名算法(DSA)，在 FIPS 186-4 中指定。
- RSA 算法，在 ANSI X9.31 中指定。
- 椭圆曲线数字签名算法(ECDSA)，在 ANSI X9.62 中指定。

提示：

你还应当了解其他两种数字签名算法，至少要知道它们的名字：Schnorr 签名算法和 Nyberg-Rueppel 签名算法。

7.4　公钥基础设施(PKI)

公钥加密的主要优点是使原本互不认识的双方之间的通信变得容易。受信任的公钥基础设施(PKI)层次使得这一点成为可能。这种信任允许结合非对称和对称算法以及哈希和数字证书，为我们提供混合加密方式。

在下面的内容中，你将了解公钥基础设施的基本组件，以及使全球安全通信成为可能的密码学概念。你将学习数字证书的组成、证书授权的作用、生成和销毁证书的过程。

7.4.1　证书

数字证书为通信双方提供了保证，保证正在与之通信的人确实具有他们所宣称的身份。数字证书本质上是个人公钥的认可副本。当用户验证证书确实是由可信证书颁发机构(CA)发布时，他们就相信这个公钥是合法的。

数字证书包含特定的身份标识信息，并且其结构由国际标准 X.509 决定。遵循 X.509 标准的证书包含下列数据：

- 证书遵循的 X.509 版本。
- 序列号(来自证书建立者)。
- 签名算法标识符(指定证书授权机构对证书的内容进行数字签名时使用的技术)。
- 发布者姓名(发布证书的证书授权机构的身份标识)。

- 有效期(指定证书有效的日期和时间：开始的日期、时间，以及结束的日期、时间)。
- 主体的名字(包括区分实体身份的唯一名字或 DN，相应实体拥有证书中包含的公钥)。
- 主体的公钥(证书的内容：证书拥有者用于建立安全通信的实际公钥)。

当前版本的 X.509(版本 3)支持证书扩展：定制变量，这些变量包含为支持对证书或各种应用程序进行跟踪而由证书授权机构插入到证书中的数据。

注意：

如果对建设自己的 X.509 证书感兴趣或只是想探究公钥基础设施的内部工作，可以从国际电信联盟(International Telecommunications Union，ITU)购买完整的官方 X.509 标准。它是通信标准的开放系统互连(Open System Interconnection，OSI)系列的一部分，可以在 ITU 网站 www.itu.int 购买电子版。

X.509 尚未正式接受为标准，因此不同厂商的实现有所不同。然而，微软和 Mozilla 在他们的 Web 客户端和服务器之间采用 X.509 作为事实上的安全套接字层(SSL)通信标准。SSL 协议的细节部分将在本章后面的“密码学应用”中进行阐述。

7.4.2 证书授权机构

证书授权机构(CA)将公钥基础设施绑定在一起。这些中立的组织机构为数字证书提供公证服务。为了从著名的 CA 处获得数字证书，必须亲自前往其代理机构，并且出示适当的身份识别文档。下面的列表中包括一些主要的 CA：

- Symantec
- Thawte
- GeoTrust
- GlobalSign
- Comodo Limited
- Starfield Technologies
- GoDaddy
- DigiCert
- Network Solutions, LLC
- Entrust

没有办法能够阻止任何组织开展 CA 性质的业务。然而，这些由 CA 发布的证书只是相当于对发布它们的组织的信任。在接到来自第三方的数字证书时，这一点是需要考虑的重要内容。如果并不认可和信任发布证书的 CA，那么根本就不应该信任这个证书。如果配置浏览器让其信任一个 CA，它会自动信任由该 CA 颁发的所有数字证书。浏览器开发者预先设置了浏览器可信任的主要 CA，以减轻用户的负担。

注册授权机构(RA)在数字证书发布之前帮助 CA 验证用户的身份。RA 本身并不直接发布证书，但是在认证过程中扮演重要的角色，从而允许 CA 远程验证用户的身份。

真实场景

证书路径确认

在学习证书授权机构的过程中，你可能会接触到证书路径验证(Certificate Path Validation，CPV)。CPV 指的是：从原始起点或可信根源至相关服务器或客户端的证书路径中的每个证书都应当考虑是否有效与合法。如果需要验证“可信”端点之间的每个链接是否保持连通、有效和可信，那么 CPV 就十分重要。

当中间系统的证书过期或被替换时，信任链或验证路径可能受到破坏，由此就会引发上述问题。通过实施所有信任阶段的重新验证，就可以重新建立所有可信链接并证明假定的信任能够得到保证。

7.4.3　证书的生成与撤消

公钥基础设施背后的技术概念相当简单。在下面的内容中，我们将研究证书授权机构建立、确认和撤消客户证书的过程。

1. 注册

当希望获得一个数字证书时，你必须首先采用某种方式向证书授权机构证明身份，这个过程被称为注册。前一小节曾经提到过，这常常涉及携带正确的身份标识文档前往证书授权机构的代理处。一些证书授权机构提供了其他认证方法，包括使用可信团体领导人提供的信用报告数据和身份认证。

一旦证书授权机构对你的身份表示满意，你就可以向其提供你的公钥。CA 接着建立一个包含你的身份识别信息和公钥副本的 X.509 数字证书。CA 随后使用其私钥对证书进行数字化签名，并且向你提供已签名数字证书的副本。最后，你可以安全地将这个证书分发给希望与之进行安全通信的人。

2. 验证

当收到来自希望与之通信的人的数字证书时，就需要通过使用 CA 的公钥检查 CA 的数字签名来验证这个证书。接着，必须检查并确保证书并没有公布在证书撤消列表(Certificate Revocation List，CRL)中。此时，假如满足下列要求，那么就可以认定在证书中列出的公钥是可信的：

- CA 的数字签名是可信的。
- 你信任 CA。
- 证书没有被列在 CRL 中。
- 证书实际上包含你信任的数据。

最后一点很微妙，但却是极其重要的要求。在信任与某人有关的信息中的身份识别内容之前，应当确信这些内容确实包含在证书中。如果某个证书包含电子邮件地址(billjones@foo.com)，但是没有个人的名字，那么就只能够确信其中包含的公钥与这个电子邮件账户相关联。CA 不能断定 billjones@foo.com 电子邮件账户的实际身份。然而，如果证书包含名字 Bill Jones 以及地址和电话号码，那么 CA 也同样担保这些内容。

数字证书验证算法内建在许多流行的 Web 浏览器和电子邮件客户端软件中，因此不必常常涉及这个特定的过程。不过，深入理解幕后的技术细节，这对于为组织机构进行正确的安全性判断来说

是十分重要的。当购买证书时，应该选择一个被广泛信任的 CA。这样做的理由是，如果一款主流的浏览器不接纳这个 CA 或将此 CA 从信任 CA 列表中移除，这将极大限制所购买证书的使用。

3. 撤消

有时，证书授权机构会由于下列某种原因需要撤消证书：

- 证书遭到破坏(例如，证书所有者不慎丢失了私钥)。
- 证书被错误地发放(例如，CA 错误地发放了一个没有进行正确验证的证书)。
- 证书的细节发生变化(例如，主体的名字发生了变化)。
- 安全性关联发生变化(例如，担保这份证书的组织机构不再雇用主体)。

提示：

撤消请求宽限期是 CA 执行被请求的撤消证书的最长响应时间，这个时间在证书实践声明(Certificate Practive Statement，CPS)中定义。CPS 规定了发布和管理证书时 CA 的利用实践。

可以使用下列两种技术来验证证书的可靠性以及确定撤消的证书：

证书撤消列表 证书撤消列表(CRL)由不同的证书授权机构进行维护，并且包含 CA 发布的已被撤消的证书的序列号以及撤消生效的日期和时间。证书撤消列表的主要缺点是它们必须定期下载并交叉参照，这样就会在证书被撤消和通知最终用户证书撤消之间存在一段时间延迟。然而，CRL 仍然是今天检查证书状况的最常见方法。

联机证书状态协议(Online Certificate Status Protocol，OCSP) 这个协议通过提供实时证书验证方法消除了认证撤消列表所带来的固有延迟。当客户端收到一份证书时，就会向 CA 的 OCSP 服务器发送 OCSP 请求。服务器随后回应这份证书的状态(有效、无效或未知)。

7.4.4 非对称密钥的管理

在公钥基础设施内，通过遵守若干最佳方法需求来维护通信安全性是非常重要的。

首先，明智地选择加密系统。前面曾经学习过，“隐藏式安全”不是一种适当的途径。选择算法公开的加密系统，其算法必须经过行业专家的彻底检查。慎重选择使用“黑箱”途径的加密系统和维护算法的秘密性，这对于密码系统的完整性来说至关重要。

必须以适当的方式选择密钥。选择密钥长度时应当考虑安全需求与性能之间的平衡。此外，应当确认密钥真正随机。密钥内的任何模式都会增加攻击者破译加密和减弱密码系统安全性的可能性。

使用公钥加密时，一定要保证私钥的机密性！在任何情况下都不能允许其他人获知你的私钥。需要记住的是，偶尔允许某人访问私钥，会持久地危害使用该密钥加密的所有通信(无论是过去、当前还是将来)，并且准许第三方能够成功地进行假冒。

密钥在服务一段时期后应当停止使用。许多组织机构具有强制的密码轮换需求，从而防止未被发现的密钥泄露。如果没有必须遵循的正式策略，那么可以基于密钥的使用频率选择适当的密钥轮换时间间隔。如果可能的话，可以几个月更改一次密钥对。

最后，备份密钥！如果由于数据损坏、崩溃或其他情况丢失包含私钥的文件，那么无疑希望具有可用的备份。此时，既可以创建自己的备份，也可以使用维护备份的密钥托管服务。在任何情况下，都需要确保以安全的方式处理备份。毕竟，备份与主密钥文件一样重要！

7.5　密码学的应用

到目前为止，你已经学习了与密码学的基础知识、各种密码学算法的内部工作原理、使用数字证书分发身份证书的公钥基础设施的应用等有关的大量内容。现在，你应该掌握了密码学的基础知识，下面将研究解决日常通信问题的密码学技术的高级应用。

在接下来的内容中，我们将介绍用密码学来保护静态数据，例如存储在便携式设备上的数据，还有传输中的数据。使用的技术有：保护电子邮件、加密 Web 通信和网络连接。

7.5.1　便携式设备

现在，笔记本电脑、上网本、智能手机和平板电脑无处不在，它们给计算世界带来了新的风险。这些设备往往包含高度敏感的信息，如果丢失或被盗，可能会给组织及其客户、员工和分支机构造成严重伤害。基于这个原因，许多组织转向加密来保护这些设备上的数据，以防止它们被错误放置和使用。

目前流行的操作系统版本都包括磁盘加密功能，使其便于应用和管理便携式设备上的数据加密。例如，微软 Windows 包括 BitLocker 和加密文件系统(Encrypting File System，EFS)技术，Mac OS X 包含 FileVault 加密，TrueCrypt 的开源软件包允许 Linux、Windows 和 Mac 系统上的磁盘加密。

各种各样的商业工具可以提供额外的功能和管理能力。这些工具之间的主要区别在于它们是如何保护存储在内存中的密钥的，它们是否提供完整的磁盘或卷加密，以及是否将与基于硬件的可信平台模块(Trusted Platform Module，TPM)进行集成并提供附加的安全性。选择加密软件的任何努力都应该包括对这些特性的分析。

提示：

在开发便携式设备的加密策略时不要忘了智能手机。大多数主要的智能手机和平板电脑平台，都包括企业级的功能，从而支持对存储在手机上的数据进行加密。

7.5.2　电子邮件

我们前面曾经多次提到过，安全性应当考虑成本效益。对于电子邮件来说，简明就是成本效益最高的选项，不过有时密码学提供了无法避免使用的特定安全服务。因为保护安全也具有成本效益，所以加密电子邮件需要遵守下列规则：

- 如果在发送邮件时需要实现机密性，那么就加密邮件。
- 如果需要维护邮件的完整性，那么就必须对邮件进行散列运算。
- 如果需要实现身份认证和完整性，那么就应当对邮件进行数字化签名。
- 如果需要实现机密性、完整性、身份认证和不可否认性，那么就应当对邮件进行加密和数字化签名。

发送者总是需要负责确保实现正确的机制，从而保证维护邮件或传输的安全性(也就是机密性、完整性、身份认证和不可否认性)与隐私性。

密码学最急需的一种应用是电子邮件的加密和签名。直到最近，加密的电子邮件仍然需要使用复杂的、笨拙的软件，这些软件需要人工干预和复杂的密钥交换过程。最近几年，人们越来越重视安全性，这导致在主流电子邮件包中使用强的加密技术。接下来，我们将介绍目前广泛使用的一些电子邮件标准。

1. 可靠隐私

1991 年，Phil Zimmerman 的可靠隐私(PGP)安全电子邮件系统出现在计算机安全领域内。它结合了之前本章“Web 信任”概念里面的 CA 层级结构。在这个概念中，必须被一个或多个 PGP 用户信任才能开始使用该系统。随后，接受他们的关于额外用户有效性的判断，扩展开来，你要信任来自初始信任判断的多级用户的“Web”。

PGP 在广泛使用的最初遇到很多障碍。最困难的障碍是美国政府的出口法令，它将加密技术视为军需品，并且禁止向美国以外的国家出口强加密技术。幸运的是，这项限制后来被取消了，并且 PGP 可以自由地出口到大多数国家。

PGP有两个可用的版本。商业版本使用RSA进行密钥交换，使用IDEA进行加密/解密，使用MD5生成消息摘要。免费版本则使用Diffie-Hellman密钥交换、Carlisle Adams/Stafford Tavares(CAST)128位的加密/解密算法以及SHA-1散列函数。

许多商业机构也提供基于 PGP 的电子邮件服务作为基于 Web 的云端邮件服务、移动设备应用程序或 Web 邮件插件。这些服务通过可管理的邮件安全服务消除了复杂的加密证书配置和维护，并以此吸引了管理员和最终用户。这一类中的产品包括 StartMail、Mailvelope、SafeGmail 和 Hushmail。

2. S/MIME

安全多用途互联网邮件扩展(Secure Multipurpose Internet Mail Extensions，S/MIME)协议很可能成为未来电子邮件加密工作的标准。S/MIME 使用 RSA 加密算法，并且已经得到包括 RSA 安全公司在内的业界主要机构的支持。S/MIME 已经被合并到大量的商业产品中，这些产品包括：

- Microsoft Outlook 和 Outlook Web Access
- Mozilla Thunderbird
- Mac OS X Mail

S/MIME 依靠 X.509 证书交换密码系统密钥。这些证书包含的公钥被用于数字签名和较长通信会话中使用的对称密钥交换。RSA 是 S/MIME 支持的唯一一个公钥密码学协议，这个协议支持 AES 和 3DES 对称加密算法。

尽管对 S/MIME 标准有强有力的产业支撑，但技术的局限性阻碍了它的广泛应用。虽然主要的桌面邮件应用程序均支持 S/MIME 电子邮件，但主流的基于 Web 的电子邮件系统不支持它(因为需要扩展浏览器的使用)。

7.5.3 Web 应用

加密被广泛用于保护 Web 传输，其主要原因在于电子商务发展的趋势以及电子商务供应商和用户对通过 Web 安全交换财务信息(如信用卡信息)的强烈愿望。接下来，我们将会介绍两种在 Web 浏览器底部显示小锁图标的技术：安全套接字(SSL)和安全传输层(TLS)协议。

SSL 协议由 Netscape 公司开发，提供对客户机/服务器之间的网站流量进行加密的服务。安全套接字层上的超文本传输协议(HTTPS)使用 443 端口在 Web 服务器和客户端浏览器之间协商加密通信会话。虽然 SSL 最初是 Netscape 为其浏览器开发的标准，但是后来微软将其吸收并使其成为 Internet Explorer 浏览器的安全标准。SSL 协议与这些产品的集成使它成为事实上的国际标准。

SSL 依赖在浏览器与 Web 服务器之间交换数字证书以协商加密/解密参数。SSL 协议的目标是建立安全的通信通道，使整个 Web 浏览器会话保持开放。它取决于对称和非对称加密的组合。具体过程涉及以下步骤：

(1) 当用户访问一个网站时，浏览器检索 Web 服务器的证书，并从中提取服务器的公共密钥。

(2) 然后，浏览器创建一个随机的对称密钥，使用服务器的公钥来加密，然后将加密的对称密钥发送到服务器上。

(3) 随后，服务器使用自己的私钥解密对称密钥，这两个系统使用对称加密密钥来交换未来的交互信息。

这种方法允许 SSL 利用非对称加密技术的先进功能，在大多数数据交换的加密和解密中使用更快的对称算法。

1999 年，安全工程师在发布 SSL 第三版时，提出了将 TLS 作为 SSL 标准的替换。与 SSL 一样，TLS 使用 TCP 端口 443。基于 SSL 技术，TLS 包含了许多安全增强功能并最终被大多数应用所采用，替代了 SSL。早期版本的 TLS 在通信双方都不支持 TLS 时可以降级支持 SSL V3.0。然而，在 2011 年 TLS v1.2 不再支持向后兼容性。

2014 年，被称为“贵宾犬”(POODLE)的攻击表明在 TLS 的 SSL 3.0 反馈机制中存在重大缺陷。为了修复这个漏洞，很多机构完全放弃对 SSL 的支持，并且现在唯一依靠 TLS 的安全性。

提示：

尽管 TLS 已经存在了 10 多年，许多人仍将其误称为 SSL。由于这个原因，TLS 也获得了 SSL 3.1 的昵称。

隐写术和水印

隐写术(steganography)是使用密码学技术在另一条消息内嵌入秘密消息的方法。这种算法是通过修改组成图像文件的数据中最不重要的数据位进行工作的。变化非常微小，以至于对图像的浏览没有明显的影响。这种技术允许通信双方以简单的方式隐藏消息，例如在其他人毫无察觉的情况下，在 Web 页面的插图里嵌入秘密的消息。

隐写术通常在图像或 WAV 文件内嵌入秘密消息。这些文件往往很大，因此即使最认真的检查人员也难以发现秘密的消息。隐写术通常用于非法或可疑活动，例如商业间谍和儿童色情。

然而隐写术也能用于合法用途。将数字水印加入到文档中，以保护知识产权就是通过隐写术完成的。只有文件的创建者知道隐藏的信息。如果有人创建了内容的非法拷贝，水印就可以用来检测拷贝并且(如通过独特的水印文件提供给原始收件人)跟踪拷贝来源。

隐写术是一个非常简单的技术，可以使用网上公开免费的工具。图 7.2 显示了一个这样的工具——iSteg。只需要指定一个包含秘密信息的文本文件和希望用来隐藏信息的图像文件。图 7.3 显示了一张嵌入了秘密消息的图片，该消息是不可能用人眼检测到的。

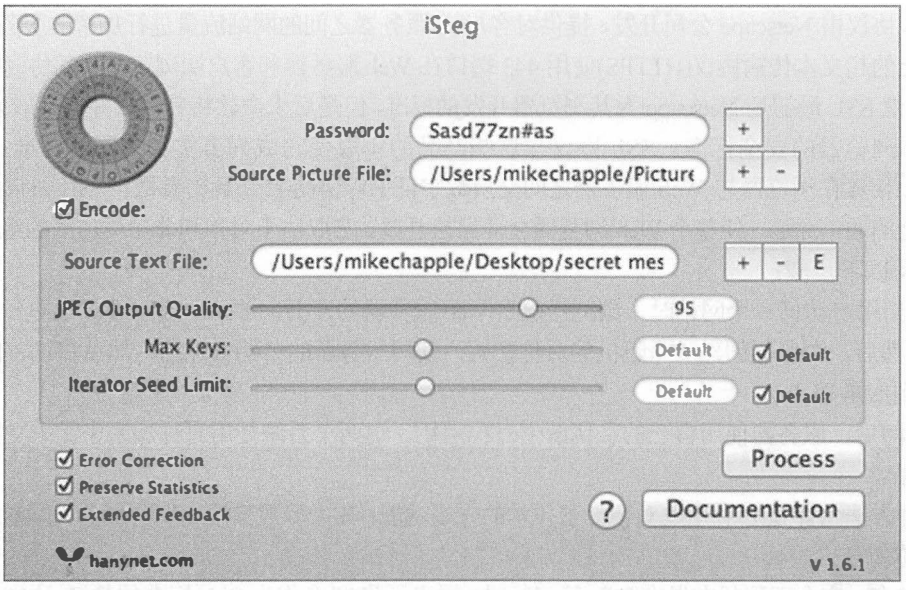


图 7.2　隐写术工具

图 7.3　嵌入了秘密消息的图像

7.5.4　数字版权管理(DRM)

数字版权管理(Digital Rights Management，DRM)软件使用加密来加强对数字媒体版权的限制。在过去 10 年中，出版商试图在各种媒体类型，包括音乐、电影和书籍中部署 DRM 方案。在许多情况下，尤其是音乐，反对者遇到 DRM 部署都会激烈反对，并认为 DRM 的使用侵犯了他们自由地享受合法授权媒体文件和制作备份的权利。

注意：

在你学习这些内容时，许多商业机构正试图部署基本上普遍失败的 DRM，因为用户拒绝该技术并把它看成一种入侵和/或阻塞。

1. 音乐 DRM

多年来音乐界一直在与盗版斗争，时间可以追溯到自制的磁带拷贝、压缩光盘和数字格式的日子。音乐发行公司试图利用各种 DRM 方案，但在消费者的压力下，大多数技术都取消了。

对于使用 DRM 技术的音乐作品销量急剧下降这种情况，苹果公司收回了他们通过 iTunes 商店出售的使用 FairPlay DRM 的音乐作品。苹果联合创始人史蒂夫·乔布斯的这一举动为后面的事情埋下了伏笔。2007 年，他发表了一封公开信，呼吁音乐公司允许苹果公司销售免费的 DRM 音乐作品。那封信的部分内容如下：

第三个选择就是完全地废弃 DRM 技术。想象一下，世界上的每个在线商店销售着开放格式编码的免费 DRM 音乐。在这样一个世界里，任何使用者能够播放从任何商店购买的音乐，任何商店都出售可以在任何播放器上播放的音乐。这显然是消费者最好的选择，苹果公司会在内心拥抱这一时代。如果 4 大唱片公司授权苹果公司他们的不受 DRM 保护的音乐作品，我们将在 iTunes 上只销售免费的 DRM 音乐。每一个 iPod 将只能播放这种免费的 DRM 音乐。

那封信的完整版在苹果公司的网站上已经看不到了，不过可以从以下网址获得完整版：http://bit.ly/1TyBm5e。

目前，DRM 在音乐中的主要应用是对于基于订阅的服务，例如 Napster 和 Kazaa，当用户订阅期结束时，用 DRM 取消用户访问和下载音乐。

注意：

对 DRM 技术的描述在这段文字中似乎看起来有点模糊？这里有一个原因：厂商通常不会透露他们 DRM 功能的细节，因为担心盗版者会利用这些信息使 DRM 方案失效。

2. 电影 DRM

电影业多年来已经使用各种 DRM 方案来解决电影盗版的全球性问题。用于保护大众传播媒体的主要技术有以下两种：

内容混乱系统(Content Scrambling System，CSS)　限制 DVD 的回放以及对使用区域的限制。这种加密方案是用一个叫作 DeCSS 的工具，在 Linux 系统中启用 CSS 来保护内容的回放。

高级内容访问系统(Advanced Access Content System，AACS)　保护存储在蓝光 HD DVD 上的媒体内容。黑客则展示获得 AACS 加密密钥的攻击并将它们张贴在互联网上。

电影制作商和黑客今天继续着猫捉老鼠的游戏；媒体公司试图保护他们的内容，而黑客企图持续访问未加密的拷贝。

3. 电子书 DRM

也许 DRM 技术最成功的应用就是图书文献的出版。当今大多数电子书使用某种形式的数字版权管理，这些技术也通过 DRM 功能来保护出版商产生的敏感文档。

提示：

今天，所有使用中的 DRM 方案都存在一个致命的缺陷：用于访问内容的设备必须获得解密密钥。如果解密密钥存储在终端用户所拥有的设备上，用户总是有机会操作该设备以获得访问密钥。

Adobe 系统通过 Adobe 的数字体验保护技术(Adobe Digital Experience Protection Technology，ADEPT)，为出售电子书提供多种格式的 DRM 技术。ADEPT 使用相结合的 AES 技术对媒体内容进行加密并用 RSA 加密受保护的 AES 密钥。许多电子书阅读器，除了亚马逊的 Kindle，都使用这项技术来保护自己的内容。亚马逊的 Kindle 电子阅读器使用多种格式的图书分发版，每个都包含自己的加密技术。

4. 视频游戏 DRM

许多视频游戏使用这样一种 DRM 技术，控制台使用一台运行的互联网云服务器来验证游戏的许可。这些技术，例如育碧的 Uplay，需要恒定的互联网连接来激活游戏。如果玩家失去了连接，游戏将停止运行。

2010 年 3 月，Uplay 系统受到拒绝服务攻击，使全球的 Uplay 游戏玩家因为之前的功能设置，使得他们的主机不能访问 Uplay 服务器，从而不能玩游戏。这导致公众的强烈抗议，随后育碧取消了持续连接的要求，将 DRM 方式更改为控制台上的游戏只需要初始激活就允许无限制使用。

5. 文档 DRM

虽然 DRM 技术最常见的用途是保护娱乐内容，但组织还是可以使用 DRM 保护存储在 PDF 文件、办公文档以及其他格式中的敏感信息的安全性。商业 DRM 产品，如 Vitrium 和 FileOpen，使用加密来保护源代码的内容，并帮助组织细致地控制文件版权。

这里是一些文档 DRM 解决方案常见的权限限制：

- 阅读文件
- 修改文件的内容
- 去除文件中的水印
- 下载/保存文件
- 打印文件
- 文件内容的截图

DRM 解决方案允许组织在需要时授予他们版权，在不再需要时进行撤消，甚至是在规定的时间到期后版权自动失效。

7.5.5 网络连接

本章我们要探讨的最后一个密码学应用是使用密码学算法提供网络连接服务。在这一节中，我们将简要介绍两种用于保护通信线路安全的方法：IPSec 和网络安全关联密钥管理协议(Internet Security Association and Key Management Protocol，ISAKMP)，此外还会讨论一些与无线网络有关的安全问题。

1. 链路加密

安全管理人员使用两种类型的加密技术来保护在网络上传输的数据的安全：

- 链路加密使用软件或硬件解决方案在两个点之间建立一条安全隧道，对进入隧道一端的所有通信数据都进行加密，并且对流出隧道另一端的所有通信数据都进行解密，从而保护整条通信线路的安全。例如，某公司通过一条数据线连接两个办公室，可以使用链路加密技术来防止攻击者在两个办公室之间的某一点进行的监控活动。
- 端到端加密用于保护双方(例如，客户端和服务器)之间的通信安全，并且可以独立于链路加密实施。在发送者和接收者之间传递使用 PGP 的邮件，就是端到端加密的例子。这种技术可以阻止入侵者监控加密链路安全端的传输数据或者通过未加密链路传送的数据。

链路加密和端到端加密技术之间的关键差异在于：在链路加密中，所有的数据(包括头、尾、地址和路由数据)也会被加密，因此每个数据包必须在每一跳(each hop)都被解密，这样数据包才能被正确地路由至下一跳，然后数据包在继续发送之前又被重新加密，这就降低了路由的速度。端到端加密技术不加密头、尾、地址和路由数据，因此数据包从一点移到另一点的速度加快了，但是这种技术更容易遭到嗅探器和偷听者的攻击。

当加密发生在 OSI 模型的较高层时，通常会使用端到端加密技术；如果加密发生在 OSI 模型的较低层，通常会使用链路加密技术。

安全外壳(SSH)是端到端加密技术的一个很好的例子。这组程序提供常见的网络应用服务(如 FTP、Telnet 和 rlogin)的加密可选方案。SSH 实际上有两个版本：SSH1(现在被认为是不安全的)支持 DES、3DES、IDEA 和 Blowfish 算法，SSH2 不支持 DES 和 IDEA，但是增加了对其他一些算法的支持。

2. IPSec

人们目前使用了多种安全体系结构，每一种都被设计用于解决不同环境中的安全问题。网络协议安全(IPSec)标准就是这样一种支持安全通信的体系结构。IPSec 是由互联网工程任务组(IETF)确立的标准体系结构，并且能够在两个实体之间建立信息交换的安全信道。

通过 IPSec 进行通信的两个实体可以是两个系统、两个路由器、两个网关或任何实体组合。尽管 IPSec 一般情况下被用于连接两个网络，但是 IPSec 也可以被用于连接单独的计算机，例如一个服务器和一个工作站，或者一对工作站(可能是发送者和接收者)。IPSec 并不规定所有的实现细节，而是一个开放的模块化架构，从而允许很多供应商、软件开发人员开发能与其他供应商的产品共同使用的 IPSec 解决方案。

IPSec 通过公钥密码学来提供加密、访问控制、不可否认性以及消息身份认证，并且一般使用 IP 协议。IPSec 主要被用于虚拟专用网(VPN)，因此可以工作在运输模式或隧道模式中。IPSec 通常与二层隧道协议(L2TP)在一起，成为 L2TP/IPSec。

IPSec 协议为安全网络通信提供了完整的基础设施。IPSec 已经得到广泛认可，并且现在许多商业性的操作系统中也提供了这个协议。IPSec 依赖于安全关联，并且存在下列两个主要组件：

- 身份验证头(Authentication Header，AH)提供消息完整性和不可否认性的保证。AH 还提供身份认证和访问控制，并且可以防止重放攻击。
- 安全封装有效载荷(Encapsulating Security Payload，ESP)提供数据包内容的机密性和完整性。ESP 还提供加密和有限的身份认证，并且可以防止重放攻击。

注意：

ESP 也提供某些有限的身份认证，但是达不到 AH 的程度。虽然 ESP 有时可以在没有 AH 的情况下使用，但是在没有 ESP 的情况下，AH 几乎不会单独使用。

IPSec 提供两种分离的操作模式。当 IPSec 在运输模式中使用时，只有数据包有效载荷被加密，这种模式为对等通信而设计。当 IPSec 在隧道模式中使用时，整个数据包(包括头)都会被加密，这个模式为网关间通信而设计。

提示：

IPSec 在现代计算机安全中是一个极其重要的概念。你一定要熟悉如上所述的组成协议以及 IPSec 操作模式。

在运行时，通过创建安全关联(Security Association，SA)来建立 IPSec 会话。SA 表示通信会话，并且记录与特定连接有关的任何配置和状态信息。SA 表示单一连接。如果期望双向信道，那么就需要两个 SA，每个方向分别使用一个 SA。此外，如果希望支持使用 AH 和 ESP 的双向信道，那么就需要建立 4 个 SA。

某些 IPSec 的最大强度就来自于能够在每个 SA 的基础上过滤或管理通信，这样一来，就可以严格管理其间存在安全关联的客户端或网关(即哪些类型的协议或服务可以使用 IPSec 连接)。此外，如果没有定义有效的安全关联，那么一对用户或网关就无法建立 IPSec 链接。

有关 IPSec 算法的详细信息，请参考第 11 章“安全网络架构与保护网络组件”中的内容。

3. ISAKMP

网络安全关联密钥管理协议(ISAKMP)通过协商、建立、修改和删除安全关联为IPSec提供后台的安全支持服务。正如你在前面一节中学到的那样，IPSec依赖于安全关联的系统。这些安全关联通过使用ISAKMP进行管理。正如在Internet RFC 2408 中阐述的一样，ISAKMP具有下列 4 个基本要求：

- 对通信对等方进行身份认证
- 建立并管理安全关联
- 提供密钥生成机制
- 防止遭受威胁(例如，重放和拒绝服务攻击)

4. 无线互联

无线网络被迅速广泛地采用，并且造成了巨大的安全风险。许多传统网络没有为本地网络主机之间的路由通信实施加密技术，并且根据假设认为：攻击者需要通过取得安全位置内网线的物理访问，从而在网络上进行偷听非常困难。然而，无线网络通过在空中传送数据，所以非常容易遭受中途数据拦截的攻击。有两个主要的无线安全类型：

有线等价隐私 安全团体最初通过引入有线等价隐私(Wired Equivalent Privacy，WEP)提供 64 和 128 位的加密选项，从而保护无线 LAN 内的通信。IEEE 802.11 中将 WEP 描述为无线网络连接标准的一个可选组件。

警告：

现在的密码分析攻击已经证明 WEP 算法中存在显著的缺陷，这可能导致在短时间内完全破坏

使用 WEP 保护的网络的安全性。一定不要使用 WEP 加密来保护无线网络。事实上，在存储网络上使用 WEP 加密会导致许多安全事件，例如 TJX 安全违规事件(在 2007 年广为人知)。再次重申，一定不要在无线网络上使用 WEP 加密。

WiFi 安全访问　通过实现临时密钥完整性协议(Temporal Key Integrity Protocol，TKIP)并消除危害 WEP 的密码学弱点，WPA(WiFi Protected Access)改进了 WEP 加密。通过将 TKIP 替换为 AES 加密算法，WPA2 进一步改善了 WPA 技术。这两种技术都是适合现代无线网络使用的安全算法。

警告：

需要记住的是，WPA 并不提供端到端的安全解决方案。WPA 只对笔记本电脑和最近的无线接入点之间的传输数据进行加密。一旦传输数据到达有线网络，数据就会被解密。

IEEE 802.1x 是另一种常用的无线安全标准，它为有线和无线网络中的身份认证和密钥管理提供了灵活的架构。为了使用 802.1x，客户端需要运行被称为 supplicant 的软件。supplicant 软件与身份认证服务器进行通信。成功进行身份认证之后，网络交换机或无线接入点就允许客户端访问无线网络。WPA 被设计为与 802.1x 身份认证服务器进行交互。

7.6　密码学攻击

与任何安全机制一样，心怀恶意的个人已经找到了许多击败密码系统的攻击方法。你要了解各种不同的密码学攻击所引起的威胁，从而使系统的风险降低到最小，这是非常重要的。

分析攻击　这是一种试图降低算法复杂性的代数运算。分析攻击关注于算法本身的逻辑性。

实现攻击　这种攻击类型利用密码学系统的实现中的弱点，关注于对软件代码的利用，不仅仅涉及错误与缺陷，而且还涉及编写加密系统程序所使用的方法。

统计攻击　统计攻击利用密码系统中的统计弱点，例如无法生成随机数和浮点错误。统计攻击试图发现驻留密码学应用程序的硬件或操作系统中的漏洞。

蛮力攻击　蛮力攻击十分简单。这种攻击尝试每种可能的、有效的密钥或密码组合。蛮力攻击涉及使用大规模的处理能力，对保护通信安全的密钥进行有系统的猜测。

针对没有缺点的协议，通过蛮力攻击发现密钥所需的平均时间与密钥的长度成正比。如果具有足够的时间，蛮力攻击总是会成功。密钥长度每增加一位，由于潜在的密钥数加倍，因此执行蛮力攻击的时间也会加倍。

有两种方法可使攻击者提升蛮力攻击的效果：

- 彩虹表提供预先计算的密码散列值，这些通常用于破解以密码散列方式存储的系统中的密码。
- 专为蛮力攻击设计和开发的专业化的、可扩展的计算硬件将大大提高这种攻击方法的效率。

加盐保存的密码

盐可能会对你的健康有害，但它可以保存你的密码！为协助打击蛮力攻击的使用，包括那些通过字典和彩虹表辅助的蛮力攻击，密码学家使用了一种称为“加密盐”的技术。

加密盐是在操作系统对密码进行哈希计算前，将随机值添加到密码的最后面。然后，将盐与其哈希值一同存储在密码文件中。当操作系统要将用户提供的密码与密码文件进行比对时，首先检索盐并将其添加到密码中。将链接的值输入到哈希函数，并将得到的哈希值与存储在密码文件中的哈希值进行比较。

要去掉额外的随机值会很麻烦，这极大地增加了蛮力攻击的难度，任何试图建立彩虹表的人都必须为每一个可能的加密盐的值建立一个单独的表。

频率分析和仅知密文攻击 在许多情况下，你唯一拥有的信息是加密后的密文信息，即所谓的仅知密文攻击。在这种情况下，频率分析就是一种已证明可行的对抗简单密码的技术。它计算每个字母出现在密文中的次数。使用你掌握的知识，字母 E、T、O、A、I 和 N 是最常见的英语字母，可以测试几个假设：

- 如果这些字母在密文中最常见，这个密码可能是移位密码，只是重新排列明文字符但不改变它们。
- 如果其他字母在密文中最常见，密码可能是某种形式的置换密码并代替明文字符。

这是对频率分析的简单概述，这个技术的众多复杂的变种可以用来对付多表密码和其他复杂的密码。

已知明文攻击 在已知明文攻击中，攻击者具有已加密消息的副本以及用于产生密文(副本)的明文消息。知道了这些消息，可以极大地帮助攻击者破解较弱的编码。例如，如果拥有同一条消息的明文和密文副本，那么破解第 6 章中介绍的凯撒密码就是一件很容易的事。

选定密文攻击 在选定密文攻击中，攻击者能够解密所选的部分密文消息，并且可以使用已解密的那部分消息来发现密钥。

选定明文攻击 在选定明文攻击中，攻击者能够加密所选的明文消息，随后可以分析加密算法输出的密文。

中间相遇攻击 攻击者可以使用中间相遇攻击击败使用两轮加密的加密算法。这种攻击导致双重 DES(2DES)很快被抛弃，并且转而使用三重 DES(3DES)这种增强的 DES 加密技术。

在中间相遇攻击中，攻击者使用已知的明文消息。然后，使用每一种可能的密钥(k1)加密明文，同时使用所有可能的密钥(k2)解密相当的密文。当发现存在匹配时，相应的密钥对(kl, k2)就代表了双重加密的两个部分。这种类型的攻击通常只需花费破解一轮加密算法(或 2_n，而不是预计的 2n* 2n)所需时间的两倍，一轮加密算法提供了最小强度的附加保护措施。

中间人攻击 在中间人攻击中，怀有恶意的人置身于通信双方之间的位置并截获所有的通信(包括密码学会话的设置)。攻击者对始发者的初始化请求做出响应，并且建立与始发者的安全会话。然后，攻击者伪装成始发者，使用不同的密钥与预期的接收者建立另一个安全会话。这样一来，攻击者就能够“坐在”通信双方的中间，读取流经的所有数据流。

提示：

注意不要混淆中间相遇攻击和中间人攻击。它们具有相似的名字，但是存在很大差异！

生日攻击 生日攻击也被称为冲突攻击或逆向散列匹配，它能够寻找散列函数一一对应特性中的缺陷，请参阅第 14 章“控制和监控访问”中对穷举攻击和字典攻击的讨论。在这种攻击中，怀有恶意的人在数字化签名的通信中寻找可以生成相同消息摘要的不同消息，从而维持原有数字签名的有效性。

提示：

别忘了，社会工程学也可以用于密码分析。如果能够获得解密密钥且只是简单地要求发送者发送密钥，就比试图破解密码系统容易得多！

重放攻击　重放攻击被用于对付那些没有结合临时保护措施的加密算法。在这种攻击中，怀有恶意的人拦截通信双方之间的加密消息(通常是身份认证的请求)，然后“重放”捕获的信息以打开新的会话。通过在每条消息中结合时间标记和过期时间，就可以防御这种攻击。

7.7　本章小结

公钥加密技术提供了一种极其灵活的基础设施，从而帮助通信之前不必彼此认识的通信双方进行简单、安全的通信。公钥加密技术还为消息的数字签名提供了架构，以便确保不可否认性和消息的完整性。

本章探讨了公钥加密技术，为大规模用户的使用提供了扩展的密码学架构。我们还讲述了一些流行的密码学算法，如链路加密技术和端到端加密技术。最后，我们介绍了公钥基础设施，这个基础设施使用证书授权机构(CA)生成包含系统用户的公钥和数字签名的数字证书(依赖于公钥密码学与散列函数的结合)。

我们还讨论了一些常见的解决日常问题的密码学技术。你学习了如何使用密码技术来保护电子邮件(使用 PGP 和 S/MIME)、Web 通信(使用 SSL 和 TLS)、对等的和网关间的网络连接(使用 IPSec 和 ISAKMP)以及无线通信(使用 WPA 和 WAP2)。

最后，我们介绍了怀有恶意的人试图阻碍或截获双方之间通信的一些常用攻击方法。这些攻击包括：密码分析攻击、重放攻击、穷举攻击(又称蛮力攻击)、已知明文攻击、选定明文攻击、选定密文攻击、中间相遇攻击、中间人攻击和生日攻击。为了提供足够的对付这些攻击的安全性，理解这些攻击十分重要。

7.8　考试要点

理解在非对称密码系统中使用的密钥类型。公钥在通信参与者之间是自由共享的，而私钥是要求保密的。为了加密消息，应当使用接收方的公钥。为了解密消息，应当使用自己的私钥。为了签名信息，也应当使用自己的私钥。为了验证签名，应当使用发送者的公钥。

熟悉三种主要的公钥密码系统。1977 年，由 Rivest、Shamir 和 Adleman 开发的 RSA 是最著名的公钥密码系统，依赖于对质数乘积进行因数分解的难度。El Gamal 是 Diffie-Hellman 密钥交换算法的扩展，依赖于模运算。椭圆曲线加密算法依赖于椭圆曲线离散对数问题，在密钥的长度相同时，能提供比其他算法更高的安全性。

知道散列函数的基本要求。优秀的散列函数具有 5 个要求：它们必须允许任意长度的输入值，提供固定长度的输出值，使得计算任意输入值的散列函数相对简单，提供单向功能并且是无冲突的。

熟悉 4 种主要的散列算法。安全散列算法(SHA)的后继算法 SHA-1 和 SHA-2 构成了政府标准的消息摘要函数。SHA-1 生成 160 位的消息摘要，SHA-2 支持最大 512 位的可变长度的消息摘要，SHA-3 还在开发制定中，而 NIST 稍晚些将发布最终版本。

知道密码加盐如何提高密码散列的安全性。当直接使用在密码文件中散列存储的密码时，攻击者可能利用预先计算值的彩虹表来识别常用的密码。在散列之前将盐添加到密码中，降低了彩虹表攻击的有效性。

理解如何产生和验证数字签名。为了数字化签名消息，首先要使用散列函数生成消息摘要。然后，用自己的私钥加密消息摘要。为了验证消息中的数字签名，需要使用发送者的公钥解密签名，随后将解密得到的消息摘要与自己产生的消息摘要进行比较。如果二者匹配，那就说明接收的消息是可信的。

了解数字签名标准(DSS)的组件。数字签名标准使用 SHA-1 和 SHA-2 消息摘要函数和下列三种加密算法中的一种：数字签名算法(DSA)、RSA 算法或椭圆曲线数字签名算法(ECDSA)。

理解公钥基础设施(PKI)。在公钥基础设施中，证书授权机构(CA)生成包含系统用户的公钥的数字证书。然后，用户把这些证书分发给希望进行通信的人。证书接收方会使用 CA 的公钥来验证证书。

了解常见的保护电子邮件安全的密码学应用。用于被加密消息的新兴标准是 S/MIME 协议。其他流行的电子邮件安全协议包括 Phil Zimmerman 的可靠隐私(PGP)。电子邮件加密的大多数用户依赖于将这项技术构建到他们的电子邮件客户端或他们的基于 Web 的电子邮件服务。

了解常见的保护 Web 活动安全的密码学应用。安全 Web 通信的事实标准是使用安全传输层协议(TLS)或旧的安全套接字层(SSL)上的 HTTP。大多数的网络浏览器都支持这两种标准。

了解常见的保护网络连接安全的密码学应用。IPSec 协议标准提供了加密网络通信的通用架构，并且被内建在许多常见的操作系统中。IPSec 的运输模式针对对等通信方式加密数据包的内容，隧道模式则针对网关间的通信方式加密整个数据包(包括头信息)。

能够描述 IPsec。IPSec 是一种在 IP 上支持安全通信的安全体系架构。IPSec 采用运输模式或隧道模式建立安全的信道。它既可以被用于在计算机之间建立直接的通信，也可以被用于在网络之间建立 VPN。IPSec 使用两个协议：身份验证头(AH)和封装安全有效载荷(ESP)。

解释常见的密码学攻击类型。穷举攻击(又称蛮力攻击)试图通过随机的组合找到正确的加密密钥。已知明文攻击、选定密文攻击和选定明文攻击都要求攻击者具有除了密文以外的其他一些信息。中间相遇攻击利用了使用两轮加密的协议。中间人攻击是欺骗通信双方与攻击者进行通信，而不是通信双方彼此之间直接通信。生日攻击尝试找到散列函数中的冲突。重放攻击则企图重用身份认证请求。

了解数字版权管理(DRM)的用途。数字版权管理(DRM)解决方案允许内容所有者执行对内容的使用限制。DRM解决方案通常保护娱乐内容，如音乐、电影和电子书，但偶尔也可见于企业中，用于保护文档中存储的敏感信息。

7.9 书面实验室

1. 如果 Bob 希望使用非对称密码向 Alice 发送机密消息，那么应当采用怎样的过程？
2. 在第一个问题所描述的情况下，Alice 应当采用怎样的过程来解密 Bob 发送的消息？
3. 阐述 Bob 对发送给 Alice 的消息进行数字化签名的过程。
4. 针对第三个问题所描述的情况，阐述 Alice 对 Bob 所发送消息中的数字签名进行验证的过程。

7.10　复习题

1. 在 RSA 公钥密码系统中，下列哪个数字总是最大？
   A. e
   B. n
   C. p
   D. q
2. El Gamal 密码体系的基础是什么加密算法形式？
   A. RSA
   B. Diffie-Hellman
   C. 3DES
   D. IDEA
3. 如果 Richard 要发送一条用公钥密码系统加密过的消息给 Sue，他用哪个密钥加密这条消息？
   A. Richard 的公钥
   B. Richard 的私钥
   C. Sue 的公钥
   D. Sue 的私钥
4. 如果用 El Gamal 公钥密码系统加密一条 2048 位的明文消息，产生的密文信息有多长？
   A. 1024 位
   B. 2048 位
   C. 4096 位
   D. 8192 位
5. Acme Widgets 目前在全公司范围内使用 1024 位的 RSA 加密标准。该公司计划从 RSA 转换成椭圆曲线加密系统。如果要保持相同的加密强度，应该使用多长的 ECC 密钥？
   A. 160 位
   B. 512 位
   C. 1024 位
   D. 2048 位
6. John 想要产生 2048 位的消息摘要，并计划发送给 Mary。如果他使用 SHA-1 散列算法，这条特定消息的消息摘要的长度是多少？
   A. 160 位
   B. 512 位
   C. 1024 位
   D. 2048 位
7. 下列哪个技术被认为是有缺陷的并且不应该再被使用？
   A. SHA-2
   B. PGP
   C. WEP
   D. TLS

8. WPA 使用什么加密技术保护无线通信?

A. TKIP

B. DES

C. 3DES

D. AES

9. Richard 收到 Sue 发送给他的加密消息。他应该用什么密钥来解密消息?

A. Richard 的公钥

B. Richard 的私钥

C. Sue 的公钥

D. Sue 的私钥

10. Richard 想要对正在发送给 Sue 的消息进行数字签名,以便于 Sue 能够确认这条消息来自于他,没有在传输过程中被篡改。他应该使用什么密钥来加密这条摘要消息?

A. Richard 的公钥

B. Richard 的私钥

C. Sue 的公钥

D. Sue 的私钥

11. 下列哪个算法不受数字签名标准支持?

A. 数字签名算法

B. RSA

C. El Gamal DSA

D. Elliptic Curve DSA

12. 哪个国际电信联盟(ITU)标准用于管理安全电子通信中的数字证书的创建和支持?

A. X.500

B. X.509

C. X.900

D. X.905

13. 什么密码系统为商业版的 Phil Zimmerman 的 PGP(可靠隐私)安全邮件系统提供加密/解密技术?

A. ROT13

B. IDEA

C. ECC

D. El Gamal

14. 什么 TCP/IP 通信端口被 TLS 通信所使用?

A. 80

B. 220

C. 443

D. 559

15. 什么类型的密码攻击提出了双重 DES(2DES)不比标准的 DES 加密有效?

A. 生日攻击

B. 选定明文攻击

C. 中间相遇攻击
D. 中间人攻击

16. 以下哪些工具可以用来提高暴力破解攻击的有效性？
A. 彩虹表
B. 分级审查
C. TKIP
D. 随机增强

17. 以下哪个链接会被 WPA 加密进行保护？
A. 防火墙到防火墙
B. 路由器到防火墙
C. 客户端到无线接入点
D. 无线接入点到路由器

18. 使用证书撤销列表的主要缺点是什么？
A. 密钥管理
B. 延迟
C. 记录保留
D. 暴力攻击的漏洞

19. 下列加密算法中的哪一个现在被认为是不安全的？
A. El Gamal
B. RSA
C. Skipjack
D. Merkle-Hellman Knapsack

20. IPSec 定义了什么？
A. 针对特定配置的所有可能的安全分类
B. 一个用于建立安全通信通道的框架
C. Biba 模型中的有效过渡状态
D. TCSEC 安全类别

第 8 章

安全模型的原则、设计和功能

本章中覆盖的 CISSP 考试大纲包含：

3) 安全工程(安全的工程学和管理)

- A. 使用安全设计原则实施和管理工程过程
- B. 理解安全模型的基本概念(例如，机密性、完整性和多级模型)
- C. 根据系统安全评价模型选择控制与对策
- D. 理解信息系统的安全保障能力(例如，内存保护、虚拟化、信任平台模型、接口、故障容错)

理解安全解决方案后面隐含的基本原则，通常有助于缩小搜寻满足特定情况下、特定安全需求的最佳控制方法的范围。在本章中，我们将讨论安全模型，包括状态机、Bell-LaPadula、Biba、Clark-Wilson、Take-Grant 以及 Brewer 和 Nash 模型。本章还将讨论政府和公司用于从安全性角度评估信息系统的通用准则和其他方法，并且着重讲述美国国防部和国际性的安全评估标准。最后，我们会讨论导致信息系统易受攻击的常见设计缺陷和其他安全相关问题。

决定如何保护系统安全的过程是十分困难且非常耗时的。在这一章中，我们将会描述这个过程，以及这个过程涉及的用于评估计算机系统的安全级别。我们将首先介绍和解释用于描述信息系统安全性的基本概念和术语，并且对安全计算、安全边界、安全性和访问监控器以及内核代码进行讨论。随后，我们将通过安全模型来阐述如何实现访问和安全控制。我们还会简要介绍如何对系统安全进行分类(例如，开放式或封闭式)，描述一组用于确保数据机密性、完整性和可用性的标准安全技术；讨论安全控制以及介绍一套标准的安全网络连接协议组。

这个领域的额外内容分布于不同的章节：第 6 章“密码学与对称加密算法”、第 7 章“PKI 和密码学应用”、第 9 章“安全脆弱性、威胁和对策”以及第 10 章“物理安全需求”。确保回顾了所有这些章，并对这个领域内的所有主题都有完整的认识。

8.1 使用安全设计原则实施和管理工程过程

在每一个系统的开发阶段都应该考虑安全，程序员应该努力为他们开发的每一个应用程序建立

安全，提供更高层次的安全性给关键应用程序和那些处理敏感信息的应用程序。在开发项目的早期阶段考虑安全是非常重要的，因为它比将安全添加到现有系统中更容易实现。下面将讨论的一些基本安全原则被应用在实施和管理硬件或软件项目工程的早期过程中。

8.1.1 客体和主体

对安全系统中任何资源的访问控制涉及两个实体。主体是请求访问资源的用户或进程。访问的意思是可以对资源进行读或写操作。客体是用户或进程想要访问的资源。需要记住的是，主体和客体针对特定的访问请求，因此对于不同的同一资源既可以成为主体，也可以在不同的访问请求中成为客体。

例如，进程 A 可能向进程 B 请求数据，为了满足进程 A 的请求，进程 B 必须向进程 C 请求数据。在这个例子中，进程 B 不仅是第一个请求的客体，而且也是第二个请求的主体，如下所示：

第一个请求 进程 A (主体) 进程 B (客体)

第二个请求 进程 B (主体) 进程 C (客体)

这也是信任传递的一个例子。信任传递的概念是：如果 A 信任 B 并且 B 信任 C，然后 A 通过传递性继承信任 C。就像数学方程：如果 A = B，B = C，那么 A = C。在前面的例子中，当 A 请求的数据从 B 而来，然后 B 从 C 请求数据，A 接收的数据本质上是从 C 而来的。信任传递存在严重的安全问题，因为可能绕过 A 和 C 之间的约束或限制，特别是如果 A 和 C 都支持和 B 进行交互的话。例如，组织可能需要禁用对 FaceBook 或 YouTube 的访问来提升雇员的生产力。虽然雇员(A)不能访问既定的某些互联网网站(C)。然而，如果雇员能够访问 Web 代理、VPN 或匿名服务，就可以将之作为一种手段来绕过本地网络限制。换句话说，雇员(A)访问 VPN 服务(B)，然后通过 VPN 服务(B)，可以访问屏蔽的互联网服务(C)；因此 A 可以通过 B，利用信任传递漏洞访问 C。

8.1.2 封闭式系统和开放式系统

可以根据下列两种不同的理念来设计和构建系统：封闭式系统被设计用于与较小范围内的其他系统协同工作，通常所有系统都来自相同的制造厂商。封闭式系统的标准一般是专有的，通常不对外公开。另一方面，开放式系统被设计为使用统一的行业标准。这些开放式系统比较容易与来自不同制造厂商但支持相同标准的系统集成在一起。

封闭式系统很难与不同的系统集成在一起，但是它们更为安全。封闭式系统通常由专用硬件和软件组成，这些软硬件是不符合行业标准的。缺乏容易集成的特点，意味着针对许多普通系统组件的攻击可能不起作用，或者这些攻击需要经过定制才能成功。许多情况中，攻击封闭式系统比攻击开放式系统更难。许多具有已知脆弱性的软件和硬件组件在封闭式系统中可能不存在。除了封闭式系统不存在已知的易受攻击的组件之外，要想发动一次成功的攻击往往需要对具体目标系统进行比较深入的了解。

一般来说，一个开放式系统与其他开放式系统相集成较为容易。例如，使用 Microsoft Windows Server 的计算机、使用 Linux 的计算机和使用 Macintosh 的计算机之间很容易建立 LAN。虽然这三种计算机使用不同的操作系统，而且至少代表着三种不同的硬件体系结构，但是它们都支持行业标准，并使得网络通信(或其他通信)变得容易。不过，这种便利的特性总是伴随着很高的代价。因为标准的通信组件被并入上述三种开放式系统，所以存在许多发动攻击的入口点和方法。通常，这种

系统的开放性使它们更容易受到攻击，并且广泛的可用性使攻击者能够查找(甚至实践)大量的潜在目标。此外，开放式系统比封闭式系统的使用程度更为普及，也更容易引起攻击者的关注。研究基本破坏技术的攻击者在开放式系统中查找到的目标比在封闭式系统中查找到的目标要多。潜在目标的更大“市场”往往意味着对开放式系统应给予更多的关注。不可否认的是，攻击开放式系统的共享知识和经验远远超过攻击封闭式系统的相关知识和经验。

开源与闭源

记住开源和闭源系统之间的区别是有用的。开源解决方案是指源代码和其他内部逻辑对公众开放。闭源解决方案是指源代码和其他内部逻辑对公众是隐藏的。开源解决方案往往依赖于公众的检查和审计，并随着时间的推移改进产品。闭源解决方案更依赖于供应商/程序员，并随着时间的推移改进产品。开源和闭源解决方案都可供出售或不收费，但长期的商用通常意味着闭源。然而，闭源代码往往是通过厂商被迫地或通过反编译进行披露。前者通常是对道德和法律的违背，而后者是道德逆向工程或系统分析的标准元素。

也有这样的情况，闭源程序既可是开放式系统，也可以是封闭式系统；对于开源程序也同样如此。

8.1.3　用于确保机密性、完整性和可用性的技术

为了保证数据的机密性、完整性和可用性，必须确保对数据进行访问的所有组件都是安全的和工作状态良好的。软件设计人员使用不同的技术来确保所设计的程序只完成要求它做的事情，而不会多做其他事情。假如某个程序对正在被另一个程序使用的内存区域进行数据读写操作，那么第一个程序实际上违反了全部的三个安全宗旨：机密性、完整性以及可用性。如果受影响的程序正在处理敏感的或秘密的数据，那么数据的机密性将不再得到保证。如果数据通过不可预测的方式被重写或更改(多个读取者和写入者不经意间访问同一共享数据时出现的常见问题)，那么就不能保证完整性。此外，如果数据的更改导致数据损坏或完全丢失，那么数据在今后也变得不可用。虽然接下来要讨论的概念全部与软件程序有关，但这些概念也都适用于所有的安全领域。例如，物理限制措施能够保证对硬件的所有物理访问都是受控的。

1. 限制

软件设计人员使用进程限制来约束程序的操作。简单来讲，进程限制允许进程只能在确定的内存地址和资源中读取和写入数据。这就是常说的沙箱。操作系统或其他一些安全组件不允许非法的读/写请求。如果进程试图执行的动作超出了为其授予的权限，那么动作会被拒绝，并且系统将采取进一步的行动，例如记录违法行为的日志。必须符合更高安全性评级的系统通常记录所有违规行为以及通过某些具体方式做出的响应。一般情况下，违规的进程会被终止。限制可以在操作系统中进行(如通过进程隔离和保护)，也可通过限制应用程序或服务(例如，www.sandboxie.com 的 Sandboxie)的使用来进行，或通过虚拟化或虚拟机(如 VMware 或 Oracle 的 VirtualBox)解决方案来进行。

2. 界限

在系统上运行的每一个进程都被分配了一个授权级别。授权级别告知操作系统进程可以执行哪些操作。在比较简单的系统中，可能只存在两个授权级别：用户和内核。授权级别告知操作系统该

如何为进程设定界限。进程的界限由对进程可以访问的内存和资源所设置的限制组成。进程在界限所划定的区域之内。在大多数系统中，这些界限为每个进程划分其使用的内存逻辑区域。操作系统负责实施这些逻辑界限并且不准许其他进程访问。更安全的系统要求从物理上限制进程。物理界限要求每个被限制的进程所运行的内存区域与其他受限进程的内存区域，通过物理方式隔开而不仅仅使用相同内存空间中的逻辑界限。对内存实施物理界限可能非常昂贵，但是也比逻辑界限更为安全。

3. 隔离

当通过实施访问界限对进程进行限制时，进程就运行在隔离状态中。进程隔离能够确保任何行为只影响与隔离进程有关的内存和资源。隔离用来保护操作环境、操作系统的内核和其他独立的应用程序。隔离是稳定操作系统的重要组成部分之一。隔离能防止某个应用程序访问只属于另一个应用程序的内存或资源，无论是好意的还是恶意的。操作系统可以提供中间服务，如剪切、粘贴和资源共享(如键盘、网络接口和存储设备访问)。

上述三个概念(限制、界限和隔离)使安全程序和操作系统的设计工作变得更为困难，但能使实现更安全的系统成为可能。

8.1.4 控制

为了确保系统的安全性，必须只有经过授权的主体才允许访问客体。控制使用访问规则来限制主体对客体的访问。访问规则声明了每个主体相对应的合法客体。进一步说，客体对某一种访问类型来说可能是合法的，但是对另一种访问类型来说可能是非法的。针对文件的访问是一种常见的控制。为了保护文件不被修改，可以将文件设置为对大多数用户来说是只读文件，而对很少一些具有文件修改权限的用户来说是可读写文件。

有两种控制：强制访问控制和自主访问控制，分别被称为 MAC(Mandatory Access Control)和 DAC(Discretionary Access Control)。在强制访问控制中，主体和客体的静态特性被用于确定访问的容许性。每个主体所具有的特性，定义了其访问资源的许可或授权。每个客体所具有的特性，定义了其分类。不同类型的安全方法以不同的方式为资源分类。例如，如果安全系统能够找出允许主体 A 所在许可级别的主体访问客体 B 所在分类级别的客体的规则，那么主体 A 就被允许访问客体 B。这被称为规则型访问控制(Rule-Based Access Control，RBAC)。预定义的规则中说明了哪种主体能够访问哪种客体。

自主访问控制与强制访问控制的不同之处在于：主体具有一些定义访问客体的能力。在受到限制的情况下，自主访问控制允许主体根据需要定义访问客体的列表。这个访问控制列表作为动态的访问规则组，并且主体能够对其进行修改。更改已实施的限制，通常与主体的身份有关。根据主体的身份，可以允许主体增加或修改访问客体的规则。

强制访问控制和自主访问控制都限制主体对客体的访问。访问控制的主要目的是：通过阻止授权或未经授权主体的未授权访问，从而确保数据的机密性和完整性。

8.1.5 信任与保证

为了生成可靠的安全产品，在体系化设计和开发之前及期间，必须集成适当的安全原则、控制和机制。安全问题不应当在事后才加以考虑，否则就会导致失察、成本增加以及可靠性降低。安全

性一旦被集成到设计中，就必须被计划、实现、测试、审计、评估、认证和最后认可。

可信系统是所有保护机制都协同工作的系统，从而能够在维护稳定和安全的计算环境的同时，为许多类型的用户处理敏感数据。保证被简单地定义为：满足安全需求的可信度。保证必须被持续地维持、更新和重新验证。无论可信系统经历已知的变化还是经过大量时间，这一点都是正确的。在任何一种情况下，变化都在某个级别上发生。变化往往是安全的对立面，并且常常降低安全性。因此，无论何时发生变化，都需要对系统重新进行评估，以便验证先前提供的安全级别是否仍然未受破坏。保证对于不同系统是不同的，并且必须针对单独系统分别建立。不过，某些保证等级或级别可以适用于许多类型相同的系统、支持相同服务的系统或部署在相同地理位置的系统。因此，信任可以通过具体的安全功能集成到系统中，而保证是在现实世界中对安全功能的可靠性和可用性的评估。

8.2　理解安全模型的基本概念

在信息安全中，模型提供了一种正式的安全策略的方式。这样的模型可以是抽象的或直观的(某些无疑是数学的)，但是都试图提供一组显式的规则，计算机能够遵循这组规则实现组成安全策略的基本安全概念、过程和措施。这些模型有助于理解如何设计和开发支持特定安全策略的计算机操作系统。

安全模型允许设计人员将抽象语句映射为描述构建硬件和软件所需算法和数据结构的安全策略。因此，安全模型使软件设计人员能够衡量自己的设计和实现。当然，这种模型必须支持安全策略的每个部分。通过这种方式，开发人员就能确认自己的安全实现可以支持安全策略。

安全令牌、功能列表和标签

若干不同的方法被用于为客体描述必要的安全特性。安全令牌是一个与资源关联的独立客体，并且描述了其安全特性。在请求访问实际的客体之前，这个令牌可以将某个客体的相关安全信息传递给实际的客体。在其他实现中，各种列表被用于存储与多个客体有关的安全信息。功能列表为每个受控客体维护一行安全特性。尽管不像令牌方式那样灵活，但是功能列表在主体请求访问客体时通常能够提供更快速的查找功能。第三种常见的特性存储器被称为安全标签(security label)，安全标签通常是客体附加的永久部分。一旦设置了安全标签，就往往不能被更改。这种永久性提供了令牌和功能列表都未提供的另一种防止篡改的防护措施。

如下所示，必须学习若干安全模型；所有这些模型都阐明了如何在计算机体系结构和操作系统设计中加入安全性：

- 可信计算模型
- 状态机模型
- 信息流模型
- 非干扰模型
- Take-Grant 模型
- 访问控制表
- Bell-LaPadula 模型
- Biba 模型

- Clark-Wilson 模型
- Brewer and Nash 模型(也被称为 Chinese Wall 模型)
- Goguen-Messguer 模型
- Sutherland 模型
- Graham-Denning 模型

尽管没有任何系统是绝对安全的，但是可以适当地设计和构建安全的系统。事实上，如果某个安全的系统遵循特定的安全标准组，那么就可以说这个系统具备某种信任级别。因此，信任可以被构建在系统内，随后能够被评估、认证和认可。但是在讨论每种安全模型之前，必须建立构建大多数安全模型的基础。这个基础就是 TCB(Trusted Computing Base，可信计算基础)。

8.2.1 可信计算基

橘皮书是美国国防部较早的一个标准(DoD Standard 5200.28，本章后面的“彩虹系列”部分会进行更详细的介绍)的俗称，这个标准将可信计算基(TCB)描述为硬件、软件和控制方法的组合，这个组合形成了实施安全策略的可信任基准。TCB 是完整信息系统的一个子集，并且应当尽可能小，从而使详细的分析能够确保系统满足设计规范和要求。TCB 是系统可以信任的遵守和实施安全策略的唯一部分。系统的每个组件并不需要都是可信任的。不过，从安全性的角度考虑系统时，评估中应该包括定义系统 TCB 的所有可信组件。

通常，某个系统中的 TCB 组件负责控制对系统的访问。TCB 必须提供访问 TCB 本身内部和外部资源的方法。TCB 组件通常对 TCB 外部的组件的活动加以限制。TCB 组件的职责就是确保系统的行为在所有的情况下工作正常并遵守安全策略。

1. 安全边界

系统的安全边界是一条假想的界限，它将 TCB 与系统的其他部分隔开(见图 8.1)。这条边界确保 TCB 与计算机系统中其他部件的不安全通信或交互不会发生。因为 TCB 要与系统的其他部分进行通信，所以安全边界必须建立安全的通道，也被称为可信路径。可信路径是建立在有着严格标准基础上的通道，在不受 TCB 安全脆弱性影响的情况下准许进行必要的通信。可信路径也保护系统用户(有时也称为主体)不受因 TCB 交换导致的危害。在本章稍后部分，在了解与正式的安全指导原则和评估标准有关的更多信息之后，你还会知道系统需要通过可信路径试图向用户交付高级别的安全性。根据本章稍后将要描述的 TCSEC 指导原则，B2 和较高级别的系统要求使用可信路径。

2. 引用监控器和内核

在实现安全系统时，必须利用 TCB 的某部分来实施针对系统资产和资源(有时称为客体)的访问控制。在准许访问请求之前验证对每种资源的访问的这部分 TCB 被称为引用监控器(见图 8.1)。引用监控器处于每个主体和客体之间，并且在准许进行任何访问请求之前验证请求主体的凭证是否满足客体的访问需求。如果不满足这种访问需求，那么访问请求就会被拒绝。实际上，引用监控视器是 TCB 的访问控制执行者。因此，授权和安全的行动和活动被允许发生，而未经授权的和不安全的活动和行动被拒绝并阻止发生。引用监控器对访问控制或授权的强制基于所需的安全模型，无论是自由支配的、强制性的、基于角色的还是访问控制的一些其他形式。引用监控器可能是 TCB 概念的一部分；它并不需要是一个实际的、独立的或独立工作的系统组成部分。

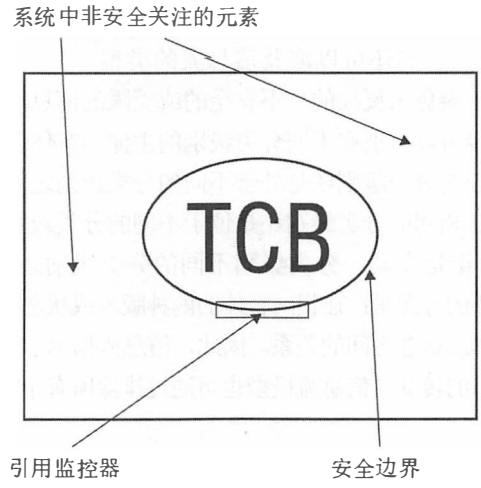


图 8.1　TCB、安全边界和引用监控器

共同工作从而实现引用监控器功能的 TCB 中组件的集合被称为安全内核。引用监控器是一种通过软件和硬件中的安全实现来实施的概念或理论。安全内核的目的是使用适当的组件实施引用监控器的功能和抵抗所有已知的攻击。安全内核使用一条可信路径与主体进行通信，并且还可以作为所有资源访问请求的中间人，从而只允许那些与系统应用的适当访问规则相匹配的请求。

引用监控器要求具有与其保护的每种资源相关的描述性信息。这种信息通常包括资源的分类级别和名称。当某个主体请求访问某个客体时，引用监控器会查阅客体的描述性信息，从而判断应当准许或拒绝访问(参看“安全令牌、功能列表和标签”部分对其工作原理的详细介绍)。

8.2.2　状态机模型

状态机模型描述了一个无论处于何种状态下总是安全的系统，这种模型基于有限状态机(Finite State Machine，FSM)的计算机科学定义。FSM 通过组合外部输入和内部计算机状态来建立所有类型的复杂系统的模型，包括解析器、解码器和解释器。给定一个输入和一个状态，FSM 就会转换至另一个状态，并且可能生成一个输出。从数学上讲，下一状态是当前状态和输入的函数：下一状态= F(输入，当前状态)。同样，输出也是输入和当前状态的函数：输出=F(输入，当前状态)。

许多安全模型都基于安全状态的概念。根据状态机模型，状态是系统在特定时刻的即时快照。如果某个状态的所有方面都满足安全策略的要求，那么这个状态就被认为是安全的。接受输入或生成输出时都会发生转换操作。转换操作总是会产生新的状态(也被称为状态转换)。所有的状态转换都必须进行评估。如果每个可能的状态转换都会导致另一个安全状态，那么系统就会被称为安全状态机。安全状态机模型系统总是会进入一个安全状态(在所有的转换中维护安全状态)，并且准许主体只以遵循安全策略的安全方式访问资源。安全状态机模型是其他许多安全模型的基础。

8.2.3　信息流模型

信息流模型关注于信息流。信息流模型以状态机模型为基础。本章稍后我们将要详细讨论的 Bell-LaPadula 和 Biba 模型都是信息流模型。Bell-LaPadula 模型的目的是防止信息从高安全级别向低

安全级别流动，Biba 模型的目的是防止信息从低安全级别向高安全级别流动。信息流模型不一定只对信息流的方向进行处理，它们还可以涉及信息流的类型。

信息流模型被设计用于避免未授权的、不安全的或受限的信息流。信息流可以出现于相同分类级别的主体和客体之间，也可以出现在不同分类级别的主体和客体之间。信息流模型准许所有被授权的信息流，无论是在相同的分类级别还是处于不同的分类级别之间。信息流模型避免了所有未授权信息流的出现，无论是在相同的分类级别还是位于不同的分类级别之间。信息流模型可以防止未经授权的所有信息流，无论是在同一分类级别不同的分类级别之间。

信息流模型另一个有趣的方面是：在相同客体的两种版本或状态存在于不同的时间点时，信息流模型被用于建立这两种版本或状态之间的关系。因此，信息流指示了客体从某个时间点的一个状态向另一个时间点的另一个状态的转变。信息流模型也可通过排除所有不确定的流途径来解决隐蔽通道。

8.2.4 无干扰模型

无干扰模型松散地建立在信息流模型的基础上。然而，无干扰模型关注的是位于较高安全级别的主体的动作如何影响系统状态，或关注于位于较低安全级别的主体的动作，而不是关注于信息流。本质上，主体 A(位于较高安全级别)的动作不应当影响主体 B(位于较低安全级别)的动作，甚至应当不引起主体 B 的注意。实际上，无干扰模型真正关注于防止位于高安全分类级别的主体 A 的动作影响位于低安全分类级别的系统状态。如果出现这种情况，那么主体 B 可能会处于不安全的状态，或者可能会演绎或推导出较高分类级别的信息。这属于一种信息泄漏类型，并且会隐式地创建隐蔽通道。因此，可以利用非干扰模型来提供一种防止恶意程序(例如，特洛伊木马)导致危害的保护形式。

真实场景

组合论

属于信息流类别的其他一些模型构建在多个系统之间的输入和输出如何彼此关联的概念之上，这些概念仿效了系统之间(而非单个系统内)的信息流。因为解释了一个系统的输出如何关联另一个系统的输入，所以它们被称为组合论。下面列出了组合论的三种公认类型：

- 级联(cascading)：一个系统的输入来自另一个系统的输出。
- 反馈(feedback)：一个系统为另一个系统提供输入，输入通过颠倒两个系统的角色进行往复(也就是说，系统 A 首先为系统 B 提供输入，随后系统 B 为系统 A 提供输入)。
- 挂接(hookup)：一个系统向另一个系统发送输入，但是也向外部实体发送输入。

8.2.5 Take-Grant 模型

Take-Grant 模型采用有向图(见图 8.2)来指示权限如何从一个主体传递至另一个主体或者如何从一个主体传递至一个客体。简单地讲，具有授权资格的主体可以向另一个主体或客体授予其所拥有的其他任何权限。同样，具有获得权限能力的主体可以从另一个主体获得权限。除了这两条主要的规则，Take-Grant(取-予)模型可采取创建规则和移除规则来生成或删除权限。这种模型的关键是使用这些规则可以让你弄清楚在系统中哪些权限可以改变，哪些可能发生泄漏(即许可权限的意外分配)，

如表 8.1 所示。

表 8.1　Take-Grant 模型的规则

规格名	作用
获取规则	允许主体获取客体的权限
授予规则	允许主体向客体授予权限
创建规则	允许主体创建新权限
移除规则	允许主体移除已有的权限

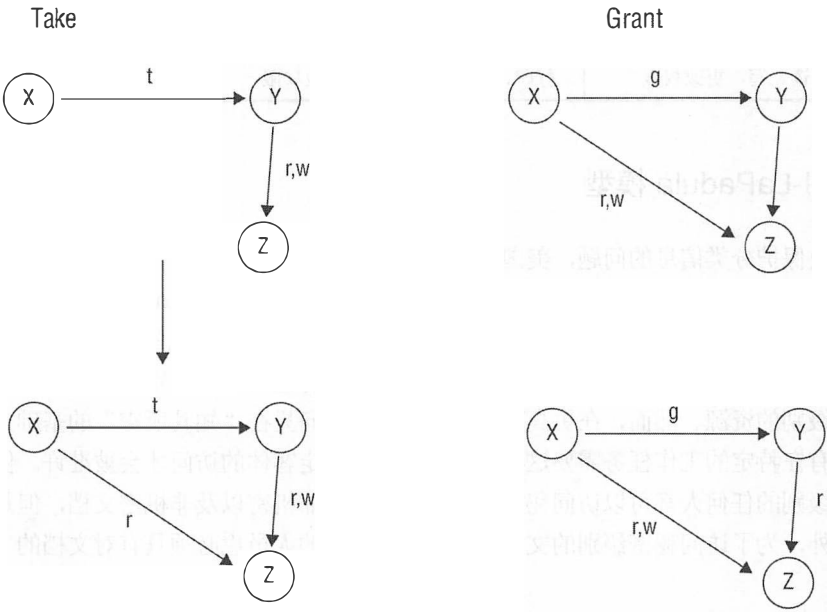


图 8.2　Take-Grant 模型示意图

8.2.6　访问控制矩阵

访问控制矩阵是一个由主体和客体组成的表，这个表指示了每个主体可以对每个客体执行的动作或功能。访问控制矩阵的每一列都是一个访问控制列表；表的每一行都是功能列表。ACL 与客体相关，它列出了每个主体可以执行的有效动作。功能列表与主体相关，它列出了可以在所有客体上执行的有效动作。从行政管理的角度看，只使用功能列表进行访问控制对于管理而言是非常可怕的。通过在每个主体上存储一个该主体对全部客体所具有权限的列表，就能够实现一种访问控制的功能列表方法。这为每个用户有效给出了一个重要的、针对安全域内客体的访问和权限环。为了去除对特定客体的访问，就必须单独操纵访问该客体的每个用户(主体)。这样一来，管理每个用户账户上的访问就比管理每个客体上的访问(也就是通过 ACL)困难许多。

- 构造访问控制矩阵模型通常涉及如下操作：构建可以创建和管理主体和客体列表的环境。
- 规划一个函数，这个函数可以返回与任何客体提供给该函数作为输入相关联的类型(这是很重要的，因为客体的类型决定了可以应用什么类型的操作)。

表 8.2 所示的访问控制矩阵适用于自主访问控制系统。通过简单地利用分类或角色来替代主体

名，我们就可以构造强制型或规则型访问控制矩阵。系统使用访问控制矩阵快速地判断主体请求对客体的操作是否得到了授权。

表 8.2 访问控制矩阵

主体	文档文件	打印机	网络文件共享
Bob	读	不能访问	不能访问
Mary	不能访问	不能访问	读
Amanda	读、写	打印	不能访问
Mark	读、写	打印	读、写
Kathryn	读、写	打印、管理打印队列	读、写、执行
Colin	读、写、更改权限	打印、管理打印队列、更改权限	读、写、执行、更改权限

8.2.7 Bell-LaPadula 模型

为了解决保护分类信息的问题，美国国防部(Department of Defense，DoD)在 20 世纪 70 年代开发了 Bell-LaPadula 模型。DoD 管理着分类资源的多个级别，并且 Bell-LaPadula 模型衍生自 DoD 的多级安全策略。DoD 使用的分类级别众多，不过在 CISSP CBK 内讨论的分类级别往往被限制为 4 个：非机密、机密、秘密以及绝密。多级安全策略规定具有任何许可级别的主体可以访问位于相同或更低许可级别的资源。然而，在更高的许可级别内，访问只在“知其所需”的基础上被准许。换句话说，只有在特定的工作任务需要这样的访问时，对特定客体的访问才会被准许。例如，具有秘密安全许可级别的任何人都可以访问秘密、机密、敏感但非机密以及非机密文档，但是不能访问绝密文档。此外，为了访问秘密级别的文档，试图进行访问的人员也必须具有对文档的“知其所需”权限。

在设计上，Bell-LaPadula 模型防止了分类信息泄漏或传输至较低的安全许可级别。通过阻止较低分类级别的主体访问较高分类级别的客体，就可以实现这个目的。根据这些限制，Bell-LaPadula 模型专注于维护客体的机密性。因此，Bell-LaPadula 模型解决了确保文档机密性所涉及的复杂性问题。然而，Bell-LaPadula 模型没有说明客体的完整性或可用性方面的内容。Bell-LaPadula 模型也是多级安全策略的首个数学模型。

真实场景

格子型访问控制

第 13 章将介绍这种非自主访问控制的通用类别。我们在这里快速复习一下与主体相关的知识(这些内容是大多数访问控制安全模型的基础)：格子型访问控制下的主体被指派在一个格子内。这些位置位于已定义的安全标签或分类级别之间。主体能够访问的客体所在的范围，只能位于为之定义格子位置的安全标签或分类级别的最小上限(高于其格子位置的距离最近的安全标签或分类级别)和最大下限(低于其格子位置的距离最近的安全标签或分类级别)之间。因此，在某个分类级别由低至高分别为公开、敏感、私有、专有和机密的商业方案中，位于私有和敏感标签之间的主体只能访问隐私和敏感数据，但是不能访问公开、专有或机密数据。格子型访问控制恰好也是信息流模型的通用类别，并且主要解决机密性问题(这也是在讨论 Bell-LaPadula 模型时提及格子型访问控制的原因)。

Bell-LaPadula 模型以状态机概念和信息流模型为基础。这种模型还采用强制访问控制和格子型概念。格子等级是由组织机构的安全策略使用的分类级别。状态机支持在任何两个状态之间都能够显式转换多个状态；使用这个概念是因为能够以数学方式证明计算机的正确性以及对文档机密性的保证。这种状态机具有下列三种属性：

- 简单安全属性(simple security property)规定主体不能读取位于较高敏感度级别的信息(也就是不能向上读)。
- *安全属性(*(star)security property)规定主体不能在位于较低敏感度级别的客体上写入信息(也就是不能向下写)，这也被称为约束属性(confinement property)。
- 自主安全属性(discretionary security property)规定系统使用访问控制矩阵来实施自主访问控制。

前两个属性定义了系统可能转换到的状态。其他的转换都是不被准许的。所有通过这些规则可以访问的状态都是安全状态。因此，Bell-LaPadula 模型系统提供了状态机模型的安全性(如图 8.3 所示)。

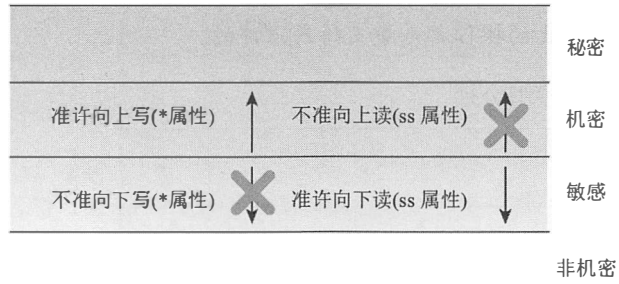


图 8.3　Bell-LaPadula 模型

注意：

在 Bell-LaPadula 模型中有个例外，就是规定了“受信任的主体”不受*安全属性的约束。受信任的主体被定义为“保证即使可能也不会破坏安全信息的传输的主体”。这意味着受信任的主体被准许不必遵循*安全属性并且可以执行向下写的操作，有必要进行有效的对象定级或重新定级。

Bell-LaPadula 属性有效地保护了数据的机密性。主体不能读取分类级别高于其级别的客体。因为一个级别上的客体所具有的数据比较低级别上的数据更为敏感或秘密，所以主体不能将某个级别的数据写入较低级别的客体(除了可信主体之外)。这个动作类似于将绝密备注粘贴到非机密的文档文件中。此外，第三种属性实施了主体能够访问客体的“知其所需”权限。

Bell-LaPadula 模型只解决数据的机密性问题，但是没有涉及数据的完整性和可用性。因为这种模型是在 20 世纪 70 年代设计的，所以并不支持目前常见的许多操作，例如文件共享和网络连接。这种模型还说明了安全层之间的安全转换，但是并没有涉及隐蔽通道问题(在稍后的第 9 章“安全脆弱性、威胁和对策”中进行介绍)。Bell-LaPadula 模型很好地处理了机密性问题，因此常常与其他处理完整性和可用性机制的模型组合使用。

8.2.8　Biba 模型

对于很多非军事组织来说，完整性比机密性更为重要。除了这种需要之外，许多关注于完整

性的安全模型也已开发出来，例如，由 Biba 和 Clark-Wilson 开发的 Biba 模型。Biba 模型是仿照 Bell-LaPadula 模型设计的。Bell-LaPadula 模型解决了机密性问题，而 Biba 模型则解决了完整性问题。Biba 模型也是建立在状态机概念的基础之上。事实上，除了反向之外，Biba 模型与 Bell-LaPadula 模型十分相似。这两种模型都使用了状态和转换，都具有基本的属性。二者的最大差异是关注的主要目标不同：Biba 模型主要保护数据的完整性。下面列出了 Biba 模型状态机的基本属性：

- 简单完整性属性(simple integrity property)规定主体不能读取位于较低完整性级别的客体(也就是不能向下读)。
- *完整性属性(*(star)integrity property)规定主体不能更改位于较高完整性级别的客体(也就是不能向上写)。

注意：

Biba 模型和 Bell-LaPadula 模型都有两个主要属性：简单属性和星号属性。不过，它们也可以被标记为公理、原则或规则。需要注意的是，简单属性总是与读操作有关，星号属性则总是与写操作有关。此外，不管是使用简单属性还是星号属性，它们都是定义不能或不应进行操作的规则。在大多数情况下，未被阻止或禁止的操作都是受支持或准许的。

图 8.4 说明了这些 Biba 模型公理。

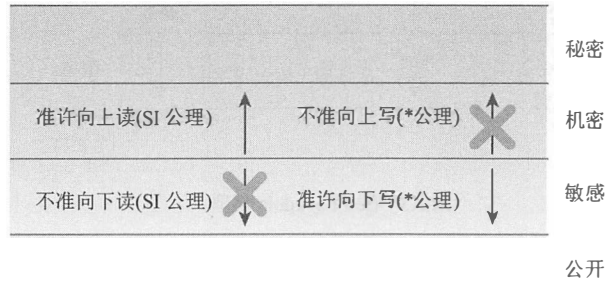


图 8.4 Biba 模型

在将 Biba 模型与 Bell-LaPadula 模型进行比较时，你会注意到它们看上去是相反的。这是由于二者关注安全性的不同方面。Bell-LaPadula 模型确保数据的机密性，而 Biba 模型则确保数据的完整性。

Biba 模型被设计用于解决下列三个完整性问题：

- 防止未授权的主体对客体的修改。
- 防止已授权的主体对客体进行未授权的修改。
- 保护内部和外部客体的一致性。

与 Bell-LaPadula 模型一样，Biba 模型要求所有客体和主体都具有分类标签。因此，数据完整性保护依赖于数据分类。

让我们看看 Biba 属性。Biba 模型的第二个属性非常简单。主体不能对位于较高完整性级别的客体进行写操作。这是很有意义的。第一个属性情况如何？为什么主体不能读取位于较低完整性级别的客体？回答这些问题需要稍加思考。可以将完整性级别想象为空气的纯净级别。你肯定不希望将弥漫着烟味的场所内的空气注入原本环境清新的房间。同样的想法也被应用于数据。在完整性十分重要的情况下，你不希望将未经验证的数据读入已验证的文档。数据污染的可能性过大时，这样

的访问就不被允许。

对 Biba 模型的批评提到了下列几个缺陷：

- 只解决了完整性问题，没有解决机密性或可用性问题。
- 专注于保护客体不受外部的威胁；假定内部的威胁已被有计划地控制。
- 没有说明访问控制管理，也没有提供分配或改变主体或客体分类级别的方法。
- 并没有防止隐蔽通道。

因为 Biba 模型关注于数据的完整性，所以与 Bell-LaPadula 模型相比，Biba 模型是商用安全模型更常见的一种选择。相比机密性而言，大多数商业组织更关心数据的完整性。

8.2.9　Clark-Wilson 模型

尽管 Biba 模型适合于商用，不过人们还是在 1987 年为商业环境专门设计了另一种模型：Clark-Wilson 模型。这种模型使用多层面途径来实施数据完整性。Clark-Wilson 模型没有定义正式的状态机，而是只通过一小组程序来定义每个数据项并允许修改。

Clark-Wilson 模型并不要求使用格子型结构，而是使用被称为三元组或访问控制三元组的主体/程序/客体(或主体/事物/客体)的三部分关系。主体并不对客体进行直接访问。客体只能通过程序进行访问。通过使用下列两条原则：格式良好的事务处理和职责分离，Clark-wilson 模型提供了保护完整性的有效方法。

格式良好的事务处理采用程序的形式。主体只能通过使用程序、接口或访问门户(见图 8.5)来访问客体。每个程序都对可以对客体做什么和不可以对客体做什么施加了特定的限制(例如，数据库和其他资源)。这有效地限制了主体的能力。这被称为约束接口。如果程序设计正确，那么三元组关系就提供了保护客体完整性的方法。

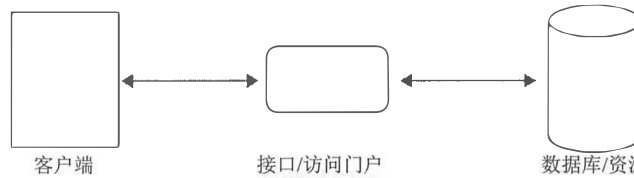


图 8.5　Clark-Wilson 模型

Clark-Wilson 模型定义了下列数据项和过程：

- 约束数据项(Constrained Data Item，CDI)：是指完整性由安全模型保护的任何数据项。
- 非约束数据项(Unconstrained Data Item，UDI)：是指不受安全模型控制的任何数据项。作为输入且未验证的任何数据或任何输出都被视为非约束数据项。
- 完整性验证过程(Integrity Verification Procedure，IVP)：扫描数据项并确认其完整性的过程。
- 转换过程(Transformation Procedure，TP)：TP 是允许更改 CDI 的唯一过程。通过 TP 限制对 CDI 的访问而形成 Clark-Wilson 完整性模型的主干(我们想知道这是否是 TPS 报告的来源)。

Clark-Wilson 模型使用安全标签来授予对客体的访问权限，但是只能通过转换过程和受限接口模型来完成。受限接口模型使用基于分类的限制，并且只提供主体特定的授权信息和功能。在某个分类级别上的主体将可以看到一组数据，并且有权访问一系列的功能；而另一个分类级别上的主体则可以看到不同的数据，并且有权访问不同系列的功能。向不同级别或分类的用户提供的不同功能，

可以通过向所有用户显示所有功能，但禁用那些不被特定用户授权或仅显示特定用户授权的功能来实现。通过这些机制，Clark-Wilson 模型确保任何用户都不能未授权地修改数据。实际上，Clark-Wilson 模型实现了职责分离。Clark-Wilson 模型的设计使其成为一种适于商用的优秀模型。

8.2.10 Brewer and Nash 模型(也叫作 Chinese Wall)

创建这种模型的目的是准许访问控制基于用户以前的活动而动态改变(这也使其成为一种状态机模型)。这种模型应用于单个集成的数据库，并且试图创建对利益冲突敏感的安全域(例如，如果 A 公司和 B 公司存在竞争关系，那么在 C 公司工作的某人虽然能够访问 A 公司的私有数据，但是也应当不被准许访问 B 公司的类似数据)。因为创建了一个数据类，这个数据类定义了哪些安全域存在潜在的冲突，对于能够访问某个属于特定冲突类的安全域的任何主体，阻止他们访问属于相同冲突类的其他任何安全域，所以这种模型被称为 Chinese Wall 模型。这个名字比喻在任何冲突类的其他所有数据周围修筑了一道长城，从而解释了该术语。因此，这种模型在每个冲突类内也使用了数据隔离原则，以便使用户置身于潜在的利益冲突状况之外(例如，公司数据集的管理)。因为公司间的关系随后会发生变化，所以也解释了动态更新冲突类的成员及定义的重要性。

考虑或思考 Brewer and Nash 模型的另一种方式是：管理员在基于分配给他们的工作职责和工作任务的基础上，对系统中的大量数据拥有完全的访问控制。然而，在对任何数据项采取行动时，管理员对任何冲突数据的访问都会被暂时阻止。只有涉及初始数据项的数据在操作过程中才能被访问。一旦任务完成后，管理员的访问将返回到完全控制。

8.2.11 Goguen-Meseguer 模型

Goguen-Meseguer模型是一个完整性模型，尽管它不如Biba和其他模型有名。实际上，这个模式被称作非干涉概念理论的基础。通常当某人讲非干涉模型时，他们实际指的是Goguen-Meseguer模型。

Goguen-Meseguer 模型基于主体可以访问的预设的域或客体列表。该模型基于自动化理论和域的隔离。这意味着主体只允许对预设客体执行预定的动作。当类似的用户被分组到他们自己的域(也就是集合)时，一个主体域的成员不能干扰另一个主体域的成员。因此，客体无法干扰其他客体的活动。

8.2.12 Sutherland 模型

Sutherland 模型是一个完整性模型。它的重点是预防对完整性支持的干扰。它正式地基于状态机模型和信息流模型。然而，它并没有直接表明保护完整性的具体机制。相反，该模型基于定义一组系统状态的想法，以及初始状态和状态转换。通过使用这些预定的安全状态来保护完整性和阻止干扰。

Sutherland 模型的一个常见例子就是被用于预防用来影响程序或活动输出的隐蔽通道(隐蔽通道在第 9 章讲述)

8.2.13 Graham-Denning 模型

Graham-Denning 模型关注主体和客体在创建和删除时的安全性。Graham-Denning 模型集合了 8

个主要的定义特定安全行为边界的保护规则或动作：

- 安全创建客体
- 安全创建主体
- 安全删除客体
- 安全删除主机
- 安全读访问权限
- 安全授予访问权限
- 安全删除访问权限
- 安全转移访问权限

通常，一组客体上的主体的特定能力或权限被定义在访问矩阵中(又名访问控制矩阵)。

8.3　基于系统安全评估模型选择控制和对策

为了特定应用而购买信息系统的人员或机构，例如，敏感数据极有价值或落入坏人手中极其危险的国家安全机构、特定数据的价值达数十亿美元的中央银行或证券交易所，通常希望了解系统的安全强度和缺陷。这样的购买者通常只愿意考虑已经预先进行正式评估并给出了安全评级的系统，从而了解自己需要哪种系统。通常购买者还必须采取其他措施以保证系统尽可能安全。

进行正式评估时，系统往往需要经历两步骤过程：

(1) 在第(1)个步骤中，系统会被测试并执行技术评估，从而确认系统的安全性能是否满足为预期使用而设置的标准。

(2) 第(2)个步骤会对系统的设计和安全标准与实际的功能和性能进行正式比较，并且负责系统安全性和准确性的人员必须决定是否采用、放弃系统，或者必须修改标准并再次进行评估。

事实上，经常雇用可信的第三方来执行这样的评估；这种测试最重要的结果是表明系统满足所有必要标准的“认证标志”。

无论在组织内部还是外部管理评估操作，选购系统的组织都必须决定接受或拒绝被建议采用的系统。组织的管理部门必须正式负责是否采用系统以及何时采用，并且应当接受与选购系统的部署和使用相关联的任何风险。

这里将介绍的三个主要评估模型或分级标准模型产品是 TCSEC、ITSEC 和通用标准。

注意：

你应该知道，TCSEC 已经被废除，并由通用标准(以及许多其他美国国防部指令)取代。但 TCSEC 仍然出现在这里，仅仅是作为历史参考，以及作为基于静态评估标准的示例，通过对比看出缺乏哪些动态(尽管主观)评估标准的优点。记住，CISSP 考试的重点关注于“为什么”安全多于“如何”实现安全，换句话说，侧重于概念和理论而不是技术和实现。因此，一些这方面的历史信息可能会出现在考题中。

8.3.1　彩虹系列

自 20 世纪 80 年代以来，政府、机构、团体和各种商业组织都不得不面对涉及信息系统挑选和

使用的风险。这种情况导致近年来出现了一系列信息安全标准，这些标准试图为各种使用类别指定最低的可接受安全标准。当购买者希望获得和部署能够保护和保留其内容，或者能够满足各种强制安全需求(例如，承办商管理与政府相关的业务时按手续必须满足的需求)的系统时，这些使用类别十分重要。在美国国防部(DoD)致力于为购买和使用的系统开发和实施安全标准时，第一组这样的标准导致在 20 世纪 80 年代出现可信计算机系统评估标准(TCSEC)。随后，在 20 世纪 90 年代中期，这个系列的所有标准都被公布出来。因为往往可以通过封面颜色来标识这些被公布的标准，所以它们被合称为彩虹系列。

按照 DoD 所使用的模式，其他政府或标准团体在彩虹系列元素的基础上构建和完善了新的计算机安全标准，其中重要的标准包括被称为信息技术安全评估标准(ITSEC)的 European 模型，这种模型在 1990 年被开发出来，并且一直使用到 1998 年。最后，TCSEC 和 ITSEC 都被所谓的通用准则替换，这种标准更为正式的名称为“IT 安全领域内通用准则认证认可协议”。美国、加拿大、法国、德国和英国在 1998 年都采用了该标准。我们将在后面详细讨论 ITSEC 和通用准则标准。

政府或其他安全意识机构在评估信息系统时，会利用各种标准评估准则。1985 年，美国国家计算机安全中心(NCSC)开发了 TCSEC，缘于其封面的颜色，我们将这个标准称为橘皮书。TCSEC 建立了从安全性角度评估独立计算机所使用的指导原则。这些指导原则涉及基本的安全功能，并且允许评估者对系统的功能性和可靠性做出度量和评级。事实上，在 TCSEC 中，功能性和安全性保证被组合在一起，而不像后来开发的安全标准那样将二者区分开来。TCSEC 指导原则被设计用于评估供应商的产品，也可以被供应商用于确保在新产品中构建所有必要的功能性和安全性保证。

接下来，我们会较为详细地介绍橘皮书本身，随后将讨论彩虹系列中其他一些重要的元素。

8.3.2 TCSEC 分类和所需功能

TCSEC 将系统提供的功能性和机密性保护等级保证组合为 4 个主要类别。这些类别随后又被进一步划分为使用数字标识的子类别(例如，C1 和 C2)。进一步说，TCSEC 的类别是通过对目标系统的评估来指派。TCSEC 适用的系统是没有互联的独立系统。TCSEC 定义了下列主要类别：

类别 A 已验证保护，这是最高的安全级别

类别 B 强制性保护

类别 C 自主性保护

类别 D 最小化保护，提供给那些被评估但不符合要求且属于其他类别的系统定级之用

图 8-6 包含了对类别 A 到 C 的详细描述，数字后缀表示任何适用的范畴。

级别标签	需求
D	最小化保护
C1	自主性保护
C2	受控访问保护
B1	标签式安全
B2	结构化保护
B3	安全域
A1	已验证保护

图 8.6 TCSEC 的级别

自主性保护(类别 C1、C2)　自主性保护系统提供了基本的访问控制。这个类别中的系统的确能提供一些安全控制方法，但是缺乏针对安全系统特定需要的更复杂且更严格的控制方法。C1 和 C2 类别的系统提供了基本的控制和用于系统安装与配置的完整文档。

- **自主性安全保护(类别 C1)**　自主性安全保护系统通过用户 ID 和/或用户组来实现访问控制。虽然对客体的访问采取了一些控制措施，但这个类别中的系统只能提供较弱的保护。
- **受控访问保护(类别 C2)**　受控访问保护系统的安全性强于 C1 系统。用户必须被单独标识后才能获得访问客体的权限。C2 系统还必须实施介质清除措施。如果实施了介质清除措施，那么在另一位用户重新使用介质之前，必须首先彻底地清除介质上的内容，从而保证不会保留先前的数据供检查和使用。此外，也必须实施限制无效或未授权用户访问的严格登录措施。

强制性保护(类别 B1、B2、B3)　强制性保护系统比类别 C 或 D 的系统提供了更多的安全控制方法。因为强制实施了更细粒度的控制，所以安全管理员能够应用只允许非常有限的主体/客体组访问的特定控制手段。这个系统类别以 Bell-LaPadula 模型为基础。强制访问控制基于安全标签。

- **标签式安全(类别 B1)**　在标签式安全系统中，每个主体和客体都有一个安全标签。通过匹配主体和客体的标签并比较它们的权限兼容性，B1 系统授予了访问权限。B1 系统提供了足够的安全保护来保留已分类的数据。
- **结构化保护(类别 B2)**　除了要求具有安全标签之外(就像在 B1 系统中一样)，B2 系统必须确保不存在隐蔽通道。操作者和管理员的职责被分隔开，并且进程也被隔离。如果分类数据需要高于 B1 系统的安全功能性，B2 系统可以满足需要。
- **安全域(类别 B3)**　通过进一步增加无关进程的分隔和隔离，安全域系统提供了更多的安全功能性。管理功能被清楚地定义并与其他用户可以使用的功能分开。B3 系统的关注点转移到简易性，从而减少了在未用的或多余的代码中所暴露出来的脆弱性。B3 系统的安全状态也必须在初始启动过程中被说明。B3 系统难以被成功攻击，并且为非常敏感的或秘密的数据提供了充分的安全控制。

已验证保护(类别 A1)　已验证保护系统在结构和使用的控制方面与 B3 系统类似。二者的差别在于开发周期。开发周期的每个阶段都使用正式的方法进行控制。在执行下一个步骤之前，设计的每个阶段都要被记入文档、评估和验证。在开发和部署的所有阶段都给予极高的安全关注度，并且是正式保证系统强安全性的唯一方式。

已验证设计系统从设计文档开始，文档中说明了所设计的系统如何满足安全策略的要求。从这里开始，每个开发步骤都要在安全策略的上下文中进行评估。功能性是至关重要的，但是保证比在较低安全类别中更加重要。A1 系统代表安全性的最高级别，被设计用于处理绝密数据。从设计到交付和安装的全过程，每个步骤都要被记入文档和进行验证。

8.3.3　彩虹系列中的其他颜色

总的来说，在 DoD 文档集合中有近 30 个标题被添加到橘皮书或进一步详细说明。尽管颜色并没有任何意义，但是却被用于描述这一系列中公布的各种标准。

注意：

重要的是要明白：彩虹系列的大部分书籍现在已经过时，并已被更新的标准、准则和指令替换。但是它们仍然在这里列出以供参考，以应对任何考试题目。

关于这个集合文档的其他重要内容如下：

红皮书 因为橘皮书只应用于未连接到网络的独立计算机，而如此多的系统却连接到网络(即使在 20 世纪 80 年代也是如此)，所以红皮书被开发出来用于在网络互联环境中解释说明 TCSEC。事实上，红皮书的正式标题是“可信网络解释”，因此可以被视为致力于从网络连接角度对橘皮书进行解释说明。很快，对于系统购买者和构建者来说，红皮书比橘皮书更为实用和重要。下面列出了红皮书的其他一些功能：

- 评定机密性和完整性的等级
- 解决通信的完整性问题
- 解决拒绝服务的防护问题
- 解决危害(也就是入侵)的防护和阻止问题
- 受限于被标记为“使用单个鉴定授权的集中式网络”的有限网络类别
- 只使用 4 种等级级别：None、Cl(Minimum)、C2(Fair)以及 B2(Good)。

绿皮书 绿皮书或“美国国防部密码管理指导原则”提供了创建和管理密码的指导原则。对于配置和管理可信系统的人来说，绿皮书十分重要。

表 8.3 提供了彩虹系列的一个更完整的书籍列表。更多关于下载书籍的信息，可访问彩虹系列网页： http://csrc.nist.gov/publications/secpubs/index.html。

表 8.3 重要的彩虹系列元素

发表编号	标题	名称
5200.28-STD	DoD 可信计算机系统评估标准	橘皮书
CSC-STD-002-85	DoD 密码管理指导原则	绿皮书
CSC-STD-003-85	在特定环境中应用 TCSEC 的指南	黄皮书
NCSC-TG-001	理解可信系统审计的指南	褐皮书
NCSC-TG-002	可信产品评估：供应商指南	天蓝皮书
NCSC-TG-002-85	PC 安全考虑	浅蓝皮书
NCSC-TG-003	理解可信系统中任意访问控制的指南	氖橘皮书
NCSC-TG-004	计算机安全术语词汇表	浅绿皮书
NCSC-TG-005	可信网络解释	红皮书
NCSC-TG-004	理解可信系统中配置管理的指南	琥珀皮书
NCSC-TG-006	理解可信系统中设计文档的指南	暗红皮书
NCSC-TG-008	理解可信系统中可信分发的指南	浅紫皮书
NCSC-TG-009	TCSEC 中计算机安全子系统的解释	威尼斯蓝皮书

考虑到构成 TCSEC 投入的所有时间和精力，我们难以理解为什么还会出现更新更高级的评估标准。随着时代的发展和技术的更新，下面列出的对 TCSEC 的主要批评能够解释目前普遍使用更新标准的原因：

- 尽管 TCSEC 重点考虑控制用户对信息的访问，但是并没有控制用户一旦获得访问权限后如何对信息进行处理。在军事和商业应用中，这都是问题。

- 考虑到来自于美国国防部，因此可以理解 TCSEC 标准关注的重点完全在于机密性，该标准认定控制用户访问数据的方式意味着不必关注数据的准确性或完整性。在认为数据的准确性和完整性比机密性更重要的商业环境中，TCSEC 不起作用。
- 除了自身强调访问控制之外，TCSEC 并不仔细处理完全实现安全策略所必需的各种人员、物理和过程化的策略问题或防范措施。此外，TCSEC 也不处理影响系统安全性的问题。
- 橘皮书本质上并不处理网络连接问题(尽管之后在 1987 年开发的红皮书能够解决类似问题)。

在一定程度上，这些批评反映了美国军方关注的唯一安全问题导致了 TCSEC 的开发。随后，当时广泛使用的主流计算工具和技术(网络连接是在 1985 年开始出现的)也产生了影响。当然，组织内日益复杂和全面的安全观点也有助于解释 TCSEC 在过程上和策略上存在不足。但是，因为 ITSEC 已基本被通用准则替换，所以在讨论通用准则之前，我们会阐述 ITSEC。

8.3.4　ITSEC 类别与所需的保证和功能性

ITSEC 代表欧洲创建安全评估标准的最初尝试，并且是作为 TCSEC 指导原则的可选方案被开发出来的。ITSEC 指导原则使用不同的类别等级来评估系统的功能性和保证。在这种环境下，系统的功能性是针对系统用户的实用价值进行衡量。系统的功能性等级描述了系统基于设计和预期目的执行所需功能的情况。保证等级表示系统以一致的方式正常工作的可靠程度。

ITSEC 将正在被评估的系统作为评估目标(Target Of Evaluation，TOE)。所有的等级都以两种类别表示为 TOE 等级。ITSEC 使用两个尺度来评定功能性和保证的等级。

系统的功能性等级从 F-D 到 F-B3(没有 F-A1)进行划分。系统的保证等级从 E0 到 E6 进行划分。通常，大多数 ITSEC 等级与 TCSEC 等级相对应(例如，TCSEC 的 C1 系统对应于 ITSEC 的 F-C1、E1 系统)。表 8.4(位于下一节“通用准则的结构”的最后部分)比较了 TCSEC、ITSEC 和通用准则的等级。

注意：

在某些实例中，ITSEC 的 F 等级使用 F1 到 F5 来定义，而不是重用 TCSEC 中的标签。这些标签的对应关系为：F1=F-C1，F2＝F-C2，F3＝F-B1，F4＝F-B2，以及 F5＝F-B3。F-D 一般不存在数字编号的 F 等级，不过在某些时候也会使用 F0 等级。因为如果不具备进行等级划分的任何功能，那么就不需要等级标签，所以 F0 标签毫无意义。

TCSEC 和 ITSEC 之间的差异十分多样化。下面列出了两个标准之间的一些重要差异：

- 尽管 TCSEC 几乎只关注机密性，但是 ITSEC 除了机密性之外还关注 TCSEC 缺少的完整性与可用性，因此覆盖了对于维护完整信息的安全性十分重要的所有三个元素。
- ITSEC 并不依赖于 TCB 的概念，并且不要求系统的安全组件在 TCB 内是隔离的。
- TCSEC 要求任何发生变化的系统都要重新进行评估，这些变化包括操作系统的升级、安装补丁或修复，以及应用程序的升级或变化等；ITSEC 在这些变化之后不要求进行新的正式评估，而是只维护评估目标。

要想了解 ITSEC(现在已基本被下一节介绍的通用准则替代)的更多信息，访问 ITSEC 的官方站点：https://www.bsi.bund.de/cae/servlet/contentblob/471346/publicationFile/30220/itsec-en_pdf.pdf。也可以查看原始的 ITSEC 说明书，网址为 http://www.ssi.gouv.fr/uploads/2015/01/ITSEC-uk.pdf。

8.3.5 通用准则

通用准则几乎是全球性的标准，涉及使用 TCSEC 和 ITSEC 以及其他标准的所有人员。最终，这导致人们能够购买 CC 评估的产品，其中 CC(Common Criteria)表示通用准则。通用准则定义了测试和确认系统安全能力的各种级别，其中级别数表明已执行测试和配置的种类。然而，我们必须认识到：即使是最高的 CC 等级，也并不等同于保证系统绝对安全或者完全没有会被加以利用的脆弱性或敏感性。通用准则被设计用做产品评估模型。

1. 通用准则的认可

除了警告和免责声明之外，加拿大、法国、德国、英国和美国的政府机构代表在 1998 年签署同意了标题为“IT 安全领域内通用准则认证认可协议”的文档，从而使通用准则成为国际性标准。ISO 将这个文档转换为名为 ISO 15408“信息技术安全的评估标准”的官方标准。下面列出了 CC 指导原则的目标：

- 增加购买者对已评估和已划分等级的 IT 产品的安全性的信心。
- 消除重复评估(除其他外，如果某个国家、机构或验证组织对特定系统的评定等级和配置遵循 CC，那么其他国家、机构或验证组织就不需要进行重复的工作)。
- 使安全评估和认证过程更有效益和效率。
- 确保 IT 产品的评估遵循高且一致性标准。
- 促进评估，并且增强已评估和已划分等级的 IT 产品的可用性。
- 评估 TOE 的功能性(也就是系统的功能)和保证(也就是系统的被信任程度)。

可以在 Web 站点 http://www.niap-ccevs.org/cc-scheme/上查找到通用准则文档。访问该站点可以得到最新版本的 CC 指导原则、使用 CC 的指南以及大量有用的其他相关信息。

通用准则过程基于两个关键元素：保护轮廓和安全目标。保护轮廓(Protection Profiles，PP)指定被评估产品(TOE)的安全需求和保护，这也是客户考虑的安全要求或“希望达到的标准”。安全目标(Security Targets，ST)指定了供应商在 TOE 内构建的安全声明。ST 被视为已实现的安全措施或供应商“提供的安全目标”。除了提供安全目标之外，供应商还提供额外的安全特性包。包是安全需求组件的中间分组，既可以被添加到 TOE 中，也可以从 TOE 中去除(就像购买新车时的可选包一样)。

将 PP 与选定供应商的 TOE 中的各种 ST 进行比较，最接近或最匹配的就是客户要购买的。为了选择当前可用的系统，客户最初基于公布或推销的评估保证级别或 EAL(Evaluation Assurance Level，后面会详细介绍 EAL 的内容)来选择供应商。使用通用准则来选择供应商，这允许客户精确地请求所需的安全性，而非不得不使用静态的固定安全级别。使用通用准则还允许供应商在设计和生成产品时具有更大的灵活性。定义良好的一组通用准则支持主体性和多用性，并且能够自动适应变化的技术和威胁环境。此外，EAL 提供了一种比较供应商系统是否更标准化的方法(和较早的 TCSEC 一样)。

2. 通用准则的结构

CC 指导原则被分为下列三部分：

部分 1 介绍和一般模型描述(Introduction and General Model)用于评估 IT 安全性和指定评估目标时涉及的一般概念与基本模型。对于不熟悉安全评估工作过程的人，或者阅读和解释评估结果时

需要寻求帮助的人来说，这部分是非常有用的介绍和说明材料。

部分 2　安全功能需求(Security Functional Requirement)描述与安全审计、通信安全、安全性的密码学支持、用户数据保护、身份标识和身份认证、安全管理、TOE 安全功能(TSF)、资源利用、系统访问以及可信路径有关的各种功能需求。这部分覆盖 CC 评估过程中能够预想到的完整安全功能范围，并且还具有解释每个功能区域的额外附录。

部分 3　安全保证(Security Assurance)涉及 TOE 在配置管理、传送和操作、开发、指导文档与生命周期支持领域的保证需求，以及保证测试和脆弱性的评估。这部分覆盖 CC 评估过程中预想到的安全保证检查和保护轮廓的完整范围，并且还具有与描述如何设计、检查和测试系统的评估保证级别相关的信息。

出现在各种 CC 文档(这些文档至少值得通读一遍)中的大多数重要信息都是评估保证级别(EAL)。表 8.4 概括了从 1 到 7 的 EAL。关于 EAL 的完整说明，可查看 CC 文档(网址为 https://www.niap-ccevs.org/)并查看最新修订的第 3 部分。

表 8.4　CC 评估保证级别

级别	保证级别	说明
EALl	功能测试	要求正确操作的一定置信度，但是在安全威胁不严重的时候可以应用该级别。当应用了适当关注的独立保证来包含个人信息时，这个级别非常有用
EAL2	结构测试	设计信息和测试结果的交付与良好的商业应用一致时可以应用该级别。在开发人员或用户要求从低级到中等的独立保证安全性时，这个级别非常有用。尤其在评估传统系统时，IT 与该级别的关系很大
EAL3	系统地测试和检查	安全工程从设计阶段开始，并且随后未发生重大更改直至完成的时候可以应用该级别。在开发人员或用户要求从低级到中等的度量保证安全性时，这个级别非常有用(包括对 TOE 及其开发的彻底研究)
EAL4	系统地设计、测试和回顾	已使用严格、确定的安全工程和良好的商业开发实践时可以应用该级别。这个级别不要求大量的专业知识、技能或资源，涉及所有 TOE 安全功能的独立测试
EAL5	半正式设计和测试	使用严格的安全工程和商业开发实践(包括专业的安全工程技术)来进行半正式测试。开发人员或用户要求高级别的度量保证安全性时(以计划好的开发方式开始，随后进行严格的开发)可以应用该级别
EAL6	半正式验证、设计和测试	在设计、开发和测试的所有阶段都使用直接、严格的安全工程技术，从而生成优良的 TOE。在需要高风险状况下的 TOE 时可以应用该级别。此时受保护资产的价值会证明额外的成本是合理的。广泛的测试减少了渗透的风险、隐蔽通道的可能性以及被攻击的脆弱性
EAL7	正式验证、设计和测试	只用于最高风险状况或涉及高价值资产的情况。这个级别限于这样的 TOE：密切关注的安全功能性需要进行广泛的正式分析和测试

尽管 CC 指导原则具有足够的灵活性和适应性来获取大多数安全需求，但是绝非完美。与其他评估标准一样，CC 指导原则并不确认用户对数据的处理方式也是安全的。CC 指导原则也没有解决特定安全范围之外的行政管理问题。与其他评估标准一样，CC 指导原则没有包含对原位置安全性的评估，也就是说不涉及与人员、组织的实践和措施或物理安全相关联的控制。同样，CC 指导原则也没有解决对电磁辐射的控制，并且不存在对明确安排的密码学算法的强度进行等级评定的标准。尽管如此，CC 指导原则仍然代表系统评定安全性等级所采用的某些最优技术。为了结束对安全评

估标准的讨论，表 8.5 简要比较了 TCSEC、ITSEC 和 CC 的各种等级。表 8.5 表明每个标准的评级有相似但不相同的评价标准。

表 8.5　安全评估标准的比较

TCSEC	ITSEC	CC	作用
D	F-D+E0	EAL0、EAL1	最小化/无保户
C1	F-C1+E1	EAL2	自主安全机制
C2	F-C2+E2	EAL3	受控访问保护
B1	F-B1+E3	EAL4	标签化安全保护
B2	F-B2+E4	EAL5	结构化安全保护
B3	F-B3+E5	EAL6	安全域
A1	F-B3+E6	EAL7	已验证安全设计

3. 行业和国际安全实施指南

除了整体的安全访问模型，如常见的 CC 标准，还有许多其他用于存储、通信、事务等各个方面的更具体或集中的安全标准。有两个标准你应该熟悉，它们是支付卡行业数据安全标准(PCI-DSS)和国际标准化组织(ISO)。

PCI-DSS 是提高电子支付交易安全要求的集合。这些标准由 PCI 安全标准委员会的成员进行制订，这些成员主要来自信用卡银行和金融机构。PCI-DSS 定义了安全管理、策略、程序、网络架构、软件设计的要求及其他关键的保护措施。关于 PCI-DSS 的更多信息，访问网站 www.pcisecuritystandards.org。

国际标准化组织是由不同国家标准组织的代表组成的世界性标准组织。国际标准化组织定义了工业和商业设备、软件、协议、管理以及其他的标准，有 6 个主要产品：国际标准、技术报告、技术规范、公开规格、技术勘误表和指南。ISO 标准已被许多行业广泛接受，甚至被采纳为各国政府的要求或法律。关于 ISO 的更多信息，访问网站 www.iso.org。

8.3.6　认证和鉴定

要求系统安全的组织需要通过一种或多种方法来评估系统满足安全要求的程度。正式的评估过程被分为两个阶段：认证和鉴定。每个阶段要求的实际步骤取决于组织选择的评估标准。参加 CISSP 考试的考生必须理解每个阶段的要求和通常用于评估系统的标准。这两个评估阶段将在接下来的两节中进行讨论，然后我们会讨论在评定系统的安全性时，必须确定的不同评估标准和需要考虑的事情。认证和鉴定过程用来评估应用程序的有效性，以及操作系统和硬件的安全性。

评估的过程为评价系统在多大程度上达到所期望的安全级别提供了一种衡量方法。因为每个系统的安全级别取决于很多因素，所以在评估过程中必须考虑所有这些因素。即使某个系统一开始就被认为是安全的，安装过程、物理环境和一般配置的详细信息都会对系统达到真正的一般性安全有所影响。由于配置或安装上的差别，两个相同的系统可以在不同的安全级别上进行评估。

提示：

接下来要使用的术语“认证”、“鉴定”和“维护”是美国国防部使用的官方术语，你应当熟悉这些术语。

认证和鉴定是软件和 IT 系统开发过程中的额外步骤，通常美国国防部的承包项目和其他在军事环境中工作的系统都要求执行这样的步骤。美国政府使用的这些术语的官方定义来源于美国国防部指令性文件 5200.40 的附件 2。

1. 认证

整个评估过程中的第一个阶段是认证。认证是对 IT 系统的技术和非技术安全特性以及其他防护措施的综合评估，这能够支持鉴定过程，从而确定特定设计和实现满足一组指定安全要求的程度。

系统认证是对计算机系统的每个部分进行技术性评估，以便评估系统与安全标准是否一致。首先，必须选择评估标准(我们将会在稍后部分探讨可以选择的标准)。一旦选择使用的标准，就要分析每个系统组件，以确定其是否达到所期望的安全目标。认证分析过程包括测试系统的硬件、软件和配置情况。在这个阶段被评估的所有控制包括行政管理控制、技术控制和物理控制。

在评估完整个系统之后，可以对结果进行评估，以便决定系统在当前环境中支持的安全级别。系统的环境是认证分析过程的一个关键部分，因此系统的安全性或多或少地依赖于其所处的环境。安全系统与网络连接的方式会改变系统的安全状况。同样，系统周围的物理安全保护措施也会影响整体的安全等级。因此，在认证系统时，必须全面考虑所有的因素。

在评估完所有的因素和确定系统的安全级别后，认证阶段就完成了。需要记住的是，认证仅对处于特定环境和配置中的系统有效。任何改变都会使认证无效。一旦为某个特定的配置认证了安全等级，就可以准备验收系统了。管理部门通过鉴定过程验收经过认证的系统的安全配置。

2. 鉴定

在认证阶段，我们测试和记录了具有特定配置的系统的安全能力。拥有了这些信息，组织的管理层就会将系统的安全能力与组织的需求进行比较。安全策略中明确指出系统的安全要求是强制性的。管理层审查认证信息并确定系统是否满足组织的安全需求。如果管理层确定系统的认证符合组织的要求，那么系统就通过了鉴定。鉴定是由指定许可机构(Designated Approving Authority，DAA)做出的正式声明，它表明准许 IT 系统使用规定的一组防护措施在可接受的风险级别以特定的安全模式运作。鉴定一旦完成，管理层就可以正式接受被评估系统的总体安全性的适用性。

注意：

认证和鉴定似乎是相似的，因此真正理解它们往往非常困难。可以参照的一个观点是：认证通常是内部的安全验证，只有你所在的组织才相信验证结果；鉴定通常是由第三方测试服务执行的，其结果在信任特定测试组织的所有人看来都是可信的。

认证和鉴定的过程通常是一个不断重复的过程。在鉴定阶段，请求通过改变系统配置或增加控制来解决安全问题的情况时有发生。需要记住的是，只要更改了配置，就必须重新认证新的配置。同样，当经过一段具体的时间后或进行了任何配置变更后，都必须重新认证系统。安全策略应当明确指出什么样的情况需要进行重新认证。优良的安全策略会列出认证有效的时间以及要求重新开始认证和鉴定过程的任何更改。

3. 认证和鉴定系统

目前有下列两种政府标准适用于计算系统的认证和鉴定：目前的美国国防部标准是风险管理框架(RMF，参见 www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf)，它于最近取代了美国国防部信息保障认证认可过程(DIACAP)以及美国国防部信息技术安全认证和认可过程(DITSCAP)；适用于其他所有美国政府行政部门、机构及其承包商和顾问的标准是美国国家安全系统委员会策略 CNSSP，参见 www.ncix.gov/publications/policy/docs/CNSSP_22.pdf，它取代了美国国家信息保障认证和认可过程(NIACAP)。然而，CISSP 可能涉及当前或以前的标准。这些过程都分为 4 个阶段：

阶段 1：定义 涉及适当的项目人员分配、关键需求的记录以及指导整个认证和鉴定过程的系统安全许可协议(System Security Authorization Agreement，SSAA)的注册、协商和创建。

阶段 2：验证 包括细化 SSAA、系统开发活动以及认证分析。

阶段 3：确认 包括进一步细化 SSAA、集成系统的认证评估、DAA 建议的开发以及 DAA 的鉴定结果。

阶段 4：后鉴定 包括维护 SSAA、系统操作、变更管理以及遵从性验证。

由美国国家安全局的信息系统安全组织管理的 NIACAP 过程概述了可以准许的三种不同鉴定类型。根据美国国家安全通信与信息系统安全指定性文件 1000，这些鉴定类型的定义如下：

- 针对系统的鉴定，评估主要的应用程序或通用支持系统。
- 针对场所的鉴定，对位于特定的自包含位置的应用程序或系统进行评估。
- 针对类型的鉴定，评估分布在许多不同位置的应用程序或系统。

8.4 理解信息系统的安全功能

信息系统的安全功能包括内存保护、虚拟化、可信平台模块、接口和容错能力。认真评估基础设施的各方面，并确保充分支撑安全是非常重要的。如果不了解信息系统的安全功能，就不可能对它们进行评估，也不可能恰当地使用它们。

8.4.1 内存保护

内存保护是一个核心的安全组件，必须对它进行设计和在操作系统中加以实现。无论程序是否在系统中执行，它都必须被执行。否则将导致不稳定、完整性的违反、拒绝服务以及信息泄露的结果。内存保护被用于防止活动进程与没有专门指派或分配的内存区域进行交互。

内存保护在整个第 9 章都会被讨论，涉及的主题包括隔离、虚拟内存、分段、内存管理和保护环。

8.4.2 虚拟化

虚拟化技术被用于在单一主机的内存中运行一个或多个操作系统。这种机制允许在任意硬件上虚拟运行任何操作系统，也允许多个操作系统同时工作在相同的硬件上。常见的例子包括 VMware、微软的虚拟 PC、微软虚拟服务器、运行 Windows Server 的 Hyper-V、Oracle 的 VirtualBox、XenServer 以及 Mac 的 Parallels Desktop。

虚拟化有很多好处，比如能够启动单个服务或需要的服务实例，还能实时扩展，以及能够为特殊的服务运行额外的 OS 版本。从用户的角度来看，虚拟化的服务器和服务与传统的服务器和服务是没有区别的。此外，损坏、崩溃或毁坏的虚拟系统的恢复通常很快，只需简单使用干净的备份版本替换虚拟系统的主硬盘文件，然后重新启动就可以了(虚拟化的其他内容和一些相关的风险都包括在第 9 章对云计算的讨论中)。

8.4.3　可信平台模块

可信平台模块(TPM)既是对主板上加密处理器芯片的描述，同时也是描述实施的通用名称。TPM 芯片用于存储和处理加密密钥，从而满足基于硬件支持/实现的硬盘加密系统。一般来说，用硬件实现比用纯软件实现硬盘加密更安全。

当使用基于 TPM 的全磁盘加密技术时，用户/操作员必须提供一个密码或物理 USB 令牌设备给计算机用于身份认证，并允许 TPM 芯片向内存释放硬盘加密密钥。虽然这看上去类似软件实现，但关键的区别是如果硬盘被从原来系统中删除，将不能被解密。只有原来的 TPM 芯片能进行加解密和访问。如果仅用软件硬盘加密，硬盘可以移到一台不同的计算机且没有任何的访问或使用限制。

硬件安全模块(HSM)用于管理/存储数字加密密钥、加速加密操作、支持更快的数字签名，以及提高身份认证的速度。HSM 通常是附加的适配器、外部设备或是 TCP/IP 网络设备。HSM 包括防篡改保护以防止滥用，即便攻击者可以对其进行物理访问。TPM 就是一个 HSM 示例。

HSM 提供大型(2048 位以上)非对称加密计算的加速解决方案，以及密钥存储安全保护。许多认证系统使用 HSM 来存储证书；ATM 和 POS 终端通常采用专有的 HSM；硬件 SSL 加速器可以包括 HSM 支持；兼容 DNSSEC 的 DNS 服务器使用 HSM 提供密钥和区域文件存储。

8.4.4　接口

在应用程序中，使用约束或受限接口的目的是限制用户在基于他们的权限上可以做什么或看到什么。具有全部权限的用户可以访问应用程序的所有功能。有限制权限的用户则被限制访问。应用程序使用不同的方法来限制接口。一个常见的方法是：如果用户没有使用功能的权限，就将功能隐藏。命令可通过菜单或右击一项提供给管理员来使用，但如果普通用户没有权限，命令则不会出现。其他时候命令可被显示，但被变暗或禁用。普通用户虽然可以看到，但无法使用。

约束接口的目的是限制或制止授权和未经授权用户的行为。这接口的使用就是 Clark-Wilson 安全模型的一种实践应用。

8.4.5　容错

容错能力是指系统遭受故障，但能持续运行的能力。容错是添加冗余组件，如在廉价磁盘冗余阵列(RAID)中添加额外的磁盘，或在故障转移集群配置中添加额外的服务器。容错是安全设计的一个基本要素，被认为是避免单点故障和实现冗余的部分措施。关于容错、冗余服务器、RAID 和故障转移解决方案的更详细信息，可参见第 18 章“灾难恢复计划”。

8.5 本章小结

安全系统不仅仅是组装起来；它们需要通过设计来支持安全性。系统的安全性必须通过它们的能力是否支持和执行了安全策略来判断。判断计算机系统的有效性，这一评估过程是认证。认证过程是对系统能力满足设计目标的技术评估。一旦系统已经令人满意地通过了技术评估，组织的管理层就开始对系统进行正式验收。正式的接受过程就是鉴定。

完整的认证和鉴定过程取决于标准评估准则。其中几个标准是为了评估计算机安全系统。最早的 TCSEC 是由美国国防部开发的。TCSEC 也被称为橘皮书，提供了对系统安全组件的功能和保障的评价准则。ITSEC 是 TCSEC 准则的另一个版本并更多用于欧洲国家。无论使用的是哪一个准则，评估过程都包括检查每个安全控制是否符合安全策略。如果系统更好执行了主体对客体访问的良好行为准则，那么安全级别就会越高。

当设计安全系统时，创建安全模型来表示系统将使用的方法，往往有助于实现安全策略。我们在这一章中讨论了几个安全模型。Bell-LaPadula 模型只支持数据的保密性由军队设计并满足军事要求。Biba 模型和 Clark-Wilso 模型以不同的方式应对数据的完整性，这两个安全模型适合于商业应用。

对所有这一切的理解应该根据预防、检测、纠正控制而形成有效的系统安全措施。这就是为什么必须知道访问控制模型及其功能的原因，包括状态机模型、Bell-LaPadula 模型、Biba 模型、Clark-Wilson 模型、信息流模型、非干扰模型、Take-Grant 模型、访问控制矩阵模型以及 Brewer and Nash 模型。

8.6 考试要点

了解每种访问控制模型的细节。了解各种访问控制模型及其功能。状态机模型确保主体访问客体的所有实例都是安全的。信息流模型被设计用于阻止非授权的、不安全的或受限的信息流。非干扰模型能够阻止一个主体的动作影响另一个主体的系统状态或动作。Take-Grant 模型规定了如何将权限从一个主体传递至另一个主体或者从一个主体传递至一个客体。访问控制矩阵是一个由主体和客体形成的表，这个表规定了每个主体能够在每个客体上执行的动作或功能。Bell-LaPadula 主体具有一个许可级别，这个许可级别只允许访问具有相应分类级别的客体。Biba 模型能够防止具有较低安全级别的主体对具有较高安全级别的客体进行写操作。Clark-Wilson 是一个依赖于审计的完整性模型，能够确保未授权的主体无法访问客体以及被授权的用户能够正确地访问客体。Biba 和 Clark-Wilson 模型实现了完整性。Goguen-Meseguer 和 Sutherland 模型关注于完整性。Graham-Denning 模型关注于主体和客体的安全建立和删除。

了解认证和鉴定的定义。认证是从技术角度评估计算机系统的每个部分，从而判断是否与安全标准相一致。鉴定是正式验收已认证的配置的过程。

能够描述开放式系统和封闭式系统。开放式系统是使用行业标准设计的，一般比较容易与其他的开放式系统进行整合。封闭式系统通常是专有硬件和/或软件，它们的设计规范一般不会公开，并且往往较难与其他系统进行整合。

知道限制、界限和隔离的含义。限制是对进程从特定内存地址读取(和写入)数据进行限制。界限是进程在读取或写入数据时不能超越的特定内存地址的范围。隔离是通过使用内存界限而将进程加以限制的一种运行模式。

能够从访问资源的角度定义客体和主体。访问的主体是提出访问资源请求的用户或进程。访问请求的客体是用户或进程希望访问的资源。

了解安全控制的工作原理及功能。安全控制使用访问规则来限制主体对客体的访问。

能够列出 TCSEC、ITSEC 和通用准则的类别。TCSEC 的类别包括已验证保护、强制性保护、自主性保护和最小化保护。表 8.5 概述并比较了 TCSEC、ITSEC 和 CC 的相当且适用的等级(需要记住的是，ITSEC 中从 F7 到 F10 的功能性等级没有对应的 TCSEC 等级)。

定义可信计算基(TCB)。TCB 组合了硬件、软件和控制(形成了实施安全策略的可信基)。

能够解释安全边界。安全边界是想象出来的，用于将 TCB 与系统其余部分分隔的界限。TCB 组件与非 TCB 组件之间的通信使用可信路径。

知道什么是引用监控器和安全内核。引用监控器是 TCB 的逻辑部分，对主体在被授予访问权限之前是否具有使用资源的权限进行确认。安全内核是实现引用监控器功能的 TCB 组件的集合。

了解信息系统的安全功能。常见的安全功能包括内存保护、虚拟化和可信平台模块(TPM)。

8.7　书面实验室

1. 说出至少 7 个安全模型。
2. 描述 TCB 的主要组成。
3. Bell-LaPadula 安全模型的两种主要的规则或原则是什么？另外，Biba 模型的两条规则是什么？
4. 开放式和封闭式系统以及开源和闭源的区别是什么？

8.8　复习题

1. 系统认证是什么？
   A. 正式接受确定的系统配置
   B. 对计算机系统每部分的技术评估，以评估其是否符合安全标准
   C. 对制造商目标的功能评估，为了让每个硬件和软件组件都满足集成标准
   D. 制造商的证明，说明所有组件都被正确安装和配置
2. 系统鉴定是什么？
   A. 正式可接受的系统配置声明
   B. 为了每个硬件和软件组件都满足集成标准，对制造商目标进行的功能评价
   C. 证明计算机系统实施安全策略的可接受的测试结果
   D. 指定两台机器之间的安全通信过程
3. 封闭式系统是什么？
   A. 围绕着最终、封闭或标准设计的系统
   B. 包括工业标准的系统
   C. 使用未公布协议的专有系统
   D. 没有运行 Windows 的任意主机

4. 以下哪一项更好地描述了限制或约束的过程?
   A. 仅可以在有限的时间下运行的过程
   B. 仅可以在一天中的某些时间运行的过程
   C. 仅可以访问某些内存空间的过程
   D. 对客体控制访问的过程
5. 访问客体是什么?
   A. 用户或进程想要访问的资源
   B. 可以访问资源的用户或进程
   C. 有效访问规则的列表
   D. 有限访问类型的序列
6. 安全控制是什么?
   A. 存储了描述客体特性的安全组件
   B. 列出所有数据分类类型的文件
   C. 有效的访问规则列表
   D. 限制访问客体的机制
7. 信息系统安全鉴定的什么类型，是在特定的、独立的位置对应用和系统进行评估?
   A. 系统鉴定
   B. 站点鉴定
   C. 应用鉴定
   D. 类型鉴定
8. TCSEC 标准定义了几种主要类型?
   A. 2
   B. 3
   C. 4
   D. 5
9. 可信计算基(TCB)是什么?
   A. 在网络上支持安全传输的主机
   B. 操作系统内核和设备驱动程序
   C. 硬件、软件和控制结合在一起实现安全策略
   D. 验证安全策略的软件和控制
10. 安全边界是什么?
   A. 围绕系统的物理安全区域的边界
   B. 把 TCB 和系统其他部分隔离的假想边界
   C. 防火墙所在的网络
   D. 计算机系统的任何连接
11. TCB 概念的什么部分验证了在授予每个资源需求权限前的每次访问?
   A. TCB 分区
   B. 信任库
   C. 引用监控器
   D. 安全内核

12. 安全模型的最佳定义是什么？

A. 安全模型描述了组织必须遵循的策略

B. 安全模型提供一个框架来实现安全策略

C. 安全模型是计算机系统每部分的技术评估，以评价与它们一致的安全标准

D. 安全模型是认证配置正式被接受的过程

13. 哪个安全模型建立在状态机模型之上？

A. Bell-LaPadula 和 Take-Grant 模型

B. Biba 和 Clark-Wilson 模型

C. Clark-Wilson 和 Bell-LaPadula 模型

D. Bell-LaPadula 和 Biba 模型

14. 哪个安全模型关注数据的机密性？

A. Bell-LaPadula 模型

B. Biba 模型

C. Clark-Wilson 模型

D. Brewer and Nash 模型

15. 哪个 Bell-LaPadula 属性阻止低级别的主体访问高级别的客体？

A. (星)安全属性

B. 不准向上写属性

C. 不准向上读属性

D. 不准向下读属性

16. Biba 模型的简单属性的含义是什么？

A. 向下写

B. 向上读

C. 不准向上写

D. 不准向下读

17. 当可信主体违反了 Bell-LaPadula 模型的星安全属性时，为了把客体写入低级别，什么可行的操作可能会发生？

A. 扰动

B. 多实例

C. 聚合

D. 移除分类

18. 什么安全方法、机制或模型揭示了一个主体访问多个客体的能力？

A. 职责分离

B. 访问控制矩阵

C. Biba 模型

D. Clark-Wilson 模型

19. 什么安全模型拥有在理论上含有名称或标签的功能，但是在解决方案中实现时，需要安全内核的名称或标签？

A. Graham-Denning 模型

B. Deployment 模型

C. 可信计算基

D. Chinese Wall

20. 下列哪一项不是 Clark-Wilson 模型的访问控制关系的一部分?

A. 客体

B. 接口

C. 编程语言

D. 主体

第 9 章

安全脆弱性、威胁和对策

本章中覆盖的 CISSP 考试大纲包含：

3) 安全工程(安全的工程学和管理)

- E. 评估和缓解安全架构、设计和解决方案元素的脆弱性
  - E.1 基于客户端(例如，applet、本地缓存)
  - E.2 基于服务器(例如，数据流控制)
  - E.3 数据库安全(例如，推理、汇聚、数据挖掘、数据分析、数据仓库)
  - E.4 大规模并行数据系统
  - E.5 分布式系统(例如，云计算、网格计算、点对点)
  - E.6 密码系统
  - E.7 工业控制系统(例如，SCADA)
- F. 评估和缓解基于 Web 的系统(例如，XML、OWASP)的脆弱性
- G. 评估和缓解移动系统的脆弱性
- H. 评估和缓解嵌入式设备和物联网系统(例如，网络使能设备、物联网(IoT))的脆弱性

本书前面的章节中，我们已经涉及了基本的安全原则，以及防止这些原则被破坏的保护机制。我们还研究了一些恶意人士为寻求规避这些保护机制而使用的特定类型攻击。至此，在讨论预防措施时，我们一直专注于策略措施和运行在系统上的软件。然而，安全专业人员也必须认真注意系统本身，并确保他们的更高级别的保护控制不是建立在摇摇欲坠的基础之上。毕竟，如果运行中的计算机存在简单的安全漏洞，并允许恶意人士轻易地完全绕过防火墙，那么即使世界上最安全的防火墙配置也不会发挥一点儿作用。

在本章中，通过开展一项被称为计算机架构的简单调查，我们将涉及这些潜在的安全关注点：计算机不同组件的物理设计。我们会从安全角度检查计算系统每一个主要的物理组件，包括硬件和固件。显然，由于受资源和时间的限制，对系统硬件组件的详细分析不会很多。然而，所有的安全专业人员都应该对这些概念至少有个基本的了解，以防止在遇到降低系统设计水平的安全事件时不知所措。

安全工程领域涉及广泛的关注点和问题，包括安全设计元素、安全体系结构、漏洞、威胁以及相关的对策。这个领域的其他元素在各章节中都有讨论：第 6 章“密码学与对称密钥算法、第 7 章

“PKI 和密码学应用”、第 8 章“安全模型的原则、设计和功能”、第 10 章“物理安全需求”。请务必回顾所有这些内容以便对这一领域的问题有个完整的了解。

9.1 评估和缓解安全脆弱性

计算机体系结构是从逻辑层次考虑的计算系统的设计和构造的工程学规范要求。许多学院的计算机工程和计算机科学专业在教学中发现，用一个学期的课程介绍计算机体系结构的基本原则是很难完成的，因此在大学阶段，相应课程经常需要两个学期才能完成。计算机体系结构课程在位级别研究 CPU 组件、内存设备、设备通信和类似主题的设计，为只进行“0”或“1”判断的单独逻辑设备定义处理路径。大多数安全专家不需要理解到这么深的程度，这些内容已经超出本书和 CISSP 考试的范围。但是，如果工作涉及这个级别的计算系统的设计的安全方面，那么建议应当更深入地研究该领域的相关知识。

初步探讨的计算机体系结构似乎与 CISSP 无关，但是大部分的安全体系结构和设计元素都基于对计算机硬件的坚实理解和实现。

提示：

系统越复杂，提供的保证越少。更多的复杂性意味着更多存在漏洞的区域以及更多需要防范威胁的区域。更多的漏洞和威胁意味着系统随后提供安全的可信度更低。

9.1.1 硬件

任何计算处理专业人士都熟悉硬件的概念。与建筑业一样，硬件是组成计算机的物理“材料”。术语“硬件”包含计算机可以实际触摸到的任何有形部分，范围从键盘、显示器到CPU、存储介质和内存条。需要小心的是，虽然存储设备(如硬盘或闪存)的物理部分可以认为是硬件，但是在这些设备里存储的、构成软件和数据的0和1集合就不属于硬件了。毕竟，无法触摸到计算机的内部，然后将一些比特和字节分离出来!

1. 处理器

通常被称为处理器的 CPU 是计算机的神经中枢，是一个芯片或多个芯片(在多处理器系统中)，负责管理所有重要的计算操作，并且直接执行或协调复杂的计算工作，从而使计算机完成预定的任务。令人惊讶的是，虽然允许计算机执行复杂的任务，但 CPU 实际上都只能执行有限的计算和逻辑操作集。操作系统和编译器负责将用于设计软件的高级编程语言翻译为 CPU 能够理解的简单汇编语言指令。限制功能的范围是有目的的：这允许 CPU 以极快的速度执行计算和逻辑操作。

注意：

对于这些年来关于计算机技术数量级的发展，可以参见 http://en.wikipedia.org/wiki/Moore's_law 上对摩尔定律的描述。

2. 执行类型

由于计算机的处理能力不断增强，因此用户对计算机有了更高的功能要求，他们希望系统用更快的速度处理信息，并且能够同时处理多种功能。于是，计算机工程师设计出了满足这些需求的一

些方法。

提示：

乍看起来，术语“多任务处理”、“多处理”、“多程序设计”和“多线程处理”似乎完全相同。然而，它们所描述的“同时办两件事”问题的方式有很大的不同。我们强烈建议你多花一些时间来仔细研究这些术语之间的差别，直到熟悉它们为止。

多任务处理　在计算处理中，多任务处理指的是同时处理两个或更多个任务。事实上，大多数系统并不是真正的多任务处理系统，它们依靠操作系统，通过仔细构造发送给 CPU 执行的命令的顺序来模拟多任务处理。毕竟，当处理器正在以几千兆赫兹的速度进行处理并发出嗡嗡声时，很难判断是在任务之间进行转换(而非同时处理两个任务)。不过，可以认定多任务处理系统在任意给定时间都能够应付多个任务或进程。

多处理　在多处理环境中，多处理器计算系统(也就是具有多个 CPU 的系统)利用多个处理器的能力完成一个应用程序的处理任务。例如，数据库服务器能够运行在包含三个处理器的系统上，如果数据库应用程序同时接收到多条独立的查询指令，那么它就可以将每条查询指令发送给不同的处理器去执行。

在具有多个 CPU 的现代系统中，具有两种常见的多处理系统类型。在刚才描述的场景中，单个计算机包含多个由一个操作系统控制的处理器，这被称为对称多处理(Symmetric MultiProcessing，SMP)。在 SMP 中，处理器不但共享通用操作系统，而且共享通用数据总线和内存资源。在这种结构类型中，系统可以使用很多个处理器。幸运的是，这种类型的计算能力足以驱动大多数系统。

某些计算密集的操作处理(例如，那些支持科学家和数学家进行研究的计算操作)要求的处理能力是一个操作系统无法独立提供的。这样的计算操作通常由一种被称为大规模并行处理(Massively Parallel Processing，MPP)的技术提供。MPP 系统中驻留了数百个甚至上千个处理器，每个处理器都具有自己的操作系统和内存/总线资源。当协调整个系统的活动并调度处理的软件遇到某个计算密集任务时，会分配某个处理器负责完成任务。这个处理器随后将任务分解为若干易于处理的部分，并把这些部分分配给其他处理器执行。那些处理器将它们的计算结果返回至协调处理器，所有计算结果在协调处理器中被重新组合并返回给提出请求的应用程序。MPP 系统的能力非常强大(不用说，成本也十分高昂)，并且是很多计算研究中使用的主要系统。

多处理系统的这两种类型都具有各自独特的优点，并且适用于不同的情况。SMP 系统非常适合以极高的速度处理简单的计算操作，而 MPP 系统适合处理庞大和复杂的计算密集任务，能将大的任务分解成若干子任务并分配给不同的处理器进行计算。

下一代多处理系统

在双核与四核处理器出现之前，创建多处理系统的唯一方式是在母板上放置两个或多个 CPU。不过，现在有了若干多核选项，这样母板上的单个 CPU 芯片就存在两条或 4 条(甚至更多条)执行路径。因为允许同时执行两个(或多个)计算，所以确实准许存在只具有单个 CPU 的多处理系统。

多程序设计　多程序设计与多任务处理非常相似。为了达到提高计算效率的目的，多程序设计通过操作系统对单个处理器上的两个任务进行协调，从而模拟两个任务同时执行的情况。在很大程度上，多程序设计是一种批量或连续执行多个进程的方式，这样一来，一个进程结束并在外围等待，其状态会被保存，同时开始处理下一个进程。同一批中的其他所有进程依次执行完成并在外围等待

之前，第一个程序并不返回进行处理。对任何单个程序来说，这种方法在完成某个任务时会导致显著的延迟。不过，对于同一批中的所有进程而言，完成所有任务所需的总时间会减少。

多程序设计被认为是一种相对过时的技术，除了在比较旧的系统中能够找到，如今已经很少使用了。多程序设计和多任务处理技术之间存在下列两个主要差异：

- 多程序设计通常在大规模系统(例如，大型机)中使用，而多任务处理在个人计算机操作系统(例如，Windows 和 Linux)中使用。
- 多任务处理通常由操作系统协调使用，而多程序设计则要求特别编写的软件，这种软件通过操作系统来协调自己的活动和执行。

多线程处理 多线程处理允许在单个进程中执行多个并发任务。与多个任务占用多个进程的多任务处理不同，多线程处理允许在单个进程中执行多个任务。线程是一个自包含的指令序列，可以与作为同一父进程一部分的其他线程并行执行。多线程处理常用于这样的应用程序：多个活动进程之间频繁的上下文切换会带来过大的开销并且降低系统效率。使用多线程处理技术，线程之间转换的开销会大大降低，因此更有效率。例如，在现代 Windows 实现中，在单个进程内从一个线程转换到另一个线程所涉及的开销大约为 40 到 50 条指令，并且不需要转移大量内存空间。相比之下，从一个进程转换到另一个进程所涉及的开销大约为 1000 条或更多条指令，并且还需要转移大量内存空间。

使用多线程处理的一个优秀例子是在一个字处理程序中同时打开多个文档。在这种情况下，实际上并没有运行字处理器的多个实例，如果多个实例同时运行，对系统的要求会很高。相反，每个文档都被视为单个字处理器进程的一个线程，并且在任何给定时间由软件选择要处理的线程。

事实上，对称多处理系统在操作系统级别使用线程。在刚才描述的字处理示例中，操作系统还包含许多控制所分配任务的线程。在单处理器系统中，操作系统每次向处理器发送一个线程进行处理。SMP 系统向每一个处理器都发送一个线程并同时加以执行。

3. 处理类型

许多安全要求较高的系统控制着被分配了不同安全级别的信息的处理任务，例如，美国政府为与国防相关的信息指派的分类级别：非保密、敏感、机密、秘密和绝密。设计计算机时一定要使用这种方法，这样就不会因疏忽把信息泄漏给未经授权的接收方。

计算机体系架构师和安全策略管理员从两个不同的方面抨击了处理器级别存在的问题。一方面是策略机制，而另一方面则是硬件解决方案。稍后两部分内容将研究这两方面的问题。

单一状态 单一状态系统要求使用策略机制来管理不同安全级别的信息。在这种类型的方案中，安全管理员准许处理器和系统每次只处理一个安全级别的问题。例如，某个系统可能被标记为只处理秘密级别的信息。这样一来，该系统的所有用户都被准许在秘密级别处理信息，从而将保护系统要处理的信息的责任从硬件和操作系统转移到控制访问系统的系统管理员的身上。

多态 多态系统能够实现更高的安全级别。这些系统是被认证过的，通过使用特定的安全机制(如本章稍后讨论的“保护机制”一节中的内容)同时处理多个安全级别。这些安全机制被设计用于阻止信息跨越不同的安全级别。某用户可能正在使用多态系统处理秘密级别的信息，同时，另一个用户正在处理绝密级别的信息。技术方面的机制能够阻止信息在这两个用户之间的交叉使用，因此也阻止了信息在不同安全级别间的交叉。

在实际应用中，因为实现必要的技术性机制的费用较高，所以多态系统的使用相对不太普遍。实现必要技术性机制的费用在某些时候被证明是值得的。无论如何，处理非常昂贵的资源(例如，大规模并行系统)时，获得多个系统的成本远远超出了实施必要的额外安全控制以便在单个系统上支持

多态操作的成本。

4. 保护机制

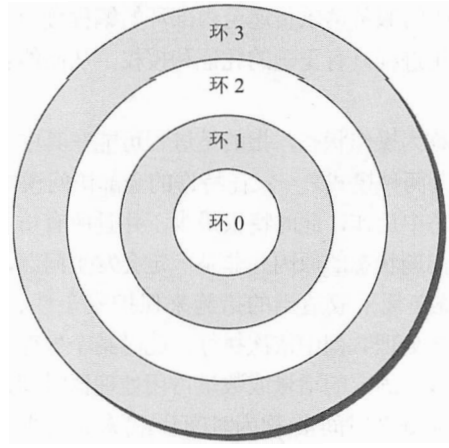
如果计算机没有运行，那么它就是一堆不能完成任何工作的塑料、硅和金属材料。计算机在运行时管理着运行时环境，运行时环境表示操作系统和活动的应用程序的组合。在运行时，计算机还能够根据用户的安全许可访问文件和其他数据。在运行时环境中，必须集成安全信息和控制来保护操作系统本身的完整性、管理被允许访问特定数据项的用户、授权或拒绝对这些数据的操作请求等。运行中的计算机在运行时实现和处理安全性的方式可以被大体描述为一个保护机制的集合。接下来会介绍各种保护机制，包括保护环、操作状态和安全模式。

提示：

因为计算机实现和使用保护机制的方式对于维护和控制安全性来说十分重要，所以读者应当理解下面将要介绍的三种保护机制(保护环、操作状态和安全模式)的定义及表现。因为这些内容十分重要，所以考试中很可能出现与这三种保护机制相关的细节问题。

保护环　保护环是一种虽然陈旧但却良好的方案，它使我们回想起使用 Multics 操作系统的时代。这种实验性的操作系统是由 Bell 实验室、MIT 和通用电气在 1963 年到 1969 年之间合作设计和构建的。尽管只是在 Honeywell 实现中得到了商业应用，不过 Multics 为计算领域带来了两个持久深远的影响。首先，Multics 导致简单的、复杂程度较低的 Unix 操作系统(针对 Multics 的文字游戏)的出现；其次，引入了操作系统设计中的保护环的概念。

从安全性的观点出发，保护环将操作系统中的代码和组件(以及应用程序、实用程序或由操作系统控制运行的其他代码)组织在如图 9.1 所示的同心环内。越进入圆环的内部，与占据特定环的代码相关联的特权级别就越高。尽管最初的 Multics 实现最大允许 7 环(从 0 到 6 进行编号)，然而现代操作系统使用的是具有 4 环(从 0 到 3 进行编号)的模型。



环 0：OS 内核/内存(驻留组件)
环 1：其他 OS 组件
环 2：驱动程序、协议等
环 3：用户级程序和应用程序

环 0-2：在监管或特权模式中运行
环 3：在用户模式中运行

图 9.1　保护环

作为最内部的环，环 0 具有最高的特权级别，并且基本上可以访问任何资源、文件或内存位置。操作系统始终驻留在内存中的部分(因此能够根据需要随时运行)被称为内核(kernel)。内核占据着环 0，并且优先占有在其他环上运行的代码。在请求各种任务、执行操作、切换进程时进出内存的操作系统的剩余部分占据着环 1。环 2 在一定程度上也是特许的，这个环驻留了 I/O 驱动程序和系统实用程序，它们能够访问应用程序和其他程序本身不能直接访问的外围设备、特殊文件等。应用程序和其他程序占据着最外层的环 3。

环模型的本质在于优先权、特权和内存分割。希望执行的任何进程必须排队等待(进程暂挂队列)。与最小环号相关联的进程总是比与较大环号相关联的进程先运行。在较低编号的环中的进程能够比较高编号的环中的进程访问更多的资源，并且能够更直接地与操作系统交互。在较高编号的环上运行的进程通常必须请求较低编号的环中的处理程序或驱动程序来获得需要的服务，有时这被称为居间访问模型。在最严格的实现中，每个环都具有自己关联的内存段。因此，较高编号的环中的进程对较低编号的环中的任何地址请求，都必须请求与该地址相关联的环中的某个辅助进程。在实践中，许多现代操作系统只将内存分为两段：一段用于系统级访问(环 0 到环 2)，常常被称为内核模式或特权模式；另一段则用于用户级程序和应用程序(环 3)，常常被称为用户模式。

从安全性的观点出发，环模型使得操作系统能够将自身与用户和应用程序隔离开并加以保护，还允许在高特权操作系统组件(例如，内核)和低特权操作系统部分(例如，操作系统的其他部分以及驱动程序和实用程序)之间实施严格的界线。在这种模型中，对特定资源的直接访问只能在特定的环中进行；同样，特定的操作(例如，进程的切换、终止和调度)也只被允许在特定的环内执行。

某个进程所占据的环决定了该进程对系统资源的访问级别(并且决定了必须从较低编号、特权更多的环内的进程中请求何种资源)。只有当客体驻留在进程自己的环内或驻留在当前边界外部的某些环内时，进程才可以直接访问这些客体(以数值方法为例，这意味着位于环 1 的某个进程能够直接访问自己环内的资源以及与环 2 和环 3 关联的任何资源，但是不能访问只与环 0 关联的任何资源)。凭借居间访问(也就是前面刚提到的驱动程序或处理程序请求)的机制常常被称为系统调用，并且往往涉及调用特定的系统或设计用于将服务请求传递至内部环的编程接口。然而，在接受这样的请求之前，调用环必须检查并确认调用进程具有正确的凭证和授权，从而能够访问数据和执行满足请求所涉及的操作。

进程状态　进程状态也被称为操作状态，指的是进程可能在其中运行的各种执行形式。在任意给定时刻，操作系统都处于下列两种模式之一：在特许的全部访问模式(也被称为监管状态)中运作；在与用户模式相关联的问题状态中运作，此时特权最少，并且所有访问请求在被授予或拒绝之前必须检查授权凭证。后者被称为问题状态的原因并非是一定会发生问题，而是因为用户访问的未许可状态意味着会发生问题，系统必须采取适当的措施来保护安全性、完整性和机密性。

在操作系统中，进程排列在处理队列中依次执行，此时某个处理器在可用时会调度这些进程的执行。许多操作系统只允许进程以固定的增量或数量占用处理器时间，某个新进程被创建时首先会进入处理队列，如果占用了整个处理时间量(称为时间片)仍未完成执行，那么这个进程就会返回处理队列并等待下一轮继续执行。此外，进程调度程序常常会选择执行具有最高特权的进程，因此排在最前面的进程并不保证能访问 CPU(因为具有较高优先权的进程会在最后时刻被抢先执行)。

根据进程是否运行，进程可以运作在下列几种状态之一：

就绪状态　在就绪状态中，进程准备在被调度执行时立刻继续或开始处理。在进程到达这个状态时，如果 CPU 可用，那么进程就会直接转移到运行模式；如果 CPU 不可用，那么进程就停留在就绪状态直至 CPU 可用。这个状态意味着：拥有立即开始执行所需的所有内存和其他资源。

等待状态　等待状态还可以被理解为“等待某种资源”，也就是说，进程准备继续执行，但是在能够继续处理之前需要等待某台设备或访问请求(某种中断)提供服务(例如，要求从文件中读取记录的某个数据库应用程序必须等待文件被定位和打开，以及查找到正确的记录集)。一些引用将此状态标记为阻塞状态，因为该状态可以阻止进一步的执行，直到某个外部事件发生为止。

运行状态　运行中的进程在 CPU 中执行直至完成、时间片到期或由于某些原因而阻塞(通常是由于生成访问设备或网络的中断并且等待中断完成)。如果进程在时间片结束时尚未完成，那么进程就会返回就绪状态并在队列中排队；如果在等待资源变得可用时阻塞进程，进程便进入等待状态并排队。

提示：

运行状态也被称为问题状态。不过，千万不要将术语“问题”与错误关联在一起。相反，可以将问题状态视为解决某个数学问题以便寻求答案。但需要记住的是，运行状态被称为问题状态是因为可能发生问题或错误，就像回答数学问题可能出错一样。问题状态不同于监管状态，因此在发生错误的事件时不会轻易影响整个系统的稳定性，而只是进程出现错误。

监管状态　在进程必须执行的动作要求大于问题状态特权组的特权时(包括更改系统配置、安装设备驱动程序或更改安全设置)，就需要使用监管状态。基本上，没有在用户模式(环3)或问题状态中出现的功能会在监管模式中实现。

停止状态　进程结束或者由于发生错误、所请求资源不可用或无法满足资源请求而必须终止时，就会进入停止状态。此时，操作系统可以恢复所有内存和被分配的其他资源，从而允许其他进程根据需要处理和重用这些内存和资源。

图 9.2 说明了各种状态之间的联系。新进程总是转移到就绪状态。从那里开始，就绪的进程常常转移到运行状态。在运行时，如果完成或终止，就进入停止状态；如果等待另一个时间片，就返回就绪状态；或者转移到等待状态，一直等到得到请求的资源为止。在决定接下来要运行的进程时，操作系统会查看等待队列和就绪队列，从而执行优先级最高并且准备运行的作业(因此，只有挂起请求已得到满足或即将得到满足的等待作业才会被考虑)。被称为程序执行或进程调度程序的内核特殊部分始终在内存中等待，这样在必须发生进程状态转移时就能够介入和处理所涉及的技术性细节。

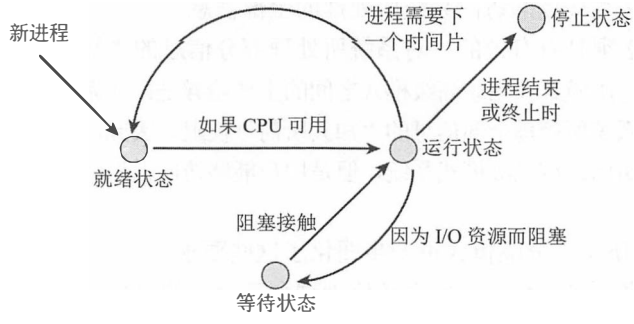


图 9.2　进程调度程序

在图 9.2 中，进程调度程序管理在就绪状态和等待状态中等待执行的进程，并且决定运行的进程在转移至另一个状态(就绪状态、等待状态或停止状态)时所发生的情况。

安全模式　美国政府为处理分类信息的系统指派了 4 种被批准的安全模式。后面的部分会讲述这几种模式。在第 1 章中，我们介绍过美国联邦政府使用的分类系统以及安全认可和安全批准的概

念。在这种环境中，唯一的新术语是“知其所需”(need to know)，指的是一种访问授权方案。在这种方案中，主体对客体的访问不仅仅考虑了特权级别，而且还考虑了涉及主体扮演角色(或执行作业)的数据的相关性。这表明主体需要访问客体，从而正确执行作业或扮演特定的角色。无论具有怎样的特权级别，不具备“知其所需”能力的主体都无法访问客体。如果需要回忆这些概念，那么请在开始学习这些内容之前复习第 1 章相关的知识。在能够部署安全模式之前，必须存在下列三种特定的元素：

- 分层的 MAC 环境
- 对能够访问计算机控制台的主体的完全物理控制
- 对能够进入计算机控制台所在房间的主体的完全物理控制

提示：

你可能很少在政府机构和公司以外的地方遇到下列模式。然而，你可能在其他环境中发现这个术语，所以建议你最好记住它。

专用模式 专用模式系统本质上相当于本章前面“处理类型”中描述的单一状态系统。对于专用系统的用户来说，存在下列三个要求：

- 每个用户都必须具有允许访问系统所处理全部信息的安全许可。
- 每个用户都必须被批准访问系统所处理的全部信息。
- 每个用户都必须具有有效的、对系统所处理全部信息的“知其所需”权限。

注意：

在所有这些模式的定义中，我们都使用了简要的短语“系统处理的全部信息”。正式的定义更为全面，并且使用了短语“处理、存储、转移或访问的所有信息”。如果希望进行更深入的研究，那么可以查看 *Department of Defense 8510.1-M DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Manual*。

系统高级模式 如下所示，系统高级模式的用户需要满足的要求稍有不同：

- 每个用户都必须具有允许访问系统所处理全部信息的有效安全许可。
- 每个用户都必须被批准访问系统所处理的全部信息。
- 每个用户都必须具有有效的、对系统所处理部分信息的“知其所需”权限。

需要注意的是，专用模式和系统高级模式之间的主要差异是：在系统高级模式的计算设备上，所有用户不必具有对系统所处理全部信息的“知其所需”权限。因此，尽管同一用户既可以访问专用模式系统，也可以访问系统高级模式系统，但是用户能够访问前者的所有数据，却被限制访问后者的部分数据。

分隔模式 如下所示，分隔模式进一步弱化了这些要求：

- 每个用户都必须具有允许访问系统所处理全部信息的有效安全许可。
- 每个用户都必须被批准访问系统中所需要访问的任何信息。
- 每个用户都必须具有有效的、对系统中所需要访问的所有信息的“知其所需”权限。

需要注意的是，分隔模式和系统高级模式之间的主要差异是：分隔模式系统的用户不必被批准访问系统中的全部信息。然而，与系统高级模式系统和专用模式系统一样的是，分隔模式系统的所有用户仍然必须具有适当的安全许可。在名为分隔模式工作站(Compartmented Mode Workstations，

CMW)的分隔模式的特殊实现中，具有必要许可的用户能够同时处理多个分隔部分的数据。

CMW 要求在客体上放置两种安全标签：敏感度级别和信息标签。敏感度级别描述了必须在哪个级别保护客体。敏感度级别在 4 种安全模式中很常见。信息标签能够防止数据分类过高，并且将额外的信息与客体关联在一起，这有助于进行与访问控制无关的适当、准确的数据标签操作。

多级模式　政府对多级模式系统的定义与前面给出的技术上的定义非常相似。然而，出于一致性的缘故，我们会使用术语许可、访问批准和“知其所需”进行表示，如下所示：

- 某些用户不具有访问系统所处理全部信息的有效安全许可。因此，访问由主体的许可级别是否优于客体的敏感度级别控制。
- 每个用户都必须被批准访问系统中所需要访问的所有信息。
- 每个用户都必须具有有效的、对系统中所需要访问的所有信息的“知其所需”权限。

在查看美国联邦政府批准的各种操作模式的要求时，你会注意到：当我们从专用系统向下转移到多级系统时，控制访问系统的用户类型的行政管理要求不断降低。然而，这不会降低限制个人访问的重要程度，这样用户只能获得授予他们的合法信息。正如在前一节中讨论的那样，这仅仅是将强制实施这些要求的责任从管理人员(他们采用物理方式限制对计算机的访问)转移到硬件和软件(它们控制多用户系统中每一位用户可以访问的信息)上。

注意：

多级安全模式也被称为受控的完全模式。

根据所需的安全许可、“知其所需”权限以及处理多许可级别数据(PDMCL)的能力，表 9.1 概述和比较了这 4 种安全模式。比较这 4 种安全模式时，我们通常认为多级模式暴露出最高的风险级别。

表 9.1　安全模式的比较

模式	安全许可	知其所需	PDMCL
专用模式	相同	无	无
系统高级模式	相同	是	无
分隔模式	相同	是	是
多级模式	不同	是	是

在表 9-1 中，如果所有用户都必须拥有相同的安全许可，那么安全许可为相同，否则为不同。如果没有被应用，或者虽然被应用但是所有用户对系统中存在的所有数据都具有“知其所需”权限，那么“知其所需”权限就为“无”；如果访问受到“知其所需”约束的限制，那么“知其所需”权限就为“是”。如果使用了 CMW 实现，那么 PDMCL 就为“是”，否则为“无”。

5. 操作模式

现代处理器和操作系统被设计为能够支持多用户环境，在这种环境中，个人计算机用户没有被授予访问系统所有组件或系统所存储全部信息的权限。基于这个原因，处理器本身支持两种操作模式：用户模式和特权模式。

用户模式　用户模式是在执行用户应用程序时 CPU 使用的基本模式。在这种模式中，CPU 只允许执行其整个指令集中的部分指令。这样设计的目的是防止用户因为执行设计得很差的代码或无意识地滥用代码而意外损坏系统，此外还保护系统及其数据免遭怀有恶意用户的攻击，这些恶意用

户可能企图通过执行精心设计的指令来避开操作系统设置的安全措施，也可能错误地执行会导致未授权访问、损害系统或有价值信息资产的动作。

用户模式内的进程常常在被称为虚拟机(VM)或虚拟子系统机的受控环境内执行。虚拟机是操作系统创建的模拟环境，能够为程序提供安全有效的执行场所。每个 VM 都与其他 VM 相隔离，并且每个 VM 都具有自己指定的内存地址空间，托管的应用程序能够使用这些空间。特权模式(也称为内核模式)中的元素负责创建和支持 VM 以及防止某个 VM 中的进程干扰其他 VM 中的进程。

特权模式 CPU 也支持特权模式，这种模式被设计用于授予操作系统访问 CPU 所支持完整指令的特权。这种模式具有很多名称，根据 CPU 制造厂商的不同，确切的术语也不同。下面列出了一些比较常见的名称：

- 特权模式
- 监管模式
- 系统模式
- 内核模式

无论使用哪个术语，基本的概念都是相同的：这种模式为在 CPU 上执行的进程授予范围很广的特权。由于这个原因，设计良好的操作系统不允许任何用户应用程序在特权模式中执行。出于安全性和系统完整性的目的，只有那些作为操作系统组成部分的进程才被允许在特权模式中执行。

提示：

不要混淆处理器模式与任何用户访问特权类型。事实上，高级处理器模式有时被称为特权模式或监管模式，与用户的角色毫无关系。所有的用户应用程序(包括系统管理员的应用程序)都在用户模式中运行。当系统管理员使用系统工具更改系统配置时，这些工具也在用户模式中运行。当用户应用程序需要执行某个特许动作时，会使用系统调用向操作系统传递请求，操作系统对请求进行评估，随后要么拒绝请求，要么同意请求并使用用户控制之外的某个特权模式进程予以执行。

9.1.2 存储器

系统中的第二个重要硬件组件就是存储器，它是计算机为了保持信息使用的便捷所需的存储位置。目前存在许多不同类型的存储器，每种存储器适用于不同的目的，接下来我们将介绍这些存储器。

1. 只读存储器

顾名思义，只读存储器(Read-Only Memory，ROM)就是 PC 能够读但是不能修改(也就是不允许写)的存储器。标准 ROM 芯片的内容在出厂时就被“烧入”，并且终端用户无法改变其中的内容。ROM 芯片通常包含“自引导指令”信息，也就是计算机在从磁盘上加载操作系统之前用于启动的信息。“自引导指令”信息包含为人熟知的每次引导 PC 时运行的通电自检(Power-On Self-Test，POST)系列诊断程序。

ROM 的主要优点在于不能被修改。用户或系统管理员意外发生的错误无法清除或修改芯片上的内容，这个特性使得 ROM 特别适于协调计算机最内层的工作。

有一种 ROM 类型可以被系统管理员在一定范围内予以修改，这种 ROM 被称为可编程只读存储器(Programmable Read-Only Memory，PROM)，并且具有如下所示的几种子类型：

可编程只读存储器 基本的可编程只读存储器(PROM)芯片在功能上与 ROM 芯片非常相似，但

是存在一个例外。在制造过程中，PROM 芯片的内容没有在工厂被“烧入”，这一点与标准的 ROM 芯片不一样。相反，PROM 芯片并入了特殊的功能，允许终端用户稍后在芯片中烧入内容。然而，烧入过程具有相似的结果：一旦数据被写入 PROM 芯片，那么就不能再被更改。本质上，PROM 芯片与 ROM 芯片的功能一样。

PROM 芯片为软件开发人员提供了一个在高速的、定制的存储芯片中永久存储信息的机会。PROM 芯片被普遍用于需要某些定制功能的硬件开发应用中，但是一旦被编程就无法再进行修改。

可擦除可编程只读存储器(Erasable PROM，EPROM)　由于 PROM 芯片相对昂贵并且软件开发人员希望能在写入数据之后修改他们的代码，于是人们开发出了可擦除 PROM(EPROM)。在这些芯片上有一个很小的窗口，当用特殊的紫外线光照射时就可以擦除芯片上的内容。这个过程完成后，终端用户就可以将新的信息烧入 EPROM，就像它之前从未编程一样。

电可擦除可编程只读存储器(Electronically ERPOM，EEPROM)　尽管有了一些擦除功能，但是 EPROM 的擦除过程仍然有些麻烦。擦除操作要求从计算机上物理拆除芯片并暴露在一束特殊的紫外线光之下。电可擦除 PROM(EEPROM)是另一种更灵活的、更友好的解决方案，使用送到芯片引脚上的电压强制进行擦除。擦除 EEPROM 时，不用从计算机上拆除芯片，这就比标准的 PROM 和 EPROM 芯片更具吸引力。

闪存　闪存是 EEPROM 的衍生概念。它是一种非易失性存储媒体，可以进行电子擦除和重写。EEPROM 和闪存主要的区别是，EEPROM 必须完全擦除后才能重写，而闪存可以以块或页的方式进行擦写。闪存是最常见的 NAND 闪存，被广泛用于存储卡、优盘、移动设备和 SSD(固态硬盘)。

2. 随机存取存储器

随机存取存储器(Random Access Memory，RAM)是可读和可写的存储器，包含计算机在处理过程中使用的信息。只有当电源持续不断供应时，RAM 才能保存其内容。与 ROM 不一样的是，当计算机电源关闭时，存储在 RAM 内的所有数据都会消失。因此，RAM 只被用于暂时存储数据。任何关键数据都不能只存储在 RAM 中；而是始终应当在另外的存储设备上保留备份副本，以防电源突然中断导致发生数据丢失的事件。下面是 RAM 的几种类型：

实际的存储器　实际的存储器(也被称为主存储器)通常是计算机中可用的最大的 RAM 存储资源。实际的存储器一般由许多动态的 RAM 芯片组成，因此，CPU 必须定期对它们进行刷新(要了解更多的信息，请参看真实场景“动态 RAM 与静态 RAM”)。

高速缓存 RAM　计算机系统包含许多高速缓存。通过将数据从速度较慢的设备取出并暂时存储在高性能的设备上，以便在希望时可以重复使用。高速缓存能够提高系统的性能，这称为高速缓存 RAM。处理器通常包含一个位于主板上的高速缓存，这个极快速的存储器被用于保持将要操作的数据。这个板上或第 1 级的高速缓存往往由不同芯片上的某个静态 RAM 高速缓存(被称为第 2 级高速缓存)进行备份，第 2 级高速缓存保存来自计算机主存储器的数据。类似地，主存储器中通常包含存储在磁性介质上的高速缓存信息。这条存储链连续向下经过存储器/存储设备层次结构，从而使得计算机能够通过保持即将使用的数据(用于 CPU 指令、数据获取、文件访问或其他操作)更容易获得来改善性能。

许多外围设备也使用主板高速缓存来减轻它们对计算机和操作系统造成的负担。例如，许多更高端的打印机包含非常大的 RAM 高速缓存，这样操作系统可以快速假脱机一项作业给打印机，并且随后可以忘记这个打印作业，也不必等待打印机对所有的请求产生输出结果。打印机可以预处理来自主板高速缓存的信息，从而释放计算机和操作系统继续执行其他任务。

真实场景

动态 RAM 与静态 RAM

目前有两种主要类型的 RAM：动态 RAM 和静态 RAM。绝大多数计算机都包含这两种 RAM，并且根据不同的目的对它们加以使用。

为了存储数据，动态 RAM 使用了一系列电容器，这些微小的电子设备能够保持电荷。电容器可能保持电荷(在内存中表示为比特 1)，也可能没有电荷(表示为比特 0)。但是，随着时间的流逝，电容器会自然放电，所以 CPU 必须花费时间来刷新动态 RAM 的内容，从而确保比特 1 不会无意中变为比特 0，以免改变存储器中的内容。

静态 RAM 建立在更加复杂的技术之上，即可以用于任何目的和用途的逻辑设备：触发器(flip-flop)。触发器是一个 ON/OFF 开关，必须把开关从一端拔到另一端，让比特从 0 转换到 1，反之亦然。因此，只要有电源供应，静态存储器就一直保存其中的内容，并且不需要 CPU 定期进行刷新。

在价格上，因为电容器比触发器便宜，所以动态 RAM 比静态 RAM 便宜。但是，静态 RAM 的运行速度比动态 RAM 快得多。对于系统设计人员来说，这就产生了权衡性能价格的问题，因此系统设计者通常会使用静态 RAM 与动态 RAM 相组合的方式，从而达到费用与性能的平衡。

3. 寄存器

CPU 还包括一种有限容量的板上存储器，即寄存器。在执行计算或处理指令时，寄存器为 CPU 的核心部分(也就是算术逻辑单元(Arithmetic-Logical Unit，ALU))提供可直接访问的存储位置。事实上，除了数据作为指令的一部分直接提供外，ALU 操纵的任何数据必须被载入寄存器。这种存储器类型的主要优点是 ALU 本身的一部分，因此计算速度与标准的 CPU 速度一致。

4. 存储器寻址

当利用存储器资源时，处理器必须具有引用存储器中不同位置的方法。解决这个问题的办法被称为寻址，并且在不同的环境中存在多种不同的寻址方案。接下来我们将讨论 5 种比较常用的寻址方案：

寄存器寻址 前面曾经提到过，寄存器直接安装在 CPU 上的非常小的存储位置。当 CPU 需要从某个寄存器中获得信息来完成操作时，可以使用寄存器地址(例如，“寄存器 1”)去访问寄存器的内容。

立即寻址 就其本身而言，立即寻址并不是一种技术上的存储器寻址方案，而是引用某些数据的一种方法，这些数据作为指令的一部分提供给 CPU 使用。例如，CPU 可能处理命令“将寄存器 1 中的数值与 2 相加”。这条命令使用两种寻址方案。第一种方案是作为命令一部分的直接寻址，即告诉 CPU 将数值 2 加进去并且不需要从某个存储器位置检索该数值。第二种方案是寄存器寻址，即命令 CPU 从寄存器 1 中取出数值。

直接寻址 在直接寻址中，要访问的存储器位置的实际地址会被提供给 CPU。这个地址必须与正在执行的指令位于相同的存储页面上。因为与重新编写立即寻址的硬编码数据相比，存储位置的内容能够更容易地被改变，所以直接寻址比立即寻址更灵活。

间接寻址　间接寻址使用的方案类似于直接寻址。但是，作为指令的一部分提供给 CPU 的存储器地址并不包含 CPU 用作操作数的真实数值。实际上，存储器地址中包含另一个存储器地址(也许位于不同的页面上)。CPU 通过读取间接地址来了解待操作数据驻留的位置，随后从这个地址取出真实的操作数。

基址+偏移量寻址　基址+偏移量寻址使用存储在某个 CPU 寄存器中的数值作为开始计算的基址。然后，CPU 将指令提供的偏移量与基址相加，并从计算得到的存储位置取出操作数。

5. 辅助存储器

“辅助存储器”这个术语通常是指磁性/光学介质或者包含 CPU 不能立刻获得的数据的其他存储设备。为了让 CPU 能够访问辅助存储器中的数据，数据必须先由操作系统读取并存储在实际的存储器中。但是，辅助存储器比主存储器的价格便宜许多，而且可以被用于存储大量的信息。在这种环境下，硬盘、软盘和光学介质(例如，CD 和 DVD)都可以作为辅助存储器使用。

虚拟存储器是一种特殊类型的辅助存储器，由操作系统负责管理，就好像实际的存储器一样。虚拟存储器中最常见的类型是绝大多数操作系统作为其内存管理功能一部分进行管理的页面文件。这种特殊格式化的文件包含先前被存储在存储器中但近期并不使用的数据。当操作系统需要访问在页面文件中保存的地址时，会查看页面是驻留在存储器中(如果驻留在存储器中，就可以立即进行访问)还是被交换到磁盘中(如果被交换到磁盘中，就会将数据从磁盘读回实际的存储器中，这个过程也被称为分页)。

使用虚拟存储器是一种廉价的方法，使得计算机在运行时拥有的存储器就好像比物理安装的实际存储器多。虚拟存储器的主要缺点是：在主存储器和辅助存储器之间交换数据时进行分页操作的速度相对较慢(微秒级的存储功能、毫秒级的磁盘系统；通常这意味着量级相差 3 个级别)，并且会消耗计算机的大量开销和减缓整个系统的速度。

6. 存储器的安全问题

存储器存储并处理数据，而某些数据可能极其敏感。因此，我们很有必要了解各种不同类型的存储器并了解它们如何存储和保留数据。任何保留敏感数据的存储器设备在由于某种原因被允许离开组织之前，应当清除里面的数据。这一点对于辅助存储器和 ROM/PROM/EPROM/EEPROM 设备来说尤其重要，原因在于这些设备在电源供应被切断后仍然可以保留数据。

然而，存储器的数据保留问题不仅限于那些被设计用于保留数据的存储器类型。前面曾经介绍过，静态 RAM 和动态 RAM 芯片是通过电容器和触发器来存储数据的(参见前面的真实场景“动态 RAM 与静态 RAM”)。从技术上讲，在电源被切断后，这些电子元件在有限的一段时间内仍有可能保存一些电量。从理论上讲，一位技术经验丰富的人可以针对这些元件采取电子方法，然后从设备上取出存储的部分数据。不过，这需要有丰富的技术方面的专业知识，除非对手拥有令人难以置信的财力和资源，否则不可能构成威胁。

当系统被关闭或 RAM 被从主板上拔出时，也有一种冻结存储器芯片以延迟驻留数据衰减的攻击，参见 http://en.wikipedia.org/wiki/cold-boot.attack。

警告：

由 RAM 芯片引起的最大安全威胁其实非常简单：RAM 芯片经常被盗。毕竟，谁也不会每天都检查自己的计算机中究竟有多少存储器？某些人可能轻易地从大量系统中拆除很少一部分存储器，

然后将这些具有很高价值的芯片放在一个小包里带出房间。然而，因为存储器芯片的价格不断下跌，所以这种威胁正在逐渐减少。

围绕存储器的最重要的一个安全问题是：在计算机使用过程中一定要控制哪些人可以对存储在存储器中的数据进行访问。这主要是操作系统的职责，并且是前面讨论的各种处理模式下主要的存储器安全问题。在本章稍后介绍的“基本安全保护机制”一节中，你将会了解到如何使用进程隔离原则，来保证进程无法在未分配给它们的存储器空间中进行读取或写入操作。如果在多级安全模式的环境下工作，那么特别需要注意的是：无论是通过直接存储器访问还是隐蔽通道(隐蔽通道的内容将在本章后面进行详细讨论)，一定要确保采取了适当的保护措施，来保护存储器内容不会在不同安全级别之间发生不必要的泄漏。

9.1.3 存储设备

我们下面将要讨论的是计算机系统组件的第三大类：数据存储设备。这些设备被用于存储计算机今后要用到的信息。我们首先讨论一些与存储设备有关的通用术语，然后介绍与数据存储相关的安全问题。

1. 主存储设备与辅助存储设备

主存储设备与辅助存储设备的概念可能会被混淆，尤其是在将它们与主存储器和辅助存储器进行比较时。分清这些概念有一种容易的方法，其实它们是一样的。主存储器也称为主存储设备，是计算机用于保存运行时 CPU 容易获得的必要信息的 RAM。辅助存储器或辅助存储设备包括人们熟悉的每天都使用的长期存储设备。辅助存储设备由磁性介质和光学介质组成，如硬盘、固态磁盘(SSD)、软盘、磁带、CD、DVD 和闪存卡等。

2. 易失性存储设备与非易失性存储设备

虽然你以前可能没有听说过使用术语“易失性”来描述存储设备，但是在讨论存储器时已经介绍了易失性的概念。存储设备的易失性只是一种用来衡量存储设备在电源被切断时丢失数据的可能性的方法。被设计用于保留数据的设备(如磁性介质)属于非易失性的，反之，诸如静态或动态 RAM 模块之类的、被设计为丢失数据的设备属于易失性的。前面曾经讨论过，在电源被切断时，采用复杂的技术有时可以把数据从具有易失性的存储器中提取出来，所以易失性与非易失性之间的界限有时也没有那么明显。

3. 随机存取与顺序存取

存储设备的存取方式有两种。随机存取存储设备允许操作系统通过使用某种寻址系统从设备内的任何位置立刻读取(有时会写入)数据。几乎所有的主存储设备都是随机存取设备。可以使用一个内存地址直接存取存储在 RAM 芯片中任何位置的信息，而不必读取在此位置之前物理存储的数据。许多辅助存储设备也是随机存取的。例如，硬盘使用可以移动的磁头系统，这种系统允许操作者直接移到磁盘上的任何位置，而不必旋转通过其前面磁道上存储的所有数据；同样，CD 和 DVD 设备使用能够将自身定位于盘片表面任何位置的光学扫描器。

另一方面，顺序存储设备并不提供这种灵活性。它们要求在到达指定位置之前读取(或快速经过)

该位置之前物理存储的所有数据。磁带驱动器是顺序存储设备的常见示例。为了存取存储在磁带中部的数据，磁带机必须物理扫描整个磁带(即使不需要处理在快进模式中经过的数据)，直至到达所期望的位置。

显而易见，顺序存取存储设备要比随机存取存储设备的操作速度慢许多。但是，此时再次需要根据成本/效益做出决定。许多顺序存取存储设备能够使用价格相对便宜的介质保存大量的数据，这个特性使得磁带机非常适合用于与灾难恢复或业务连续性计划(参见第 3 章“业务连续性计划”和第 18 章“灾难恢复计划”)相关联的备份任务。在需要备份的情况下，通常有数量巨大的数据需要存储，但是这些数据很少进行存取。这种情况恰好就可以使用顺序存储设备！

9.1.4　存储介质的安全性

我们在前面讨论了与主存储设备有关的安全问题。当涉及辅助存储设备的安全问题时，主要需要关注下列三点，同时它们也反映了主存储设备引起的问题：

- 即使在数据被删除之后，数据仍然可能保留在辅助存储设备上。这种情况被称为数据剩磁。大多数具备一定技术水平的计算机用户都知道，使用相应的实用程序能够从磁盘上重新找回已经被删除的文件。从技术上讲，还存在从已经被重新格式化(通常被称为清除)的磁盘上重新找回数据的可能性。如果确实希望从辅助存储设备上删除数据，那么就需要使用专门设计的实用程序来破坏设备上相应数据的所有磁道，或者破坏或销毁辅助存储设备，从而使其无法被修复(通常称为净化)。
- 固态硬盘对于净化呈现出独特的问题。SSD 损耗均衡意味着有经常未被标记为“存活”状态的数据块，当它被关闭复制以降低磨损平整块(lower wear leveled bolcks)时仍保存了数据的副本。这意味着对于固态硬盘的数据安全措施，传统的归零是无效的。
- 辅助存储设备还很容易被盗。经济上的损失不是主要因素(毕竟，CD-R 光盘甚至硬盘值不了多少钱)，但是机密信息的丢失会带来极大的风险。如果某人将公司的商业机密复制在软盘上并带走，这样造成的巨大损失远远越过磁盘本身的价值。因此，重要的是要使用全磁盘加密，以减少未经授权的实体获取数据的风险。由于 SSD 的损耗均衡技术，在 SSD 存储数据之前对其进行全盘加密是一个良好的安全实践。这将减少任何明文数据驻留在休眠块(dormant blocks)中的机会。幸运的是，许多 HDD 和 SSD 设备本身提供设备加密。
- 对存储在辅助存储设备上的数据进行访问，是计算机安全专家所面对的最紧要的问题之一。对于硬盘来说，通过结合操作系统的访问控制往往就可以对数据进行保护。可移动介质的安全则面临着极大的挑战，因此对它们的保护经常需要使用密码技术。

9.1.5　输入和输出设备

输入和输出设备往往被视为基本的、原始的外围设备，并且一般不会受到很多的关注，除非它们无法正常工作。然而，即使是这些基本的设备，对于系统来说一样存在安全风险。安全专家应当意识到这些风险，并且必须确保使用了恰当的控制方法来降低风险。下面将讨论某些特殊输入和输出设备存在的风险。

1. 显示器

显示器似乎相当安全。毕竟，它们只是显示由操作系统呈现的数据。当关掉显示器时，数据就从屏幕上消失了并且无法被恢复。然而，有一种被称为 TEMPEST 的技术会危及显示器上所显示数据的安全性。

TEMPEST 技术可以从一定距离外甚至另一个地点探测到每台显示器所发出的电子辐射(被称为 Van Eck 辐射)。这种技术还被用于阻止类似的活动。各种证据已经表明：使用一辆停靠街旁的装有此设备的箱式货车，就可以轻松读取办公楼内显示器屏幕上的内容。遗憾的是，实施阻止 Van Eck 辐射所需的保护控制措施是非常昂贵的(需要大量的铜)，并且使用起来相当麻烦。通常，CRT 显示器更容易产生辐射，而液晶显示器的电磁泄漏则少得多(有人这么宣传但没有提供关键数据支撑)。关于任意显示器最大争议的最大风险仍然是肩窥或相机的长焦镜头。

2. 打印机

虽然处理起来比较简单，但是打印机也存在一定的安全风险。由于组织使用了物理安全控制措施，因此带着打印出来的敏感信息走出办公室要比带着软盘或其他磁性介质离开更容易。此外，如果打印机是共享的，那么用户可能会忘了及时取回他们打印出来的敏感信息，因而容易被人偷窥。许多现代的打印机也在本地存储数据，这些数据往往存储在硬盘驱动器上，有一些还保留着无限期的打印拷贝。打印机通常被暴露在网络上以方便访问，因此往往不是设计为安全系统。在组织的安全策略中，最好能够解决这些问题。

3. 键盘/鼠标

键盘、鼠标和类似的输入设备并非不存在安全脆弱性，但所有这些设备都容易受到 TEMPEST 技术的监控。还有，键盘容易受到简单的“窃听”。一种简单的设备可以被放在键盘内部或放在连接电缆旁，从而能够截获所有的击键行为，并且可以使用无线电信号将它们传送到远程接收器。这与使用 TEMPEST 技术进行监控具有相同的效果，但却使用比较便宜的装置。此外，如果键盘和鼠标是无线的(包括蓝牙)，那么它们的无线电信号也能够被截获。

4. 调制解调器

随着宽带和无线网络的广泛应用，调制解调器逐渐成为过时且很少使用的计算机组件。不过，在现有的台式机和笔记本电脑中，调制解调器仍然是硬件配置中的常见部分。不管是否常用，用户系统中存在调制解调器往往是安全管理员最苦恼的问题之一。调制解调器允许用户在网络内创建非受控的访问点。在最坏的情况中，如果配置不正确，那么调制解调器会产生相当严重的安全脆弱性，从而致使外部人员突破保护机制的安全防线并直接访问网络资源。最糟糕的是，调制解调器会生成一条可选的出口通道，内部用户可以使用它将数据泄漏到组织外部。但是，请记住，只有当调制解调器连接到可操作的有线电话线时，这个漏洞才能被利用。

除非是出于商业原因而必须使用调制解调器，否则应当在组织的安全策略中重点考虑禁止使用调制解调器。在这些情况下，安全管理人员应当了解所有调制解调器在网络中的物理位置和逻辑位置，并确保它们被正确配置和给予适当的保护措施以阻止非法使用。

5. 输入/输出结构

与通用输入/输出(I/O)操作相关的某些计算机活动(并非单独的设备)也具有安全含义。需要在一定程度上熟悉手动输入/输出设备配置，以便将旧式的外围设备(这些设备没有自动配置或支持即插即用设置)集成到现代 PC 中。在旧式设备上进行手动配置所要求的三种操作涉及下列内容：

存储映射 I/O　对于许多设备类型来说，存储映射 I/O 是一种用于管理输入/输出的技术。更确切地说，CPU 管理的地址空间部分能够通过一系列映射的内存地址或位置提供对某些设备类别的访问。这样一来，通过读取映射存储位置，实际上从相应的设备中读取输入(在设备通知输入可用时，会在系统级自动复制至这些存储位置)。同样，通过写入映射存储位置，实际上可以将输出发送至相应的设备(在 CPU 通知输出可用时，在系统级将这些存储位置的输出自动复制至相应设备)。

从配置的角度看，确认只有一台设备映射到某个特定的存储地址范围以及这个存储地址范围只用于处理设备 I/O 是非常重要的。从安全性的角度看，对映射存储位置的访问应当由操作系统居间调停，并且应当得到正确的授权和访问控制。

中断(IRQ)　中断(IRQ)是中断请求的缩写，这种技术通过特殊的中断控制器为特定设备指派特定的信号线。当某个设备希望为 CPU 提供输入时，它会在为其指派的 IRQ 上发送信号(在使用两个级联的 8 线中断控制器的旧式 PC 中，IRQ 号的范围通常为 0-16；在使用三个级联的 8 线中断控制器的新式 PC 中，IRQ 号的范围通常为 0-23)。较新的符合 PnP 的设备实际上可以共享单个中断(IRQ 号)，较旧的、过时的设备通常必须独占使用唯一的 IRQ 号(两个或多个设备被分配相同的中断号时会发生众所周知的中断冲突，最佳的识别方法是所有受影响的设备都无法被访问)。从配置的角度看，找出对过时设备有用的未用 IRQ 号有时是个不断尝试的过程。从安全性的角度看，只有操作系统能够在足够高的特权级别间接访问 IRQ，以便防止篡改或意外的错误配置。

直接内存访问(Direct Memory Access，DMA)　直接内存访问(DMA)像具有两条信号线的通道一样工作，其中一条线是 DMA 请求(DRQ)线，另一条则是 DMA 确认(DACK)线。不需要 CPU 帮助就可以直接交换实际存储器中数据的设备使用 DMA 来管理这样的访问。通过使用 DMA 的 DRQ 线，某个设备通知 CPU 希望直接访问(可能是读、写或读写组合)另一个设备(通常是实际的存储器)。CPU 授权访问，随后允许这个访问独立进行，同时阻止对所涉及内存位置的其他访问。直接访问完成后，设备使用 DACK 线通知 CPU 可以再次允许先前被阻止的、对相关内存位置的访问。与要求 CPU 调停访问和允许 CPU 在内存访问进行中处理其他任务相比，直接访问更为快速。DMA 常用于准许硬盘驱动器、光驱、显卡和多媒体卡管理与实际存储器之间的大量数据传输。从配置的角度看，管理 DMA 地址以保持设备地址的唯一性以及确认这样的地址只用于 DMA 信号发送，是非常重要的。从安全性的角度看，只有操作系统才能够调停 DMA 的分配以及访问 I/O 设备的 DMA 的使用。

如果理解了通用的IRQ分配，并且理解了存储映射I/O和DMA的工作原理以及相关的安全问题，那么就足以应对CISSP考试。如果还没有达到这个程度，那么还需要继续学习相关知识。此时，PC Guide网站上对系统存储器的完美概述(www.pcguide.com/ref/ram/)能够提供你需要掌握的所有内容。

9.1.6　固件

“固件”(在某些范围内也被称为微码)这个术语被用于描述在ROM芯片中存储的软件。这种软件很少被更改(只要软件被存储在与EPROM/EEPROM不同的真正的ROM芯片上，那么实际上从不更改)，并且经常被用于驱动计算设备的基本计算操作。有两种类型的固件：在主板上的BIOS以及通

用的内部或外部固件。

1. BIOS

基本输入输出系统(Basic Input/Output System，BIOS)包含独立于操作系统的原始指令，这些指令被用于启动计算机和从磁盘加载操作系统。BIOS 被包含在一个固件设备中，在启动时能够由计算机立即访问。在大多数计算机中，BIOS 被存储在 EEPROM 芯片上以帮助版本升级。BIOS 的升级过程被称为“闪存 BIOS”。

曾经有几个恶意代码被嵌入到 BIOS/固件中的例子。还有一类攻击被称为 phlashing，此攻击会恶意更改官方 BIOS 或固件，把恶意代码安装到设备中，使其可被远程控制或具备其他的恶意功能。

自 2011 年以来，大多数系统制造商已通过 UEFI(Unified Extensible Firmware Interface，统一可扩展固件接口)取代了传统系统主板的 BIOS。UEFI 是硬件和操作系统之间的一种更先进的接口，但保持了对传统 BIOS 服务的支持。

2. 设备固件

为了完成任务，许多硬件设备(如打印机和调制解调器)还需要一些有限的处理能力，以便最小化操作系统自身的负担。在许多情况下，这些“迷你型”操作系统完全被包含在相应设备上的固件芯片内。与计算机的 BIOS 一样，设备固件往往被存储在 EEPROM 设备上，从而可以在需要时进行更新。

9.2 基于客户端

基于客户端漏洞会使用户及其数据和系统面临遭受攻击和破坏的风险。客户端攻击是能够损害客户的任何攻击类型。一般情况下，当讨论攻击时，攻击的主要目标是服务器或服务器端组件。客户端或客户端集中攻击的目标是客户机本身或客户机上的进程。客户端攻击的一个常见例子是恶意网站，它们将恶意的移动代码(如 applet)通过脆弱的客户端浏览器传送到客户端。客户端攻击可以发生在任何通信协议上，而不只是 HTTP。另一类基于客户端的潜在漏洞，是本地缓存中毒的风险。

9.2.1 applet

上面已经介绍过，代理是用户系统发送的、能够对远程系统上存储的数据进行查询和处理的代码对象。applet 执行相反的功能，这些代码对象被从服务器发送至客户端以便执行某些操作。事实上，applet 实际上是一些自包含的小型程序，这些程序的执行独立于发送它们的服务器。

设想有一台 Web 服务器，它为 Web 用户提供多种财务工具。其中一个工具可能是抵押计算器，这个工具能够处理用户的财务信息，并且基于贷款本金和期限以及贷款人的信用信息提供月抵押付款。这些数据并非在服务器上进行处理，然后向客户端系统返回结果，而是由远程 Web 服务器向本地系统发送一个可以自己执行这些计算的 applet。这为远程服务器和终端用户提供了很多优点：

- 处理压力被转移至客户端，Web 服务器上的资源得到了释放，从而能够处理更多用户的请求。
- 客户端可以使用本地资源处理后得到数据，而不是等待远程服务器的响应。在很多情况下，这可以更快地响应对输入数据的修改。

- 在正确编程的 applet 中，Web 服务器并不接收作为输入信息提供给 applet 的数据，因此可以维护财务数据的安全性和隐私性。

然而，与代理一样，applet 也引入了许多安全问题。applet 准许远程系统向本地系统发送执行代码。安全管理员必须采取措施，确保这些代码是安全的，并且正确地屏蔽恶意活动。此外，如果没有逐行地分析这些代码，那么终端用户就永远不能确定这个 applet 是否包含特洛伊木马组件。例如，抵押计算器可能确实在终端用户不知情或没有得到终端用户准许的情况下向 Web 服务器传送回敏感的财务信息。

下面将探讨两个常用的 applet 类型：Java applet 和 ActiveX 控件。

Java applet　Java是由Sun Microsystems公司开发的独立于平台的编程语言。大多数编程语言使用的编译器能够定制生成在特定操作系统中运行的应用程序。这需要使用多个编译器为所支持的每个平台生成不同版本的、单独的应用程序。Java引入了Java虚拟机(JVM)，因此不存在上述限制。每个运行Java代码的系统都会下载本操作系统所支持的JVM版本。JVM随后获得Java代码，并且将其转换为指定系统可以执行的格式。这种方案的最大优点在于代码可以在操作系统间共享，而不需要进行修改。Java applet是在Internet上传输的简短的Java程序，以便在远程系统上执行各种操作。

在 Java 平台的设计过程中，安全性是首要的考虑因素，并且 Sun 公司的开发团队创建了“沙箱”的概念，从而对 Java 代码施加特权限制。沙箱将 Java 代码对象与操作系统的其他部分隔离开，并且强制实施关于对象可访问资源的严格规则。例如，为了防止 Java applet 窃取信息，沙箱会禁止 Java applet 从内存区域(专门为其分配的区域除外)中检索信息。遗憾的是，虽然沙盒通过 Java 减少了恶意事件的种类，但是还存在其他很多已被广泛利用的漏洞。

ActiveX 控件　ActiveX 控件是 Microsoft 公司针对 Sun 公司的 Java applet 的应对产品。ActiveX 控件与 Java applet 的操作形式很相似，但使用多种语言中的一种，包括 Visual Basic、C、C++和 Java。在 Java applet 和 ActiveX 控件之间存在两种主要的区别。首先，ActiveX 控件使用 Microsoft 公司专有的技术，因此，只能在运行 Microsoft 浏览器的系统上执行。其次，ActiveX 控件不受 Java applet 中沙箱的限制，它对 Windows 操作系统环境具有全部的访问权限，并且可以执行很多特权操作。因此，在决定下载执行哪种 ActiveX 控件时必须采取特殊的预防措施。很多安全管理员已经采取了稍微有些苛刻的态度，也就是禁止从某些可信站点之外的所有站点下载任何 ActiveX 内容。

Microsoft 已经宣布和发布新的浏览器代码，称为斯巴达项目。这种新的浏览器将不包括对 ActiveX 控件的支持，而计划推出的 Intemet Explorer 10 还包括 ActiveX，这表明 Microsoft 也可能要淘汰 ActiveX。

9.2.2　本地缓存

本地缓存是暂时存储在客户端上的任意内容，用于将来重新使用。一个典型的客户端上有许多本地缓存，包括 ARP 缓存、DNS 缓存以及互联网文件缓存。ARP 缓存投毒攻击由攻击者回应 ARP 广播查询并发送伪造的回复而引发。如果客户端在有效的回复之前收到错误的回复，那么虚假的应答将用来填充 ARP 缓存，而真实的回复将被看成外面的开放查询而被丢弃。ARP 缓存的动态内容，不论是否中毒或合法，都将一直缓存直到发生超时(通常是 10 分钟)。ARP 为了制作数据传输的以太网报头，而将 IP 地址解析为相应的 MAC 地址。一旦一个 IP 到 MAC 地址的映射不在缓存内，那么攻击者在客户端执行 ARP 广播查询时就会得到另一个机会去毒害 ARP 缓存。

ARP 缓存投毒的第二种形式是创建静态 ARP 实体，这通过 ARP 命令执行而且必须是在本地执

行。但这很容易通过木马、缓冲区溢出或社会工程攻击在客户端完成。静态 ARP 实体是永久性的，即便系统重新启动。一旦发生 ARP 投毒，无论是针对永久实体还是动态条目，客户端传输的数据流都将发送给非预期的其他系统。这是由于 IP 地址被映射到错误或不同的硬件地址(即 MAC 地址)造成的。ARP 缓存投毒或 ARP 投毒是中间人攻击的手段之一。

另一种比较流行的中间人攻击方式是通过 DNS 缓存投毒。类似于 ARP 缓存，一旦客户端从 DNS 服务器收到响应，响应将被缓存并用于将来使用。如果虚假信息可以反馈到缓存中，那么重定向通信是很容易的。有许多可以执行 DNS 缓存中毒的手段，包括主机投毒、授权 DNS 服务器攻击、缓存 DNS 服务器攻击、DNS 查找地址改变以及 DNS 查询欺骗。

主机文件是静态文件并可在支持 TCP/IP 协议的系统中找到，其中包含域名和关联 IP 地址的硬编码索引。虽然主机文件今天主要被用于动态 DNS 查询系统，但仍可作为后备措施或强制性手段。管理员或黑客可以在主机文件中添加内容，在 FQDN(Fully Qualified Domain Name，完全合格的域名)和 IP 地址选择之间进行设置。如果攻击者能够将虚假信息存储到主机文件中，那么当系统启动时，主机文件的内容将被读入内存，它们将被优先考虑。与动态查询不同，动态查询最终将超时并从缓存中失效，而主机文件中的条目是永久生效的。

授权 DNS 服务器攻击的目的是改变原有主机系统的 FQDN 原始记录。授权 DNS 服务器拥有文件区域或数据库域。如果原始数据集被改变，那么最终这些变化将在整个互联网上传播开来。然而，对授权 DNS 服务器的攻击通常会很快被发现，所以很少能导致漏洞蔓延。因此，大多数攻击者将目光转向缓存 DNS 服务器。缓存 DNS 服务器可以是任意 DNS 系统，它们缓存从其他 DNS 服务器获得的 DNS 信息。大多数公司和 ISP 向他们的用户提供缓存 DNS 服务器。托管在缓存 DNS 服务器上的内容不会被世界范围内的安全团体所关注，而是由当地 ISP 维护。因此，对缓存 DNS 服务器的攻击可悄然发生直到一段时候后才被发现。有关缓存 DNS 服务器攻击如何发生的详细信息，可参见 http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html 网址上的“Kaminsky DNS 漏洞图解指南”。虽然这些攻击都集中在 DNS 服务器，但它们将最终影响客户端。一旦客户端进行动态 DNS 解析，从授权 DNS 服务器或缓存 DNS 服务器接收到的信息将被暂时存储在客户端的本地 DNS 缓存中。如果信息是虚假的，那么客户端的 DNS 缓存就中毒了。

DNS 投毒四分之一的例子集中在发送另一个 IP 地址给客户端作为 DNS 服务器，为客户端提供域名查询服务。DNS 服务器地址通常是通过 DHCP 分配给客户端的，但也可以静态分配。即使所有 DHCP 指定的 IP 配置的其他元素已经分配，也仍然可以在本地修改静态分配的 DNS 服务器地址。攻击改变客户端的 DNS 服务器查询地址可以通过脚本来执行(类似于前面提到的 ARP 攻击)或直接攻击 DHCP 服务器。一旦客户端使用错误的 DNS 服务器，它们的查询将被发送到黑客控制的 DNS 服务器，这将会得到已中毒的响应结果。

DNS 投毒五分之一的例子为 DNS 查询欺骗。当这种攻击发生时，黑客可以监听客户端向 DNS 服务器发送查询。攻击者然后发送回虚假的信息响应。如果客户端接受虚假的响应，它们会对这些信息进行本地 DNS 缓存。当真正的答复到达时，却被丢弃，因为原来的查询已被响应。无论这种 DNS 攻击如何进行，错误的条目都将写入客户端的本地 DNS 缓存中。因此，所有的 IP 通信都将被发送到错误的端点。这将允许黑客通过操纵虚假的端点建立中间人攻击，然后再将通信数据转发到正确的目的地。

关于本地缓存三分之一的关注是临时互联网文件或互联网文件缓存。这些临时存储的文件从互联网网站下载，并被客户端当前或以后使用。这个缓存主要包含网站内容，但其他的互联网服务也可以使用文件缓存。各种各样的利用方式，如分裂响应攻击，可以使客户端下载内容并将其存储在

缓存中，而这些内容不是预期的 Web 页面请求内容。移动代码脚本攻击也可以用来在缓存中写入错误内容。一旦文件已被缓存投毒，那么即使当合法的 Web 文档进行缓存调用时，恶意的内容也将被激活。

减轻或解决这些攻击并不那么简单或直接，并不是简单的补丁或更新就可防止这些对客户端漏洞的攻击。这是因为这些攻击利用了内置到各种协议、服务和应用中的正常和适当的机制。因此，无法通过补丁来修复缺陷，更多的防御集中在监测和预防方面。通常作为开始，应保持操作系统和应用程序修补来自各自厂商的补丁。下一步，安装主机入侵检测系统和网络入侵检测工具来观察这些类型的滥用。定期审计 DNS 日志、DHCP 系统日志以及本地客户端系统日志、可能的防火墙、交换机和路由器日志以及时发现异常或可疑事件。

9.3　基于服务端

基于服务器关注的重要领域是数据流控制，其中也可能包括客户端。数据流是进程之间、设备之间、网络之间的数据或是通信信道之间的数据的流动。对数据流加以管理能确保不仅以最小延迟的有效方式传输，还使用散列确保吞吐数据的可靠性和使用加密确保机密性。数据流控制同样还确保接收系统不被通信流量导致过载，尤其是 dropping(泪滴)连接或恶意的甚至是自我造成的拒绝服务。当数据溢出发生时，数据可能丢失、损坏或触发重传。这些结果是不利的，并且通常实施数据流控制来防止这些问题的发生。数据流控制可以通过网络设备，包括路由器和交换机，还有网络应用和服务进行提供。

9.4　数据库安全

数据库安全是任何使用大规模数据集作为基础资产的组织的重要组成部分。如果没有数据库安全性方面的努力，业务任务可以被中断，保密信息将被泄露。在 CISSP 考试中知道有关数据库安全的若干问题是很重要的，包括聚合、推理、数据挖掘、数据仓库和数据分析。

9.4.1　聚合

SQL 提供了很多函数，这些函数能够将一个或多个表中的记录组合在一起，以生成可能有用的信息。这个过程被称为聚合(aggregation)。聚合并非没有安全漏洞。聚合攻击被用来收集大量的低安全级别的或低价值的事物，将它们结合起来创造较高安全级别或有价值的东西。

虽然这些功能相当有用，但是也对数据库中信息的安全性带来了非常大的风险。例如，假设一个低职衔的军事记录员负责更新基地之间人员和设备的调配记录。作为职责的一部分，这个记录员可能被授予必要的数据库权限，从而能够对 personnel 表进行查询和更新。

军队可能没有考虑到个人调动请求(例如，Jones 中士从 X 基地被调往 Y 基地，属于分类信息。记录员可以访问这些信息，但是在一般情况下，Jones 中士已经通知了朋友和家人他要被调往 Y 基地。然而，通过使用聚合函数，记录员可能能够计算全球每个军事基地的部队数量。这些部队级别常常受到军事机密的严格保护，但是低职衔的记录员却能够使用聚合函数在大量未分类的数据中推

论出这些内容。

因此，严格控制对聚合函数的访问并且充分估计可能展示给未授权个体的潜在信息，这对数据库安全管理员来说是特别重要的。

9.4.2 推理

由推理攻击引出的数据库安全问题与数据聚合威胁带来的问题很相似。与聚合类似，推理攻击利用几个非敏感信息片的组合，从而获得对应该属于更高级分类的信息的访问能力。然而，推理要利用人的推断能力，而不是现代数据库平台的简单数学计算能力。

下面是一个经常被引用的推理攻击示例：为了准备一份高级别报告，在一家大公司工作的会计获准检索公司工资的全部开销，但是没有获准访问员工个人的工资信息。会计必须利用过去的有效日期来准备这些报告，因此被获准访问在过去一年中任意日期的工资总计。假如会计还必须知道不同员工的雇用和解聘日期，并且可以访问这些信息。这就为推理攻击打开了一道大门。如果某位员工是某天被雇用的唯一人员，那么会计现在能够检索到那一天和之前一天的工资总计，并且推导出这名员工的工资，而这应该是用户不允许直接访问的敏感信息。

与聚合类似，对于推理攻击的最好防范是对赋予个人用户的特权保持持续警惕。此外，数据的故意混淆可能被用来防止对敏感信息的推理。例如，如果会计只能够检索到最大约 100 万人的工资信息，那么将不可能获得任何有关员工个人的有用信息。最后，可以使用数据库分区(本章早先已讨论)帮助降低这些攻击。

9.4.3 数据挖掘和数据仓库

很多公司都使用了被称为数据仓库的大型数据库，以存储大量用于专用分析技术的多种数据库信息。数据仓库常常包含生产数据库出于存储限制或数据安全性考虑而通常未予存储的详细历史信息。

另一种被称为数据字典的存储类型常常用于存储与数据相关的关键信息，包括用法、类型、源、关系和格式。DBMS 软件通过读取数据字典来决定用户访问数据的访问权限。

数据挖掘技术准许分析人员对数据仓库进行搜索，从而寻找历史数据中潜在的相关信息。例如，分析人员可能发现在冬季电灯泡的需求总是在增加，那么在确定价格和促销策略时就可以使用这条信息。数据挖掘技术导致对可以用于预测未来活动的数据模型的开发。

数据挖掘活动产生元数据。元数据是关于数据的数据或关于信息的数据。元数据不完全是数据挖掘操作的结果，其他的功能或服务也可以生成元数据。可以认为元数据是数据挖掘的数据浓缩。它也可以是超集、子集或是大的数据集表示。元数据可以是重要的、有意义的、相关的、异常的或数据集的畸变元素。

元数据的一个常见安全例子是安全事件报告。事故报告通过使用安全审计数据挖掘工具，从日志审计数据仓库中提取元数据。在大多数情况下，元数据比在仓库中的数据块具有更高的价值。更高的敏感性(由于泄露)。因此，元数据存储在被称为数据集市的更安全的容器中。

数据仓库和数据挖掘技术对于安全专家来说十分重要，这主要有两个原因。首先，前面曾经提到过，数据仓库包含大量潜在的敏感信息，它们容易受到聚合和推理攻击。安全专家必须确保恰当的访问控制，并且采取其他一些安全手段保护数据。其次，在数据挖掘技术被用来开发基于统计异

常的入侵检测系统的基准时，实际上可以作为安全工具使用。

9.4.4　数据分析

数据分析是对原始数据进行检查的科学，检查重点是从大量的信息中提取有用的信息。数据分析的结果可以集中于重要的异常值，或正常之外的例外或标准项，或所有数据项的总结，或一些集中的提取和有兴趣信息的组织。数据分析是一个不断发展的领域，越来越多的组织对他们的顾客和产品收集惊人的数据量。对庞大信息量的处理已经要求全新的数据库结构和分析工具类别，甚至拿起了“大数据”的昵称。

大数据是指那些已经变得非常大的数据集合，以至于对它们采用传统的分析或处理手段是无效的、效率低下的和不充分的。大数据涉及众多的困难挑战，包括收集、存储、分析、挖掘、传输、分发和结果演示。如此大量的数据已经具备揭示细微差别和特质的潜力，而那种一般的数据集则无法解决。从大数据中进行学习的潜力是十分巨大的，但处理大数据的负担同样十分沉重。随着数据量的增加，数据分析的复杂性也在增加。大数据分析要求在大规模并行或分布式处理系统中进行高性能的分析。在安全方面，众多组织正在努力访问数据并收集范围更广、更为详尽的事件数据。这一数据收集的目标是评估合规性、提高效率、提高生产力、检测违规行为。

9.4.5　大规模并行数据系统

并行数据系统或并行计算是一个计算系统，被设计用于同时进行大量的计算，但并行数据系统往往远远超出了基本的多处理能力。它们通常包括将一个大的任务划分成更小元素的概念，然后将每个子元素分发到不同的子处理系统进行并行计算。这中实现基于这样一个思路：有些问题如果拆解成更小的任务并同时处理，可以更有效地得到解决。并行数据处理可以通过使用不同的 CPU 或多码 CPU，使用虚拟系统或它们的任意组合来完成。大规模并行数据系统必须关注性能、功耗和可靠性/稳定性问题。涉及 1000 个或更多个处理单元的复杂性往往随着巨大的计算能力会导致意想不到的问题和风险的增加。

大规模并行数据系统的竞技场仍在发展中，这可能是因为很多管理问题尚未被发现以及仍然还有待解决的已知问题。大规模并行数据管理在管理大数据上可能是一个关键的工具，并往往涉及云计算、网格计算、对等计算解决方案。这三个概念将在下面的部分进行阐述。

9.5　分布式系统

随着计算技术从主机/终端模型(用户可以物理分布，但是所有功能、活动、数据和资源都驻留在单个集中化的系统中)演化到客户端/服务器模型(用户可以独立操作功能完善的台式机，但是仍然在网络化的服务器上访问服务和资源)，安全控制与概念也在演化。这意味着客户端具有计算和存储能力，多个服务器通常也如此。因此，安全性必须涉及方方面面，而不是只涉及单个集中化的主机。从安全性的角度看，这意味着：因为处理和存储分布在多个客户端和服务器上，所以所有这些计算机都必须得到适当的安全保护；此外，客户端和服务器之间的网络链接(在某些情况下，这些链接可能并非完全是本地的)也必须得到适当的安全保护。当评估安全体系架构时，确保包括需求评估和分

布式体系结构相关的风险评估。

在完整的主机/终端系统中，分布式体系结构容易出现意想不到的脆弱性。台式机系统可能包含存在泄露风险的敏感信息，因此必须加以保护。单独的用户可能缺乏一般的安全意识，因此内在的体系结构必须弥补这些不足。因为用户需要通过访问网络服务器和服务来执行作业，所以桌面 PC、工作站和便携式电脑都能够在分布式环境的其他位置提供对关键信息系统的访问途径。由于准许用户计算机访问网络及其分布资源，组织必须认识到：如果用户计算机被滥用或受到危害，那么用户计算机也会成为威胁。这种软件和系统的漏洞与威胁必须以恰当的方式进行应对。

通信设备也会提供不期望的分布式环境入口点。例如，附属于某台连接组织网络的台式机的调制解调器会使网络容易遭受拨号攻击。同样，从互联网下载数据的用户增加了自己和其他系统感染恶意代码和特洛伊木马的风险。台式机、便携式电脑和工作站(以及相关联的磁盘或其他存储设备)可能无法防范物理入侵或盗窃。最后，在数据只驻留在客户机上时，我们无法使用适当的备份保证数据的安全(服务器往往可以进行适当的备份，而客户机则无法进行适当的备份)。

通过前面介绍的分布式体系结构中的潜在脆弱性，应当明白这样的环境要求采取许多防护措施来实现适当的安全性，并确保消除、缓解或补救这些脆弱性。客户端必须受到对其内容及用户内容实施防护措施的策略的约束。下面列出了这些防护措施：

- 电子邮件必须被过滤，从而使其无法成为恶意软件的感染者；电子邮件也必须受到支配正确使用和限制潜在不利条件的策略的约束。
- 必须创建下载/上传策略，从而能够过滤进出的数据并阻挡可疑的内容。
- 系统必须受到可靠的访问控制的约束，这样的访问控制可能包括多因素身份认证和/或生物学测定因素，从而约束对台式机的访问并阻止对服务器和服务的未授权访问。
- 应当安装和使用图形用户界面机制和数据库管理系统，以便约束和管理对关键信息的访问。
- 对客户机上存储的文件和数据应用适当的文件加密操作(事实上，对于容易在组织范围之外丢失或被盗的便携式电脑和其他移动计算设备来说，驱动器级的加密是一种不错的方法)。
- 必须分开和隔离在用户模式和监管模式中运行的进程，从而阻止对高特权进程和功能进行未授权和不期望的访问。
- 必须创建保护域，从而使某个客户端遭受的损害不会自动危害整个网络。
- 必须按照安全分类级别或组织的敏感度清晰地标记磁盘和其他敏感材料；应当结合过程化进程和系统控制来帮助防止对敏感材料的未授权或不期望的访问。
- 应当使用某种与客户端代理软件(能够从客户端确定和捕获在安全备份存储归档位置存储的文件)一起工作的集中化备份实用程序对台式机上的文件进行备份(在理想情况下还应当备份服务器中的文件)。
- 台式机用户需要定期接受安全意识培训，从而保持正确的安全意识。此外，我们还应当告知用户潜在的风险并指示他们如何正确地应对这些风险。
- 台式计算机及其存储介质要求防范环境危险(如温度、湿度、断电/电压波动等)。
- 因为可能与组织内使用户返回工作状态的其他系统和服务一样重要(或者更重要)，所以台式计算机必须包含在灾难恢复计划和业务连续性计划中。
- 在分布式环境中构建和使用的自定义软件的开发人员也需要考虑安全性，包括使用规范的方法(例如，代码库、变更控制机制、配置管理以及补丁和更新部署)进行开发和部署。

通常，对分布式环境进行防护意味着了解环境可能存在的脆弱性以及应用相应的安全防护措施。这些安全防护的范围从技术解决方案和控制一直延伸到管理风险与试图限制或避免损失、破坏、有

害泄漏的策略和措施。

当应对漏洞和威胁时，正确理解对策原则是非常重要的。一些具体对策原则在第 2 章“人员安全和风险管理概念”的“风险管理”中进行了讨论，但共同的一般性原则就是深度防御。深度防御是一条普遍的原则，被用于提供保护性多层屏障来抵御各种形式的攻击。要让有问题的流量或数据穿过有着防火墙、IDS 和有责任心的管理人员的防御工事网络，比起突破单独的防火墙更加困难，这个推断看起来非常合理。为什么不应该怀疑自己的防御呢？深度防御在文字或理论的同心圆中使用多种类型的访问控制。这种分层的安全形式有助于组织避免单一安全位置。单一的或要塞心态是相信单一安全机制能提供足够的所有需要的安全性。遗憾的是，每个单独的安全机制都有漏洞或工作区只等被黑客发现和滥用。只有通过智能组合对策，构造和防御才可以抵御重大和持久的破坏企图。

9.5.1　云计算

云计算是一个流行的术语，指的是计算的一个概念，即处理和存储是通过网络连接而非在本地进行。云计算通常被认为是基于互联网的计算。最终，处理和存储仍然发生在某个地方的计算机上，但区别是，不再需要当地的运行者有能力或当地有能力。这允许一个更大的用户群根据需求利用云资源。从最终用户的角度来看，所有的计算工作，都在“云端”执行，而计算的复杂性与它们无关。

云计算是虚拟化、互联网、分布式结构以及可随处访问数据和资源的自然延伸和演变。但是，云计算也存在一些问题，包括隐私问题、合规性困难、使用开/闭源解决方案、采用开放标准以及基于云计算的数据是否实际上是安全的(或甚至是可保护的)。

这里列出一些云计算的概念：

平台即服务　平台即服务(PaaS)的概念是提供计算平台和软件解决方案作为虚拟的或基于云的服务。从本质上讲，这种类型的云计算解决方案提供了一个平台的所有方面(即操作系统和完整的解决方案)。PaaS 的主要吸引力是避免了在本地购买和维护高端的硬件和软件。

软件即服务　软件即服务(SaaS)是 PaaS 的衍生物。SaaS 提供对特定软件应用或套件的按需在线访问而不需要本地安装。在许多情况下，只有很少的本地硬件和操作系统的局限性。SaaS 可以实现订阅服务(例如，Microsoft Office 365)、付费服务或免费服务(例如，Google Docs)。

基础设施即服务　基础设施即服务(IaaS)将 PaaS 模式带到了另一个方向，不但提供了按需操作的解决方案，还提供了完全外包的选择。这可以包括实用或定量的计算服务、管理任务自动化、动态规模、虚拟化服务、政策执行、管理服务和托管的/过滤的互联网连接。最终，IaaS 允许企业通过云系统快速扩展新的软件或基于数据的服务/解决方案，而不必在本地安装大量的硬件。

9.5.2　网格计算

网格计算是并行分布处理的一种形式，这种形式松散地把大量的处理节点组合在一起，为实现某个处理目标而工作。网格成员可以在随时的间隙时间进入和离开网格。通常，网格成员只有当它们的处理能力没有本地工作负担的情况下才会加入网格。当系统处于空闲状态时，它可以加入一个网格组，下载一小部分的工作，然后开始计算。当系统离开网格时，它保存任务并可上传已完成或部分的工作成果给网格。网格计算的许多有趣用途已被开发，包括的项目范围有：寻求智慧外星生物、进行蛋白质折叠、预测天气、地震建模、规划财务决策和解决素数问题。

网格计算关心的最大安全问题是每个工作包的内容潜在的完全暴露。许多网格计算项目是完全

开放的，所以没有任何限制，谁都可以在本地运行和处理应用程序，并参与网格的项目。这就意味着，网格成员可以保存每个工作包的副本并检查内容。因此，网格项目将不能保持保密性，以及也不适用于隐私、机密或专有数据。

网格计算每时每刻的计算能力都可能发生巨大变化。工作包有时回不来、回来晚或有损坏地返回。这将需要大量的返工，并导致工程在速度、进程、响应上的不稳定性，以及整个项目和每个网格成员的延时。对时间敏感的项目可能因为没有足够的计算时间而不能在指定时间期限内完成任务。

网格计算经常用一台中央核心服务器来管理项目、跟踪工作数据包并整合返回的工作分组。如果中央服务器过载或离线，会发生网格的彻底失败或崩溃。然而，通常当中央网格系统不可访问时，网格成员也可完成它们目前的本地任务，然后定期轮询去发现什么时候中央服务器重新联机。还有一个潜在的风险，就是一台被恶意控制的中央网格服务器可能被利用来攻击网格成员，或欺骗网格成员去执行非网格社区所期望的恶意行为。

9.5.3 点对点

点对点(Peer-To-Peer，P2P)技术是网络和分布式应用程序的解决方案，用于在点对点实体间共享任务和工作负载。这类似于网格计算，与网格计算的主要区别是：点对点没有中央管理系统，并且所提供的服务通常是实时的，而不是作为计算能力的集合。P2P 的常见例子包括许多 VoIP 服务，如 Skype、BitTorrent(用于数据/文件分布)和 Spotify(流媒体音频/音乐发行)。P2P 解决方案的安全问题包括传播盗版材料、有偷听分布式内容的能力、缺乏中央控制/监督/管理/过滤以及为服务消耗潜在可用带宽。

注意：

密码系统在第 6 章“密码学与对称加密算法”以及第 7 章“PKI 和密码学应用”中已进行详细描述。

9.6 工业控制系统

工业控制系统(ICS)是一种用于控制工业生产过程和机器的计算机管理设备。ICS 广泛应用于众多的工业行业，包括制造、装配、发电、配电、供水、污水处理、石油精炼。有几种 ICS 种类，包括集散控制系统(DCS)、可编程逻辑控制器(PLC)和数据采集与监控系统(SCADA)。

DCS 单元通常可以在工业处理方案中看到，负责从单个地点的大型网络环境中收集数据和实施控制。DCS 系统的一个重要方面是控制分布在所监测环境中的元件，如制造车间或生产线，以及集中监控场所向局部控制器发送命令，同时收集状态和性能数据。DCS 系统可以是模拟或数字系统，这取决于正在执行的任务或正在控制的设备。例如，液体流量值 DCS 系统将是一个模拟系统，而电压调节器 DCS 系统可能是一个数字系统。

PLC 是有效的单用途或专门用途的数字计算机。它们通常被部署用于各种工业机电自动化管理与操作，如装配线或大规模的数字灯光显示控制系统(如体育场内或拉斯维加斯大道上的巨型显示系统)。

SCADA 系统可以作为独立的设备使用，也可与其他 SCADA 系统组成网络或是与传统 IT 系统组成网络。大多数 SCADA 系统以最小的人机接口设计。通常，它们使用机械按钮和旋钮，或者使

用简单的液晶屏接口(类似于在一台商用打印机或 GPS 导航装置上看到的)。然而，网络 SCADA 设备可能有更复杂的远程控制软件接口。理论上，SCADA、PLC、DCS 单元和它们的最小人机接口的静态设计应该防止系统陷入危险或被修改。然而，这些工业控制设备很少集成安全，特别是在过去。但近年来有几个关于工业控制系统的著名威胁；例如，Stuxnet 首次在位于核设施的 SCADA 系统中放置了 rootkit。许多 SCADA 厂商已经开始实施安全，改进他们的解决方案以避免或至少减少未来的威胁。

9.7　评估和缓解基于 Web 系统的脆弱性

在基于 Web 的系统中有各种各样的应用和系统脆弱性与威胁，并且范围在不断扩大。脆弱性包括涉及 XML 和 SAML，以及许多在开放式 Web 应用程序安全项目(OWASP)中讨论的其他问题。

XML 利用是一种编程攻击，用来伪造信息并将其发送给访客或导致他们的信息系统在未授权的情况下丢弃信息。对 XML 攻击日益关注的一个领域是安全断言标记语言(SAML)。SAML 的滥用往往集中于网络认证。SAML 是一种在安全域之间基于 XML 的组织会话，用于交换通信、认证和授权的细节，通常运行于 Web 协议之上。SAML 通常用来提供基于 Web 的 SSO(Single Sign-On)解决方案。如果攻击者可以伪造 SAML 通信或窃取访问者的访问令牌，他们就可以绕过认证并获得对网站的未授权访问。

OWASP 是一个非营利性的安全项目，其重点在于提高在线或基于 Web 的应用程序的安全性。OWASP 不仅仅是一个组织，也是一个大型社区，可以一起自由地分享信息、方法、工具、更好的编码实践及更安全的架构部署等相关技术。更多的信息发布和社区参与，访问 www.owasp.org 网站。

9.8　评估和缓解移动系统的脆弱性

智能手机和其他移动设备呈现不断增加安全风险的趋势，因为它们开始能够把互联网与企业网络联系在一起。当个人拥有的设备被允许进入和离开有保障的设施，而不进行限制、监督或控制时，有潜在的危害是无疑的。

恶意内部人员可以通过外部不同类型的存储设备把恶意代码带入内部，这些设备包括手机、音频播放器、数码相机、存储卡、光盘和 USB 设备。这些存储设备还可以用来泄漏或窃取内部机密和私人数据，以至于泄露到外部(你认为维基解密的大部分内容是从哪里来的？)恶意的内部人员可以执行恶意代码、访问危险的网站或故意执行有害活动。

移动设备通常包含敏感数据，如联系人、短信、电子邮件和可能的记录及文档。任何具有相机功能的移动设备可以拍摄敏感信息或场地照片。移动设备的丢失或被盗可能意味着个人和/或公司的秘密遭受泄露。

注意：

由个人拥有的设备可以任意地由下面这些术语来表述：便携式设备、移动设备、个人移动设备(PMD)、个人电子设备或便携式电子设备(PED)和个人拥有设备(POD)。

移动设备是黑客和恶意代码的共同目标。不在便携式设备中存储敏感信息是很重要的；运行防

火墙和防病毒产品(如果可能的话)；并保持系统锁定和/或加密(如果可能的话)。

许多移动设备还支持 USB 连接桌面或笔记本电脑以同步通话记录和通讯录，以及传输文件、文档、音乐、视频等。

此外，移动设备对窃听不免疫。通过使用恰当的复杂设备，大多数手机的通话可以被窃听，更不用说在 15 英尺范围内的任何人都可以听到你说话。因此需要注意手机谈话，尤其是在公共场所时。

移动设备提供广泛的安全功能。然而，对这一功能的支持与对该功能的正确配置和启用不是一回事。只有当安全功能处于强制时才能获得安全保障。请务必检查所有所需的安全功能是否按预期正常运行在你的设备上。

Android

Android 是谷歌在 2005 年开发的一种基于移动设备的操作系统。2008 年发布了第一款安装了 Android 系统的设备。Android 源代码是通过 Apache 授权开放的，但大多数设备还是包括商用软件。虽然 Android 主要用在手机和平板电脑上，但它在广泛的设备上还是得到了应用，包括电视机、游戏机、数码相机、微波炉、钟表、电子阅读器、无绳电话甚至滑雪护目镜。

在手机和平板电脑上使用的 Android 允许广泛的用户定制：可以安装 Google Play 商店里的应用程序，也可以安装来自未知的外部源(如亚马逊的应用商店)的应用程序，此外许多设备支持用定制或修改版本更换默认版本的 Android 系统。然而，当 Android 在其他设备上使用时，它的实现更接近一个静态系统。

无论静态与否，Android 都有众多的安全漏洞。这些漏洞包括暴露于恶意的应用程序、运行恶意网站的脚本以及允许不安全的数据传输。Android 设备通常提升 root 权限(会破坏数据的安全和访问限制)，以给予用户充分的 root 级别的设备访问及底层配置设置权限。提升 root 权限增加了设备的安全风险，因为所有的运行代码都继承了 root 权限。

随着新版本的更新发布，Android 系统的安全性也得到了改进。用户可以调整众多的配置设置，以减少漏洞和风险。此外，用户可安装应用程序来为平台添加额外的安全功能。

iOS

iOS 是苹果公司用于 iPhone、iPad、iPod 等可移动设备以及苹果电视的操作系统。iOS 没有授权给任何非苹果硬件使用。因此，苹果公司完全控制 iOS 的特性和能力。然而，iOS 不是静态环境，因为用户可以从苹果超过 100 万应用的应用商店中安装任何一款应用。另外，iOS 经常发生越狱(打破苹果的安全和访问限制)，允许用户从第三方安装应用并获得更多控制和底层设置权限。越狱的 iOS 设备降低了其安全性，并使设备面临潜在的威胁。用户可以调整设备设置以增强 iOS 设备的安全性，也可安装诸多应用程序来添加安全功能。

9.8.1 设备安全

设备安全可以在一定范围内为移动设备提供潜在的安全选项或功能。不是所有的便携式电子设备(PED)都有很好的安全特性。但是，即使设备具有安全功能，但除非它们能被启用和正确配置，否则也是没有价值的。在做出购买决定之前，一定要考虑新设备的安全选项。

1. 全设备加密

一些移动设备，包括便携式电脑、平板电脑以及手机，均可提供设备加密。如果一台设备上大多数或所有的存储媒介都可以被加密，这将是一个有价值的功能。然而，加密不是对数据保护的保证，特别是在设备被盗而被解锁，或者系统本身有已知的后门攻击漏洞时。

当使用 IP 语音(VoIP)服务时，可以在移动设备上使用语音加密。计算机类似设备之间使用的 VoIP 服务比传统电话或典型手机更有可能提供一个加密选项。当语音会话被加密时，窃听谈话内容就变得毫无价值。

2. 远程擦除

如果设备丢失或被盗，远程擦除或远程清除就成为一种常见的措施。远程擦除可以让你远程地删除设备上的所有数据甚至配置设置。擦除过程可以通过移动电话服务或互联网连接进行触发。然而，远程擦除不是对数据安全性的保证。小偷可能足够聪明，他们会在转储数据时防止连接触发擦除功能。此外，远程擦除大部分是删除操作。使用反删除或数据恢复工具可以恢复擦除的设备上的数据。为了确保远程擦除破坏后恢复数据，应对设备进行加密。因此，反删除操作只会恢复加密数据，而攻击者无法对其进行破译。

3. 锁定

在移动设备上锁定类似于公司工作站上的账户锁定。当用户未能提供他们的凭据并多次重复尝试时，账户或设备被禁用(在一段时间内锁定)或直到管理员清除锁定标志。

移动设备可以提供锁定功能，但仅在锁屏已被配置的情况下才启用。然而，简单的屏幕滑动就可访问该设备并没有提供足够的安全性，因为身份认证过程没有发生。有些设备在尝试访问时，在发生多次认证失效的情况下会触发更长的时延。一些设备允许在触发数分钟的锁定之前设置尝试的次数(如三次)。其他设备则保持锁定并要求使用不同的账户或密码/代码重新进行访问。

4. 锁屏

锁屏是为了防止有人随便拾起并能使用你的手机或移动设备。然而，大多数的锁屏可以通过绘制图案或在数字键盘上键入数字来解锁。两者都不是真正的安全操作。锁屏可能有变通办法，如通过紧急呼叫功能访问电话应用程序。如果黑客通过蓝牙、无线或 USB 电缆等方式连接到设备上，锁屏就不一定真的能保护设备。

锁屏通常在一段时间后被触发。大多数电脑如果系统被闲置几分钟，它们将自动触发密码保护的屏幕保护程序。同样，许多平板电脑和手机在 30-60 秒后触发锁屏，并且屏幕变暗或关闭显示。如果设备处于无人值守状态或遭受丢失或被盗，锁定功能确保其他人很难访问你的数据或应用。解锁设备时必须输入密码、代码或 PIN、绘制模式；提供眼球或面部识别、扫描指纹或使用接近设备(如近场通信(Near-Field Communication，NFC))和射频识别(Radio-Frequency IDentification，RFID)环或片。

注意：

近场通信(NFC)是在靠近设备之间建立无线通信的标准。它可以让你执行一种类型的自动同步和实现设备之间的关联，通过一起触摸它们来把它们靠近在几英寸范围内。NFC 常见于智能手机和移动设备配件。它通常用于执行设备到设备的数据交换，建立直接通信，或者通过与无线接入点链

接并借助 NFC 访问更复杂的服务，如 WPA-2 加密的无线网络。因为 NFC 是一种基于射频的技术，所以它不是没有漏洞。NFC 攻击可包括中间人攻击、窃听、数据操纵和重放攻击。

5. GPS

许多移动设备都包括一个 GPS 芯片，以支持和受益于本地化的服务，如导航，所以有可能跟踪这些设备。GPS 芯片本身通常只是一个在轨 GPS 卫星的信号接收器。然而，移动设备上的应用程序可以记录设备的 GPS 位置，然后报告给一个在线服务。可以使用 GPS 跟踪以监控自己的运动、跟踪他人(如未成年人或送货人员)的运动或跟踪一台被盗的设备。但对于 GPS 的跟踪工作，移动设备必须通过互联网或无线电话服务来交流位置信息。

6. 应用控制

应用控制是一种设备管理解决方案，可以限制设备上应用的安装，也可以被用来强制安装特定的应用或执行某些应用的设置，以支持安全基线或保持其他形式的合规性。应用控制往往通过限制用户的能力，来安装来自未知来源或提供非工作相关功能的应用，以减少对恶意程序的暴露。

7. 存储分隔

存储分隔被用来人为地在存储介质上划分不同类型或数值的数据。在移动设备上，设备制造商和/或服务提供商可以使用存储分隔将设备的操作系统及预装应用程序与用户安装程序和用户数据进行隔离。一些移动设备管理系统进一步实施隔离，将公司数据和应用程序与用户数据和应用程序分离。

8. 资产跟踪

资产跟踪是一个管理过程，用于保持对库存的监督，如已部署的移动设备。资产跟踪系统可以是被动的或主动的。被动系统依赖于资产本身来定期检查或当办公室里每一次员工工作时检测设备的存在。主动系统使用轮询或推送技术向设备发送查询以获取响应。

可以使用资产跟踪来验证设备仍然处于被指定授权用户的手中。一些资产跟踪解决方案可以定位丢失或被盗的设备。

一些资产跟踪解决方案在硬件库存管理上进行扩展，它们可以监督已安装的应用程序、应用程序的使用、存储的数据以及设备上的数据访问。可以使用这种类型的监控，以验证安全指引的合规性或检查机密信息是否暴露给未经授权的实体。

9. 库存控制

术语“库存控制”可描述硬件资产的跟踪(已在前面的主题中讨论)。然而，它也可以指使用移动设备作为一种手段在仓库或存储柜中跟踪库存。大多数移动设备都有一个摄像头。通过移动设备的相机，应用程序可以通过拍照或扫描条形码的方式来跟踪实物。具备 RFID 和 NFC 功能的移动设备也能够与已使用电子标签的对象及其容器进行交互。

10. 移动设备管理

移动设备管理(Mobile Device Management，MDM)是一个管理移动设备的软件解决方案，该方案解决员工使用移动设备访问公司资源的挑战性任务。MDM 的目标是提高安全性，提供监测、远

程管理、支持和故障排除。许多 MDM 解决方案支持广泛的设备型号并可跨越多个服务提供商进行操作。可以使用 MDM 通过移动网络或 Wi-Fi 连接来推送或删除应用程序，管理数据并强化配置。MDM 不仅可以用来管理公司拥有的设备，也可以用来管理个人拥有的设备(如在自带设备(Bring-Your-Own-Device，BYOD)环境中)。

11. 设备访问控制

如果希望锁定手机并提供真正的安全，那么在手机或其他移动设备上使用一个强大的密码将是一个很好的思路。然而大多数移动设备并不安全，即使有一个强大的密码，仍可通过蓝牙、无线或 USB 电缆访问该设备。对于一个特定的移动设备，如果其系统支持锁定功能来阻止访问该设备，那么这个功能是有价值的。当设备上出现一段时间的活动闲置或手动初始化时，该功能设置将自动触发。当你支持设备密码和存储加密时，通常可以获得这个好处。

应该考虑更多的可行方法来减少对移动设备的未授权访问。许多 MDM 解决方案可以强制锁屏配置和防止用户禁用该功能。

12. 可移动存储

许多移动设备支持可移动存储。有些设备支持 microSD 卡，该卡可用于在移动设备上扩展存储。然而，大多数手机在添加或删除存储卡时需要取出背板、移除电池。更大的手机、平板电脑和笔记本电脑提供在设备侧面方便插入的卡槽。

许多移动设备还支持外接 USB 存储设备，如闪存驱动器和外部硬盘驱动器。这可能需要一条特殊的(On-The-Go，OTG)电缆。

此外，还有移动存储设备可以通过板载无线接口提供蓝牙或 Wi-Fi 的方式访问存储数据。

13. 关闭不使用的功能

虽然启用安全功能对于它们获得任何有利影响是必要的，但是删除那些对业务任务和个人使用无关的应用程序和禁用其功能，同样也很重要。启动的功能和安装的应用范围越广，利用或软件缺陷给设备和存储的数据带来损害的可能性就越大。常见的安全措施，例如加固，可减少对移动设备的攻击面。

9.8.2　应用安全

除了管理移动设备的安全性，还需要专注于这些设备上使用的应用程序和功能。关于台式机或笔记本电脑系统的大多数软件的安全考虑就像安全实践常识一样，同样适用于移动设备。

1. 密钥管理

密钥管理始终是加密时涉及的一个关注点。大多数密码系统问题都出在密钥管理而不是算法上。好的密钥选择基于随机数的质量和可用性。大多数移动设备必须依赖本地的、不好的随机数产生机制，或在无线链路上访问更强大的随机数发生器(RNG)。一旦创建密钥，它们需要以尽量减少暴露损失或风险的方式进行存储。密钥存储的最佳选择通常是可移动硬件和可信平台模块(TPM)，但手机和平板电脑很少提供这些选择。

2. 凭证管理

处在中心位置的凭据存储被称为凭据管理。对于广泛的互联网网站和服务，每一个都有自己特定的登录要求，使用独特的名称和密码将是负担。凭据管理解决方案提供了一种方法来安全地存储大量的凭据集。通常这些工具在需要时使用主凭证集(优选多因子)来解锁数据集。一些凭证管理选项甚至可以为应用程序和网站提供自动登录选项。

3. 认证

移动设备上的认证或对移动设备的认证通常相当简单，特别是对于移动电话和平板电脑来说。然而，滑动或模式访问不应该被认为是真正的认证。如有可能，使用密码、提供 PIN、提供眼球或人脸识别、扫描指纹或使用距离装置(如 NFC、RFID 环或块)。这意味着如果正确实施，小偷将难以绕过设备认证。正如前面提到的，需要谨慎地结合设备认证与设备加密，以阻止通过连接电缆访问存储的信息。

4. 地理标记

具有 GPS 支持的移动设备，支持在使用设备拍摄照片时不仅嵌入拍摄照片的日期/时间信息，还可以嵌入纬度和经度形式的地理位置标记。这将允许攻击者从社交网络或类似网站上查看照片并确定究竟在何时何地拍摄。地理标记可用于非法目的，例如确定一个人什么时候进行正常的日常活动。

5. 加密

加密往往是有用的，无论数据处于存储还是传输中，能提供对未授权数据访问的保护机制。大多数移动设备提供某种形式的存储加密。当使用它们时，加密应该被启用。一些移动设备提供了本地支持的通信加密，但大多数可以运行附加软件(应用程序)，它们可以添加加密的数据会话、语音通话和/或视频会议。

6. 应用白名单

应用白名单是禁止未授权软件能够被执行的安全选项。白名单也被称为默认拒绝或隐含拒绝。在应用安全中，白名单阻止任何或所有软件(包括恶意代码)的执行，除非它们在预先批准的例外名单中：白名单。这是来自于典型安全设备立场的重要违背，就是被默认允许和被异常拒绝(也就是常说的黑名单)。

由于恶意软件的增长，应用白名单的方法是为数不多的几个选项，以维护对设备和数据安全的真实承诺。然而，没有任何安全解决方案是完美的，包括白名单。所有已知的白名单解决方案可以通过内核级漏洞和应用程序的配置问题绕过。

9.8.3 BYOD 关注点

BYOD 是一项策略，允许员工在工作中携带自己的个人移动设备并使用这些设备连接(或通过)公司网络业务资源和/或互联网。虽然 BYOD 可以提高员工的士气和工作满意度，但却增加了组织的安全风险。如果 BYOD 策略是开放式的，那么任何设备可以连接到公司网络。并不是所有的移动

设备都有安全功能，因此这样的策略不符合设备连上生产网络的标准。BYOD 策略应强制要求特定的设备以减少这种风险，但它可能会要求公司为那些无法购买自带兼容设备的员工购买设备。关于许多其他的 BYOD 问题将在下面的章节中讨论。

用户需要了解在工作中使用他们自己的设备的好处、限制和后果。阅读并签署 BYOD 策略，参加回顾和培训计划以具备充足、合理的意识。

1. 数据所有权

当个人设备用于业务任务时，会发生个人数据和业务数据混合在一起的可能性。一些设备可以支持存储分隔，但不是所有的设备都可以提供数据类型隔离。建立数据所有权是十分复杂的。例如，如果一台设备丢失或被盗，公司可能希望触发远程擦除，擦除该设备上所有有价值的信息。然而，员工往往会抵抗这一点，尤其是在设备有被发现或返回的任何希望时。擦除可以抹去所有的企业和个人数据，这可能对个人而言是重大损失——尤其是如果设备没有恢复，擦除看起来会是过度反应。应建立数据所有权明确的策略。一些 MDM 解决方案可以提供数据隔离、分隔，支持业务数据处理且不影响个人数据。

BYOD 策略有关数据所有权和针对移动设备的备份。业务数据和个人数据应该受到备份解决方案的保护，无论是提供给设备上的所有数据的单一解决方案，还是为每种种类或类型数据提供的单独解决方案。这降低了在远程擦除事件中数据丢失的风险，以及设备故障或损坏的风险。

2. 所有权支持

当员工的移动设备遭遇了故障、错误或损坏，谁将负责设备的维修、更换或技术支持？BYOD 策略应该确定什么样的支持将由公司提供，什么样的支持留给个人。如果相关，还包括他们的服务提供商。

3. 补丁管理

BYOD策略应该定义个人拥有移动设备的补丁管理方法和机制。是否是由用户负责安装更新？是否是由用户安装所有可用的更新？设备安装前是否应由公司对更新进行测试？更新是否通过无线方式处理(通过服务提供商)或Wi-Fi？是否有无法使用的移动操作系统版本限制？需要什么补丁或更新级别？

4. 反病毒管理

BYOD 策略应该规定反病毒软件、反恶意软件以及反间谍扫描软件是否要在移动设备上安装。策略应说明被推荐的产品/应用程序的使用，以及这些解决方案的设置。

5. 取证

BYOD 策略应该解决相关移动设备的取证和调查。用户需要知道某个安全的违法或犯罪活动事件是否可能涉及自己的设备，是否可能受到强制要求收集这些设备的证据。一些证据的收集过程可能是破坏性的，一些法律调查则可能需要没收设备。

6. 隐私

BYOD 策略应该解决隐私和监控问题。当个人设备用于工作时，在用户享受使用个人设备用于

工作的便利时往往会失去一些或所有隐私。员工可能需要同意在他们的移动设备上进行跟踪和监控，即使不在公司的财产范围和工作时间以内。个人应考虑到在 BYOD 下使用个人设备，此时设备将被视为准公司资产。

7. 在线/不在线

BYOD 策略应解决个人移动设备在线和不在线的处置。BYOD 的在线处置包括安装安全、管理和生产应用程序以及实现安全和生产配置设置。BYOD 不在线处置包括正式的业务数据擦除以及移除任何特定的业务应用。在某些情况下，可能规定完整的设备擦除和出厂恢复。

8. 遵守公司策略

BYOD 策略应清楚地表明：使用个人移动设备的业务活动并不表明可不遵守公司的策略。员工应该将 BYOD 设备视为公司财产，从而保持其与所有限制的合规性，甚至当其离线或处在休息时间时。

9. 用户接受

BYOD 策略需具体明确所有在工作中使用个人设备的内容。对于许多用户来说，BYOD 下的限制、安全设置和 MDM(移动设备管理)跟踪实施会比他们期望的更为苛刻。因此，组织应该在容许个人设备到生产环境之前努力充分解释 BYOD 策略的细节。只有当一名员工表示同意和接受时，通常通过签名，才能将他们的设备上线。

10. 架构/基础设施考虑

在实施 BYOD 时，组织应评估他们在网络和安全方面的设计、架构和基础设施。如果每个员工都带来个人设备，网络上设备的数量可能加倍。这需要规划来处理 IP 分配、通信隔离、数据的优先级管理、提高入侵检测系统(IDS)和入侵防御系统(IPS)监测负荷，以及提高带宽消耗，包括内部和互联网连接。大多数移动设备支持无线功能，所以这可能需要更强大的无线网络以及处理 Wi-Fi 拥塞和干扰。BYOD 需要考虑触发的额外基础设施成本。

11. 法律问题

公司律师应该对 BYOD 的法律问题进行评估。在业务任务的执行中，使用个人设备可能意味着风险负担增加和数据泄漏的责任。BYOD 可能让员工高兴，但对组织而言可能并不值得或并非实现有效的成本节约。

12. 可接受策略

BYOD策略应参考本公司可接受的使用策略或包括专注于独特问题的移动设备特定的策略版本。随着在工作中使用个人移动设备，将增加信息泄露、信息分发以及不适当的内容访问的风险。员工们应该保持清醒的意识，在工作中的首要目标是完成生产任务。

13. 机载摄像头/视频

BYOD 策略需要解决移动设备的机载摄像头问题。一些环境不允许任何类型的相机，这就要求 BYOD 设备没有相机。如果相机是允许的，应当清晰地在文档中说明可以使用或不可以使用的范围

并向员工进行解释。移动设备可以作为存储设备，向外部供应商或服务提供一条备用的无线连接通路，也可用于图像采集并通过视频泄露机密信息或设备。

9.9　评估和缓解嵌入式设备和物联网系统的脆弱性

嵌入式系统是通过计算机实现的一个更大系统的一部分。嵌入式系统通常围绕与更大的产品相关的一系列有限和特定的功能而进行设计，并成为它的一个组成部分。嵌入式系统可能由在典型计算机系统中找到的相同组件组成，也可能是一个微控制器(集成芯片与主板上的内存和外设端口)。嵌入式系统的例子包括网络连接打印机、智能电视、空调控制、智能家电、智能恒温器、福特 SYNC(一个车辆终端的微型嵌入式系统)以及医疗器械。

关于嵌入式系统的另一个类似的概念是静态系统(又名静态环境)。静态环境是一组不改变条件、事件和周边的环境。理论上，一旦理解，就知道静态环境不提供新的或令人惊讶的元素。静态的 IT 环境可以是任何系统，其用户和管理员的目的是保持环境不变。整个目标是防止或最大程度减少用户可能导致降低安全性或操作功能性的实施变更。

在技术上，静态环境是应用程序、操作系统、硬件设置或网络被配置为满足特定的需要、能力或功能，然后保持设置不变。然而，尽管使用了“静态”这个术语，但没有真正的静态系统。因为总是存在改变环境的情况，如硬件故障、硬件配置变更、软件缺陷、软件设置的变更或漏洞，最终导致不希望的操作参数和实际上的安全入侵。

9.9.1　嵌入式系统和静态系统的示例

支持网络功能的设备是那些本身有网络功能的便携或非便携设备。通常假定存在问题的网络是无线网络，主要是由移动通信公司提供。然而，也可以指连接 Wi-Fi 的设备(特别是当它们可以自动连接时)、可以通过无线电信服务共享数据连接的设备(如移动热点)，以及拥有可插入标准以太网电缆的 RJ-45 有线连接插孔的设备。支持网络功能的设备，包括智能手机、平板电脑、智能电视、机顶盒或 HDMI 流媒体播放器(如 Roku 播放器、亚马逊 Fire TV 或谷歌 Android TV/Chromecast)，网络连接的打印机、游戏系统以及其他更多的设备。

注意：

在某些情况下，支持网络功能的设备可能支持蓝牙、NFC 等无线连接技术。此外，一些供应商提供的设备，可以在本身不具备网络支持的情况下添加网络功能。这些附加的设备可能被视为支持网络功能的设备(或者更具体地说，支持网络的设备)，它们的合力增强设备也可被视为支持网络的设备。

网络物理系统指的是提供一种计算手段来控制物理世界中某样东西的设备。在过去，这些可能被称为嵌入式系统，但网络物理的类别似乎更侧重于物理世界的结果，而不是计算方面。网络物理设备和系统本质上是机器人技术和传感器网络中的关键要素。基本上，可以使运动发生在现实世界中的任何计算装置都是机器人元素，而任何这样可以检测物理条件(如温度、光、运动、湿度)的设备被称为传感器。网络物理系统的例子包括增强或协助人类能力的假肢、车辆碰撞躲避、空中交通管制协调、精密机器人手术、危险条件下的远程操作，以及车辆、设备、移动设备和建筑物的节能。

网络物理系统、嵌入式系统和具备网络功能的设备的一种新扩展是物联网(IoT)。物联网是设备的集合，可以通过互联网与其他设备或通过控制台来影响和监视真实世界。物联网设备可能被标记为智能设备或智能家居设备。许多办公建筑物内的工业环境控制思路是找到自己的方式为小型办公室或个人家庭消费者提供更多可用的解决方案。物联网不仅限于静态定位设备，也可以用于土地、空气、水上车辆或移动设备的关联方面。

大型机是高端计算机系统并用于执行高度复杂的计算和提供大容量的数据处理。老式的大型机可以被认为是静态环境，因为它们通常围绕单一的任务进行设计或支持单一的关键任务应用。这些配置没有提供显著的灵活性，但它们确实提供了高稳定性并能长期运行。许多主机能够运营数十年。

现代大型机更灵活，通常用于为支持众多的虚拟机提供高速计算能力。每个虚拟机都可以拥有一个独特的操作系统并反过来支持广泛的应用。如果一个现代大型机为操作系统或应用程序提供固定或静态的支持，它就可被认为是静态环境。

游戏机，无论是家庭系统还是便携式系统，都是潜在的静态系统的例子。游戏控制台的操作系统一般是固定的，只有当供应商发布系统升级时才会改变。这样的升级往往混合了操作系统、应用程序和固件的改进。虽然游戏控制台功能一般都集中在玩游戏和媒体，但现代控制台可能会提供对一系列改善和第三方应用程序的支持。更灵活和对开放式应用程序的支持，将使成为静态系统的可能性减小。

车辆计算系统可以包括用于监视发动机性能和优化制动、转向及悬挂的组件，也可包含和驾驶、环境控制及娱乐相关的内置元素。早期的车辆系统是静态环境，很少或根本没有能力进行调整或改变，尤其是由车主/司机进行调整。现代车辆系统可提供更广泛的功能，包括连接移动设备或运行自定义的应用程序。

9.9.2 安全方法

嵌入式系统和静态系统的安全问题包括以下事实：大多数集中在如何最大限度地降低成本和无关的功能上。这往往会导致缺乏安全性且难于升级或安装补丁。由于嵌入式系统在真实世界中是一种控制机制，因此一个安全漏洞可能会造成对人和财产的损害。

静态环境、嵌入式系统和其他有限或单一用途的计算环境需要安全管理。虽然它们可能没有广泛的攻击面，并且没有暴露过多的风险，但作为通用的计算机，它们仍然需要适当的安全治理。

1. 网络分隔

网络分隔涉及控制网络设备之间的流量。完整或物理的网络分隔发生在网络与所有外部通信完全隔离时，这时传输仅限于处于分隔网络的设备之间。可以在交换机上通过 VLAN 或其他通信控制手段，包括 MAC 地址、IP 地址、物理端口、TCP 或 UDP 端口、协议、应用程序过滤、路由和访问控制管理来实现逻辑网络的分隔。网络分隔可以用来隔离静态环境，以防止变更和/或因可到达而被利用。

2. 安全层

当不同级别分类或灵敏度不同的设备被分组在一起时，就存在安全层，从而对不同级别的分组进行隔离。这种隔离可以是无条件或单向的。例如，较低级别可能无法启动与更高级别的通信，但更高级别可以初始与较低级别的通信。隔离也可以是逻辑上或物理上的。逻辑隔离要求对数据包使

用分类标签，它们必须被尊重并在网络管理、操作系统和应用上进行强制实施。物理隔离需要实现不同安全级别网络之间的网络分隔或空间隔断。

3. 应用防火墙

应用防火墙是设备、服务器插件、虚拟服务或系统过滤器，定义了在服务和所有用户之间严格的通信规则。目的是成为服务器端防火墙特定的应用程序，以防止特定应用协议和载荷攻击。

网络防火墙是一种硬件设备，通常被称为专为一般网络过滤而设计的装置。网络防火墙的目的是提供全网的广泛保护。

这两种类型的防火墙十分重要并在多个情况下是相关的。每一个网络都需要一道网络防火墙。许多应用程序服务器需要一道应用防火墙。然而，有了应用防火墙的位置并非不需要网络防火墙。应该使用两个防火墙来进行相互补充，而不是把它们视为竞争性解决方案。

4. 手动升级

手动更新应该用在静态环境下以确保只实施测试和授权更改。使用自动更新系统将允许未检测的更新引进未知的安全性降级。

5. 固件版本控制

类似于手动更新软件，在静态环境中严格控制固件是十分重要的。固件更新应该在手动的基础上实现，并且只有通过测试和审查才能进行。对固件版本控制的监督应着眼于保持稳定的操作平台，同时尽量减少危险暴露和停机时间。

6. 包装

包装是指用来封闭或包含其他东西。包装在安全社区是众所周知的，往往被关联到木马恶意软件。这种包装用来将一台良性主机与恶意的有效载荷结合起来。

包装也可作为封装解决方案。一些静态环境可能被配置为拒绝更新、更改或软件安装，除非它们通过一条控制信道引入。控制信道可以是特定的包装器。该包装器可以包括完整性和认证功能，以确保只有预期和授权的更新被应用于系统中。

7. 控制冗余和多样性

与任何安全解决方案一样，依靠单一的安全机制是不明智的。深度防御以同心圆或平面层方式使用多层访问控制。这种分层的安全形式有助于组织避免整体单一的安全状态。整体的心态是相信单一的安全机制可完全提供所需的足够安全性。通过冗余和多样性的安全控制，静态环境可以避免单一安全功能失效的陷阱，使得环境有多个机会转移、拒绝、检测并阻止任何威胁。遗憾的是，没有任何安全机制是完美的。每一个单独的安全机制都有漏洞或变通方案，在等待着被黑客发现和滥用。

9.10　基本安全保护机制

操作系统内对安全机制的需求来自于如下简单的事实：软件是不可信的。无论来自何人或何处，

第三方软件总是不可信的。这并不是说所有软件都是恶意的，而是说明一种保护观点：所有第三方软件都是 OS 创建者之外的人编写的，这样的软件可能导致问题。因此，将所有非 OS 软件都视为存在潜在危害性，这允许操作系统通过使用软件管理保护机制来阻止许多灾难的发生。OS 必须利用保护机制来保持计算环境的稳定并且进程间彼此隔离。如果没有这些努力，那么数据的安全性永远是不可靠的，甚至是不可能的。

在设计安全系统时，计算机系统设计人员应当遵守许多种通用的保护机制。这些原则是更通用的安全规则的特定实例，用于管理安全计算实践。在开发的早期阶段就在系统中引入安全设计，将有助于确保整个安全架构的成功和可靠。接下来将把保护机制分为两个方面加以讨论，即技术机制和策略机制。

9.10.1 技术机制

技术机制是系统设计人员针对系统建立的控制措施。我们将介绍下列 5 种机制：分层法、抽象、数据隐藏、进程隔离和硬件分隔。

1. 分层法

通过分层法处理，可以实现与用于操作模式的环模型(本章前面讨论过)类似的结构，并且能够应用于每一个操作系统进程。分层法将进程最敏感的功能放在中心，并且用逐渐扩大的同心圆代表敏感度较低的功能(使用稍有不同的方式，有时也采用术语“较高层”和“较低层”进行阐述，从较低层进入较高层时，安全性与特权会被减弱或减少)。讨论 OS 体系结构时，保护环的概念十分常见，但并非唯一的。使用与环不同的级别概念也可以表示相同的基本思想。在这样的系统中，最高级别具有最大的特权，而最低级别则具有最小的特权。

使用“级别”替代“环”

讨论多层或多级系统时，常常会应用许多与保护环概念相同的特性和约束。以一幢高层公寓建筑为例，租金较低的公寓往往位于较低的楼层。到达公寓的中间层时，公寓往往更大，视野往往开阔。最后，位于顶层(或最高几层)的公寓总是最宽敞的，并且租金也是最贵的(常常是豪华的顶层房间)。通常，如果居住在大楼中低租金的公寓内，就不能乘坐电梯到达租金更贵的更高楼层；如果居住在中间楼层的公寓内，那么除了豪华房间所在的楼层，可以乘坐电梯到达任何楼层；如果居住在豪华的顶层房间，那么可以乘坐电梯到达自己想去的任何楼层。在办公楼和宾馆内，也可以发现这样的楼层约束系统。

分层或多级系统的顶端与保护环方案的中心环相同。同样，分层或多级系统的底部与保护环方案的外环相同。级别通常与层相同，往往与环也是相同的(至少在保护和访问概念方面是相同的)。此外，级别、层或环可以被称为域(也就是具有单一特征的客体集合)。

层与层之间的通信只能使用定义良好的特定接口，以便提供必要的安全性。来自外部(低敏感度)层的所有入站请求都必须经过严格的身份认证和授权检查，然后才能被允许继续进行(或者在未通过检查的情况下被拒绝)。为安全性使用的分层法类似于使用安全域和格子型安全模型，安全性以及对特定主体和客体的访问控制与指定的层和特权相关联，并且从外部层移至内部层时访问特权会增加。

事实上，不同的层只能通过特定的接口进行通信，这种接口被设计用于维护系统的安全性和完

整性。即使低安全性的外部层依赖于来自更高安全性的内部层的服务和数据，它们也仍然只知道如何与这些内部层接口，但是对内部层的内部结构、特征或其他细节毫无了解。为了维护层的完整性，内部层既不了解也不依赖于外部层。无论任何一对层之间存在何种安全关系，都不会对对方造成影响(因此每个层都不会遭受其他层的篡改)。最后，外部层不能违反或重写内部层强制实施的任何安全策略。

2. 抽象

抽象是支持面向对象编程的领域的基本原则之一。它属于“黑箱”原则，即认为对象(或操作系统组件)的用户没有必要知道对象的工作细节，而是只需知道使用对象的正确语法和作为结果返回的数据的类型(也就是如何发送输入和接收输出)。这往往涉及对数据或服务的中间访问，就像用户模式中的应用程序使用系统调用请求管理员模式中的服务或数据一样(根据请求者的凭证和特权授予或拒绝这种请求)，而不是获得直接的、非中间的访问。

抽象的另一种安全应用方式引入了对象组(有时也被称为类)，此时访问控制和操作权限被分配给对象组，而不是在每个对象的基础上进行分配。这种方式允许安全管理员方便地定义和命名对象组(通常与作业角色或职责有关)，并且使权限和特权管理变得更为容易(当把对象加入某个类时，就能赋予权限和特权，从而不必单独针对每个对象管理权限和特权)。

3. 数据隐藏

数据隐藏是多级安全系统的一个重要特征，它能够确保存在于某个安全级别的数据对于运行在不同安全级别的进程来说是不可见的。数据隐藏背后的重要概念是：保证不必知道在某个级别访问和处理数据所涉及细节的人无法偷偷摸摸地或违法地了解和查看这些细节。从安全性的角度看，数据隐藏依赖于将客体置入不同于主体所占用容器的其他安全容器中，从而对不必对客体细节进行了解的人隐藏相关的细节。

4. 进程隔离

进程隔离要求操作系统为每个进程的指令和数据提供不同的内存空间。此外，还要求操作系统强制实施这些分界，以阻止某一进程读取或写入属于另一个进程的数据。使用进程隔离技术主要有下列两个优点：

- 阻止未经授权的数据访问。进程隔离是多级安全模式系统的基本要求之一。
- 保护进程的完整性。如果没有这样的控制措施，那么设计糟糕的进程可能会出现错误，并且将数据写入分配给其他进程的内存空间，从而导致整个系统不稳定，而不仅仅是影响错误进程的执行。在更恶意的情况下，进程可能试图(甚至可能成功)读取或写入超出其处理范围的内存空间、入侵或攻击其他进程。

通过在每个用户或每个进程的基础上实现所谓的虚拟机，许多现代操作系统都满足了对进程隔离的需求。虚拟机表示具有处理环境的用户或进程，处理环境包括内存、地址空间以及其他关键的系统资源和服务，并且使这个用户或进程看起来像是对整个计算机进行唯一、排他性的访问。在不需要了解可能在同一台计算机上同时执行操作的其他用户或进程的情况下，这种方式允许每个用户或进程进行独立操作。作为操作系统提供的对系统的中间访问的一部分，进程隔离机制映射了用户模式中的虚拟资源和访问，从而能够使用监管模式调用来访问对应的实际资源。这种机制不仅为编程人员提供了方便，而且也防止单独的用户或进程遭受其他用户或进程的影响。

5. 硬件分隔

硬件分隔的目的与进程隔离类似：用于阻止对属于不同进程/安全级别的信息的访问。二者的主要差异是：硬件隔离通过使用物理方式的硬件控制措施来强制实施这些要求，而不是通过操作系统强加的逻辑进程隔离控制方法。硬件分隔较为少见，通常被限制在国家安全实现中。在这种实现中，额外的成本和复杂度由所涉及信息的敏感度和未授权访问或泄露固有的风险抵销。

9.10.2 安全策略与计算机体系结构

正如安全策略指导组织中日常的安全操作、过程和措施一样，它在设计和实现系统时也扮演了重要的角色。无论系统完全由硬件组成、完全由软件组成还是由软件和硬件组合而成，情况都是如此。在这种情况下，安全策略的角色是告知和指导某些特殊系统的设计、开发、实现、测试和维护。因此，这种安全策略主要关注于单一的实现努力(尽管可能改编自其他类似的实现努力，但是应当尽可能准确和完整地反映目标)。

对于系统开发人员而言，安全策略最好通过文档形式定义一组规则、实践和措施，它们描述了系统应当如何管理、保护和分布敏感的信息。阻止信息从较高安全级别流向较低安全级别的安全策略被称为多级安全策略。随着系统开发的进行，应当针对所有适用的系统组件或元素(包括以下全部或其中的一部分：物理的硬件组件、固件、软件以及组织如何交互和使用系统)设计、构建、实现和测试安全策略。总之，安全考虑应该贯穿项目的整个生命周期，而不是到最后才考虑，否则更容易遭受失败。

9.10.3 策略机制

正如任何安全程序一样，还应当采用适当的策略机制。这些机制是基本计算机安全原则的扩展，但是本节所描述的应用情况是针对计算机体系结构和设计的。

1. 最小特权原则

在第 13 章“管理身份与认证”中，将介绍与一般安全性有关的最小特权原则以及如何应用于计算系统的用户。这条原则对于计算机和操作系统的设计也非常重要，尤其是在应用于系统模式时。当设计操作系统进程时，无论什么时候都应当始终确保进程在用户模式中运行。在特权模式中执行的进程数目越多，为了获得监管系统访问特权的怀有恶意的人发现的系统潜在脆弱性的数目就越多。一般而言，最好使用 API 来请求监管模式服务，或者在必要时，从用户模式应用程序将控制权传递至可信的、保护良好的监管模式进程(而非将这样的程序或进程一起提升至监管模式)。

2. 特权分离

特权分离的原则建立在最小特权原则的基础之上，它要求使用细粒度化的访问特权，也就是说，给每一种类型的特权操作分配不同的特权。这就允许设计人员分配执行特定监控功能的权限，同时不需要授予不受限制访问系统的权限。特权分离还允许查看对服务的单个请求或对资源的单个访问，针对访问控制进行检查，以及基于请求用户的身份或者基于所属用户组或用户的安全角色来准许或拒绝请求。

职责分离可以被视为针对管理员的最小特权原则的应用。在大多数中到大型的组织中存在许多管理员，每个管理员会被分配不同的任务。因此，单个管理员往往不可能具有对整个环境或基础设施的完全访问权限。例如，某位用户管理员不需要支持重新配置网络路由、格式化存储设备或完成备份功能的特权。

职责分离也是一种用于防止访问特权和工作任务分配出现冲突的工具。例如，负责编码的人员不能完成测试和实现编码的任务。同样，负责账户支付工作的人员不能负责账户的收款工作。通过正确地实现职责分离，就可以安全地管理许多这样的作业或任务冲突。

3. 可问责性

可问责性是任何安全设计中的一个重要组成部分。许多安全要求较高的系统都包含强制实施个人特权操作行为可问责性的物理设备，例如，手写访问日志和无法修改的审计跟踪。然而，一般而言，这样的功能依赖于系统是否能够监控发生于系统资源和配置数据上的活动与交互，以及是否能够保护生成的日志不会被未授权访问或更改，以便日志提供准确可靠的活动和交互记录，这些记录说明了每个用户(包括管理员或其他具有高特权级别的可信个体)在系统中的活动历史。为了支持可问责性，除了需要可靠的审计和监控系统之外，还需要灵活的授权系统和完美的身份认证系统。

9.11　常见的缺陷和安全问题

任何安全体系结构都不是绝对安全的。每个计算机系统中都存在缺点和脆弱性。安全模型和体系结构的目的是要尽可能多地解决已知的缺陷。下面将讨论一些比较常见的影响计算机系统的安全问题。你不仅应当理解每一个安全问题，而且需要知道它们如何降低了整个系统的安全性。某些问题和缺陷彼此重叠，并且被攻击者以一种创造性的方式用于攻击系统。虽然下面的讨论中覆盖了最常见的缺陷，但是还不够详尽。攻击者往往是非常狡猾的。

9.11.1　隐蔽通道

隐蔽通道是用于传递信息的方法，通常不用于通信。因为隐蔽通道的路径通常不用于通信，所以不会受到系统正常安全控制方法的保护。使用隐蔽通道提供了违反、绕过或回避安全策略而不被发现的一种方法。隐蔽通道是安全架构脆弱性的一个重要例子。

正如你想象的那样，隐蔽通道与公开通道是对立的。公开通道是一种已知的、预期的、被授权的、经过设计的、受监控的和受控的通信方法。

目前存在下列两种基本的隐蔽通道类型：

时间隐蔽通道　通过以一种可预测的方式改变系统组件的性能或更改资源的时间安排来传达信息。使用时间隐蔽通道通常是一种比较复杂的传送数据的方法，并且难以检测。

存储隐蔽通道　通过将数据写入其他进程可以读到的公共存储区域来传达信息。当评估软件安全时，需要注重评估任意进程将信息写入内存中任意位置时，是否可能被其他的进程读取。

这两种隐蔽通道都是依靠使用通信技术与其他未经授权的主体交换信息。因为隐蔽通道的性质是与众不同的，并且位于正常的数据传送环境之外，所以对其进行检测十分困难。针对任何隐蔽通道活动的最佳防护措施是实现审计和分析日志文件。

9.11.2 基于设计或编码缺陷的攻击和安全问题

较差的设计方法、可疑的实现应用和措施，或者不充分的测试，都可能导致特定的攻击。某些攻击是由蓄意的设计方案导致的，此时代码中构建了能够回避访问控制、登录或其他安全检查的特殊入口点，这些代码往往是在开发阶段添加的，但是在投入生产时未被去除。从我们的角度出发，因为这些入口点通过设计避开了安全措施，所以它们恰如其分的名字为后门，本章稍后的“维护钩子和特权程序”部分会进行更多的介绍。广泛的测试和代码检查要求找出这样隐蔽的访问方式，在开发的最后阶段能够轻易地去除后门，但在测试和维护阶段，却极难检测后门。

尽管功能测试对于商业代码或应用来说非常普遍，但是随着对病毒和蠕虫攻击、SQL 注入攻击、跨站脚本攻击和广泛使用的联机公共站点偶尔受到毁损或破坏的广泛宣传，对安全问题的单独测试在近几年来逐步受到关注和赢得信誉。接下来，我们将介绍常见的攻击或安全脆弱性来源，这些来源是由于设计、实现、预先释放代码清除故障或完全彻底的编码错误导致的。尽管可以避免，但是查找和修复这样的缺陷要求从开发项目启动时就严格采用注重安全的设计方式，并且需要额外的时间和精力进行测试和分析。尽管这有助于解释软件安全性往往存在的可悲状态，但是决不可原谅！

1. 初始化和失败状态

在毫无准备的情况下，系统突然崩溃，接着又重新恢复，这个过程就可能存在两个会危及系统安全控制的机会。许多系统在关机过程中会卸载安全控制。可信恢复能够保证在发生系统崩溃时，所有的控制措施都完整无缺。在可信恢复的过程中，系统能确保在安全控制失效的情况下不发生任何访问活动。甚至在系统恢复阶段，所有控制方法都还在完整地运行着。

例如，假设系统崩溃时，还有一个数据库事务正在为被分类为绝密数据的数据库向磁盘写入数据。没有受到保护的系统可能会允许未经授权的用户在数据写入磁盘之前访问这些临时数据。支持可信恢复的系统能够保证不会发生破坏数据机密性的行为，即使在系统崩溃的过程中也是如此。这个过程要求通过精心的策划和详细的步骤来处理系统故障。虽然自动恢复过程构成了整个恢复过程的一部分，但是人为的干预仍然是必要的。很显然，如果需要这样的人工操作，那么对执行恢复操作的人员进行适当的身份标识和身份认证同样也是必不可少的。

2. 输入和参数检查

缓冲区溢出是一种声名狼藉的安全破坏行为。在编程人员未能充分验证输入数据时，尤其是在没有对软件接受为输入的数据量进行限制时，就会出现缓冲区溢出。因为这样的数据往往存储在某个输入缓冲区内，所以在超出缓冲区正常的最大空间时，额外的数据就被称为溢出。因此，试图将恶意入侵或代码作为程序输入部分时导致的攻击类型被称为缓冲区溢出。遗憾的是，在许多系统中，在高特权级别或与接受这种输入的进程相联系的任何特权级别遭到攻击的系统常常会直接造成数据溢出。对于几乎所有类型的操作系统(包括 Windows、Unix、Linux 与其他操作系统)来说，在任何已知的安全脆弱性种类中，缓冲区溢出提供了最易见和最深切的危害和攻击机会。

缓冲区溢出脆弱性的责任方往往是编写非净化代码的编程人员。如果编程人员能够尽职，那么可以完全消除缓冲区溢出，不过在将数据存储到任何数据结构之前，编程人员必须检查所有的输入数据和参数(并且限制作为输入提供的数据量)。验证数据的有效性是消除缓冲区溢出的唯一方法。除此之外，一旦发现缓冲区溢出，受影响的系统就必须以常见的方式应用关键的安全更新，从而避

免遭受攻击。

真实场景

检查代码是否存在缓冲区溢出

在 2002 年初，习惯以 Microsoft 公司发言人身份出现的 Bill Gates 公布了“可信计算计划”，这个计划希望通过改变一系列设计原理来从安全角度解决 Microsoft 操作系统和应用程序中长期存在的安全问题。对这个话题的讨论从 2002 年持续到 2003 年，而缓冲区溢出主题反复出现(实际上比 Microsoft 安全公告报告的与这类问题相关的安全缺陷更为频繁，在涉及安全的编程错误中，缓冲区溢出仍然是最严重和最常见的错误类型之一)。作为其他许多开发组织和软件开发环境构建器(开发人员用于创建其他软件的软件工具)经常遇到的情况，对防范缓冲区攻击的意识的提高导致开发过程中的许多阶段发生了变化：

- 设计人员必须为输入数据指定边界或规定可接受的输入值，并且在请求输入时必须限制要接受、分析和处理的数据量。
- 构造请求、接受和处理输入的代码时，开发人员必须遵循上述限制。
- 测试人员必须通过检查确保不会发生缓冲区溢出，并且在测试输入处理代码时尝试回避或绕开安全设置。

著名的信息安全专家 Bruce Schneier 在其著作 *Secrets & Lies: Digital Security in a Networked World* (Wiley, 2004)中提出了一个重要论点：安全测试实际上与标准测试活动(例如，单元测试、模块测试、验收测试和质量保证检查，请参看术语表)大相径庭；作为开发过程的一部分，标准测试是软件多年以来例行完成的活动。Microsoft 公司(以及其他开发公司)尚未明确的是：改变设计和测试原理是否就等同于采取严格措施挫败缓存区溢出(Microsoft 报告的某些较为严重的安全漏洞持续被缓存区溢出或缓存区溢位困扰，或者将这种脆弱性的起因标识为“未经检查的缓冲区”)。

3. 维护钩子和特权程序

维护钩子程序是只有系统开发人员才知道的系统入口点。这些入口点也被称为后门。虽然维护挂接程序的存在明显地违反了安全策略，但是它们仍然出现在许多系统中。后门的最初目的是：出于维护系统的原因或者在正常的访问由于疏忽导致失效时，能够提供有保证的访问。后门存在的问题是：这种访问类型避开了所有的安全控制措施，并且为所有知道后门存在的人提供了不受限制的访问。必须明确禁止这些入口点，并且通过监控审计日志来发现那些表明可能是未经授权的管理员访问行为。

另一种常见的系统脆弱性是程序在执行过程中安全级别被提高的情况。这些程序必须被认真编写和测试，从而不会允许任何出口点和/或入口点存在，以防提高主体的安全级别。确保所有运行在较高安全级别的程序都只能被适当的用户访问，并且这些用户会坚决抵制滥用。

4. 增量攻击

某些攻击形式以缓慢的、渐进的增量方式发生，而不是通过明显的或可识别的活动来危害系统的安全性或完整性。数据欺骗和 salami 攻击就是两种这样的攻击形式。

当攻击者获得访问系统的权限并且在存储、处理、输入、输出或事务处理期间对数据进行细小

的、随机的或增量的改变时(而不是明显地改变文件内容或破坏、删除整个文件)，就会发生数据欺骗。如果没有通过执行加密或某种完整性检查(例如，校验和或消息摘要)并在每次文件读写时都加以应用来保护文件和数据，那么就很难检测这些变化。加密的文件系统、文件级别的加密技术或某些文件监控形式(包括诸如 Tripwire 之类的应用程序所执行的完整性检查)通常足以保证不会发生数据欺骗。数据欺骗通常被认为是一种大多由内部人员、很少由外部人员(也就是外部入侵者)进行的攻击。很显然，因为数据欺骗是一种修改数据的攻击，所以我们将其视为主动攻击。

根据所有已公布的报告，salami 攻击更为神奇。这种攻击的名字指的是系统化地削减账户或其他财务记录中的资产，并且每次都有规律地减少少量资产值。打个比方，顾客将购买的意大利香肠送入切片机进行加工，攻击者每次都只偷取一小片香肠。在现实应用中，尽管没有这种攻击的文字记录，但是大多数安全专家都承认 salami 攻击是可能的，尤其会涉及组织的内部人员。只有通过适当的职责分离和对代码的适当控制，组织才能完全阻止或消除这种攻击。设置金融交易监控器来跟踪很小的资金或价值转移有助于检测这样的活动，向员工正式通报这种活动也有助于防止 salami 攻击企图。

注意：

如果对 salami 攻击或 salami 技术感兴趣，那么读者可以观看电影《办公空间》、《通天神偷》和《超人 3》。

9.11.3 编程

我们已经在前面提到过编程中的最大缺陷：缓存区溢出，它是由于编程人员没有检查或净化输入数据的格式和/或大小而造成的。在程序中还存在其他潜在的缺陷。任何不能妥善处理异常的程序都处于不稳定状态的危险之中。程序为了执行正常的任务而提升了自己的安全级别以后，就很有可能导致崩溃。如果攻击者在适当时成功地使程序崩溃，那么他们就能达到较高的安全级别并造成对系统机密性、完整性和可用性的损害。

无论是直接执行还是间接执行，所有的程序都必须经过完整的测试以遵从安全模型。确认你所安装的任何软件使用的都是最新版本，并且知道任何已知的安全脆弱性。因为每种安全模型和每种安全策略都是不同的，所以必须确保执行的软件不会超出准许的授权。编写安全代码是很困难的，不过确实是可能的。确保使用的所有程序在设计时都考虑了安全性问题。

9.11.4 计时、状态改变和通信中断

计算机系统执行任务时具有严格的精确度。计算机的优越性在于可重复执行任务。攻击者可以根据任务执行的可预测性来开发攻击程序。常见的算法的事件顺序是先检查可用资源，然后在被准许的情况下进行访问。检查时间(Time Of Check，TOC)是指主体检查客体状态的时间。在返回要访问的客体之前，系统可以做出几种决定。当做出可以访问客体的决定时，程序在使用时间(Time Of Use，TOU)访问客体。在 TOC 与 TOU 之间存在的时间差对于攻击者来说是充足的，攻击者能够在这段时间内用另一个符合自己需要的客体来替换原先的客体。检查时间到使用时间(Time-Of-Check-To-Time-Of-Use，TOCTTOU)攻击通常被称为竞争条件，这是由于攻击者与合法的进程进行竞争，从而希望在客体被使用之前对其进行替换。

TOCTTOU 攻击的一个经典例子是：数据文件在其身份被验证之后和读取数据之前被替换。通过将数据文件替换为攻击者选择和设计的另一个文件，攻击者就能够以多种方式控制程序的活动。当然，攻击者必须对要攻击的程序和系统有深入了解。

同样，当资源的状态或整个系统发生改变时，攻击者可以试图在两种已知的状态之间采取行动。通信中断也为攻击者提供了一段可以利用的短暂时间。在资源的状态检查出现在对资源采取行动之前的任何时候，都存在发起潜在攻击的机会窗口。这些攻击必须在安全策略和安全模型中加以解决。TOCTTOU 攻击、竞争条件漏洞利用及沟通障碍被称为状态攻击，因为它们攻击一个系统状态过渡到另一个状态之间的时差、数据流控制和数据传输。

9.11.5　技术和过程完整性

评估和理解系统架构中的漏洞是很重要的，特别是关于技术和流程的整合方面。由于多种的技术和复杂的过程在规划新的和定制的业务功能时相互交叉，新的问题和安全问题就会显现出来。随着系统的集成，注意力应该放在潜在的单点故障方面，以及面向服务架构(Service-Oriented Architecture，SOA)的紧迫弱点上。SOA 构造了新应用或目前没有的功能，而且独立且区别于软件服务。由于应用结果通常是新的；因此安全问题也是未知的、未经检验的和无保户的。所有新的部署，特别新的应用或函数，需要彻底被审查之后，它们才能被允许进入和运行于生产网络或发布到互联网上。

9.11.6　电磁辐射

因为计算机硬件是由各种电子元件构造而成的，所以许多计算机硬件设备在正常运转的过程中都会放射出电磁辐射(Emit Electromagnetic，EM)。与其他计算机或外围设备进行通信的过程也会产生可能会被拦截的电磁波。通过拦截和处理来自键盘和计算机显示器的电磁辐射，我们甚至有可能重新生成键盘输入或显示器输出的数据。我们也可以被动地(也就是没有真的窃听电缆)检测和读取在网段上经过的网络数据包。这些辐射泄漏可能会引起严重的安全问题，但是通常比较容易解决。消除电磁辐射拦截的最容易方法是，通过电缆屏蔽或放入导管来降低辐射，以及通过物理安全控制方法阻止未授权人员和设备过于靠近设备或电缆。通过降低信号强度和在敏感设备周围增加物理缓冲区，就能够大幅度地减少信号辐射被拦截的风险。

前面曾经讨论过，某些 TEMPEST 技术能够防止 EM 辐射被偷听。这些技术包括法拉第笼、干扰或噪声发生器以及控制区。法拉第笼是一种作为 EM 容器使用的特殊外壳，往往类似于铜网箱。使用法拉第笼时，任何 EM 信号都不能进出被其包围的区域。干扰或噪声发生器的思想是：存在过多干扰时，检出某个信号十分困难或毫无可能。因此，通过广播自己的干扰，我们就能够阻止不希望的 EM 拦截。这个概念的唯一问题是必须确保干扰不会影响设备的正常操作。确保这个条件的一种方法是使用控制区，也就是用于限制故意的广播干扰的法拉第笼。例如，如果希望只在办公场所的几个房间内使用无线连接，那么就可以使用信号法拉第笼将这些房间包围起来，然后在控制区外放置若干噪声发生器。这样就允许在指定的房间内使用正常的无线连接，但是在指定区域之外的任何位置都不能正常使用无线连接和进行偷听。

9.12 本章小结

安全计算系统的设计是一个复杂的任务，并且许多安全工程师把他们的整个职业生涯都专注于理解信息系统最内在的工作方式,并确保支持他们所需的核心安全功能可在目前的环境中安全运行。许多安全专家不一定需要深入理解这些原则，但他们至少应该有一个广泛的了解，并帮助在过程中增强他们组织的安全性。

这样的理解开始于硬件、软件和固件的考察，以及这些零件怎么融入安全难题中。理解普通计算机和网络组织、架构和设计的原则，包括寻址(物理的和符号的)、地址空间和存储空间之间的差异，以及机器类型(真实、虚拟、多态、多任务、多编程、多进程、处理器、多用户)。

此外，安全专业人员必须对运行状态(单态、多态)、运行模式(用户模式、监管模式、特权模式)、存储类型(主存、辅存、真实存储器、虚拟存储器、易失性存储器、非易失性存储器、随机存储器、顺序存储器)和保护机制(分层、抽象、数据隐藏、进程隔离、硬件分隔，最小特权原则、特权分离、可问责性)有坚实的理解。

无论一个安全模型是多么复杂，攻击者都能利用一些存在的缺陷。一些缺陷，如缓冲区溢出和被程序员引入的维护钩子，还有其他的缺陷，如隐蔽通道，是架构设计问题。重要的是要了解这些问题的影响并修改安全架构，以便适当弥补。

9.13 考试要点

能够解释多任务处理、多线程处理、多处理器和多程序设计之间的差异。多任务处理是在一台计算机上同时执行多个应用程序，并由操作系统管理。多线程处理允许在一个进程内执行多个并发任务。多处理器是使用多个处理器以提高计算能力。多程序设计与多任务处理类似，但是在大型机系统上使用并且需要特殊的程序设计。

理解单一状态处理器和多态处理器之间的差异。单一状态处理器能够一次只在一个安全级别运行，而多态处理器可以同时在多个安全级别运行。

描述由美国联邦政府认可的用于处理分类信息的 4 种安全模式。专用系统要求所有用户对在系统中存储的所有信息都具有适当的许可级别、访问特权和“知其所需”要求。系统高级模式则去除了“知其所需”要求。分隔模式去除了“知其所需”要求和访问特权要求。多级模式则去除了上述所有三个要求。

解释大多数现代处理器使用的两种分层操作模式。用户应用程序在有限的指令集环境中运行，这被称为用户模式。操作系统在特权模式下执行受控的操作，这种模式也被称为系统模式、内核模式和监管模式。

描述计算机使用的不同存储器类型。ROM 是非易失性的，并且终端用户无法写入数据。PROM 芯片仅允许终端用户写入一次数据。通过紫外线光照射可以擦除 EPROM 芯片中的数据，然后再重新写入数据。可以用电流擦除 EEPROM 芯片中的数据，然后再重新写入数据。RAM 芯片是易失性的，当计算机的电源被切断后，芯片中的内容会丢失。

了解有关存储器组件的安全问题。目前有三种主要的安全问题与存储器组件有关：电源切断后，数据仍有可能保留在芯片上；存储器芯片容易被盗；在多用户系统中控制对存储器的访问。

描述计算机使用的存储设备的不同特征。主存储设备与存储器相同。辅助存储设备有磁性和光

学介质两种，在 CPU 能够使用这些数据之前，先要将数据读入主存储器。随机存取存储设备可以在任何位置读取数据，然而顺序存取存储设备需要扫描物理存储的所有数据后才能到达指定的位置。

了解有关辅助存储设备的安全问题。目前有三个与辅助存储设备有关的安全问题：可移动介质能够被用于窃取数据；必须应用访问控制和加密技术来保护数据；即使在删除文件或格式化介质后，数据也仍可能保留在介质上。

理解输入和输出设备会带来的安全风险。输入/输出设备会遭到偷听和窃听(能够将数据偷带出组织，还能够创建可以进入组织系统和网络的未授权、不安全的入口点)。一定要能够识别和缓解这些脆弱性。

理解 I/O 地址、配置和设置。操作传统 PC 设备要求对 IRQ、DMA 和存储映射 I/O 有一定了解。要准备好识别和处理潜在的地址冲突和错误配置，并且能够集成传统设备与即插即用(PnP)组件。

理解使用固件的目的。固件是被存储到 ROM 芯片上的软件。在计算机层次上，固件包含了启动计算机所需的基本指令。固件还被用于在外围设备(如打印机)中提供操作指令。

能够描述进程隔离、分层法、抽象、数据隐藏和硬件分隔。进程隔离能够确保进程只能访问它们自己的数据。分层法在一个进程内创建不同的安全域并限制彼此之间的通信。抽象能够在不要求了解算法或设备内部工作原理的情况下生成“黑箱”接口。数据隐藏阻止信息被来自不同安全级别的进程读取。硬件分隔使用物理控制措施实现进程的隔离。

理解安全策略如何帮助完成系统的设计、实现、测试和部署。安全策略的作用是通知和指导某些特定系统的设计、开发、实现、测试和维护。

理解云计算。云计算是一个流行的术语，指的是一个计算的概念，即处理和存储是通过网络连接到其他地方运行而不是在本地运行。云计算通常被认为是基于互联网的计算。

理解移动设备的安全。设备安全涉及为移动设备提供可以利用的潜在安全选择或功能范围。不是所有的便携式电子设备(PED)都有好的安全特性。PED 安全功能包括整个设备的加密、远程擦除、锁定、锁屏、GPS、应用控制、存储分隔、资产跟踪、目录控制、移动设备管理、设备访问控制、移动存储和禁用未使用的功能。

理解移动设备应用安全。在移动设备上使用的应用程序和功能需要被保护。相关概念包括密钥管理、证书管理、身份认证、地理标记、加密、应用白名单和可传递的信任/认证。

理解 BYOD。自带设备(BYOD)是一项策略，允许员工携带自己的个人移动设备进行工作，然后使用这些设备来连接(或穿过)公司网络的业务资源和/或互联网。虽然 BYOD 可以提高员工士气和工作满意度，但却增加了组织的安全风险。相关问题包括数据所有权、所有权支持、补丁管理、防病毒管理、取证、隐私、登录/关闭登录、企业策略的一致性、用户接受、架构/基础设施的考虑、法律问题、可接受的使用策略以及机载摄像机/视频。

理解嵌入式系统和静态环境。嵌入式系统通常相对于较大的产品来说只是其中一个组件，通常被设计围绕着一组有限的特定功能。静态环境是应用程序、操作系统、硬件集合或为了特殊需求、能力或功能而配置的网络，然后设置为保持不变。

理解嵌入式系统和静态环境下的安全问题。静态环境、嵌入式系统和其他有限或单一用途的计算环境需要安全管理。这些技术包括网络分隔、安全层、应用防火墙、手动更新、固件版本控制、包装、控制冗余和多样性。

理解如何在计算机体系结构中应用最小特权、特权分离和可问责性。最小特权原则确保只有少量进程被授权在监管模式下运行。特权分离增加了安全操作的粒度。可问责性确保可以使用审计跟踪追溯到操作源。

能够解释什么是隐蔽通道。隐蔽通道是用于传送信息的任何方法，但是通常不用于信息通信。

理解什么是缓冲区溢出和输入检查。当编程人员在将数据写入特定内存地址之前没有检查输入数据的大小时，就可能会发生缓冲区溢出。事实上，对输入数据有效性的任何验证失败都会导致安全性受到破坏。

描述安全体系结构的常见缺陷。除了缓冲区溢出以外，编程人员在部署系统后还会留下后门和特权程序。即使设计良好的系统也可能遭到 TOCTTOU 攻击。任何状态改变都为攻击者提供了危及系统安全的潜在机会。

9.14 书面实验室

1. 什么术语用来描述允许多个同时活动的各种计算机机制？
2. 系统处理分类信息的 4 种安全模式是什么？
3. 说出用于描述存储的三对方面或功能上的名称。
4. 说出在分布式体系结构中发现的一些漏洞的名称。

9.15 复习题

1. 许多 PC 操作系统提供一个功能，这个功能使它们能够支持单处理器系统中的多个应用程序同时执行。什么术语用于描述这种能力？

   A. 多程序
   B. 多线程
   C. 多任务
   D. 多处理器

2. 什么技术为组织提供对 BYOD 设备的最佳控制？

   A. 应用白名单
   B. 移动设备管理
   C. 加密移动存储
   D. 地理标记

3. 你有三个应用程序在支持多任务处理的单核单处理器系统上运行。这些应用程序的其中一个为文字处理程序，并同时管理两个线程。其他两个应用程序只使用一个线程来运行。在任何给定时间有多少个应用线程在处理器上运行？

   A. 1
   B. 2
   C. 3
   D. 4

4. 什么类型的美国联邦政府计算机系统要求所有访问系统的个人都需要知道所有由该系统处理的信息？

   A. 专用模式

B. 系统高级模式
C. 间隔模式
D. 多级模式

5. 在标准 PC 中不常被发现而嵌入式系统中有的安全风险是什么？
A. 软件缺陷
B. 访问互联网
C. 在物理环境中的控制机制
D. 电源丢失

6. 什么类型的内存芯片允许最终用户仅能写入信息到内存中一次，然后永久地保存这些不可能擦除的信息？
A. ROM
B. PROM
C. EPROM
D. EEPROM

7. 什么类型的内存芯片，当从计算机中取出并暴露在一种特殊类型的紫外光下之后，信息仅会被擦除？
A. ROM
B. PROM
C. EPROM
D. EEPROM

8. 以下哪种类型的内存可能会保留从计算机中取出后的信息，因此也代表了安全风险？
A. 静态 RAM
B. 动态 RAM
C. 辅助存储器
D. 物理内存

9. 减少移动设备上的数据丢失风险的最有效手段是什么，例如笔记本电脑？
A. 设置强登录密码
B. 减少存储在移动设备上的敏感数据
C. 使用一根电缆线
D. 加密硬盘

10. 什么类型的电气部件作为构建动态 RAM 芯片的主要部分？
A. 电容器
B. 电阻器
C. 触发器
D. 晶体管

11. 下面存储设备中的哪一个为了在网络环境中保持数据安全性，最有可能需要加密技术？
A. 硬盘
B. 备份磁带
C. 可移动设备
D. RAM

12. 在下列哪种安全模式中，你会放心所有用户都具有通过系统处理所有信息的访问权限，但不必知道所有的信息？

A. 专用模式
B. 系统高级模式
C. 间隔模式
D. 多级模式

13. 移动电话窃听最常被忽视的方面与下列哪些情形有关？

A. 存储设备加密
B. 锁屏
C. 偷听通话
D. 无线网络

14. 什么类型的存储设备通常用于包含一台计算机的主板 BIOS？

A. PROM
B. EEPROM
C. ROM
D. EPROM

15. 什么类型的存储直接提供给 CPU，并且往往是 CPU 的一部分？

A. RAM
B. ROM
C. 寄存器
D. 虚拟内存

16. 什么类型的寻址方案是数据实际提供给 CPU 作为参数传递给指令？

A. 直接寻址
B. 立即寻址
C. 基址偏移
D. 间接寻址

17. 什么类型的寻址方案支持本地 CPU 包含实际计算的内存地址？

A. 直接寻址
B. 立即寻址
C. 基址偏移
D. 间接寻址

18. 哪些安全原则有助于阻止用户访问分配给其他用户用以运行应用程序的内存空间？

A. 特权分离
B. 分层
C. 进程隔离
D. 最小特权

19. 哪些安全原则授权只有最小数量的操作系统进程时可以在监管模式下运行？

A. 抽象
B. 分层
C. 数据隐藏

D. 最小特权

20. 哪些安全原则采用进程隔离的概念和使用物理控制来实现？

A. 硬件分隔

B. 数据隐藏

C. 分层

D. 抽象

第 10 章

物理安全需求

本章中覆盖的 CISSP 考试大纲包含：

3) 安全工程(安全的工程学和管理)

- J. 应用安全原则到场所和设施设计中
- K. 设计和应用物理安全
  - K.1 配线柜
  - K.2 服务器机房
  - K.3 介质存储设施
  - K.4 证据存储
  - K.5 受限和工作区域安全(例如，运营中心)
  - K.6 数据中心安全
  - K.7 基础设施和 HVAC 注意事项
  - K.8 水的问题(例如，漏水和水灾)
  - K.9 火灾预防、检测和抑制

7) 安全运营(例如，基本概念、调查、实践管理、灾难恢复)

- O. 应用和管理物理安全
  - O.1 周边(例如，访问控制和监控)
  - O.2 内部安全(例如，陪同要求/访问控制、钥匙和锁)

物理和环境安全的话题在多个知识域中被提及，主要是知识域 3) 安全工程(安全的工程学和管理)和知识域 7)安全运营(例如，基本概念、调查、实践管理、灾难恢复)。在 CISSP 认证考试的通用知识体(CBK)中，这两个知识域的多个小节涉及关于设施安全的主题和问题，包括基本原则、设计和实施、消防、周边安全、内部安全以及其他更多内容。

物理安全的目的是防止受到物理威胁。下面列出了最常见的一些物理威胁类型：火灾和烟尘，水灾(水位上涨/下降)、地壳运动(地震、山崩、火山爆发)、暴风雨(大风、闪电、雨、雪、冰雹等)、怠工/故意破坏、爆炸/毁坏、建筑物倒塌、有毒物质、设施损失(电力、供热、冷却、空气、水)、设备故障、盗窃和人员损失(罢工、疾病、访问、运输)。

本章将研究上述每一种问题，并且讨论针对这些问题的安全措施和对策。在许多情况中，如果严重的物理威胁(例如，爆炸、阴谋破坏或自然灾难)成为现实，那么就需要灾难恢复计划或业务连续性计划。要了解更多的信息，请读者参看第 3 章“业务连续性计划”和第 18 章“灾难恢复计划”。

10.1 应用安全原则到选址和设施设计

当缺乏对物理环境的控制时，即使管理、技术或逻辑访问控制得很好，也不能提供足够的安全性。如果怀有恶意的人获得了对设备的物理访问，那么他们可以做任何想做的事，包括从泄漏、更改到破坏的所有事情。物理控制是你的第一道防线，而人员则是你最后考虑的因素。

实现和维护物理安全性有很多方面的内容和要素，其中一项核心或基本要素是选择或设计将要容纳 IT 基础设施并在其中完成组织的经营活动的设施。选择和设计安全设施的过程必须预先订立计划。

10.1.1 安全设施计划

安全设施计划描述了组织的安全要求的轮廓，并且着重强调为了提供安全性所用的方法和机制。这样的计划通过被称为关键路径分析的过程进行开发。关键路径分析是一种系统工作，可以确定关键任务应用、过程和操作以及所有必要的支持要素之间的关系。例如，一台在互联网上销售商品的电子商务服务器依赖于互联网访问、计算机硬件、电气技术、温度控制和存储设施等。

当正确执行关键路径分析时，支撑组织的必要的相互依赖和相互作用就会形成。一旦分析完成，那么结果将作为一列安全条目提供服务。设计安全 IT 基础设施的首要步骤是为组织及其计算机的基本要求提供安全性。这些基本要求包括电气技术、环境控制(如建筑、空调、保温、湿度控制等)和供水/污水处理。

在检查关键路径时，已完成的评估或潜在的技术融合是很重要的。技术融合是不同的技术、解决方案、工具和系统在随着时间的推移进行发展和合并的趋势。这往往导致多个系统执行相同或冗余的任务，或导致一个系统接管另一个系统的特性和功能。虽然在某些情况下，这可能导致更高的效率和成本节约，但它也可以表示为单个故障点并使它成为黑客和入侵者眼中更有价值的目标。例如，如果语音、视频、传真和数据流量都共享一条单一的连接路径，而不是各自不同的路径，那么所有破坏主连接的单一行为只需要入侵者或窃贼切断外部通信即可。

安保人员应参与场所和设施的设计考虑。否则，对于现存的逻辑安全，在许多物理安全方面的内容可能会被忽略。随着安保人员参与到物理设施设计中，可以确信作为组织的长期安全目标将不仅受到策略、人员和电子设备的支撑，而且也受到建筑本身的安全支撑。

10.1.2 场所选择

场所的选择应该以组织的安全需要为基础。成本、地点和大小都很重要，但是解决安全要求始终应当放在首位。当选择一处场所建立设施或选择预先就有的建筑时，应该确认已经对这个地点的每个方面都进行了仔细检查。

对资产的保护很大程度上取决于场所的安全性，这涉及大量的考虑因素。在整个场所选择过程

中，场所的位置和构造起到了至关重要的作用。容易遭受暴乱、打劫、非法闯入和野蛮破坏的场所或高发案区域内的场所显然都是不合适的，但是我们往往无法对这个问题进行规定或控制。因为无法避免诸如地质断裂带、龙卷风/飓风区和邻近自然灾难区域之类的环境威胁，所以环境威胁也是场所选择中非常棘手的问题。

毗邻其他建筑物和业务是另一个至关重要的考虑因素。这些因素具有怎样的吸引力，并且会对运作或设施造成怎样的影响？如果一家附近的企业吸引了太多的顾客，产生大量的噪音，导致振动或需要处理危险的材料，它们可能会伤害你的员工或建筑物。和其他元素一样，临近的应急响应人员是另一个考虑因素。某些公司有能力购买或修建自己的园区，这样就不必考虑路程远近的问题，从而能够进行严格的访问控制和监控。不过，并非所有公司都具有这样的财力，因此必须采用可用的和能够担负得起的方法。

至少要确保建筑物的设计要求能够应对极端的天气，并且能够阻拦或防御明显的非法闯入企图。容易受到攻击的进入位置(例如，窗户和门)往往就是此类分析。此外，还应当评估非法闯入容易借助的遮挡视线的物体(例如，树木、灌木或人为因素)。

10.1.3　可视性

可视性是十分重要的。周围地形什么样？在不引人注意的情况下骑车或步行接近设施容易吗？周围区域的组成也很重要，是在居民区、商业区或工业区吗？或是在其附近？当地的犯罪率有多高？最近的紧急事件服务机构(如消防队、医院和警察局)在哪里？这个区域都有什么独特的潜在危险(如化学工厂、无家可归者庇护所、大学、建筑工地等)？

10.1.4　自然灾害

另一个需要关注的方面是这个地区的自然灾害影响。这个地区是否容易发生地震、泥石流、灰岩坑、火灾、洪水、飓风、龙卷风、陨石、降雪、降雨、结冰、潮湿、炎热和极度寒冷等灾害？必须准备应付自然灾害，并且使 IT 环境经受得住灾害事件的影响，或者可以容易地进行替换。前面提到，业务连续性与灾难恢复计划的主题会在第 3 章和第 18 章进行阐述。

10.1.5　设施的设计

在进行设施的设计时，需要理解组织所需的安全等级。在设计开始之前，必须计划并设计恰当的安全等级。

需要考虑的一些重要问题包括易燃性、防火等级、建筑材料、负载定额、布局和诸如墙壁、门、天花板、地板材料、HVAC、电力、供水、污水处理和煤气供给之类的因素。暴力入侵、应急通道、入口阻挡、进出口、警报的使用和传导率同样也是需要评估的其他重要因素。设施中的每个元素都应该根据对保护 IT 基础设施和人员的利弊进行评估(例如，水和空气从设施内部向外部的正向流动)。

还有一个行之有效的学派思想——“安全架构”，经常被称为环境设计预防犯罪(Crime Prevention Through Environmental Design，CPTED)。指导思想是通过结构化的物理环境和周围环境，在潜在的罪犯做出任何犯罪行为之前影响其个人决定。国际 CPTED 协会是关于这个主题信息的极佳来源(www.cpted.net)，此外，也可参阅奥斯卡纽曼的书《创造的防御空间》，由 HUD 的政策发展和研究

办公室进行发行(可以在 www.defensiblespace.com/book.htm 网址获得免费的 PDF 下载)。

10.2 设计和实施物理安全

用于对物理安全进行管理的安全控制可以分为三组：行政性的、技术性的和物理性的。由于它们都用于描述访问控制的相同类别，因此记住这些分组的物理安全特性是十分重要的。行政性的物理安全控制包括设施构造和选择、场地管理、人员控制、意识培训和紧急事件响应及规程。技术性的物理安全控制包括访问控制、入侵检测、警报、闭路电视(CCTV)、监控、保温、通风、空调(HVAC)、电源以及火灾检查和排除。物理性的物理安全控制包括围墙、照明、锁、建筑材料、陷阱、狗和警卫。

真实场景

公司财产与个人财产

在许多普通业务环境中，物理安全控制既有可视的一面，也有不可视的一面。我们可以在邮局、街边小店和自己计算环境的特定区域看到物理安全控制。物理安全控制无处不在，某些人甚至基于存在的物理安全控制(例如，公共进出的大门或安全的房屋构成)来选择自己的住所。

Alison 是某大型技术公司专门从事数据管理的安全分析人员，这个公司拥有能够处理物理安全违规问题的安全员工(保安、管理员等)。

Brad 的私人车辆最近在公司的停车场经历过一次入侵。他询问 Alison 是否发现或记录到破门进入其车辆的人员，但是因为车辆属于个人物品而非公司财产，所以 Alison 没有应对员工资产受损的相应控制措施或规章制度。

我们很容易想到 Brad 非常泄气，但是他理解 Alison 保护的是公司的业务，而不是保护个人物品。那么，在什么时间和场合有必要实现针对公司财产和个人财产的安全措施？通常，在涉及或可能涉及商业资产的任何场合都可以采用这样的安全措施。Brad 将公司的车辆停在公司的停车场，那么 Alison 可能会附带考虑非法侵入所涉及的 Brad 的私人物品，但是即便如此，她也仍然不负责保护这些物品的安全。另一方面，在关键人员(大多数企业的主管人员、敏感岗位的安全分析人员、地区领导等)也是受保护的重要资产时，安全保卫的范围往往会被扩展，进而将保护这些人员的个人物品也作为资产保护和风险缓解的一部分内容。当然，如果针对员工及其携带物品的危险成为一个问题时，那么使用钥匙卡保护停车场的安全以及在每一层都安装监控设备就非常有意义。简单来说：如果发生侵入的成本超过了安装防护设备的成本，那么最好立刻安装防护设备。

为具体环境设计物理安全性时，需要牢记控制措施的功能顺序：

(1) 阻拦
(2) 拒绝
(3) 检测
(4) 延缓

被部署的安全控制措施应当打消对物理资产进行访问的起初念头(也就是边界限制)。如果失败，那么就应当拒绝对物理资产的直接访问(例如，关闭保险库大门)。如果拒绝失败，那么系统就需要

检测入侵(例如，使用运动探测器)，并且应当充分地延缓入侵，以便职权机构能够进行响应(例如，对资产的线路加以锁定)。因此，记住下面的部署先后顺序是十分重要的：首先阻拦，然后拒绝，然后检测，然后延缓。

10.2.1　设备故障

无论组织选择购买和安装的设备的质量如何，设备最终都会出现故障。了解这一事实并做好准备，这将确保 IT 基础设施的持续可用，并且有助于保护好资源的完整性和可用性。

为做好设备出现故障的准备，可以采取许多种形式。在一些任务不是很紧急的情况下，只要知道在哪里能购买到替换部件就可以了，48 小时的替换时间期限是比较充分的。在其他情况下，维持现场有替换部件是强制性的要求。需要记住的是，系统返回到完整的正常功能状态的响应时间与这种解决方案所涉及的维护成本成正比。成本包括存储、运输、预先购买以及维护现场安装和恢复专业技术。在某些情况中，维护现场替换是不可行的。对于这种情况，与硬件供应商签订服务级别协议(SLA)是十分必要的。SLA 清楚地定义了供应商在发生设备故障的紧急情况下所提供的响应时间。

对老化的硬件进行替换和/或修理应该制定时间表。这些操作的时间表应该以为每种设备估计的平均无故障时间(Mean Time To Failure，MTTF)和平均修复时间(Mean Time To Repair，MTTR)为基础。MTTF 是指设备在特定的操作环境中预计正常工作的寿命。MTTR 是设备修理需要的平均时间。某一设备可以在灾难性故障发生之前经历多次修复过程。一定要保证在所有设备的 MTTF 到期之前进行替换的时间安排。另一个额外的测量参数是平均故障间隔时间(Mean Time Between Failure，MTBF)。这是关于第一个故障发生后与随后任何故障之间时间差的估计。如果 MTTF 和 MTBF 的值相同或非常相似，厂家往往只列出 MTTF 来代表这两个值。

设备送外修复时，需要在修复期间使用替代的解决方案或备份设备。通常，在出现小故障时进行修理是可以接受的，但是等到出现大故障时再进行更换，就是一种无法接受的安全实践。

10.2.2　配线间

配线间使用一个小柜子，里面的通信电缆通过使用布线架来归置。今天，配线间仍用于归置目的，而且也是重要的基础设施。现代的配线间是整个建筑或一个楼层中连接到其他重要设备的网络电缆所在的地方，如配线架、交换机、路由器、局域网扩展和骨干渠道。配线间一个更专业的技术名称是房屋线缆分布室。有一个或多个机架互联设备安放在一个配线间是非常常见的(见图 10.1)。

为了保证最大线缆传输限制，大型建筑物里需要多个配线间。对于常用的铜制双绞线布线，最大传输长度为 100 米。然而，在嘈杂的电磁环境中，这种运行长度会显著减少。配线间也可作为一个便利的位置把多个楼层连接在一起。在这样的多层配置中，配线间通常直接位于各自楼层的上方或下方。

配线间通常也用于存放和管理建筑物中其他重要设备的线缆，包括报警系统、断路器面板、电话冲压块、无线接入点和包括安全摄像头的视频系统。

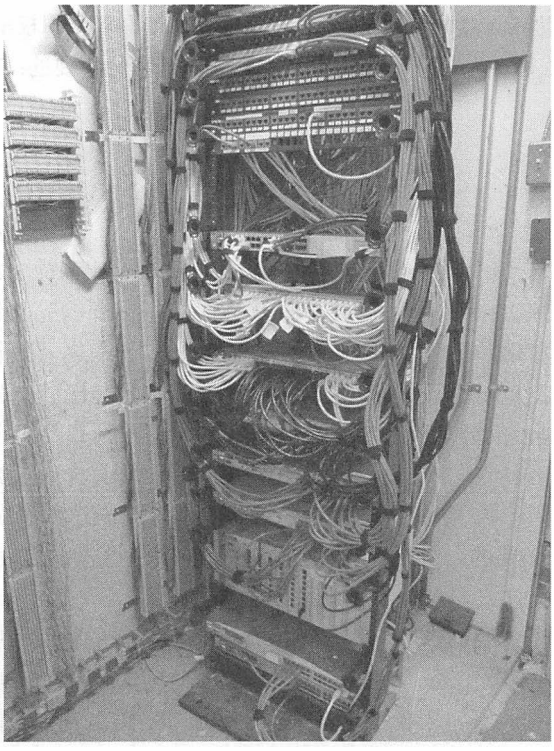


图 10.1　典型的配线间

(源自 https://www.flickr.com/photos/clonedmilkmen/4390901323/)

配线间的安全是非常重要的。大部分的安全重点是在防止未授权的物理访问方面。如果一个未授权的入侵者获准访问该地区，他们可能偷取设备、拖拉或切断电缆，甚至安放窃听设备。因此，配线间的安全策略应包括如下可靠规则：

- 从不把配线间作为通用的存储区。
- 有足够多的锁。
- 保持区域的整洁。
- 不要存放易燃易爆物品。
- 设置视频来监控内部的配线间活动。
- 使用开门传感器来记录日志。
- 不要把钥匙给除了授权管理人员之外的任何人。
- 对配线间的安全和内容进行定期的物理检查。
- 把配线间纳入组织的环境管理和监控，以确保有适当的环境控制和监控，以及检测破坏性条件，如洪水或火灾。

告知建筑管理员关于配线间的安全策略和访问限制是同样重要的，这将进一步减少未授权的访问尝试。

10.2.3　服务器机房

服务器机房、数据中心、通信机房、配线间、服务器保管室和 IT 机房是被封闭的、受限的和受

保护的房间，这里放置着关键的服务器和网络设备。集中化的服务器机房不需要与人相协调。事实上，服务器机房的人为协调因素越少，对偶然的和已确定的进攻所进行的防护就越多。与人不协调的因素可能包括哈龙、PyroGen 或其他替代哈龙的氧气排放量火灾检测和灭火系统、低温、微弱或无照明和堆放的设备，因此几乎没有行走或移动空间。服务器机房应该设计成对 IT 基础设施提供最佳支持和操作，并且可以防止未经授权的人进入和妨碍系统运行。

服务器机房应设在建筑物的核心位置。尽量避免放置在底层、顶层和地下室。此外，服务器机房应远离水、气和污水管道，这些管道泄漏或泛滥的风险太大，可能会造成严重的损坏和故障停机时间。

提示：

服务器机房的墙壁还应当至少达到 1 小时防火时间的防火等级。

真实场景

使服务器不可接触

在 IT 安全领域流传的一个笑话是：计算机的最佳保护方法之一是断开它与网络的连接并密闭在没有门窗的房间内。当然，这只是玩笑，情况还没有那么严重。但是，这个笑话包含很多道理，并且具有一定的讽刺意味。

Carlos 为某家金融银行管理安全进程和平台，并且了解单向系统和不可到达设备的所有相关信息。在不到一秒钟的时间内发生的众多敏感业务交易中，其中一次错误的交易会给数据或交易参与方带来极大的风险。

凭借自己的工作经验，Carlos 知道最难以访问的和最不友好的地方保管着最有价值的资产，因此他将许多计算机都放在独立的银行保险库内。只有天才级的小偷、技巧高超的攻击者、保险箱窃贼和富有决心的计算机攻击者才有可能突破 Carlos 的安全防御。

并非所有商业应用和过程都保证这种极端的保护类型。除了保险库之外，还可以建议通过怎样的安全措施使服务器更难以访问？在不能腾空使用保险库时，选择访问受限的地下室或者没有窗户以及只有一个进出口的内室都是不错的替代方案。关键在于：首先选择访问受限的房间，然后在入口(尤其是未授权的入口)设立防范严密的障碍。门口的 CCTV 监控和房间内的运动探测仪也有助于保持对人员进出的敏感性。

10.2.4　介质存储设施

介质存储设施应该被设计用于安全地保存空白介质、可重用介质和安装介质。无论是硬盘、闪存、光盘或磁带，介质都应被控制用来防止偷窃和破坏。新的空白介质应该保持安全，以防止偷窃或恶意软件植入。

可重用介质，如 U 盘、闪存卡或移动硬盘，应该被保护以防止被盗和残留数据恢复。残留数据是指通过标准的删除或格式化过程之后残留在存储设备上的剩余数据元素。使用这样的过程虽然清除了目录结构和簇的标记，但在簇中留下了原始数据。简单的反删除工具或数据恢复扫描器通常就能恢复和访问这些文件。限制对介质的访问和使用安全的擦除方案能够减少这种风险。

安装介质需要防止偷窃和恶意软件植入。这将确保在需要进行新的安装时，介质是可用的和安

全的。

这里有一些实现安全介质存储设施的方法：

- 把介质存放在上锁的柜子或保险箱中。
- 有库管理员或保管员来管理对带锁的介质柜的访问。
- 使用存入/取出流程来跟踪谁在检索、使用和返回存储介质。
- 对于重用介质，当被返还时，运行安全磁盘擦除或归零(通过无意义的数据(比如零)来取代擦除数据的过程)过程来删除所有残留数据。

对于更注重安全的组织，在介质上放置安全说明标签以指明分类用途或者在资产上使用 RFID/NFC 资产跟踪标签，是非常有必要的。使用像保险箱一样的存储柜比使用办公架子也更重要。更高的保护级别还可以包括对火灾、洪水、电磁场和温度的监测和保护。

10.2.5 证据存储

证据存储正在迅速成为所有企业的必备品，而不仅仅限于相关执法机构。随着网络犯罪事件的不断增加，保留日志、审计跟踪和其他数字事件的记录是十分重要的。为了将来比较的需要，保留驱动器的图像镜像或虚拟机快照也是必要的。这也涉及企业内部调查或以执法为基础的电子取证分析。在这两种情况下，保留可能被用作证据的数据集，对于企业内部调查或网络犯罪执法部门调查是最有利的结论。

安全证据存储可能涉及以下：

- 一个专用的存储系统以区别于生产网络
- 当没有新的数据集传输到存储系统时就将存储系统离线
- 阻断存储系统和互联网的连接
- 跟踪证据存储系统的所有活动
- 计算存储在系统中所有数据的哈希值
- 限制安全管理员和法律顾问的访问
- 对所有存储在系统上的数据进行加密

在当地的法规、行业或合同义务中，可能对证据存储解决方案有额外的安全要求。

10.2.6 受限的和工作区域安全(例如，运营中心)

工作区和参观区域的设计和配置都应该仔细考虑。对设施内所有地方的进入要求不应该等同对待。进入含有更高价值或重要资产的区域应该受到限制。例如，任何进入此设施的人应该能够进入休息室和使用公共电话，但是只有网络管理员和安全人员才能够进入服务器机房。有价值的和保密的资产应该放置在设施的核心保护区或中心地区。实际上，应该专注于部署物理保护的同心圆。这种配置类型要求较高的授权级别才能进入组织的更敏感区域。

墙壁或隔离物可以被用于隔开类似但却不同的工作区域。这样的分隔阻止了偶然的偷窥和偷听。肩窥是指通过留意显示器或操作者敲击键盘来收集系统中的信息。从地板到天花板之间的全封闭墙壁应该被用于分隔不同敏感度和机密性的区域(当使用虚假或隔离的天花板时，墙壁应该对此进行切断并在多个或少数的区域之间，提供不可打破的物理屏障)。

每个工作区都应当进行评估，并且像 IT 资产分类一样分门别类。只有具有与工作区分类相应的

许可或分类的人才应当被准许进入相应区域。不同用途或应用的区域应当分配不同的访问或限制级别。区域内提供的对资产的使用越多，对谁可以进入区域以及可以执行的活动的限制就越大。

设施安全设计过程应该支持内部安全的实施和维护。除了在适当的工作场所管理员工外，还应该解决访客和访客控制问题。是不是有访客陪同的要求，应该实施哪种访客控制？除了基本的物理安全工具，如钥匙和锁，其他机制，如陷阱门、摄像机、写日志、保安人员和 RFIDID 标签，也应进行部署。

10.2.7　数据中心安全

对于许多组织而言，他们的数据中心和服务器机房有且只有一个。之前的章节“服务器机房”，包含了对服务器机房和数据中心同样适用的主题讨论，无论怎么样都可以认为这些标签是同义词。

对于一些组织，数据中心是外部场所，用来容纳他们大部分的后端服务器、数据存储设备和网络管理设备。这可能是在主要办事场所附近的一个独立建筑物，也可能是一个远处场所。数据中心可能属于组织并由组织专门管理，也可以从某个数据中心提供商租用服务。数据中心可以是单租户配置或多租户配置。无论怎么变化，除了单个服务器机房所关注的以外，许多其他的概念也是相关的。

在许多数据中心和服务器机房中，各种技术控制经常被作为管理物理访问的访问控制机制。这些控制包括智能卡/信用卡以及接近式读卡器和入侵检测系统(IDS)。

1. 智能卡

智能卡是信用卡大小的身份证、员工证或安全通行证，卡上具有磁条、条形码或植入的集成电路芯片。智能卡包含了经过授权的可以被用于身份识别和/或身份认证目的的持卡人信息。某些智能卡甚至具有处理信息的能力或被用于在内存芯片上存储一定数量的数据。下列短语或术语指的都是智能卡：

- 包含集成电路(IC)的身份令牌
- 处理器 IC 卡
- 具有 ISO 7816 接口的 IC 卡

智能卡常常被视为一种完整的安全解决方案，但却并不被认为是完全的解决方案。与任何安全机制一样，这种解决方案具有自己的缺陷和脆弱性。智能卡容易遭受物理攻击、逻辑攻击、特洛伊木马攻击以及社会工程学攻击。大多数情况下，智能卡被用于多因子配置，因此，智能卡被盗或丢失不容易发生冒名替代的后果。最常见的用于智能卡的多因子认证要求使用 PIN。可在第 13 章“管理身份与认证”中发现更多的信息。

记忆卡是具有磁条的、计算机可读的 ID 卡。与信用卡、借记卡或 ATM 卡一样，记忆卡能够保存少量的数据，但是无法像智能卡一样处理数据。记忆卡通常作为一种双因子控制措施，也就是说，往往要求用户物理拥有卡片(第 2 类因素)以及知道卡片的 PIN 号码(第 1 类因素)。记忆卡易于拷贝或复制，因此在安全环境中被视为无法充分地实现身份认证目的。

2. 接近式读卡机

除了智能卡和无记忆卡以外，接近式读卡机也可以被用于控制物理访问。接近式读卡机可以是无源设备、场源设备或发送应答器。接近式设备由经过授权的持卡人携带或持有，当持卡人通过接

近式读卡机时，接近式读卡机能够确定持卡人的身份及其是否已被授权进行访问。无源设备反映了或以其他方式改变了由读卡机产生的电磁场。读卡机能检测到这种改变。

无源设备不具有活动电子，只是具有特定属性的小磁场(如 DVD 上常见的防盗设备)。场源设备是一种电子设备，当进入由读卡机产生的电磁场时会被激活。这种设备实际上生成从 EM 场到电源本身的电流(如要求卡片距离数英寸时才能开门的读卡机)。发送应答器是自有电源的设备，并且发射由读卡机接收的信号。这种设备可以连续工作，也可以只在按下按钮时工作(如公路收费站或车库开门系统)。

除了智能卡、无记忆卡和接近式读卡机以外，还可以使用无线射频识别(RFID)或生物测定学方面的访问控制设备来管理物理访问。要了解对生物测定设备的描述，请参看第 13 章。这些和其他的设备，例如线缆锁，都能支持设备的保护和安全。

3. 入侵检测系统

入侵检测系统是自动化的或人工的系统，这种系统被设计用于检测未经授权的个人企图发起的入侵、破坏或攻击行为，未授权入口点的使用情况，以及在未经授权的时间或非正常时间发生的犯法事件。用来监控物理行为的入侵检测系统包括保安人员、自动化访问控制、运动探测仪以及其他特殊的监控技术(这些内容在之前的章节“移动检测”和后面的章节“入侵报警”中有更详细阐述)。

物理的入侵检测系统也被称为防盗警报器，用于检测未经授权的活动并通知管理机构(内部的安全部门或外部的执法部门)。最常见的入侵检测系统类型是在入口点使用包含箔片的简单电路(也就是干触点开关)，以便在门或窗被打开时开始检测工作。

入侵检测机制只有在连接入侵警报器时才有用(可参看本章后面的“入侵报警”)。入侵警报器会通知管理机构相关的物理安全违规行为。

任何入侵检测和警报系统都具有导致失效的两个方面：如何获得电源以及如何进行通信。如果系统断电，那么就不可能工作。因此，可靠的入侵和警报系统都具有存储能量足以支持 24 小时操作的备用电池。

如果通信线路被截断，那么警报系统就不起作用，并且无法通知安全人员以及应急服务机构。因此，可靠的入侵和警报系统都具有监控线路的心跳传感器。心跳传感器机制既可以不断地，也可以定时地检查测试信号。一旦接收站无法检测到心跳信号，那么就会自动触发警报。上述两种措施被设计用于防止入侵者对检测和警报系统的规避。

4. 访问滥用

无论使用哪一种形式的物理访问控制，为了阻止滥用、伪装和尾随，还必须部署保安人员或其他监控系统。物理访问控制的滥用示例包括敞开安全门、绕过锁或访问控制。伪装是指使用其他人的安全 ID 获得进入某座设施的权限。尾随是指跟随着某个人通过受到安全保护的门或通道，而自己并没有接受身份识别或身份认证。这样的检测滥用可以通过建立审计跟踪和保持访问日志来完成。

即使针对物理访问控制，审计跟踪和访问日志也仍然是非常有用的工具。它们可能需要保安人员手工建立，也可能是在有足够的自动化访问控制机制(例如，智能卡和某些接近式读卡机)的情况下自动生成。主体在请求进入时，身份认证过程的结果和安全门被保持打开状态的时间是审计跟踪和访问日志中包含的重要因素。除了电子方式或纸质文档跟踪之外，还应当考虑使用 CCTV(闭路电视)进行入口点的监控。CCTV 支持将审计跟踪和访问日志与可视化的事件历史记录进行比较。对于重新构建入侵、破坏或攻击事件来说，这些信息非常关键。

5. 放射防护

许多电子设备都会放射能够被未授权人员截获的电子信号或射线。这些信号可能包含机密的、敏感的或私有的数据。放射设备的最常见示例是无线互联设备和移动电话，但是其他许多设备的放射信号也易于被截获。这些设备可能包括显示器、调制解调器以及内部和外部介质驱动器(如硬盘驱动器、USB 存储驱动器和 CD 等)。如果使用合适的设备，未授权用户就能够截获电磁或射频信号(合称为放射信号)并抽取出机密数据。

很明显，如果组织之外的人员能够截获设备向外发送的信号，那么就需要采取安全预防措施。用于阻止放射攻击的对策和防护类型被称为瞬时电磁脉冲设备屏蔽技术(TEMPEST)设备。TEMPEST 最初是一个政府研究项目，目的是防止电子设备受到核爆炸产生的电磁脉冲(EMP)所带来的破坏。随后这个项目被扩展为监控放射信号和防止放射截获的常规研究。因此，TEMPEST 是一个涉及大量活动的正式名称，而不仅仅是针对特定用途的缩写词。

TEMPEST 的一些对策有法拉第笼、白噪声和控制区。

法拉第笼　可以是箱子、移动房屋，也可以是被设计为具有金属外壳的整个建筑物，通常是完全包围区域所有面(也就是前、后、左、右、上、下)的金属网。这个金属外壳具有能够产生电容效应(因此以法拉第命名)的弱电，从而可以防止所有电磁信号(放射信号)逸出或进入由法拉第笼围绕的区域。法拉第笼能够非常有效地阻拦 EM 信号。事实上，在有效的法拉第笼的内部，移动电话无法使用，并且无法接收广播或电视信号。

白噪声　白噪声指的是一直广播虚假通信数据，从而掩盖和隐藏实际存在的放射信号。白噪声可以由另一个非机密来源的实际信号、特定频率的连续信号、随机的可变信号(例如，在广播电台或电视台之间听到的白噪声)甚至导致截获设备失效的干扰信号组成。在区域边界的周围生成白噪声是最为有效的，此时白噪声通过向外广播以保护需要放射信号才能完成正常运作的区域内部。

注意：

白噪声描述了能够淹没有意义信息的任何随机的声音、信号或过程。白噪声覆盖的范围从可听见的频率到不可听见的电子传输，并且可能涉及通过创建线路或通信噪声以掩饰来源或干扰侦听设备的故意而为的行为。

控制区　控制区是第三种 TEMPEST 对策，它只是在受保护区域环境内实现法拉第笼或白噪声，在受保护区域环境外则不采取任何措施。控制区可以是一间房屋、一层楼或整座建筑。控制区是所需设备使用和支持放射信号的区域(例如，无线互联、移动电话、无线电和电视信号)。在控制区外部，我们需要使用不同的 TEMPEST 对策来阻止对放射信号的拦截。

10.2.8　基础设施和 HVAC 注意事项

电力公司供应的电源并不总是连续的和平稳的。大多数电子设备需要平稳的电力供应才能正常工作。由于电源的波动而导致设备损坏的事情经常发生。许多组织通过几种方法来选择管理他们自己的电源。不间断电源供应(Uninterruptible Power Supply，UPS)是一种自充电的电池类型，可以为敏感的设备提供连续和平稳的电力。UPS 基本的工作方式是：从壁装电源插座上取得电力并存储在电池中，将电力从电池中输出，然后把这些电力提供给与之相连的任何设备，通过电池中的直流电，UPS 能够维持连续和平稳的电力供应。UPS 还有第二种功能，这种功能通常作为产品的卖点。UPS

在主要电源出现故障或无法获得的情况下能够提供持续的电力供应。UPS 可以提供数十分钟或数小时的电力，持续时间依赖于它的容量和设备所需的用电量。在某些情况下，备份电池可以用来提供紧急的电力供应。然而，这样的基础设备不可能被视为 UPS。

另一种确保设备不会因为电源波动而造成损坏的方法是使用带有电涌保护器的配电盘。电涌保护器包含一根保险丝，它在电源功率剧烈变化而造成对设备的损坏之前熔断。但是一旦电涌保护器的保险丝熔断或电路因跳闸切断，电流就会被完全中断。只有当突发的电力中断不会造成设备损坏或引起损失的情况下，我们才使用电涌保护器。否则，使用 UPS 应该是最好的选择。

如果希望维持很长时间的电力并且不会造成停电，那么需要一台现场发电机。这种发电机在电力无法供应的情况下被自动切换过来。大多数发电机运转时都使用液态或气态的燃料水槽，为了保证可靠性，必须维持充足的燃料。发电机被认为是电源的替换或后备方案。

与电源相关的问题有很多。下面是应当熟悉的一组电源术语：

故障(fault) 电力瞬间消失

中断(blackout) 电力完全消失

电压不足(sag) 瞬间电压降低

降压(brownout) 长时间低电压

脉冲(spike) 瞬间高电压

电涌(surge) 长时间高电压

起动功率(inrush) 电源开始的电涌通常与连接的电源有关，无论电源是主电源还是替换/辅助电源

噪声(noise) 持续不断的电源干扰

瞬时现象(transient) 短时间的线路杂音干扰

平稳(clean) 完全平稳的电流

接地(ground) 电路中的电线是接地的

降压是一个有趣的电力问题，这是因为它的定义参考了美国国家标准协会(ANSI)的电力相关标准。在长时间的低压情况被标记为降压之前，ANSI 允许电压在电源和设施仪表之间可以降低 8 个百分点，在设施仪表和壁装电源插座之间可以降低 3.5 个百分点。ANSI 标准进一步明确区分了这样的问题：仪表之外的低电压由电力公司修复，而仪表内部的降压则是自身的责任。

1. 噪声

噪声造成的问题不仅会影响设备的功能，还可能会干扰通信、传输和播放的质量。由电流产生的噪声会影响任何一种依赖于电磁传播机制的数据传输，例如电话、蜂窝电话、电视、音频、无线电和网络机制。

电磁干扰(EMI)有两种类型：普通模式和导线模式。普通模式的噪声是由电源或运转的电子设备的火线和地线之间的电势差产生的。导线模式的噪声是由电源或运转的电子设备的火线和中线之间的电势差产生的。

与此类似的问题是射频干扰(RFI)，它与 EMI 一样，会影响许多系统。RFI 由很多常见的电器产生，这些电器包括荧光灯、电缆、电子加热器、计算机、电梯、电动机和电磁铁。因此，在部署 IT 系统和设施组件时考虑这类设备的位置是十分重要的。

保护电力供应和保护设备不受到噪声干扰，这是为 IT 基础设施维护高效和功能稳定的环境的重要部分。这种保护措施所采取的步骤包括：提供充足的电力条件，建立合适的接地措施，屏蔽所有

电缆，以及限制暴露在 EMI 和 RFI 源中。

2. 温度、湿度和静电

除了考虑电源问题，维护环境还包括控制采暖、通风和空调(HVAC)的机制。主要放置计算机的房间应该保持温度在华氏 60 到 75 度之间(摄氏 15 到 23 度)。然而，有一些极端环境，运行的设备低至华氏 50 度，而其他的则运行在华氏 90 度以上。计算机房间的湿度应当维持在 40%和 60%之间。湿度太高会导致侵蚀，湿度太低则会产生静电。即使在不产生静电的地毯上，如果环境中的湿度太低，那么仍然可能产生两万伏特的静电放电。如表 10.1 所示，即使很少的静电放电也可能毁坏电子设备。

表 10.1　静电电压及可能造成的损坏

静电电压(伏特)	可能造成的损坏
40	造成敏感电路和其他电子元件的损坏
1000	造成显示器显示时的不规则闪动
1500	造成硬盘上所存储数据的损坏
2000	突然性系统关闭
4000	打印机故障或元件损坏
17 000	永久性电路损坏

10.2.9　水的问题(例如，漏水和水灾)

环境安全策略和措施中应当解决水的问题，例如漏水和水灾。管道泄漏不会每天都发生，但是在真的发生时，经常会造成重大的损失。

水和电是不能接触的。如果计算机系统与水相接触了(特别是在系统运行时)，那么就会发生损坏事故。水电接触会造成人员触电身亡的严重风险。只要有可能，就要将放置服务器的房间和重要计算机设备远离任何水源或传输管道。还可能希望在关键任务系统的地板周围安装水检测电路。水检测电路具有警报装置，如果水正在侵入设备，那么就会发出警报。

为了将紧急事件减到最少，一定要熟悉关闭阀门和排水装置的位置。除了监控管道漏水之外，还应该对所在区域处理暴雨或水灾的设施的能力进行评估。这些设施是位于小山上还是山谷中？是否有足够的排水装置？是否有发生水灾或积水成患的历史？放置服务器的房间是位于地下室还是在一层？

10.2.10　火灾的预防、检测和抑制

火灾的预防、检测和抑制绝不能被忽略。保护人员不受到伤害应当始终是所有安全或防护系统最重要的目标。除了保护人员安全以外，设计防火检测和灭火措施的目的是将由火、烟、热和灭火材料引起的损失最小化，特别是与 IT 基础设施相关的部分。

基本的防火教育涉及对起火三角形(如图 10.2 所示)的了解。图中三角形的三个角分别表示燃料、高温和氧气，三角形内部表示上述三种元素的化学反应。起火三角形的目的在于说明：如果去除起火三角形 4 个元素中的任何一个，就能够灭火。如下所示，不同的抑制介质针对火的不同方面：

- 水能够抑制高温
- 苏打酸和其他干粉能够抑制燃料供应
- 二氧化碳能够抑制氧气供应
- 哈龙替代物与其他非易燃气体能够干扰化学燃烧和/或抑制氧气供应

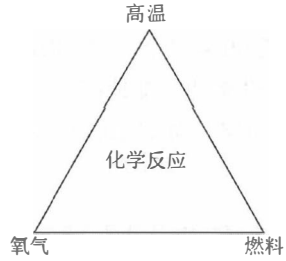


图 10.2　起火三角形

选择抑制介质时，考虑抑制介质针对的起火三角形元素、在实际中的表现、抑制介质通常的有效性以及抑制介质在具体环境中的效果是十分重要的。

除了理解起火三角形之外，还应该了解起火的各阶段，这也非常有用。起火具有很多个阶段，图 10.3 说明了 4 个最重要的阶段：

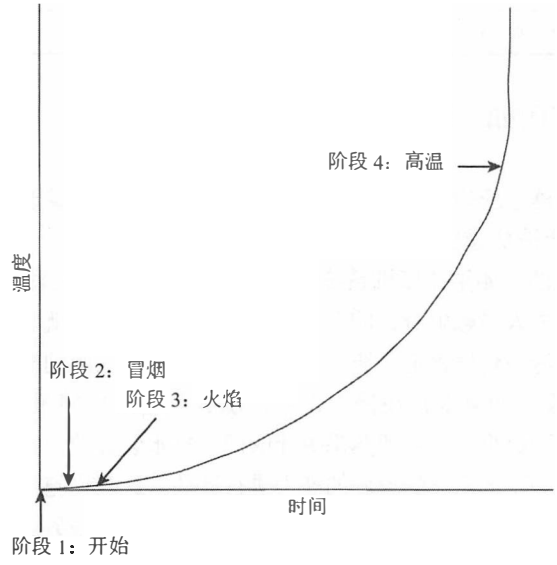


图 10.3　起火的 4 个主要阶段

阶段 1：开始阶段　这个阶段只存在空气电离，不存在冒烟。

阶段 2：冒烟阶段　在这个阶段，起火点出现烟雾。

阶段 3：火焰阶段　这是肉眼能够看到火焰的阶段。

阶段 4：高温阶段　在这个阶段，起火时间已经相当长，此时温度极高，并且燃烧区域内的所有东西都在燃烧。

越早检测到起火，就越容易使用相应的抑制介质灭火，并且造成的破坏越小。

防火管理的一个基本措施是进行适当的人员意识培训。每个人都应该非常熟悉他们所在设施的灭火机制。每个人都应该熟悉在他们主要的工作地点至少有两条安全撤离通道，并且无论在设施的

何处都必须知道如何找到撤离通道。所有人员都应该接受培训，知道灭火器的位置和使用方法。火灾或一般应急响应培训中包含的其他内容有心肺复苏(Cardio Pulmonary Resuscitation，CPR)、紧急关闭程序以及预先设定聚会地点或安全验证机制(如留言箱)。

提示：

数据中心发生的大多数火灾都是由配电插座过载导致的。

1. 灭火器

目前有几种不同类型的灭火器。了解针对不同火灾的灭火器类型，对于扑灭火灾是十分重要和有效的。如果灭火器使用不当，或灭火器的使用方式不正确，那么就无法扑灭火灾，并且反而会导致火灾的进一步蔓延和增强。灭火器只有在火势刚刚开始时才起作用。表 10.2 列出了三种常见的灭火器类型。

表 10.2　灭火器分类

级别	火灾类型	灭火材料
A	普通的易燃品	水、苏打酸(干粉或液态化学物质)
B	液体	二氧化碳、哈龙*、苏打酸
C	电子	二氧化碳、哈龙*
D	金属	干粉

* 哈龙或 EPA 批准的哈龙替代物

提示：

因为水在与燃烧的液体相接触时，液体会浮在水的表面，所以在 B 类火灾中无法使用水进行灭火。因为存在触电的可能性，所以在 C 类火灾中也不能使用水进行灭火。因为金属燃烧会产生氧气，所以氧气抑制方法不适用于金属类火灾。

2. 防火检测系统

为了适当地保护设施免遭火灾，就要求安装自动化检测和抑制系统。目前有许多类型的防火检测系统。当达到某一特定温度时，设定好温度的检测系统就会触发灭火抑制装置。触发器通常是带洒水头的金属或塑料元件，在某一特定的温度下会融化。温度上升比率检测系统在温度的改变速度达到某一特定级别时就会触发灭火抑制装置。火焰激发系统是根据火焰的红外线能量来触发灭火抑制装置。烟感系统则根据光电或放射性电离传感器来触发灭火抑制装置。

大多数防火检测系统可以与火灾响应服务通知机制链接在一起。在灭火抑制装置被触发时，这些链接在一起的系统会通过发出自动的消息或警报来通知本地的火灾响应团队以及请求援助。为了更有效率，需要有策略地放置防火检测装置。不要忘记在吊顶和升降式地板内、服务器机房内、私人办公室和公共区域内、HVAC 室内、升降梯内以及地下室内等地方放置防火检测装置。

可以基于放水灭火系统或气体释放系统使用灭火机制。在人性化的环境中，放水系统最常见；而在通常无人居住的机房，气体释放系统更合适。

3. 放水灭火系统

目前有 4 种主要的放水灭火系统：

- 湿管道系统(也称为封闭头系统)总是充满了水。当灭火装置被触发时，就会立刻放水。
- 干管道系统中包含被压缩的空气。一旦灭火装置被触发，空气泄漏，打开水阀，从而使管道充满水并放出水来。
- 洪水系统是干管道系统的另一种形式，它使用较粗的管道，因此能排出大股的水流。洪水系统对于放置了电子设备和计算机的环境不太适合。
- 预先响应系统是干管道/湿管道系统的组合系统。这种系统一直作为干管道系统存在，直至检测到有火灾(烟、热及其他)发生，然后向管道中充满水。由于充分受热，洒水头触发器被融化之后释放出水。如果在洒水头被触发之前火被熄灭，那么管道可以被手工排空并重新设置。这种系统还允许在洒水头触发之前进行人工干预，以便停止放水。

预先响应系统是最适合用于计算机和人都存在的环境的洒水系统。

提示：

基于水的灭火系统最常见的故障原因是人为错误，例如，在火灾发生时水源被关闭，或者在没有发生火灾时触发放水。

4. 气体释放系统

气体释放系统通常比放水系统更有效。然而，气体释放系统不应当被部署在有人的环境中。气体释放系统通常从空气中抽走氧气，因此对人是非常危险的。这种系统使用加压的气体灭火介质，如二氧化碳、哈龙或 FM-200(哈龙替代物)。

哈龙是一种非常有效的灭火化合物，但它在华氏 900 度时会转变为有毒的气体。除此以外，它还会污染环境(它是一种臭氧耗尽的物质)。在 1994 年，EPA 禁止在美国生产哈龙，同时，在 1994 年后，进口已生产的哈龙产品是非法的(在 2003 年 12 月 31 日后停止生产哈龙 1301、哈龙 1211 和哈龙 2403)。不过，根据蒙特利尔协议，应当联系哈龙再循环设施，以便重新装满释放物质；EPA 正搜寻已生产的哈龙并减少制造新的哈龙。

由于哈龙存在许多问题，因此通常被更加环保和毒性较小的介质替代。下面列出了经 EPA 批准的哈龙的替换物质(更多信息可参考 http://www.epa.gov/ozone/snap/fire/halonreps.html)：

- FM-200(HFC-227ea)
- CEA-410 或 CEA-308
- NAF-S-III(HCFC Blend A)
- FE-13(HCFC-23)
- Argon(IG55)或 Argonite(IG01)
- Inergen(IG541)

也可以用低压水雾替代哈龙，但是这种系统通常不用在计算机房间或电子设备存储设施中。低压水雾是用于快速降低指定区域温度的水汽。

5. 损失

防火检测和灭火措施还涉及处理可能产生的环境污染和由火灾引起的损失。火灾引起的破坏性要素包括烟和热，还包括灭火抑制介质(如水或苏打酸)。烟对大多数存储设备都会造成损坏。热会损坏所有的电子或计算机组件。例如，华氏 100 度会损坏存储磁带，华氏 175 度会损坏计算机硬件(也就是 CPU 和 RAM)，华氏 350 度则会损坏纸质材料(如变形或变色)。

灭火抑制介质可能会引起电路短路、加快侵蚀或导致设备无法使用。在设计火灾响应系统时，必须考虑上述所有问题。

警告：

不要忘记：在出现火灾时，除了火焰与选定灭火抑制介质导致的损失之外，消防员使用水龙头喷水以及在搜寻时使用斧子寻找火源都会给你带来损失。

10.3　实施和管理物理安全

很多类型的物理访问控制机制都可以部署在能控制、监视和方便管理设备的环境中。其中的范围是从障碍物到检测机制。在某个场所内各个不同的部门或区域都应该明确标出是公用还是私用，或是有权限限制的。每一个这样的区域都要求有唯一且集中的物理访问控制、监视和预防机制。以下章节会讨论很多可能用来分开、隔离和控制访问到不同区域的场所的机制，包括内部和外部安全。

10.3.1　周边(例如，访问控制和监控)

建筑物或校园位置的入口也很重要。单入口可极大地提供安全性，但多个入口在紧急情况下可提供更好的疏散性。附近有什么类型的道路？什么交通工具方便(火车、公路、飞机、航运)？一天中的流量级别是什么？

请记住，可访问性也受限于对周边安全的需要。访问和使用的需要应结合和满足边界安全的实施和运行。物理访问控制的使用、监控人员、设备的进入和离开，还有审计/记录所有的物理事件，是维护整体组织安全的关键要素。

1. 栅栏、大门、旋转门和陷阱

栅栏是外围设备。栅栏被用于在受到特殊安全保护级别的区域和其他区域之间进行明确的隔离。用栅栏筑围墙可以包括广泛的成分、材料和建造方法，可能包括地上的画线、铁丝网、带刺铁丝网、水泥墙和使用激光、运动探测仪或热源探测仪的不可见防线。如下所示，不同类型的栅栏对于不同类型的入侵者有效：

- 3 到 4 英尺高的栅栏可以阻挡偶然的侵犯。
- 6 到 7 英尺高的栅栏难以攀越，可以阻止大多数入侵者，但信心坚定的入侵者除外。
- 带有 3 股带刺铁丝网的 8 英尺或更高栅栏甚至可以阻挡信心坚定的入侵者。

大门是栅栏上受到控制的出入点。为了维持栅栏整体的有效性，大门的阻挡程度必须与栅栏的阻挡程度相同。铰链和锁闭/闭合机制应该进行加固，以防止损坏、破坏或拆卸。当大门关闭时，不应该提供任何额外的出入脆弱性。门的数量应当尽可能最少。大门可由保安人员操作，在没有保安人员时，推荐使用看门狗或 CCTV(闭路电视)。

旋转门(参见图 10.4)每次只可以进一个人，并且常常限制为单方向转动。要么只允许进门，要么只允许出门。旋转门基本上可以等同于安全的旋转门。

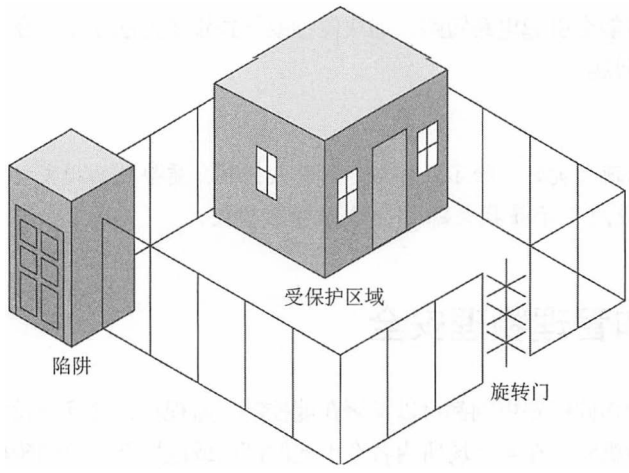


图 10.4　具有陷阱和旋转门的安全物理边界

陷阱(同样参看图 10.4)是通常由保安人员守护的双重门设置。陷阱的目的是牵制主体，直至其身份得到确认和验证。如果经过证明他们可以被授权进入，那么内部的门打开，从而准许这些人员进入设施或周围的附属地区。如果他们没有得到授权，那么两扇门都保持关闭并锁住，直至警卫(通常是保安人员或警察)到来将这些闯入者护送离开设施或因非法入侵逮捕他们(这也被称为迟滞特性)。通常，陷阱包括阻止跟随捎带和尾随的措施。

2. 照明

照明是最常用的一种边界安全控制形式。照明的主要目的是阻拦那些偶然的入侵者、闯入者、小偷和希望在黑暗中实施恶意行为的潜在窃贼。然而，照明不是强有力的阻拦设施，不应该被用作主要的或唯一的防护机制，除非使用照明的区域具有很低的威胁程度。

照明应当不照亮保安人员、看门狗、巡逻岗哨或其他类似的安全保卫者。应该将照明与保安人员、看门狗、闭路电视或入侵检测或监控机制的形式结合在一起使用。照明不能给周围的居民、道路、铁路、机场等带来麻烦或问题。此外，在攻击者非法闯入期间，照明也不能因为强光或反射使保安人员、看门狗和监控设备受到干扰，否则更利于攻击者。

美国国家标准和技术研究院(NIST)制定的使用照明的边界保护标准中规定了关键区域应该是 2 烛光英尺远、8 英尺高的被照亮区域。与照明使用相关的另一个问题是光源的放置。标准模糊地规定灯柱的间距应当与照明区域的直径相等。也就是说，如果照亮区域的直径为 40 英尺，那么灯柱的间距同样应当为 40 英尺。

3. 保安和看门狗

所有的物理安全控制，无论是静止的阻碍物还是主动的检测和监视机制，最终都要依靠人的介入来阻止实际的入侵和攻击。保安可以完成这个工作。保安可能沿边界进行部署，或者被部署在边界内。他们监视着进出口，或者监控着进行检测和监视的显示器。保安的真正优势在于他们能够适应任何环境或情况并做出反应。保安能够记住并识别攻击和入侵的行为和方式，可以适应正在改变的环境，并且能够作出判断和决定。在需要立即的、现场的事态控制和决策制定时，保安常常是恰当的安全控制选择。

遗憾的是，使用保安并不是完美的解决方案。对保安的部署、维护和依赖有很多缺点。不是所

有的环境和设施都支持部署保安。这可能是由于实际环境中存在不适合人的因素，或是设施的规划、设计、位置和建筑的原因。不是所有的保安都是可信赖的。预先筛选、联系和培训无法保证不会出现低效的和不可靠的保安。

即使保安开始很可靠，他们也容易受伤、生病、请假，容易被迷惑和遭受社会工程学攻击，甚至可能由于滥用一些资源而无法被继续雇佣。此外，他们有时更注重自我保护，而不是保护被保卫设施的安全。这可能意味着，保安只有在生命没有受到威胁时才会对设施进行保护。而且，保安通常不知道设施内的操作范围，因此并没有彻底地准备好应付所有的情况。最后一点，保安的费用很高。

看门狗可以替代保安，它们常常作为边界的安全控制措施进行部署。作为侦测和威慑的一种形式，看门狗是非常有效的。然而，喂养狗的费用很高，并且需要高标准的养护，同时还会带来极高的保险和责任要求。

10.3.2　内部安全(例如，陪同要求/访问者控制、钥匙和锁)

如果设备采用限制区域来控制物理安全，那就需要用机制来控制访问者。通常会有一名护卫被指派给访问者，并且密切监视他们的进出入和活动。未跟踪到外人进入保护区之后的行动将会导致大部分被保护的资产遭受恶意攻击。使用钥匙、密码锁、徽章、运动探测器、入侵报警等也会对访问者控制有好处。

1. 钥匙和密码锁

锁使得被关闭的门保持闭合。它们被用于阻止缺乏正确授权的人。锁是身份标识和身份认证机制的强硬形式。只有具有正确的钥匙或密码，才会被授权准许进入。使用钥匙的锁是最常见的和最廉价的物理访问控制设备形式，常常被称作预置锁。这种锁容易被撬开，撬锁往往被归类于加垫片的锁的攻击机制。

真实场景

锁的使用

钥匙或密码锁各自的用途是什么？

记忆力不好的用户往往会出现遗忘问题。Elise 经常忘记自己的密码组合，而 Francis 上班时从来就没记住过携带安全钥匙卡。Gino 对自己的行政管理模式感到悲观，因此宁愿在所有正当的地方都使用密码锁和钥匙卡。

在哪种情况或条件下使用密码锁，在哪种场合选择使用钥匙或钥匙卡？如果出现密码锁或钥匙丢失，哪种选项的风险更大？能否确定这些单点故障不会为受保护的资产带来显著的风险？

许多组织通常在设施的不同区域使用不同形式的钥匙或密码锁。在选定的公共出入口(如从外部进入建筑物、进入房间)使用钥匙和钥匙卡，密码锁则被用于各自独用的入口处(如存储柜、文件柜等)。

可编程的锁或密码锁能够提供比预置锁更广泛的控制。一些可编程的锁可以被配置使用多种有效的访问号码，也可能包括采用键盘、智能卡、密码设备的数字或电子控制。例如，电子访问控制

(EAC)锁由下列三种元素组成：保持门关闭的电磁体、验证主体和使电磁体失效的凭证读卡机，以及重新使用电磁体的闭门感应器。

锁可以作为边界进出访问控制设备，从而代替保安。保安在得到访问授权之前对身份进行核实，进而打开和关闭闸门以准许访问。此外，锁本身也可以作为验证设备对进出进行授权或限制。

2. 员工证

员工证、身份证或安全 ID 都是物理身份标识和/或电子访问控制设备的形式。员工证既可以像指示有效员工或来访者的名字标签一样简单；也可以像智能卡或标记设备一样复杂，以便采用多因素身份认证对身份进行核实和证实，为进入设施、特定的房间或使用受保护的工作站提供身份认证和授权。员工证常常包括照片、带有编码数据的磁条和个人信息，从而帮助保安核实身份。

员工证可能被用在物理访问主要受到保安控制的环境中。在这样的情况中，员工证成为保安的可见身份标识工具。它们可以通过比较本人和照片，并且参照印刷好的或电子的被授权人员花名册确定人员是否可以进入。

员工证还可以在由扫描设备守卫而非保安守卫的环境中使用。在这样的环境中，员工证既可以被用于进行身份标识，也可以被用于身份认证。当员工证被用于身份标识时，首先要在设备上刷卡，随后员工证的持有者必须提供一个或多个身份认证要素(如密码、密码短语，如果使用了生物测定设备，那么还涉及生物学特性)。当员工证被用于身份认证时，员工证的持有者要提供 ID、用户名等，然后刷卡进行身份认证。

3. 运动探测仪

运动探测仪或运动传感器是在特殊区域内使用的、用于感知物体运动的设备。运动探测仪的类型有很多种，包括红外线、热能、波形、电容、光电和无源音频。

- **红外运动探测仪**　对被监控区域红外照明模式的显著变化进行监视。
- **热能型运动探测仪**　对被监控区域内的热能等级和模式的显著变化进行监视。
- **波形运动探测仪**　向被监控的区域发射连续的弱超声波或高频微波，并且对反射波的显著扰动或变化进行监视。
- **电容运动探测仪**　对被监控物体周围区域的电场或磁场变化进行探测。
- **光电运动探测仪**　通常在没有窗户或保持昏暗的房间内部使用。
- **无源音频运动探测仪**　对被监控区域内的非正常声音进行侦听。

4. 入侵警报

无论何时显示环境中出现重大或有意义的变化，运动探测仪都会发出警报。警报是一种分离机制，可以引发威慑、防护和/或通知。

威慑报警　引发威慑警报可能会采用额外的加锁、关门等措施。这种警报的目的是使得进一步的入侵或攻击变得更难。

排斥报警　引发排斥警报声通常听起来像汽笛或钟声，并且会将灯打开。这些警报类型被用于令入侵者或攻击者气馁，从而不再继续他们的恶意或入侵行为，并且离开这个设施。

通知报警　引发通知警报对于入侵者/攻击者来说常常是缄默的，但是它们会记录事故的相关数据，并且通知管理员、保安和执法机构。事故的记录可以采取日志文件和/或闭路电视磁带的形式。缄默警报的目的是将授权的安全人员带到入侵或攻击的位置，以便期望抓住进行有害活动的人。

报警也通过它们所在的地方(本地、集中、专有或辅助)被归类。

本地报警　本地警报系统必须广播可听到的警报信号(最大可到 120 分贝)，这个信号最远可以传播 400 英尺。此外，本地警报系统必须受到保护，通常应由保安进行保护，以防止损害和损坏。为了使警报系统有效，附近必须有安全团队或保安，他们可以在警报被触发后立即进行响应。

集中式警报系统　可能在本地没有警报，在警报触发时会通过信号通知远程或集中式监控站。大多数中央集中式系统都是很知名的公司或是国家安全公司，如 Brinks 和 ADT。专有系统类似于中央系统，但托管组织有他们自己的现场保安人员等待并响应安全破坏。

辅助警报系统　辅助警报系统可以加入本地或集中式警报系统。当安全边界被破坏时，紧急服务机构将被通知和对事件做出响应，并抵达相应地点。这些紧急服务机构可能包括消防、警察和医疗服务。

两种或多种类型的入侵报警系统能够集成到单个解决方案中。

5. 二次验证机制

当运动检测器、传感器和报警器被使用时，二次验证机制应该在适当的位置。随着这些设备的灵敏度增高，错误触发会经常发生。无害的事件，如动物、鸟类、昆虫或授权人员的出现，可能触发错误警报。使用两个或两个以上的检测和传感器系统，并要求警报发出之前的短时内有两个或两个以上的快速成功触发。这可以显著减少错误警报，并提高报警显示实际入侵或攻击的可能性。

CCTV 是一种安全机制，涉及运动探测器、传感器和报警器。然而，CCTV 并不是自动化的检测和响应系统。CCTV 需要人员观看捕获的视频来检测可疑和恶意的活动，并触发报警。安全摄像头可以扩大保安人员的有效可见范围，因此增大了监控的范围。在许多情况下，CCTV 不作为主要的检测工具，因为要支付高费用给坐在那里观看视频屏幕的人。相反，它用来作为一个二次或后续机制，当自动化系统触发后进行审查。事实上，审计和审计跟踪的使用逻辑同样用于 CCTV 和事件记录。CCTV 是预防措施，而审查事件记录是检测措施。

真实场景

二次验证

和前面的真实场景描述的一样，Gino 处在安全破坏不断的风险中，因为 Elise 经常会忘记(因此写下)每一个密码，而 Francis 习惯性地忘记钥匙卡的位置。当其他人拥有这些物品的任何一个并知道如何或在哪里使用它们时，将会发生什么？

Gino 的最大优势就是已经在工作产所建立了若干二次验证机制，这可能包括一个 CCTV 系统，这个系统在某些指定地区进行监视，并识别使用钥匙卡访问或输入密码组合的人员的脸。当追踪意外或有意非法访问时，即使穿过检查点入口和出口的录像记录也都是有帮助的。

通过已知的“问题用户”或“问题身份”，许多安全系统可以在这些身份被使用时发出通知或警报。人员随访可以或不可以保证，具体取决于可用的系统以及未经授权的访问可能带来的风险。但在任何时候 Elise(或有人使用这个身份)登录到系统或使用 Francis 的钥匙卡进入，一名巡视和走动的保安人员可以被安排来确保一切事情向好的方面发展。当然，让 Elise 和 Francis 的经理劝告他们适当地使用(存储)密码和钥匙卡以及让他们了解相关潜在风险，也可能是一个好主意。

真实场景

部署物理访问控制

在现实世界中，将部署多层物理访问控制来管理设施内授权和未授权的人流。最外层的将是照明。场所的整个外周应清楚地被照亮，这将有助于简单地识别人员，并使得更容易注意到入侵者和威慑潜在入侵者。在灯光的区域内，放置栅栏或墙以防止入侵。栅栏或墙上的特定控制点应该设置入口或出口。这些地方应该有门、旋转门或陷阱门，并通过 CCTV(闭路电视)和保安人员进行监控。所有入口点在授权进入前，都必须要求进行识别和认证。

在设施内，属于不同敏感或保密级别的区域应明显被分开和划分，这是特别适用于访问者访问的公共领域和地区。当任何人从一个区域移到另一个区域时，应要求额外的识别/认证过程。最敏感的资源和系统几乎都要和最有特权的人员隔离，并且要位于建筑物的中央。

6. 环境和生命安全

保护环境的基本要素和保护人员生命是设施内物理访问控制和安全维护的一个重要方面。不论在任何情况和任何条件下，保护人员生命是安全的最重要方面。因此，对于所有安全解决方案来说，防止人员遭受生命伤害是最重要的目标。

对人员生命安全进行维护的部分内容是维护设施的基本环境。在很短的时间内，人们可以在没有水、食物、空调和电力的条件下生存下来。但在某些情况下，这些元素的损失可能会有灾难性的后果或可更直接导致即刻发生及危险的问题。洪水、火灾、有毒物质的释放以及自然灾害都会威胁人员生命以及设施的稳定性。物理安全措施应注重保障人员生命，然后才是恢复环境的安全性和恢复 IT 基础设施的必要功能。

人员应该永远是重中之重。只有在人员生命安全的情况下，才能考虑解决业务连续性问题。许多组织采取人员紧急计划(Occupant Emergency Plan，OEP)指导和协助在灾难发生时维持人员生命安全。OEP 提供了如何减少对生命的威胁、防止损伤、管理压力、处理迁移以及提供安全监控保护财产的指导，并保护资产避免在物理事件中遭受损害。OEP 不解决 IT 问题或业务连续性问题，而只解决人员和一般财产问题。BCP 和 DRP 才解决 IT、业务连续性和恢复问题。

7. 隐私责任和法律需求

个人信息的安全性也需要在任何组织的安全策略中得到解决。此外，安全策略必须符合行业和管辖权内的现行监管要求。

隐私意味着保护个人信息不被泄露给未经任何授权的个人或实体。在今天的网络世界里，公共信息和私人信息之间的界限往往是模糊的。例如，关于网上冲浪的习惯信息是私人的还是公众的？没有你的同意，这些信息可以合法收集吗？并且收集信息的组织可以出售你未分享的信息去获利吗？此外，个人信息远不止网上生活习惯的信息；还包括你是谁(姓名、地址、电话、种族、宗教、年龄等)，你的健康和医疗记录，你的财务记录，甚至你的犯罪或法律记录。一般这样的信息可放入个人身份信息(PII)标题的下面，如 NIST 发布的“保护个人身份信息(PII)机密性指南”。该指南可通过访问以下网址在线获得：http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf。

处理隐私是任何有员工的组织的一个要求。因此，隐私是所有组织的一个核心问题。对于任何组织，隐私保护应该在安全策略中是一个核心任务或目标设定。关于个人隐私问题的讨论，在第 4 章“法律、法规和合规性”中有更多的描述。

8. 合规要求

每个组织都运营在一定的行业和管辖权内。这两个实体(可能还有附属的实体)把法律要求、限制和规定强加到它们领域内的组织实践中。这些法律要求可以应用于软件许可、雇佣限制、处理敏感资料，并符合安全规定。

遵守所有适用的法律规定是维护安全的一个关键部分。法律法规要求对于行业或国家(也经常是州和城市)都一定在基础安全建设方面被视为底线和基础。

10.4　本章小结

如果没有对物理环境进行控制，那么行政性或技术性/逻辑性的访问控制就无法提供足够的安全性。如果怀有恶意的人可以获得对设施或设备的物理访问权限，那么他们就会拥有这些设施或设备。

实现和维护物理安全有很多方面的内容和要素。其中一个核心要素是选择或设计能够容纳 IT 基础设施和支持组织运营的场所。必须先订立计划，这个计划概述了组织的安全需求，并且强调了用于提供安全性的方法或机制。这样的计划通过被称为关键路径分析的过程进行开发。

实现对物理安全进行管理的安全控制可以分为三组：行政性的、技术性的和物理性的。行政性的物理安全控制包括场地的构造和选择、场地管理、人员控制、意识培训和紧急事件响应及规程。技术性的物理安全控制包括访问控制、入侵检测、警报、CCTV(闭路电视)、监视、HVAC、电源以及火灾检查和排除。物理性的安全控制包括围墙、照明、锁、建筑材料、陷阱、看门狗和警卫。

物理访问控制机制具有很多类型，它们可以被部署在环境中来控制、监视和管理对设施的访问。这些类型可以包括从阻碍机制到检测机制的很多内容，这些内容包括栅栏、大门、旋转门、陷阱、照明、保安、看门狗、钥匙锁、密码锁、员工证、运动探测仪、传感器和警报。

技术控制最常作为管理物理访问的访问控制机制，其中包括智能卡/无记忆卡和生物学测定。除了访问控制之外，物理安全机制还包括审计跟踪、访问日志和入侵检测系统等形式。

配线间和服务器机房是重要的基础设施元素，需要对它们进行保护。它们通常用来容纳核心网络设备和其他敏感设备。保护措施包括足够的锁、监视、访问控制和定期的物理检查。

介质存储安全应包含一个库检测系统，存储在一个上锁或安全的柜子内，以及消磁并重复使用介质。

物理访问控制和维护设施安全的一个重要方面是：保护环境中的基本要素和保护人员的生命安全。在所有环境中和所有的条件之下，安全性最重要的方面是保护人的安全。避免对人员的伤害是所有安全解决方案中最重要的目标。提供稳定的电源以及管理环境也同样重要。

防火检测和灭火措施绝不能被忽略。除了保护人员不受到伤害以外，设计防火检测和灭火措施的目的是将由火、烟、热和灭火材料引起的损失最小化，特别是与 IT 基础设施相关的部分。

人应该是最优先的考虑对象。只有在人员安全后才应考虑业务连续性。

10.5 考试要点

理解为什么缺乏物理安全就没有安全性。缺乏对物理环境的控制，那么行政性的或技术性的/逻辑性的访问控制就无法提供足够的安全性。如果怀有恶意的人可以获得对设施或设备的物理访问权限，那么他们就会进行他们想要做的任何事情，包括从破坏到泄密乃至更改的任何事情。

能够列举行政性的物理安全控制。行政性的物理安全控制包括场地的构造和选择、场地管理、人员控制、意识培训和紧急事件响应及规程。

能够列举技术性的物理安全控制。技术性的物理安全控制包括访问控制、入侵检测、警报、CCTV、监视、HVAC、电源以及火灾检查和排除。

能够指出物理安全的物理控制。物理安全的物理控制包括栅栏、照明、锁、建筑材料、陷阱、看门狗和警卫。

理解控制的作用顺序。控制的作用顺序依次是：阻拦、拒绝、检测和延缓。

理解选择场地和设计建筑设施的主要内容。确定场地方面的主要内容包括可视性、周围地形、地区的可到达性以及自然灾害的影响。设计建筑设施方面的主要内容是要理解组织需要的安全等级，在建筑设计开始之前制定计划。

理解如何设计和配置安全工作区域。对设施内所有地方的进入要求不应该等同对待。包含更高价值或重要资产的地区的进出应该受到限制。有价值的和机密的资产应该放在设施提供的保护核心或中心地区。同样，集中放置的服务器或计算机机房不需要人员协调。

理解配线间的安全问题。现代的配线间是整个建筑或一个楼层中连接到其他重要设备的网络电缆所在的地方，如配线架、交换机、路由器、局域网扩展、骨干渠道。配线间大部分的安全集中在防止未授权的物理访问。如果未授权入侵者进入该区域，他们可能会偷盗设备、拖拉或切断电缆甚至安放窃听设备。

理解在安全设施内如何管理来访者。如果设备通过受限制的区域控制物理安全，那么就需要具备管理来访者的方法。来访者经常会被指派一名陪同，并且他们的访问和行动都要受到严密监视。当外来人员被授权进入受保护的区域时，未能对他们的行动进行跟踪可能会导致针对保护程度最高的资产的恶意行为。

理解为管理物理安全而进行的安全控制的三种策略，并且能够举出它们的例子。用于对物理安全进行管理的安全控制可以分为三组：行政性的、技术性的和物理性的。理解何时以及如何使用这些类型，并且能够列出每种类型的例子。

理解介质存储的安全需求。介质存储设施应该被设计用于安全地保存空白介质、可重用介质和安装介质。关注的问题包括盗窃、数据损坏和数据的残余恢复。对介质存储设备的保护包括带锁的柜子或保险箱、使用库管理员或保管员、实施存入/取出过程以及利用介质消磁。

理解证据存储的问题。证据存储用来保留用于恢复、内部调查和电子取证调查的日志、驱动图像、虚拟机快照和其他数据。保护措施包括专用/隔离存储设施、离线存储、活动跟踪、哈希管理、访问限制和加密。

理解物理访问控制的常见威胁。无论使用哪一种形式的物理访问控制，为了阻止滥用、伪装和尾随，必须同时配备保安人员或其他监控系统。物理访问控制的滥用是指打开安全门或者绕过锁或访问控制措施。伪装是指使用其他人的安全 ID 获得进入某座设施的权限。尾随是指跟随着某人通过受到安全保护的门或通道，而本身没有接受身份识别或获得授权。

理解对审计跟踪和访问日志的需要。对于物理访问控制来说，审计跟踪和访问日志也是非常有用的工具。它们可能需要保安人员手工建立，或者在有足够的自动化访问控制机制(例如，智能卡和某些接近式读卡机)的情况下自动生成。还可以考虑使用 CCTV(闭路电视)进行入口点的监控。CCTV(闭路电视)能够将审计跟踪和访问日志与可视化的事件历史记录进行比较。这些信息对于重新构建入侵、破坏或攻击事件非常关键。

理解对平稳电源的需要。电力公司供应的电源并不总是连续的和平稳的。大多数电子设备需要平稳的电力供应才能正常工作。由于电源的波动而导致设备损坏的事情经常发生。许多组织机构通过几种方法来选择管理他们自己的电源。不间断电源供应(UPS)是一种自充电的电池类型，可以为敏感的设备提供连续和平稳的电力。UPS 在主要电源出现故障或无法获得的情况下，还能够提供持续的电力供应。UPS 可以提供数十分钟或数小时的电力，这取决于它的容量和设备所需的用电量。

理解常用的电力术语。知道下列术语的定义：故障、中断、电压不足、降压、脉冲、电涌、起动功率、噪声、瞬时现象、平稳和接地。

理解如何控制环境。除了考虑电源问题，维护环境还包括控制采暖、通风和空调(HVAC)的机制。主要放置计算机的房间应该保持温度在华氏 60 到 75 度之间(即摄氏 15 到 23 度)。计算机房间的湿度应该维持在 40%和 60%之间。湿度太高会导致侵蚀，湿度太低会导致产生静电。

知道什么是静电。即使在不产生静电的地毯上，如果环境中的湿度太低，那么也仍然可能产生两万伏特的静电放电。即使很少的静电放电也可能毁坏电子设备。

理解管理漏水和水灾的需求。环境安全策略和措施中应当解决漏水和水灾问题。管道漏水不会每天都发生，但当真的发生时，经常会造或重大的损失。水和电是不能相容的。如果计算机系统与水接触了(特别是在系统运行时)，那么就会发生损坏事故。只要有可能，就要让放置服务器的房间和重要计算机设备远离任何水源或传输管道。

理解防火检测和灭火措施的重要性。防火检测和灭火措施绝不能被忽略。保护人员不受到伤害应该始终是所有安全或保护系统中最重要的目标。除了保护人员不受到伤害以外，设计防火检测和灭火措施的目的是将由火、烟、热和灭火材料引起的损失最小化，特别是与 IT 基础设施相关的部分。

理解由于火灾和灭火材料可能导致的环境污染和损失。火灾引起的破坏性要素包括烟和热，也包括灭火介质(如水或苏打酸)。烟对大多数存储设备都会造成损坏。热会损坏所有的电子或计算机组件。灭火抑制介质可能会引起电路短路、加快侵蚀或导致设备无法使用。在设计火灾响应系统时，必须解决所有这些问题。

理解人员的隐私和安全。在所有的情况下，安全最重要的作用方面是保护人。因此，防止对人的伤害是所有安全解决方案中最重要的目标。

10.6　书面实验室

1. 哪种设备有助于定义组织的边界，同时也能够阻拦偶然的非法进入？
2. 哈龙型灭火技术存在什么问题？
3. 消防队灭火后会带来哪些潜在的问题？

10.7 复习题

1. 以下哪一项是安全中最重要的方面?
   A. 物理安全
   B. 入侵检测
   C. 逻辑安全
   D. 意识培训
2. 对于新的设施，有什么方法可以用来制定出组织的需要?
   A. 日志文件审计
   B. 关键路径分析
   C. 风险分析
   D. 存货清单
3. 通常什么基础设施组件位于多个楼层的相同位置，用于把每个楼层网络连接在一起以提供便利?
   A. 服务器机房
   B. 配线间
   C. 数据中心
   D. 介质柜
4. 以下哪一项不是设施或场地的安全关注的设计元素?
   A. 工作区和访客区的隔离
   B. 限制对高价值或重要区域的访问
   C. 位于设施核心或中央位置的机密区域
   D. 对设施内所有位置的相同访问
5. 为了维持最有效和安全的服务器机房，以下哪一项不必是真的?
   A. 必须和人共存
   B. 必须包括非水灭火装置的使用
   C. 湿度必须保持在 40%到 60%之间
   D. 温度必须保持在华氏 60 到 75 度。
6. 下列哪个典型的安全措施的执行不涉及包含可重用移动介质的存储设施?
   A. 雇佣库管理员或保管员
   B. 使用存入/取出过程
   C. 哈希
   D. 在返回的介质上使用净化工具
7. 以下哪一项是一套双门，往往由保安人员保护，并且用于容纳主体，并直到他们的身份和授权信息被验证?
   A. 大门
   B. 旋转门
   C. 陷阱
   D. 接近式传感器

8. 周边安全设备或机制的最常见形式是什么？

A. 保安人员

B. 栅栏

C. CCTV(闭路电视)

D. 照明

9. 以下哪一项不是使用保安人员的缺点？

A. 保安人员通常不了解设施内操作的范围

B. 并非所有环境和设施都支持保安人员

C. 并非所有安全人员自身就是可靠的

D. 预先筛选、联系和培训并不能保证安全人员的有效和可靠

10. 基于水的灭火系统中最常见的故障原因是什么？

A. 缺水

B. 人

C. 离子检测器

D. 在吊顶上探测仪的布放

11. 物理访问控制设备最普通和便宜的是什么？

A. 照明

B. 保安人员

C. 钥匙锁

D. 栅栏

12. 什么类型的运动检测仪能感应到被监控对象周围电场或磁场的变化？

A. 波形检测仪

B. 光电检测仪

C. 热能检测仪

D. 电容检测仪

13. 以下哪一项不是触发物理安全报警的典型类型？

A. 预防

B. 威慑

C. 排斥

D. 通知

14. 无论使用何种形式的物理访问控制，保安人员或其他监控系统都必须被部署来阻止以下问题，但除了哪一个？

A. 尾随

B. 间谍

C. 伪装

D. 滥用

15. 所有安全解决方案中最重要的目标是什么？

A. 暴露阻止

B. 维护完整性

C. 人身安全

D. 维持可用性

16. 计算机机房理想的湿度范围是什么？

A. 20%至 40%

B. 40%至 60%

C. 60%至 75%

D. 80%至 95%

17. 什么电压等级的静电会引起存储在硬盘中的数据的破坏？

A. 4000 伏特

B. 17 000 伏特

C. 40 伏特

D. 1500 伏特

18. B 类灭火器不会使用下列哪个灭火材料？

A. 水

B. 二氧化碳

C. 哈龙或可接受的哈龙替代品

D. 苏打酸

19. 对于计算机设施，基于水的灭火系统最好的类型是什么？

A. 湿管系统

B. 干管系统

C. 预先响应系统

D. 洪水系统

20. 在发生火灾和除非灭火的情况下，下列哪一项不是造成计算机设备损坏的罪魁祸首？

A. 热

B. 灭火介质

C. 烟

D. 照明

第 11 章

网络安全架构与保护网络组件

本章中覆盖的 CISSP 考试大纲包含：

4) 通信与网络安全(设计和保护网络安全)

- A. 应用安全设计原则到网络架构中(例如，IP 和非 IP 协议、分段)
  - A.1 OSI 和 TCP/IP 模型
  - A.2 IP 网络
  - A.3 应用多层协议(例如，DNP3)
  - A.4 汇聚协议(例如，FCoE、MPLS、VoIP、iSCSI)
  - A.5 软件定义网络
  - A.6 无线网络
  - A.7 使用密码学维护通信安全
- B. 保护网络组件
  - B.1 硬件的操作(例如，调制解调器、交换机、路由器、无线接入点、移动设备)
  - B.2 传输介质(例如，有线、无线、光纤)
  - B.3 网络接入控制设备(例如，防火墙、代理)
  - B.4 终端安全
  - B.5 内容分发网络
  - B.6 物理设备

计算机和网络由于通信设备、存储设备、处理设备、安全设备、输入设备、输出设备、操作系统、软件、服务、数据和人融合而产生。CISSP CBK 指出，深入地了解这些硬件和软件知识是实现和维护安全性的基本要素。本章将讨论在网络连接、线缆连接、无线连通性、TCP/IP 及相关协议、网络设备、防火墙中作为指导原则的 OSI 模型。

CISSP 认证考试的“通信与网络安全”领域涉及与网络组件相关的主题(例如，网络设备和协议)，特别是它们的工作方式以及与安全的关系。本章和第 12 章“安全通信和网络攻击”会讨论这个领域。只有阅读和学习了这两章的内容，才能确保全面了解 CISSP 认证考试的基本内容。

11.1 OSI 模型

通过协议使得网络上的计算机之间通信成为可能。协议是一组规则和约束，它们定义了数据在网络介质上(例如，双绞线、无线传输等)如何传输。在网络发展的初期，许多公司都曾具有自己的专有协议，这意味着不同供应商的计算机之间的交互常常非常困难，甚至无法进行交互。在努力解决这个问题的过程中，国际标准化组织(ISO)在 20 世纪 80 年代初开发了针对协议的 OSI 参考模型。明确地说，ISO 7498 定义了 OSI 参考模型(更常用的名称是 OSI 模型)。理解 OSI 模型及其与网络设计、部署和安全性的关系对于准备 CISSP 考试来说必不可少。

为了适当地建立安全数据通信，充分了解计算机通信中涉及的所有技术是很重要的。从硬件、软件到协议、加密，此外还需要知晓很多细节，理解标准和遵循流程。另外，安全网络架构和设计的基础是十分全面通用的知识，涉及OSI模型、TCP/IP模型还有IP网络。

11.1.1 OSI 模型的历史

OSI 模型不是第一个，或许也不是唯一一个试图简化网络互连协议或建立通用通信标准的模型。事实上，作为今天得到最广泛使用的协议，TCP/IP(基于 DARPA 模型，这种模型现在也被称为 TCP/IP 模型)早在 20 世纪 70 年代初期就已被开发出来，而 OSI 模型直到 20 世纪 70 年代末期才被开发出来。

OSI协议的开发为所有计算机系统建立了一个通用的通信结构或标准。实际的OSI协议从来没有得到过广泛采用，但是OSI协议背后的理论，也就是OSI模型，却被大家很容易接受了。作为一个抽象的架构或理论模型，OSI模型说明了在理想硬件上的理想环境中协议应该怎样工作。因此，OSI 模型已经成为一个所有协议都可以与其比较和对照的通用参考点。

11.1.2 OSI 功能

OSI 模型把网络任务划分到 7 个不同的层中。在两台计算机之间的每一层负责执行数据交互(换句话说，网络通信)过程中对应的特定任务。这些层通常从低到高以数字标注(见图 11.1)。它们通常用各自的名称或层数称呼。例如，第 3 层也就是常说的网络层。这些层用来具体表明信息流如何通过不同的通信层面。每一层都与上面的层和下面的层进行直接通信，加上其他对等的层而形成通信伙伴系统。

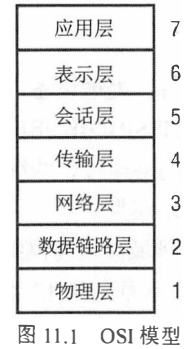


图 11.1 OSI 模型

OSI 模型对于网络产品供应商们是一个开放式的网络架构指南。这个标准或指南为开发新的协

议、网络服务甚至硬件设备提供了一个通用的基础。根据 OSI 模型，供应商们能够确保他们的产品可以与其他公司的产品集成在一起，并且会得到操作系统的广泛支持。如果所有的供应商都开发各自的网络架构，那么不同供应商的产品之间将几乎无法实现互通性。

OSI 模型的真正优点在于它对网络互连实际工作方式的描述。在最基本的概念中，网络通信出现在物理连接中(无论物理连接是铜线上的电子、光纤中的光子还是空气中的无线电信号)。物理设备建立了信道，电子信号能够通过信道从一台计算机传递至另一台计算机。这些物理设备信道只是 OSI 模型定义的 7 种逻辑通信类型中的一种。OSI 模型的每一层都通过一个逻辑信道与另一台计算机上的对等层进行通信。这样一来，通过识别远程通信实体以及验证接收数据的来源，基于 OSI 模型的协议就能够支持某种身份认证类型。

11.1.3　封装/解封装

基于 OSI 模型的协议采用了一种被称为封装的机制。通过每一层从上一层接收到数据后，封装会给数据添加一个报头，并且还可能添加一个报尾，然后才将数据传输到下一层。随着报文在每一层的封装，报文的大小也在不断增长。数据从 OSI 模型的应用层向下移动至物理层时，在每一层都会发生封装。数据从 OSI 模型的物理层向上移动至应用层时，在每一层发生的逆向操作称为解封装。封装/解封装过程如下所示：

(1) 应用层创建报文。

(2) 应用层将报文传递至表示层。

(3) 表示层通过向报文添加信息对它进行封装。信息通常只被添加到报文的开始部分(称为报头)；不过，某些层也会在报文的结尾部分添加内容(称为报尾)，如图 11.2 所示。

(4) 向下传递报文并且添加每层指定信息的过程将一直持续，直到报文到达物理层。

(5) 在物理层，报文被转换为表示比特的电子脉冲，并且通过物理连接进行传输。

(6) 处于接收状态的计算机从物理连接中截获这些比特，并且在物理层重新创建报文。

(7) 物理层将报文从比特转换为数据链路帧，并且将报文向上发送至数据链路层。

(8) 数据链路层剥离信息，并且将报文向上发送至网络层。

(9) 解封装的过程一直持续，直到报文到达应用层。

(10) 当报文到达应用层时，报文中的数据被发送至预期的软件接收者。

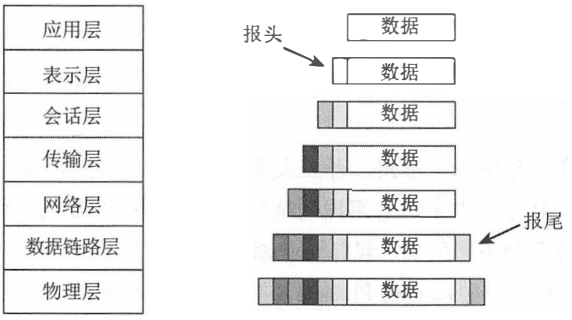


图 11.2　OSI 模型的封装示例

被每一层去除的信息包括指令、校验和等，它们只能被最初添加或创建这些信息的对等层理解(参看图11.3)。这些就是建立确保不同计算机上的对等层能够进行通信的逻辑信道的信息。

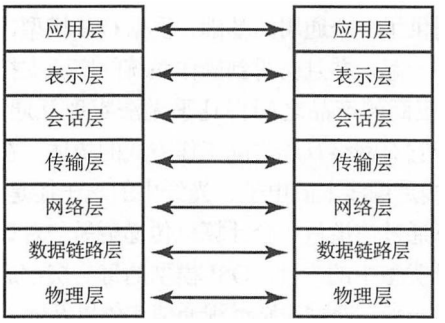


图 11.3 OSI 模型的对等层逻辑信道的示例

发送至应用层(第7层)上协议栈中的报文被称为数据流。直至到达传输层(第4层)，报文仍然保持着数据流的标签，报文在传输层被称为段(使用TCP协议时的称呼)或数据报(使用UDP协议时的称呼)。在网络层(第3层)，报文被称为数据包。在数据链路层(第3层)，报文被称为帧。在物理层(第1层)，数据已经被转换为能够通过物理连接介质传输的比特。图11.4说明了每一层如何通过这个过程来改变数据。

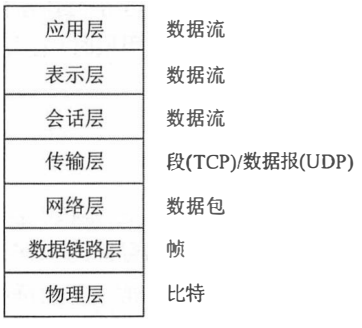


图 11.4 OSI 模型的数据名称

11.1.4 OSI 分层

理解OSI模型每一层的功能和职责将有助于理解网络通信的运作原理、攻击对网络通信的影响以及如何实施保护网络通信的安全措施。接下来的章节中，我们将从最底层开始对每一层进行讨论。

注意：

要了解 TCP/IP 协议栈的更多信息，请在维基百科站点 http://en.wikipedia.org 上搜索 “TCP/IP”。

记忆 OSI

尽管有人认为 OSI 在实际中很少应用，并且大多数技术人员并未经常使用 OSI，然而 OSI 模型及其相关概念仍然在 CISSP 考试中占据着牢固的地位。为了最大限度地掌握 OSI，必须首先能够按照正确的顺序记住 OSI 的 7 个不同的层。记忆这些层的一个常见方法是根据每一层名字的首字母生成助记语，我们比较喜欢的一个助记语是 Please Do Not Teach Surly People Acronyms。根据这个助记语，就能够记忆从物理层到应用层的各层。还有一个助记语，是从应用层向下：All Presidents Since Truman Never Did Pot。此外还存在其他一些记忆模式，不过需要确认它们采用的顺序是由上至下还是由下至上。

1. 物理层

物理层(第 1 层)从数据链路层接收帧，并把帧转换为可以通过物理连接介质传送的比特。物理层还负责接收来自物理连接介质的比特，并且将比特转换为数据链路层所使用的帧。

物理层包含了会告诉协议如何应用硬件来发送和接收比特的多种设备驱动程序。物理层还涉及电气规范、协议和接口标准，如下所示：

- EIA/TIA-232 和 EIA/TIA-449
- X.21
- 高速串行接口(High-Speed Serial Interface，HSSI)
- 同步光网络(Synchronous Optical Network，SONET)
- V.24 和 V.35

通过设备驱动程序和这些标准，物理层控制吞吐率、处理同步、管理线路噪音和介质访问，并且决定使用数字、模拟或光脉冲信号在物理硬件接口上传输和接收数据。

工作在物理层上的网络硬件设备包括网络接口卡(NIC)、集线器、中继器、集中器和放大器。这些设备执行基于硬件的信号操作，例如，从一个连接端口向其他所有端口发送信号(集线器的要做操作)，或者为了支持更长的传输距离而对信号进行放大(中继器要做的操作)。

2. 数据链路层

数据链路层(第 2 层)负责将来自网络层的数据包格式化为可以进行传输的适当格式。这种适当的格式由网络硬件和网络技术决定，并且存在多种可能性，如以太网(IEEE 802.3)、令牌环(IEEE 802.5)、异步传输模式(Asynchronous Transfer Mode，ATM)、光纤分布式数据接口(Fiber Distributed Data Interface，FDDI)和铜线分布式数据接口(Copper DDI，CDDI)。数据链路层内保留了一些技术特有的协议，这些协议将数据包转换为适当格式的数据帧。一旦数据帧完成了格式化，就会被发送至物理层进行传输。

下面列出了数据链路层内驻留的协议：

- 串行线路网络协议(SLIP)
- 点对点协议(PPP)
- 地址解析协议(ARP)
- 反向地址解析协议(RARP)
- 二层转发协议(L2F)
- 二层隧道协议(L2TP)
- 点对点隧道协议(PPTP)
- 综合服务数字网络(ISDN)

在数据链路层上对数据执行的部分处理过程包括向数据帧添加硬件的源地址和目的地址。硬件地址指的是介质访问控制(MAC)地址，它是一种用十六进制表示法表示的 6 字节(48 比特)二进制地址(例如，00-13-02-1F-58-F5)。地址的前三个字节(24 比特)指示了物理网络接口的供应商或制造商。这被称为组织唯一标识符(Organizationally Unique Identifier，OUI)。OUT 由 IEEE 进行注册并控制发行。OUI 可以用于通过 IEEE 网站 http://standards.ieee.org/regauth/oui/index.shtml 发现网卡制造商。后三个字节(24 位)代表一个独特的数字并被分配给该接口的制造商。没有两个设备可以在同一个本地以太网广播域中具有相同的“同一个”地址；否则会发生地址冲突。确保在私有企业网络中所有的

MAC 地址都是唯一的，这是一种非常好的做法。虽然 MAC 地址的设计应该是唯一的，但因为供应商的错误有可能导致产生重复的地址。当这一切发生时，必须更换网卡硬件或将 MAC 地址更改(例如，欺骗)到非冲突的替代地址。

EUI-48 到 EUI-64

MAC 地址是 48 位的，并已使用了数十年。一种类似的地址方案是 EUI-48。EUI 代表扩展的唯一标识符。对于 IEEE 802，原始的 48 位 MAC 地址方案采纳了原来的 Xerox 以太网地址方案。MAC 地址通常是用来识别网络硬件的，而 EUI 用来识别其他类型的硬件以及软件。

IEEE 认为 MAC-48 已经过时，并且也应该倾向于弃用 EUI-48。

现在也有从 EUI-48 向 EUI-64 转换过渡的举动。这是为未来在全世界范围普及 IPv6 做准备，也为网络设备和网络软件包的指数级数量增长准备，所有这一切都需要一个唯一的标识符。

MAC-48 和 EUI-48 地址可以用 EUI-64 进行表示。在 MAC-48 示例中，两个额外的字节 FF:FF 被添加到 OUT(头 3 个字节)和单独的网卡(最后 3 个字节)中间，例如 cc:cc:cc:FF:FF:ee:ee:ee。在 EUI-48 示例中，则增加两个额外的字节 FF:FE，例如 cc:cc:cc:FF:FE:ee:ee:ee。

在 OSI 模型的数据链路层(第 2 层)的协议中，你应该熟悉其中的两个协议：地址解析协议(ARP)和反向地址解析协议(RARP)。使用 ARP 将 IP 地址解析为 MAC 地址。使用 MAC 地址能够将某个网段(例如，通过集线器的线路)上的通信数据从源系统定向至目标系统。使用 RARP 将 MAC 地址解析为 IP 地址。

数据链路层包含两个子层：逻辑链路控制(Logical Link Control，LLC)子层和 MAC 子层。这些层的细节内容并不是 CISSP 考试的关键。

工作在第 2 层(数据链路层)的网络硬件设备包括交换机和桥。这些设备都支持基于 MAC 的路由通信。交换机从一个端口接收数据帧，并且根据目的 MAC 地址从另一个端口发送数据帧。MAC 目标地址用于确定数据帧是否要通过桥从一个网络传送至另一个网络。

3. 网络层

网络层(第 3 层)负责向数据中添加路由和寻址信息。网络层接收来自于传输层的数据段，并且通过添加信息创建数据包。数据包包括源 IP 地址和目的 IP 地址。

路由协议位于这一层，包括下列协议：

- 网络控制报文协议(Internet Control Message Protocol，ICMP)
- 路由信息协议(Routing Information Protocol，RIP)
- 开放式最短路径优先(Open Shortest Path First，OSPF)
- 边界网关协议(Border Gateway Protocol，BGP)
- 网络组管理协议(Internet Group Management Protocol，IGMP)
- 网际协议(IP)
- 网际协议安全(IPSec)
- 互联网分组交换协议(Internetwork Packet Exchange，IPX)
- 网络地址转换(Simple Key Management for Internet Protocol，NAT)
- 网络简单密钥管理协议(SKIP)

网络层负责提供路由或传送信息，但是不负责保证传输已进行验证(这个工作由传输层负责)。

网络层还管理着错误检测和节点数据通信(也就是通信控制)。

非 IP 协议

非 IP 协议是作为一种替代 IP 并工作在 OSI 的网络层的协议。在过去，非 IP 协议被广泛使用。然而，与 TCP/IP 的主导地位和成功相比，非 IP 协议已成为专用网络的范畴。三个最被认可的非 IP 协议是 IPX、AppleTalk 和 NetBUI。互联网分组交换协议(IPX)是 IPX/SPX 协议的常用套件(虽然没有严格的要求)的一部分，并使用于 20 世纪 90 年代的 Novell NetWare 网络中。AppleTalk 协议是一套由苹果公司开发并使用于 Macintosh 系统网络上的协议，最早版本于 1984 年初发布。在 2009 年，Mac OS X V10.6 发布后取消了苹果操作系统对 AppleTalk 的支持。IPX 和 AppleTalk 都可作为 IP 协议网关，在死区网络中实现 IP 方案(死区是指一个网段使用另一个网络层协议而不是 IP)。NetBIOS 扩展用户界面(NetBEUI，又名 NetBIOS 帧协议或 NBF)是最为广泛认知的一个微软协议，在 1985 年开发出来用于支持文件和打印机共享。微软已经通过将 NetBIOS 工作于 TCP/IP 上(NBT)，使得 NetBEUI 支持现代网络。这反过来又支持服务器消息块(Server Message Block，SMB)协议，也被称为通用互联网文件系统(Common Internet File System，CIFS)。作为低层协议，NetBEUI 已不再获得支持；只有 SMB 和 CIFS 仍在使用。

当非 IP 协议在私有网络中使用时，存在潜在的安全风险。因为非 IP 协议是罕见的，大多数防火墙无法对这些协议的数据包头、地址或有效载荷执行内容过滤。因此，当涉及非 IP 协议时，防火墙通常阻止所有或者允许所有。如果组织依赖于一个使用非 IP 协议的服务，那么可能不得冒着让防火墙通过所有的非 IP 协议的风险。这是在私有网络内存在非 IP 协议之间的网络段时主要考虑的问题。然而，非 IP 协议可以封装在 IP 协议中并在互联网上进行通信。在封装的情况下，IP 防火墙很少能够在这样的封装上执行内容过滤，并且因此安全性必须设置为允许所有或拒绝所有。

工作在第三层的网络层硬件设备包括路由器和桥式路由器。路由器基于速度、跳数、优先级等信息决定了数据包传输的最佳逻辑路径。路由器使用目的 IP 地址来指导数据包的传输。桥式路由器主要在第三层工作，不过必要时也会在第二层工作，这是一种先尝试路由、在失败时默认桥接的设备。

路由协议

路由协议分为两个主要类别：距离矢量和链路状态。距离矢量路由协议维护一个目的网络以及距离和方向的跳数列表(也就是到达目的地所经过的路由器数量)。链路状态路由协议维护一张所有已连接网络的拓扑图，并且使用这张拓扑图确定到达目的地的最短路径。距离矢量路由协议的常见例子包括 RIP、IGRP 和 BGP，而链路状态路由协议的常见例子则是 OSPF。

4. 传输层

传输层(第 4 层)负责管理连接的完整性并控制会话。传输层接收来自于会话层的 PDU(又名协议数据单元、数据包单元或数据负荷单元，是一个在网络层流经的包含信息和数据的容器)并将其转换为数据段。传输层控制网络上设备的寻址或引用方式，以及在节点(也被称为设备)之间建立通信连接，还有定义会话的规则。会话规则指定每个数据段中可以包含多少数据、如何验证传输数据的完整性、如何确定数据是否丢失。会话规则在握手过程中建立(请参考本章中的“传输层协议”中讨论的“TCP/IP 的 SYN/ACK 三步握手过程”)。

传输层在两台设备之间建立了一个逻辑连接，并且提供了能够确保数据传递的端到端传输服务。这一层包括针对分段、排序、错误检查、 数据流控制、错误纠正、复用和网络服务优化的机制。下

面列出了一些在传输层上运作的协议：

- 传输控制协议(TCP)
- 用户数据报协议(UDP)
- 顺序数据包交换(SPX)
- 安全套接字层(SSL)
- 传输层安全(TLS)

5. 会话层

会话层(第 5 层)负责在两台计算机之间建立、维护和终止通信会话。这一层管理对话模式或对话控制(单工、半双工、全双工)，并为分组和恢复建立检查点，以及重新传输上一次验证检查点以来失败或丢失的 PDU。下面列出了一些在会话层上运行的协议：

- 网络文件系统(NFS)
- 结构化查询语言(SQL)
- 远程过程调用(RPC)

通信会话能够以下列三种不同模式中的一种模式进行操作：

- **单工** 单向直接通信
- **半双工** 双向通信，但是每次只有一个方向可以发送数据
- **全双工** 双向通信，此时数据可以同时在两个方向上进行传输

6. 表示层

表示层(第 6 层)负责将从应用层接收的数据转换为遵从 OSI 模型的任何系统都能理解的格式。它向数据中强行添加通用的或标准的结构和格式化规则。表示层还负责加密和压缩。因此，它成为网络和应用程序之间的接口。通过确保数据格式能够被两个系统支持，表示层准许不同的应用程序通过网络交互。大多数文件或数据格式在这一层上出现，包括图像、视频、音频、文档、电子邮件、Web 页面和控制会话等格式。下面列出了表示层内存在的一些格式标准：

- 美国信息交换标准代码(ASCII)
- 扩充二进制编码的十进制交换码(EBCDIC)
- 标签图像文件格式(TIFF)
- 联合图像专家组(JPEG)
- 运动图像专家组(MPEG)
- 音乐设备数字接口(MIDI)

真实场景

怎样记忆如此多的层和协议

对于这 7 层和 50 多个协议，去记忆各层存在的协议可能十分困难。创建闪示卡是帮助记忆的一种方法。每张卡片的正面写下协议的名字，背面则写下层的名字。打乱卡片顺序后，将不同的协议堆放在表示不同层的位置。放置完所有协议以后，通过查看卡片背面的层名来检查记忆状况。重复这个过程，直至能够正确放置所有协议。

7. 应用层

应用层(第 7 层)负责将协议栈与用户的应用程序、网络服务或操作系统连接在一起。它准许应用程序与协议栈进行通信。应用层确定远程的通信方是否可用和可访问，还确保有足够的资源用于支持被请求的通信。

应用程序并不位于应用层内；相反，传输文件、交换信息和连接远程终端等任务所需的协议和服务都在这一层。很多应用专用的协议也在应用层内，例如下面这些协议：

- 超文本传输协议(HTTP)
- 文件传输协议(FTP)
- 行式打印机后台程序(LPD)
- 简单邮件传输协议(SMTP)
- 远程登录(Telnet)
- 普通文件传输协议(TFTP)
- 电子数据交换(EDI)
- 邮局协议第三版(POP3)
- 互联网消息访问协议(IMAP)
- 简单网络管理协议(SNMP)
- 网络新闻传输协议(NNTP)
- 安全远程过程调用(S-RPC)
- 安全电子交易(SET)

有一种网络设备(或服务)工作在应用层，名叫网关。但是，应用层网关是一种特定类型的组件。网关作为协议转换工具使用。例如，IP-to-IPX 网关接收采用 TCP/IP 协议的入站通信，并且在转换为 IPX/SPX 协议的通信后实现出站传输。应用防火墙也工作在这一层。其他网络设备或过滤软件也可以在这一层监测或修改数据流。

11.2　TCP/IP 模型

与 OSI 参考模型的 7 层相比较，TCP/IP 模型(也称为 DARPA 或 DOD 模型)仅由 4 层组成。TCP/IP 模型的 4 层为：应用层、传输层(也称为主机到主机层)、网际层(有时称为互联网层)和网络接入层(然而网络接口层和网络访问层都会被用到)。图 11.5 对 TCP/IP 模型的 4 层结构与 OSI 模型的 7 层结构进行了比较。TCP/IP 协议族是在 OSI 参考模型出现前被开发的。因为网络连接中已经部署了 TCP/IP 协议族，所以 OSI 参考模型的设计人员在设计时注意了确保 TCP/IP 协议族适用该模型的问题。

TCP/IP 模型的应用层对应于 OSI 模型的第 5、第 6 和第 7 层。TCP/IP 模型的主机到主机层对应于 OSI 模型的第 4 层。TCP/IP 模型的网际层对应于 OSI 模型的第 3 层。TCP/IP 模型的网络接入层对应于 OSI 模型的第 1 层和第 2 层。

后来，由于混淆、误解或偷懒，TCP/IP 模型层次的名字往往变得与 OSI 模型层次的名字相同。TCP/IP 模型的应用层已经借用了 OSI 模型的一个层次名，这是轻而易举的。TCP/IP 模型的主机到主机层有时被称为传输层(OSI 模型的第 4 层)。TCP/IP 模型的网际层有时被称为网络层(OSI 模型的第 3 层)。TCP/IP 模型的网络接入层有时被称为数据链路层(OSI 模型的第 2 层)。

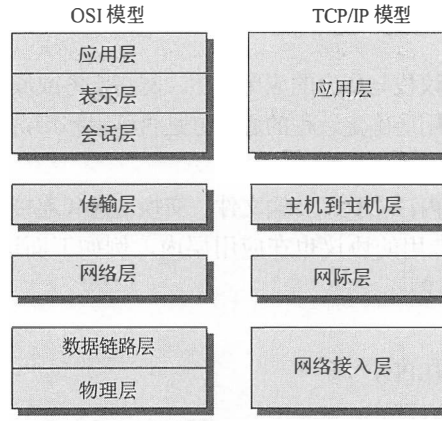


图 11.5　OSI 模型与 TCP/IP 模型的对比

提示：

由于 TCP/IP 模型层次的名字与 OSI 模型层次的名字可以交换使用，因此根据各种上下文确定所涉及的模型十分重要。除非专门指出，我们往往认定讨论的是 OSI 模型，这是因为它是最广泛使用的网络参考模型。

11.2.1　TCP/IP 协议族概述

TCP/IP 是使用最广泛的协议，但它并不是一个单独的协议，而是一个由许多单独的协议组成的协议栈(如图 11.6 所示)。TCP/IP 是一个基于开放式标准的、独立于平台的协议。然而，这既是它的优点，也是它的缺点。TCP/IP 几乎可以在所有可用的操作系统中找到，但是它耗用了相当数量的资源，并且由于其设计目的是便于使用而不是安全，因此容易遭到攻击。

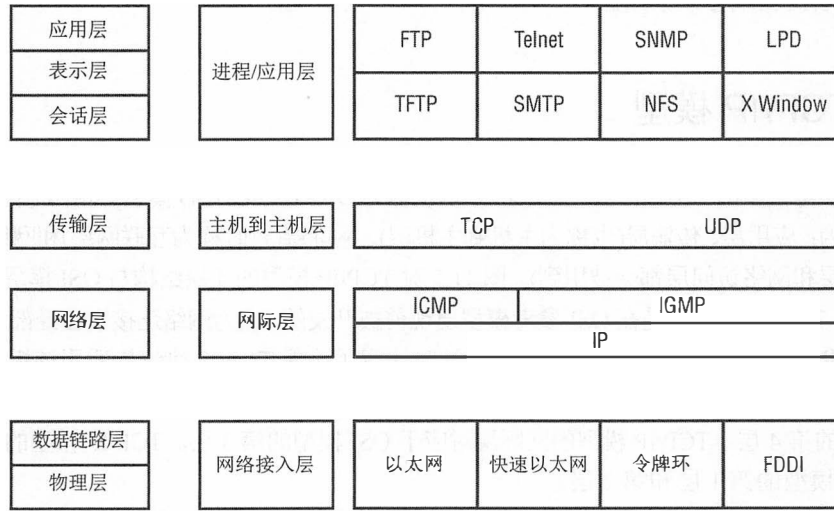


图 11.6　TCP/IP 模型的 4 个层次及其组成协议

TCP/IP 可以使用两个系统之间的 VPN 链接进行安全保护。VPN 链接通过加密增加了隐私性、机密性和身份认证，并且维护数据的完整性。用于建立 VPN 的协议包括点对点隧道协议(PPTP)、二

层隧道协议(L2TP)和网际协议安全(IPSec)。另一种提供协议级别安全性的方法是采用 TCP 包装。通过在用户 ID 或系统 ID 的基础上限制对端口和资源的访问，TCP 包装可以作为能够起到基本防火墙作用的应用程序。TCP 包装是基于端口的访问控制形式。

1. 传输层协议

TCP/IP 两个主要的传输层协议是 TCP 和 UDP。TCP 是一个面向连接的协议，而 UDP 是一个无连接的协议。当一个通信连接在两个系统之间建立起来时，它通过端口的使用完成操作。TCP 和 UDP 都有 65 536 个端口。因为端口号是 16 位二进制数，所以端口总数为 2^16 或 65 536，并且从 0 到 65 535 进行编号。端口(也被称为套接字)就是通信链接两端在传输数据时同意使用的地址号。端口允许单个 IP 地址能够支持多个同时发生的通信，并且每个端口都使用一个不同的端口号。

这些端口中的前 1024 个(端口 0~1023)被称为知名端口或服务端口，这是由于它们已经按照标准分配给所支持的服务。例如，端口 80 是用于 Web(HTTP)传输的标准端口，端口 23 是用于 Telnet 的标准端口，端口 25 是用于 SMTP 的标准端口。可以在“通用应用层协议”部分看到对考试有参考价值的端口列表。

端口 1024~49151 被称为已注册软件端口。这些端口具有注册到 IANA(www.iana.org)的一个或多个互联软件产品，目的是为试图连接其产品的客户端提供一个标准的端口编号系统。

因为通常被客户端随机使用为源端口，所以端口 49152~65535 被称为随机端口。在客户端和服务器之间协商初始服务或已注册端口之外的数据传输管道时，某些网络连接服务也会使用这些随机端口，例如通用 FTP 进行的数据传输。

端口编号

IANA 推荐 49 152 到 65 535 之间的端口用于动态或私有端口。然而不是所有的 OS 都遵从这个规定，例如：

- 伯克利软件分发(BSD)使用 1024 到 4999 之间的端口
- 许多 Linux 内核使用 32 768 到 61 000 之间的端口
- 微软公司 Windows Server 2003 及以前的版本使用 1025 到 5000 之间的端口
- Windows Vista、Windows 7 和 Windows Server 2008 使用 IANA 定义的端口范围
- FreeBSD 从 4.6 版本后，使用 IANA 建议的端口范围

传输控制协议在OSI模型的第4层(传输层)上运作。这个面向连接的协议能够支持全双工通信，并且使用了可靠的会话。TCP是面向连接的，这是因为它在两个系统之间使用握手过程建立一个通信会话。当握手过程完成时，就会建立能够在客户端和服务器之间支持数据传输的通信会话。这个三步骤的握手过程(见图11.7)如下所示：

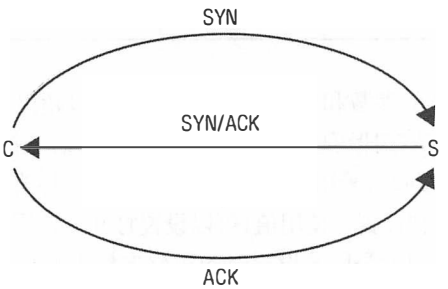


图 11.7　TCP 三次握手

(1) 客户端向服务器发送 SYN(同步)数据包。

(2) 服务器使用 SYN/ACK(同步和确认)数据包响应客户端。

(3) 客户端使用 ACK(确认)数据包响应服务器。

当通信会话结束时，可以使用两种方法断开 TCP 会话连接。第一种也是最常用的方法是使用 FIN(finish)数据包来代替 SYN 数据包。一旦所有的数据传输完毕，会话的每一方都会发送一个 FIN 标记包，触发对方通过一个 ACK 标记包进行确认。因此，它需要 4 个包来完成一个 TCP 会话。第二种方法是使用 RST(reset)数据包，此类数据包能够使会话立即和突然终止(请参看稍后章节讨论的 TCP 报头标记)。

一个 TCP 传输的信息段是有顺序的。在不管接收顺序的情况下，通过将接收的信息段重新排序为正常的排列顺序，接收者就能够重构最初的通信。TCP 会话的数据通信会使用一个确认信号定期进行验证。确认是由接收端反馈给发送端，通过设置 TCP 报头中的序列值来确认收到发送方发送窗口内最后发送的序列号。发送确认数据包之前传输的数据包数被称为传输窗口。数据流通过名为滑动窗口的机制受到控制。在发送确认信号之前，TCP 能够使用不同大小的窗口(也就是不同的传输数据包数)。较大的窗口允许更快的数据传输速度，但是只应当被用在数据丢失或损坏最小化的可靠连接上。在通信连接不可靠时，应当使用较小的窗口。在需要数据发送时，就应当利用 TCP。因为 TCP 会话的可靠性在使用时会有所变化，所以滑动窗口允许动态地改变这个大小。在发送窗口的所有数据包未接收完的情况下，不会发送任何确认数据包。当时间超时后，发送方将会重新发送整个传输窗口中的数据包。

与 UDP 协议相比，TCP 报头相对复杂。TCP 报头的长度为 20 到 60 字节，这个报头被分为若干部分或字段，表 11.1 详细描述了这些内容。

表 11.1 TCP 报头构造(按照从报头开始到结束的顺序)

比特数	字段
16	源端口
16	目的端口
32	序列号
4	数据偏移量
4	预留使用
8	标志(参看表 11.2)
16	窗口大小
16	校验和
16	紧急指针
可变	各种选项；大小必须是 32 比特的倍数

所有这些字段都具有独特的参数和要求，其中大多数字段超出了CISSP的考试范围。不过，你应当熟悉标志字段的细节。标志字段可以包含对一个或多个标志或控制位的指示项。这些标志指示TCP数据包的功能，并且请求接收方采用特定的方式进行响应。标志字段的长度为8比特，其中每个比特位置都表示单个标志或控制设置，使用值1可以设置打开，使用值0则可以设置关闭。有些情况下，可以一次性启用多个标志(也就是同时设置SYN和ACK标志时TCP三步握手中的第二个数据包)。表11.2详细说明了标志控制比特。

表 11.2　TCP 报头标记字段值

标志比特指示项	名字	描述
CWR	拥塞窗口大小	用于管理拥塞链接上的传输，参看 RFC 3168
ECE	ECN-Echo(明确拥塞通知)	用于管理拥塞链接上的传输，参看 RFC 3168
URG	紧急	指示紧急数据
ACK	确认	确认同步或关闭请求
PSH	推送	指示需要立即推送数据加以应用
RST	重置	导致 TCP 会话立即断开连接
SYN	同步	请求使用新的序列号进行同步
FIN	结束	请求对 TCP 会话的正常关闭

另一个重要的细节是，在 IP 报头协议字段中，表示 TCP 的值为 6(0x06)。协议字段值是在每个 IP 数据包中都能找到的标签或标志，它告知接收系统所接收数据包的类型。IP 报头的协议字段指示下一个封装协议的标识，也就是来自当前协议层的载荷包含的协议(例如，ICMP 或 IGMP)或上一层的协议(例如，TCP 或 UDP)。想象一下从深冻冰箱取出用肉店包装纸包装的未知肉数据包上的标签。如果没有标签，那么不得不打开肉数据包来查看包裹的是什么肉。但是，如果有标签，那么就可以快速查找或过滤自己感兴趣的肉制品。要想了解其他协议字段值，访问 www.iana.org/assignments/protocol_numbers。

不熟练的攻击者纠缠真正的安全人员

这是记住 8 个 TCP 报头中至少最后 6 个标志位的好方法。第一和第二个标志位(CWR 和 ECE)现在很少使用，因此通常被忽略/忽视。然而，最后的 6 个标志位(URG、ACK、PHS、RST、SYN 和 FIN)在今天仍很常见并被广泛使用。

请记住，这 8 个标志位是 8 个二进制位置(即一个字节)，可以用任何十六进制或二进制格式显示。例如，0x12 是字节 00010010 的十六进制表示。这个特定字节的排列表明第 4 个和第 7 个标志位被启用。通过标志位的设计(使用每个标志位一个字母，留下 CWR 和 ECE 并用 XX 取代它们)，XXUAPRSF 是 000A00S0，或设置 SYN/ACK 标志位。注意：在 TCP 报头标志位字节的十六进制表示通常在数据包捕获工具的原始数据显示栏显示，如 Wireshark，在偏移位置 0x2F。这是一个基于标准的以太网 II 型的报头，是一个标准的 20 字节的 IP 头，也是一个标准的 TCP 报头。

可以通过使用短语“不熟练的攻击者纠缠真正的安全人员”来记住这个标志的顺序，其中每个单词的第一个字母对应标志位 3 到 8 的第一个字母。

真实场景

协议发现

在任何时候，典型的 TCP/IP 网络都会使用数百种协议。可以使用嗅探器来发现当前网络中所应用的协议。但是，在使用嗅探器之前，必须确保具有适当的特权或授权。如果没有获得批准，那么使用嗅探器就会被视为像窃听未受保护的网络通信一样的安全违规行为。如果在工作中不能获得特权，那么可以在家庭网络上进行尝试。首先，下载和安装嗅探器，例如 Wireshark。随后，使用嗅探器监控网络上的活动，看看在家庭网络上能够发现多少被应用的协议(也就是 TCP/IP 的子协议)。

使用嗅探器的另一个步骤是分析被捕获数据包的内容。选择一些不同的协议数据包，并且查看它们的报头。找到 TCP、ICMP、ARP 和 UDP 数据包，比较各自报头的内容。尝试定位这些协议使用的特殊标记或字段编码。你可能会发现在协议中存在许多自己以前不知道的信息。

用户数据报协议(UDP)也在 OSI 模型的第 4 层(传输层)上运作，它是一种无连接的、“尽力而为的”通信协议。UDP 不提供错误检测或纠正，不使用序列，不使用流量控制机制，不使用预先建立的会话，并且被认为是不可靠的。UDP 具有极低的系统开销，因此能够快速传输数据。不过，只有在数据传输并非绝对必要时，我们才会使用 UDP。用于音频和/或视频的实时或流式通信经常会使用 UDP。在 IP 报头协议字段中，表示 UDP 的值为 17(0x11)。

前面曾经提到过，与 TCP 报头相比，UDP 报头相对简单。UDP 报头的长度为 8 个字节(64 位)。UDP 头被分为 4 个部分或字段(每个 16 位长)：

- 源端口
- 目的端口
- 报文长度
- 校验和

2. 网络层协议和 IP 网络基础

TCP/IP 协议族中的另一个重要协议在 OSI 模型的网络层上运作，这种协议就是网际层协议(IP)。IP 为数据包提供了路由寻址。路由寻址是全球性互联网通信的基础，这是因为它提供了身份标识手段并规定了传输路径。与 UDP 类似，IP 是无连接的、不可靠的数据报服务。IP 不保证传送数据包或以正确顺序传送数据包，并且不保证只进行一次传送。因此，必须在 IP 上使用 TCP，从而获取可靠的和受控的通信会话。

IPv4 与 IPv6

IPv4 是全世界范围内最广泛应用的网络协议版本。不过，新版本 IPv6 主要替代和改善了网络寻址和路由。IPv4 使用 32 位的寻址模式，而 IPv6 则使用 128 位进行寻址。IPv6 提供了许多在 IPv4 中不可用的新功能。IPv6 的一些新功能包括作用域地址、自动配置和 QoS 优先值。作用域地址使管理员能够进行分组以及随后阻止或允许对网络服务(例如，文件服务器或打印)的访问。自动配置排除了对 DHCP 和 NAT 的需求。QoS 优先值允许基于优先顺序内容来管理通信。

2000 年以后发布的大多数操作系统既可以直接支持也可以通过插件支持 IPv6。但是，人们接受 IPv6 的速度缓慢。大多数 IPv6 网络目前都部署在大公司、研究实验室或大学内。

IP 等级

任何安全专业人员都必须了解 IP 寻址和 IP 等级的基础知识。如果对 IP 寻址、子网划分、等级以及其他相关主题还比较陌生，那么就需要花费一定的时间进行相应的学习。表 11.3 和表 11.4 概述了 IP 等级与默认子网的关键细节。完整的 A 类子网可以支持 16 777 214 台主机，完整的 B 类子网可以支持 65 534 台主机，而完整的 C 类子网则可以支持 254 台主机。D 类子网被用于多播，E 类子网被保留给将来使用。

表 11.3　IP 等级

等级	开头的二进制数字	第一个字节的十进制范围
A	0	1~126
B	10	128~191
C	110	192~223
D	1110	224~239
E	1111	240~255

表 11.4　IP 等级默认的子网掩码

等级	默认的子网掩码	相当的 CIDR
A	255.0.0.0	/8
B	255.255.0.0	/16
C	255.255.255.0	/24

注意，全部的 A 类地址中，整个 127 段被用来留给环路地址，尽管实际中只使用了一个环路地址。

子网划分的另一个选项是使用无类域间路由选择(Classless Inter-Domain Routing，CIDR)。CIDR 没有使用采用完整点分十进制表示法的子网掩码，而是使用掩码位。因此，CIDR 通过斜线被添加在 IP 地址之后，例如，使用 172.16.1.1/16 代替 255.255.0.0。与传统的子网掩码技术相比，CIDR 的一个重要优点是能够将多个不相邻的地址集组合在单个子网内。例如，我们可以将若干 C 类子网组合为一个更大的子网分组。如果对 CIDR 感兴趣，那么可以在维基百科站点上通过查看 CIDR 文章来获得详细信息，或者访问 IETF 关于 CIDR 的 RFC 文档(http://tools.ietf.org/html/rfc4632)。

ICMP 和 IGMP 是运行于 OSI 模型网络层上的其他协议。

ICMP　网络控制报文协议(ICMP)用于确定某个网络或特定链接的健康状况。ping、traceroute、pathping 以及其他网络管理工具都利用了 ICMP。ping 实用程序利用了 ICMP 的回应(echo)命令数据包，并且使用它们对远程系统进行试探。因此，可以使用 ping 来确定远程系统是否联机、远程系统是否正常响应、中间系统是否支持通信以及支持通信的中间系统的性能效率级别。ping 实用程序包括重定向功能，这个功能允许将回应响应发送至与原始系统不同的目的地。

遗憾的是，ICMP 的功能往往被各种基于带宽的拒绝服务攻击所利用，例如，ping of death 攻击、smurf攻击和 ping洪泛攻击。这个事实已经形成今天的网络如何处理 ICMP 流量，导致许多使用 ICMP 的网络限制或至少限制，其吞吐率。ping of death 攻击发送一个畸形的大于 65 535 字节(大于最大 IPv4 数据包大小)的数据包给一台计算机并试图让其崩溃。smurf 攻击通过欺骗广播 ping 对目标网络产生巨大的流量，ping 数据包泛洪攻击是一个基本的拒绝服务(DoS)攻击，它消耗目标可用的所有带宽。

你应当认识到与 ICMP 相关的一些重要细节。首先，IP 报头协议字段中表示 ICMP 的值为 1(0x01)。其次，ICMP 报头中的类型字段定义了 ICMP 载荷内所包含报文的类型或目的。可定义的类型超过 40 种，但是只有 7 种是常用的类型(参看表 11.5)。可以在 www.iana.org/assignments/icmp-parameters 站点上查看 ICMP 类型字段值的完整列表。值得注意的是，列出的许多类型可能也支持编码。编码只是额外的数据参数，这种参数能够提供与 ICMP 报文载荷的功能或目的相关的更多细节。一个事件会导致一个 ICMP 响应的一个例子是，当尝试连接到 UDP 服务端口时，服务和端口不

在目标服务器上实际使用；这会导致一个 ICMP 类型 3 响应被发送回原点。由于 UDP 没有手段发送错误，协议栈将切换使用 ICMP 完成该任务。

表 11.5 常用的 ICMP 类型字段值

类型	功能
0	回声应答
3	目的地不可到达
5	重定向
8	回声请求
9	路由器通告
10	路由器请求
11	超时

IGMP 网络组管理协议(IGMP)允许系统支持多播。多播是将数据传输给多个特定的接收者(RFC 1112 讨论了执行 IGMP 多播操作的要求)。IP 主机使用 IGMP 注册其动态的多播组成员。已连接的路由器也使用 IGMP 来发现这些组。通过使用 IGMP 多播操作，服务器在一开始就可以只传输单个数据信号，从而不必为每个预定的接收者分别传输数据信号。借助于 IGMP，如果数据到达预定接收者的路径有分叉，那么最初的单个信号就会在路由器处被复用。IP 报头协议字段中表示 IGMP 的值为 2(0x02)。

ARP 与反向 ARP 对于逻辑和物理寻址模式的互操作性来说，地址解析协议(ARP)与反向地址解析协议(RARP)是必不可少的。ARP 用于将 IP 地址(用于逻辑寻址的 32 位二进制数)解析为介质访问控制(MAC)地址(用于物理寻址的 48 位二进制数)——或者 EUI-48——甚至 EUI-64。通过使用 MAC 地址，某个网段上(例如，通过一个集线器的线缆)的通信从源系统定向至目的系统。RARP 用于将 MAC 地址解析为 IP 地址。

ARP 和 RARP 的运作都需要使用缓存和广播。将 IP 地址解析为 MAC 地址(或者将 MAC 地址解析为 IP 地址)的第一个步骤是查看本地 ARP 缓存。如果本地 ARP 缓存中已经存在所需的信息，那么就会使用这些信息。有时，使用名为 ARP 缓存污染的技术会滥用这种活动，此时攻击者会在 ARP 缓存中插入伪造的信息。如果 ARP 缓存中不存在所需的信息，那么就会传输一个采用广播形式的 ARP 请求。如果被查询地址的所有者位于本地子网内，那么它就能够响应所需的信息。如果被查询地址的所有者不在本地子网内，那么系统会默认使用默认的网关来传输通信数据。随后，默认的网关(也就是路由器)需要执行自己的 ARP 或 RARP 进程。

3. 常见的应用层协议

在 TCP/IP 模型的应用层(包括 OSI 模型的会话层、表示层和应用层)上，驻留着许多特定于应用或服务的协议。对于 CISSP 考试来说，了解这些协议的基础知识及相关的服务端口十分重要：

远程登录(Telnet)，TCP 端口 23 这是一个终端仿真网络应用，支持能够执行命令和运行应用程序的远程连通性，但是不支持文件传输。

文件传输协议(FTP)，TCP 端口 20 和 21 这是一个支持文件交换的网络应用，文件交换要求进行匿名的或特定的身份认证。

普通文件传输协议(TFTP)，UDP 端口 69 这是一个支持文件交换的网络应用，文件交换不要

求进行身份认证。

简单邮件传输协议(SMTP)，TCP 端口 25　这个协议用于从客户端向邮件服务器以及从一个邮件服务器向另一个邮件服务器传送邮件。

邮局协议(POP3)，TCP 端口 110　这个协议用于将邮件服务器收件箱中的邮件传送至邮件客户端。

互联网消息访问协议(IMAP)，TCP 端口 143　这个协议用于将邮件服务器收件箱中的邮件传输至邮件客户端。IMAP 比 POP3 更安全，并且能够从邮件服务器中取出邮件头，在不必先下载至本地客户端的情况下就可以直接从邮件服务器中删除邮件。

动态主机配置协议(DHCP)，UDP 端口 67 和 68　DHCP 将端口 67 用于服务器点对点响应，将端口 68 用于客户端请求广播。在系统启动时，DHCP 用于为系统指派 TCP/IP 配置设置。DHCP 提供了对网络寻址的集中化控制。

超文本传输协议(HTTP)，TCP 端口 80　这个协议用于从 Web 服务器向 Web 浏览器传送 Web 页面元素。

安全套接字层(SSL)，TCP 端口 443　这是一个在会话层上运作的、像 VPN 一样的安全协议。SSL 原本设计用于支持安全的 Web 通信(HTTPS)，不过它能够保护任何应用层协议通信的安全。

行式打印后台程序(LPD)，TCP 端口 515　这是一个用于管理打印作业以及向打印机发送打印作业的网络服务。

X 视窗(X Window)，TCP 端口 6000~6063　这是一个用于命令行操作系统的 GUI API。

引导协议(BootP)/动态主机配置协议(DHCP)，UDP 端口 67 和 68　这个协议用于通过自动分配 IP 配置以及下载基本的 OS 元素来连接无盘工作站和网络。BootP 是 DHCP 的前身。

网络文件系统(NFS)，TCP端口2049　这是一个用于支持在不同系统之间共享文件的网络服务。

简单网络管理协议(SNMP)，UDP 端口 161(UDP 端口 162 用于跟踪信息)　这个网络服务被用于通过从中央监控站轮询监控设备来收集网络健康和状况信息。

11.2.2　分层协议的应用

正如你从前面的章节中看到的，TCP/IP 协议套件包括几十个跨越不同协议栈层的单独协议。因此，TCP/IP 是一个多层协议。TCP/IP 的多层设计有许多好处，特别是关系到它的封装机制。例如，Web 服务器和 Web 浏览器之间的通信工作在一个典型的网络连接上，HTTP 封装在 TCP 中，TCP 又封装在 IP 中，而 IP 又封装在以太网中。这个封装可以用以下方式进行展示：

```
[ Ethernet [ IP [ TCP [ HTTP ] ] ] ]
```

然而，这不是 TCP/IP 封装支持的程度。除此之外，它也可以添加额外的封装层。例如，添加 SSL/TLS 加密通信会使得 HTTP 和 TCP 之间插入一种新的封装：

```
[ Ethernet [ IP [ TCP [ SSL [ HTTP ] ] ] ] ]
```

同理，又可以用诸如 IPSec 的网络层加密进行进一步封装：

```
[ Ethernet [ IPSec [ IP [ TCP [ SSL [ HTTP ] ] ] ] ] ]
```

然而，封装并不总是用于良好的初衷。有许多隐蔽的信道通信机制，在一个授权的协议中使用封装隐藏或隔离另一个未授权的协议。例如，如果一个网络阻止 FTP 但允许 HTTP，那么利用诸如

HTTP 隧道的工具就可以用来绕过这个限制。这导致出现以下所示的封装结构：

```
[ Ethernet [ IP [ TCP [ HTTP [ FTP ] ] ] ] ]
```

通常情况下，HTTP 带有与自己 Web 相关的载荷，但通过 HTTP 隧道工具，标准的有效载荷被另一个协议取代。这种错误封装甚至可以在较低的协议栈中出现。例如，ICMP 通常用于网络健康测试而不是一般通信。然而，随着诸如 Loki 的出现，ICMP 被转换为支持 TCP 通信的隧道协议。Loki 的封装结构如下：

```
[ Ethernet [ IP [ ICMP [ TCP [ HTTP ] ] ] ] ]
```

另一个关注的领域是，对无界封装的支持将带来在 VLAN 之间跳跃的能力。VLAN 通过逻辑标签分离实现网络分段。这种被称为跳跃攻击的攻击通过创建二次封装 IEEE 802.1Q VLAN 标签的方式来进行：

```
[ Ethernet [ VLAN1 [ VLAN2 [ IP [ TCP [ HTTP ] ] ] ] ] ]
```

通过这样的两次封装，第一次遇到的交换机将剥离第一个 VLAN 标签，接下来的交换机将被内部 VLAN 标签欺骗并将流量转移到其他 VLAN 中。

多层协议提供以下好处：

- 可以在更高层使用更为广泛的协议
- 封装可以和不同的层进行合作
- 在更为复杂的网络中支持灵活性和弹性

多层协议有以下几个缺点：

- 允许隐蔽信道
- 过滤机制可被绕行
- 逻辑上实现的网络段边界可以被逾越

DNP3

DNP3(分布式网络协议)是CISSP CBK专门提出的与多层协议相关的内容。DNP3主要用于电力和水利行业的使用和管理，主要用来支持数据采集系统和系统控制设备之间的通信，包含子站计算机、RTU(远程终端单元，通过嵌入式微处理器来控制设备)、IED(智能电子设备)和SCADA主站(即控制中心)。DNP3是一个开放的公共标准。DNP3是一个多层协议且功能类似于TCP/IP，因为它有链路、传输和传输层。关于DNP3的更多细节，请查看http://www.dnp.org/AboutUs/DNP3%20Primer%20Rev%20A.pdf。

11.2.3 TCP/IP 的脆弱性

TCP/IP 的脆弱性有很多。在各种操作系统中，不正确地实现 TCP/IP 堆栈很容易遭受缓冲区溢出攻击、SYN 泛洪攻击、各种 DoS 攻击、碎片攻击、过长数据包攻击、欺骗攻击、中间人攻击、劫持攻击以及编码错误攻击。

除了这些侵入式攻击以外，TCP/IP(以及大多数协议)还常常遭受通过监控或嗅探进行的被动式攻击。网络监控是对信息流量模式进行监控，从而获得网络相关信息的行为。数据包嗅探是从网络中捕获数据包并期望从信息数据包内容中抽取出有用信息的行为。有效的数据包嗅探器可以抽取出用户名、密码、电子邮件地址、加密密钥、信用卡号、IP 地址和系统名等信息。

数据包嗅探和其他攻击在第 13 章会有进一步的讨论。

11.2.4　域名解析

寻址和命名操作是使网络通信成为可能的重要组成部分。如果没有寻址方案，那么互联的计算机就无法被区分或指定通信的目的地。同样，如果没有命名方案，那么人们就不得不凭借记忆和依赖编号系统来识别计算机。例如，记忆“Google.com”比记忆“64.233.187.99”容易得多。因此，绝大多数命名方案是为人制定的，而不是为计算机制定的。

理解在基于 TCP/IP 的网络中使用的寻址和命名的基本概念相当重要。我们应当意识到三个不同的层。它们在这里以相反顺序进行罗列，这是因为这三层是最为基础的。

- 第三层或底层，是 MAC 地址层。MAC 地址或硬件地址是“永久”的物理地址。
- 第二层或中间层，是 IP 地址层。IP 地址是在 MAC 地址上“临时”赋予的逻辑地址。
- 最顶层是域名。域名或计算机名是在 IP 地址上“临时”赋予的友好转换约定。

“永久”与“临时”地址

为这两个形容词加上引号的原因是它们并不完全准确。MAC 地址被设计为永久的物理地址。但是，某些 NIC 支持 MAC 地址变化，而且大多数现代操作系统(包括 Windows 和 Linux)也能够做到这一点。NIC 支持 MAC 地址变化时，变化在硬件上发生。操作系统支持 MAC 地址变化时，变化只在内存中发生，不过对其他所有网络实体来说，就像硬件发生了变化一样。

因为只是逻辑的，并且 DHCP 或管理员能够随时对其进行修改，所以 IP 地址是临时的。然而，现实中还存在一些系统静态分配 IP 地址的例子。同样，计算机名或 DNS 名也是逻辑的，因此能够被管理员更改。

命名和寻址系统为每个网络连接组件授予其所需的信息，并使这些系统尽可能简单地使用这些信息。人们得到人性化的域名，网络连接协议得到与路由器友好的 IP 地址，网络接口则得到物理地址。不过，为了允许彼此之间的互操作性，上述三种模式必须被链接在一起。因此，人们开发了域名系统(DNS)和 ARP/RARP 系统。DNS 将人性化的域名解析为相应的 IP 地址。随后，ARP 将 IP 地址解析为相应的 MAC 地址。这两种解析操作都具有自己的逆过程，也就是 DNS 逆向查找和 RARP(请参看本章前面的“ARP 和反向 ARP”部分)。

阅读更多的 DNS 内容

关于对 DNS 最新的阐述，包括其操作、已知问题以及 Dan Kaminski 漏洞，请访问“An Illustrated Guide to theKaminsky DNS Vulnerability”(http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html)。

有关 DNS 的描述，尤其是对抗 Kaminski 漏洞，请访问 www.dnssec.net。

11.3　汇聚协议

汇聚协议是专业或专有协议和标准协议的融合，例如 TCP/IP 协议。汇聚协议的主要好处是使用现有的 TCP/IP 网络基础设施支持特殊或专有主机而不用特殊部署修改后的网络硬件。这能有效地节

约成本。然而，作为专有协议的实现，并不是所有的汇聚协议提供相同的吞吐量或可靠性。这里描述了一些汇聚协议的常见例子：

以太网光纤通道(FCoE) 光纤通道是网络存储解决方案(存储区域网络(SAN)或网络附加存储(NAS))的一种形式，允许高达 16Gbps 的上行高速文件传输。设计目的是要在光纤线缆上运行，之后支持在铜电缆上运行，并提供更便宜的选择。光纤通道通常需要自己专用的基础设施(单独的线缆)。然而，以太网光纤通道(FCoE)可以用来支持在现有的网络基础设施上使用。FCoE 用来在以太网网络上封装光纤通道通信，通常需要 10 Gbps 以太网以便支持光纤通道协议。通过这一技术，光纤通道作为网络层或 OSI 第三层协议，替换 IP 作为标准的以太网网络负载。

MPLS(多协议标签交换) MPLS(多协议标签交换)是一种高通过、高性能的网络技术，它将数据在网络中以基于最短路径的标签而不是更长的网络地址进行传输。这种技术节省了传统的基于 IP 的路由过程，这个过程可能相当复杂。此外，设计 MPLS 的目的是通过封装处理广泛的协议。这样，网络就不局限于 TCP/IP 和兼容的协议。MPLS 支持许多其他网络技术的使用，包括 T1/E1、ATM、帧中继、SONET 和 DSL。

互联网小型计算机系统接口(iSCSI) 互联网小型计算机系统接口(iSCSI)是一个基于 IP 的网络存储标准。这项技术可以用来支持位置独立的文件存储、传输，以及对局域网、广域网的检索，或者公共互联网连接。iSCSI 通常被认为是光纤通道的一种低成本替代方案。

IP 语音(VoIP) IP 语音(VoIP)是用于在 TCP/IP 网络上传输语音和/或数据的一种隧道机制。因为 VoIP 往往更便宜并提供了广泛的功能和选项，它已经取代或具备取代 PSTN 的潜力。VoIP 可以用在计算机网络上，作为传统电话和移动设备的替换。而且，VoIP 还能够支持视频和数据传输，让视频会议和项目远程协作成为可能。VoIP 以商用和开源的方式被使用。一些 VoIP 解决方案需要专门的硬件来代替传统的手机/基站，或允许这些设备连接到 VoIP 系统并使用原有功能。某些 VoIP 解决方案是软件方式，例如 Skype，它允许用户使用现有的扬声器、麦克风或耳机来代替传统的电话听筒。其他更多是基于硬件方式，如 magicJack，它允许使得现有的 PSTN 电话设备插入 USB 适配器，利用互联网进行 VoIP 的使用。通常，VoIP 到 VoIP 通话是免费的(假设采用相同或兼容的 VoIP 技术)，而 VoIP 与陆地线路的通话通常以每分钟费用的方式进行计费。

软件定义网络(SDN) 软件定义网络(SDN)是一种独特的对网络进行操作、设计和管理的方法。该概念基于这样一个理论，即传统网络设备配置的复杂性(如路由器和交换机)经常强迫组织依附于某单一的设备厂商(如思科)，这不仅限制了网络的灵活性，而且难以应对不断变化的物理和商业条件。SDN 旨在把控制层(即网络服务的数据传输管理)和基础设施层(即硬件和基于硬件的设置)分离。此外，它还移除了 IP 寻址、子网、路由以及诸如此类从需求到被固化程序编码或解释的传统网络概念。

SDN 提供了一种直接从中央位置进行网络设计的新方法，它是灵活的、与厂商无关的并且基于开放标准。利用 SDN 使得组织可以不从单一供应商采购设备。相反，它允许组织混合和匹配需要的硬件，如选择最划算的或最高通过性能的设备而不管供应商是谁。之后，通过集中管理接口进行配置和管理硬件控制。此外，在硬件上的应用设置可以根据需要动态地进行变更和调整。

另一种关于 SDN 的思考方式是其有效的网络虚拟化。它允许数据传输路径、通信决策树以及流量控制在 SDN 控制层是虚拟化的，而不是在每个设备的基础硬件上进行处理。

11.4　内容分发网络

内容分发网络(CDN)或内容转发网络，是资源服务的集合，被部署在互联网的许多数据中心以提供低延迟、高性能和所承载内容的高可用性。CDN 通过分布式数据主机提供客户所需的多媒体性能质量，而不是将媒体内容存储在单一位置的单一主机上，并向互联网的其他地方进行内容分发。这是一种地理和逻辑负载均衡的结果。在所有资源发起请求的负荷下，没有哪个服务器或群集服务器会变得有压力，且托管服务器变得更接近于发起请求的客户。总的结果是较低的延迟和更高质量的吞吐量。目前有很多 CDN 服务提供商，包括 CloudFlare、Akamai、Amazon CloudFront、CacheFly 和 Level 3 Communication。

大多数CDN关注于服务器的物理分布，然而基于客户的CDN也是可能的。这通常被称为P2P(点对点)。最被广泛认可的 P2P CDN 是 BitTorrent。

11.5　无线网络

无线网络因为易于部署和相对低廉的成本，所以成为一种连接企业和家庭系统的流行方法。它将网络变得比以往任何时候都更灵活。工作站和便携式系统不再绑在一根电缆上，它们可以在部署无线接入点的信号范围内自由漫游。然而，随着这种自由的到来，带来了额外的漏洞。从历史上看，无线网络已经相当不安全了，主要是因为最终用户和组织缺乏知识以及设备制造商提供的不安全默认配置。无线网络正遭受任何有线网络中存在的同样的漏洞、威胁和风险，此外还增加了远程窃听、数据包嗅探以及新的 DoS 和入侵形式。正确地管理无线网络以提供可靠的访问性及安全性并不总是一个简单或直接的主题。本节将探讨各种无线安全问题。

数据泄露是数据通过电磁信号进行传输。几乎所有计算机或网络活动都会遭遇某种形式的数据泄露。然而，这个词经常用于指多余的泄露或是由于泄露而导致的数据风险。

当电子移动时就会发生泄露。电子运动产生电磁场。如果能读到电磁场的话，可以在其他地方再次创造，以便复制电子流。如果原来的电子流被用来通信数据，那么重新创建的电子流也可以重新创建原始数据。这种形式的电子窃听听起来像科幻小说，但却是科学事实。美国政府从 20 世纪 50 年代一直以来都在 TEMPEST 项目下研究电磁泄漏安全。

防止窃听和数据窃取需要多方面的努力。首先，必须保持对所有电子设备的物理访问控制。其次，未经授权的人员仍然可能接近或进行物理访问，必须使用屏蔽设备和屏蔽介质。最后，应该使用安全的加密协议发送任何敏感数据。

11.5.1　保护无线接入点

无线覆盖单元是在物理环境中无线设备可以接入到无线接入点的区域。无线覆盖单元可导致环境中的安全泄露，允许攻击者轻易连接到无线网络。应该调整无线接入点的强度，以确保用户接入认证的最大化和攻击者接入的最小化。做这些工作需要单独的无线接入点的独特位置、外罩防护以及噪声屏蔽。

802.11 是IEEE下无线网络通信的标准。各种版本(技术上称为修订)已经在无线网络硬件上得到了应用，这些标准包括 802.11a、802.11b、802.11g和 802.11n。802.11X有时用来泛指整个协议族。

然而，推荐用 802.11 进行命名，因为 802.11x容易和 802.1x混淆，802.1x是一个与无线无关的认证技术。每一个 802.11 技术的修订版本都要比之前的稍微好些——2Mbps、11Mbps、54Mbps和 200+Mbps，表 11.6 描述了各个版本。802.11 标准还定义了有线等效保密(WEP)，它在无线通信时提供防窃听保护。802.11b、802.11g和 802.11n都使用同样的频率。此外，它们保持向后兼容性。

表 11.6　802.11 无线网络修订版

802.11 及修订版	速率	频率
802.11	2Mbps	2.4GHz
802.11a	54Mbps	5GHz
802.11b	11Mbps	2.4GHz
802.11g	54Mbps	2.4GHz
802.11n	200+Mbps	2.4GHz 或 5GHz
802.11ac	1Gbps	5GHz

部署无线网络时，应该部署无线接入点并使用基础设施模式而不是点对点模式。点对点模式意味着任意两个无线网络设备，包括两个无线网络接口卡(NIC)，能在不需要中心控制认证的情况下进行通信。基础设施模式意味着需要一个无线接入点，系统上的无线网卡之间不能互联。无线接入点的无线网络接入控制应该进行强化。

基础设施模式的概念有几个变化模式，包括独立模式、有线扩展模式、企业扩展模式和桥接模式。独立模式指无线接入点连接无线客户端但是没有提供任何有线资源。无线接入点服务就像一个无线交换机。有线扩展模式指无线接入点连接无线客户端到有线网络。企业扩展模式指多个无线接入点(WAP)用来连接巨大的物理区域到同一个有线网络。每一个无线接入点都使用相同的扩展服务集标识符(ESSID)，因此客户端能在更换区域时保持网络连接，即使它们的无线网卡从一个无线接入点到另一个无线接入点改变关联。桥接模式发生在当无线连接用于连接两个有线网络的情况。这通常发生在有线桥接不方便时，例如，在地面或建筑物之间连接网络，使用专用的无线桥接器。

注意：

SSID(服务集标识符)通常被滥用于表示无线网络的名称。技术上有两种类型的 SSID: 扩展服务集标识符(ESSID)和基本服务集标识符(BSSID)。ESSID 是使用无线基站或 WAP 的无线网络名称。BSSID 是使用 ad hoc 或点对点模式(未使用无线基站或 WAP)时无线网络的名称。然而，在基础设施模式下运行时，BSSID 是拥有 ESSID 基站主机的 MAC 地址，用于区分扩展无线网络中的多个基站。

真实场景

无线信道

对指定频率的无线信号的细分称为信道。可以把它想象为同一条高速公路上不同的车道。在美国有 11 个频道，在欧洲有 13 个频道，而在日本有 17 个频道。这样的差异源于当地法律对频率的管理规范(可参考美国联邦通信委员会的国际版本)。

无线客户端和接入点之间的无线通信发生在单一的信道上。但是，当两个或两个以上的接入点在物理位置上比较接近时，其中一个信道上的信号可以干扰另一个信道上的信号。避免这一情况发生的方法是设置物理上接近接入点的信道，以尽可能地减少信道重叠干扰。例如，如果一个建筑有 4 个接入点并设置在沿着建筑物长度的一条线上，信道设置可能是 1、11、1 和 11。然而，如果建筑物是广场且每一个角落放置一个接入点，则信道设置可能需要 1、4、8 和 11。可以想象信号在单一的信道中就像是在高速公路车道上的宽负载卡车。如果每个车道中都有大型重卡车，那么在这些车道中同时通行卡车就存在危险。同样，在相邻信道中的无线信号会互相干扰。

11.5.2　保护 SSID

为无无线网络分配服务集标识符(SSID，无论是 BSSID 还是 ESSID)是为了区分是这个无线网络还是另一个无线网络。如果多个基站或无线接入点都参与同一个无线网络，则定义一个扩展服务集标识符(ESSID)。SSID 类似于工作组的名称。如果无线客户端知道 SSID，它们就可以通过配置无线网卡和对应的 WAP 进行通信。知晓 SSID 并不总是意味着同意登录，不过，由于 WAP 可以使用众多的安全功能，从而阻止不必要的访问。默认 SSID 由厂商进行定义。由于这些默认 SSID 是众所周知的，因此标准的安全实践表明 SSID 在部署之前应该进行变更。

SSID 广播由 WAP 通过信标帧进行特殊传输。它允许在无线覆盖范围内的任意无线网卡尽可能简单地进行无线网络连接。然而，这个默认的 SSID 广播应禁用以便保持无线网络的私密性。即便如此，攻击者仍然可以用无线嗅探器借由无线客户端和 WAP 之间的传输发现 SSID。因此，禁用 SSID 广播并不是一个真正的安全机制。相反，应使用 WPA2 作为一个可靠的身份认证和加密解决方案而不是试图隐藏无线网络的存在。

关闭 SSID 广播

无线网络通常通过称为信标帧的特殊数据包来宣告它们的 SSID。当 SSID 广播时，任何拥有自动检测和连接功能的设备不仅可以看到网络，也可以开始与网络进行连接。网络管理员可以选择禁用 SSID 广播以便隐藏自己的网络，从而免受未经授权人员的访问。然而，SSID 仍然需要直接从基站进行发送，使用无线数据包嗅探器的人仍然可以发现。因此，如果网络不供公众使用，则 SSID 应被禁用，但需要意识到隐藏 SSID 不是真正的安全机制，因为具备基础无线知识的任何黑客都可以很容易地发现 SSID。

11.5.3　执行现场勘测

用于发现不需要无线接入的物理环境区域的一种方法是执行现场勘测。现场勘测的过程是调查在环境中部署无线接入点所需的信号强度。这项任务通常包括携带便携式无线设备进行现场行走观察，留意无线信号的强度，并据此在建筑图上进行标注。

执行现场勘测来确保无线设备使用的所有位置具备足够的信号强度，同时在同一时间，最大限度地减少或消除不允许无线接入位置(公共区域、跨楼层、其他房间或建筑外)的无线信号。现场勘测对于评估现有无线网络的部署、扩展当前应用的计划以及未来部署计划非常有用。

11.5.4 使用加密协议

在使用无线链路进行正常的网络通信之前，IEEE 802.11 标准定义了两种由无线客户端向无线接入点进行验证的方法。这两种方法是开放系统认证(Open System Authentication，OSA)和共享密钥认证(Shared Key Authentication，SKA)。OSA 没有真正的认证要求。只要无线电信号可以在客户端和 WAP 之间传输，通信即被允许。而且，使用 OSA 的无线网络通常以明文发送一切信息，因此未提供任何保密或安全。SKA 意味着在进行网络通信时必须进行某种形式的身份认证。802.11 标准定义了有线等效保密(WEP)协议为 SKA 的可选技术之一。随后，对原标准 802.11 进行了修订，增加了 WPA、WPA2 以及其他的技术。

1. WEP

有线等效保密(WEP)被定义为 IEEE 802.11 标准，目的在于为无线网络提供与有线或通信电缆网络相同级别的安全性和加密。WEP 提供无线传输保护中对数据包嗅探和窃听攻击的防护。

WEP 的另一个好处是，它可以被配置来防止未经授权的无线网络访问。WEP 使用预定义的共享密钥，然而并非典型的动态对称密码方案，共享密钥是静态的并在所有的无线接入点和设备接口之间进行共享。此密钥用于在无线链路传输之前加密数据包，从而提供机密性保护。哈希值用来验证接收的数据包在传输过程中不被修改或遭受损坏。因此，WEP 也提供完整性保护。知晓或拥有的密钥不仅可以加密通信，同时也可作为一种基本的身份认证，没有则禁止进入无线网络。

WEP 在发布的同时几乎就被破解。目前，可以在不到一分钟的时间就破解 WEP，从而使它成为毫无价值的安全防范。幸运的是，已有 WPA 和 WPA2 来替代 WEP。WPA 是对 WEP 的改进，它不使用静态密钥来加密所有的通信。相反，它和每一个主机协商一个单独的密钥。然而，一个单一的口令被用来授权与基站之间的关联(例如，让一个新客户建立连接)。如果密码不够长，它可能被猜到，通常建议采取 14 个字符或更长的口令。

WEP 加密采用 RC4 流密码算法，它是一个对称流加密算法(可以参阅第 6 章“密码学与对称密钥算法”以及第 7 章“PKI 和密码学应用”以获得更多关于该加密算法的信息)。由于 RC4 在设计和实现上的缺陷，WEP 在若干地方存在薄弱点，它们是使用静态的公共密钥和薄弱的 IV(起始向量)。由于这些缺点，对 WEP 进行破解后可以获得足够的、使用不当的 IV 以发现 WEP 密钥。这种攻击现在可以在不到 60 秒的时间内进行。当 WEP 密钥被发现后，攻击者就可以加入网络，并监听所有其他无线客户端的通信。因此，不应该使用 WEP。WEP 并没有提供真正的保护，可能会导致产生一种虚假的安全感。

2. WPA

WPA 被设计用来替代 WEP；它是一个临时的解决办法，直到新的 802.11i 修订版完成。制作新修订花费了数年的时间，因此 WPA 在市场上得以立足并且直到今天仍然被广泛使用。此外，WPA 可用于大多数设备，包括不支持 802.11i 特性的一些低端硬件。

802.11i 是代替 WEP 加密解决方案的修订协议。然而，当 802.11i 定稿时，WPA 解决方案已经被广泛使用，所以不能使用原来计划的 WPA 名称，于是被称为 WPA2。但这并不表明 802.11i 是 WPA 第二版。事实上，它们是完全不同的技术。802.11i 或 WPA2 实现了类似于 IPSec 的概念并为无线通信带来最好、最新的加密和安全性。

WPA 基于 LEAP 和 TKIP 加密体系并通常使用安全加密用于认证。遗憾的是，使用单个静态的密码将彻底损坏 WPA 的安全性。攻击者可以简单地在 WPA 网络中运行暴力猜测攻击以发现密码。如果密码是 14 位字符或更长，这通常是时间问题，但并非不可能无法破解。此外，无论是 WPA 的 LEAP 还是 TKIP 加密选项，目前都可以使用不同的破解技术进行破解。尽管 WPA 比 WEP 更复杂，但 WPA 不再提供长期可靠的安全。

3. WPA2

最后，一种新的确保无线安全的方法被开发出来，并且截至目前仍然被认为是安全的。这就是被称为 802.11i 或 WPA2 的修订方案。这是一种新的加密方案，称为计数器模式密码块链接消息认证码协议(Counter Mode Cipher Block Chaining Message Authentication Code Protocol，CCMP)，这是基于 AES 的加密方案。到目前为止，还没有实际的攻击能破坏正确配置的 WPA2 无线网络加密。

4. 802.1X/EAP

WPA 和 WPA2 都支持称为企业认证的 802.1X/EAP，这是一个标准的基于端口的网络访问控制协议，确保客户端在没有发生正确认证时不能和资源发生通信联系。802.1X 是一种有效允许无线网络利用现有的网络基础设施进行认证服务的协议。通过使用 802.1x，其他技术和解决方案，如 RADIUS、TACACS、证书、智能卡、令牌和生物识别设备，可以被集成到无线网络中并提供包括进行交互和多因子认证的技术。

EAP(Extensible Authentication Protocol，可扩展认证协议)是认证框架而不是具体的认证机制。实际上，EAP 可以允许新的认证技术与现有无线或点对点连接技术兼容。有超过 40 种不同的 EAP 认证方法获得广泛支持。这些 EAP 方法包括 LEAP、EAP-TLS、EAP-SIM、EAP-AKA 和 EAP-TTLS。不是所有的 EAP 方法都是安全的。例如，EAP-MD5 和之前版本的 LEAP 也会被破解。

5. PEAP

PEAP(Protected EAP，受保护的可扩展认证协议)通过 TLS 隧道封装 EAP 方法，提供了认证和潜在的加密功能。由于 EAP 最初被设计用于在物理上隔离通道，因此假定固定通路，EAP 通常是不加密的。所以，PEAP 可以为 EAP 方法提供加密。

6. LEAP

LEAP(Lightweight EAP，轻量级可扩展认证协议)是 Cisco 专有的，用于 WPA 替代 TKIP。在 802.11i/WAP2 系统被批准为标准之前，它被开发用于应对 TKIP 地址不足的情况。一种称为 Asleap 的攻击工具在 2004 年发布，该工具可以破解 LEAP 提供的最终脆弱保护。如果可能，应尽量避免使用 LEAP 并建议使用 EAP-TLS 作为一种替代。但如果已使用 LEAP，强烈推荐使用复杂的密码。

7. MAC 过滤器

MAC 过滤器是一系列授权的无线客户端接口 MAC 地址，这些地址被无线接入点用来阻断那些未经授权的设备。虽然这是一个有用的特性，但是它难以管理，并且往往只使用在小型、静态的环境中。此外，黑客通过基本的无线黑客工具就可以发现有效客户端的 MAC 地址，然后伪装成该地址对无线客户端发起攻击。

8. TKIP

TKIP(Temporal Key Integrity Protocol，临时密钥完整性协议)被设计为替代 WEP 而不需要更换无线硬件。TKIP 在无线网络 802.11 WPA 的名称下得到应用。TKIP 改进了很多，包括密钥的混合功能，该功能在使用 RC4 算法密钥进行加密之前结合了初始向量(IV，一个随机数)与安全的根密钥；一个序列计数器被用来防止报文重放攻击；同时还使用了一种强大的称为 Michael 的完整性检查。

TKIP 和 WPA 在 2004 年被 WPA2 正式取代。此外，对 WPA 和 TKIP 的特定攻击(如 WPAtty 和基于 GPU 的攻击工具)都验证了 WPA 提供的安全性是不可靠的。

9. CCMP

CCMP(计数器模式密码块链接消息认证码协议)用于取代 WEP 和 TKIP/WPA。CCMP 使用 AES(高级加密标准)和 128 位的密钥。CCMP 是 802.11i 制定的在 802.11 无线网络中首选的标准安全协议。到目前为止，还没有攻击能成功破解 AES/CCMP 加密。

11.5.5 天线位置的确定

在部署无线网络时，天线位置应该是一个值得关注的问题。不要在适当的现场勘测完成之前就固定到一个特定的位置。将无线接入点和/或它的天线放置在一个可能的位置，然后测试不同位置的信号强度和连接质量。只有在确认该潜在的天线位置提供了令人满意的连接后，才应该进行永久性的固定。

在寻找最佳天线位置时应考虑以下准则：

- 使用中央位置
- 避开固体物理障碍物
- 避开反射或其他平整的金属表面
- 避开电气设备

如果基站具有外部的全向天线，通常它们应该在垂直方向进行垂直定位。如果使用定向天线，指向所需使用的区域的焦点。记住，无线信号会受到干扰、距离和障碍物的影响。当设计安全的无线网络时，工程师可以选择定向天线，以避免在不希望的地区提供广播信号或在专门覆盖的区域具有更强的信号。

11.5.6 天线类型

有很多各种各样的天线类型可用于无线客户端和基站。许多设备可以用更强的(例如，信号增强)天线替代原有的标准天线。

标准的直杆或杆天线是一种全向天线，可以在垂直于天线本身的方向上发送和接收信号。在大多数基站和一些客户端设备上可发现这种天线类型。这种类型的天线有时也被称为基础天线或橡胶天线(事实上大多数天线由橡胶涂层覆盖)。

其他大多数类型的天线是定向的，这意味着它们专注于某个主要方向的发送和接收能力。一些例子包括 Yagi 天线、cantenna 天线、面板天线和抛物面天线。Yagi 天线的结构和屋顶上传统的电视天线是相似的。Yagi 天线从一个截面直杆在主杆的方向捕捉特定的无线电频率。cantenna 天线由一

段封闭的许多管子构成。它们沿着管的开口方向集中。一些第一代的 cantenna 天线选取 Pringles 薯片罐进行制作。平板天线是一种平板设备，只关注于面板的一个侧面。抛物面天线则用来聚焦从很远的距离发来的或微弱来源的信号。

11.5.7　调整功率水平控制

一些无线接入点提供了物理或逻辑调整天线功率水平的功能。功率控制通常由厂家设定为适用于大多数的情况。但是，如果在进行现场勘测和调整天线位置后，无线信号仍然无法令人满意，功率水平调整可能是必要的。然而，要记住改变信道，避免反射和信号散射表面以减少干扰，往往可以更有效地改善连接可靠性。

当调整功率水平时，要进行微调，而不是试图将设置最大化或最小化。此外，需要注意初始/默认设置以便必要时可以返回到该设置。在每一次功率水平调整后，在重新进行现场勘测和质量测试之前重置/重新启动无线接入点。有时降低功率水平可以提高性能。需要记住，一些无线接入点能够提供比一些国家许可规定更高的功率水平。

11.5.8　使用强制门户

强制门户是一种认证技术，它将新连接的无线 Web 客户端重定向到强制门户访问控制页面。这个门户页面可能需要用户输入付款信息、提供登录凭据或输入访问代码。强制门户也被用来给用户显示可访问的使用策略、隐私策略和跟踪策略，用户必须同意策略才能接入网络进行通信。强制门户经常用于提供公共用途的无线网络，如酒店、餐馆、酒吧、机场、图书馆等。当然，它们也可用于有线以太网连接。

11.5.9　一般的 Wi-Fi 安全措施

这里基于无线安全和配置选项的细节，给出了在部署 Wi-Fi 网络时应遵循的指南或程序。这些步骤是为了考虑应用和安装。此外，这些步骤并不意味着哪一步提供更多的安全性。例如，使用 WPA2 相对于 SSID 广播禁用能提供真正的安全性。下面是具体步骤：

(1) 改变默认的管理员密码。

(2) 关闭 SSID 广播。

(3) 变更 SSID 到特定的方式。

(4) 如果无线客户端比较少且是静态的，启用 MAC 过滤。

(5) 考虑使用静态 IP 地址，或配置保留的 DHCP(仅适用于小型部署)。

(6) 开启支持的身份认证和加密的最高形式。如果不提供 WPA2，那么使用 WPA 和 WEP 提供非常有限的保护也比未加密的网络好得多。

(7) 把无线视为远程访问，并使用 802.1x 进行访问管理。

(8) 把无线视为外部接入，把 WAP 和有线网络用防火墙进行隔离。

(9) 把无线视为攻击者的入口，用 IDS 监控所有 WAP 到有线网络的通信流量。

(10) 需要对无线客户端和 WAP 之间的通信进行加密，换句话说，需要 VPN 连接。

注意：

通常，添加数据加密层(WPA2 和 IPSec VPN)和其他形式的过滤，无线链路将降低高达 80%的有效吞吐量。此外，在相对基站更远的距离和存在干扰的存在下，将进一步减少有效吞吐量。

无线攻击

即使有无线安全的保护，无线攻击也仍然可以发生。有各种不断增加和变化的攻击，专门针对许多有线和无线网络的工作环境。少部分攻击也专注于无线网络。例如，有一个技术的合集，通常被称为战争驾驶，用于发现使用中的无线网络。此活动包括使用无线接口或无线检测器来定位无线网络信号。一旦攻击者知道无线网络的存在，他们就可以利用嗅探器收集无线数据包并进行调查。通过使用正确的工具，攻击者可以发现隐藏的 SSID、活动中的 IP 地址、有效的 MAC 地址，甚至无线用户使用的认证机制。从那里，攻击者可以抓取和使用专门的破解工具，尝试突破连接或试图进行中间人攻击。保护机制越陈旧，保护能力越薄弱，攻击的成功性和时效性就越高。

11.6 保护网络组件

互联网上包括了无数信息服务和众多应用程序，包括 Web、电子邮件、FTP、Telnet、新闻组和聊天室等。互联网还是怀有恶意的人的家园，这些人的主要目的就是定位他人的计算机并提取有价值的数据，利用他人的计算机发动进一步的攻击，或者通过某些方式进行破坏。我们应当熟悉互联网，并且通过自己的联机实践能够容易地识别互联网的优点与弱点。由于互联网的成功与全球化应用，互联网的许多技术被改编或集成到专用的商业网络。这就出现了两种新的网络形式：内部网和外部网。

内部网是一种专用网络，被设计用于集成与建立在互联网上的相同信息服务。依赖于外部服务器(也就是在公共的互联网上放置的服务器)在内部提供信息服务的网络不被视为内部网。内部网为用户提供对内部服务器上的 Web、电子邮件和其他服务的访问，这些服务对于专用网络外部的任何人来说都是不可访问的。

外部网是互联网和内部网之间的中间网络。外部网是组织网络中被分离出的一部分，因此对于专用网络来说，它是一个内部网，但是它还为公共的互联网提供信息服务。外部网常常被预留给特定的合作伙伴或客户使用，并且极少依赖于公共网络。供公共消费的外部网通常被标记为隔离区(DMZ)或边界网络。

网络通常不被配置为单一的大集合系统。通常网络被分隔或细分成较小的组织单位。这些更小的单位、分组、分段或子网络(即子网)可以用来提高网络的各个方面：

提高性能 网络分隔可以通过组织方案提高性能，这样经常通信的系统位于同一个网段，而很少或无任何通信的系统位于其他网段。

减少通信 网络分隔往往能减少通信拥塞和容纳通信问题，如广播风暴、单独的网络分段。

提高安全性 网络分隔可提高安全性，可通过隔离数据流以及需要用户接入认证的网络段来加以实现。

可以通过基于交换机的 VLAN、路由器或防火墙抑或它们的组合进行网络分隔。私有局域网或内部网、DMZ 和外部网都是网络分隔的类型。

正在设计安全网络时(无论是专用网络、内部网还是外部网)，必须对众多的网络连接设备进行

评估。对于安全网络来说，不是所有这些组件都是必要的，但它们都是可能对网络安全性产生影响的常用网络设备。

11.6.1　网络接入控制

网络接入控制(NAC)是一种访问控制环境中通过严格遵守和实施安全策略的概念。NAC 领域的目标如下：

- 预防/减少 0-day 攻击
- 加强网络通信的安全策略
- 使用验证完成访问控制

NAC 的目标可以通过使用强大且详细的安全策略来达到。这些措施明确了从客户端到服务器以及所有内部或外部沟通中每台设备的安全控制、过滤、预防、检测和响应。NAC 作为一种自动检测和响应系统，可以实时反应，在威胁引起损坏或破坏之前就对其进行阻断。

最初，802.1x(提供基于端口的 NAC)被认为体现了 NAC，但大多数的支持者认为 802.1x 仅仅是 NAC 的一种简单形式或者只是完整 NAC 解决方案的组成部分。

NAC 可以通过进入前评估方式或进入后评估方式，或结合这两种方式进行应用：

- 进入前评估方式需要系统满足当前的安全要求(如应用补丁和杀毒软件更新)才被允许与网络进行通信。
- 进入后评估方式基于用户的活动允许访问或拒绝访问，是预定义的授权矩阵。

其他围绕 NAC 的问题包括客户端/系统代理与整体网络监控(非代理)；带外与带内监测；以及分解任何补救、隔离或强制门户策略。这些和其他的 NAC 问题必须在实施之前进行考虑和评估。

11.6.2　防火墙

防火墙是管理和控制网络通信的必要工具。防火墙是一种用于过滤通信的网络设备，并且通常部署在专用网络与互联网的连接之间，也可以部署在公司内的不同部门之间。如果没有防火墙，那么就无法限制来自互联网的恶意通信进入专用网络。防火墙基于已定义的一组规则(也被称为过滤器或访问控制列表)对通信进行过滤。这些规则本质上是一组指令，这组指令被用于区分已授权的通信和非授权的或恶意的通信。只有已授权的通信才被允许通过防火墙所提供的安全屏障。

防火墙被用于阻止或过滤通信。针对未请求的通信和从外部连接专用网络的企图，以及基于内容、应用、协议、端口或源地址来阻止已知的恶意数据、消息或数据包，防火墙都是最有效的。防火墙能够对公共网络隐藏专用网络的结构和寻址方案。大多数防火墙都提供广泛的日志记录、审计和监控性能，以及警报和基本的入侵检测系统(IDS)功能。

防火墙通常不能阻止通过其他已授权通信信道传送的病毒或恶意代码，不能防止未授权的但由用户无意或有意造成的信息泄漏，不能防范防火墙之后的恶意用户所进行的攻击，也不能在数据离开或进入专用网络之后对其进行保护。不过，可以通过特殊的插件模块或同类产品(例如，防病毒扫描装置和 IDS 工具)来添加这些功能。这些防火墙设备可通过预设配置去执行所有(或大多数)附加功能。

除了记录网络通信活动之外，防火墙还应当记录下面这些事件：

- 防火墙的重启
- 无法启动的代理或依赖服务

- 崩溃或重新启动的代理或其他重要服务
- 对防火墙配置文件的更改
- 防火墙运行时的配置或系统错误

防火墙只是总体安全解决方案的一部分。在使用防火墙的情况下，许多安全机制会集中在一个位置，因此防火墙可能出现单点故障。防火墙故障往往是由人为错误和不当配置造成的。防火墙不对子网内(也就是防火墙之后)的通信提供保护，而是只对通过防火墙的、从一个子网到另一个子网的通信提供保护。

防火墙的基本类型有 4 种：静态的数据包过滤防火墙、应用级网关防火墙、电路级网关防火墙以及状态检测防火墙。此外，通过将两种或多种防火墙类型组合为单个防火墙解决方案，也可以创建混合的或复杂的网关防火墙。大多数情况下，使用多级别防火墙能够更好地控制通信过滤。不管怎样，接下来将要介绍各种防火墙类型，并且还将讨论防火墙部署的体系结构。

静态的数据包过滤防火墙 静态的数据包过滤防火墙通过检查报文头部的数据进行通信过滤。通常，过滤规则关注于源地址、目的地址和端口地址。使用静态过滤时，防火墙不能为用户提供身份认证，也不能告知数据包来自专用网络内部还是外部，并且很容易受到虚假数据包的欺骗。静态的数据包过滤防火墙被称为第一代防火墙，在 OSI 模型的第 3 层(网络层)上工作。此外，这种防火墙也被称为屏蔽路由器或常用路由器。

应用级网关防火墙 应用级网关防火墙也被称为代理防火墙。代理是一种可以将数据包从一个网络复制到另一个网络的机制；为了保护内部或专用网络的身份，复制过程还改变了源地址和目的地址。应用级网关防火墙基于用于传送或接收数据的网络服务(也就是应用)来过滤通信。每种应用类型都必须具有自己唯一的代理服务器。因此，应用级网关防火墙包括很多独立的代理服务器。由于每个信息数据包在通过防火墙时都必须经过检查和处理，因此这种类型的防火墙对于网络的性能会产生负面影响。应用级网关防火墙被称为第二代防火墙，并且在 OSI 模型的应用层(第 7 层)上工作。

电路级网关防火墙 电路级网关防火墙用于在可信合作伙伴之间建立通信会话，在 OSI 模型的会话层(第 5 层)上工作。SOCKS(来自安全套接字，就像 TCP/IP 端口一样)是电路级网关防火墙的通用实现。电路级网关防火墙也称为电路代理，在电路的基础上管理通信，而不是基于通信的内容管理通信。这种防火墙只基于通信电路的终点名称(也就是源地址、目的地址以及服务端口号)来许可或拒绝转发决策。因为它们代表对应用级网关防火墙概念的更改，所以电路级网关防火墙仍然被视为第二代防火墙。

状态检测防火墙 状态检测防火墙(也被称为动态包过滤防火墙)对网络通信的状态或环境进行评估。通过查看源地址和目的地址、应用习惯、起源地以及当前数据包与同一会话先前数据包之间的关系，状态检测防火墙就能够为已授权的用户和活动授予广泛的访问权限，并且能够积极地监视和阻止未授权的用户和活动。状态检测防火墙通常比应用级网关防火墙更有效。状态检测防火墙被视为第三代防火墙，并且在 OSI 模型的网络层和传输层(第 3 层和第 4 层)上工作。

1. 多宿主防火墙

某些防火墙系统具有多个接口。例如，多宿主防火墙必须至少具有两个过滤通信的接口(具有两个接口的防火墙被称为双宿主防火墙)。应该禁用所有多宿主防火墙的 IP 转发功能，以便使过滤规则控制所有通信，而非允许接口之间存在软件支持的捷径。堡垒主机或屏蔽主机只是位于专用网络和不可信网络之间的防火墙系统。通常，堡垒主机位于连接专用网络和不可信网络的路由器之后。

所有入站通信都被路由至堡垒主机，随后堡垒主机作为专用网络内所有可信系统的代理。堡垒主机不仅负责过滤进入专用网络的通信，而且还负责保护内部客户端的身份。

注意：

术语“堡垒”来源于中世纪的城堡建筑风格，其中，堡垒警戒室位于主入口的前面，从而提供第一层防御保护。使用这个术语描述防火墙，表明防火墙的作用相当于接受入站攻击的牺牲性主机。

屏蔽子网位于两个路由器之间，并且堡垒主机就位于这个子网内，除此之外，屏蔽子网与屏蔽主机(也就是堡垒主机)在概念上相似。所有入站通信都被定向至堡垒主机，并且只有由堡垒主机代理的通信才能够通过第二个路由器进入专用网络。这种方式会创建一个子网，在该子网内，某些外部访问者被允许与网络提供的资源进行通信。上面介绍的就是 DMZ 的概念，DMZ 是一个被设计为外部访问者能够访问的网络区域，不过这个区域仍然与组织的专用网络相隔离。DMZ 常常是公共 Web、电子邮件、文件以及其他资源服务器的宿主。

2. 防火墙部署的体系结构

防火墙部署的体系结构一般有三种：单层、双层和三层(也被称为多层)。

你能从图 11.8 中看到，单层部署将专用网络置于防火墙之后，防火墙通过路由器连接互联网(或者其他某些不可信网络)。单层部署只用于针对一般的攻击。这种体系结构只提供最低限度的保护。

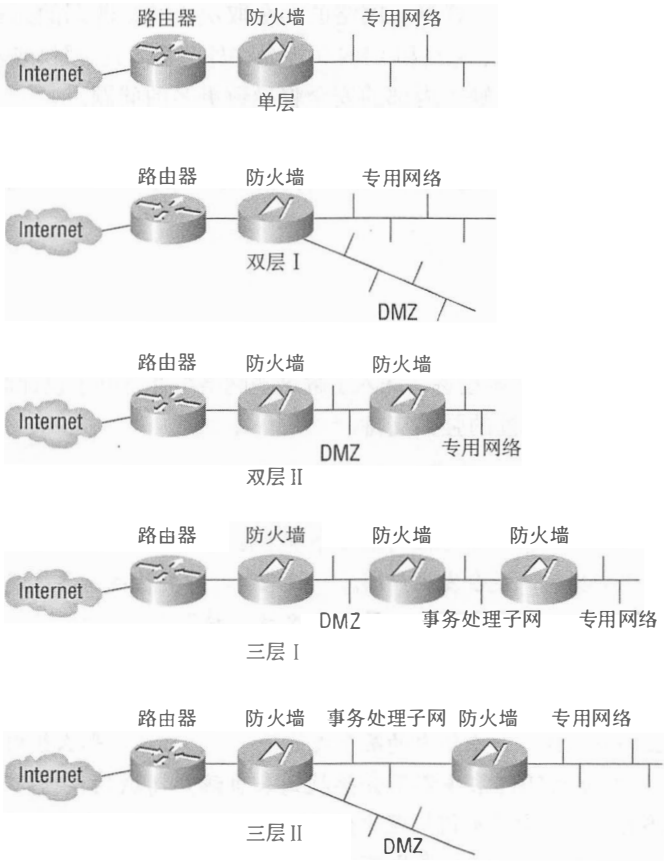


图 11.8　防火墙部署的三种体系结构

双层部署体系结构可能采用两种不同的设计方式之一。一种设计使用一个具有三个或更多个接口的防火墙，另一种设计则串联使用两个防火墙。这种体系结构允许存在一个 DMZ 或公共可访问的外部网。在第一种设计中，DMZ 位于主防火墙的其中一个接口；而在第二种设计中，DMZ 位于两个串联的防火墙之间。DMZ 用于驻留外部用户能够访问的信息服务器系统。防火墙根据其严格的过滤规则将通信路由至 DMZ 或可信网络。这种体系结构引入了中等级别的路由和过滤复杂性。

三层部署体系结构是在专用网络与互联网之间用防火墙隔离的多个子网部署。后续的每个防火墙都使用更严格的过滤规则，只接受可信来源的通信。最外面的子网往往是 DMZ。中间的子网可以作为事务处理子网，在这种子网内，系统需要支持在 DMZ 中驻留的复杂的 Web 应用程序。第三个或后端子网能够支持专用网络。这种体系结构是最安全的，不过其设计、实现和管理也是最复杂的。

11.6.3 终端安全

终端安全的概念是指每个单独设备必须维护本地安全，不论其网络或通信信道是否提供安全。有时这被表示为“末端设备应对自己的安全负责”。然而，一个更清晰的视角是网络中的任何脆弱点，无论其是否是在边界上、在服务器上或在客户端上，都对组织内的所有元素构成风险。

传统的安全取决于网络的边界入口，通过诸如应用防火墙、代理服务器、集中式病毒扫描程序，甚至是 IDS/IPS/IDP 解决方案来为网络中的所有内部节点提供安全保障。这已经不被认为是最佳行业实践，因为内部威胁和外部威胁一样多。网络的安全取决于其最薄弱的元素。

当更多远程访问服务，包括拨号、无线和 VPN 可能允许外部实体 (已授权或未授权)来访问专用网络而不必经过边界安全检查时，缺乏内部的安全将导致更多的问题。

终端安全应视为在每个单独主机上提供足够安全努力的一个方面。每个系统都应该有合适的安全组合，包含本地主机防火墙、反恶意软件扫描、身份认证、授权、审计和垃圾邮件过滤器以及 IDS/IPS 服务。

11.6.4 其他网络设备

当构建一个网络时，会使用许多设备。深入了解这些网络组件有助于设计避免单点故障的 IT 基础架构，并且能够提供对可用性的强大支持。

冲突与广播

当两个系统同时在只支持单条传输路径的连接介质上传送数据时，就会发生冲突。当单个系统向所有可能的接收者传输数据时，就会发生广播。一般来说，冲突往往需要被避免和阻止，而广播有时则是有用的。对冲突和广播的管理引入了一个名为“域”的新术语。

冲突域是一个互联系统组，如果组内的任何两个(或多个)系统同时进行传输，那么就会发生冲突。冲突域外部的任何系统都不会与冲突域内部的任何成员发生冲突。

广播域也是一个互联系统组，如果组内的某个成员传输广播信号，那么组内的其他所有成员都会接收到广播。广播域外部的任何系统都不会接收到来自该广播域的广播信号。

在设计和部署网络时，应当考虑如何管理冲突域和广播域。使用任何第二层或更高层设备可以分隔冲突域，使用任何第三层或更高层设备则可以分隔广播域。域被分隔时，就意味着部署设备另一侧的系统是不同域的成员。

下面列出了一些网络中的硬件设备：

中继器、集中器和放大器　中继器、集中器和放大器用于加强线缆段上的通信信号以及连接使用相同协议的网段。通过在较长的线缆上部署一个或多个中继器，这些设备就能用于延长特定线缆类型的最大长度。中继器、集中器和放大器在 OSI 模型的第 1 层上工作。中继器、集中器或放大器两侧的系统都位于相同的冲突域和广播域内。

集线器　集线器用于连接多个系统以及连接使用相同协议的网段。它们将入站通信在所有出站端口上进行中继。这确保了通信将到达预计的主机。集线器是一种多端口的中继器，它在 OSI 模型的第 1 层上工作。集线器两侧的系统都位于同一冲突域和广播域内。大多数组织有非集线器的安全策略来限制或减少窃听的风险，因为集线器是一种过时的技术，交换机已替代它们。

调制解调器　传统的陆线调制解调器(调制器-解调器)是一种通信装置，其在模拟信号和数字信息之间进行覆盖或调制，以支持在公共电话网络(PSTN)线路上进行计算机通信。在 20 世纪 60 年代到 90 年代中期，调制解调器通常指广域网通信。调制解调器后来被包括 ISDN、DSL 调制解调器、电缆调制解调器、802.11 无线调制解调器以及各种形式的无线调制解调器的数字宽带技术替代。

注意：

调制解调器这个术语通常被不正确地用于称呼那些并不真正进行调制解调的设备。大多数被称为调制解调器(电缆、DSL、ISDN、无线调制解调器等)的现代设备是路由器而不是调制解调器。

桥　桥用于将两个网络(即使是拓扑结构、线缆连接类型和速度不同的网络)连接在一起，以便连接使用相同协议的网段。桥将通信从一个网络转发至另一个网络。将使用不同传输速率的网络连接在一起的桥可以缓存数据包，直至这些数据包被转发至较慢的网络，这被称为存储转发设备。桥在 OSI 模型的第 2 层上工作。桥两侧的系统位于相同的广播域内，不过所在的冲突域不同。

交换机　如果不使用集线器，那么可以考虑使用交换机或智能集线器。交换机知道在每个出站端口上连接的系统的地址。与在所有出站端口上中继通信不同，交换机只在已知存在的目的地所在的出站端口外对通信进行中继。交换机能够更有效地进行流量传递、建立隔离的冲突域以及提高数据的总体吞吐量。在用于创建 VLAN 时，交换机也可以创建隔离的广播域。如果采用这样的配置，那么广播只允许在单个 VLAN 内，不允许从一个 VLAN 顺利地穿越至另一个 VLAN。交换机主要在 OSI 模型的第 2 层上工作。当交换机具有额外的功能时(如路由)，那么也可以在 OSI 模型的第 3 层上工作(例如，在 VLAN 之间进行路由的情况)。在第 2 层上工作的交换机，其两侧的系统位于同一广播域内，不过所在的冲突域不同。在第 3 层上工作的交换机，其两侧的系统位于不同的广播域和冲突域内。交换机用于连接使用相同协议的网段。

路由器　路由器用于控制网络上的通信流，并常用来连接相似的网络以及控制两者之间的通信流。路由器既可以利用静态定义的路由表进行工作，也可以采用动态的路由系统。动态的路由协议有很多种，例如 RIP、OSPF 和 BGP。路由器在 OSI 模型的第 3 层上工作。路由器两侧的系统属于不同的广播域和冲突域。路由器用于连接使用相同协议的网段。

桥式路由器　桥式路由器是一种由路由器和桥组成的组合设备。桥式路由器首先尝试路由，如果路由失败，那么就默认进行桥接。因此，桥式路由器主要在 OSI 模型的第 3 层上工作，不过必要时也可以在第 2 层上工作。在第 3 层上工作的桥式路由器，其两侧的系统位于不同的广播域和冲突域内。在第 2 层上工作的桥式路由器，其两侧的系统位于相同的广播域内，不过所在的冲突域不同。桥式路由器用于连接使用相同协议的网段。

网关　网关能够连接使用不同网络协议的网络。通过将通信的格式转换为与每个网络采用的协

议或传输方法都兼容的形式，网关就可以负责从一个网络向另一个网络传输通信信息。网关也被称为协议转换器，既可以作为独立硬件设备，也可以作为一种软件服务(例如，IP-to-IPX 网关)。网关两侧的系统位于不同的广播域和冲突域内。网关用于连接使用不同协议的网段。网关具有很多类型，包括数据、邮件、应用、安全和互联网。网关通常在 OSI 模型的第 7 层上工作。

代理 代理是一种不需要在协议之间进行转换的网关。相反，代理能够充当网络的中介、过滤器、缓存服务器甚至 NAT/PAT 服务器。代理代表另一个系统执行操作或请求服务，并且连接使用相同协议的网段。代理最常被用于为专用网络中的客户端提供互联网访问，同时又保护客户端身份的环境中。代理从客户端接受请求，更改请求者的源地址，维持与客户端请求的映射，并且将更改过的请求数据包发出。这种机制就是通常所说的网络地址转换(NAT)。一旦接收到回应，代理服务器就会通过查看映射来决定预定的客户端，然后将数据包发送给该客户端。代理两侧的系统位于不同的广播域和冲突域内。

网络基础架构的详细清单

如果得到了组织的批准，那么全面查看或记录构成组织的网络的重要组件。看看你能够在网络内查找到多少种不同的网络设备。此外再观察一下设备部署模式，例如，是否总是以并联或串联方式部署设备？要了解设备的功能，是只需观看外观还是必须查看型号？

LAN 扩展 LAN 扩展是一种远程访问的多层交换机，用于通过 WAN 链接连接远距离网络。令人奇怪的是，LAN 扩展会创建 WAN，但是经销商却避开使用 WAN 术语，而是只使用 LAN 和扩展的 LAN 来称呼这种设备。之所以这样做的原因是：标准的 WAN 设备与复杂的概念和术语联系在一起，采用 LAN 术语能够使人们更容易理解这种设备，并且更容易开展营销工作。最终，LAN 扩展是与 WAN 交换机或 WAN 路由器相同的产品(我们同意 Douglas Adams 的观点，他坚信应当用宇宙飞船将销售人员、律师和电话推销人员运送到宇宙的最远端)。

注意：

虽然通过使用诸如防火墙和代理的过滤设备来管理网络安全是很重要的，但我们不能忽视对终端安全的需要。终端是网络通信链路的终点。一端通常在服务器资源一侧，而另一端通常是客户机请求使用网络资源。即使使用安全通信协议，滥用、误用、疏忽或恶意的行为仍可能发生在网络上，因为它起源于一个终端。从一端到另一端的所有方面的安全性通常被称为端到端的安全性，必须加以解决。任何不安全的端点最终都会被发现和滥用。

11.7 布线、无线、拓扑和通信技术

在网络上建立安全性相比管理操作系统和软件要涉及更多的内容。还必须解决物理问题，这些问题包括布线、无线、拓扑和通信技术。

LAN 与 WAN

网络的两个基本类型是 LAN 和 WAN。LAN (局域网)通常是覆盖某一楼层或某一栋建筑物的网络，一般存在于有限的地理范围内。WAN(广域网)通常是指在相距遥远的远程网络之间建立的长距离连接。

WAN 连接和通信链接可能包括专用线路技术和数据包交换技术。常见的专用线路技术包括专用或租用线路，以及 PPP、SLIP、ISDN 和 DSL 连接。数据包交换技术包括 X.25、帧中继、异步传输模式(ATM)、同步数据链路控制(SDLC)和高级数据链接控制(HDLC)。数据包交换技术使用虚拟电路代替专用的物理线路。虚拟电路只有在需要时才会建立，这使得传输介质得到了有效使用，并且极为经济有效。

11.7.1　网络布线

对于网络的设计、布局和能力来说，网络中使用的连通性介质的类型十分重要。如果没有进行正确的连线，那么网络可能无法覆盖整个企业，也可能无法支持必需的通信流量。事实上，网络故障(也就是影响可用性)的最常见原因是线路故障或配置错误。因此，理解不同类型的网络设备和技术使用不同的线缆连接类型至关重要。每种线路类型都存在特有的有效长度、吞吐率以及连通性要求。

1. 同轴电缆

同轴电缆(coaxial cable 或 coax)是 20 世纪 70 年代和 80 年代流行的网络连线类型。在 20 世纪 90 年代初期，由于双绞线连接的广泛使用和表现出的出色能力(稍后将进行详细阐述)，对同轴电缆的使用越来越少。同轴电缆的中心是一根铜线，外面包着一层绝缘物质，再往外是一层导电的编织屏蔽物，并且由最外面的绝缘外皮包裹着。

由于线缆中央的铜芯和编织屏蔽层作为两根独立的导线，因此准许在同轴电缆上进行双向通信。同轴电缆的设计使其能够完全抵抗电磁干扰(EMI)，能够支持高带宽(对比同时代的其他技术)，并且提供比双绞线更长的可用长度。由于双绞线成本更加低廉且安装简便，对同轴电缆最终失去了主导地位。同轴电缆需要使用网段终结器，而双绞线则不需要。同轴电缆体积较为庞大，并且最小弧形半径也要比双绞线的大(弧形半径是指线缆可以弯曲而不破坏内部导线的最小长度)。另外，随着交换网络的广泛部署，由于采用了结构化布线模式，线缆距离的问题已经变得不再那么重要。

同轴电缆具有两种主要类型：细缆和粗缆。细缆也被称为 10Base2，通常用来将系统连接到粗缆主干线路。细缆可以扩展到 185 米的距离，并且能够提供高达 10Mbps 的吞吐率。粗缆也被称为 10Base5，可以扩展到 500 米的距离，并且能够提供高达 10Mbps 的吞吐率。

同轴电缆的常见问题如下：

- 同轴电缆的弯曲会超出最大弧形半径，从而破坏中心导线
- 部署同轴电缆的长度超过推荐的最大长度(10Base2 的最大长度为 185 米，10Base5 的最大长度为 500 米)
- 在同轴电缆末端没有正确使用 50 欧姆电阻器

2. 基带和宽带线缆

标记大多数网络连线技术所使用的命名规则都遵从语法“XXyyyyZZ”。XX 表示线路类型所提供的最大速度，例如 10Base2 线路提供的最大速率为 10Mbps。yyyy 表示线路的基带或宽带特性，例如 10Base2 线缆的基带特性。基带线缆一次只能传输一个单独的信号，宽带线缆则可以同时传输多个信号。绝大多数网络连线都采用基带线缆。然而，在特定的配置中使用时，同轴电缆可以被用

作宽带连接，例如线缆调制解调器。ZZ 既可以表示线缆所能提供的最大应用距离，也可以表示线缆技术的速记形式，例如 10Base2 线缆可以提供大约 200 米的距离(实际上是 185 米，近似为 200 米)，10Base-T 或 100Base-TX 中的 T 或 TX 表示双绞线(需要注意的是，100Base-TX 使用两条 5 类 UTP 或 STP 线路实现，一条用于接收，另一条用于发送)。

表 11.7 列出了最常用的网络线缆连接类型的重要特性。

表 11.7 常用网络线缆连接类型的重要特性

类型	最大速率	距离	安装难度	受 EMI 影响程度	成本
10Base2	10Mbps	185 米	中等	中等	中等
10Base5	10Mbps	500 米	高	低	高
10Base-T(UTP)	10Mbps	100 米	低	高	很低
STP	155Mbps	100 米	中等	中等	高
10Base-T/10Base-TX	100Mbps	100 米	低	高	低
1000Base-T	1Gbps	100 米	低	高	中等
光纤	2Gbps 以上	2 公里以上	很高	不受影响	很高

3. 双绞线

与同轴电缆相比，双绞线相当细，而且非常灵活。双绞线由 4 对线缆组成，这 4 对线双绞在一起，并且被包在 PVC 绝缘皮内。如果在外皮之下、线缆的周围包有一层金属箱片，那么这条线就被称为屏蔽双绞线(STP)。这层金属箔片对外部 EMI 提供了额外保护。没有这层金属箔片的双绞线被称为非屏蔽双绞线(UTP)。UTP 常常只被大家称为 10Base-T、100Base-T 或 1000Base-T，这些现在已被认为是一种过时的技术。

UTP 和 STP 的线缆由细铜线组成，它们被成对地双绞在一起。线缆的缠绕可以使线缆免受外部的无线电频率干扰、电子干扰和磁性干扰，并且降低了线对之间的串扰。由于电流会产生电磁辐射，因此一组线会被另一组线感应，这样在数据传输时就会发生串扰。线缆中的每个线对都以不同的程度进行缠绕(也就是每英寸距离内进行缠绕)，这样当信号在一对线上传递时，就不会交错到另一对线上。缠绕得越紧(每英寸进行的缠绕越多)，那么对内部和外部干扰以及串扰的屏蔽也就越强，因此吞吐的能力也就越大(也就是说，具有更大的带宽)。

UTP 线缆有几种类型。不同的种类来自于使用的线对缠绕的松紧、导线的质量和外部绝缘层的质量。表 11.8 列出了 UTP 的类别。

表 11.8 UTP 的类别

UTP 类别	吞吐率	说明
1 类	只用于语音	不适用于网络，但是可用于调制解调器
2 类	4Mbps	不适用于大多数网络，常常用于大型机中的主机到终端的连接
3 类	10Mbps	主要用于 10Base-T 以太网(在令牌环网中只提供 4Mbps 的吞吐率)
4 类	16Mbps	主要用于令牌环网
5 类	100Mbps	用于 10Base-TX、FDDI 和 ATM 网络
6 类	155Mbps	用于高速网络
7 类	10Gbps	用于千兆速率的网络

注意：

5e 类是 5 类的增强版本，被设计用于防止远端串扰。在 2001 年，TIA/EIA-568-B 不再认可最初的 5 类规范。现在，100Base-T 甚至 1000Base-T 部署采用的标准都为 5e 类标准。

下面列出了使用双绞线的最常见问题：

- 使用错误的双绞线线缆类型来完成高吞吐率的网络连接
- 部署的双绞线线缆长度超过推荐的最大长度(也就是 100 米)
- 在具有显著干扰的环境中使用 UTP

4. 导线

导线型网络线缆的距离受到金属导线电阻的限制。作为最常用的导线，铜线是最好、最便宜的可用于室温环境下的一种导线。然而，铜线对于电流还是存在电阻，这使得信号的强度和质量在超出线缆的长度时会降低。

注意：

阻燃线缆是一种用燃烧时不会释放毒烟的特殊材料包围的线缆，就像传统的 PVC 覆盖布线。使用阻燃线缆往往需要遵从建筑规范，尤其当建筑物存在会聚集瓦斯气体的封闭空间时更应当注意。

每种线缆类型定义的最大长度，指的是在哪一点信号降低的程度开始对数据传输的有效性产生干扰。信号的这种降低被称为衰减。在使用中，线缆的长度常常可能超出定额，但是错误和重传的数量将在这条线缆上增加，最终会导致网络的性能变得很差。随着传输速率的提高，衰减将表现得更加显著。如果要提高传输速率，建议大家使用较短的线缆。

距离长的线缆常常可以通过使用中继器或集中器得到补充。中继器是一个信号放大设备，它更像是车载或家用录音机的放大器。中继器将输入数据流的信号强度增大，然后从它的另一个端口重新广播出去。除了具有两个以上的端口之外，集中器与中继器进行同样的操作。但是，连续使用的中继器不能多于 4 个(参看下面的“5-4-3 规则”)。

5-4-3 规则

5-4-3 规则用于在树型拓扑中部署以太网或其他 IEEE 802.3 共享访问网络的情况(也就是有一个中央主干，并且具有一些分散的枝杈)。这条规则定义了在网络设计中可以使用的中继器/集中器和网段的数量。这条规则规定，在任意两个节点之间(节点可以是任意类型的处理实体，例如服务器、客户端或路由器)，可以最多存在由 4 个中继器/集中器连接的 5 个网段，这 5 个网段中只有 3 个网段可以使用(也就是可以连接额外的或其他的用户、服务器或网络设备)。

5-4-3 规则不适用于交换网络，也不适用于使用桥或路由器的情况。

针对建立在导线基础上的网络线缆，存在一种备选方案，那就是光纤。光纤传输的是光脉冲，而不是电子信号，好处在于速率相当快，而且几乎不会受到窃听和干扰。然而，光纤的安装困难且价格昂贵，因此所提供的安全性和性能建立在高昂的成本之上。

11.7.2 网络拓扑

计算机和网络连接设备的物理布局和组织被称为网络拓扑结构。逻辑拓扑结构指的是通过网络连接在一起的系统被分组在一个可信集合内。物理拓扑结构并不总与逻辑拓扑结构相同。网络的物理布局存在 4 种基本的拓扑结构：环型、总线型、星型和网状型。

环型拓扑结构 环型拓扑结构将每个系统像圆周上的点一样连接在一起(如图 11.9 所示)。连接介质像一条单向的传输环。每次只有一个系统可以传输数据。传输管理通过一个令牌实现。令牌是一个数字通行证，它绕着环运动，直至被系统捕获。拥有令牌的系统能够传输数据。数据和令牌被传送到特定的目的地。在数据绕环传递时，每个系统都要查看自己是否就是数据的预定接收者。如果不是，则继续传递令牌。如果是，则读取数据。一旦数据被接收，令牌即被释放，并且返回到环中继续绕行，直到被另一个系统捕获。如果环中的任意一段出现故障，那么所有的绕环通信都将终止。为了防止单点故障，某些环型拓扑结构的实现采用了容错机制，例如反向运行的双环。

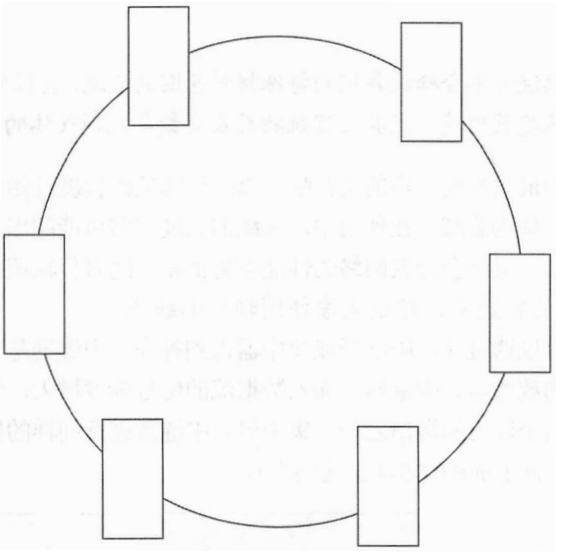


图 11.9 环型拓扑结构

总线型拓扑结构 总线型拓扑结构将每个系统都连接到一条主干线或骨干线。总线上所有的系统都可以同时传输数据，这样就可能导致冲突。当两个系统同时传输数据时，就会出现冲突，信号会相互产生干扰。为了避免这种情况的发生，系统采用冲突避免机制，这种机制主要对当前其他任意的通信进行“侦听”。如果侦听到通信，那么系统会等待片刻并再次进行侦听。如果没有侦听到通信，那么系统就传输其数据。当数据在总线型拓扑结构上进行传输时，网络上的所有系统都在侦听这些数据。如果数据的目的地址不是某个特定的系统，那么该系统就会忽略这个数据。总线型拓扑结构的好处在于，如果单个网段出现了故障，那么其他所有网段上的通信仍然能够继续进行而不被中断。不过，中央干线仍然存在着单点故障隐患。

总线型拓扑结构有两种类型：线型和树型。线型总线型拓扑结构采用单条主干线路，所有的系统都直接连接到干线上。树型总线型拓扑结构采用单条主干线路，其分支可以支持多个系统。图 11.10 说明了这两种拓扑结构类型。总线在今天很少使用的主要原因是：它必须在两端有终接器并且在整个网络中容易出现断网的情况。

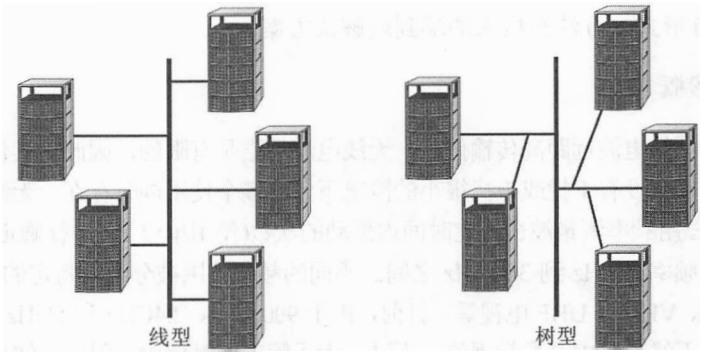


图 11.10　线型总线型拓扑和树型总线型拓扑

星型拓扑　星型拓扑结构采用了一个集中式连接设备，这个设备可以是一台简单的集线器或交换机。每个系统都通过一个专用的网段连接到中央集线器(如图 11.11 所示)。如果任意一个网段出现故障，那么其他网段仍然可以继续运作。然而，中央的集线器却是一个单点故障点。总的来说，星型拓扑结构使用了比其他拓扑结构更少的线缆连接，并且更容易确定受损的线缆。

一条逻辑总线和一个逻辑环可以被实现为一个物理的星型拓扑结构。以太网是基于总线的技术，它可以被部署为一个物理的星型拓扑结构，但是集线器设备实际上是逻辑总线连接设备。同样，令牌环是基于环的技术，它可以通过使用多站访问部件(Multistation Access Unit，MAU)被部署为一个物理的星型拓扑结构。MAU 准许线缆段被部署为星型，同时以内部的设备形成逻辑环连接。

网状型拓扑结构　网状型拓扑结构使用很多路径将一个系统与其他系统连接在一起(如图 11.12 所示)。全交叉拓扑结构将每个系统与网络中的其他所有系统都连接在一起。部分交叉拓扑结构将很多系统连接到其他很多系统。网状型拓扑结构为系统提供了冗余连接，这样，即使多个网段出现故障，也不会对连通性造成严重的影响。

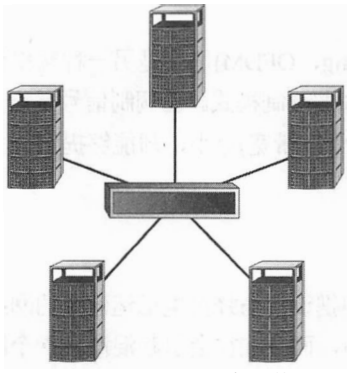


图 11.11　星型拓扑结构

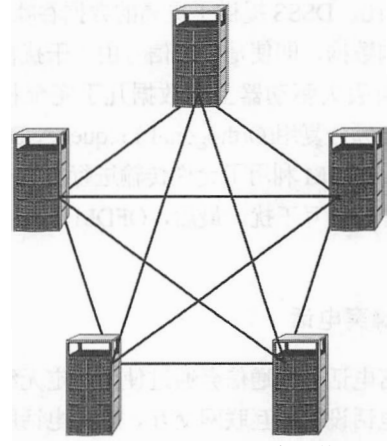


图 11.12　网状型拓扑结构

11.7.3　无线通信与安全性

无线通信是一种快速扩展的技术，这种技术用于网络连接、连通性、通信以及数据交换。从字面上看，数千种协议、标准和技术都可以被标记为无线的，其中包括蜂窝电话、蓝牙、无绳电话和无线网络。随着无线技术的持续快速增长，组织的安全性必须超出其本地网络的范围。安全性应当

是涉及通信的所有形式、方法和技术的端到端解决方案。

1. 无线的一般概念

无线通信使用无线电波远距离传输信号。无线电波频谱是有限的，因此对其使用时必须进行适当的管理，从而保证在没有干扰或干扰很小的情况下允许多个使用同时存在。无线电波频谱使用频率进行测量或区分。用频率测量波在特定时间内振动的次数(使用单位 Hz 进行确定)或者每秒的振动次数。无线电波的频率在 3Hz 到 300GHz 之间。不同的频率范围被分配给特定的用途。例如，AM 和 FM 无线电广播、VHF 和 UHF 电视等。目前，由于 900MHz、2.4GHz 和 5GHz 频率是免执照的，所以这几种频率在无线产品中是最常用的。不过，为了管理同时使用有限的无线电频率，人们开发了某些频谱使用技术。这些技术包括扩频、FHSS、DSSS 或 OFDM。

注意：

大多数设备不是在所有可用频率内运作，而是在一小部分频率内运作。这是因为需要考虑频率使用规则(美国的相应规则是 FCC)、功率消耗和对干扰的预期。

扩频指的是通信可以通过多个频率同时发生。因此，一条报文可以被分为若干片段，所有片段同时进行发送，不过每个片段都使用不同的频率。实际上，这是一种并行通信而不是串行通信。

跳频扩频(Frequency Hopping Spread Spectrum，FHSS)是扩频概念的早期实现。然而，这种技术并非以并行方式发送数据，而是以串行方式传输数据，同时不断改变所使用的频率。可用频率的整个范围都会被使用，但是每次只使用一个频率。发送者改变频率时，为了接收到信号，接收者必须遵循相同的跳频模式。FHSS 被设计用于帮助最小化干扰，而不是只使用会受到影响的单一频率。在实际使用中，通过不断切换频率，干扰就被最小化。

直接序列扩频(Direct Sequence Spread Spectrum，DSSS)以并行方式同时利用所有可用频率。与 FHSS 相比，DSSS 提供了更高的数据吞吐率。DSSS 也使用被称为碎片码的特殊编码机制来允许接收方重构数据，即使是部分信号由于干扰被破坏也同样适用。这种情况与 RAID-5 的奇偶位允许重新创建所丢失驱动器上的数据几乎完全相同。

正交频分复用(Orthogonal Frequency-Division Multiplexing，OFDM)仍然是另一种频率使用的变化形式。OFDM 利用了允许传输进行更紧密压缩的数字多载波调制模式。已调制信号是正交的，因此不会导致相互干扰。最后，OFDM 需要的频率组(也就是信道带宽)更小，却能够提供更大的数据吞吐率。

2. 蜂窝电话

蜂窝电话无线通信会通过使用特定无线电波频率组的便携设备与蜂窝电话运营商的网络以及其他蜂窝电话设备或互联网交互。蜂窝电话所使用的技术很多，而且往往会引起混淆。一个比较容易混淆的地方是 2G 和 3G 术语的使用。这些术语并非指专门的技术，而是指第几代蜂窝电话技术。因此，1G 是第一代(主要是模拟技术)，2G 是第二代(主要是数字技术，3G 和 4G 同样如此)，依此类推。当系统集成第二代和第三代技术时，我们甚至会讨论 2.5G。表 11.9 尝试澄清一些容易混淆的问题(只列出了部分无线电话技术)。

表 11.9　部分无线电话技术

技术	第几代
NMT	1G
AMPS	1G
TACS	1G
GSM	2G
iDEN	2G
TDMA	2G
CDMA	2G
PDC	2G
HSCSD	2.5G
GPRS	2.5G
W-CDMA	3G
TD-CDMA	3G
UWC	3G
EDGE	3G
DECT	3G
UMTS	3G
HSPDA	3.5G
WiMax - IEEE 802.16	4G
XOHM (WiMax 的推广名)	4G
Mobile Broadband - IEEE 802.20	4G
LTE(Long Term Evolution)	4G

这个表所列的一些技术被标记为 4G，然而它们未实际满足 4G 类技术的要求。国际电信联盟无线电通信部门(ITU-R)于 2008 年定义了 4G，但在 2010 年默许运营商可以把他们那些不满足 4G 要求的技术称为 4G 技术，只要其满足未来兼容的服务要求。在 2014 年底，5G 标准进入了人们的考虑范围。新的 5G 技术正在发展中，但截至 2015 年还没有 5G 网络进行部署并提供给公众使用。

就蜂窝电话无线传输而言，需要记住一些关键问题。首先，并非所有蜂窝电话通信数据都是语音；蜂窝电话常常被用于传输文本甚至计算机数据。其次，对于蜂窝电话提供商网络上的通信，不管是语音、文本还是数据，都不一定是安全的。再次，使用特定的无线嗅探装备能够截获蜂窝电话传输的信息。实际上，连接的服务商基站能够被模拟进而导致中间人攻击。最后，如果使用蜂窝电话连通性访问互联网或办公网络，那么攻击者甚至还可能获得其他的攻击、访问和破坏手段。这些设备中的一些能潜在地成为网桥，进而创建一条不安全的通道来进入你的网络。

接下来讨论一种重要的蜂窝电话技术：无线应用协议(Wireless Application Protocol，WAP)。WAP 不是一个标准，而是一个功能行业驱动的协议栈。借助具备 WAP 能力的设备，从蜂窝电话或 PDA 通过互联网上的蜂窝电话运营商网络和网关接入公司网络，用户就能够与公司网络通信。WAP 是一套共同工作的协议族，其中无线传输层安全(Wireless Transport Layer Security，WTLS)协议能够提供与 SSL 或 TLS 相似的安全连通性服务。

无线应用协议与无线接入点

无线应用协议因为使用同样的缩写(WAP),所以通常会和无线网络(802.11)混淆在一起。在 802.11 中，WAP 指无线接入点。记住它们之间的区别：

- 通过无线应用协议，移动设备使用移动电话网络同互联网建立通信链路。
- 通过无线网络，组织可部署自己的无线接入点，以允许组织的无线客户端连接到本地网络。

对于电信公司提供的 WAP 或其他任何安全服务来说，必须认识到一个非常重要的安全问题：我们不可能从通信服务提供商那里获得真正的端对端保护。美国的通信协助法律实施法案(CALEA)授权：只要能出示搜查证，无论涉及任何技术的所有电信公司都必须允许能够窃听语音和数据通信。因此，电信公司无法为客户提供端到端的加密。在通信路径上的某些位置，通信数据必须被恢复为明文形式，随后在到达目的地的余下路径上才被重新置为安全形式。WAP 按照下面的方式遵循 CALEA 法律：在移动的设备与电信公司使用 WAP/WTLS 的主服务器之间建立一个安全链接；在能够被重新封装入 SSL、TLS、IPSec 以便继续传输至其预期的目的地之前，数据会被转换为明文形式。知道这个问题之后，我们可以适当地使用电信服务，尽可能地在电信公司链接中传输预先加密的数据，而不是传输未加密的明文数据。

WAP 1.0 在 1999 年开始应用于大多数欧洲移动电话。WAP 2.0 发布于 2002 年。今天，极少部分移动电话仍使用 WAP。在 3G 和 4G 技术(包括 GSM、EDGE、HPDSA 和 LTE)中，这个机制用于支持移动电话和互联网之间的 TCP/IP 通信。

3. 蓝牙(802.15)

蓝牙或 IEEE 802.15 个人局域网(PAN)是与无线安全性有关的另一个区域。蜂窝电话的听筒、麦克风、鼠标、键盘、GPS 设备以及其他许多接口设备和外围设备都通过蓝牙连接。许多这样的连接都使用被称为配对的技术来建立，使用这种技术时，主设备通过扫描 2.4GHz 无线电频率来查找可用的设备，随后一旦发现存在可用的设备，就会使用一个 4 位的 PIN 来“授权”配对。这个过程确实可以减少偶然配对的数量，但是 4 位 PIN 并不安全(更不用说默认的 PIN，往往为 0000)。此外，被称为蓝牙劫持的技术能够在你不知情的情况下配对你的设备，并且可以使用这些设备，或者可以从这些设备中提取信息。这种攻击形式能够使攻击者访问你的联系人列表、数据甚至谈话。蓝牙窃听这种攻击允许黑客远程控制蓝牙设备的特性和功能。这可能包括打开麦克风的能力，使用手机作为音频监控。幸运的是，蓝牙通常只具有 30 英尺的限定范围，不过某些设备在 100 米之外也能够运作。虽然蓝牙使用了加密，但并不是动态加密，而且往往通过适当的工作就能够破解。蓝牙用于非敏感或非机密的活动。只要有可能，最好修改设备的默认 PIN。不要使设备停留在发现模式，在没有活动使用时总是关闭蓝牙。

4. 无绳电话

无绳电话存在往往被忽视的安全问题。无绳电话被设计使用任何一个免执照频率(也就是 900MHz、2.4GHz 或 5GHz)。许多不同类型的设备都使用了这三个免执照频率，包括无绳电话、婴儿监视器、蓝牙设备和无线网络连接设备。常常被忽视的问题是：因为信号极少加密，所以无绳电话很容易被偷听。使用频率扫描仪，任何人都能够监听你的谈话。

5. 移动设备

智能手机和其他移动设备正显示出不断增加的安全风险，因为它们变得越来越能够与互联网以及企业网络进行交互。移动设备通常支持内存卡，并且可能会将恶意代码注入或将机密数据带出企业。许多移动设备还支持 USB 连接桌面终端或笔记本电脑以进行同步通信，例如传输文件、文档、音乐、视频等。设备本身通常包含敏感数据，例如通信录、短信、电子邮件，甚至记录和文件。

移动设备的遗失或失窃意味着个人和企业机密的破坏。

移动设备已成为黑客和恶意代码的攻击目标。不在移动设备上保存敏感信息是十分重要的。在设备上运行防火墙和防病毒产品(如果可提供的话)并且保持系统锁定或加密(如果可行的话)。

此外，移动设备无法避免窃听。使用正确类型的精良设备，大多数移动电话可以被窃听，更不用说事实上 15 英尺范围内的任何人都可以听到你说话。员工应该被培训在公共场所谨慎使用手机进行谈论。

在移动设备上可提供广泛的安全功能。然而，支持安全功能与合理配置及启用不是一样的事情，只有当强制使用安全功能时，安全的好处才能获得。请务必检查所有允许连接到组织网络上任意设备的所有需要的安全功能按预期要求运行。

注意：

属于个人的设备可以是以下任意类型：便携式设备、移动设备、个人移动设备(PMD)、个人电子设备或便携式电子设备(PED)以及个人拥有设备(POD)。

关于管理移动设备安全性的更多信息请参见第 9 章“安全脆弱性、威胁和对策”，特别是“评估和减轻移动系统的脆弱性”一节。

11.7.4　LAN 技术

LAN(局域网)技术存在三种主要类型：以太网、令牌环和 FDDI。虽然还存在其他少数局域网技术，但是它们的使用不如这三种类型广泛。此外，CISSP 考试仅涉及这三种主要类型。LAN 技术之间的大多数差别存在于数据链路层及其以下层。

1. 以太网

以太网是一种共享介质的 LAN 技术，也称为广播技术。这意味着它准许很多设备在相同的介质上进行通信，但是要求每台设备轮流通信并且执行冲突检测和避免操作。以太网采用广播域和冲突域。广播域是一个物理的系统组，这个组中的所有系统成员都会接收到由组中单个系统发送的广播。广播是传输到特定地址的消息，它指示所有的系统都是预计的接收者。

冲突域包含若干系统组，在冲突域内，如果两个系统同时进行传输，就会发生数据冲突。当两条被传输的消息企图同时使用网络介质时，就会出现数据冲突，这会导致其中一条或两条消息出现讹误。

以太网可以支持全双工通信(也就是完全双向的通信)，并且往往使用同轴电缆或双绞线连接。以太网最常在星型或总线型拓扑上部署。以太网基于 IEEE 802.3 标准。单独的以太网数据单元被称为帧。快速以太网能够支持 100Mbps 吞吐量。千兆以太网则能支持 1000Mbps(1Gbps)吞吐量。万兆以太网则能支持 10 000Mbps (10Gbps)吞吐量。

2. 令牌环

令牌环采用令牌传递机制来控制哪些系统可以在网络介质上传输数据。令牌在 LAN 所有成员形成的逻辑环上进行传递。令牌环可以采用环型或星型网络拓扑。由于令牌环的性能有限，比起以太网来说成本又高，而且会增加部署和管理的难度，今天已极少使用。

令牌环可通过使用多站访问组件(MAU)部署物理星型结构。MAU允许电缆段部署为星型结构，同时内部设备使用逻辑令牌连接。

3. 光纤分布式数据接口(FDDI)

光纤分布式数据接口(FDDI)是一种使用两个环的高速令牌传递技术，其中信息流在两个环上沿相反的方向传输。FDDI 常用作大型企业网络的主干，它的双环设计允许实现自愈，即从环中去除故障网段，并且利用剩下的部分内部环和外部环建立单个环。虽然 FDDI 价格昂贵，但是在快速以太网和千兆以太网出现之前常常被用在校园环境中。价格稍便宜、距离有限且速度更慢的版本称为铜线分布式数据接口(CDDI)。CDDI 也更容易遭到干扰和偷听。

4. 辅助技术

大多数网络并非只包含一种技术，而是包含众多技术。例如，以太网并不只是一个单独的技术，而是支持其通用以及预期活动和行为的多个辅助技术的超集。以太网包括数字通信、同步通信和基带通信技术，并且支持广播、多播和单播通信以及带有冲突检测的载波侦听多路存取(Carrier-Sense Multiple Access with Collision Detection，CSMA/CD)。许多 LAN 技术，例如以太网、令牌环和 FDDI 都可能包括下面所介绍的辅助技术。

5. 模拟和数字

对于许多网络通信形式来说，常见的一种辅助技术是在物理介质(例如，线缆)上实际传输信号所使用的机制。传输机制分为两种类型：模拟和数字。

- 使用频率、幅度、相位、电压等发生变化的连续信号时，就会进行模拟通信。连续信号的差异会产生波形(与数字信号的方波形成对照)。连续信号的差异导致实际通信的发生。
- 通过使用非连续的电子信号以及状态改变或开关脉冲，就会出现数字通信。

在长距离传输或存在干扰时，数字信号比模拟信号更可靠。这是因为数字信号的既定信息存储方法利用了直流电压，其中有电压代表值 1，无电压代表值 0。这些开关脉冲创建了一个二进制数据流。由于长距离传输和干扰所造成的衰减，模拟信号会发生变化和讹误。与数字信号只有两种状态相比，模拟信号具有无限多的变化被用于信号编码，因此在衰减增长时，对信号的多余更改会导致数据抽取工作更加困难。

6. 同步和异步

某些通信使用时钟或定时活动进行同步。通信既可以是同步的，也可以是异步的。

- 同步通信依赖于定时或时钟机制，这种机制基于独立的时钟或数据流内嵌的时间标记。同步通信通常能够支持非常高速的数据传送。

- 异步通信依赖于停止和开始定界位来管理数据的传输。因为使用了定界位以及传输的停止和开始特征，所以异步通信最适用于数据量较少的传输。公用电话交换网(PSTN)调制解调器就是异步通信的一个绝佳示例。

7. 基带和宽带

在一个线缆段上能够同时发生的通信数取决于使用的是基带技术还是宽带技术。

- 基带技术只能支持单个通信信道，它使用直流电应用于线缆，其中有电流表示二进制信号 1，无电流表示二进制信号 0。基带是一种数字信号形式。以太网就是基带技术。
- 宽带技术能够支持多个同时发生的信号。宽带使用频率调制来支持许多信道，每个信道都支持一个截然不同的通信会话。宽带适用于高吞吐率，尤其适用于若干信道复用的情况。宽带是一种模拟信号形式。有线电视和线缆调制解调器、ISDN、DSL、T1 以及 T3 都是宽带技术的示例。

8. 广播、多播和单播

另一种辅助技术确定了单个传输能够到达的目的地数量，具体的选项是广播、多播和单播。

- 广播技术支持与所有可能的接收者进行通信。
- 多播技术支持与多个特定的接收者进行通信。
- 单播技术只支持与某个特定接收者的单一通信。

9. LAN 介质访问

最后要介绍的是，至少有 5 种 LAN 介质访问技术用来避免或阻止传输冲突。这些技术定义了所有位于相同冲突域内的多个系统如何进行通信，其中一些技术主动防止冲突，另外一些技术则对冲突做出响应。

载波侦听多路存取(CSMA)　这是一种使用下列步骤进行通信的 LAN 介质访问技术：

(1) 主机侦听 LAN 介质，从而确定 LAN 介质是否正在使用。

(2) 如果 LAN 介质未被使用，那么主机就传输其通信数据。

(3) 主机等待确认信号。

(4) 如果超时未接收到确认信号，那么主机从步骤(1)开始重新执行操作。

CSMA 并不直接解决冲突。如果发生冲突，那么通信就不成功，因此也不会接收到确认信号。这样会导致发送系统重新传输数据和重新执行 CSMA 过程。

带有冲突避免的载波侦听多路存取(CSMA/CA)　这是一种使用下列步骤进行通信的 LAN 介质访问技术：

(1) 主机具有两个与 LAN 介质的连接：入站连接和出站连接。主机侦听入站连接，从而确定 LAN 介质是否正在使用。

(2) 如果 LAN 介质未被使用，那么主机就请求传输特权。

(3) 如果超时之后仍未获得特权，那么主机从步骤(1)开始重新执行操作。

(4) 如果被授予特权，那么主机就通过出站连接传输其通信数据。

(5) 主机等待确认信号。

(6) 如果超时之后仍未收到确认信号，那么主机从步骤(1)开始重新执行操作。

AppleTalk和 802.11 无线网络连接是利用CSMA/CA技术的网络例子。CSMA/CA试图通过在任意

指定时间内只授予单个通信特权来避免冲突。CSMA/CA系统要求指定一个主系统，这个主系统能够响应请求以及授予发送数据传输的特权。

带有冲突检测的载波侦听多路存取(CSMA/CD) 这是一种使用下列步骤进行通信的 LAN 介质访问技术：

(1) 主机侦听 LAN 介质，从而确定 LAN 介质是否正在使用。

(2) 如果 LAN 介质未被使用，那么主机就传输其通信数据。

(3) 在数据传输的同时，主机侦听冲突(也就是两台或多台主机同时传送数据的情况)。

(4) 如果检测到冲突，那么主机就会传输一个停发信号。

(5) 如果接收到停发信号，所有主机都会停止数据传输。每台主机都会等待一个随机的时间周期，然后从步骤(1)开始重新执行操作。

以太网利用了 CSMA/CD 技术。通过使冲突域的每个成员在重新开始传输过程之前都进行随机的短时间等待，CSMA/CD 可以响应冲突。遗憾的是，准许冲突发生以及随后对冲突的响应或反应会导致传输延迟以及要求重复传输，这会导致损失 40%左右的潜在吞吐量。

令牌传递 这是一种使用数字令牌进行通信的 LAN 介质访问技术。持有令牌的主机有权传输数据。一旦传输完成，主机就会将令牌释放给下一个系统。令牌传递用在令牌环网络中，例如 FDDI。由于持有令牌的系统才有权传输数据，因此令牌环能够防止冲突。

轮询 这是一种使用主从配置进行通信的 LAN 介质访问技术。一个系统被标记为主系统，其他所有系统则被标记为从属系统。主系统依次轮询或了解每个从属系统是否需要传输数据。如果某个从属系统表达了这种需求，那么就会被授予传输数据的特权。一旦该系统的传输结束，主系统就继续轮询下一个从属系统。同步数据链接控制(SDLC)就使用了轮询。

轮询通过使用许可系统来解决冲突。轮询是 CSMA/CA 方法的逆过程。虽然二者都使用主从结构，但是 CSMA/CA 允许从系统请求特权，而轮询则由主系统提供特权。轮询可以被配置为授予某个(或多个)系统具有比其他系统更高的优先权。例如，如果标准的轮询模式为 1、2、3、4，那么就可以指定系统 1 优先，轮询模式相应会变化为 1、2、1、3、1、4。

11.8 本章小结

在网络中设计、部署和维护安全性需要熟悉涉及网络连接的各种技术，这些技术包括协议、服务、通信机制、拓扑结构、线缆、端点和网络连接设备。

OSI 模型是一个对所有协议进行评估的标准。理解 OSI 模型是如何运用的以及如何应用于现实中的协议，有助于系统设计者和系统管理员改善系统的安全性。TCP/IP 模型直接起源于协议并大致对应 OSI 模型。

大多数网络采用 TCP/IP 作为主要的协议。然而，在 TCP/IP 网络中还存在许多子协议、支持协议、服务和安全机制。对于这些不同实体的基本理解有助于设计和部署安全的网络。

除了路由器、集线器、交换机、中继器、网关和代理之外，防火墙也是网络安全性的重要组成部分。防火墙有 4 种主要类型：静态数据包过滤、应用级网关、电路级网关以及状态检测。

汇聚协议在现代网络中是很常见的，包括 FCoE、MPLS、VoIP 和 iSCSI。软件定义网络和内容分发网络已经扩大了网络的定义，还扩大了网络的使用。广泛的硬件组件可以用来构建网络，而不仅仅是通过布线来将所有设备绑定到一起。了解每种布线类型的优点和缺点是设计安全网络的一部分。

无线通信有许多形式，包括手机、蓝牙(802.15)和网络(802.11)。无线通信更容易受到干扰、窃听、拒绝服务、中间人攻击。

有三个局域网技术在 CISSP CIB 中提到：以太网、令牌环和 FDDI。每个都可以被用来部署安全的网络。也有几个常见的网络拓扑结构：环型、总线型、星形型和网格型。

11.9　考试要点

了解 OSI 模型的各层和每一层所使用的协议。OSI 模型的 7 层以及各层所支持的协议如下：

- 应用层：HTTP、FTP、LPD、SMTP、Telnet、TFTP、EDI、POP3、IMAP、SNMP、NNTP、S-RPC 和 SET。
- 表示层：加密协议(例如，RSA 和 DES)与格式化类型(例如，ASCII、EBCDICM、TIFF、JPEG、MPEG 和 MIDI)。
- 会话层：NFS、SQL 和 RPC。
- 传输层：SPX、SSL、TLS、TCP 和 UDP。
- 网络层：ICMP、RIP、OSPF、BGP、IGMP、IP、IPSec、IPX、NAT 和 SKIP。
- 数据链路层：SLIP、PPP、ARP、RARP、L2F、L2TP、PPTP、FDDI 和 ISDN。
- 物理层：EIA/TIA-232、EIA/TIA-449、X.21、HSSI、SONET、V.24 和 V.35。

全面了解 TCP/IP。了解 TCP 和 UDP 之间的差异。熟悉 4 个 TCP/IP 层及其与 OSI 模型的对应关系。此外，还要理解知名端口的使用，并且熟悉相关的子协议。

了解不同的线缆类型及其长度和最大吞吐率。线缆连接类型包括 STP、10Base-T(UTP)、10Base2(细缆)、10Base5(粗缆)、100Base-T、1000Base-T 和光纤。还应当熟悉从 1 类到 7 类的 UTP。

熟悉常用的 LAN 技术。常用的 LAN 技术是以太网、令牌环和 FDDI。此外还应当熟悉：模拟通信与数字通信；同步通信与异步通信；基带通信与宽带通信；广播、多播和单播通信；CSMA、CSMA/CA 和 CSMA/CD；令牌传递；轮询。

了解安全的网络体系结构和设计。网络安全应考虑 IP 和非 IP 协议、网络访问控制、使用安全的服务和设备、管理多层协议以及实现端点安全。

了解网络分段的各种类型和目的。网络分段可以用来管理流量、提高性能并加强安全性。网络分段或子网的例子包括内部网、外部网和 DMZ。

了解不同的无线技术。手机、蓝牙(802.15)和无线网络(802.11)都称为无线技术，即使它们是完全不同的。了解它们的差异、优势和弱点。了解安全 802.11 网络的基础知识。

了解光纤通道。光纤通道是一种网络数据存储解决方案(例如 SAN(存储区域网络)或 NAS(网络附加存储))，允许高速文件传输。

了解 FCoE。FCoE(以太网光纤通道)用来封装光纤通道中的以太网网络通信。

了解 iSCSI。iSCSI(互联网小型计算机系统接口)是一个基于 IP 的网络存储标准。

了解 802.11 和 802.11a、b、g、n 和 ac。802.11 是 IEEE 标准的无线网络通信。版本包括 802.11(2Mbps)、802.11a(54Mbps)、802.11b(11Mbps)、802.11g(54Mbps)、802.11n(600Mbps)和 802.11ac (1.3+Mbps)。802.11 标准定义了有线等效保密(WEP)。

了解现场勘测。现场勘测是调查环境中的位置和信号强度以达到部署无线接入点所需条件的过程。这个任务通常涉及利用便携式无线设备进行步行探寻以观测无线信号的强度，并映射这一场景

或建筑的示意图。

了解 WPA。WEP 的早期选择 WPA。这种技术虽有改进但本身仍是不完全可靠的。它基于 LEAP 和 TKIP 密码体系并使用一个密码短语。

理解 WPA2。WPA2 是一种新的加密方案，称为计数器模式密码块链接消息认证码协议(CCMP)，是基于 AES 的加密方案。

了解 WEP。有线等效保密(WEP)是由 IEEE 802.11 定义的标准，目的是在无线网络上提供等同于有线或有线网络同一水平的安全和加密。WEP 提供对抗数据包嗅探和窃听攻击的无线传输保护。WEP 的第二个好处是能够防止未经授权的无线网络访问。WEP 使用预定义的共享密钥。

了解 EAP。EAP(可扩展认证协议)不是一个特定的认证机制；它是一个认证框架。实际上，EAP 允许新的认证技术与现有的无线或点对点连接技术相兼容。

了解 PEAP。PEAP(受保护的可扩展认证协议)通过 TLS 隧道封装 EAP，提供了认证和加密的可能性。

了解 LEAP。LEAP(轻量级可扩展认证协议)是 Cisco 专有的，用于 WPA 替代 TKIP。协议的设计是为了在 802.11i/WAP2 被批准为标准之前以应对 TKIP 的不足。

了解 MAC 过滤。MAC 过滤器是一个授权的无线客户端接口 MAC 地址列表，用于无线接入点以阻止所有非授权设备的访问。

了解 SSID 广播。无线网络定期在一个称为信标帧的特殊数据包内公布它们的 SSID。当 SSID 进行广播时，具有自动检测和连接的任何设备不仅能够看到网络，也可以主动与网络进行连接。

了解 TKIP。TKIP(临时密钥完整性协议)被设计用于替代 WEP 且不需要更换传统的无线硬件。TKIP 在 802.11 无线网络中得到应用并被称为 WPA(Wi-Fi Protected Access)。

了解 CCMP。设计 CCMP(计数器模式密码块链接消息认证码协议)是为了取代 WEP 和 TKIP/WPA。CCMP 使用 AES(高级加密标准)和 128 位的密钥。

了解强制门户。强制门户是一个认证技术，它将一个新的无线 Web 客户端连接重定向到一个访问控制接口页面。

了解天线的类型。各种类型的天线可用于无线客户端和基站。这些天线包括全向天线以及许多定向天线，如 Yagi 天线、cantenna 天线、面板天线和抛物线天线。

了解现场勘测。现场勘测使用 RF 信号探测器对无线信号的强度、质量和干扰进行正式评估。

了解标准的网络拓扑结构。有环型、总线型、星型和网状型几类。

了解常用的网络设备。常用的网络设备包括防火墙、路由器、集线器、桥、中继器、交换机、网关和代理。

理解不同类型的防火墙。防火墙有 4 种基本类型：静态的数据包过滤、应用级网关、电路级网关以及状态检测防火墙。

了解用于连接 LAN 和 WAN 通信技术的协议服务。它们是帧中继、SMDS、X.25、ATM、HSSI、SDLC、HDLC 和 ISDN。

11.10 书面实验室

1. 说出 OSI 模型各层的名字并以数字形式对从顶部到底部的各层进行编号。
2. 说出布线中的三个问题以及应对这些问题的方法。

3. 在无线设备中最大化地使用可用无线电频率的技术有哪些？
4. 讨论用于保护 802.11 无线网络的方法。
5. 如果知情，说出局域网共享介质访问技术和使用它们的示例。

11.11　复习题

1. 下列哪一层是 OSI 模型的第 4 层?
   A. 表示层
   B. 网络层
   C. 数据链路层
   D. 传输层
2. 什么是封装?
   A. 改变数据包的源地址和目标地址
   B. 当数据在 OSI 模型中向下移动时增加报头和报尾
   C. 验证一个人的凭证
   D. 保护证据，直到它们已经被恰当收集
3. OSI 模型的哪一层用简单模式、半双工模式、全双工模式管理通信？
   A. 应用层
   B. 会话层
   C. 传输层
   D. 物理层
4. 以下哪一个最不能抵抗 EMI?
   A. 细缆
   B. 10Base-T UTP
   C. 10Base5
   D. 同轴电缆
5. 以下哪一个不是网络分段的示例？
   A. 内部网
   B. DMZ
   C. 外部网
   D. VPN
6. 以下哪一个不是非 IP 协议?
   A. IPX
   B. UDP
   C. AppleTalk
   D. NetBEUI
7. 如果你是 bluejacking 攻击的受害者，以下哪个设备被攻陷了？
   A. 防火墙
   B. 交换机

C. 蜂窝电话

D. web cookies

8. 下列哪个网络技术基于 IEEE 802.3 标准?

A. 以太网

B. 令牌环

C. FDDI

D. HDLC

9. 什么是 TCP 包装器?

A. 一个在交换机上使用的封装协议

B. 一个应用，可以作为基本的防火墙功能并通过用户 ID 和系统 ID 来实现访问控制

C.一个安全协议，用于在 WAN 链路上保护 TCP/IP 通信

D. 一个 TCP/IP 隧道机制，用于非 IP 网络

10. 什么是多层协议具备的优点，同时也是潜在的威胁？

A. 吞吐量

B. 封装

C. 哈希完整性检测

D. 逻辑地址

11. 通过检查源地址和目标地址、应用程序使用情况、来源以及同一会话中前数据包和当前数据包之间的关系，_____防火墙能够授予广泛的访问授权并积极监视用户，以及活动和阻止未经授权的用户和活动。

A. 静态数据包过滤

B. 应用级网关

C. 状态检查

D. 电路级网关

12. _____ 防火墙是第三代防火墙。

A. 应用级网关

B. 状态检测

C. 电路级网关

D. 静态数据包过滤

13. 关于防火墙，下列哪一项不是正确的？

A. 它们都能够记录流量信息。

B. 它们能阻隔病毒。

C. 它们能基于可疑攻击发出问题警报

D. 它们仍不能防止内部攻击

14. 以下哪个不是可路由协议?

A. OSPF

B. BGP

C. RPC

D. RIP

15. _____ 是智能集线器，因为它知道在每个出站端口上连接的系统的地址。它不是重复每个出站端口上的流量，而只重复目的地已知的出站流量。

A. 中继器

B. 交换机

C. 桥

D. 路由器

16. 下列哪一项不是 802.11 无线网络相关的技术？

A. WAP

B. WPA

C. WEP

D. 802.11i

17. 哪种无线频率访问方法提供不受干扰的最大吞吐量？

A. FHSS

B. DSSS

C. OFDM

D. OSPF

18. 什么安全概念鼓励管理员在每台主机上安装防火墙、防病毒扫描器和 IDS？

A. 端点安全

B. 网络访问控制(NAC)

C. VLAN

D. RADIUS

19. RARP 执行什么功能？

A. 它是一种路由协议。

B. 它将 IP 地址转换为 MAC 地址。

C. 它将物理地址解析成逻辑地址。

D. 它管理多重流。

20. 在大型的物理环境中，无线网络部署何种形式的基础设施模式支持众多接入点只使用单一的 SSID？

A. 独立

B. 有线扩展

C. 企业扩展

D. 桥

第 12 章

安全通信和网络攻击

本章中覆盖的 CISSP 考试大纲包含：

4) 通信与网络安全(设计和保护网络安全)

- C. 设计和建立安全通信信道
  - C.1 语言
  - C.2 多媒体协助(例如，远程会议技术、即时通信)
  - C.3 远程访问(例如，VPN、屏幕截取、虚拟应用/桌面、远程办公)
  - C.4 数据通信(例如，VLAN、TLS/SSL)
  - C.5 虚拟网络(例如，SDN、虚拟 SAN、访客操作系统、端口隔离)
- D. 阻止和缓解网络攻击

对以静态形式驻留在存储设备中的数据进行安全保护是相当简单的。只要维持物理访问控制并实现适当的逻辑访问控制，保持存储文件的机密性和完整性对于已授权的用户来说还是可行的。然而，一旦数据被应用程序使用或在网络连接上进行传输，那么对数据进行安全保护的过程就变得困难多了。

通信安全性包括很广泛的问题，这些问题涉及将电子信息从一处传送到另一处。通信可能发生于两个地方的系统之间，也可能发生于同一商业网络的系统之间。一旦涉及传输方式，数据在面对机密性、完整性和可用性的过多威胁时会变得极易遭受破坏。幸运的是，很多这样的威胁都能够通过正确的对策得以减轻或消除。

通信安全性被设计用于检测、防止甚至纠正数据传输错误(也就是完整性保护)。在网络支持数据的交换和共享时，通信安全性维护了网络的安全性。本章会涉及通信安全性、脆弱性和对策的许多内容。

在 CISSP 认证考试中，通信与网络安全域涉及网络组件(例如网络设备和协议)的相关主题、它们具体是如何作用的以及它们和安全的相关性。该域在本章和第 11 章中进行讨论。一定要阅读和研究这两章中的材料以保证 CISSP 认证考试的必备材料得以完全覆盖。

12.1 网络与协议安全机制

TCP/IP 是在大多数网络和互联网上使用的主要协议。但是，这种健全的协议也存在许多安全缺陷。在改善 TCP/IP 安全性的努力中，人们开发了很多子协议、机制或应用程序，从而能够保护传输数据的机密性、完整性和可用性。记住下面这一点十分重要：即使是 TCP/IP 的单个基础协议，也仍然存在数百个(否则数千个)单独的用于互联网的协议、机制和应用程序，它们中的某些被设计用于提供安全性服务。某些能够保护完整性，某些能够保护机密性，其他一些则可以提供身份认证和访问控制。接下来，我们将讨论一些较常见的网络和协议安全机制。

12.1.1 安全通信协议

为特定应用通信信道提供安全服务协议被称为安全通信协议。下面列出了一些常见的安全通信协议：

IP 简单密钥管理(Simple Key Management for Internet Protocol，SKIP) 这是一种用于保护无会话数据报协议的加密工具。SKIP 被设计为与 IPSec 相结合，并且在 OSI 模型的第 3 层上工作。SKIP 能够对 TCP/IP 协议族的任何子协议进行加密。SKIP 在 1998 年被互联网密钥交换(Intemet Key Exchange，IKE)代替。

软件 IP 加密(software IP encryption，swIPe) 这是另一种第 3 层 IP 安全协议。它通过使用封装协议来提供身份认证、完整性和机密性。

安全远程过程调用(S-RPC) 这是一种身份认证服务，并且只是防止在远程系统上在未经授权的情况下执行代码的手段。

安全套接字层(SSL) 这是一种由 Netscape 开发的加密协议，目的是保护 Web 服务器和 Web 浏览器之间的通信。SSL 可以被用于保护 Web、电子邮件、FTP 甚至 Telnet 通信的安全。SSL 是一个面向会话的协议，提供了机密性和完整性。SSL 使用 40 位密钥或 128 位密钥进行部署。

传输层安全(TLS) TLS 的功能类似于 SSL，但使用更健壮的认证和加密协议。

SSL 和 TLS 都有以下功能特性：

- 支持在不安全的网络中提供安全的客户端-服务器通信，并防止篡改、欺骗和窃听。
- 支持单向认证。
- 使用数字证书支持双向认证。
- 通常实现为一个 TCP 包的初始载荷，允许它封装所有的更高层协议的有效载荷。
- 可以应用在低层，比如在第 3 层(网络层)作为 VPN，这被称为 OpenVPN。

此外，TLS 能用于加密 UDP 和会话初始协议(Session Initiation Protocol，SIP)连接(SIP 是一个和 VoIP 有关联的协议)。

安全电子交易(Secure Electronic Transaction，SET) 这是一种在互联网上进行交易传输时所使用的安全协议。SET 的基础是 RSA 加密以及数据加密标准(DES)。主要的信用卡公司都支持 SET，例如 Visa 和 MasterCard。然而，SET 没有被互联网广泛接受；相反，由 SSL/TLS 加密的会话是安全电子商务的首选机制。

注意：

上述 5 种安全通信协议(SKIP、swIPe、S-RPC、SSL/TLS 和 SET)只是一些可用的选项示例。记

住还有许多其他的安全协议，如 IPSec 和 SSH。

12.1.2　身份认证协议

在远程系统和服务器(或网络)之间开始建立连接之后，第一个进行的操作应当是验证远程用户的身份，这个操作被称为身份认证。下面列出了一些身份认证协议，这些协议能够控制如何交换登录凭证以及在传输过程中是否对登录凭证进行加密：

挑战握手身份认证协议(Challenge Handshake Authentication Protocol，CHAP)　这是在 PPP 链接上使用的一种身份认证协议。CHAP 对用户名和密码进行加密，通过使用不能重放的挑战-响应对话来执行身份认证操作。在建立的通信会话持续期间，CHAP 也会定期对远程系统重新进行身份认证，从而认证远程客户端的持久性身份。这个活动对用户是透明的。

密码身份认证协议(Password Authentication Protocol，PAP)　这是一种用于 PPP 的标准身份认证协议。PAP 以明文的形式传递用户名和密码。PAP 没有提供任何形式的加密；只是简单地提供了一种从客户端向身份认证服务器传输登录凭证的手段。

可扩展身份认证协议(Extensible Authentication Protocol，EAP)　这是一个身份认证架构，而不是一种实际的协议。EAP 允许自定义身份认证安全解决方案，例如支持智能卡、令牌和生物测定学(参见下方“EAP、PEAP 和 LEAP”中关于基于 EAP 的其他协议)。

上述三种身份认证协议最初用在拨号 PPP 连接上。现在，大量的远距离连接技术(包括宽带和 VPN)都应用了这些协议与其他很多较新的身份认证协议和概念。

EAP、PEAP 和 LEAP

受保护的可扩展认证协议(PEAP)将 EAP 封装在一条 TLS 隧道中。PEAP 优于 EAP 是因为 EAP 假设信道已经被保护，但是 PEAP 实施自己的安全措施。PEAP 在 802.11 无线连接上用于保障通信安全。PEAP 可以采用 WPA 和 WPA-2 连接。

PEAP 也优于思科专有的 EAP，即轻量级的 EAP 协议(LEAP)。LEAP 是思科对不安全 WEP 的初始响应。LEAP 支持频繁的再认证和 WEP 密钥的变化(WEP 使用单个认证和一个静态密钥)。然而，LEAP 可以被各种工具和技术进行破解，包括漏洞利用工具 Asleap。

12.2　安全的语音通信

语音通信的脆弱性与 IT 系统安全无关。然而，随着语音通信解决方案开始通过使用数字设备和 IP 语音(VoIP)技术在网络上加以应用，保护语音通信的安全就变成了日益重要的问题。当语音通信在 IT 基础设施上发生时，实现能够提供身份认证和完整性的机制就十分重要。要维护机密性，就必须在传输时采用加密服务或协议来保护语音通信。

常规的专用分支交换(Private Branch Exchange，PBX)或 POTS/PSTN 语音通信容易遭受截获、偷听、分机窃听和其他利用。对组织物理位置范围内的语音通信的控制往往要求维护物理安全性。组织外部的语音通信安全通常是提供租用服务的电话公司的职责。如果语音通信的脆弱性对于支撑安全策略来说是个重要的问题，就应当部署语音通信专用的加密通信机制。

12.2.1 互联网语音协议(VoIP)

VoIP 是一种将语音封装成 IP 数据包，并支持音频电话通过 TCP/IP 网络进行连接的技术。VoIP 已经成为企业和个人一种流行和廉价的电话解决方案。

选择 VoIP 解决方案时保持安全性，确保 VoIP 提供你所期望的隐私性和安全性，是十分重要的。一些 VoIP 系统本质上是纯明文形式的通信，这将容易被拦截和窃听；其他系统是高度加密的，这将阻止和挫败任何干扰或窃听企图。

VoIP 并不是没有问题。黑客可以用众多潜在的攻击方式来攻击 VoIP 解决方案：

- 呼叫 ID 可以轻易被任意 VoIP 工具进行伪造，因此黑客可以执行语音钓鱼(VoIP 钓鱼)攻击或在网络中进行语音垃圾邮件(SPIT)攻击。
- 呼叫管理系统和 VoIP 电话本身的漏洞可能会使它们容易受到 OS 攻击和 DoS 攻击。如果设备或软件的主机操作系统或固件有漏洞，离黑客攻击往往也就不远了。
- 黑客可能会通过欺骗呼叫经理或终端用户进行协商或回应的方式发动中间人(MitM)攻击。
- 根据部署方式，在交换机中部署VoIP电话也有类似部署桌面终端和服务器系统相同的风险。这可能导致发生类似 VLAN 中的 802.1x 认证证伪和 VoIP 跳跃(跳过验证通道)。
- 由于VoIP流量也是网络流量，对于不加密的VoIP流量可以通过解码的方式来窃听VoIP通信。

12.2.2 社会工程学

怀有恶意的个人可以通过名为社会工程学的技术来利用语音通信。社会工程学是不认识的人获得组织内部某个人信任的一种方式。擅长社会工程学的人可以使员工相信他们是上层管理人员、技术支持人员、咨询人员等。一旦获得信任，受害者常常会被怂恿在系统中修改他们的用户账户，例如重新设置密码。其他攻击包括指示受害者打开特定的电子邮件附件、启动某个应用程序或者连接特定的 URL。无论实际的活动是什么，这种攻击总是有目的性地打开一个后门，从而使攻击者利用后门获得网络的访问权限。

组织内的人使得公司容易受到社会工程学攻击。仅仅是一点点信息或一些事实，就常常可能使得受害者透露机密信息或从事不负责任的活动。社会工程学攻击利用了人类的一些特点，例如，对别人的基本信任以及懒惰。忽略差异、心不在焉、遵从命令、假设别人知道的比他们实际做的多、愿意帮助别人以及害怕受到训斥也可能导致社会工程学攻击。由于受害者从内部开放了访问路径，并且在安全屏障上有效地打通了一个入口，因此攻击者常常能够避开广泛的物理和逻辑安全控制。

真实场景

社会工程学的魔力

社会工程学是一个极富吸引力的主题。社会工程学是能够进入技术几乎完美的安全环境的途径，是针对组织内部人员进行攻击的技巧。虽然 CISSP 考试不涉及这方面的内容，但是通过许多优秀的、与社会工程学相关的资源、示例和讨论，不仅可以增强对这种安全问题的防范意识，而且还会觉得极为有趣。可以通过搜索术语“社会工程学”来搜寻相关的书籍与在线视频，说不定你会沉迷于这些信息或视频示例。

防止社会工程学攻击的唯一途径是教会用户如何应对和沟通只有语音的通信。下面给出了一些指导原则：

- 在语音通信显得奇怪、不恰当或意外时，务必始终保持谨慎。
- 总是要求提供身份证明。身份可以是驾照号或社会保险号，这些号码很容易进行验证。此外还可以采取这样的方式：在办公室内找一个能够识别呼叫者声音的人来接听呼叫。例如，如果呼叫者声称自己是部门经理，那么可以通过请求其管理助手来接听呼叫，以便确认呼叫者的身份。
- 对所有只有语音的网络更改或活动请求，都要求回叫授权。当初始客户端连接断开时，回叫授权就发生了，并且服务器为了执行第二轮认证，以预定数量回呼客户端。
- 对信息(用户名、密码、IP 地址、经理名字、拨入号码等)进行分类，并明确指出在语音通信中可以讨论甚至确认什么信息。
- 如果某人在电话中请求秘密的信息，而这个人应当知道在电话中提供特定信息违反了公司的安全策略，那么就必须询问为什么需要这些信息并再次验证其身份。此外，这件事还应该报告给安全管理员。
- 永远不要基于只有语音的通信分发或更改密码。
- 始终安全地处理或销毁所有的办公室文档(根据安全策略和合规要求)，特别是包含 IT 基础设施或其安全机制相关信息的任何文案或一次性介质。

12.2.3　伪造与滥用

对语音通信的另一种威胁是 PBX 伪造和滥用。许多 PBX 系统都会被恶意的攻击者用于躲避收费和隐藏自己的身份。被称为飞客(phreaker)的恶意攻击者滥用电话系统的方式与攻击者滥用计算机网络的方式几乎完全相同。飞客可能能够获得对个人语音信箱的未授权访问，也可能重定向消息、阻止访问以及重定向入站和出站呼叫。

针对 PBX 伪造和滥用的对策与许多保护典型计算机网络的预防措施相同，包括逻辑或技术上的控制、行政管理性控制以及物理性控制。下面列出了设计 PBX 安全解决方案时需要记住的一些要点：

- 考虑使用信用卡或呼叫卡系统来替换通过 PBX 的远程访问或长途呼叫。
- 限制只有工作任务需要的已授权用户才能够拨入和拨出。
- 对于拨入调制解调器，使用未公开的电话号码，这些号码在语音号码同区段范围之外。
- 阻止或禁止任何未指定的访问码或账户。
- 定义可接受的使用策略，并且培训用户如何正确地使用系统。
- 记录和审计 PBX 上的所有活动，并且在审计跟踪中查看是否存在安全和使用违规。
- 禁止维护调制解调器(例如，通过供应商远程管理、更新和调整已部署产品来远程访问调制解调器)和账户。
- 修改所有默认配置，尤其是密码和与行政性管理或特权功能相关联的能力。
- 阻止远程呼叫(也就是允许远程呼叫者先拨入 PBX，然后再次拨出，从而将所有收费都指向 PBX 主机)。
- 部署直接拨入系统访问(Deploy Direct Inward System Access，DISA)技术，从而减少外部的 PBX 伪造(但是需要确认恰当的配置；请查看下面的“DISA：遭受的危害及其修复”)。
- 使供应商或服务提供商的更新保持系统是最新的。

此外，维护对所有 PBX 连接中心、电话入口或配线间的物理接入控制能够防止攻击者在现场进行直接入侵。

真实场景

DISA：遭受的危害及其修复

人们通常认可对 PBX 系统的“安全”改善是直接拨入系统访问(DISA)，此系统被设计为通过为用户指派访问码来帮助管理 PBX 的外部访问和外部控制。尽管概念引人注目，但是这种系统会遭到飞客的危害和滥用。一旦外部的飞客获悉了 PBX 访问码，他们往往能够完全控制和滥用公司的电话网络，这包括使用 PBX 将长途呼叫的计费指向公司的电话账户，而不是指向飞客的电话账户。

为了获得所期望的安全改善，DISA 必须像其他任何安全特性一样被正确地安装、配置和监控。简单地拥有 DISA 是不够的。确认禁止组织不需要的所有特性，设计复杂的和难以猜测的用户码/密码，然后打开审计功能来监测 PBX 的活动。

飞客行为(phreaking)是一种针对电话系统的特定攻击类型。飞客使用各种技术回避电话系统，从而获得免费的长途呼叫、更改电话服务的功能、窃取特殊的服务甚至导致服务中断。某些飞客工具是实际的设备，而其他飞客技术则只是使用正常电话的特定方式。无论实际使用的工具或技术是什么，飞客工具都被称为有色盒(黑盒、红盒等)。这些年来，飞客开发和广泛应用了许多盒技术，但是只有一些技术仍然适用于目前基于分组交换的电话系统。下面列出了对于考试需要了解的一些飞客工具：

- 黑盒用于操纵线电压，以便窃取长途服务，往往只是用户使用电池和线夹定做的电路板。
- 红盒用于模拟硬币存入付费电话时的声音，通常只是较小的磁带录音机。
- 蓝盒用于模拟与电话网络主干系统直接互动的 2600Hz 声音，可以是哨子、磁带录音机或数字音频生成器。
- 白盒用于控制电话系统，是一种双音多频(Dual-Tone MultiFrequency，DTMF)生成器(也就是键盘)。白盒既可以是用户定制的设备，也可以是大多数电话修理人员所用装备中的一部分。

注意：

你可能已经知道，蜂窝电话的安全性逐渐开始令人焦虑。被捕获的电子序列号(Electronic Serial Number，ESN)和移动标识号(Mobile Identification Number，MIN)可以被刻录到空的手机中，从而生成一个克隆版。使用克隆版手机时，所产生的费用会计入原所有者的蜂窝电话账户。而且，使用无线电频率扫描仪能够截获谈话与数据传输。此外，紧邻位置的任何人也可能偶然听到至少一方的通话内容。因此，在公共场合一定不要谈论机密的、私有的或敏感的话题。

12.3 多媒体协作

多媒体协作是使用不同的多媒体通信解决方案来支持远程协作(人们通过远程在一个项目上一同工作)。通常，协作允许人员跨越不同的时区同时工作。协作可以通过多媒体功能用于跟踪变化。协作可以和电子邮件、聊天、VoIP、视频会议、电子白板的使用、在线文档编辑、实时文件交换、版本控制以及其他工具进行合作。这些通常是先进远程会议技术的典型特性。

12.3.1　远程会议

远程会议技术用于让任何产品、硬件或软件可以和远程关系人之间相互交互。这些技术和解决方案有许多其他称呼：数字化协作、虚拟会议、视频会议、软件或应用协作、共享白板服务、虚拟培训解决方案等。只要是帮助人们进行沟通、交换数据、在材料/数据/文件上进行协同或者在一起工作以执行任务的任何服务，都可以被认为是远程会议技术服务。

无论实施什么形式的多媒体协作，都必须对随之而来的安全影响进行评估。服务是否使用强大的身份认证技术？通信发生于开放的协议还是加密的隧道？方案是否允许真正的内容删除？是否审核和记录用户的活动？多媒体协作和其他形式的远程会议技术可以改善工作环境，允许来自世界各地的广泛多样的工作者投身进来，但这个好处仅存在于通信解决方案的安全性得以保证的情况之下。

12.3.2　即时消息

即时消息(Instant Messaging，IM)是一种机制，允许两个用户在互联网上的任何位置进行实时文字聊天。一些 IM 工具允许文件传输、多媒体、语音和视频会议以及更多的功能。有些形式的 IM 是基于点对点的服务，而另一些则使用集中控制服务器。基于对等的 IM 容易让最终用户来部署和使用，但从企业的角度来看却是难以管理的，因为它通常是不安全的。它有很多漏洞：容易遭受数据包监听，缺乏真正的本地安全功能，没有提供隐私保护。

许多形式的即时消息缺乏共同的安全特性，如加密或用户隐私。许多 IM 客户端都容易通过它们的文件传输功能遭受恶意代码植入或感染。此外，IM 用户经常受到各种形式的社会工程学攻击，如模仿或说服受害者泄露应该保护的机密信息(如密码)。

12.4　管理电子邮件的安全性

电子邮件是一种最广泛和最常用的互联网服务。在互联网上使用的电子邮件基础设施主要由电子邮件服务器组成，电子邮件服务器通过使用简单邮件传输协议(SMTP)接收来自客户端的消息，向其他服务器传送这些消息，并且将消息存放到用户的基于服务器的收件箱中。除了电子邮件服务器之外，这个基础设施还包括电子邮件客户端。客户端通过邮局协议版本 3(POP3)或互联网消息访问协议(IMAP)从基于服务器的收件箱中检索电子邮件。客户端借助于 SMTP 与电子邮件服务器进行通信。互联网兼容的所有电子邮件系统都依赖于 X.400 标准定位和处理邮件。

Sendmail 是 Unix 系统中最常用的 SMTP 服务器，Exchange 是 Microsoft 系统中最常用的 SMTP 服务器。除了这两种主流产品以外，还存在很多可选的产品，这些产品都共享相同的基础功能，并且都符合互联网电子邮件标准。

如果要部署 SMTP 服务器，那么必须为入站和出站电子邮件正确地配置身份认证。SMTP 被设计为邮件中继系统，这意味着由它将电子邮件从发送者中继至预定的接收者。然而，我们希望避免 SMTP 服务器成为开放中继(也被称为开放中继代理或中继代理)，开放中继是一种在接受和中继电子邮件之前并不对发送者进行身份认证的 SMTP 服务器。开放中继是垃圾邮件发送者的主要目标，其原因在于它允许垃圾邮件发送者借助于不安全的电子邮件基础设施发送大量的邮件。当开放中继被锁定变为关闭或认证中继时，越来越多的 SMTP 攻击通过劫持认证用户账户而发生。

12.4.1 电子邮件安全性的目标

对于电子邮件来说，在互联网上使用的基本机制提供了有效的消息分发，但是缺乏为机密性、完整性甚至可用性提供的控制。换句话说，基本的电子邮件并不安全。不过，通过很多方式可以增强电子邮件的安全性。增强的电子邮件安全性可能满足下面列出的一个或多个目标：

- 提供不可否认性
- 限制只有预定的接收者能够访问邮件(例如，隐私性和机密性)
- 维护邮件的完整性
- 对邮件源进行身份认证和校验
- 验证邮件的传输
- 对邮件的内容或附件的敏感度进行分类

正如 IT 安全性的内容一样，电子邮件的安全性首先依赖于由更高级管理人员批准的安全策略。对于这个安全策略，必须解决下列问题：

- 电子邮件可接受的使用策略
- 访问控制
- 隐私
- 电子邮件管理
- 电子邮件的备份和保管策略

可接受的使用策略定义了在组织的电子邮件基础设施上能够执行和不能执行的活动。它常常规定可以发送和接收专业的、面向业务的电子邮件和数量有限的个人电子邮件。针对执行个人事务(也就是为其他组织工作，包括自己创业)、非法的、不道德的活动或攻击性通信，以及对生产、收益或公共关系产生不利影响的其他任何活动，往往需要施加特定的限制。

对电子邮件的访问控制应当是持续的，这样用户才能够只访问他们的特定收件箱和电子邮件存档数据库。这条规则的扩展规定：无论是被授权的还是未被授权的用户，都不能访问他人的电子邮件。访问控制应当同时提供合法的访问以及某些隐私级别，至少对同事和未授权的入侵者保密。

组织实现、维护和管理电子邮件所使用的机制和过程应当清晰明了。终端用户可能不需要了解电子邮件的管理细节，但是必须了解电子邮件是否是保密的通信。近年来，在很多法律案件中电子邮件成为双方攻防的重点，归档的邮件被用作证据，这往往会令邮件的发送者或接收者十分恼火。如果电子邮件要进行保留(也就是备份和归档存储，以备将来使用)，那么需要让用户意识到这种情况。如果审计人员希望查看电子邮件是否违规，那么也需要通知用户。一些公司选择电子邮件在被销毁之前只保留三个月，而其他一些公司则选择电子邮件保留数年时间。你所在的国家以及所从事的行业往往规定了电子邮件的保留策略。

12.4.2 理解电子邮件的安全性问题

部署电子邮件安全性的第一个步骤是要认识电子邮件特有的脆弱性。用于支持电子邮件的协议并不采用加密。因此，所有的邮件都按照向电子邮件服务器提交的形式进行传输，这种形式往往是明文。这个脆弱性使得电子邮件很容易被截获和偷听。不过，在与电子邮件安全性相关的各种问题中，自身缺乏加密是最不重要的。

电子邮件是病毒、蠕虫、特洛伊木马、破坏性宏文件以及其他恶意代码利用的最常用传输机制。对各种脚本语言、自动下载能力和自动运行特性的支持的增加，已经将电子邮件内容和附件中的超级链接变成了对所有系统的严重威胁。

在源验证方面，电子邮件几乎没有提供任何方法。即使攻击者是新手，对电子邮件的源地址进行欺骗也是轻而易举的。电子邮件头部既可以在源地址处进行修改，也可以在传输过程中的任何位置进行修改。此外，通过直接连接电子邮件服务器的 SMTP 端口，也能够将电子邮件直接传送至电子邮件服务器上的用户收件箱。至于传输中的修改问题，我们应当认识到：电子邮件本身没有确保邮件在源和目的地之间不被修改的完整性检查。

此外，电子邮件本身也可以作为攻击机制。当足够多的邮件被指向单个用户的收件箱或者通过特定的 SMTP 服务器时，就可能导致拒绝服务服务(DoS)。这种攻击常常被称为邮件炸弹，并且只是通过邮件使系统溢出的 DoS 攻击。此时，DoS 既可能是存储容量遭到消耗的结果，也可能是处理能力过度使用的结果。无论是哪一种情况，结果都是一样的：合法的邮件无法被发送。

像电子邮件泛洪溢出和恶意代码附件一样，多余的电子邮件也被视为一种攻击。发送多余的、不适当的或无关的邮件被称为垃圾邮件攻击。垃圾邮件攻击常常令人生厌，它不仅消耗本地的系统资源，而且还消耗互联网上的系统资源。由于邮件的源地址通常都是欺骗性的地址，因此垃圾邮件往往很难被阻塞。

12.4.3　电子邮件安全性解决方案

为电子邮件增强安全性是可能的，但是所做的工作都应与正在交换的邮件的价值和机密性相符。可以在不需要对基于互联网的整个 SMTP 基础设施进行全面修改的情况下，使用某些协议、服务和解决方案(包括 S/MIME、MOSS、PEM 和 PGP)为电子邮件添加安全性。我们已在第 7 章“PKI 和密码学应用”中深入讨论过 S/MIME。

安全多用途互联网邮件扩展(S/MIME)　S/MIME 是一种电子邮件安全标准，通过公钥加密和数字签名为电子邮件提供身份认证和隐私保护。通过 X.509 数字证书能够提供身份认证，隐私则是通过使用公钥密码学标准(PKCS)加密提供的。使用 S/MIME 可以构成两种类型的邮件：签名的邮件和安全封装的邮件。签名的邮件提供了完整性和对发送者的身份认证。安全封装的邮件提供了完整性、对发送者的身份认证以及机密性。

MIME对象安全服务(MOSS)　MIME对象安全服务可以为邮件提供身份认证、机密性、完整性和不可否认性。MOSS利用了MD2 和MD5 算法、RSA公钥以及数据加密标准(DES)，从而提供了身份认证和加密服务。

隐私增强邮件(PEM)　隐私增强邮件是一种电子邮件加密机制，使用 RSA、DES 和 X.509 提供了身份认证、完整性、机密性和不可否认性。

域名密钥识别邮件标准(DKIM)　DKIM 是一种手段，确保了合法邮件被组织通过域名身份认证来发送。详情可查看 http://www.dkim.org。

良好的隐私(PGP)　良好的隐私(PGP)是一个使用多种加密算法对文件和电子邮件进行加密的公-私密钥系统。第一版 PGP 使用 RSA，第二版使用国际数据加密算法(IEDA)，但是以后的版本提供了算法选择。PGP 不是标准，而是一款自主开发的产品，获得互联网草根阶层的广泛支持。

真实场景

免费的 PGP 解决方案

PGP 最初是任何人都可以使用的免费产品，但是随后又被分为两个不同的产品。PGP 是一款商业产品，而 OpenPGP 是一个正在开发的标准，GnuPG 依从这个标准，并且这个标准被免费软件基金会独立开发。如果以前没有用过 PGP，那么我们建议为首选的电子邮件平台下载适当的 GnuPG 版本。这个安全解决方案无疑能够改善电子邮件的隐私性和完整性。在 http://gnupg.org 站点上，你可以了解到 GnuPG 的更多相关信息。

通过使用这些和其他用于电子邮件和通信传输的安全机制，可以减少或消除很多邮件的安全脆弱性。数字签名可以帮助消除假冒。对邮件的加密减少了偷听的问题，并且使用电子邮件过滤器能够将垃圾邮件和邮件炸弹维持在最小数量。

网络中电子邮件网关系统上的附件阻塞功能可以减轻来自恶意附件的威胁。可以建立 100%无附件的策略，或者只对那些已知的或被怀疑为恶意的附件进行阻塞，例如那些具有可执行的或脚本文件扩展名的附件。如果附件是电子邮件通信的必需部分，那么需要依靠对用户的培训和反病毒工具进行保护。培训用户避免与可疑人和意外附件接触，从而大大减少通过电子邮件传送恶意代码的风险。反病毒软件对于已知病毒一般是有效的，但是对于新的或未知的病毒几乎起不到保护作用。

真实场景

传真的安全性

由于电子邮件的广泛使用，传真通信已不再那么流行。电子文档很容易通过电子邮件的附件形式进行交换。打印的文档被扫描后也可以很容易地通过电子邮件进行传送，就像传真一样。不过，我们仍然必须在整体的安全计划中涉及传真通信的问题。大多数调制解调器使用户能够连接远程计算机系统和收发传真。很多操作系统内置了传真功能，而且存在多种在计算机系统上使用的传真产品。从某台计算机的传真/调制解调器发出的传真可以被另一台计算机或常规的传真机所接收。

虽然使用趋势已经衰退，但是传真仍然代表一种易于遭受攻击的通信途径。与其他任何电话通信一样，传真能够被截获，并且很容易被偷听。如果记录下完整的传真通信，那么通过另一台传真机就能够重放此通信，从而可以提取出被传送的文档。

可以通过部署某些机制来改善传真的安全性，这些机制包括传真加密器、链路加密、活动日志以及异常报告。传真加密器使传真机能够使用某种加密协议来扰乱即将外发的传真信号。使用加密器时，接收方的传真机也必须支持相同的加密协议，从而能够对文档进行解密。链路加密指的是使用加密的通信路径传输传真信号，就像 VPN 链接或安全的电话链接一样。活动日志和异常报告能够用于检测传真中表现为攻击征兆的异常活动。

除了传真传输的安全性之外，考虑传真接收的安全性也十分重要。自动打印的传真可能长时间搁置在已处理文件盒内，因此很容易被非预定的接收者看到。研究表明：添加 CONFIDENTIAL、PRIVATE 等横幅反而会引起和激发无关人员的好奇心。因此，务必禁止自动打印。此外，避免传真利用能够保留已打印传真图像的色带或墨盒。考虑将传真系统与网络集成在一起，从而不必在纸上打印传真，而是通过电子邮件将传真发送给预定的接收者。

12.5　远程接入安全管理

远程交换(或远程连接)已成为商业计算的一种常见特征。远程访问使身处远方的客户端能够建立与某个网络的通信会话。客户端可以采用这样的形式建立通信会话：

- 使用调制解调器直接拨号登录远程访问服务器
- 在互联网上通过 VPN 连接至某个网络
- 通过瘦客户端(thin-client)与某个终端服务器系统相连接

前两个示例使用了功能完备的客户端，这些客户端建立的连接使其就像直接连接到 LAN 一样。最后一个示例使用终端服务器建立了来自某个瘦客户端的连接。这种情况下，所有计算动作都在终端服务器系统中发生，而不是在远程客户端上发生。

远程交换也通常涉及电话通信。电话是指提供给组织的电话服务的方式集合，或是组织使用电话服务进行语音和/或数据通信的机制集合。传统上，电话包括普通旧式电话服务(POTS)——也被称为公共交换电话网络(PSTN)——结合调制解调器。然而，专有分组交换机(PBX)、VoIP 和 VPN 也通常用于电话通信。

真实场景

远程访问和远程交换技术

远程办公是在远程场所(即主办公室以外)进行工作。事实上，有一个很好的机会让你把某种形式的远程交换作为当前工作的一部分。远程交换客户端使用许多远程访问技术同中央办公室局域网建立连接。远程访问技术主要有 4 种类型:

特定服务　特定的远程访问为用户提供远程连接、操作或与单一服务交互，例如电子邮件。

远程控制　远程控制授予远程用户能够完全控制另一个与他们存在物理距离的系统。连接的显示器和键盘的响应使得用户感觉好像他们是直接连接到远程系统。

屏幕抓取/抓取　这个词可以用在不同的情况下。首先，它有时被用来指远程控制、远程访问或远程桌面服务。这些服务也被称为虚拟应用或虚拟桌面。这个想法是，将目标机器上的屏幕进行抓取并显示给远程操作员。因此远程访问资源在远距离传输过程中会有额外的风险、泄露和损害，因此使用屏幕抓取加密就十分重要。

其次，屏幕抓取这个技术可以让一个自动化的工具来和人机接口互动。例如，一些独立的数据收集工具在它们的运行中使用搜索引擎。然而，大多数搜索引擎必须通过正常的Web接口才能使用。例如，谷歌要求所有的搜索都通过一个谷歌搜索表单域进行(在过去，谷歌提供了一个API接口来支持其他产品与其后端直接交互。不过，谷歌终止了这一做法以支持广告与搜索结果的整合)。屏幕抓取技术可以与人性化设计的Web前端进行交互，并将网页结果解析提取为相关信息。Foundstone/McAfee的SiteDigger就是这类产品的一个很好的例子。

远程节点操作　远程节点操作只是拨号连接的另一个名称。远程系统连接到远程访问服务器，该服务器向远程客户端提供网络服务和可能的互联网接入。

POTS 和 PSTN 指传统的固定电话连接。POTS/ PSTN 连接过去是许多企业唯一或主要可以获得高速、高性价比和无处不在的远程连接方式。一旦无线宽带服务越来越多，用于家庭用户的 POTS/ PSTN 互联网连接也将逐步消失。POTS/ PSTN 连接有时还作为远程连接宽带解决方案失效后的备份

选项。作为农村的互联网连接及远程连接方案，当 ISDN 或 VoIP 不存在或不符合成本效益时，就可以使用一条标准的语音线路用作连接。

当远程访问功能在任何环境下进行部署时，安全必须考虑和实施，并对私有网络进行保护，防备远程并发访问。

- 远程访问用户在被授予访问之前应严格认证。
- 只有那些为了完成他们的任务而需要远程接入的用户才被允许建立远程连接。
- 所有远程通信应进行保护以防止截取和窃听。通常这需要一个加密解决方案，为认证流量以及所有的数据传输提供有力保护。

在开始传输敏感的、有价值的或个人信息前，建立安全通信信道是很重要的。远程访问会构成几个潜在的安全问题点，如果不受保护和充分监测：

- 远程连接的任何人都可以尝试打破组织的安全性，物理安全效益会被降低。
- 远程工作者可能使用不安全或较不安全的远程系统访问敏感信息，这就增加了敏感信息遭受更大损失、破坏和泄露的风险。
- 远程系统可能遭受恶意代码攻击，并作为载体将恶意软件带入私有局域网。
- 远程系统本身可能也不安全，因此会被未经授权实体使用或遭受偷窃的风险。
- 远程系统可能会更难以排除故障，特别是涉及围绕远程连接的问题。
- 由于远程系统潜在的、不频发的连接或缓慢的吞吐量，远程系统可能不容易升级或修补补丁。

12.5.1 计划远程接入安全

当列出远程访问安全管理策略时，务必解决以下问题：

远程连接技术 每一种远程连接都存在自己特有的安全问题。仔细查看当前连接选项的各个方面，这可能包括调制解调器、DSL、ISDN、无线网络、卫星以及电缆调制解调器。

传输保护 加密协议、加密连接系统、加密的网络服务或应用程序存在多种形式。根据远程连接需要组合使用适当的安全服务组合，这可能包括 VPN、SSL、TLS、SSH、IPSec 以及 L2TP。

身份认证保护 除了保护数据通信之外，还必须确保所有登录凭证都是安全的。为了保证登录凭证的安全，就需要使用某种身份认证协议，甚至需要授权使用集中的远程访问身份认证系统，这可能包括密码认证协议(PAP)、挑战握手认证协议(CHAP)、扩展认证协议(EAP 及其扩展的 PEAP 或 LEAP)、远程认证拨号用户服务(RADIUS)以及终端访问控制器访问控制系统(TACACS+)。

远程用户支持 远程访问用户可以定期寻求技术支持。必须通过某种途径以提供最有效的技术支持，这可能包括解决软件和硬件问题以及用户的培训问题等。如果组织无法为远程用户的技术支持提供合理的解决方案，就可能导致生产力的损失、远程系统的破坏或整体性违反组织的安全。

如果很难或不可能将安全性保持在与私有 LAN 远程系统相似的水平，远程访问应当重新考虑。网络访问控制(NAC)有助于此，但会导致更新和补丁传输速度较慢的连接。

使用远程访问或建立远程连接的权限必须受到严格的控制。通过使用基于用户身份、工作站身份、协议、应用、内容以及时间的过滤器、规则或访问控制，就能够控制和约束远程连接的使用。

为了只允许获得授权的用户进行远程访问，可以使用回叫和呼叫者 ID。回叫是一种机制，这种机制在最初联系时断开与远程用户的联系，随后立即使用预定义的电话号码(也就是在用户账户安全数据库中已定义的电话号码)尝试重新连接。回叫有一种用户自定义模式，不过这种模式并未用于安

全性，而是被用于将长途话费的收取对象由远程客户端转移至公司。呼叫者 ID 验证的用途与回叫相同，不过需要通过电话号码来验证授权用户的物理位置(通过电话号码)。

任何安全策略都必须有一个标准的要素，就是与专有网络相连接的所有系统上不能存在未授权的调制解调器。还可能需要进一步指定安全策略，以指示可移植系统必须在连接网络之前去除所有调制解调器，或者必须使用禁用调制解调器设备驱动程序的硬件配置文件进行启动。

12.5.2　拨号协议

在建立远程连接时，必须使用某些协议来管理连接的实际创建方式，并为其他协议建立工作于其上的通用通信基础。重要的是，只要有可能就要选择支持安全性的协议。最低限度，确保身份认证的手段是必要的，增加数据加密也是首选。拨号协议的两个最主要的例子——PPP 和 SLIP，不仅为真正的拨号连接，也为一些 VPN 连接提供连接的管理。

点对点协议(PPP)　是一种全双工协议，用于在各种非 LAN 连接上传输 TCP/IP 数据包，这些连接包括调制解调器、ISDN、VPN 和帧中继等。PPP 得到了广泛支持，并且是拨号互联网连接的传输协议选项。通过使用各种协议(例如，CHAP 或 PAP)，PPP 身份认证能够受到保护。PPP 是 SLIP 的替换协议，并且可以支持任何 LAN 协议，而不只是支持 TCP/IP。

网络串行线路协议(SLIP)　是一种较旧的技术，用于支持异步串行连接(例如，串行线缆或调制解调器拨号)上的 TCP/IP 通信。SLIP 已很少使用，不过仍然得到很多系统的支持。SLIP 只能够支持 IP 协议，需要静态的 IP 地址，不提供差错检测或纠正功能，并且不支持压缩。

注意：

在许多专有的拨号协议中，有一种是 Microcom 联网协议(MNP)。MNP 是 20 世纪 90 年代在 Microcom 调制解调器上出现的，支持自己的差错控制形式(也就是 Echoplex)。

12.5.3　集中化的远程身份认证服务

随着远程访问逐渐成为组织商业活动中的一个要素，在远程客户端和专用网络之间添加安全层往往显得十分重要。集中化的远程身份认证服务(例如，RADIUS 和 TACACS+)就提供了这种额外的保护层。这些机制为远程客户端进行局域网或当地客户端操作提供了一个隔离的认证和授权过程。隔离对于安全是很重要的，因为如果 RADIUS 或 TACACS+服务器受到损害，那么只有远程连接受到影响，而网络的其他部分不受影响。

远程认证拨号用户服务(RADIUS)　这种机制用于集中完成远程拨号连接的身份认证。对使用 RADIUS 服务器的网络进行配置，从而使远程的访问服务器将拨号用户的登录凭证发送至 RADIUS 服务器进行身份认证。这个过程类似于域客户端向域控制器发送登录凭证以进行身份认证的过程。

终端访问控制器访问控制系统(TACACS+)　这种机制能够替换 RADIUS。TACACS 具有三种可用的版本：最早版本的 TACACS、扩展的 TACACS(XTACACS)以及 TACACS+。TACACS 集成了身份认证和授权过程。XTACACS 保持了身份认证、授权和记账过程的分离。TACACS+通过增加双因素身份认证增强了 XTACACS。TACACS+是这个产品线最流行和相关的版本。

12.6 虚拟专用网络

虚拟专用网(VPN)是一条通信隧道，可以在不可信的中间网络上提供身份认证和数据通信的点对点传输。大多数 VPN 使用加密技术来保护封装的通信数据，但是加密对于 VPN 连接而言并非必需的。

VPN 最常与通过互联网在两个距离遥远的网络之间建立安全的通信路径相关联。不过，VPN 可以存在于任何地方，包括专用网络内或连接 ISP 的终端用户之间。VPN 可以连接两个网络或两个单独的系统。VPN 能够连接客户端、服务器、路由器、防火墙以及交换机。在为依赖于有风险或脆弱性的通信协议或技术的旧应用(尤其是通过网络进行通信时)提供安全性时，VPN 也非常有用。

VPN 在不安全的或不可信的中间网络上提供了机密性和完整性，但是并不提供和保证可用性。VPN 也比较广泛地用到像 Netflix 和 Hulu 对服务定位的要求，从而提供了(有时怀疑)匿名性。

12.6.1 隧道技术

在能真正理解 VPN 之前，必须先理解隧道技术。隧道技术是网络的通信过程，通过将协议包封装到其他协议包中来保护协议包的内容。封装是在不可信的中间网络上建立通信隧道的逻辑错觉。这条虚拟路径存在于通信两端的封装和拆装实体之间。

事实上，给祖母发送信件时也会涉及使用隧道系统。书写个人信件(协议包的主要内容)并将它装进信封(隧道协议)，这封信通过邮递服务(不可信的中间网络)被发往预期的收信人。隧道技术可以用在很多场合(如绕过防火墙、网关、代理或其他通信控制设备时)。通过将受限制的内容封装到已授权传输的数据包中，就可以实现旁路。由于通信控制设备不了解数据包中包含的实际内容，因此隧道处理能防止通信控制设备阻止或丢弃通信。

隧道技术常常被用于使其他情况下会断开的系统之间能够进行通信。如果两个系统由于缺乏网络连通性而断开，那么可以通过调制解调器的拨号连接或其他远程访问或广域网(WAN)网络连接服务来建立通信连接。实际的 LAN 通信被封装在由临时连接使用的任意通信协议中，例如调制解调器拨号环境中的点对点协议(PPP)。如果两个网络通过某个使用不同协议的网络相连接，那么被分隔网络的协议常常可以被封装在中间网络的协议内，从而提供通信路径。

无论实际的环境如何，隧道技术通过将内部协议的内容和通信数据包包裹或包装在中间网络或连接所使用的已授权协议中，对它们进行保护。如果主协议是不可路由的并且为了维持网络上支持最小数量的协议，就可以使用隧道技术。

真实场景

隧道技术的扩散

隧道技术是通信系统内的一种常见活动，很多人经常在不知不觉的情况下使用隧道技术。例如，每当使用安全的 SSL 或 TLS 访问 Web 站点时，就会用到隧道技术，此时明文 Web 通信通过隧道技术被装入 SSL 或 TLS 会话。此外，如果使用互联网电话或 VoIP 系统，那么语音通信会通过隧道技术被装入某种 VoIP 协议。

在日常生活中，还会遇到多少使用隧道技术的实例?

如果封装协议的操作涉及加密，那么隧道技术可以提供通过不可信的中间网络传输敏感数据的方法，并且不必担心丢失机密性和完整性。

隧道技术并不是没有问题。由于大多数协议都包含自身的错误检测、错误处理、确认和会话管理功能，因此隧道技术通常不是一种有效的通信方法。正因为如此，在传输单独的报文时，一次使用多个协议会混合额外的开销。而且，隧道技术生成了更大的或者数量更多的信息包，这也会消耗额外的网络带宽。如果没有足够的带宽，那么隧道技术会很快使网络饱和。此外，隧道技术是一种点对点的通信机制，并且设计时没有考虑对广播通信的处理。隧道技术也使得在某些情况下监控流量的内容变得很难，但不是不可能，这为安全从业者制造了不少麻烦。

12.6.2　VPN 的工作原理

VPN 连接能够被建立在其他任何网络通信连接上，这些连接可以是典型的 LAN 线缆连接、无线 LAN 连接、远程访问拨号连接、WAN 连接，甚至可以是客户端访问办公室 LAN 时使用的互联网连接。VPN 连接就像一条典型的直接 LAN 线缆连接，唯一的区别可能是速率，而速率依赖于客户端系统和服务器系统之间的中间网络和连接类型。在一条 VPN 连接上，客户端可以像通过一条 LAN 线缆直接连接那样执行完全相同的操作和访问相同的资源。

VPN 可以连接两个单独的系统或两个完整的网络。二者唯一的区别在于：被传输的数据只有在位于 VPN 隧道内时才会受到保护。网络边界上的远程访问服务器或防火墙是 VPN 的起点或终点。因此，通信在源 LAN 中没有受到保护，在边界 VPN 服务器之间得到了保护，一旦到达目的地，LAN 就不再受到保护。

穿越互联网进行远距离网络连接的 VPN 连接常常是替代直接连接或租用线路的便宜选择。两条至本地 ISP 的、支持 VPN 的高速互联网连接的成本，往往远小于其他任何可用连接方式的成本。

12.6.3　常用 VPN 协议

使用软件或硬件解决方案都可以实现 VPN。不管采用哪种解决方案，总是存在 4 种常用的 VPN 协议：PPTP、L2F、L2TP 和 IPSec。PPTP、L2F 和 L2TP 在 OSI 模型的数据链路层(第 2 层)上工作。PPTP 和 IPSec 被限制在 IP 网络中使用，而 L2F 和 L2TP 则被用于封装任何 LAN 协议。

注意：

SSL/TLS 也可以被用来作为 VPN 协议，而不只是作为工作在 TCP 之上的会话加密。CISSP 考试似乎并不包括 SSL/TLS VPN 的内容。

1. 点对点隧道协议

点对点隧道协议(PPTP)是从拨号协议点对点协议(PPP)开发出来的一种封装协议，工作在 OSI 模型的数据链路层(第 2 层)上，并且被用在 IP 网络中。PPTP 在两个系统之间创建了一条点对点隧道，并且封装了 PPP 包。通过与 PPP 支持相同的身份认证协议，PPTP 为身份认证通信提供了保护。这些身份认证协议包括：

- Microsoft 挑战握手身份认证协议(MS-CHAP)
- 挑战握手身份认证协议(CHAP)

- 密码身份认证协议(PAP)
- 扩展身份认证协议(EAP)
- Shiva 密码身份认证协议(SPAP)

注意：

CISSP 考试的重点是 PPTP 的 RFC 2637 版本，而不是微软版本的实现，微软版本进行了专门修改并使用微软点对点加密(MPPE)来支持数据加密。

PPTP 使用的最初隧道协商过程并没有加密。因此，包含发送者和接收者 IP 地址(可以包括用户名和散列密码)的会话建立通信包可能被第三方截获。PPTP 被用在 VPN 上，但是它常常被第二层隧道协议(L2TP)代替。L2TP 可以使用 IPSec 为 VPN 提供通信加密。

PPTP 不支持 TACACS+和 RADIUS。

2. 二层转发协议和二层隧道协议

思科公司开发了自己的 VPN 协议：第二层转发协议(L2F)，这是一种相互的身份认证隧道机制。然而，L2F 并不提供加密。L2F 没有得到广泛部署，并且很快被 L2TP 取代。正如它们的名字所暗示的，它们都工作在 OSI 模型的第 2 层上。它们都可以封装任何局域网协议。

二层隧道协议(L2TP)源自于 PPTP 和 L2F 的组合。L2TP 会在通信的端点之间建立一条点对点的隧道。L2TP 缺乏内置的加密方案，而是通常依赖 IPSec 作为安全机制。L2TP 还支持 TACACS+和 RADIUS。IPSec 通常为 L2TP 用做一种安全机制。

3. IP 安全协议

目前最常用的 VPN 协议是 IPSec。IPSec 既是一个独立的 VPN 协议，也是用于 L2TP 的安全机制，并且只能用于 IP 通信。IPSec 提供了安全的身份认证以及加密的数据传输。IPSec 具有下列两个主要的组件或功能：

身份认证头(AH) AH 提供身份认证、完整性以及不可否认性。

封装安全有效载荷(ESP) ESP 提供了加密，从而能够保护传输数据的机密性，不过也可以执行有限的身份认证操作。ESP 在网络层(第 3 层)上工作，并且可以用在传输模式或隧道模式中。在传输模式中，对 IP 数据包数据进行了加密，但是对数据包的头部并没有进行加密。在隧道模式中，对整个 IP 数据包都进行了加密，并且新的数据包头被添加至 IP 数据包，从而能够控制通过隧道进行的传输。

表 12.1 说明了 VPN 协议的主要特征。

表 12.1 VPN 协议的主要特征

VPN 协议	自带身份认证保护？	自带数据加密？	支持的协议	支持拨号连接？	同时存在的连接数
PPTP	是	否	只支持 IP	是	单个点对点连接
L2F	是	否	只支持 IP	是	单个点对点连接
L2TP	是	否(可以使用 IPSec)	支持任何协议	是	单个点对点连接
IPSec	是	是	只支持 IP	否	多个连接

VPN 设备是一种网络增件设备，用于创建与服务器或客户端系统分隔开的 VPN 隧道。对于互联系统来说，对 VPN 设备的使用是透明的。

12.6.4　虚拟局域网

虚拟局域网(VLAN)被用于硬件上以实施网络分隔。VLAN 在网络上进行逻辑隔离而不改变其物理拓扑。

VLAN 由交换机创建。默认情况下，交换机上的所有端口都属于 VLAN #1。但随着交换机管理员更改每个端口上的 VLAN 分配，不同的端口可以组合在一起并且使用各自不同的 VLAN 端口名称。这样，在同一个网络上可以创建多个逻辑网络分段。

在相同 VLAN 中的端口之间通信是没有阻碍的。不同 VLAN 之间的通信可以通过使用路由功能拒绝或支持。路由可以由外部路由器或交换机的内部软件提供(可由多层交换机提供)。

因为安全或性能的原因，VLAN 管理使用 VLAN 控制流量。VLAN 执行多个流量管理功能，其中一些是与安全相关的：

- 控制和限制广播流量。阻断子网和 VLAN 中的广播。.
- 隔离网络分段间的流量。默认情况下，不同 VLAN 之间没有提供彼此之间通信的路由。也可以允许 VLAN 间的通信，但是要在特定的 VALN 间(或 VLAN 的特定成员间)指定拒绝过滤。
- 减少网络监听的脆弱性。
- 防止广播风暴(多余的网络广播流量泛洪)。

一些 VLAN 部署的另一个元素是端口隔离或私有端口。这些私有 VLAN 的配置是为了使用一个专用的或预留的上行端口。私有 VLAN 或端口隔离 VLAN 的成员仅可以通过预定的出口或上行端口进行相互通信。一种端口隔离的常见示例是在酒店里。酒店网络可以被配置以便于将每个房间或套房的以太网端口隔离在单独的 VLAN 中，从而达到相同单元的实体可以通信而不同单元的实体不能通信的效果。但是，所有这些私有 VLAN 都有一条到互联网(即上行端口)的路径。

提示：

VLAN 的作用就像子网，但是记住它们不是真正的子网。VLAN 是由交换机生成的。子网却是由 IP 地址和子网掩码构成的。

用于安全的 VLAN 管理

不需要彼此通信去完成工作任务/功能的任何网段都不应该能够这样做。使用 VLAN 允许必要的，而阻断/拒绝任何不必要的。需要记住，“默认拒绝；允许例外”不仅仅是一条防火墙规则，而且是一条安全通用准则。

12.7　虚拟化

虚拟化技术用来在单一主机的内存中承载一个或多个操作系统。这种机制允许在任意硬件上虚拟任意的操作系统。这样的操作系统也被称为客户端操作系统。根据这个观点，存在在计算机硬件

上直接安装的原始或宿主操作系统,被托管在虚拟机管理系统上的额外操作系统是客户端操作系统。它同样允许多个操作系统同时使用相同的硬件进行工作。常见的例子包括 VMWare、微软的 Virtual PC 和 Virtual Server、Windows Server 2008 的 Hyper-V、VirtualBox 和苹果的 Parallels。

从用户的角度看，虚拟化的服务器和服务与传统的服务器和服务没有区别。

虚拟化有几个好处，例如，能够在需要的情况下，启动单个服务器或服务的实例，实时的可扩展性，并且能够运行应用程序所需的额外操作系统版本。此外，从受损、崩溃或损坏的虚拟系统恢复往往十分简单快捷：只需要用干净的备份版本简单取代虚拟系统的主硬盘文件，然后重新启动即可。

在安全性方面，虚拟化提供了几个好处。整个虚拟系统的备份比同等安装在本地硬件上的系统更容易和更快速。另外，当出现错误或问题时，虚拟系统可以在几分钟内被备份替换。虚拟系统的恶意代码破坏或感染很难影响主机操作系统，这将有利于进行安全测试和实验。

虚拟化被用于各种各样的新的体系结构和系统设计解决方案。云计算是一种最终的虚拟化形式(更多关于云计算的信息，请参阅第 9 章“安全脆弱性、威胁和对策”)。本地(或至少在组织的私有基础设施中)，虚拟化可以用在宿主服务器、客户端操作系统、受限的用户接口(即虚拟桌面)应用以及其他更多的应用。

12.7.1 虚拟化软件

虚拟化应用程序是一种软件产品，它的部署方式是让它误以为在和一个完整的主机操作系统进行交互。一个虚拟(或虚拟化)应用被打包或封装，使它具备移动性和在不用完整安装原有主机操作系统的情况下运行。虚拟应用能充分利用原始主机操作系统，并包含在封装气泡中(技术上称为虚拟机或 VM)，它的运作/功能就类似于传统的安装。虚拟应用的一些形式被用于 USB 驱动器上的移动应用(简称应用)。其他虚拟应用被设计运行在另一个宿主操作系统平台上，例如运行在 Linux 操作系统上的 Windows 应用。

“虚拟桌面”这个术语指的是至少三种不同类型的技术：

- 一种远程访问工具，允许用户访问远程的计算机系统，并允许他远程查看和控制远程桌面显示、键盘、鼠标等。
- 虚拟应用概念的扩展，封装多个应用和一些“桌面”形式，或用于移动性和跨操作系统的外壳。这种技术给用户提供了平台的一些功能/效益/应用，而无需多台电脑、双启动或虚拟化整个操作系统平台。
- 扩展或扩展桌面，它们的尺寸大于使得用户可使用多个应用程序的布局，以方便使用按键或鼠标动作间的切换。

第 8 章“安全模型的原则、设计和功能”和第 9 章“安全脆弱性、威胁和对策”中有更多关于安全架构和设计的虚拟化信息。

12.7.2 虚拟化网络

操作系统虚拟化的概念已经引发了其他虚拟化的话题，例如虚拟化网络。虚拟化网络或网络虚拟化是将硬件和软件网络组件组合成单一合成实体。由此产生的系统允许软件控制所有网络功能：包括管理、流量整形、地址分配等。单一的管理控制台或接口可以用来监视网络的每一个方面，而

在过去，一个任务需要在每个硬件组件里都有硬件的存在。虚拟化网络已经成为全球企业范围内部署和管理的一种流行方式。它们允许组织实施或调整其他有意思的网络解决方案，包括软件定义网络、虚拟 SAN、客户端操作系统以及端口隔离。

软件定义网络(SDN)是一种独特的网络操作、设计和管理方法。该概念基于这样一个理论，即传统网络设备配置(如路由器和交换机)的复杂性经常强迫组织依附于单一的设备厂商，如思科，从而限制了网络的灵活性而难以应付不断变化的物理和商业条件。SDN 旨在从控制层(即网络服务的数据传输管理)分离基础设施层(即硬件和基于硬件的设置)。此外，它消除了 IP 寻址、子网、路由的传统网络概念，以及以此类推的需要被托管应用进行编程或破译的需求形式。

SDN 提供了一种新的直接从中心位置编程的网络设计方式，它是灵活的、厂商无关的并基于开放标准。利用 SDN 使得组织可以不再从单一供应商采购设备。相反，允许组织混合和匹配需要的硬件，如选择最划算的或最高通过性能的设备，而无论供应商是谁。然后通过集中管理界面控制硬件的配置和管理。此外，应用于硬件的设置可以根据动态的需求进行变更和调整。

对 SDN 的另一种思考方式是有效的网络虚拟化。它使数据传输路径、通信决策树和流控都在 SDN 控制层进行虚拟化，而不是在每个设备的基础硬件上进行处理。

虚拟化网络的发展所产生的另一个有趣概念是虚拟 SAN(存储区域网络)。SAN 是一种网络技术，它将多个单独的存储设备组合成单一综合的网络访问存储容器。虚拟 SAN 或软件定义共享存储系统是一种虚拟网络或 SDN 上的 SAN 虚拟重构。

12.8　网络地址转换

隐藏内部客户端的身份、隐蔽私有网络设计以及使公共 IP 地址租用成本最低，这些功能都可以通过使用网络地址转换(NAT)方便地实现。NAT 是一种将包头中的内部 IP 地址转换为公共 IP 地址，从而在互联网上进行传输的机制。

人们开发 NAT 是为了允许专用网络使用任何 IP 地址集，并且不会与具有相同 IP 地址的公共互联网主机发生冲突或抵触。事实上，NAT 将内部客户端的 IP 地址转换为外部环境中的租用地址。

NAT 提供了很多优点，包括：

- 能够只使用一个(或几个)租用的公共 IP 地址将整个网络连接到互联网。
- 始终能够在与互联网通信的情况下，将 RFC 1918 中定义的专用 IP 地址用于专用网络。
- NAT 通过互联网隐藏 IP 地址方案和网络拓扑结构
- NAT 还通过限制连接提供了保护，从而使只有来自于内部受保护网络的连接才被准许从互联网返回网络。因此，大多数入侵攻击会被自动击退。

真实场景

你使用 NAT 了吗？

无论是办公室还是家庭，大多数网络都利用了 NAT。至少可以通过三种途径来判断自己的网络是否利用了 NAT。

1) 查看自己客户端的 IP 地址，如果属于 RFC 1918 中定义的地址，并且仍然能够与互联网交互，那么你的网络就利用了 NAT。

2) 查看代理、路由器、防火墙、调制解调器或网关设备的配置，了解是否配置了 NAT。显然，这个操作需要获得授权才能访问网络连接设备。

3) 如果客户端IP地址不属于RFC 1918中定义的地址，那么将其与互联网认为的地址相比较。通过访问任何IP检查Web站点(常用的一个站点是http://whatismyipaddress.com)就可以完成这个操作。如果客户端IP地址与http://whatismyipaddress.com站点确定的地址不同，那么你的网络就使用了NAT。

注意：

通常，安全专家提到的 NAT 实际上是 PAT。从定义上看，NAT 将一个内部的 IP 地址映射为一个外部的 IP 地址。但是，端口地址转换(PAT)将一个内部的 IP 地址映射为一个外部 IP 地址和端口号的组合。因此，PAT 理论上在单个外部租用 IP 地址上可以支持 65 536(2^16)个来自内部客户端的、同时发生的通信。如果使用 NAT，那么租用的公共 IP 地址数必须与期望同时发生的通信数相同；如果使用 PAT，那么可以租用较少的公共 IP 地址，内部客户端数量与外部租用 IP 地址数量的适当比率为 100∶1。

在很多硬件设备和软件产品中都可以找到NAT，这些设备和产品包括防火墙、路由器、网关和代理。NAT 只能用在 IP 网络中，并且在 OSI 模型的网络层(第 3 层)上工作。

12.8.1 专用 IP 地址

近来，由于对公共 IP 地址不足和安全担忧的增加，NAT 的使用得到了快速增长。IPv4 的可用地址空间只有 40 亿个(2^32)左右，但是全世界还在部署比可用唯一 IP 地址更多的设备。幸运的是，互联网和 TCP/IP 的早期设计者具有很好的前瞻性，他们为专用的无限制的网络留出了一些地址空间。这些 IP 地址通常被称为专用 IP 地址，在 RFC 1918 中进行了定义，如下所示：

- 10.0.0.0~10.255.255.255(整个 A 类范围)
- 172.16.0.0~172.31.255.255(16 个 B 类范围)
- 192.168.0.0~192.168.255.255(255 个 C 类范围)

真实场景

不能再次进行 NAT!

在某些情况下，我们需要对已进行NAT的网络重新进行NAT。这就会发生重新进行NAT的操作:

需要在已进行 NAT 的网络内生成一个孤立的子网，并且尝试通过将驻留新子网的路由器与已有网络提供的单个端口连接在一起来完成这样的操作。

此外，如果具有只能提供单个连接的 DSL 或线缆调制解调器，但是却具有多台计算机或者希望在环境中添加无线通信，那么也可能出现这种情况。

通过连接 NAT 代理路由器或无线接入点，我们往往可以尝试对先前已进行 NAT 的网络重新进行 NAT。启用或禁用这个功能的一个配置设置是所使用的 IP 地址范围。同一子网不可能重新进行 NAT。例如，如果已有的网络提供 192.168.1.x 地址，那么在新的 NAT 子网中就不能使用相同的地址范围。因此，修改新的路由器/WAP 配置，从而对稍有不同的地址范围(例如，192.168.5.x)执行 NAT，也就不会出现冲突的情况。这似乎显而易见，但是如果没有认识到问题的实质，那么就会得到不希望看到的结果。

所有的路由器和通信控制设备被配置为在默认情况下不转发来自或到达这些 IP 地址的通信。换句话说，专用 IP 地址在默认情况下不进行路由。因此，它们不能直接用于互联网上的通信。然而，它们可以被轻松地用在专用网络中，相应的专用网络可能没有使用路由器，或者可能只对路由器的配置进行了少许改动。通过允许从 ISP 处租用较少的公共 IP 地址，结合使用专用 IP 地址与 NAT 能够大大减少连接互联网的成本。

警告：

因为所有公共可访问的路由器会丢弃包含来自专用 IP 地址范围的源或目的 IP 地址的数据包，所以在互联网上试图直接使用这些 RFC 1918 范围的地址是无用的。

12.8.2　状态 NAT

进行 NAT 操作时，会在内部客户端生成的请求、客户的内部 IP 地址以及联系的互联网服务的 IP 地址之间维护一个映射。当 NAT 从客户端接收到请求数据包时，就会将数据包的源地址从客户端的地址修改为 NAT 服务器的地址。这个变化以及目的地址被记录在 NAT 映射数据库中。一旦从互联网服务器接收到应答，NAT 就将应答的源地址与存储在映射数据库中的地址进行匹配，然后使用链接的客户端地址将响应数据包重定向至预定的目的地。由于维护了客户端和外部系统之间通信会话的相关信息，因此这个过程被称为状态 NAT。

NAT 可以在一对一的基础上进行操作，这时一次只有单个内部客户端可以通过其中一个租用的公共 IP 地址进行通信。如果数量比公共 IP 地址更多的客户端试图进行互联网访问，那么这种配置类型就会导致瓶颈的出现。例如，如果只有 5 个租用的公共 IP 地址，那么第 6 个客户端必须等到有一个地址被释放后才能在互联网上传输通信数据。其他 NAT 形式使用了多路复用技术，此时端口号被用于准许在单个租用的公共 IP 地址上管理来自多个内部客户端的通信。从技术上讲，这种 NAT 复用方式被称为端口地址转换(PAT)或超载的 NAT，但似乎行业内仍然使用术语 NAT 来指这个新的版本。

12.8.3　静态 NAT 与动态 NAT

可以使用的 NAT 有两种模式：静态 NAT 和动态 NAT。

静态 NAT　将特定的内部客户端的 IP 地址永久地映射到特定的外部公共 IP 地址时，就会使用静态模式的 NAT。即使使用 RFC 1918 定义的 IP 地址，静态 NAT 也会允许外部实体与专用网络内部的系统进行通信。

动态 NAT　动态模式的 NAT 允许多个内部客户端使用较少的租用公共 IP 地址。因此，即使租用的公共 IP 地址较少，较大的内部网络也仍然能够访问互联网。这种模式使出现公共 IP 地址滥用的情况最少，并且将互联网访问成本降至最低。

在动态模式的 NAT 实现中，NAT 系统维护了一个映射数据库，从而使来自互联网服务的所有响应信息正确地路由至最初的内部请求客户端。NAT 常常与代理服务器或代理防火墙相结合，从而提供额外的互联网访问和内容缓存功能。

因为 NAT 更改了数据包头，而 IPSec 依赖数据包头来阻止安全违规，所以 NAT 并不直接与 IPSec 相容。不过，某些版本的 NAT 代理被设计为在 NAT 上支持 IPSec。IPSec 是一种基于标准的机制，

这种机制为点对点 TCP/IP 通信提供了加密保护。

12.8.4 自动私有 IP 地址寻址

一旦 DHCP 分配失败，自动私有 IP 地址寻址(APIPA)，又叫作本地链路地址分配(在 RFC 3927 中有定义)，会为系统指派 IP 地址。APIPA 基本上是一项 Windows 功能。APIPA 为每个失败的 DHCP 客户端指派位于 169.254.0.1 到 169.254.255.254 范围内的一个 IP 地址(以及默认 B 类子网掩码 255.255.0.0)。这允许系统与同一广播域内其他配置 APIPA 的客户端进行通信，但是不能跨越路由器与任何系统通信，也不能与正确分配了 IP 地址的任何系统通信。

注意：
不要混淆 APIPA 和 RFC 1918 中定义的私有 IP 地址范围。

APIPA 通常不直接涉及安全。然而，它仍然是一个需要理解的重要问题。如果发现一个系统被分配一个 APIPA 地址而不是有效的网络地址，这说明存在问题。这个问题可能和电缆损坏或 DHCP 服务器电源故障一样平凡，但也可能是对 DHCP 服务器恶意的攻击症状。你可能会被要求解释 IP 地址分配问题出自哪里。你应该能够识别一个地址是否是公共地址、RFC 1918 私有地址、APIPA 地址或环回地址。

IP 地址数字转换

IP 地址和子网掩码实际上是二进制数，并且通过在二进制中使用，所有的路由和流量管理功能才得以实现。因此，了解十进制、二进制甚至十六进制之间的转换是非常必要的。此外，也不要忘记如何将十进制点符号表示的 IP 地址(例如，172.16.1.1)转换为相应的二进制形式(也就是 10101100000100000000000100000001)，甚至还可能需要将这个 32 位的二进制数转换为单个十进制数(也就是 2 886 729 985)。当试图验证模糊的地址时，掌握数字转换的知识是有帮助的。如果对这一领域不熟悉，那么可以利用在线转换工具，例如下面的网址：http://www.mathsisfun.com/binary-decimal-hexadecimal-converter.html

真实场景

回送地址

另一种应当小心不要与 RFC 1918 混淆的 IP 地址是回送(loopback)地址。回送地址完全是一种软件实体。这种 IP 地址被用于创建通过 TCP/IP 协议连接自身的软件接口。即使网络硬件和相关的设备驱动程序丢失、损坏或失效，回送地址也能够允许对本地网络设置进行测试。从技术上讲，完整的 127.x.x.x 网络被预留给回送使用。不过，只有 127.0.0.1 地址得到了广泛使用。

近来，Windows XP SP2 (可能还有其他更新)限制客户端只能将127.0.0.1用作回送地址，这会导致某些使用127.x.x.x网络服务的高端范围内其他地址的应用程序失败。在限制客户端只能使用127.0.0.1地址时，Microsoft会尝试打开无用的A类地址。虽然对于Microsoft来说是成功的，但是这种策略只对现代的Windows系统产生影响。

12.9　交换技术

两个系统(单独的计算机或 LAN)通过多个中间网络连接时，从一个系统向另一个系统传输数据包的任务是非常复杂的过程。为了简化这个任务，交换技术应运而生。下面首先介绍第一种交换技术：电路交换。

12.9.1　电路交换

电路交换最初是为了管理公共电话交换网中的电话呼叫而开发的。使用电路交换技术时，在两个通信方之间会创建一条专用的物理路径。一旦建立了呼叫，两个通信方之间的连接在会话过程中就将持续保持。这种交换技术提供了固定的或已知的传输时间、统一级别的通话质量，并且极少出现数据丢失或者通信中断的状况。电路交换系统使用了永久的物理连接。不过，这里的术语“永久”只是针对每个通信会话而言。在单一对话中，通信双方的物理连接路径永久地贯穿始终。连接路径被断开后，即使相同的通信双方再次进行通信，也有可能组装一条不同的路径。在单一对话期间，通信的全过程使用相同的物理或电子路径，并且这条路径只能被用于该通信。电路交换授权当前的通信双方专用的一条通信路径。只有在会话结束后，其他的通信双方才能重新使用这条路径。

真实场景

现实生活中的电路交换

在现代社会中(或者说近 10 到 15 年以来)，实际上很少存在电路交换。在数据和语音通信中，普遍存在的是接下来将要讨论的分组交换。数十年前，我们总是将公共电话交换网(PSTN)作为电路交换的主要示例，然而随着数字交换与 VoIP 系统的出现，这样的状况已经一去不返。不过，这并非意味着现实生活中不存在电路交换，而是仅仅说明电路交换不再用于数据传输。相反，仍然能够在铁路广场、灌溉系统甚至电力分布系统中发现电路交换的存在。

12.9.2　分组交换

随着计算机通信的日益增长和语音通信的萎缩，科技人员最终开发了一种新的交换形式。发生分组交换时，报文或通信先被分为若干小段(往往根据所使用的协议与技术分为长度固定的分组)，然后通过中间网络发送至目的地。每个数据段都有自己的头部，头部中包含源与目的信息。所有中间系统都会读取数据段头部中的信息，并且使用这些信息将每个分组分发至各自希望到达的目的地。每条信道和通信路径都只能在某个分组确实利用该信道进行传输时才保留供其使用，一旦分组完成发送，这条信道就会被其他通信所使用。

分组交换并不实施通信路径的排他性。因为逻辑寻址指示了通信信息如何穿越通信双方之间的中间网络，所以分组交换可以被视为一种逻辑传输技术。表 12.2 比较了电路交换与分组交换。

表 12.2 电路交换与分组交换的比较

电路交换	分组交换
连续通信	突发通信
已知的固定延迟	可变延迟
面向连接	无连接
易受连接损耗的影响	易受数据损耗的影响
主要用于语音通信	用于任何通信类型

关于安全性，需要考虑一些潜在的问题。分组交换系统将来自不同来源的数据放在相同的物理连接上。这可能会导致数据泄露、数据损坏或数据丢弃。通常需要适当的连接管理、通信隔离和加密，来防止共享物理路径的关注问题。分组交换网络的一个好处就是，它不像电路交换一样依赖于特定物理连接。因此，如果或者当一条物理路径被破坏或离线，一条备用路径可以用来继续数据/包的传递。电路交换网络经常由于物理路径被侵害而导致中断。

12.9.3 虚电路

虚电路(也被称为通信路径)是一种在两个指定端点之间的分组交换网上创建的逻辑路径或电路。在分组交换系统中，存在下列两类虚电路：

- 永久虚电路(Permanent Virtual Circuit，PVC)
- 交换虚电路(Switched Virtual Circuit，SVC)

PVC 类似于专用租用线，这种逻辑电路始终存在并等待客户发送数据。PVC 在使用前创建，但在传输结束后拆除。SVC 更像是拨号连接，因为虚电路在使用前必须使用可获得的最好的路径，然后在传输完成后进行链路拆解。在任何一种虚电路类型中，当一个数据包进入虚电路连接的点 A 时，这个数据包会被直接发送至点 B 或虚电路的另一端。然而，一个数据包的实际路径可能与同一传输中其他数据包的传输路径不同。换句话说，作为虚电路终端的点 A 和点 B 之间可能存在多条路径，但是进入点 A 的所有数据包最终都会被传输至点 B。

PVC 像是双向无线点或对讲机。无论通信何时需要，按下按钮便可以说话；无线电重新自动打开预设的频率(即虚电路)。SVC 更像是一个短波或业余无线电。每一次你想与某人进行通信时，你必须调整发射机和接收机到一个新的频率。

12.10 WAN 技术

WAN 连接用来把远端网络、节点或单个设备连接在一起。虽然可以提高通信和效率，但也会给数据带来风险。适当的连接管理和传输加密对于确保安全的连接是必要的，尤其是在公共网络上连接时。广域网连接和远程连接技术可以分为两大类：

专线(也叫作租线或点对点连接)是一种长期保留以供指定客户使用的线路(参看表 12.3)。专线始终保持畅通，并且随时等待传输通信数据。客户的 LAN 与专用 WAN 链路之间的连接始终是开放和确定的。一条专线连接两个指定终端，并且一共只连接这两个终端。

表 12.3　专线示例

技术	连接类型	速度
0 级数字信号(DS-0)	部分 T1	64Kbps 至 1.54Mbps
1 级数字信号(DS-1)	T1	1.544Mbps
3 级数字信号(DS-3)	T3	44.736Mbps
欧洲数据传输格式 1	E1	2.108Mbps
欧洲数据传输格式 3	E3	34.368Mbps
线缆调制解调器或线缆路由器		10Mbps 以上

非专线是一种在发生数据传输前需要建立连接的线路。非专线能够用于连接使用同种非专线的任何远程系统。

用不同的运营商网络连接实现故障冗余

为了在使用专线或与运营商的网络连接(也就是帧中继、ATM、SONET、SMDSF 和 X.25 等)时实现容错，必须部署两个冗余连接。如果想得到更大的冗余，那么还可以购买来自两个不同电信公司或服务提供商的连接。不过，在使用来自两个不同服务提供商的连接时，必须确认这两个服务提供商没有连接相同的地区主干网或共享任何主要的网络。如果没有财力部署第二条专线，那么可以考虑非专线的 DSL、ISDN 或线缆调制解调器连接。在主专线出现故障时，这些廉价的选择仍然能够在一定程度上满足使用需求。

标准的调制解调器、DSL 以及 ISDN 都是属于非专线的例子。数字用户线路(DSL)技术利用升级电话网使用户的通信速度达到 144Kbps 至 6Mbps(或更高)的水平。DSL 存在多种格式，例如 ADSL、xDSL、CDSL、HDSL、SDSL、RASDSL、IDSL 与 VDSL，每种格式的区别在于所提供的下行带宽和上行带宽有所变化。

提示：

针对考试而言，不必尝试死记各种 DSL 子格式的所有细节，而是只需要理解 DSL 的总体概念。

从电话总机(也就是电话网中特有的一种分配节点)开始，DSL线路的最大传输距离大约为 1000米。

综合业务数字网(ISDN)是一种完全数字化的电话网，能够同时支持语音通信和高速数据通信。ISDN 服务存在两种标准等级或格式：

- **基本速率接口(Basic Rate Interface, BRI)**为客户提供的连接具有两个 B 信道和一个 D 信道。B 信道支持 64Kbps 的吞吐量，被用于数据传输。D 信道则用于呼叫的建立、管理与拆除，带宽为 16Kbps。尽管 D 信道没有被设计用来支持数据传输，但 BRI ISDN 仍然号称为客户提供的总吞吐量为 144Kbps。
- **主速率接口(Primary Rate Interface, PRI)**为客户提供的连接具有 2 至 23 个 64Kbps 的 B 信道和一个 64Kbps 的 D 信道。因此，我们部署的 PRI 最小为 192Kbps，最大可以达到 1.544Mbps。不过需要记住的是，因为包含不能用于实际数据传输的 D 信道(至少在大多数正常的商业应用中情况如此)，所以这些数字指的是带宽而不是数据吞吐量。

提示：

当考虑连接方式时，千万不要忘记卫星连接。即使是在基于线路、无线电波或视线的通信无法到达的场所，卫星连接也仍然可能提供高速通信解决方案。不过，由于覆盖范围过大，因此卫星也被认为是不安全的。任何人都能够截获卫星通信。当然，如果使用了强加密，那么卫星通信也是相当安全的。以卫星广播为例，只要拥有收音机，就能够在任何地方接收到广播信号。但是，如果没有开通付费服务，那么无法正常收听到广播。

12.10.1 WAN 连接技术

对于在多个地点，甚至包括国外合伙人之间需要通信服务的公司来说，可以使用的 WAN 连接技术有很多。这些 WAN 技术在成本与吞吐量方面的差异相当大。不过，大多数 WAN 技术都具有对所连接 LAN 或系统透明的共同特征。WAN 交换机、专门的路由器或边界连接设备提供了在网络运营商服务与公司 LAN 之间所需的所有接口。边界连接设备也称为信道服务单元/数据服务单元(Channel Service Unit/Data Service Unit，CSU/DSU)。这些设备将 LAN 信号转换为 WAN 运营商网络所使用的格式，反之亦然。CSU/DSU 包含数据终端设备/数据电路终端设备(Data Terminal Equipment/Data Circuit-Terminating Equipment，DTE/DCE)，这些设备为 LAN 的路由器(DTE)与 WAN 运营商网络的交换机(DCE)提供了实际的连接点。CSU/DSU 起到了转换器、存储转发设备与链路调节器的作用。WAN 交换机只是 LAN 交换机的特殊形式，也就是针对特定类型的运营商网络在结构中内置了 CSU/DSU。运营商网络(或 WAN 连接技术)存在多种类型，如 X.25、帧中继(Frame Relay)、ATM 与 SMDS。

12.10.2 X.25 WAN 连接

X.25 是一种出现较早的分组交换技术，并且在欧洲范围内被广泛应用。这种技术使用永久虚电路在两个系统或网络之间建立特定的点对点连接。X.25 是帧中继的前身，二者的运作方式几乎一模一样。不过，与帧中继或 ATM 相比，X.25 自身的性能较低、吞吐速率较慢，因此在逐步走向衰落。

12.10.3 帧中继连接

与 X.25 一样，帧中继也是一种使用 PVC(详情可查看对虚电路部分的讨论)的分组交换技术。然而与 X.25 不一样的是，帧中继在一条 WAN 运营商服务连接上支持多条 PVC。帧中继是一种使用分组交换技术在通信终端之间建立虚电路的第二层连接机制。专线或租用线的成本主要取决于通信终端之间的距离，而帧中继的成本主要取决于传输的数据量。帧中继网络是一种共享介质，提供点对点通信的虚电路就被创建在这种介质中。所有虚电路都是独立的，并且彼此不可视。

承诺信息速率(Committed Information Rate，CIR)是一个与帧中继相关的重要概念。CIR 是服务提供商向客户保证的最小带宽，通常远小于服务提供商网络的实际最大带宽。根据具体约定，每位客户可能使用不同的 CIR。在有可用的额外带宽时，服务提供商可以允许客户在短时间内使用超出约定的 CIR，这也被称为按需分配带宽。尽管乍听起来似乎是一个显著的优势，然而现实情况是客户占用额外的带宽时需要附加计费。作为面向连接的分组交换传输技术，帧中继在 OSI 模型的第 2 层(也就是数据链路层)上运作。

帧中继要求在每个连接点上都使用 DTE/DCE。客户拥有 DTE (类似于路由器或交换机，并且为客户的网络提供对帧中继网络的访问)。帧中继服务提供商拥有 DCE，从而完成数据在帧中继网络上的实际传输以及为客户建立和维护虚电路。

12.10.4　ATM

与诸如帧中继之类的分组交换不同，异步传输模式(ATM)是一种信元交换 WAN 通信技术。这种技术将通信分片为若干长度固定为 53 字节的信元。通过使用长度固定的信元，ATM 更有效率，并且能够提供更高的吞吐量。ATM 既可以使用 PVC ，也可以使用 SVC。ATM 提供商保证租用服务的最小带宽与指定的质量等级。只要再付一定的费用，客户就可以在服务网络可用的情况下根据需要占用额外的带宽；与前面介绍帧中继时提到的一样，这种方式被称为按需分配带宽。ATM 是一种面向连接的分组交换技术。

12.10.5　SMDS

交换式多兆位数据服务(SMDS)是一种无连接的分组交换技术。通常，SMDS 用于连接多个 LAN，从而组成城域网(MAN)或 WAN。如果需要连接极少通信的远程 LAN，那么 SMDS 往往是首选的连接机制。SMDS 支持高速的突发通信量，并且支持按需分配带宽。SMDS 机制将数据分片为若干小的传输信元。考虑到使用了相似的技术，所以可以将 SMDS 视为 ATM 的前身。

12.10.6　专门的协议

某些 WAN 连接技术需要使用其他专门的协议来支持各种各样特殊的系统或设备。下面列出了其中三种协议：SDLC、HDLC 与 HSSI。

同步数据链路控制(SDLC)　同步数据链路控制被用在专门租用线路的永久物理连接上，从而为大型机(如 IBM 系统网络体系结构(SNA)系统)提供连通性。运作在 OSI 模型第 2 层(即数据链路层)上的 SDLC 使用了轮询技术，是一种面向比特的同步协议。

高级数据链路控制(HDLC)　高级数据链路控制是 SDLC 的改进形式，专门针对同步串行连接而设计。HDLC 支持全双工通信，并且支持点对点连接与多点连接。与 SDLC 一样，HDLC 使用了轮询技术，同样运作在 OSI 模型的第 2 层(即数据链路层)上。此外，HDLC 还提供流控制，并且包括差错检测与校正。

高速串行接口(HSSI)　高速串行接口是一个 DTE/DCE 接口标准，它定义了复用器和路由器如何连接高速网络运营商服务(如 ATM 或帧中继)。复用器是一种能够实现在单条线路或虚电路上传输多种通信或信号的设备。HSS 定义了接口或连接点的电气与物理特征，因此该协议运作在 OSI 模型的第 1 层(即物理层)上。

12.10.7　拨号封装协议

点对点协议(PPP)是一种封装协议，被设计用于支持在拨号或点对点连接上传输 IP 通信数据。PPP 允许通过 WAN 设备的多供应商互用性来支持串行连接。所有拨号连接与大多数点对点连接在本质上都属于串行连接(与并行连接相对)。PPP 包含众多通信服务，这些通信服务包括 IP 地址的分配与管理、同步通信的管理、标准化封装、复用、连接配置、连接质量测试、差错检测以及特性或

选项协商(例如，对压缩的协商)。

PPP 最初被设计用于支持针对身份认证的 CHAP 和 PAP 协议。不过，最新版本的 PPP 也支持 MS-CHAP、EAP 以及 SPAP 协议。此外，PPP 还可以用于支持网际包交换协议(IPX)和 DECnet 协议。PPP 在 RFC 1661 文档中被记录为互联网标准。PPP 替代了串行线路互联网协议(SLIP)。SLIP 只支持半双工通信，没有提供身份认证，不存在差错检测能力，并且要求人工建立与关闭链路。

12.11 各种安全控制特性

在为网络通信选择或部署安全控制时，需要根据现实环境、性能和安全策略来评估许多特性，接下来我们将详细讨论这些问题。

12.11.1 透明性

顾名思义，透明性是服务、安全控制或访问机制的一种特性，这种特性确保服务、安全控制或访问机制对于用户来说是不可见的。就安全控制而言，透明性往往是一种必要的特征。安全机制越透明，用户就越难避开安全机制，甚至无法察觉到安全机制的存在。借助于透明性，某个功能、服务或约束存在的痕迹难以被直接发现，其对性能的影响也是极小的。

在某些情况下，例如当管理员在检测、评估或调整系统的配置时，透明性可能需要更多地作为可配置特征而非固定特征。

12.11.2 验证完整性

为了验证数据传输的完整性，可以使用称为散列总数的检验和。在某条消息或某个分组被发送至通信路径之前，散列函数会对其执行运算。散列运算得到的散列总数被添加到消息的末尾，也就是消息摘要。一旦接收到消息，目标系统也会对这条消息执行散列运算，并且将运算得到的结果与先前的散列总数相比较。如果两个散列总数匹配，那么很大程度上可以确信这条消息在传输期间未被更改或者没有出现讹误。散列总数类似于循环冗余校验(CRC)，二者都可以作为完整性工具使用。在大多数安全事务系统中，散列函数用于保证通信的完整性。

真实场景

校验散列值

校验文件的散列值通常是一个不错的做法。这个简单的工作能够防止使用破损的文件，也能够防止意外接收有害的数据。某些入侵检测系统(IDS)与系统完整性验证工具将散列法作为检查文件经过一段时间是否被修改的手段。采用这种方法时，需要为驱动器上的每个文件都创建一个散列值，同时将所有散列值存储在一个数据库内，随后定期为文件重新计算散列值，并且对照原有的散列值校验新的散列值。只要发现散列值有所不同，就应当审查这个文件。

散列的另一个常见用法是验证下载的数据。许多可信的互联网下载站点为其下载文件提供了 MD5 和 SHA 散列总数。至少可以采用两种方式来利用这些散列值。第一种方式，使用能够自动校验已下载文件散列值的下载管理软件。第二种方式，使用某种散列计算工具(如 md5sum 或 sha1sum)，自己生成已下载文件的散列值，随后手动比较生成的散列值与下载站点提供的散列值。这种机制确保系统最终下载的文件能够与下载站点提供的文件完全匹配。

记录序列校验与散列总数校验类似，但是并不校验内容的完整性，而是校验分组或消息序列的完整性。许多通信服务使用记录序列校验来验证消息的任何部分都未丢失以及消息的所有元素都具有正确的顺序。

12.11.3　传输机制

传输日志是一种关注于通信的审计形式。传输日志记录了源端、目的端、时间标记、标识码、传输状态、数据包数量、消息长短等的相关细节。这些信息有助于解决故障和跟踪未授权通信，在系统中，还可以用来提取相应的数据，从而了解系统的工作方式。

传输错误校正是面向连接的或面向会话的协议和服务内置的一种能力。如果确定某条消息全部(或部分)出现损坏、被更改或丢失，那么可以请求消息源重新发送整条或部分消息。在传输差错校正系统发现通信存在问题时，重发控制确定是重发整条消息还是重发部分消息。重发控制还可以确定是发送散列总数的多个副本还是 CRC 值的多个副本，以及确定是使用多条数据路径还是使用多条通信信道。

12.12　安全边界

安全边界是任何两个具有不同安全要求或需求的区域、子网或环境之间的交线。安全边界存在于高安全性区域和低安全性区域之间，例如某个 LAN 和互联网之间。识别网络上和现实世界中的安全边界十分重要。一旦确定了安全边界，就需要部署某些控制和机制，从而控制跨越这些安全边界的信息流。

安全区域之间的分界线可能有很多形式。例如，客体可能具有不同的分类，每种分类都定义了哪些主体可以对哪些客体执行哪些操作。分类之间的区别就是安全边界。

安全边界还存在于物理环境和逻辑环境之间。为了提供逻辑安全性，必须采用与提供物理安全性不同的安全机制。二者都必须存在，从而提供完整的安全结构，并且都必须被包含在安全策略中。然而，它们之间是有区别的，在安全解决方案中必须作为独立的组件进行评估。

安全边界，例如保护区域和未保护区域之间的地带，始终应当进行清楚的定义。在安全策略中规定在哪一点上控制开始或结束，并且在物理和逻辑环境中确定这一点是非常重要的。逻辑安全边界是电子通信与组织在法律意义上负责的设备或服务的交界点。大多数情况下，这些交界的接口都是明确标记的，并且未授权主体会被告知不能访问。如果试图访问，则会受到起诉。

物理环境中的安全防线常常是逻辑环境中安全防线的反映。大多数情况下，组织化法律意义上负责的范围决定着物理区域中的安全策略范围。这可能是办公室的墙壁、建筑物的墙壁或园区周围的围墙。在受保护的环境中会张贴许多警告标志，这些警告标志指示未授权的访问是被禁止的，并

且企图进行访问的行为将被阻止和起诉。

在将安全策略转换为实际的控制时，必须分别考虑所有的环境和安全边界。简单地推导出可用的安全机制，这将为特定的环境和情况提供最合理的、最划算的和最有效的解决方案。然而，所有的安全机制都必须对要保护的客体的价值进行衡量。如果部署成本高于受保护客体的价值，那么这样的对策是不可取的。

12.13 网络攻击与对策

与 IT 基础设施的其他方面易受攻击非常类似，通信系统也容易受到攻击。理解威胁以及可能的对策对于保护运行环境来说是很重要的部分。如果可能的话，那么能够导致对数据、资源或个人产生危害的任何行为或环境都必须得到解决和缓解。需要记住的是，损害不仅包括破坏或损坏，还包括泄漏、访问延迟、拒绝访问、伪造、资源浪费、资源滥用和损失。针对通信系统安全性的常见威胁包括拒绝服务、偷听、假冒、重放和修改。

12.13.1 DoS 和 DDoS

拒绝服务攻击是一种资源消耗型攻击，以阻碍受害系统上的合法活动为主要目标。拒绝服务攻击将使目标无法响应合法流量。

有两种基本的拒绝服务攻击：

- 利用硬件或软件的漏洞进行攻击。这种利用软件的弱点、错误或标准特性导致系统发生挂起、冻结、消耗所有系统资源等情况。最终的结果是受害计算机无法处理任何合法的任务。
- 通过巨量的垃圾网络流量以泛洪的方式充满受害者的通信管道。这些攻击有时被称为流量生成或泛洪攻击。最终结果是受害计算机无法发送或接收合法的网络通信。

无论发生何种情况，受害者都没有能力执行正常的操作(服务)。

DoS 不是单一的攻击，而是一整类攻击。一些攻击利用操作系统软件中的缺陷，而其他的则把重点放在安装的应用程序、服务或协议上。一些攻击利用具体的协议，包括互联网协议(IP)、传输控制协议(TCP)、网际控制消息协议(ICMP)和用户数据报协议(UDP)。

DoS 攻击通常发生在攻击者和受害者之间。然而，它们并不总是那么简单。多数 DoS 攻击使用某种形式的中间系统(通常是不愿意和不知情的参与者)把攻击者隐藏起来不让受害者发现。例如，如果攻击者将攻击数据包直接发送给受害者，受害者将可能发现攻击者是谁。这虽然增大了难度，但不是不可能，通过使用欺骗(更详细的描述在本章其他地方)就能实现。

许多 DoS 攻击开始于破坏或渗透一个或多个中间系统，然后将中间系统作为发起点或攻击平台。这些中间系统通常被称为第二受害者。攻击者在这些系统中安装远程控制工具，这通常被称为僵尸或代理。然后，在指定的时间或根据攻击者发起的命令，对受害者发起 DoS 攻击。受害者可以能够发现造成 DoS 攻击的僵尸状态系统，但可能无法找到实际的攻击者。通过僵尸系统发起的攻击称为分布式拒绝服务(DDoS)攻击。在大量不知情的第二受害者中大量部署僵尸就变成了僵尸网络。

下面是针对这些攻击的一些对策和防御措施：

- 添加防火墙、路由器和入侵检测系统(IDS)来检测 DoS 流量和自动阻断端口或过滤基于源或目的地址的数据包。

- 与服务提供商保持良好沟通以便在 DoS 攻击发生时请求过滤服务。
- 在外部系统上禁用 echo 回复。
- 在边界系统上禁用广播特性。
- 阻断伪造数据包进入或离开网络。
- 保持所有系统已安装来自供应商的最新安全更新补丁。
- 考虑使用像 Cloud Flare 的 DDoS 缓解或 Prolexic 这样的商用 DoS 保护/响应服务。虽然可能很昂贵，但它们往往是有效的。

有关 DoS 和 DDoS 的进一步讨论，可参阅第 17 章“事件预防和响应。”

12.13.2　偷听

顾名思义，偷听是为了复制目的而对通信信息进行简单的侦听。复制采用的形式是：将数据记录到存储设备中，或者将数据记录到尝试动态从通信流中提取出原始内容的提取程序中。一旦通信内容的副本落入攻击者手中，他们就常常会从中提取出很多类型的机密信息，例如用户名、密码、处理过程、数据等。

偷听通常需要对IT基础设施进行物理的接入，从而将物理的记录设备连接到开放的端口或电缆接头，或者在系统中安装软件记录工具。偷听常常很容易通过网络通信捕获或监控程序实现，或者通过协议分析系统(常被称为嗅探器)实现。由于使用的是被动攻击方式，因此检测偷听设备和软件通常较为困难。如果偷听或窃听变成更改通信数据或在其中添加数据，就成了主动攻击。

真实场景

你也能在网络上窃听

网络上的窃听是收集通信介质上数据包的行为。作为合法的网络客户端，只能看到为系统指定的通信。但是，如果使用适当的工具(以及得到组织的授权)，就能够看到通过网络接口的所有数据。嗅探器，例如 Wireshark 和 NetWitness，以及专用的偷听工具，例如 T-Sight、Zed Attack Proxy (ZAP) 和 Cain & Abel，能够显示在网络上执行的具体操作。某些工具只显示原始网络包，另外一些工具则重新组装原始数据并将它们实时显示在屏幕上。我们鼓励拟使用一些偷听工具进行实验(只能针对被适当允许的网络)，从而使你亲身体验从网络通信中可以收集到哪些信息。

维护物理接入的安全性，从而防止未授权的人员访问你的 IT 基础设施，这种方法能够对付偷听。为了保护来自网络外部的通信或者防范来自内部的攻击，对通信传输使用加密(例如，IPSec 或 SSH)和一次性身份认证方法(即一次性填充或令牌设备)将极大地降低偷听的有效性和及时性。

常见的偷听威胁是维护可靠通信安全性的一个主要动机。与存储中的数据相比，传输中的数据往往更容易被截获。而且，通信线路可能位于组织的控制范围之外。因此，保证在内部基础设施之外安全可靠地传输数据极其重要。某些常用的网络健康以及通信可靠性评估和管理工具(例如，嗅探器)能够用于实现非法目的，所以为了防止滥用，必须对这些工具进行严格控制和监督。

12.13.3　假冒/伪装

假冒或伪装是指假装成某人或某事，从而获得对系统的未授权访问。这通常意味着认证证书被

窃取或遭受篡改以满足(即成功地绕过)认证机制。这不同于欺骗，欺骗是提出了一个虚假的身份但没有任何证据(如错误地使用 IP 地址、MAC 地址、电子邮件地址、系统名称、域名等)。假冒往往可以通过捕获网络服务会话设置中的用户名和密码加以实现。

对付假冒攻击的解决方案包括：使用一次性填充和令牌身份认证系统，使用Kerberos，使用加密，从而增加从网络通信中提取身份认证凭证的难度。

12.13.4 重放攻击

重放攻击是假冒攻击的分支，可以利用通过偷听捕获的网络通信进行攻击。重放攻击企图通过对系统重放被捕获的通信来重建通信会话。可以使用一次性身份认证机制和序列化会话身份标识来防范重放攻击。

12.13.5 修改攻击

修改攻击能够更改捕获的数据包，然后将其放回系统中。被修改的数据包被设计为能够避开改良的身份认证机制和会话排序的限制。针对修改重放攻击的对策包括数字签名验证与数据包校验与验证。

12.13.6 地址解析协议欺骗

地址解析协议(ARP)是 TCP/IP 协议族的一个子协议，工作在 OSI 模型的网络层(第 3 层)上。ARP 用于通过轮询使用系统的 IP 地址来发现系统的 MAC 地址。ARP 通过广播含有目的地 IP 地址的请求数据包进行运作，具有这个 IP 地址的系统(或其他一些已经具有该地址的 ARP 映射的系统)就会使用相关联的 MAC 地址进行应答。被发现的 IP-MAC 映射会被存储在 ARP 缓存中，并且被用于指示数据包的传输方向。

提示：

如果有兴趣了解滥用 ARP 系统对通信造成的误导，那么可以考虑使用能够完成这种功能的攻击工具进行实验。某些出名的、执行 ARP 欺骗攻击的工具包括 Ettercap、Cain & Abel 和 arpspoof。将这些工具与网络嗅探器结合使用(以便查看结果)，你会深入了解这种网络攻击形式。不过，和其他实验一样，只能在被适当许可的网络上执行这些活动，否则你的攻击行为可能会带来法律风险。

ARP 映射可能受到欺骗攻击。欺骗为请求的 IP 地址系统提供假的 MAC 地址，从而将通信重定向至另一个目的地。ARP 攻击常常是中间人攻击的一个元素。这种攻击涉及在源系统的 ARP 缓存中，将目的地的 IP 地址冒改为入侵者系统的 MAC 地址。入侵者查看从源系统接收到的所有数据包后，才将这些数据包转发至实际预定的目的系统。对付 ARP 攻击的手段包括：为关键系统定义静态的 ARP 映射，监控 ARP 缓存中的 MAC-IP 地址映射，或者使用 IDS 检查系统通信中的异常以及 ARP 通信中的变化。

12.13.7　DNS 投毒、欺骗和劫持

DNS 投毒和 DNS 欺骗也被称为解析攻击。当攻击者更改 DNS 系统中域名到 IP 地址的映射并将流量重定向到假冒系统或简单地执行拒绝服务时，DNS 投毒就发生了。当攻击者发送一个虚假响应给请求系统，并抑制来自有效 DNS 服务器的真正响应时，DNS 欺骗就发生了。这也是技术上竞争条件的利用。为阻止因投毒和欺骗而引起虚假 DNS 结果的措施包括：仅允许授权的 DNS 修改、限制传输区域和记录所有 DNS 特权活动。

2008 年，一个相当重大的漏洞被 Dan Kaminsky 发现并向全世界公开。该漏洞存在于本地或缓存 DNS 服务器从权威身份的根服务器获取特定域信息的方式中。通过发送不存在的子域虚假应答给缓存 DNS 服务器，攻击者可以劫持整个域解析的详细信息。关于解释 DNS 如何工作，以及解释这个漏洞如何威胁当前 DNS 架构，可访问“An Illustrated Guide to the Kaminsky DNS Vulnerability”，具体链接为 http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html。

关于 DNS 劫持漏洞，唯一能解决的办法就是升级 DNS 到域名系统安全扩展 (DNSSEC)。有关详细信息，请访问 dnssec.net。

12.13.8　超链接欺骗

此外，与 ARP 相关联的另一种攻击是超链接欺骗。这种类似于 DNS 欺骗的攻击用于将通信重定向至欺诈系统或冒名系统，或者简单地将通信发送至预定目的地之外的任何地方。超链接欺骗既可以采用 DNS 欺骗的形式，也可以只是简单地在发送给客户端的文档的 HTML 代码中修改超链接 URL。因为大多数用户并不通过 DNS 验证 URL 中的域名，而是认定超链接是合法的并进行单击，所以超链接欺骗攻击往往都会成功。

真实场景

进行网络钓鱼？

超链接欺骗并不仅限于 DNS 攻击。事实上，任何试图通过滥用 URL 或超链接来误导合法用户前往恶意站点的攻击活动都被视为超链接欺骗。欺骗是对信息进行篡改，包括篡改 URL 及其可信目的地和原始目的地之间的关系。

网络钓鱼是另一种经常使用超链接欺骗的攻击。网络钓鱼意味着诱骗他人上钩，从而获得信息。这种攻击可以采用很多形式，包括使用伪造的 URL。

务必提防电子邮件、PDF 文件或产品文档中的任何 URL 或超链接。如果希望访问通过这种方式提供的站点，那么可以在 Web 浏览器中手工键入地址，从而使用自己已有的 URL 书签或可信的搜索引擎查找该站点。这些方法可能会给你带来较多的工作量，但是却建立了一种获得良好服务的安全行为模式。现实生活中存在太多的攻击者，稍有疏忽或懈怠，那么盲目使用提供的链接和 URL 就很容易遭到攻击。

与网络钓鱼相关的攻击是假冒身份，这种攻击通过假冒他人获得你的个人信息。假冒身份攻击常常被用于获取个人身份细节并转卖给他人，而购买者则会滥用你的信用和名誉。

对超链接欺骗攻击的防护手段包括防止 DNS 欺骗、保持系统更新补丁并在使用互联网时采取同样谨慎的预防措施。

12.14 本章小结

远程访问安全管理需要安全系统设计者提出解决与策略、工作任务和加密相关问题的硬件、软件组合的实现方案，这包括部署安全通信协议。本地和远程连接的安全认证是整体安全的一个重要基本元素。

对于网络、语音和其他形式的通信而言，保持对通信路径的控制是维护保密性、完整性和可用性的关键。许多攻击都集中于侦听、拦截，或以其他方式干扰数据从一个位置传输到另一个位置。幸运的是，有合理的对策可以帮助减少或消除这些威胁。

隧道或封装，意味着使用一个协议的消息可以通过另一个协议在网络或通信系统中进行传输。隧道可以结合加密技术，以安全地发送消息。VPN 正是基于加密隧道。

VLAN 是由交换机产生强加的网络分段。VLAN 用于将网络逻辑分隔成网段而不改变网络的物理拓扑。VLAN 用于通信流量管理。

远程办公或远程连接，已成为商业计算的一个共同的特点。当在任何环境中部署远程访问能力时，必须考虑安全性以便为私人网络提供保护，应对远程访问难题。远程访问用户应在授予访问权限前进行严格认证，可以使用 RADIUS 或 TACACS 实现认证。远程访问服务包括 IP 语音(VoIP)、多媒体协作和即时通信。

NAT 用来隐藏专用网络的内部结构以及让多个内部客户通过少数几个公网 IP 地址访问互联网。NAT 通常是边界安全设备的默认功能，如防火墙、路由器、网关和代理。

在电路交换中，一条专用的物理路径将在两个通信方之间建立。把消息或通信分解成小的分段(通常是固定长度的数据包，这取决于采用的协议和技术)，并发送到中间网络，最终到达目的地时，分组交换就发生了。分组交换系统内有两种类型的通信：路径和虚电路。虚电路是在两个指定节点之间，创建在分组交换网络上的逻辑路径或电路。有两种类型的虚电路：永久虚电路(PVC)和交换虚电路(SVC)。

WAN 链路或远程连接技术，可以分为两个主要类别：专线和非专线。专线连接两个特定的端点并且只有这两个端点。非专线在需要数据传输时才进行连接。非专线可以用同样的非专线连接任何远程系统。 WAN 连接技术类型包括 X.25、帧中继、ATM、SMDS、SDLC、HDLC 和 HSSI。

当选择或部署网络通信的安全控制时，需要按照所在环境、能力和安全策略评估诸多特性。安全控制应该对用户透明。哈希和 CRC 校验可用于验证消息的完整性。记录序列用来保证传输序列的完整性。传输日志有助于检测通信滥用。

虚拟化技术用来在一台主机的内存中启动和运行一个或多个操作系统。这个机制允许几乎任意操作系统在任意硬件上运行，还允许多个操作系统同时在同一硬件上工作。虚拟化提供了几个好处，例如，能够在需要的情况下启动单个服务器或服务的实例、实时的可扩展性，并且能够运行应用程序所需的操作系统版本。

基于互联网的电子邮件是不安全的，除非采取措施以确保它的安全。为了电子邮件的安全，应该提供不可否认性、限制用户访问权限、确保完整性得到维护、验证消息来源、核实交付，甚至对敏感内容进行分类。这些安全措施在实施解决方案之前必须在安全政策中全部声明。它们经常以可

以接受的使用政策、访问控制、隐私声明、电子邮件管理程序、备份和保留政策的形式出现。

电子邮件是一种常见的恶意代码传递机制。过滤附件、使用防病毒软件，并对用户进行教育是有效对抗攻击的对策。垃圾邮件或邮件泛滥是一种形式的拒绝服务攻击，可以通过过滤器和 IDS 进行阻断。电子邮件可以使用 S/MIME、MOSS、PEM 和 PGP 来改善安全性。

通过使用加密保护文件的传输并防止窃听，可以提高传真和语音的安全性。有效培训用户是对抗社会工程学攻击的对策。

安全边界是一个安全区域和另一个安全区域之间的边界划分，也可以是安全区域和非安全区域之间的边界划分。两者都必须在安全策略中加以应对。

通信系统容易受到许多攻击，包括分布式拒绝服务(DDoS)、窃听、假冒、重放、篡改、欺骗、ARP 和 DNS 攻击。幸运的是，存在有效的对策应对以上这些问题。PBX 欺骗和滥用，以及盗用电话线也是必须解决的问题。

12.15　考试要点

理解围绕远程访问安全管理的问题。远程访问安全管理需要安全系统设计者连同策略、工作任务和密码学等问题一起，提出硬件和软件组合的解决方案。

熟悉各种可能在 LAN 和 WAN 中用于数据通信的协议和机制。这些协议和机制包括 SKIP、SWIPE、SSL、SET、PPP、SLIP、CHAP、PAP、EAP 和 S-RPC，还包括 VPN、TLS/SSL 和 VLAN。

了解什么是隧道技术。隧道技术利用另一个协议封装可以使用某个协议传输的消息。此处所讲的另一个协议常常通过加密来保护消息内容的安全。

理解 VPN。VPN 建立在加密隧道技术的基础上，能够作为点对点方案提供身份认证和数据保护。常见 VPN 协议包括 PPTP、L2F、L2TP 以及 IPSec。

能够解释 NAT。NAT 保护专用网络的寻址方案，准许专用 IP 地址的使用，并且使多个内部客户端能够利用有限的几个公共 IP 地址访问互联网。NAT 得到许多安全边界设备的支持，这些边界安全设备包括防火墙、路由器、网关和代理。

理解分组交换和电路交换之间的差异。在电路交换中，通信双方之间会创建一条专用的物理路径。发生分组交换时，消息或通信先被分为若干小段，然后通过中间网络发送至目的地。分组交换系统内存在两种逻辑路径或虚电路：永久虚电路(PVC)和交换虚电路(SVC)。

理解专线和非专线之间的差异。专线是一种长期保留以供指定客户使用的线路。专线示例包括 Tl、T3、E1、E3 以及线缆调制解调器。非专线是一种在发生数据传输前需要建立连接的线路。非专线能够用于连接使用同种非专线的任何远程系统。非专线示例包括标准的调制解调器、DSL 以及 ISDN。

了解和远程访问安全相关的问题。熟悉远程访问、拨号连接、屏幕截取、虚拟应用/桌面和一般远程办公的安全关注点。

了解各种 WAN 技术。了解大多数 WAN 技术都需要信道服务单元/数据服务单元(CSU/DSU)，它们也被称为 WAN 交换机。运营商网络和 WAN 连接技术存在多种类型，例如 X.25、帧中继、ATM 与 SMDS。某些 WAN 连接技术需要使用其他专门的协议来支持各种各样特殊的系统或设备，其中三种协议是 SDLC、HDLC 和 HSSI。

理解 PPP 和 SLIP 之间的差异。点对点协议(PPP)是一种封装协议，被设计用于支持在拨号或

点对点连接上传输 IP 通信数据。PPP 包含众多通信服务，这些通信服务包括 IP 地址的分配与管理、同步通信的管理、标准化封装、复用、链路配置、链路质量测试、差错检测以及特性或选项协商(例如，对压缩的协商)。PPP 最初被设计用于支持针对身份认证的 CHAP 和 PAP。不过，最新版本的 PPP 也支持 MS-CHAP、EAP 以及 SPAP。PPP 代替了串行线路网络协议(SLIP)。SLIP 只支持半双工通信，没有提供身份认证，不存在差错检测能力，并且要求人工建立与关闭链路。

理解安全控制的常见特征。安全控制应当对用户透明。散列总数和 CRC 校验可以用于验证消息的完整性。记录序列用于确保传输的序列完整性。传输日志记录能够帮助检测通信的滥用情况。

理解如何实现电子邮件的安全性。互联网电子邮件基于 SMTP、POP3 和 IMAP，其本身是不安全的。电子邮件可以受到保护，但是必须在安全策略中说明所使用的保护方法。电子邮件的安全性解决方案包括 S/MIME、MOSS、PEM 或 PGP 的使用。

了解如何实现传真的安全性。传真的安全性主要基于使用加密的传输或通信线路来保护通过传真发送的内容，主要目标是防止截获。活动日志和异常报告能用于检测传真中表现为攻击征兆的异常活动。

了解与 PBX 系统相关联的威胁以及针对 PBX 伪造的对策。针对 PBX 伪造和滥用的对策与许多保护典型计算机网络的预防措施相同，包括逻辑或技术性控制、行政管理性控制以及物理性控制。

理解与 VoIP 相关的安全问题。VoIP 的风险包括呼叫者 ID 欺骗、语音钓鱼、SPIT、呼叫管理软件/硬件攻击、电话硬件攻击、DoS、MitM、欺骗和交换机跳跃等。

识别什么是飞客。飞客行为是一种针对电话系统的特定攻击类型。飞客使用各种技术回避电话系统，从而获得免费的长途呼叫、更改电话服务的功能、窃取特殊的服务甚至导致服务中断。常用的飞客工具包括黑盒、红盒、蓝盒和白盒。

理解语音通信的安全性。语音通信系统容易受到很多攻击，特别是当语音通信成为网络服务的重要部分时。使用加密通信可以获得机密性。为了防止受到拦截、偷听、分机窃听和其他形式的利用，必须部署相应的对策。熟悉各种语言通信类型，例如 POTS、PSTN、PBX 和 VoIP。

能够解释什么是社会工程学。社会工程学是不认识的人获得组织内部某个人信任的一种方式。擅长社会工程学的人可以使员工相信他们是上层管理人员、技术支持人员或服务台人员等。受害者常常会被怂恿在系统中修改他们的用户账户，例如重新设置密码。对付这种类型攻击的主要对策是对用户进行培训。

解释安全边界的概念。安全边界可以是受保护区域之间的分界，也可以是受保护区域和非受保护区域之间的分界。二者都必须在安全策略中加以说明。

理解与通信安全性相关联的各种攻击和对策。通信系统容易受到很多攻击，包括拒绝服务攻击(DDoS)、偷听、假冒、重放、修改、欺骗以及 ARP 和 DNS 攻击。要能够列出每种攻击的有效对策。

12.16 书面实验室

1. 阐述 IPSec 的传输模式和隧道模式的不同。
2. 阐述 NAT 的好处。
3. 电路交换和分组交换的主要区别是什么？
4. 关于电子邮件有哪些安全问题，有哪些安全对策可以进行应对？

12.17　复习题

1. _____是一种数据链路层连接机制，使用分组交换技术在通信方之间建立虚电路。
   A. ISDN
   B. 帧中继
   C. SMDS
   D. ATM
2. 隧道连接可以在除了以下哪一项之上进行建立？
   A. WAN 链路
   B. 局域网路径
   C. 拨号连接
   D. 孤立系统
3. _____是一种标准算法，用于提供点对点 TCP/IP 流量加密？
   A. UDP
   B. IDEA
   C. IPSec
   D. SDLC
4. 以下哪个 IP 地址不是 RFC 1918 中定义的私有网络地址？
   A. 10.0.0.18
   B. 169.254.1.119
   C. 172.31.8.204
   D. 192.168.6.43
5. 以下哪一个不能在 VPN 上进行连接？
   A. 两个远程互联局域网
   B. 两个在同一局域网内的系统
   C. 一个连接到互联网的系统和一个连接到互联网的局域网
   D. 两个无中介网络连接的系统
6. 如果网络使用 NAT 代理，需要什么才能允许外部客户端通过内部系统发起连接会话？
   A. IPSec 隧道
   B. 静态 NAT
   C. 静态私有 IP 地址
   D. 反向域名解析
7. 下列哪种 VPN 协议不提供本地数据加密？(选择所有可能选项)
   A. L2F
   B. L2TP
   C. IPSec
   D. PPTP
8. 以下哪个 OSI 层提供 IPSec 协议功能？
   A. 数据链路层

B. 传输层
C. 会话层
D. 网络层

9. 以下哪一项不是 RFC 1918 中定义的不能在互联网上进行路由的私有 IP 地址段?
A. 169.172.0.0~169.191.255.255
B. 192.168.0.0~192.168.255.255
C. 10.0.0.0~10.255.255.255
D. 172.16.0.0~172.31.255.255

10. 以下哪一个不是 NAT 的好处?
A. 隐藏内部 IP 地址
B. 大量的内部客户端可共享少数公共的互联网地址
C. 在内部网络中使用 RFC 1918 中定义的私有地址
D. 过滤网络流量以预防蛮力攻击

11. 安全控制的一个重要好处是可以运行在用户不知不觉的情况下，这个特性称为?
A. 隐形
B. 透明
C. 导流
D. 躲在平原的视线

12. 为互联网传送邮件设计安全系统时，以下哪一项是最不重要的?
A. 不可否认性
B. 可用性
C. 信息完整性
D. 访问限制

13. 关于电子邮件保留策略，下列哪一项是通常不是必须与用户讨论的元素?
A. 隐私
B. 审计审查
C. 保持器长度
D. 备份方法

14. 邮件本身被当成攻击机制，这种攻击称为?
A. 伪装
B. 邮件炸弹
C. 欺骗
D. smurf 攻击

15. 为什么垃圾邮件难以阻止?
A. 阻断入站信息的过滤器通常没有那么有效
B. 源地址通常都进行了欺骗
C. 攻击成本很低
D. 垃圾邮件可导致拒绝服务攻击

16. 下列哪一种类型的连接可以被描述为一条逻辑电路，总是存在并等待客户发送数据?
A. ISDN

B. PVC

C. VPN

D. SVC

17. 除了维护、更新系统和进行物理访问控制，下面哪一项是应对 PBX 欺骗和滥用的最有效反制措施？

A. 加密通信

B. 改变默认密码

C. 使用传输日志

D. 录音和归档所有的会话

18. 以下哪个攻击可以用来绕过即使是最好的物理和逻辑安全机制来访问系统？

A. 蛮力攻击

B. 拒绝服务

C. 社会工程学

D. 端口扫描

19. 以下哪一项不是拒绝服务攻击？

A. 利用程序的一个漏洞让它消耗 100%的 CPU 计算能力

B. 向一个系统发送恶意构成的数据包，导致它死机

C. 向某个已知的用户账户发起蛮力攻击

D. 向某个地址发送成千上万封电子邮件

20. 下列哪个验证协议不提供加密或登录凭据保护？

A. PAP

B. CHAP

C. SSL

D. RADIUS

第 13 章

管理身份与认证

本章中覆盖的 CISSP 考试大纲包含：

5. 身份与访问管理

- A. 物理控制与资产的逻辑访问
  - A.1 信息
  - A.2 系统
  - A.3 设备
  - A.4 设施
- B. 管理人员和设备的身份与认证
  - B.1 身份管理实施(例如，SSO、LDAP)
  - B.2 单/多因素认证(例如，因素、强度、错误、生物特征)
  - B.3 可问责性
  - B.4 会话管理(例如，超时、屏保)
  - B.5 身份的注册与证明
  - B.6 联合身份管理(例如，SAML)
  - B.7 证书管理系统
- C. 身份整合服务(例如，云身份)
- D. 第三方身份整合服务(例如，内部部署)
- G. 管理身份与访问开通生命周期(例如，开通、审查)

身份与访问管理域关注的是授予和撤消访问系统数据或执行系统操作的特权问题。主焦点是识别、认证、授权和可问责性。本章和第 14 章“控制和监控访问”将讨论身份与访问管理域范围内的所有目标。一定要阅读和学习这两章的内容，以确保了解与该域相关的所有必要知识。

13.1 控制对资产的访问

控制对资源的访问是安全性的一个中心话题，并且你将发现许多不同的安全控制会结合在一起

来提供访问控制。资产可以包括信息、系统、设备、设施和人员。

信息 组织的信息包括与其相关的所有数据。这些数据可能存储在服务器、电脑和其他小型设备的简单文件夹中，也可能存储在服务器群组的巨大数据库中。访问控制试图阻止对这些信息的未授权访问。

系统 组织的系统包括提供一种或多种服务的所有 IT 系统。比如，一个用于存储用户文件的简单文件服务器就是一个系统。再比如，与数据库服务器协同工作来提供电子商务服务的 Web 服务器也可以称为系统。

设备 设备包括所有的计算系统，包括服务器、台式电脑、便携式笔记本电脑、平板电脑、智能手机和外部设备等，比如打印机。越来越多的组织采用自备设备(BYOD)，允许员工将他们的个人设备连接到组织的网络。虽然这些设备是所有者的财产，但存储在这些设备上的组织的数据仍然属于组织的资产。

设施 组织的设施包括组织拥有或租赁的所有有形场所。可能是单独的一间房、一栋建筑或几栋建筑的综合体。物理安全控制有助于保护设施。

人员 为组织工作的人员也是组织的宝贵资产。保护人员的主要方法之一就是确保有足够的安全措施以防止人员受伤或死亡。

13.1.1 主体与客体的对比

访问控制所涉及的内容不仅仅是控制哪些用户可以访问哪些文件或服务，还涉及主体和客体之间的关系。从客体到主体的信息传输称作访问，理解主体和客体的定义是非常重要的。

主体 主体是活动的实体，通过访问被动客体来获得客体的信息或数据。主体可以是用户、程序、进程、文件、计算机或访问资源的任何东西。通过授权后，主体就可以修改客体。

客体 客体是提供信息给活动主体的被动实体。客体可以是文件、数据库、计算机、程序、进程、打印机和存储介质等。

提示：

通常以用户一词代替主体，以文件一词代替客体，如此可简化关于访问控制的主题。例如，在主体访问客体时，可以看作用户在访问文件。然而，清楚主体不只是用户以及客体不只是文件也很重要。

你可能已经注意到了一些实例，如程序和电脑，它们既可当作主体，也可当作客体。这是因为主客体的角色可来回转变。很多情况下，当两个实体相互作用时，它们会执行不同的功能。它们有时可能是在请求信息，而有时是在提供信息。主要区别是，主体通常是主动的实体，从被动客体处接收信息或数据。客体通常是被动的实体，用于提供或寄存信息或数据。

比如，向用户提供动态 Web 页面的常见 Web 应用程序。用户通过访问 Web 应用程序检索网页，因此应用程序启动时是客体。随后当 Web 应用程序访问用户电脑以检索 cookie 以及基于检索到的 cookie 访问数据库，从而进一步检索用户信息时，又转换为主体角色。最后，当 Web 应用程序把动态 Web 页面发送给用户时，又转变为客体角色。

13.1.2　访问控制的类型

一般来说，访问控制是与所有控制访问资源相关的硬件、软件或管理类策略或程序，目标是向授权主体提供访问并阻止任何未经授权的蓄意访问。访问控制的总体步骤如下：

(1) 识别和认证试图访问资源的用户或其他主体。

(2) 确定访问是否获得授权。

(3) 基于主体身份允许或限制访问。

(4) 监测和记录访问尝试。

这些步骤包含很多控制。主要的三种控制类型是预防、检测和纠正。无论何时，都可以阻止任何类型的安全问题或事件。当然，并不是总能阻止，也并非总会发生意外事件。一旦发生意外，你会希望尽快检测出该事件，如果检测到了，你会希望做出修正。

另外 4 种访问控制类型通常是制止、恢复、指引和补偿访问控制。

读到下文所列控制时，你会注意到有些举例所列控制不止出现在一种访问控制类型中。比如，围绕建筑四周的防护栏(或以周长进行定义的设备)可以成为预防性控制，因为是从本身物理结构上阻止进入建筑场地的可能。然而，这也是一种制止性控制，因为对那些企图进入场地的人也起到了制止作用。

预防性访问控制　预防性访问控制试图阻碍或阻止有害的或未授权活动的发生。预防性访问控制的示例包括围墙、锁、生物测定学、陷阱、灯照、警报系统、职责分离、岗位轮换、数据分类、渗透测试、访问控制方法、加密、审计、使用安全摄像头或闭路电视(CCTV)、智能卡、回叫程序、安全策略、安全意识培训、反病毒软件、防火墙和入侵防御系统。

检测性访问控制　检测性访问控制试图发现或检测有害的或未授权的活动。通常，检测性控制并不实时进行，而是在活动出现后运作。检测性访问控制的示例包括保安、移动探测仪、记录和检查安全摄像头或闭路电视(CCTV)捕获的事件、岗位轮换策略、强制休假策略、审计跟踪、蜜罐、入侵检测系统、违规报告、对用户的监管和检查以及事故调查。

纠正性访问控制　纠正性访问控制是为了在发生有害的或未授权的操作后，将系统还原至正常的状态。纠正性访问控制试图纠正发生安全事件造成的任何问题。纠正性访问控制通常较为简单，例如终止恶意软件活动或重启系统。纠正性访问控制的示例包括移除和隔离病毒的反病毒解决方案、确保丢失数据被恢复的备份和存储计划，以及能修改环境以阻止攻击过程的入侵检测系统。

注意：

第 16 章“管理安全运营”将更深入地覆盖入侵检测系统和入侵防御系统。

威慑性访问控制　部署威慑性访问控制是为了试图吓阻违反安全策略的活动。威慑和预防性访问控制比较类似，但是威慑性访问控制经常依赖人员去决定是否采取有害的行动。相反，预防性访问控制实际阻止了有害活动。一些示例包括策略、安全意识培训、锁、围墙、安全徽章、保安、陷阱和安全摄像头。

恢复性访问控制　恢复性访问控制是为了在出现违反安全策略的情况后修复或还原资源、功能与性能。与纠正性访问控制相比，恢复性访问控制响应访问违规的性能更高级、更复杂。恢复性访问控制的示例包括备份和还原、容错驱动系统、系统镜像、服务器群集、反病毒软件以及数据库或虚拟机影像。

指令性访问控制 指令性访问控制是为了指示、限制或控制主体的活动，从而强制或鼓励主体遵从安全策略。指令性访问控制的示例包括安全策略需求或标准、张贴通告、疏散路线出口标志、监控、监督和规程。

补偿性访问控制 当主控制不能用时，或者当需要对主控制增加有效性时，补偿性访问控制提供了另一种选择。举个例子，组织的安全策略可能规定全体员工需要使用智能卡，但新员工需要很长的时间才能拿到智能卡。因此，组织用硬令牌作为补偿性访问控制来为员工解决这个问题。这些令牌提供了比用户名和密码更强的认证功能。

根据实现方式，访问控制还可以进一步分类。访问控制能够分为行政管理性访问控制、逻辑/技术性访问控制以及物理性访问控制。前面提到的任何访问控制都能归入这些实现的类型中。

行政管理性访问控制 行政管理性访问控制是依照组织的安全策略和其他规则或需求，而定义的策略与过程。它们有时被称为管理控制。这些控制主要关注两个方面：人员与业务实践。行政管理性访问控制的示例包括策略、过程、雇用准则、背景调查、数据分类、安全意识和培训、报告与回顾、人员控制以及测试。

逻辑/技术性访问控制 逻辑性访问控制(也称为技术性访问控制)作为硬件或软件机制用于提供对这些资源和系统的保护。顾名思义，它们使用技术。逻辑或技术性访问控制的示例包括认证方式(例如，密码、智能卡、生物测定学)、加密、受限接口、访问控制列表、协议、防火墙、路由器、入侵检测系统以及阀值级别。

物理性访问控制 物理性访问控制是能物理触摸到的东西。它们包括部署以预防、监控或检测与设施内的系统或区域直接接触的物理机制。物理性访问控制的示例包括保安、围墙、移动探测仪、闭锁的门、密封窗、灯照、线缆保护、笔记本电脑锁、徽章、磁条卡、看门狗、摄像头、陷阱以及报警器。

提示：

在准备 CISSP 考试时，需要能够识别所有类型的控制。例如，应该认识到防火墙是一种预防性控制，因为它可以通过阻断通信来防止被攻击；而入侵检测系统(IDS)是一种检测性控制，因为它可以检测到正在发生的攻击或已经发生的攻击。你也应该能够识别所有的逻辑/技术性访问控制。

13.1.3 CIA 三要素

组织施行访问控制机制的一个主要原因就是预防损失。IT 损失主要有三种：机密性损失、可用性损失以及完整性损失。预防这些损失的发生对 IT 安全性而言是不可或缺的，它们经常被称为 CIA 三要素(有时也被称为 AIC 三元素或安全三元素)。

机密性 访问控制能帮助确保只有被授权的主体可以访问客体。当未被授权的实体成功访问了系统或数据时，就导致了机密性损失。

完整性 完整性确保数据或系统配置在未经授权的情况下不会被修改，或者如果发生了未经授权的更改，安全控制能够检测出发生的变化。如果客体发生了未被授权或不希望发生的改变，就导致了完整性损失。

可用性 给予主体对客体的授权请求必须在合理的时间范围内。换句话说，系统和数据应在用户和其他主体需要时能为它们所用。如果系统不能进行操作或无法访问数据，就导致了可用性损失。

13.2　比较身份标识与认证

身份标识是主体声称或自称某个身份的过程。主体必须向系统提供身份标识，才能够启动身份认证、授权和可问责过程。提供的身份标识可以是输入用户名、刷卡、出示令牌设备、说一段话，也可以是将脸、手掌或手指靠近照相机或扫描设备。认证的一条核心原则就是所有的主体必须有唯一的身份。

通过与有效身份数据库中的一个或多个因素进行比对，身份认证能够认证主体的身份，如用户账户。用于核实身份的身份认证信息属于私人信息，需要保护。例如，密码很少以明文存储在数据库中。相反，身份认证系统把密码以散列形式存储在认证数据库内。主体和系统对身份认证信息的保密能力直接反映了系统的安全级别。

身份标识和认证总是被放在一起成为单一的双步过程。第一步是提供身份标识，第二步是提供身份认证因素。如果缺少这两步，主体就不能获得访问系统的能力。

每种认证技术或因子都有各自的优缺点。因此，在系统使用环境中进行机制评估十分重要。例如，存储绝密资料的设施需要非常强大的认证机制。相比之下，课堂环境的身份认证设施要明显弱一点。

提示：

身份识别和认证可以简化为只要用户名和密码。用户凭借自己的用户名可以进行识别，凭借密码进行认证(或证明其身份)。当然，还有很多识别认证方法，但这种简化形式相对而言更加清晰。

13.2.1　身份的注册和证明

用户首次获得身份的过程就是注册过程。组织在招聘过程中，新员工要提供适当文件以证明他们的身份。然后，人力资源部门的人事专员就开始为这些新员工创建他们的用户 ID。

由于安全身份认证方法的不同，注册过程也会随之更为复杂。例如，如果组织使用指纹生物认证法进行认证，注册时也就需要捕捉用户指纹。

身份证明因用户交互网站的不同而不同，比如银行网站。当用户首次试图创建账户时，银行需要对用户的身份进行额外认证。通常是让用户提供双方都可知的信息(如账号)以及个人信息(如用户的身份证号或社会安全号)。

在首次注册时，银行还会要求用户提供其他信息，如用户喜欢的颜色、他们亲属的中间名或第一辆车的型号。之后，如果用户需要更改密码或转账，银行可以询问用户这些问题作为证明用户身份的方法。

13.2.2　授权与可问责性

访问控制系统的两个额外安全元素是授权和可问责性。

授权　依据主体的证明身份授予其客体访问权限。例如，管理员基于用户的证明身份授予用户访问文件的权限。

可问责性　在执行审计时用户和其他主体要对自己的行为负责。审计负责追踪主体并且记录他们对主体的访问，需要在单个或多个审计日志中创建审计跟踪。例如，当用户阅读、修改或删除文

件时审计会进行记录。审计具有可问责性。

有效的访问控制系统除了满足授权和可问责性外，还需要强大的身份识别和认证机制。主体有独特的身份并能通过认证证明自己的身份。管理员基于主体的身份给予他们访问的权限。基于认证后的身份进行用户行为的记录具有可问责性。

相比之下，如果用户登录不需要凭据，那么所有用户都是匿名用户。这种情况不可能对特定用户进行授权限制。日志仍然可以记录事件，但是无法识别是哪些用户做了何种操作。

1. 授权

授权就是指出谁获得信任以执行某具体操作。如果某个行为获得许可，主体就获得了授权；如果未获得许可，就是未被授权。这里有一个简单的例子：如果用户试图打开一个文件，授权机制会进行检查以确保该用户至少有读取该文件的权限。

意识到下面这一点很重要：如果用户或其他实体可以在某系统成功认证，不能仅仅因为他们被成功认证就表示他们有权访问某个或所有东西。相反，主体访问特定客体的权限要基于他们被认证的身份。授权过程确保了执行所请求的活动或客体访问是可能的，但要基于该主体拥有的权限。

身份识别和认证在访问控制方面“要么全有，要么全无”，而不管用户的认证信息是否被承认。相比之下，授权却各不相同。例如，用户可以读取文件但不能进行删除，或是可以打印文档但不能改变打印队列。

2. 可问责性

审计、记录和监控都具有可问责性，以此确保主体对自己的行为要担负责任。审计是通过日志对主体行为进行问责和记录的过程。日志通常记录的是谁采取了行动、行动发生的时间和地点，以及发生了什么样的行动。一个或多个日志创建了审计跟踪表，研究人员可以用此表重塑事件以及确认安全事件。当调查者审查审计跟踪的内容时，他们可以提供证据以确认人们对自我行为应担负的责任。

对可问责性强调的虽少，但却很重要。可问责性必须依靠有效的识别和认证，但不需要有效的授权。换句话说，在识别和认证用户身份后，可问责性机制(如审计日志)就可以跟踪用户的活动，即使他们试图访问并没有获得授权的资源。

13.2.3 认证因素

认证的三种基本方法也被称为类型或因素。它们是：

类型 1 类型 1 身份认证因素是“你知道什么”。这些内容示例包括密码、个人标识码(PIN)或密码短语。

类型 2 类型 2 身份认证因素是“你拥有什么”。用户拥有能够帮助他们提供身份认证的物理设备，示例包括智能卡、硬令牌、记忆卡和 USB 驱动器。

注意：

智能卡和记忆卡之间的主要差异是：智能卡具有处理数据的能力，而记忆卡只用于存储信息。例如，智能卡包括微处理器，还可以用证书进行认证、对数据进行加密、进行电子邮件的数字签名等。记忆卡仅存有用户认证信息。

类型 3　类型 3 身份认证因素是“你是什么或者你做什么”。这里指的是某个身体部分或人的生物行为特征。“你是什么”的示例包括指纹、语音波纹、视网膜样本、虹膜样本、脸部形状、掌纹和手型等。“你做什么”的示例包括签名和击键力度，也称为生物行为特征。

在正确实施了这些类型的控制后，访问控制也逐渐增强，其中类型 1 最弱，类型 3 最强。换句话说，密码(类型 1)是最弱的，指纹(类型 3)要比密码强一些。然而，攻击者仍然可以绕过类型 3 的身份认证因素。例如，攻击者可以用熊软糖制作指纹以欺骗指纹阅读器。

你的位置是什么

除了上述三种常见的身份认证因素(“你知道什么”、“你拥有什么”、“你是什么”)之外，另一个值得注意的因素是“你的位置是什么”。通过识别主体登入的计算机终端、进行连接操作的电话号码(通过呼叫者的 ID 来标识)或国家(通过 IP 地址来标识)，确定主体的物理位置。“你的位置是什么”访问控制强制主体存在于某个特定的位置。例如，考虑用户从他们的家里拨入远程访问时，呼叫者 ID 和回拨技术用于认证用户是否实际在家里拨入。

这个因素不依靠它的拥有者，因为一个专注的攻击者可以欺骗任何类型的地址信息。因此，只有和其他因素联合使用才会有效。

13.2.4　密码

最常见的身份认证技术是使用类型 1 认证方式(“你知道什么”)的密码(用户输入的一串字符)。密码是静态的。静态密码在一段时间(例如，30 天)保持不变，因此静态密码是最弱的认证方式。密码是较差安全机制的原因有很多，其中包括：

- 用户常常选择他们很容易记忆的密码，因此这些密码易于猜测或破解。
- 随机生成的密码很难记忆，因此很多用户都会将它们写下来。
- 密码很容易共享和遗忘。
- 窃取密码的手段有很多，包括观察、监听网络和盗取安全数据库。
- 密码的传递常常通过明文或使用易于破解的协议进行。攻击者用网络监听捕捉这些密码。
- 密码数据库常常存储在可访问的联机公共位置。
- 通过穷举攻击可以快速破解短密码。

密码加密

密码很少以明文存储。相反，系统会使用散列算法(比如 PBKDF2(Password-Based Key Derivation Function 2))创建密码散列。散列是一个数值，如果密码相同，该算法总是会创建出相同的数值。当用户输入密码进行身份认证时，系统会对密码进行散列操作并将这些信息与存储的散列密码相比较。如果它们是一样的，系统就成功认证了用户身份。

1. 创建强密码

由用户创建的强密码是最有效的。强密码十分长，会用到多个字符类型，如大写字母、小写字母、数字和特殊字符。组织在总的安全策略中通常会包括书面密码策略。IT 安全专家利用技术控制执行这些策略，比如，技术密码策略能执行对密码的限制要求。下面的列表包含一些常见的密码策略设置：

最长使用期 这个设置需要用户定期更改密码，如每 45 天更改一次。

密码复杂性 密码复杂性是指密码包含多少字符类型。使用大写字母、小写字母、符号和数字的 8 字符密码远比只使用数字的 8 字符密码安全。

密码长度 密码长度是密码的字符数量。密码越短，越容易被破解。举例来说，密码破解者可以用不到一秒钟的时间破解一个复杂的 5 字符密码，但破解一个复杂的 12 字符密码几乎不可能。许多组织要求特权账户的密码至少达到 15 个字符长。这种要求克服了在一些 Windows 系统上存储密码的弱点。

密码历史功能 许多用户有交替使用两个密码的习惯。密码历史功能可以记住前一个密码的特定值，如此可防止用户使用之前用过的密码。这一功能通常与最短密码使用期结合使用，能够防止用户不断修改密码，直到设置成原来用过的一个密码。最短密码使用期通常设置为一天。

用户常常不明白对强密码的需要。即使他们这样做，也往往不知道创造他们可以很容易记住强密码。下面的建议可以帮助他们创建强密码：

- 不要用名字的任何部分、登录名、电子邮件地址、员工号码、社会保险号码、电话号码、分机号码或其他标识身份的名字或代码的任何部分。
- 不要使用社交网络的个人资料信息，如家庭成员的名字、宠物的名字或出生日期。
- 不要使用字典中的单词(包括国外字典的单词)、俚语或行业缩略词。
- 应使用非标准的大写和拼写方法。
- 应利用特殊字符和数字来代替字母。

在某些环境中，系统自动为用户账户创建了初始密码。产生的密码经常是组合密码，其中包括两个或更多个不相关的数字或符号连接在一起的形式。计算机容易生成组合密码，但它们不应该被长期使用，因为它们很容易受到密码猜测攻击。

2. 密码短语

比基本密码更有效的密码机制是密码短语。密码短语类似于密码字符的字符串，但对于用户具有独特的意义。为了简化记忆，密码短语往往是修改过的自然语言语句。例如，“I passed the CISSP exam”会被转换为这样的密码短语“IP@$$edTheCISSPEx@m”。使用密码短语有不少优点。使用穷举攻击工具很难破解密码短语，而且密码短语鼓励使用含大量特征的长的字符串，但仍然很容易记住。

3. 认知密码

认知密码是另一种密码机制。认知密码通常是一系列问题，这些问题应该是只有主体才知道的事实或预定义的结果。认证系统通常在账户初始注册过程中收集这些问题的答案，但它们可以被收集或更改。例如，主体可能会被询问如下 3 至 5 个问题：

- 你的生日是哪一天？
- 你母亲的名字是什么？
- 你的第一个部门领导是谁？
- 你的第一个宠物叫什么名字？
- 你喜欢的运动是什么？

后来，系统能够使用问题进行身份认证。如果用户正确地回答了所有问题，系统完成对用户的身份认证。最有效的密码认知系统能收集数个问题的答案，然后在每次使用时会列出不同问题的组

合。认知密码经常与自助密码重置系统或辅助密码重置系统协同使用。例如，如果用户忘记原来的密码，他们可以寻求帮助。然后密码管理系统会要求用户回答一个或多个认知密码问题，这些问题一般只有用户知道。

注意：

与认知密码相关的缺陷之一是，信息是通过互联网传送的。打比方说，攻击者如果能够攻破萨拉•佩林(Sarah Palin，2008 年副总统候选人)的个人雅虎电子邮件账户，再通过从社交媒体页面得知的关于萨拉•佩林的个人信息，就能够回答雅虎找回程序显示的问题。最好的认知密码系统允许用户创建自己的问题和答案，这就给攻击者增加了很多难度。

13.2.5　智能卡和令牌

智能卡和硬令牌，或者你持有的一些东西都属于身份认证类型 2。这一类型通常会和另一种认证因素结合使用，很少单独使用，从而能够提供多因素的身份认证。

1. 智能卡

智能卡是信用卡大小的 ID 或徽章，中间嵌入了集成电路芯片。智能卡包含用于识别和/或认证的授权用户信息。最新的智能卡包含一个微处理器和一个或多个证书。证书用于非对称加密，比如加密数据或数字签名的电子邮件等(关于非对称加密的内容在第 7 章“PKI 和密码学应用”中有详细介绍)。智能卡能够防止篡改，为用户提供了一种携带和使用复杂加密密钥的简单方法。

用户在进行身份认证时将卡插入智能卡阅读器。通常要求用户输入与智能卡相匹配的个人识别码或密码，作为身份认证的第二因素。

注意：

注意，智能卡既可以进行身份识别，也可以进行身份认证。然而，因为用户可以共享或交换智能卡，所以这不是有效的识别方法。实行智能卡时大多会要求用户另外设置一个身份认证因素，如 PIN 或一套用户名和密码。

美国政府内部人员使用通用访问卡(CAC)或个人身份认证卡(PIV)。CAC 和 PIV 卡是智能卡，里面包含了所有者的照片和其他识别信息。用户四处走动时需要像戴徽章一样带着它们，登录时要把它们插入电脑的读卡器。

2. 令牌

令牌或硬令牌是一种密码生成设备，用户可以随身携带。现在，常用令牌都包含一个显示器，能够显示 6 到 8 位号码。身份认证服务器存储着令牌的详细内容，所以在任何时候，服务器都可以知道用户令牌上显示的号码。令牌通常要与另一个身份认证机制结合使用。例如，用户可以输入用户名和密码(你知道的身份认证因素)，然后输入令牌上显示的号码(你必须持有的身份认证因素)。这就是多因素的身份认证。

硬令牌使用的是一次性动态密码，这比静态密码安全得多。令牌的类型有两种：同步动态密码令牌和异步动态密码令牌。

同步动态密码令牌　创建同步动态密码的硬令牌是基于时间的，并与身份认证服务器保持同步。

它们定期生成一个新密码，如每隔 60 秒。这也就要求令牌和服务器必须有精确的时间。常用方法是要求用户在 Web 页面上输入用户名、静态密码和一次性动态密码。

异步动态密码令牌 异步动态密码不使用时间。相反，该硬令牌依据算法和递增计数器生成密码。当使用递增计数器时，它会创建一个一次性的动态密码，这个密码会一直保持不变，直到用于身份认证。有些令牌在用户输入由令牌身份认证服务器提供的 PIN 码时，会生成一次性密码。例如，用户首先要向 Web 页面提交用户名和密码，在认证用户信息后，认证系统将用令牌的标识符和递增计数器创建一个数字并发送给用户。这个数字在用户每次认证时都会改变，所以被称为一次值(nonce，全称为“number used once”，意思是仅使用一次的数字)。这个数只能在设备上生成属于用户的一次性正确密码。用户把这串数字输入令牌中，令牌就会生成一个密码。然后，用户把这个密码输入网站方可完成身份认证过程。

硬令牌能提供强大的身份认证，但也有缺点。如果电池没电或设备中断了，用户将无法访问。

一次性密码生成器

一次性密码是每次使用时都会变化的动态密码。很少有人能够记住过于频繁变化的密码，但一次性密码能够有效地实现安全目的。一次性密码生成器可以为用户创建密码，从而能够合理地部署一次性密码。使用基于设备的身份认证系统，在不必对用户记忆力提出过高要求的情况下，特定环境就能够受益于一次性密码的强大安全性。

13.2.6 生物识别

另一种常用的身份认证和身份标识技术是使用生物识别。生物识别因素属于类型 3 身份认证类别，即“你是什么”。

生物识别因素可以用于识别或认证技术，或两者兼而有之。使用生物因素而非用户名或账户 ID 作为识别因素，需要将提供的生物图案与数据库中存储登记和授权的图案进行一对多的搜索比对。捕捉一个人的单人图像，然后在数据库中搜索匹配，就是典型的一对多搜索示例。作为识别技术，生物识别因素可用于物理访问控制。

使用生物识别因素作为身份认证技术，需要与主体提供存储的身份图样进行一对一的生物识别图样比对。换句话说，用户提供了一种身份，在提供生物因素时就要核对该因素是否与之前提供的身份相匹配。作为身份认证技术，生物识别因素可用于逻辑访问控制。

生物特征通常是指生理或行为上的特征。生物生理识别方法包括指纹、面部扫描、视网膜扫描、虹膜扫描、手掌扫描(也称为手掌特征或手掌纹理)、手形和语音模式。生物行为识别方法包括动态签名和击键模式(击键力学)。这些有时被称为“你做什么”的身份认证。

指纹 指纹就是人们 4 指和大拇指上的可见图样。每个人的指纹都是独一无二的，其作为物理安全身份识别已有几十年。指纹读取器现在通常装在笔记本电脑和 USB 闪存驱动器中，用作身份识别和认证方法。

脸部扫描 脸部扫描利用脸部的几何图样来进行检测和识别。如果曾经看过电视节目 *Las Vegas*，你可能已经看到过他们如何利用一个人的图片，然后匹配数据库中的面部特征。这使他们能够快速地识别一个人。同样，在访问安全空间，例如安全库之前，脸部扫描被用于识别和认证。

视网膜扫描 视网膜扫描关注的是眼睛后方血管的图案。虽然视网膜扫描是最精确的生物识别身份认证形式(能够区分同卵双胞胎)，但却最不被人接受，原因在于会泄露个人医疗状况，如高血

压与妊娠。旧的视网膜扫描方式会往用户的眼睛里吹气，但新的往往用红外光代替。

虹膜扫描　作为第二精确的生物测定学身份认证形式，虹膜扫描关注的是瞳孔周围的有色区域。不过，虹膜扫描无法对同卵双胞胎进行区分。虹膜扫描通常被认为比其他任何生物测定学因素具有更长的身份认证期限。这是因为在人的一生中，虹膜相对保持不变(除非眼睛受损或患上眼疾)。虹膜扫描对比视网膜扫描更容易被大部分人接受，但是通过用一些高品质的图像代替人的眼睛，一些扫描器会被欺骗。此外，精度会受到灯光变换的影响。

手掌扫描　手掌扫描(有时被称为手掌特征或手掌纹理)通过扫描手掌进行识别。用近红外光测量手掌的静脉模式，这些跟指纹一样，是独一无二的。不需要接触扫描仪，只需要把手掌放在扫描仪的上方。例如，佛罗里达州的许多学校使用手掌扫描仪在午餐时间识别学生身份，一些医院也用手掌扫描仪来识别病人。一些手掌扫描仪，包括手指扫描和测量手背、折痕和凹槽的布局，进行整只手的扫描。

手形　手形技术用于识别手部的物理尺寸，包括手掌和手指的宽度与长度。它能捕获手的轮廓，但不能捕捉指纹细节或静脉模式。很少单独使用手形，因为很难靠这种方法识别出一个人。

心跳/脉搏模式　该模式涉及测量用户的脉搏与心跳次数，从而确保是真实用户提供了生物识别因素。这种技术通常作为支持其他某种生物识别类型的辅助生物识别因素。一些研究人员提出心跳是独一无二的，认为可以用心电描记法进行身份认证。然而，这方面到现在为止还没有研发或全面测试出一种可靠的方法。

声音模式识别　这种生物特征识别技术依靠一个人说话的声音特点，称为声纹。用户说出一个特定的短语，然后认证系统对此进行记录。在进行身份认证时，他们要重复这一短语，然后再与原始语音比较。声音模式识别有时可作为额外的身份认证机制，但很少单独使用。

注意：

语音识别常常与声音模式识别相混淆，但它们是不同的。语音识别软件，如听写软件，可以从声音中提取通话信息。换句话说，声音模式识别是在区分声音与声音之间的不同，以便用作识别或认证，而语音识别是在区分词语与人声之间的区别。

签字力度　这种生物识别因素识别主体如何书写字符串。签字力度查看主体的书写动作以及书写样本中的特征。签字力度因素的成功依赖于用笔的压力、笔划方式、笔划长度以及提笔时间点。不过，创建书写样本的速度通常不是重要的因素。

击键模式　击键模式(又称击键力度)通过分析抬指时间与按压时间来确定主体使用键盘的方式。抬指时间指的是前后两次击键之间的时间，而按压时间指的是按下一个键的时间。使用击键模式进行身份认证非常廉价、毫无侵扰，并且对于用户来说(包括使用与注册)往往是透明的。遗憾的是，使用击键模式来保证安全性这种方式容易产生重大偏差。用户行为的细小变化会显著地影响这种生物测定学身份认证，例如，只使用一只手击键、手部冰冷、站着而不是坐着、更换键盘以及手部或手指受伤等。

使用生物识别是希望为地球上的每一个人都提供唯一的身份标识。遗憾的是，目前的生物测定学技术尚未实现这一点。然而，专注于认证物理特性的技术非常有用。

1. 生物识别因素的错误率

生物特征设备的最重要方面是它的准确性。为使用生物特征识别，生物识别设备必须能够检测出信息的微小差异，如某人视网膜中血管的变化或色调，还有声音的音色。因为大多数人基本类似，

生物识别方法通常导致负面的和不正确的认证。生物识别设备通过检查他们生产的不同类型错误来衡量执行情况。

类型 1 错误 类型 1 错误发生在当一个正确的主体没有被认证时，这也被称为错误的身份认证。例如，当 Dawn 用她的指纹来认证自己时，系统不正确地拒绝她。对于正确用户的类型 1 错误率被称为错误拒绝率(False Rejection Rate，FRR)。

类型 2 错误 类型 2 错误发生在当无效认证发生时，这也被称为假正确身份认证。例如，如果黑客 Joe 没有账户，但他用自己的指纹进行身份认证并且系统承认了他，这就是假正确身份认证。类型 2 错误率被称为错误接受率(False Acceptance Rate，FAR)。

许多生物识别设备都能够灵敏地加以调整。当生物识别设备过于灵敏时，类型 1 错误(错误拒绝)会更加常见。当生物识别设备不够敏感时，类型 2 错误(误报)会更加常见。

可以通过交叉错误率(Crossover Error Rate，CER)比较生物识别设备的整体质量，交叉错误率也被称为相等错误率(Equal Error Rate，ERR)。图 13.1 显示了当一台设备设置为不同灵敏度水平时，FRR 和 FAR 的百分比。FRR 和 FAR 比例相等的点是 CER，CER 作为标准的评估值来比较不同的生物识别设备的精度。低 CER 的设备比高 CER 的设备更准确。

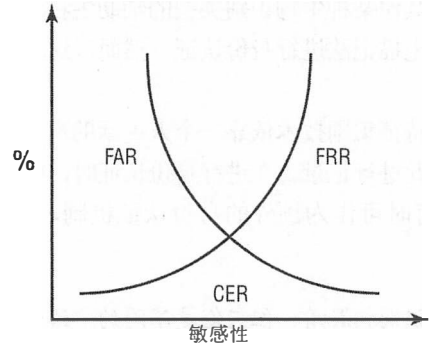


图 13.1 CER 点的 FRR 和 FAR 错误率

没必要将操作设备的灵敏度设置在 CER 的水平，并且这也经常是不可取的。例如，组织可能会使用面部识别系统允许或拒绝访问某个安全区域，因为他们想确保未经授权的人不能访问。在这种情况下，组织将灵敏度设置得非常高，所以类型 2 错误(误收)就很少有机会发生。这可能会导致更多误拒，但是在这个场景中误拒比误收更容易接受。

2. 生物识别注册

有一些因素会使生物识别设备变得不太有效和不可接受，这些因素包括登记时间、吞吐能力以及认可度。对于生物识别设备来说，主体只有被登记或注册，设备才能作为身份标识或身份认证机制使用。在注册过程中，主体的生物识别因素必须被采样并存储在设备的数据库中。被存储的生物识别因素的采样被称为基准轮廓(reference profile)或基准模板(reference template)。

扫描和存储生物识别因素所需的时间在很大程度上依赖于使用的物理或性能特征。利用生物识别机制进行登记的时间越长，用户就越不愿意接受这种麻烦。一般而言，登记时间超过两分钟是不可接受的。如果使用随时间变化的生物识别特征(如人的语调、头发或签字模式)，就必须定期进行重新登记。

主体一旦被登记，系统扫描和处理主体所需的时间就被视为吞吐能力。生物识别特征越复杂、

越详细，处理的时间也就越长。通常，主体接受吞吐能力的时间为 6 秒钟或更短。

13.2.7　多因素身份认证

多因素认证是使用两个或多个因素进行认证。双因素身份认证需要使用两个不同的因素来提供身份认证。例如，在杂货店用支票付账时，通常需要提供驾照(“你拥有什么”)和 PIN 码(“你知道什么”)。类似地，智能卡通常需要用户插入卡片到读卡器中并且也要输入 PIN 码。一般情况下，使用不同类型的因素，身份认证就更安全。

提示：

多因素身份认证必须使用多种类型或多个因素，比如你知道的一些因素和你持有的一些因素。相比之下，要求用户输入密码和 PIN 并不能算作多因素身份认证，因为这两种方法都属于一种身份认证因素(你知道的因素)。

当使用两个相同的因素时，系统的强度并不会超过单独使用其中一个因素的系统的强度。只要攻击能够窃取或获得特定因素的一个实例，那么相同的攻击就能够窃取或获得特定因素的所有实例。例如，同时使用两个密码并不比只使用一个密码更安全，这是由于如果密码破解攻击能够成功破解一个密码，那么这种攻击就能够破解两个密码。

相比下来，使用两个或多个不同的因素时，两个或多个不同的攻击类型或攻击方法要想成功，就必须收集所有相关的身份认证元素。例如，如果令牌、密码和生物识别因素共同被用于身份认证，那么只有在偷窃物品、破解密码与生物识别复制攻击同时成功的情况下才能进入指定系统。

13.2.8　设备认证

从历史上看，用户只能通过公司拥有的系统登录网络，如桌面电脑等。举例来说，在一个 Windows 域中，用户的计算机要加入这个域，计算机账户和密码要与用户的账户和密码相似。如果计算机没有加入该域，或其凭证与域的控制器不同步，用户将无法用这台电脑登录。

如今，越来越多的员工在工作时会携带自己的设备，然后将这些设备连接到网络进行工作。一些组织接纳这一行为，但会实施 BYOD 安全策略，以此作为控制措施。这些设备没必要加入一个域，但也有可能对这些设备实行身份识别和认证措施。

一种方法是设备指纹。用户可以在组织中对自己的设备进行注册，并将这些设备与他们的用户账户联系起来。注册期间，设备认证系统会捕获设备特性，通常还需要让用户用此设备访问一个网页。然后注册系统能通过特征识别出这些设备，如操作系统和版本、Web 浏览器、浏览器字体、浏览器插件、时区、数据存储、屏幕分辨率、cookie 设置和 HTTP 头。

当用户从此设备登录时，身份认证系统能通过注册设备检查该用户的账户。然后，它会根据此注册设备认证用户设备的特征。尽管这些特性可能会随时间变化，但时间已证明这是一种成功的设备认证方法。组织通常会使用第三方工具，比如安全身份认证提供者(IdP)，进行设备认证。

13.3 实施身份管理

身份管理技术分为两类：集中式和分散式(或分布式)。

- 集中式访问控制意味着所有的授权认证都由系统内的单个实体执行。
- 分散式访问控制或分布式访问控制意味着授权认证由位于系统中的不同实体执行。

集中式与分散式访问控制具有所有集中式或分散式系统的优缺点。集中式访问控制可以由小型团队或个人进行管理。由于所有的更改都在单个位置进行，因此管理开销较小。此时，单个更改就可以影响整个系统。

分散式访问控制常常需要几个团队或多个人参与。由于更改必须在许多地方实现，因此管理开销较大。随着访问控制点的增加，系统的一致性维护工作变得越来越困难。对任何个人接入控制点所做的更改，需要在每个接入点进行多次重复更改。

13.3.1 单点登录

单点登录(Single Sign-On，SSO)是一种集中式访问控制技术，允许主体只在系统上认证一次并且可以不用认证身份而访问多个资源。例如，用户可以在网络上进行一次认证，然后就可以访问整个网络资源，不用被提示进行再次认证。

SSO 对用户来说非常方便，但在安全性上也有所加强。当用户需要记住多个用户名和密码时，他们经常会写下来，最终反而降低了安全性。如果只有一个密码，用户是不太可能写下来的。SSO 还通过降低主体需要的账户数量，让管理也更加容易。

SSO 的主要缺点是：一旦账户被破解，恶意主体就会拥有不受限制的访问权限。但是，大多数 SSO 系统含有保护用户凭据的方法。

以下各节讨论几种常见的SSO机制。

13.3.2 LDAP 和集中式访问控制

单个组织经常使用集中式的访问控制系统。例如，目录服务是一个集中式数据库，里面包含了主客体信息。许多目录服务建立在轻量级目录访问协议(Lightweight Directory Access Protocol，LDAP)的基础上。例如，Microsoft 动态目录域服务就是以 LDAP 为基础的。

可以把 LDAP 目录看作网络服务和资产的电话目录。用户、客户和流程可以搜索目录服务以找到所需系统或资源的存储地方。主体在执行查询和查找活动前，必须认证目录服务。即使在认证后，目录服务依据主体权限也只会显示关于主体的某些信息。

访问控制系统经常会用到多个域和信任关系。安全域是主客体的集合，共用一个安全策略，单个域可以独立于其他域单独操作。信任是域和域之间建立的安全桥梁，允许用户从一个域访问另一个域中的资源。信任可以是一种方式，也可以是两种方式。

13.3.3 LDAP 和 PKI

在整合数字证书以便传输时，公钥基础设施(PKI)使用 LDAP。第 7 章对 PKI 做了深入介绍，但

简而言之，PKI 是一组技术，在证书的整个生命周期中实现对数字证书的管理。很多时候，客户需要向证书授权组织(CA)进行有关证书信息的咨询活动，此时 LDAP 就是用到的协议之一。

LDAP 和集中式访问控制系统可用于支持单点登录功能。

13.3.4　Kerberos

票证身份认证这种机制采用第三方实体证实身份并提供身份认证。最常用的，也是最知名的票证系统是 Kerberos。

注意：

Kerberos 的名字源于希腊神话。一只长有三个头的狗名为 Kerberos，它守护着通往阴间的大门。这只长有三个头的狗脸朝内，目的是防止逃跑而非防止进入。

Kerberos 给用户的提供是单点登录解决方案以及能够保护登录信息。现在的 Kerboros 5 版本依赖的是对称密钥加密(又称密钥式密码)，使用的是对称加密的高级加密标准(AES)协议。Kerberos 使用端对端安全机制保障认证通信的机密性和完整性，有助于预防窃听和重放攻击。理解 Kerberos 所用的几个不同元素很重要：

密钥分发中心　密钥分发中心(Key Distribution Center，KDC)是提供身份认证服务的可信第三方。Kerberos 使用对称密钥加密认证需要登录服务器的客户。所有客户和服务器都用 KDC 做了注册，所有网络成员的密钥都由 KDC 维持。

Kerberos 身份认证服务器　身份认证服务器托管 KDC 的功能：票据授予服务(Ticket-Granting Service，TGS)和身份认证服务(Authentication Service，AS)。然而，可能在另一台服务器上托管票据授予服务。身份认证服务认证或拒绝票据的真实性和及时性。这台服务器通常被称为 KDC。

授予票证　授予票证(Ticket-Granting Ticket，TGT)通过 KDC 提供主体已认证的证明，并授权请求访问其他客体的票据。TGT 已进行加密，并且包括对称密钥、过期时间和用户的 IP 地址。主体在请求访问客体的票据时，会出示 TGT。

票据　票据是加密的信息，证明主体已被授权访问某个对象。票据有时被称为服务票据(Service Ticket，ST)。主体请求访问客体的票据，如果他们已经进行认证，并被授权访问对象，Kerberos 会向他们发放一张票据。Kerberos 票据有特定的寿命和使用参数。一旦票据到期，就必须要求客户续期或申请新票据以继续与任何服务器通信。

Kerberos 需要账户数据库，这通常包含在目录服务中。它使用客户、网络服务器和 KDC 之间的票据交换来证明身份并提供身份认证。这允许客户端从服务器请求资源，但客户端和服务器都应该能够确保双方的身份。这些加密的票据也确保登录凭证、会话密钥和认证消息不会以明文传输。

Kerberos 登录过程如下：

(1) 用户将用户名和密码键入客户端。

(2) 客户端使用 AES 加密用户名，然后传输至 KDC。

(3) KDC 使用已有证书的数据库来认证用户名。

(4) KDC 产生一个同步密钥，用于客户端和 Kerberos 服务器间的通信。它加密用户密码的散列值。KDC 也生成一个有加密时间戳的授予票证(TGT)。

(5) KDC 然后传输加密过的同步密钥和加密过的带有时间戳的 TGT 给客户端。

(6) 客户端安装 TGT，一直使用直至期满。客户端也使用用户的散列解密对称密钥。

注意：

请注意客户的密码从来没有在网络上进行传播，但它已经过认证。服务器使用散列的用户密码加密对称密钥，且只能用散列的用户密码来解密。只要用户输入正确的密码，这一步就发挥作用。然而，如果用户输入不正确的密码，就失败了。

当客户端要访问一个对象时，如托管在网络上的资源，它必须通过 Kerberos 服务器请求票据。下面是这个过程涉及的步骤：

(1) 客户端将其 TGT 发送回 KDC，同时请求访问某个服务器或服务。

(2) KDC 认证 TGT 的有效性并查看其访问控制矩阵，从而认证用户是否拥有能够访问所请求资源的足够权限。

(3) KDC 生成一个服务票据，然后将它发送至客户端。

(4) 客户端发送票据至服务器或服务主机。

(5) 服务器或服务主机通过 KDC 认证服务票据的有效性。

(6) 一旦认证了用户身份与授权，Kerberos 活动就完成了。服务器或服务主机随后建立与客户端的会话，从而开始进行通信或数据传输。

作为一种多用途的身份认证机制，Kerberos 可以用在本地 LAN、本地登录、远程访问以及客户端-服务器资源请求中。然而，Kerberos 存在单点故障，也就是 KDC 会出现单点故障。如果 KDC 被破解，那么网络中所有系统的秘密密钥也都会被破解。此外，如果 KDC 离线，那么就无法对主体进行身份认证。

它也有严格的时间要求和默认的配置要求，即所有的系统彼此要在 5 分钟内同步时间。如果一个系统不同步或时间被改变了，以前发出的 TGT 将不再是有效的，系统将无法接收任何新的票据。实际上，客户端将被拒绝访问任何受保护的网络资源。

13.3.5 联合身份管理和 SSO

在相当长一段时间内，SSO 在内部网络上是常见的，但在互联网上不常见。然而，随着基于云的应用程序的爆发式增长，用户访问互联网资源渐渐开始需要 SSO 解决方案。联合身份管理是一种能够满足这一需求的 SSO 形式。

身份管理是对用户身份和凭证的管理。联合身份管理超越了单一的组织。多个组织可以加入一个联盟或一个组，他们同意通过一个方法共享彼此的身份。每个组织的用户在各自的组织登录一次且在他们的凭证和联合身份相匹配后，他们就可以使用这个联合身份来访问这一组中任何其他组织的资源。

联盟可以由一个大学校园、多个大学校园、多个共享资源的组织或者其他可以达成共同联合身份管理系统的组织内的多个不相关的网络构成。联盟的成员将组织中的用户身份与联合身份相匹配。

例如，许多企业在线培训网站使用联合 SSO 系统。当组织与在线培训公司协调员工访问事宜时，他们还需要协调联合访问所需的细节。一个常见的方法是将用户的内部登录 ID 和联合身份进行匹配。组织内的用户使用正常的登录 ID 进行登录。当用户用 Web 浏览器访问培训网站时，联合身份管理系统使用他们的登录 ID 来检索匹配的联合身份。如果找到匹配，用户就会被授予联合身份被授予的网页访问权。

管理员在后台管理这些细节，过程对用户来说通常都是透明的。用户不需要再次输入他们的凭证。

如果有多家企业联盟，那么当他们互相交流时就需要找到一种共同语言，这是一种挑战。他们通常会有不同的操作系统，但他们仍需拥有共同语言。为满足这一需要，这些联合身份系统常常使用安全声明标记语言(SAML)或服务配置标记语言(SPML)。作为背景，此处对一些标记语言进行了简短描述。

超文本标记语言　超文本标记语言(HTML)普遍用于展示静态网页。HTML 源自标准通用标记语言(SGML)和通用标记语言(GML)。HTML 使用标签描述数据的显示方式，以操控文本的大小和颜色。例如，H1 后的标签将文本作为一级标题显示，可表示为：<H1>I Passed The CISSP Exam</H1>。

可扩展标记语言　可扩展标记语言(XML)超越了对数据显示方式的描述，而实现了对数据本身的描述。XML 所包含的标签可以将数据描述为任何所需的样子。例如，以下标签识别了作为测验结果的数据：<Exam Results>Passed</Exam Results>。

多家供应商的数据库可以将数据输入为 XML 格式，或从 XML 格式输出数据，从而使 XML 成为用于信息交流的共同语言。现已创建许多特定模式，因此这些企业清楚地知道为实现特定目的该用何种标签。

安全声明标记语言　安全声明标记语言(SAML)是一种基于 XML 的语言，普遍用于联合组织之间交换认证和授权(AA)信息，常为浏览器访问提供单点登录(SSO)功能。

服务配置标记语言　服务配置标记语言(SPML)是基于 XML 的新框架，但是出于联合身份单点登录目的，专门设计用于用户信息交换。SPML 基于目录服务标记语言(DSML)，而 DSML 能够以 XML 格式显示基于轻量级目录访问协议(LDAP)的目录服务信息。

访问控制标记语言　访问控制标记语言(XACML)用于在 XML 格式内定义访问控制策略，并且通常实现基于角色的访问控制。XACML 有助于给联盟中的所有成员提供保证，保证他们向不同角色授权相同级别的访问。

提示：

SAML 是互联网上流行的 SSO 语言。XACML 已经成为流行的软件定义网络应用。

13.3.6　其他单点登录的例子

美国麻省理工学院开发的安全认证系统(Kerberos)也许是组织内单点登录最为广泛认可和部署的形式，但并不是同类中的唯一。在本节中，我们总结了你也许会遇到的其他单点登录系统。

在登录会话开始时，脚本访问或登录脚本通过自动化处理发送登录凭证，从而建立通信连接装置。即使环境仍需要单独的身份认证过程来连接每个服务器或资源，脚本访问通常也可以模拟单点登录访问。单点登录技术不可用时，脚本在环境中可实现单点登录。脚本和批处理文件通常包含明文形式的访问凭证，所以应被存储在受保护的区域内。

欧洲安全多环境应用系统(SESAME)是一个基于邀请的认证系统，它被开发出来是为了解决 Kerberos 的缺点。然而，SESAME 并没有解决 Kerberos 的所有问题。新一代的 Kerberos 和多家供应商的实施都绕过了 SESAME，最终解决了 Kerberos 最初版本的所有问题。在安全行业，SESAME 已不再被认为是一款可行的产品。

KryptoKnight 是 IBM 开发的一个基于邀请的认证系统。它与 Kerberos 相似，但是使用对等认证而非第三方认证。KryptoKnight 被纳入 NetSP 产品。SESAME、KryptoKnight 和 NetSP 从未盛行，并且再也不会被广泛使用。

OAuth(意为公开认证)和 OpenID 是应用于网络单点登录的较新的例子。OAuth 是一个开放标准，它与 HTTP 协作，允许用户以单一账户登录。例如，用户可登录他们的谷歌账户，并用同一账户登录 Facebook 和 Twitter。谷歌支持 OAuth 2.0，而 OAuth 2.0 不向后兼容 OAuth 1.0。OAuth 2.0 被编号为 RFC 6749。OpenID 也是一个开放标准，但是它由电脑软件公司 OpenID Foundation 维护，而非作为 IETF RFC 标准。OpenID 可与 OAuth 连同使用，也可单独使用。

13.3.7 证书管理系统

当单点登录不可用时，证书管理系统为用户的凭证保存提供存储空间。用户可为需要一套不同凭证的网站和网络资源存储凭证。证书管理系统确保这些凭证已加密，从而防止未经授权的访问。

例如，Windows 系统包含证书管理器工具。用户将他们的凭证输入证书管理器，必要时，操作系统检索用户的凭证，并自动提交。在网站上应用时，用户输入 URL、用户名和密码。当用户之后访问网站时，证书管理器会自动识别 URL 并提供凭证。

第三方证书管理系统也可用。例如，KeePass 允许存储凭证，是一款免费软件。凭证储存于一个加密数据库中，用户可用主密码解锁。一旦解锁，用户可轻松地复制他们的密码，并粘贴成网站形式。它也可用于配置应用程序，自动输入凭证到网页形式。当然，用一个强大的主密码来保护其他所有凭证十分重要。

13.3.8 整合身份服务

身份服务为识别和认证提供了额外工具。其中一些工具是为那些基于云的应用程序具体设计的，而其他的工具是第三方身份服务，为组织内部使用而设计(内部部署)。

身份即服务或身份和访问即服务(IDaaS)，是一个第三方服务，提供身份和访问管理。IDaaS 为云有效提供单点登录，并在内部客户访问那些基于云的软件即服务(SaaS)应用程序时特别有用。谷歌公司的箴言“一个谷歌账户登录所有谷歌产品”就是这一技术的体现。用户只需登录他们的谷歌账户一次，就可以访问谷歌多个基于云的应用程序，不必再次进行登录。

再举一个例子，Office 365 结合安装的应用程序和 SaaS 应用程序来提供办公应用程序。用户的全套办公应用系统都安装在他们的用户系统中，还可以使用 OneDrive 连接到云存储。这就使用户可以在多个设备上编辑并共享文件。当人们在家使用 Office 365 时，微软提供 IDaaS，使得用户通过云在 OneDrive 上对访问他们的数据进行认证。

当雇员在企业内使用 Office 365 时，管理员可以与第三方服务集成网络。例如，Centrify 提供与微软活动目录集成的第三方 IDaaS 服务。一旦配置完成，用户登录到域名，然后不必再次登录就可以访问 Office 365 云资源。

13.3.9 管理会话

无论使用何种认证系统，重要的是管理会话，以防止未经授权的访问。这包括与应用程序在普通电脑(如台式电脑)上的会话或网络会话。

台式电脑和笔记本电脑包含屏幕保护程序。当开启的电脑不被使用时，屏幕保护系统通过展示随机的图案或不同的照片，或者只是简单的白屏，来改变电脑显示。屏幕保护程序保护了较旧电脑

的屏幕，但是新的显示器并不需要这些。然而，屏幕保护程序仍被使用，并有可启用的密保功能。此功能显示登录屏幕，迫使用户退出屏幕保护程序前再次进行身份认证。

屏幕保护程序有一个可以配置的几分钟时间范围。通常设置为 10 至 20 分钟之间。如果将其设置为 10 分钟，屏幕保护程序就会在系统空闲 10 分钟后激活。若系统空闲 10 分钟或更长，就需要用户再次登录。

一段时间后安全网络会话也会终止。例如，在网上银行界面建立一个安全会话，但是在 10 分钟内没有进行交互操作，该应用程序就会使你掉线。在某些情况下，应用程序会提示你即将掉线。这些提示通常给你单击网页的机会，这样就可以保持在线。如果开发者不实施这些自动掉线功能，就会允许用户在登录的情况下保持浏览器会话打开，甚至在用户没有下线的情况下关闭浏览器标签，浏览器会话也会暂时保持开启。这时，若他人访问浏览器，该用户的账户就很容易受到攻击。

13.3.10　AAA 协议

提供认证、授权和可问责性的协议叫作 AAA 协议。它们提供集中式访问控制，并且附带虚拟专用网(VPN)和其他类型的网络访问服务器的远程访问系统。它们可以保护内部局域网认证系统和其他服务器免受远程攻击。当使用一个单独的系统进行远程访问时，对系统的成功攻击只会影响远程访问用户。换句话说，攻击者不会有内部账户的访问权限。为智能手机用户提供访问的移动 IP 也使用 AAA 协议。

这些 AAA 协议使用的是本章前面描述的访问控制元素，包括识别、认证、授权和可问责性。它们确保用户用有效的凭据来进行身份认证，并根据已证实的身份来认证用户已被授权连接到远程访问服务器。此外，追踪元素可以跟踪用户的网络资源使用情况，并达到计费目的。一些常见的 AAA 协议有 RADIUS、TACACS+以及 Diameter。

1. RADIUS

远程认证拨号用户服务器(RADIUS)主要用于远程连接的身份认证。当组织有不止一台网络访问服务器(或远程访问服务器)时，RADIUS 通常会被用到。用户可以连接到任何一台网络访问服务器，服务器会将用户的凭据传送给 RADIUS 服务器来认证用户的身份和权限，并对其进行追踪。在这种情况下，网络访问服务器就相当于 RADIUS 客户端，RADIUS 则作为身份认证服务器。RADIUS 服务器还为多个远程访问服务器提供 AAA 服务。

许多互联网服务提供商(ISP)使用 RADIUS 进行身份认证。用户可以在任何地方访问 ISP，ISP 服务器会将用户的连接请求发送给 RADIUS 服务器。

组织也可以使用 RADIUS 协议，并与回调安全程序同时执行，进而实现进一步的保护。用户拨入，并在身份认证后，RADIUS 服务器会终止连接，并对用户预定义的电话号码发起呼叫。如果用户的凭据被盗用，回调安全程序将会阻止入侵者使用。

RADIUS 采用用户数据报协议(UDP)，并只加密交换密码而不会加密整个会话，但可以使用附加协议来对数据会话进行加密。目前的 RADIUS 版本是在 RFC 2865 中定义的。

提示：

RADIUS 在网络访问服务器和共享认证服务器之间提供 AAA 服务。网络访问服务器是 RADIUS 认证服务器的客户端。

2. TACACS+

终端访问控制器访问控制系统(TACACS)作为 RADIUS 的一种替代系统被引入。思科后来推出了扩展 TACACS(XTACACS)，并将其作为一项专有协议。然而，TACACS 和 XTACACS 如今都不常用。后来，又推出了 TACACS +，并被作为一个开放的公开记录协议，成为三个协议中最常用的一个。

相比于早期版本和 RADIUS，TACACS+做了一些改进。它将认证、授权以及可问责性分为独立的流程，并可以在三台独立的服务器上进行托管。其他版本则是将其中的两个或三个流程合并为一个流程。此外，TACACS+可以加密所有的认证信息，而不仅仅像 RADIUS 一样只是加密密码。TACACS 和 XTACACS 使用的是 UDP 端口 49，而 TACACS+使用的是 TCP 端口 49，从而为数据包的传输提供了更高的可靠性。

3. Diameter

基于 RADIUS 和 TACACS+的成功应用，又开发出了一个名为 Diameter 的 RADIUS 的增强版本。它支持多种协议，包括传统 IP、移动 IP 和 IP 语音(VoIP)。因为支持许多附加的命令，所以尤其在支持漫游服务的情况下特别受欢迎，例如无线设备和智能手机。虽然 Diameter 是 RADIUS 的升级版本，但是其并不兼容 RADIUS。

Diameter 使用的是 TCP 端口 3868 或 SCTP 端口 3868，相比于 RADIUS 使用的 UDP 端口来说，提供了更高的可靠性。Diameter 也支持 IPSec 和 TLS 加密。

注意：

在几何中，圆的半径(RADIUS)是从中心到边缘的距离，直径(Diameter)是从边缘到边缘的两倍半径的距离。Diameter 这个名称也意味着 Diameter 要比 RADIUS 好两倍。这可能不完全准确，但相比于 RADIUS 来说，Diameter 改进了许多，并且强调了 Diameter 是后开发出来的，是一种改进后的协议。

13.4 管理标识和访问开通生命周期

身份信息和访问开通生命周期是指账户的创建、管理和删除。虽然这些行为看似很平凡，但对于系统的访问控制能力来说是非常重要的。如果没有正确定义和维护用户账户，系统就无法建立准确的身份信息，进行身份认证，提供授权或跟踪问责。正如前面提到的，当主体以某身份进入服务器时，就会进行身份认证。身份通常是用户账户，但也包括计算机账户和服务账户。

访问控制管理是指在账户的使用过程中所涉及的任务和职责的集合，包括管理账户、访问和跟踪问责。这些任务包含在身份信息和访问开通生命周期的三个主要职责中：开通、账户审核和账户撤消。

13.4.1 开通

身份管理的第一步是创建新账户并为其开通相应的权限。创建新的用户账户通常是一个简单的过程，但这一过程必须通过组织的安全策略程序来保护和保障。用户账户不是因管理员的一时兴起

或响应随机请求而创建的。相反，合理地开通账户可以确保人员在创建账户时遵循了特定的程序。

新用户账户的初始创建通常被称为注册或登记。注册过程创建了一个新的身份，并建立了系统需要进行身份认证的因素。全面准确地完成注册过程是至关重要的。个人身份通过组织认为的有必要的各种方式的认证也同样重要。在准许注册进入任何一个安全系统前，照片、ID、出生证明、背景检查、信用检查、安全检查认证、FBI 数据库搜索甚至通话记录都是认证身份的有效方式。

许多组织都有自动的账户开通系统。例如，一个人一旦被公司录用，HR 部门完成初步身份鉴定和处理步骤，然后会给 IT 部门发送创建账户的请求。IT 部门通过一个应用程序输入雇员信息，比如雇员的姓名和他们所属的部门，该应用程序会根据定义好的准则来创建账户。自动开通系统创建的账户都是一致的，例如，总是以同样的方式创建用户名并总是处理重复的用户名。如果准则规定了用户名应该包含姓和名，那么如果有一个全名叫 Suzie Jones 的雇员，应用程序就会为其创建一个名为 suziejones 的用户账户。如果该组织雇用了另一个有相同全名的雇员，第二个用户名可能就是 suziejones2。

如果组织使用的是群组(或角色)，应用程序可以根据用户的部门或工作职责自动将新的用户账户添加到相应的群组。群组中早已有合理的权限分配，所以这一步也规定了新用户的权限。

作为招聘过程的一部分，新员工要接受组织安全政策和程序方面的培训。在招聘完成之前，员工通常需要进行审查，并签署一项协议，承诺拥护组织的安全标准。协议中通常会包括合理的账户使用策略。

在用户账户的整个使用过程中，需要对其进行持续维护。有稳定的组织层级、较低的员工流动率和晋升率的企业相比于不稳定的组织层级、较高的员工流动率和晋升率的企业，对用户账户的管理显著较低。大多数的账户维护工作是处理权限的变更。应该建立类似于创建新用户账户的程序，来管理用户账户在使用过程中访问权限变更的问题。未经授权而增加或减少账户的访问能力，可能会造成严重的安全影响。

13.4.2　账号审核

应定期检查账户，以确保有正在运行的安全策略。检查内容包括确保不活跃的账户被禁用以及员工没有过多的特权。

许多管理员使用脚本来定期检查不活跃的账户。例如，脚本可以定位在过去 30 天没有登录的用户账户，并自动禁用它们。同样，脚本可以检查特权组(如管理员组)的成员账户，并删除未授权的账户。在审计程序中经常会有正式的账户评审。

过渡特权和特权蠕变

需重点防范访问控制方面的两个问题：特权过渡和特权蠕变。当用户拥有超过其工作任务所需的特权时，就发生了特权过渡。如果发现某用户账户拥有过渡特权，应立即撤回对其来说不必要的特权。特权蠕变是指用户账户随工作角色和工作任务的改变而逐渐积累特权。之所以会出现这种情况，是因为向用户增加了新的任务和新的特权，但对用户不再需要的特权未做消除。特权蠕变会导致特权过渡。

这两种情况都违反了最小化权限这一基本的安全原则。权限最小化原则是指仅授予用户完成工作任务和工作职能所需的权限。账户审核能有效地发现这些问题。

13.4.3 账号撤消

无论员工出于何种原因(包括员工休假)离开公司，及时禁用他们的用户账户十分重要。员工休假的情况也要包含在内。只要有可能，人事专员应有执行此项任务的能力，因为他们能及时意识到员工可能会因某种原因辞职。举例来说，人事专员了解哪些员工即将终止雇佣关系，他们在员工离职面谈时应禁用相关账户。

如果员工在离职面谈后仍拥有用户账户的访问权限，危害会很大。即使离职员工不会采取恶意行动，但如果其他员工发现密码，也可能会使用该账户。这时账户的使用日志会记录离职员工而不是真正操作者的行为。

在某些情况下，该账户还有其他功用，例如访问加密数据，此种情况下不应立即注销账户。如果确定账户不再使用，即可注销。一般情况下，账户禁用 30 天后会自动注销，但是这也依公司需求而定。

许多系统可以设置账户的终止期。这对临时员工和短期员工十分实用，也就是在终止期时自动禁用账户。例如，对于一位签订了 30 天用工合同的临时工来说，其账户会于 30 天后自动禁用。这样就可以在没有持续行政监督的情况下，也对账户起到相应控制的作用。

真实场景

未及时撤回账户访问权限的危害

房利美公司(通过以下实例)意识到在解雇员工后，未及时撤回账户访问权限的危害。2008 年 11 月 24 日下午 2 点左右，该公司解雇了一名 Unix 工程师。该员工在下午 4 点 45 分交回了工作证，但其行政访问权限却保留至当天晚上 10 点。

在被解雇后，该员工远程访问房利美公司的服务器，在合法脚本中插入了恶意代码，并设置其每天上午 9 点运行。这段恶意代码是一个逻辑炸弹，设置的运行时间是 2009 年 1 月 31 日，此设置一旦成功运行，将摧毁房利美公司多达 4000 台服务器的数据，并且许多专家认为，房利美公司要想恢复服务器功能，至少需要一周的时间。

万幸的是，在恶意代码插入一周后，该公司的另一名工程师发现了这一情况，因此没有造成任何损失。但是，如果人事专员在离职面谈时就禁用其账户，这样的事件就完全可以避免。

13.5 本章小结

CISSP CBK 的第 5 知识域的内容是身份与访问管理，包括允许和限制资产访问的操作、管理和执行等方面。资产包括信息、系统、设备、设施和人员等。访问控制将基于主体和客体间的关系对访问权限进行限制。主体是活跃实体(如用户)，客体是被动实体(如文件)。

访问控制主要分为三种类型：预防、检测和纠正。预防性访问控制是为了防患于未来。检测性访问控制是指在事故发生后进行检测，并尽力纠正问题，访问控制以行政管理性、逻辑性和物理性访问控制的方式实施。行政管理性访问控制也就是所说的管理控制，包括工作准则和工作规程。逻

辑性访问控制也叫技术性访问控制，通过技术方式实现。物理性访问控制通过使用物理方法保护主体。

访问控制的 4 个要素包括：识别、认证、授权和可问责性。主体(用户)需要一个身份(如用户名)，然后利用认证机制(如密码)证明这一身份。主体认证后，授权机制控制其访问权限，审计跟踪记录他们的行为，这样他们就必须为其行为负责。

身份认证的三种方法包括：你知道什么(如密码或 PIN)，你拥有什么(智能卡或令牌)以及你是什么(通过生物识别技术可以认证的某些生理或行为特征)。多因素认证即使用一种以上的认证方法，比单一认证方法更安全。

单点登录用户仅需认证一次就可以访问网络上的所有资源，不必再次认证。Kerberos(麻省理工学院开发的安全认证系统)是一种流行的单点登录认证协议，采用票据进行认证。 Kerberos 通过主体数据库、对称加密和时间同步系统发送票据。

联合身份管理可以使单点登录访问多个组织。多个公司建立或加入一个联盟，并且同意以某种方式在多公司之间共享身份。用户在自己组织内进行认证后，不需再次认证就可访问其他公司的资源。SAML 是互联网上用于单点登录访问的常见协议。

AAA 协议提供认证、授权和可问责性。广泛使用的 AAA 协议是 RADIUS、终端访问控制器访问控制系统(TACACS+)和 Diameter。

身份和访问开通生命周期包括为用户主体创建、管理和注销账户。服务开通的最初步骤包括创建账户并授权对客体适当的访问权限。当用户工作变化时，他们经常要求改变最初的访问权限。账户审核过程可以确保账户修改后的访问权限遵循最小化权限原则。当员工离开公司时，应及时禁用账户，不需要时应注销账户。

13.6　考试要点

了解主体和客体的区别　你可能发现 CISSP 考题和安全文档中通常使用术语主体和客体，所以知道它们之间的区别是很重要的。主体是活跃的实体(例如，用户)，他们可以访问被动客体(例如，文件)。用户是主体，在执行操作或完成一项工作任务时访问客体。

了解访问控制类型　对于本章提出的几种控制类型，你应该能够加以区分。访问控制包括预防措施(阻止有害的和未经授权的活动发生)、检测措施(发现有害的和未经授权的活动)和纠正措施(在有害的和未经授权的活动发生后，使系统恢复正常)。另外还有以下几种控制措施。制止措施通过鼓励人们避免有害行动而阻止人们违反安全准则。恢复措施是指在违反安全准则的行为发生后，试图修复和恢复资源、功能和能力。指引措施通过指导、限制或控制客体的行为来执行或鼓励对安全准则的遵守。补偿措施为目前的控制方法提供其他选择，帮助执行和支持安全准则。

了解访问控制的实施方法　访问控制以行政管理性访问控制、逻辑性访问控制和物理性访问控制的方式实施。行政(管理)性控制包括执行整个访问控制的准则或规程。逻辑/技术性控制包括用于管理资源和系统访问权限的硬件或软件，并对资源和系统提供保护。物理性控制包括部署物理屏障，物理屏障用于阻止与系统的直接接触，阻止访问系统或进入设备所在区域。

理解识别和认证的区别　访问控制依赖于有效的识别和认证，所以了解它们之间的区别十分重要。主体需要一个身份，身份对于使用者来说可能就是用户名。主体通过认证信息来证明身份(例如，匹配用户名和密码)。

理解授权和可问责性的区别 主体认证后，系统根据他们的身份来授权对客体的访问权限。审计日志和审计追踪记录的事件包括行为主体的身份。有效的识别、认证和审计构成可问责性。

理解三种认证方法的细节 身份认证的三种方法包括：你知道什么(例如，密码或 PIN)，你拥有什么(智能卡或令牌)以及你是什么(通过生物识别技术可以认证的某些生理或行为特征)。多因素认证即包括一种以上的认证方法，比单一认证方法更安全。密码是最弱的一种认证方式，但是可以通过增强复杂程度和密保问题来提高安全性。智能卡包括微处理器和加密证书，令牌可以提供一次性密码。生物识别法通过人体特征(例如指纹)来识别用户。交叉识别率验证了生物识别法的准确性。研究显示，第一类错误(错误拒绝率)和第二类错误(错误接受率)的发生概率相同。

理解单点登录 单点登录(SSO)是指主体一经授权允许即可访问多个客体，系统不必再次认证的一种机制。Kerberos 是最常见的运用于组织的一种单点登录方法，使用对称加密、采用票据认证身份并提供授权。当多个公司想要使用同一单点登录系统时，他们经常会使用联合身份管理系统。在该系统中，公司联盟或公司团体通常会达成统一的授权方法。SAML(安全断言标记语言)常用于共享联合身份信息。其他的单点登录方法是脚本访问，例如 SESAME 和 KryptoKnight。OAuth 协议和 OpenID 协议是目前应用于网络的两种较新的单点登录技术。在很多大型公司，例如谷歌，OAuth 2.0 远比 OAuth 1.0 更受欢迎。

理解 AAA 协议的目的 有多种协议提供了集中身份认证、授权以及可问责服务。网络访问(或远程访问)系统使用 AAA 协议。例如，一台网络访问服务器作为客户端使用 RADIUS 服务器，RADIUS 服务器就提供 AAA 协议。RADIUS 使用用户数据报协议(UDP)，仅需口令加密。终端访问控制器访问控制系统(TACACS+)使用传输控制协议(TCP)，以加密整个会话。Diameter 协议是为了提升 RADIUS 协议而出现的，但是 Diameter 协议与 RADIUS 协议不兼容。Diameter 协议被越来越广泛地应用于移动 IP 系统，例如智能手机。

理解身份及访问服务开通生命周期 身份及访问服务开通生命周期是指账户的创建、管理和注销。服务开通账户要确保拥有完成任务所需的适当权限。定期审核可以确保账户不会拥有过渡特权，并且遵循最小化权限原则。撤回包括当员工离开公司时应及时禁用账户，不需要时应注销账户。

13.7 书面实验室

1. 说出至少三种访问控制类型的名称。
2. 描述三个主要因素的身份认证类型。
3. 说出允许用户在多个组织一次登录，不用再次认证的访问资源的方法。
4. 识别身份和访问服务开通生命周期中的三个主要元素。

13.8 复习题

1. 以下哪一项不是组织想要用访问控制保护的资产？
   A. 信息
   B. 系统
   C. 设备

D. 设施

E. 以上都不是

2. 以下哪一项关于主体是正确的？

A. 主体总是用户账户。

B. 主体总是提供或承载信息或数据的实体。

C. 主体是始终接收有关客体或客体数据的实体。

D. 单一实体永远无法在主体和客体之间改变。

3. 哪种访问控制类型采用围栏、安全策略、安全意识培训和防病毒软件来防止出现不必要的或未经授权的活动？

A. 预防

B. 检测

C. 纠正

D. 指令

4. 哪个访问控制类型采用硬件或软件机制来管理对资源和系统的访问，并提供对这些资源和系统的保护？

A. 行政管理性访问控制

B. 逻辑/技术性访问控制

C. 物理性访问控制

D. 预防性访问控制

5. 下列哪一项最能表示控制资产访问时的主要目标？

A. 保持系统和数据的机密性，完整性和可用性。

B. 确保只有合法的对象可以在系统上进行认证。

C. 防止未经授权地访问对象。

D. 确保所有主体进行认证。

6. 用户用登录 ID 和密码登录。登录 ID 的目的是什么？

A. 认证

B. 授权

C. 问责

D. 识别

7. 可问责性不需要下列哪一项？

A. 识别

B. 认证

C. 审计

D. 授权

8. 可以用什么来防止用户使用两个口令进行轮转？

A. 密码复杂度

B. 密码历史记录

C. 密码年龄

D. 密码长度

9. 下列哪一项最能说明密码短语的好处?

A. 简短。

B. 很容易记住。

C. 包括一个单独的字符集。

D. 容易破解。

10. 下列哪一项是类型 2 认证因素的例子?

A. 你有什么

B. 你是什么

C. 你做什么

D. 你知道什么

11. 组织分发设备给员工。这些设备每 60 秒产生一次密码。组织内的托管服务器在任何给定的时间知道这个密码。这是什么类型的设备?

A. 同步令牌

B. 异步令牌

C. 智能卡

D. 通用访问卡

12. 下列哪一项基于主体的物理特征来认证?

A. 账户 ID

B. 生物识别技术

C. 令牌

D. PIN

13. 生物识别设备的交叉错误率(CER)说明了什么?

A. 表示灵敏度过高。

B. 表示灵敏度太低。

C. 说明错误拒绝率等于错误接受率的点。

D. 当足够高时,表明生物识别设备是高度精确的。

14. 一种生物识别系统已经错误拒绝了一个有效用户,指示该用户无法识别。这是什么类型的错误?

A. 类型 1 错误

B. 类型 2 错误

C. 交叉错误率

D. 相等错误率

15. Kerberos 的主要目的是什么?

A. 机密性

B. 完整性

C. 认证

D. 可问责

16. 以下哪一项是支持联合身份管理系统的最佳选择?

A. Kerberos

B. 超文本标记语言(HTML)

C. 可扩展标记语言(XML)

D. 安全断言标记语言(SAML)

17. 在 RADIUS 架构中，网络接入服务器的功能是什么？

A. 认证服务器

C. 客户端

C. AAA 服务器

D. 防火墙

18. 以下哪个 AAA 协议基于 RADIUS，并支持移动 IP 和 IP 语音电话？

A. 分布式访问控制

B. Diameter

C. TACACS+

D. TACACS

请参考下面的场景回答第 19 和第 20 题。

一名管理员在一个组织里工作了 10 多年。他已经在公司内部的不同部门之间换岗多次，并保留了任职期间在每一个工作岗位上的特权。最近，主管告诫他不要对系统进行未授权的更改。但是他又一次对系统做出了一个未授权的更改，这导致一个意想不到的中断，管理层决定终止他在公司的工作。第二天他回到办公室，清理办公桌和随身物品。在此期间，他安装了一个恶意脚本，并设置在接下来每月的第一天运行逻辑炸弹。该脚本将更改管理员密码、删除文件并关闭数据中心的 100 台服务器。

19. 下列哪条基本原则会被在职期间的管理员违反？

A. 隐式拒绝

B. 可用性损失

C. 防御性特权

D. 最小特权

20. 只要被雇佣，这个用户的账户会发现存在什么问题？

A. 策略需要强认证

B. 多因素认证

C. 记录

D. 账户审查

第 14 章

控制和监控访问

本章中覆盖的 CISSP 考试大纲包含：

身份与访问管理

- E. 实施和管理授权机制
  - E.1 基于角色的访问控制(RBAC)模型
  - E.2 基于规则的访问控制模型
  - E.3 强制访问控制(MAC)
  - E.4 自主访问控制(DAC)
- F. 保护和缓解对访问控制的攻击

第 13 章“管理身份与认证”提出了几个与 CISSP 认证考试通用知识体系(CBK)中的身份与访问管理域相关的重要主题。本章基于这些主题，并包括一些常见的访问控制模型的关键信息，还包括关于如何预防或缓解访问控制攻击的信息。一定要阅读和研究每一章的材料，以确保完全覆盖这一知识域的关键内容。

14.1 对比访问控制模型

第 13 章重点关注身份和认证。认证对象后，下一步就是授权。授权主体访问客体的方法根据不同 IT 系统所使用的访问控制方法的不同而不同。

提示：

主体是访问被动对象的活跃实体，客体是向活跃主体提供信息的被动实体。例如，当用户访问文件时，用户就是主体，文件就是客体。

访问控制技术有几个类别，CISSP CIB 中明确提到了 4 个：自主访问控制(DAC)、强制访问控制(MAC)、基于角色的访问控制(role-BAC)和基于规则的访问控制(rule-BAC)。以下部分介绍了这些模型所使用的一些基本原则，并对模型进行了更深入的描述。

14.1.1 对比许可、权限和特权

研究访问控制主题时，你会经常遇到许可、权限和特权这些术语。有些人交替使用这些术语，但它们的意思并不总是一样。

许可 一般情况下，许可是指授予对象的访问权以及对具体访问权内容的确定。如果对文件有读取许可，就能打开和阅读文件。可以授予用户权限来创建、读取、编辑或删除文件服务器上的一个文件。类似地，可以授予用户对文件的访问权限，所以在这种情况下，访问权和许可是同义的。例如，你可能被授予读取和执行应用程序文件的许可，这样你就有了运行应用程序的权限。此外，你可能被授予数据库内的数据权限，这使你能够在数据库中检索或更新信息。

权限 权限主要是指对一个对象采取行动的能力。例如，一个用户可能有权修改电脑上的系统时间或有权恢复备份数据。这是一个微妙的区别，并不强调。然而，你很少会看到将在系统上采取行动的许可称为权限。

特权 特权是许可和权限的结合。例如，电脑管理员会有完整的特权，允许管理员在电脑上有充分的许可和权限。管理员将能够在计算机上执行任何操作并访问任何数据。

14.1.2 理解授权机制

访问控制模型使用许多不同类型的授权机制或方法来控制谁可以访问特定的对象。下面简要介绍一些常见的机制和概念。

隐式拒绝 访问控制的基本原则是隐式拒绝，并且为大多数授权机制所使用。隐式拒绝原则确保了对一个对象的访问被拒绝，除非访问已被显式地授予一个主体。例如，想象管理员明确授予 Jeff Full 对一个文件的完全控制权限，但不显式地把权限授予其他任何人。Mary 没有任何访问权，即使管理员没有明确拒绝来自她的访问。相反，隐式拒绝原则拒绝给予 Mary 和除 Jeff Full 以外的任何其他人访问权。

访问控制矩阵 访问控制矩阵是一个包括主体、客体和分配权限的表格。当主体想要执行某个动作时，系统检查访问控制矩阵来确定主体是否有适当的权限来执行该动作。例如，一个访问控制矩阵可以包括一组文件作为客体，一组用户作为主体。它将显示每个用户为每个文件授予的确切权限。注意，内容远远超过单个访问控制列表(ACL)。在这个例子中，在矩阵中列出的每个文件都有单独的 ACL，列明了授权用户和他们被分配的权限。

功能表 功能表是确定分配给主体特权的另一种方式。它们不同于 ACL，因为功能表关注主体(如用户、组或角色)。例如，为会计角色创建的功能表将包括会计角色可以访问的所有客体列表，以及分配给会计角色对这些对象的特定权限。相比之下，ACL 专注于客体。ACL 是一些会列出被授权访问文件的所有用户和/或组及其具体授权内容的文件。

提示：

ACL 和功能表的区别是专注点。ACL 专注于客体，能识别对任何特定客体授予的主体访问权。功能表专注于主体，能识别主体可以访问的客体。

限制接口 应用程序使用限制接口来根据用户的特权限制用户可以做什么或看什么。拥有完整特权的用户对应用程序的所有功能都有访问权。拥有限制特权的用户访问权有限。应用程序使用不

同的方法限制接口。如果用户没有权限使用它，那么一种常见的方法是隐藏功能。例如，管理员可以通过菜单或右击某项来获得命令，但如果普通用户没有权限，命令就不会出现。其他时候，应用程序显示菜单项，但它们是暗的或禁用的。普通用户可以看到菜单项，但无法使用。

内容有关的控制　内容有关的控制基于客体中的内容来限制对数据的访问。数据库视图是基于内容的控制。视图从一个或多个表中检索特定列，创建一个虚拟表。例如，数据库中的客户表可能包括客户名称、电子邮件地址、电话号码和信用卡数据。基于客户的视图只会向用户展示客户名称和电子邮件地址，但没有别的信息。被授予访问视图权限的用户可以看到客户名称和电子邮件地址，但不能访问底层表中的数据。

上下文相关的控制　上下文相关的访问控制需要在授予用户访问权之前进行特定的活动。例如，考虑在网上销售数码产品的交易的数据流。用户将产品添加到购物车中，开始结账过程。结账流程的第一页显示购物车中的商品，下一个页面收集信用卡数据，最后一页确认购买并提供下载数码商品的指令。如果用户不先完成购买过程，系统会拒绝对下载页面的访问。也可以使用日期和时间控制作为上下文相关的控制。例如，可以基于当前日期和/或时间限制对计算机和应用程序的访问。如果用户试图在允许时间之外的时间访问资源，系统就会拒绝他们的访问。

知其所需　这条原则确保主体只在他们的工作任务和工作职能有要求时被授予访问权。主体可能有访问机密或限制数据的许可，但没有获得数据访问授权，除非他们真正需要来执行工作。

最小特权　最小特权原则确保主体只被授予他们执行工作任务和工作职能所需的特权。这一原则有时和“知其所需”原则混为一谈。唯一的区别在于，最小特权还将包括在系统上采取行动的权利。

职责分离　这一原则确保敏感功能被分成由两个或两个以上员工执行的任务，这有助于通过创建制衡系统来防止欺诈和错误。

14.1.3　用安全策略定义需求

安全策略是一个定义了组织安全需求的文档，它识别需要保护的资产，以及安全解决方案应该去保护它们的程度。一些组织将安全策略创建为一个单独的文件，其他组织创建多个安全策略，各自关注单独的区域。

策略是访问控制的一个重要元素，因为它们帮助组织内的人员了解什么安全需求是重要的。高层领导批准安全策略，并且在这一过程中对组织的安全需求进行广泛的概述。然而，安全策略通常不涉及有关如何满足安全需求或如何实现策略的细节。例如，它可能会说明实现和执行职责分离和最小特权原则的必要性，而不会说明如何这样做。组织内的专业人士使用的安全策略将作为实现安全需求的指导。

提示：

第 1 章“通过原则和策略的安全治理”中对安全策略有更深度的说明，包括有关标准、步骤和指导方针的详细信息。

14.1.4　部署深度防御

组织使用深度防护策略实现访问控制。这使用多层访问控制来提供多层安全。例如图 14.1，其中显示了用两台服务器和两个磁盘来表示组织要保护的资产。入侵者或攻击者需要攻克多层防御才

能到达这些受保护的资产。

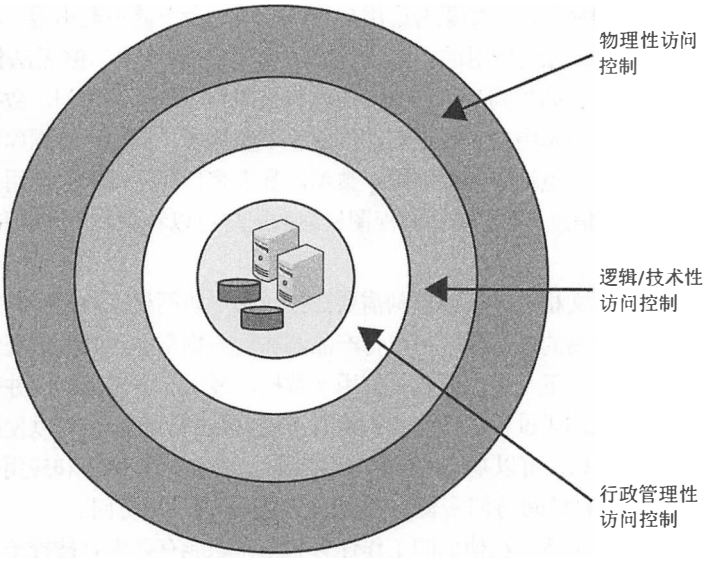


图 14.1　多层安全的深度防护

组织使用多种方法实施控制。不能仅依靠技术来提供安全；也必须使用物理性访问控制和行政管理性访问控制。例如，如果一台服务器有超强认证但被存储在一张无防备的办公桌上，一个小偷可以容易偷到，并不慌不忙地侵入系统。同样，用户可能有很强的密码，但是社会工程师可以忽悠无知的用户放弃密码。

深度防御的概念强调了几个重要的点：

- 组织的安全政策，这是管理访问控制之一，通过定义安全需求为资产提供了一层防御。
- 人员是防御的重要组成部分。然而，他们需要接受适当的培训和教育来实现、符合、支持组织安全策略中定义的安全元素。
- 行政管理性、技术性和物理访问控制的结合提供更为强大的防御。只使用行政管理性、技术性或物理访问控制之一会带来脆弱性，攻击者可以发现和利用这些脆弱性。

14.1.5　自主访问控制

使用自主访问控制(DAC)系统允许客体的所有者、创建者或数据保管者控制和定义主体对该客体的访问。所有客体都有拥有者，并且访问控制基于客体所有者的自由决定。例如，如果用户创建了一个新的电子表格文件，那么该用户就是这个文件的所有者。作为文件的所有者，用户可以更改文件的权限，从而准许或拒绝其他主体进行访问。基于身份的访问控制是 DAC 的一个子集，因为系统根据用户身份识别并分配资源所有权给身份。

常常使用针对客体的访问控制列表(ACL)来实现 DAC 模型。每个 ACL 都定义了对主体准许或限制的访问类型。因为客体的所有者可以改变针对客体的 ACL，所以自主访问控制并不提供集中控制的管理系统。访问对象很容易改变，特别是与强制访问控制的静态特性相比。

在 DAC 环境中，管理员可以轻松地挂起用户的权限(在他们离开时，例如度假)。同样的，很容易禁用账户(当用户离开组织时)。

提示：

在自主访问控制模型中，每个客体都有所有者(或数据保管员)，所有者完全控制他们的客体。ACL 中保存着权限(如文件的读取和修改)，所有者可以很容易地更改权限。这使得模型非常灵活。

14.1.6　非自主访问控制

可自由支配和不可任意支配的访问控制之间的主要区别在于如何对它们进行控制和管理。管理员会对不可任意支配的访问控制进行集中管理，并可以做出影响整个环境的改变。相比之下，自主访问控制模型允许所有者做出自己的更改，且他们所做的更改不会影响环境中的其他地区。

在非 DAC 模型中，访问不关注用户的身份。相反，支配整个环境的静态规则组管理访问。非 DAC 系统集中控制且易于管理(尽管不灵活)。一般来说，任何不是可自由支配的模型都是非可任意支配的模型，这包括基于规则、基于角色和基于格子的访问控制。

1. 基于角色的访问控制

采用基于角色或基于任务的访问控制系统基于主体的角色或分配的任务定义主体访问对象的能力。基于角色的访问控制(role-BAC)经常使用组来实现。

例如，一家银行有信贷员、出纳员、经理。管理员可以创建一个名为“信贷员”的组，将每个信贷员的用户账户加入这个组，然后为这个组指定适当的权限，如图 14.2 所示。如果组织雇用新的信贷员，管理员只需将新的信贷员添加到这个信贷员组，新员工会自动拥有和这个组中其他信贷员相同的权限。管理员将为出纳员和经理采取类似的措施。

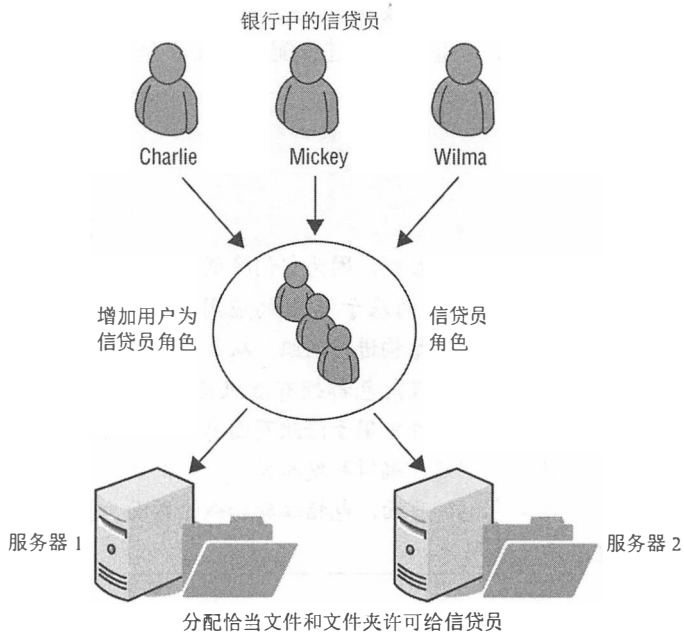


图 14.2　基于角色的访问控制

这有助于通过防止特权蠕变实施最小特权原则。特权蠕变是用户随着角色和访问需求的变化不断积累特权的趋势。理想情况下，当用户改变在组织内的工作时，管理员会撤消用户特权。然而，

当特权直接分配给用户时，识别和撤消所有不需要的用户特权就是极具挑战性的任务。

管理员可以轻松地取消不需要的权限，只需从一个组中删除用户的账户。一旦管理员从组中删除一个用户，该用户就不再享有分配给该组的特权。例如，如果一个信贷员转至另一个部门，管理员可以把该信贷员的账户从信贷员组中删除。这会将信贷员组的所有特权都从该用户账户中删除。

管理员通过工作描述或工作功能确定角色(组)。在许多情况下，组织会通过组织结构图记录层级结构。位于管理职位的用户相比担负临时工作的用户对资源的访问权更大。

基于角色的访问控制在有频繁人事变动的动态环境中是有用的，因为管理员只需将新用户添加到适当的角色就可以轻松地授予多个权限。值得注意的是，用户可以属于多个角色或组。例如，使用相同的银行场景，经理可能属于经理角色、信贷员角色以及出纳员角色。这使得经理可以访问银行员工能够访问的所有资源。

提示：

一个关于基于角色的访问控制模型的特色观点是：主体可以通过他们在角色中的资格对资源享有访问权。角色是基于工作或任务的，管理员会对角色分配特权。role-BAC 模型对于实施最小特权原则非常有用，因为特权可以通过从角色中移除用户账户而被很容易地撤消。

很容易混淆 DAC 和 role-BAC，因为它们都可以使用组来将用户组织到可管理单元中，但它们在部署和使用上不同。在 DAC 模型中，客体有所有者，所有者确定谁有权访问。在 role-BAC 模型中，管理员确定主体特权，并将特权分配给角色或组。在严格的 role-BAC 模型中，管理员不会把特权直接分配给用户，而只会通过将用户账户添加到角色或组中来授予特权。

另一种与 role-BAC 相关的方法是基于任务的访问控制(TBAC)。TBAC 与 role-BAC 相似，但不是每个用户被分配一个或多个角色，而是会被分配一系列的任务。这些都与为用户账户相关的个人分配的工作任务相关。在 TBAC 下，重点是通过分配任务而不是通过用户身份来控制访问。

真实场景

应用程序角色

许多应用程序都使用基于角色的访问控制，因为它们降低了维护应用程序的总劳动力成本。举一个简单的例子，WordPress 是一个流行的基于 Web 的应用程序，用于博客和内容管理系统。

WordPress 包括 5 个角色，按照层次结构进行组织。从最少特权到最多特权的用户为订阅者、投稿者、作者、编辑和管理员。每个高级角色都拥有低级角色的所有权限。

订阅者可以修改在他们的用户配置文件中用于修改页面感观的一些元素。投稿者可以创建、编辑和删除自己发表的帖子。作者可以创建、编辑和发布帖子。他们还可以编辑和删除自己发表的帖子，并上传文件，甚至还可以管理网站的页面，包括编辑和删除页面。管理员可以在网站上做任何事，包括管理潜在的主题、插件和用户。

2. 基于规则的访问控制

基于规则的访问控制(rule-BAC)使用一套规则、限制或过滤器来确定能以及不能出现在系统上的东西，包括给予主体访问客体的权限，或授予主体执行某个动作的能力。有关 rule -BAC 模型的一个独特特征是：它们有适用于所有主体的全局规则。

rule-BAC 模型的一个常见例子是防火墙。防火墙包括 ACL 中的一组规则或过滤器，由管理员定义。防火墙检查所有流经防火墙的流量，并只允许符合规则的流量通过。

防火墙包含一条最终规则(称为隐式拒绝规则)，会拒绝所有其他流量。例如，最终规则可能会通过否认所有来显示防火墙应该阻止网络内外的所有其他流量。换句话说，如果流量不符合以往任何显式定义规则的条件，那么最终规则就确保流量被阻塞。最终规则有时在 ACL 中是可视的，这样就可以看到它。其他时候，隐式拒绝规则作为隐含的最终规则，但并没有在 ACL 中明确说明。

注意：

我们在本书中使用了一些缩略词，如 DAC、MAC、rule -BAC、role-BAC。不过，CISSP 考试通常会在考题中拼出所有术语和缩略词。研究每个模型及其特征。然而，你不需要记住缩略词。

3. 基于属性的访问控制

传统的 rule-BAC 模型包括适用于所有用户的全局规则。然而，rule-BAC 的一个高级实现是基于属性的访问控制模型(ABAC)。ABAC 模型使用包括多个属性的规则的策略。许多软件定义的网络应用程序使用 ABAC 模型。

例如，CloudGenix 创建了一个软件定义的广域网(SD-WAN)解决方案，用于实现以允许或阻止流量的策略。管理员使用普通语句创建了 ABAC 策略，如“使用平板电脑或智能手机允许经理访问广域网”。这允许拥有经理角色的用户使用平板电脑或智能手机访问广域网。注意这是如何对 rule-BAC 模型进行改善的。rule-BAC 适用于所有用户，但 ABAC 可以更具体。

4. 强制访问控制

强制访问控制(MAC)模型依赖于分类标签的使用。每个分类标签代表一个安全域或安全领域。安全域是共享公共安全策略的主客体集合。例如，安全域可以有秘密标签，MAC 模型将以同样的方式用秘密标签保护所有对象。当主体有匹配的秘密标签时，它们只能访问带有秘密标签的客体。此外，主体获得秘密标签的要求对于所有主体来说都是一样的。

基于用户的许可等级，他们会有分配给他们的标签，这是一种特权。同样，客体由标签来标明它们的分类水平或敏感度。例如，美国军方使用绝密、秘密和机密标签对数据进行分类。管理员可以对具有绝密许可的用户授予访问绝密数据的权利。然而，管理员不能对低级许可的用户授予访问绝密数据的权利。

私营部门的组织经常使用的标签包括机密(或专用)、私人、敏感和公开。政府使用的标签由法律规定，而私营部门可以自由使用他们选择的任何标签。

MAC 模型通常被称为基于格子的模型。图 14.3 显示了一个基于格子的 MAC 模型示例。这让人想起花园中的格子，如用来帮助玫瑰攀爬的玫瑰格。标记为机密、私人、敏感和公开的水平线标记了分类水平的上界。例如，在公开和敏感之间的区域包括标记为敏感的客体(上限)。具有敏感标签的用户可以访问敏感数据。

MAC 模型还允许标签识别更多的安全域。在机密部分(私人和机密之间)，有 4 个独立的安全域，标记为 Lentil、Foil、Crimson 和 Matterhorn。这些都包括机密数据，但保存在单独的隔间，以便获得附加保护层。持有机密标签的用户还需要额外的标签来访问这些隔间的机密数据。例如，为访问 Lentil 数据，用户需要机密标签和 Lentil 标签。同样，带有 Domino、Primrose、Sleuth 和 Potluck 标签的隔间包括私人数据。用户需要私人标签和隔间标签才能访问相应隔间中的数据。

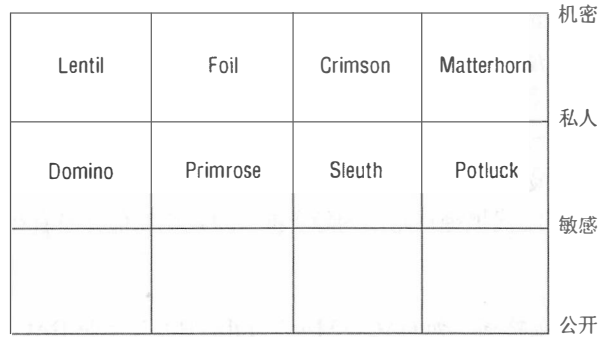


图 14.3 基于格子的访问控制所提供的边界表示

图 14.3 中的标签是二战军事行动的名字，但组织可以为标签设定任何名称。关键是这些部分为客体(如数据)提供了额外的隔间划分级别。注意，敏感数据(公开和敏感边界之间)没有任何额外标签。拿有敏感标签的用户可以访问带有敏感标签的任何数据。

组织内的人员识别标签，并定义它们的含义以及获取标签的要求。管理员然后将标签分配给主体和客体。标签到位后，系统基于分配的标签决定访问权。

在 MAC 模型中使用隔间划分使得“知其所需”原则变得必要。拥有机密标签的用户不会自动获得对机密部分隔间的访问权。然而，如果他们的工作要求他们访问特定的数据，如带有 Crimson 标签的数据，管理员可以给他们分配 Crimson 标签，使他们获得 Crimson 隔间的访问权。

强制访问控制是禁止的而非许可的，它使用隐式的拒绝哲学。如果用户没有获得对数据的具体访问授权，系统会拒绝他们访问相关联的数据。MAC模型比DAC模型更安全，但不够灵活、不可扩展。

提示：

MAC 和基于规则的访问控制之间的区别因素是：MAC 控制有标签，而基于规则的访问控制不使用标签。

安全分类表示敏感度层次。例如，如果认为军事安全标签有绝密、保密、机密和非机密，绝密标签就包括最敏感的数据，而非机密就是最不敏感的。因为有这个层次，具有最高机密数据许可的人就能够访问保密及敏感度更低的数据。然而，分类不需要包括较低水平。因此可以使用 MAC 标签，以便对高级标签的许可不包括对较低级标签的许可。

提示：

MAC模型的关键在于每个客体和主体都有标签。这些标签是预定义的，系统基于被分配的标签决定访问权。

MAC 模型中的分类使用以下三种类型的环境之一：

分层环境 分层环境将有序结构中的各个分类标签与低安全等级、中安全等级、高安全等级相互联系，如分别为机密、保密和绝密。结构中的每个级别或分类标签都相关。一个级别的许可授予主体访问这一级别以及更低级客体的权限，但禁止访问更高级别的所有客体。例如，有绝密许可的人可以访问绝密数据和保密数据。

隔间区分环境 在隔间区分环境中，一个安全域和另一个安全感之间没有关系。每个域代表一个单独的隔间。为了获取对某个客体的访问权，主体必须有对其安全域的具体许可。

混合环境 混合环境结合了分层和隔间区分的概念，以使每个等级水平可能包含更多细分等级，

与安全域的剩余部分相隔离。主体必须有正确的许可，以及在某个特定隔间的“需知”数据来获得对隔间区分客体的访问。混合 MAC 环境提供对访问的粒状控制，但随着增长变得越来越难以管理。图 14.3 就是混合环境的一个例子。

14.2　理解访问控制攻击方式

正如第 13 章所述，访问控制的一个目标是要阻止针对客体的未授权访问，包括访问任何系统信息(如网络、服务、通信连接、计算机和未授权访问数据等)。除了控制访问，IT 安全方法能够防止未授权的披露和变更，并提供一致的资源可用性。换句话说，IT 安全方法试图防止机密性破坏、完整性破坏和可用性破坏。

基于此，安全专家需要知道常见的攻击方法，以便他们能够采取积极的措施来加以阻止，以及在它们发生时进行识别，并适当地回应。以下部分对风险元素进行了快速回顾，并说明了一些常见的访问控制攻击。

虽然这部分侧重访问控制攻击，但重要的是意识到有许多其他类型的攻击，这在其他章节中有介绍。例如，第 6 章“密码学与对称加密算法”中包括各种密码分析攻击。

骇客、黑客和攻击者

骇客指的是那些心怀恶意之人，他们有意对个人或系统进行攻击。他们企图破坏系统的安全性并加以利用。他们的一贯动机是内心的贪婪、对权利的欲望以及博取他人的认可。他们的行为会导致他人财产的损失(如数据和知识产权)、系统瘫痪、安全受到威胁、受到负面的社会舆论、市场份额减少、利润率降低甚至丧失生产力。在很多情况下，骇客简直就是罪犯。

在 20 世纪 70 和 80 年代，黑客被认为是科技的热心家，并非心怀恶意。然而，现在媒体却用黑客这一术语来代替骇客。随着被人们广泛使用，黑客的定义也随之改变。

为了避免读者在本书中产生混淆，我们使用攻击者这一术语来表示心怀恶意的入侵者。任何企图利用系统的漏洞泄露机密、危害系统的完整性和/或可用性的行为，都可视为一次攻击。

14.2.1　风险元素

第 2 章“人员安全和风险管理概念”涉及风险以及风险管理的更深层面，但值得重申的是，一些术语只适合用在访问控制攻击的情境下。风险指的是某种潜在的威胁将利用某种漏洞造成某种损失(如对某项资产的损害)的可能性。威胁指的是某个事件发生的趋势，可能会产生某种不良的后果。这不仅包括罪犯或其他攻击者进行的潜在攻击行为，还包括自然灾害，如洪灾或地震等，以及员工的意外举动。漏洞指的是任何类型的脆弱性。这种脆弱性可能是因为硬件或软件的缺陷或限制，或是因为安全控制的缺失，如没有在电脑上安装杀毒软件。

风险管理指的是通过执行控制和应对措施试图减少或消除漏洞或减少潜在威胁的影响。消除风险是不可能的，或者说是不可取的。相反，组织应将重点放在减少那些对其有极大损害的风险上。需要注意的是，风险管理过程初期的重要步骤如下：

- 识别资产
- 识别威胁

- 识别漏洞

1. 识别资产

资产评估指的是确定各种资产的实际价值并对它们进行目标优选。风险管理就是将重点放在价值最高的资产上，并执行控制来减少风险对这些资产的影响。

资产的价值不仅仅是其购买价。例如，一台网络服务器一天能够产生一万美金的销售额，这个价格远高于仅仅购买硬件和软件的价格。假如这台服务器失效，将导致直接销售额的亏损，也将失去客户对商家的信任。

注意：

资产的实际价值受许多无形因素的影响，客户对商家的信任便是其中之一。

了解资产的价值也有助于成本效益分析，这样可以确定不同类型安全控制的成本效益。例如，如果资产价值成千上万美元，那么花费一百美元来购买有效的安全控制是合理的。相反，如果要花费几百美金去防止偷窃一个价值十美金的鼠标，就是一笔很不划算的支出。通常情况下，组织反而会愿意接受低价值资产的相关风险。

在发生访问控制攻击的情况下，评估数据的价值很重要。例如，如果攻击者要危害一台数据库服务器，下载内含隐私数据和信用卡信息的客户数据库，则意味着这家公司将损失惨重。具体损失并不总是那么容易估量的，不过对索尼公司的攻击事件可以提供部分视角(参见“索尼公司的数据泄漏事件”)。

专家估计，仅仅是索尼游戏机就造成 1.71 亿美金的直接损失。有极大的可能是，许多游戏玩家已经选择放弃索尼游戏机，并/或购买别的与之相匹敌的产品。那么，这些损失是不是可以防止呢？许多信息安全专家的回答是肯定的。因为这些攻击事件及其在 2011 年首次网络攻击事件发生数月前解雇大量信息安全专家，所以在 2011 年的黑帽会议中，索尼被提名为“前所未有的失败”。

这可能仅仅只是因为索尼之前没有识别其数据库中那些数据的价值。然而，在 2011 年的攻击事件之后，索尼有了可以计量的数据，运用这些数据可以估量损失的费用。有效的资产评估能够在这样的重大损失发生之前确定数据的价值。

真实场景

索尼公司的数据泄露事件

索尼公司在 2011 年遭受了多次数据泄露，然后在 2014 年再次遭遇。这些事件严重损害了索尼公司的形象。

发生于 2011 年 4 月的大量数据外泄导致攻击者窃取了索尼游戏站点 7700 万的客户账户数据。2011 年 5 月，袭击者盗用了 2450 万索尼在线娱乐账户。2011 年 6 月，对索尼影业的攻击盗取了 100 多万个用户账户，袭击者夸口说他们使用单 SQL 注入式攻击来检索数据(要获取更多有关注入式攻击的信息，可参阅第 21 章“恶意代码和应用程序攻击”)。2011 年 10 月，索尼锁了近 100 000 个游戏站点账户，并给用户发送邮件，表示攻击者窃取了用户的认证信息。索尼鼓励这些用户“选择独特、难猜的密码”，暗示事件因客户的错误导致。具有讽刺意味的是，索尼可能是正确的，因为许多用户在多个网络账户上使用的都是同一个密码。然而，最近接二连三的袭击发生后，用户对索尼的建议持怀疑态度。

攻击者在 2014 年 11 月和 12 月启动了另一个攻击，成功击溃整个网络达好几天。攻击者获得超过 100 TB 的数据，并发布了一些有害的信息(如关键内部邮件)。

2. 识别威胁

识别资产并确定优先级后，组织试图识别对有价值系统的任何可能威胁。威胁建模指的是识别、理解和分类潜在威胁的过程。目标之一是识别对这些系统的威胁潜在列表和分析威胁。

提示：

攻击者并不是唯一的威胁。威胁可以是自然事务，比如洪水或地震，也可能是偶然的，比如用户不小心删除一个文件。然而，考虑访问控制时，威胁主要是未经授权的个人(通常是攻击者)对资源的未经授权的访问。

威胁建模并不意味着是一个单独的事件。相反，组织在系统设计过程的早期开始威胁建模并在其整个生命周期中进行持续是很常见的。例如，微软利用其安全开发生命周期过程来考虑和实施产品开发每个阶段的安全。这支持了箴言“设计安全、默认安全、部署和沟通安全”(也称为 SD3 + C)。微软在这个过程中有两个主要目标：

- 减少安全相关的设计和编码缺陷的数量
- 减少剩余缺陷的严重程度

换句话说，试图减少漏洞，以及减少任何依然存在的漏洞的影响。总的结果是减少风险。

3. 威胁建模方法

因为存在几乎无限可能的威胁，所以重要的是要使用结构化的方法来识别相关的威胁。例如，一些组织使用以下一种或多种方法：

专注资产　这种方法使用资产估值结果，并试图识别对有价值资产的威胁。人员评估特定资产来确定他们对攻击的敏感性。如果资产托管数据，人员评估访问控制来识别可以绕过身份认证或授权机制的威胁。

专注攻击者　一些组织识别潜在的攻击者，并基于攻击者的目标识别他们代表的威胁。例如，政府可以识别潜在的攻击者，并识别攻击者想要做什么。他们可以使用这些知识来识别和保护相关资产。这种方法面临的一个挑战是，之前可能没有被认为是一种威胁的新的攻击者会出现。例如，索尼公司可能没有考虑 2014 年袭击之前来自他国政府的攻击。

专注软件　如果组织开发软件，那么可以考虑针对软件的潜在威胁。几年前，组织一般不开发自己的软件，而现在这很正常。具体地说，大多数组织都有网络，许多还创建自己的网站。花哨的网站虽能吸引更多的流量，但也需要更复杂的编程并且会受到额外的威胁。第 21 章讲的是应用程序攻击和 Web 应用程序安全性。

如果组织将攻击者确定为潜在的威胁(而不是自然威胁)，威胁建模尝试确定攻击者的目标。有些攻击者可能想禁用系统，而其他攻击者可能想要窃取数据，每个目标都代表一个单独的威胁。一旦组织识别了这些威胁，就会基于标的资产的优先级进行分类。

4. 高级持续性威胁

任何威胁模型都应该考虑已知威胁的存在，一种相对较新的威胁是高级持续性威胁(APT)。APT

指的是一起工作的一群攻击者，高度积极、熟练、有耐心。他们有先进的知识和各种技能，能够检测并利用漏洞。他们持之以恒，并专注于利用一个或多个特定目标而不是任何机会目标。各国政府通常会投资 APT。然而，一些有组织的犯罪团伙也会投资和经营 APT。

过去，要让你的网络安全，你只需要比其他网络安全。攻击者会攻击简单的目标，而避免安全网络。你可能还记得这句老话“被灰熊追赶时需要跑多快？”答案是：“只要比你那一组人中跑得最慢的人快一点就可以。”

然而，如果你拿着一罐蜂蜜，灰熊可能会忽视其他人，而只注意你。这就是 APT 要做的，通过想在目标那里获得的东西来对具体目标进行追击。这里有几个例子，安全专家将其归因于 APT：

美国国防部 2008 年，一名军事成员将受感染的 U 盘插入电脑，攻击便开始了。恶意软件传播到高度机密网络，在 14 个月的时间定期通过互联网发送数据包。Operation Buckshot Yankee 最后在 2009 年根除了此恶意软件。

法国政府 2011 年，一次成功的鱼叉式网络钓鱼攻击使得攻击者控制了法国商务部的 150 台电脑。攻击者针对法国商务部特定的电子邮件地址并骗取了源地址，标明邮件来自商务部的其他员工。这些邮件包含恶意附件。用户打开附件后，攻击者可以在用户系统上创建后门，并远程访问它们。攻击者在长达三个多月的时间里都从这些后门获取文件。

RSA 2011 年 3 月，攻击者使用社交工程电子邮件，利用 Adobe Flash 的零日漏洞。攻击者能够窃取与 RSA 的 SecurID 令牌设备相关的信息。然后使用这些信息来欺诈承包商，如 Lockheed Martin 公司和 L-3 通信公司等。

Stuxnet Stuxnet 是一个利用了多个零日漏洞的蠕虫病毒，它对伊朗核设施造成了大量破坏。一些报告随后表示，Stuxnet 是由美国和以色列联合操作的，名为 Operation Olympic Games。这是在 2010 年发现的。

有关 APT，要记住的一个重点是，它们可以针对任何公司而不只是政府。

5. 识别脆弱性

在识别有价值的资产和潜在威胁后，组织将执行漏洞分析。换句话说，试图发现这些系统在潜在威胁面前的弱点。在访问控制的情境下，漏洞分析试图识别不同访问控制机制的优缺点，以及利用了弱点的潜在威胁。

脆弱性分析是一个持续的过程，包括技术和管理措施。在较大的组织中，可能会有特定的人把脆弱性分析作为一项全职工作。他们定期进行漏洞扫描，寻找各种各样的漏洞并报告结果。在规模较小的组织中，网络管理员可以定期运行脆弱性扫描，如每周或每月一次。

风险分析通常会包括脆弱性分析，评价系统和环境的已知威胁和漏洞，然后就是利用漏洞的渗透测试。

14.2.2 常见的访问控制攻击

访问控制攻击试图绕过访问控制方法。第 13 章提到过，访问控制始于识别和授权，访问控制攻击往往试图窃取用户凭证。攻击者窃取了用户凭证后，就可以通过登录用户和访问用户的资源进行在线模拟攻击。其他情况下，访问控制可以绕过身份认证机制而只窃取数据，就像本章前面提到的索尼攻击一样。

本书涵盖了多种攻击，下面将介绍一些与访问控制直接相关的常见攻击。

1. 访问聚合攻击

访问聚合是指收集多个非敏感信息块，并将它们结合起来获得敏感信息。换句话说，一个人或一个组织可以收集有关系统的多个事实，然后使用这些事实发动袭击。

侦察攻击是访问聚合攻击，它结合多种工具来识别系统的多个元素，如 IP 地址、开放端口、运行服务、操作系统等。攻击者还对数据库进行聚合攻击。第 20 章“软件开发安全”涵盖了聚合攻击和推理攻击，间接允许使用聚合和推理技术实现对数据的未授权访问。

结合深度防御、“知其所需”和最小特权原则有助于防止聚合攻击。

2. 密码攻击

如第 1 章中所述，密码是最弱形式的认证。如果攻击者成功发动密码攻击，攻击者可以访问账户和授权给账户的所有资源。如果攻击者发现根或管理员密码，攻击者可以访问任何其他账户及其资源。如果攻击者在戒备森严的环境中发现特权账号的密码，环境的安全性就不能再被完全信任。攻击者可以创建其他账户或后门来访问系统。组织可能不会接受风险，而是选择重建整个系统。

强大的密码有助于防止密码攻击，这种密码包括至少 8 个字符，并至少有 4 个字符类型(大写字母、小写字母、数字和特殊字符)中的三个。随着密码破解者的本事越来越大，有些人认为强密码必须至少有 15 个字符，尽管普通用户很难相信。安全专家通常知道怎样让密码变得强大，而很多用户不知道，用户使用一种字符类型的短密码是很常见的。例如，攻击者发布了他们从前面提到的一次索尼攻击中盗取的账户信息。

微软在开发安全方面的最有价值专家 Troy Hunt 分析了这些密码(www.troyhunt.com/2011/06/brief-sony-password-analysis.html)。分析表明，用得最多的 10 个密码是 seinfeld、password、winner、123456、purple、sweeps、contest、princess、maggie 和 9452。攻击者可以使用一种常见的密码破解工具在不超过几秒钟的时间内发现这些密码。

注意：

大多数安全专家知道他们不应该使用简单的密码，如 123456 这种。然而，安全专家仍然有时会忘记，用户创建这些简单密码是因为他们没有意识到风险。许多终端用户从安全培训中受益。

以下部分使用字典攻击、暴力攻击、彩虹表攻击和嗅探方法描述了常见的密码。有些攻击对于网络账户来说是可能的。然而，更常见的是，攻击者窃取账户数据库后离线破解密码。

字典攻击

字典攻击通过使用预定义数据库或常见预定义密码列表中所有可能的密码来发现密码。换句话说，攻击者会从通常可以在字典中找到的单词数据库开始。字典攻击数据库还包括经常用作密码的字符组合，但可能不会在字典中找到。例如，可能会在许多密码破解字典中看到之前提到的在索尼账户数据库中找到的密码列表。

此外，字典攻击经常会扫描差别构建式密码。差别构建式密码是之前用过的密码，但仅有一个字符不同。例如，password1 是对 password 更改一个字符后的密码，其他的 Password、1password 和 passXword 也是。攻击者在生成彩虹表时经常使用这种方法(在本章后面讨论)。

提示：

有些人认为使用外国字词作为密码不容易遭受字典攻击。但是，密码破解字典会包括外国字词，而且通常也是这么做的。

暴力攻击

暴力攻击(又称蛮力攻击)试图通过系统尝试所有可能的字母、数字和符号组合来发现用户账户的密码。攻击者通常不会手动输入这些，而是借助程序，可以通过编程的方式尝试所有的组合。混合攻击一般是先进行字典攻击，然后用差别构建式密码执行一种暴力攻击。

密码越长、越复杂，暴力攻击耗时越长、造价越高。随着可能性的增加，执行一次详尽攻击的成本也在上升。换句话说，密码越长越多，包括的字符类型就越多，对暴力攻击就越安全。

密码和用户名存储在受保护系统的账户数据库文件中。然而，密码不是作为纯文本存储，系统和应用程序通常会散列密码，并只存储散列值。

当用户用散列密码进行身份认证时，会发生以下三个步骤：

(1) 用户输入凭据，如用户名和密码。

(2) 用户的系统散列密码并发送散列到身份认证系统。

(3) 身份认证系统将这个散列与存储在密码数据库文件中的散列进行比较。如果匹配的话，就表示用户输入了正确的密码。

这提供了两个重要的保护。密码不以明文在网络中传输，因为它们容易遭受嗅探攻击。密码数据库不以明文存储密码，因为攻击者更容易发现密码，如果他们访问到密码数据库的话。

然而，密码攻击工具会寻找创建了和存储在账户数据库文件中的条目相同的散列值的密码。如果成功了，就可以使用密码登录到账户。

例如，假设密码 IPassed 的存储散列值是 1A5C7G(尽管实际散列将会更长)。暴力密码工具将会猜到密码、计算散列，并将其与存储的散列值进行比较。这也被称为比较分析。当密码破解工具找到一个匹配的散列值时，就表明猜测的密码很可能就是原始密码。在这种情况下，该工具会破解出密码。

如果两个单独的密码创建了相同的散列，就会导致碰撞。碰撞是不理想的，在理想情况下碰撞是不可能发生的，但一些散列函数(如 MD5)不可能不遇到碰撞。这就使攻击者创建了一个和存储在账户数据库文件中的散列密码有相同散列的不同密码。

根据现代计算机的进行速度和采用分布式计算的能力，暴力攻击对一些强大的密码甚至都是成功的。实际发现密码的时间取决于用于散列它们的算法和计算机的性能。

许多攻击者在暴力攻击中使用图形处理单元(GPU)。一般来说，许多 GPU 比台式电脑中的大多数 CPU 有更强的处理能力。Blogger Vijay Devakumar 使用旧的基于 CPU 的解密工具 Cain & Abel 和新的基于 GPU 的工具 ighashgpu 来运行一些测试。报道称，Cain & Abel 用了 1 小时 30 分钟来追踪一个 6 字符密码，而 ighashgpu 破解相同的密码花了不到 4 秒时间。

提示：

攻击者有足够的时间可以使用离线的强力攻击发现任何密码。然而，更长的密码导致更长的时间，这使得攻击者破解它们不可行。例如，一个使用 4 种字符类型的 12 字符密码可能需要数千年的时间来破解。

生日攻击

生日攻击关注于寻找碰撞，其名称来自于一种称为生日悖论的统计现象。生日悖论认为，如果把 23 个人关在一个房间，那么任何两人同一天生日的可能性有 50%。这不是指的同一年，而是指同样的月份和日期，如 3 月 30 日。

闰年有 2 月 29 日，一年有 366 天。如果有 367 人在一个房间里，就会有 100%的机会获得至少两个有相同生日的人。将这个房间的人数减少到 23，仍然有 50%的机会让任何两人有相同的生日。

这类似于发现具有相同散列的任何两个密码。如果一个散列函数只能创造 366 个不同的散列，那么攻击者(他只有 23 个散列样本)有 50%的机会发现两个密码有相同的散列。散列算法可以创建超过 366 个不同的散列，但关键是，生日攻击方法不需要对所有可能的散列进行匹配。

从另一个角度来看，想象你一个人在房间里，你想寻找和你同一天出生的人。在本例中，你需要房间中有 253 人，才能达到找到有相同生日的人 50%的概率。即使需要房间里有更多的人，也不需要房间里有 366 人以找到匹配。

同样，一些工具有可能会提出另一个创建了与给定散列相同散列的密码。例如，如果知道管理员账户密码的散列是 1A5C7G，一些工具可以识别一个将会创建相同散列 1A5C7G 的密码。不一定是相同的密码，但如果可以创建相同的散列，就和原始密码一样有效。

可以通过使用带有足够位数的散列算法(使碰撞变得在计算上不可能)和用盐(在“彩虹表攻击”一节进行讨论)来降低生日攻击的成功性。曾经有一段时间，MD5(使用 128 位)被认为是不受碰撞影响的。然而，随着计算能力不断提高，MD5 并不是免碰撞的。SHA-3(安全散列算法版本 3 的简称)可以使用多达 512 位的密钥，并被认为能够防御生日攻击和碰撞，至少现在是这样。计算能力不断提高，所以在某种程度上，SHA-3 将被替换为另一个散列算法，它用更长的散列和/或更强的密码学方法创建散列。

彩虹表攻击

通过猜测、散列，然后与有效的密码散列进行比较来寻找密码需要很长时间。然而，彩虹表可以通过使用大型预先计算的散列数据库来减少时间。攻击者猜测密码(用字典攻击或暴力攻击)、对其进行散列，然后把猜到的密码和所猜到密码的散列放入彩虹表中。

密码破译器可以将彩虹表中的每个散列和被盗密码数据库文件的散列进行比较。传统的密码破解工具必须在对比散列之前猜测密码并对其进行散列。然而，当使用彩虹表时，密码破译器猜测和计算散列不会花费任何时间。只是在找到匹配之前对散列进行比较。这可以大大减少破解密码所花费的时间。

提示：

许多不同的彩虹表都是可以免费下载的。有着使用 4 种字符类型的 14 字符密码的散列的彩虹表大约是 7.5 GB 大小。尽管下载需要花一些时间，但攻击者愿意等待。然而，使用 15 个字符或更多字符的密码将击败大多数彩虹表攻击。

许多系统一般通过“撒盐”密码来减少彩虹表攻击的有效性。盐是一组随机位，在散列前加到密码中。加密方法在散列前就加入附加位，使攻击者更难以使用彩虹表破解密码。然而，考虑到足够的时间，仍然可以使用暴力破解“撒盐”密码。将盐与长的、复杂的密码结合确实会显著降低彩虹表的有效性。

嗅探攻击

嗅探捕获通过网络发送的数据包，以便对数据包进行分析。嗅探器(也称为数据包分析器或协议分析器)是一个软件，通过网络捕获流量。管理员使用嗅探器来分析网络流量和排除故障。

当然，攻击者也可以使用嗅探器。嗅探攻击(也称为窥探攻击或窃听攻击)在攻击者使用嗅探器

捕获通过网络传播的信息时发生。它们可以捕获和阅读任何在网络上以明文发送的数据，包括密码。

Wireshark 是一种广受欢迎的协议分析器，可以免费下载。图 14.4 展示了具有相对较小捕获量内容的 Wireshark，并演示了攻击者如何捕获和读取以明文在网络上发送的数据。

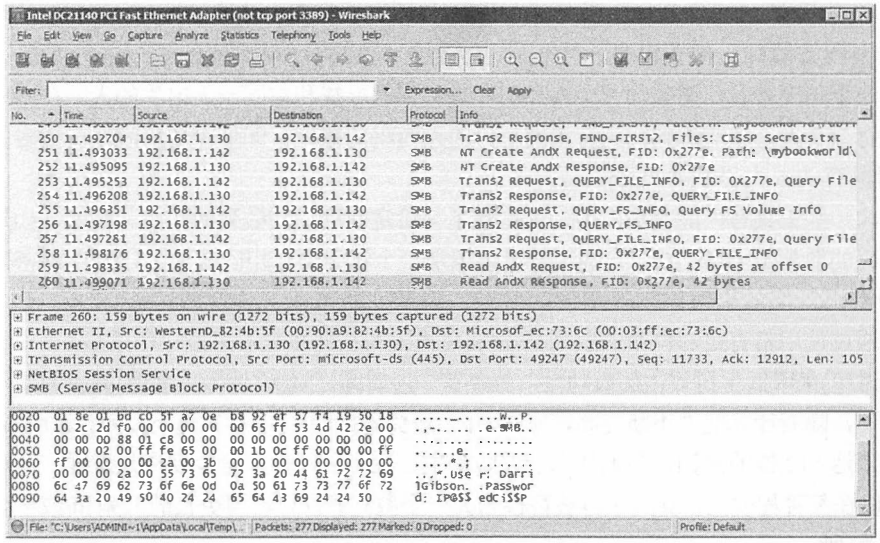


图 14.4 Wireshark 捕获

顶部窗格中显示了选择的包 260，可以在底部窗格中看到这个包的内容。里面包括文本 USer:DarrilGibson；PasswordIP@$$edCi$$P。如果在顶部窗格中看到第一个数据包(包号 250)，可以看到打开文件的名称是 CISSP Secrets.txt。

可有效预防嗅探工具的几项技术如下：

- 对通过网络发送的所有敏感数据(包括密码)进行加密。这样攻击者就不能通过嗅探器读取加密文件。例如，Kerberos 通过加密票据来防止攻击，攻击者不能通过嗅探器读取票据的内容。
- 当加密无效时，使用一次性密码。一次性密码可以成功阻止嗅探攻击，因为该密码只能使用一次。即使攻击者获取了一次性密码，也没有用。
- 使用物理安全保护网络设备。通过控制路由器和交换机的物理访问来阻止攻击者在这些设备上安装嗅探程序。
- 通过监控网络来阻止嗅探器。入侵检测系统能监控网络嗅探器，如若发现，便会发出警报。

3. 电子欺骗攻击

电子欺骗(伪装)是指假装成某物或某人等。电子欺骗的种类很多。例如，攻击者可以使用他人的凭证进入某建筑物或访问 IT 系统。一些应用程序能模拟合法的登录界面。攻击程序可以创建一个和操作系统极其类似的登录界面。当用户输入凭证时，虚假的应用程序就会获取用户的凭证，随后发起攻击。一些钓鱼攻击(稍后将在本章进行描述)可以使用虚假网站进行模拟。

在 IP 欺骗攻击中，攻击者使用虚假的 IP 地址代替合法的源 IP 地址来隐藏身份或模拟真实系统。在访问控制攻击中使用的其他钓鱼软件类型包括邮件欺骗和电话欺骗。

邮件欺骗 制作者通常伪装邮件地址，形成邮件来自其他来源的假象。钓鱼攻击经常通过此种方式欺骗用户，让他们认为邮件来自可靠的来源。但回件地址可能完全不同，只有当用户真正回复时，邮件程序才会显示地址。但是，此时用户却常常忽略这一问题。

电话欺骗　来电显示服务使得用户可以识别任何来电号码。电话欺骗可使来电者更改电话号码，这在网络电话(VoIP)系统中是一种常见技术。近来攻击者常用的一项技术是使用与被呼叫者同一地区的号码代替真正的呼叫号码，使之看起来像本地呼叫。

4. 社会工程学攻击

有时，直接询问是得到别人密码的最简单方式，这也是社会工程学常用的一种方法。社会工程学陷阱是指攻击者通过欺骗(包括虚假奉承、假装或行为默许)尝试获取他人信任的行为。攻击者试图诱骗人们透露不愿透露的信息或执行他们不会执行的行为。通常社会工程学的目的是获得进入 IT 基础设施或物理设施的权限。

例如，老练的社会工程学攻击人员可使未受过专业训练的咨询处工作人员相信，他们是高层管理相关人员，目前在外地出差忘记了密码。如果员工信以为真，就会重置密码并将新密码提供给攻击者。有时，社会工程学攻击人员诱骗普通用户暴露他们自己的密码，为攻击者提供账户访问权限。员工学习社会工程学常用诡计可有效减少此类攻击事件的发生。

社会工程学攻击通过电话、私人和邮件形式发生。不法分子通常冒充技术维修人员，例如，冒充电话维修技术员来获取物理访问。如果他们获得访问网络基础设施的权限，他们就可以安装嗅探器盗取敏感数据。在提供访问权限之前，核实访客身份可降低此类模拟攻击事件的发生。

有时，社会工程学只是试图偷瞄电子屏幕上的信息或观察用户敲击键盘。这就是所谓的肩窥。屏幕过滤器可以限制攻击者的视线。另外，密码隐藏(用其他字符(例如，星号)来代替实际密码字符)常用于防止肩窥发生。

5. 网络钓鱼

网络钓鱼是一种社交工程陷阱，它试图诱骗用户，使之掉以轻心，从而打开附件或链接。它通常试图伪装成合法公司来获取用户凭证或个人认证信息，比如用户名、密码或信用卡信息。攻击者随机发送垃圾钓鱼邮件，他们对收件人无从知晓，但希望得到用户回复。钓鱼邮件告知用户虚假信息，称用户如果不采取行动，公司将锁定其账户。例如，邮件可能显示公司发现其账户存在可疑活动，如果该用户不认证用户名和密码，将锁定其账户。

简单的钓鱼攻击告知用户出了问题，要求收件人使用用户名、密码和其他信息回复电子邮件。电子邮件的发件地址通常伪装成合法地址，但是用户回件地址由攻击者操控。复杂的钓鱼攻击包含貌似合法的虚假网站链接。例如，如果钓鱼邮件描述 PayPal 账户出了问题，虚假网站就会模拟 PayPal 网站。如果用户输入凭证，网站会盗取信息并将信息发送给攻击者。

有时，发送钓鱼邮件的目的是在用户系统上安装恶意软件。信息中可能包含被感染病毒的文件，例如附件，并且诱导用户将其打开。邮件可能包括一个网站链接，使得在用户不知情的情况下进行偷渡式下载。

注意：

偷渡式下载是指当用户浏览网站时，在用户不知情的情况下自动安装的一种恶意软件。偷渡式下载利用了浏览器或插件程序的漏洞。

一些恶意网站试图诱骗用户下载和安装软件。例如，近些年颇受攻击者追捧的勒索软件。攻击者通过恶意附件和偷渡式下载进行发送，鼓励用户下载并安装。密码储物柜(CryptoLocker)是其变种之一。一旦安装，就会对用户硬盘驱动中的所有数据进行加密。它会对用户造成威胁，如果不支付

赎金(例如，300 美元或更多)，攻击者将会删除加密密钥，用户数据将永远消失。即使警察在 2014 年破译了网络运行的源密码储物柜勒索软件，但是其变种不久就死灰复燃。

个人可通过以下简单规则来规避网络钓鱼等常见风险的发生：

- 对未知邮件或匿名邮件保持怀疑态度。
- 千万不要打开未知邮件的附件。
- 千万不要通过邮件分享敏感信息。
- 对邮件中的任何链接保持怀疑态度。

钓鱼攻击有几种不同的变体，包括鱼叉式钓鱼、捕鲸和语音钓鱼。

鱼叉式钓鱼

鱼叉式钓鱼是一种针对特定用户组的钓鱼方式，如某特定组织的员工。可能来自组织内的同事或合作者，也可能由外部来源引发。

例如，攻击者会利用 Adobe PDF 文件中的零日漏洞嵌入恶意代码。如果用户打开此文件，用户系统就会被安装恶意软件。攻击者命名 PDF 文件为 FY12…合同指南，并在电子邮件中叙述到这是在提供合同签约的最新信息。它们会向政府的知名承包商，如洛克希德 • 马丁公司的特定电邮地址发送电子邮件。如有任何承包商打开此类文件，就会在其系统上安装恶意软件，攻击者可以远程访问这些受感染的系统。

注意：

零日漏洞的存在是因为应用程序供应商还不知道或者还没有发布漏洞补丁。FY12…合同指南利用PDF文件中的漏洞进行攻击。尽管Adobe修补了这个漏洞，但攻击者还会发现新的应用程序漏洞。

捕鲸

捕鲸是钓鱼的一种形式，目标是高层人员或高管，比如公司的 CEO 和总裁。比较著名的一次捕鲸攻击了大约 20 000 个目标，多是企业资深高管的电子邮件，邮件标注了每个收件人的名字并声明他们要被法院传讯。它还包含了一个链接，可以获取关于传讯的更多信息。如果执行者单击链接，网站就会弹出一条消息，表示需要安装一个浏览器插件才能读取文件。

同意安装插件的高管实际上是安装了一款恶意软件，这款软件会记录他们的键盘输入以获取他们浏览不同网站的登录凭证。这款软件还能让攻击者远程访问高管的系统，允许攻击者安装其他的恶意软件，或读取系统上的所有数据。

语音钓鱼

攻击者除了主要通过电子邮件发起网络钓鱼攻击外，他们还会使用其他的手段欺骗用户，如即时通信(IM)和网络电话(VoIP)。

语音钓鱼也是钓鱼的一种变体形式，使用的是电话系统或 VoIP。常见的攻击方式是给用户打自动电话，向用户解释关于信用卡账户的相关问题，鼓动用户进行信息认证或确认，如信用卡号、有效期和卡背面的安全码。语音钓鱼攻击通常会把来电显示号码模拟成来自有效的银行或金融组织。

智能卡攻击

智能卡与密码相比，身份认证效果更好，特别是在把它们与另外一种认证因素结合使用时，比如个人识别号码(PIN)。然而，智能卡也易受攻击。旁路攻击是一种被动的、非侵入性的攻击，目的是观察设备操作。当攻击成功后，攻击者能够得到有价值的信息，包括信用卡信息，如加密密钥。

智能卡包含一个微处理器，但它没有内功率。相反，当用户将卡插入到读卡器中时，读卡器会向卡片进行供电。读卡器有一个电磁线圈，这个线圈能激发电子卡片。这为智能卡传输数据提供了足够的电力。

旁路攻击会分析发送给读卡器的信息。有时，它们可以使用电力监控攻击或微分功率分析攻击来测量芯片的功耗，以提取信息。在时序攻击中，它们可以监控处理时间，然后根据不同计算需要的时间获取信息。故障分析攻击试图引发错误，比如向卡片提供很少的电力以获取有价值的信息。

拒绝服务攻击

拒绝服务(DoS)攻击会阻止系统进行处理或阻止对合法流量或资源请求的响应。当系统失效后，所有对系统的合法访问都会出现阻塞、中断或迟缓。举一个简单的例子，如果一台服务器没有足够的物理安全保护，攻击者就可能拔掉它，将它从服务中删除。

DoS 攻击经常发生在网络上，包括互联网。一些 DoS 攻击允许攻击者在服务器上安装恶意代码。比如，攻击者可以通过下载安装驱动或代码，进而在 Web 服务器上显示恶意弹出窗口。这种恶意代码会在用户访问受感染网页时感染用户系统。

6. 防护方法汇总

以下列表总结了很多安全措施，可以防止访问控制方面的攻击。然而，值得注意的是，这个保护列表不够全面，无法对抗所有的攻击类型。你会发现本书中还有其他的额外控制可以帮助防止攻击。

对系统的物理访问控制。关于安全性的一句名言是，“如果攻击者无限制地对计算机进行物理访问，攻击者就会拥有它”。如果攻击者可以对身份认证服务器进行物理访问，他们就可以在很短时间内盗取密码文件。一旦攻击者盗取了密码文件，他们就可以在线下进行密码破解。如果攻击者成功下载密码文件，就可以认为所有的密码都存在危险。

对文件的电子访问控制。严格控制和监控对密码文件的电子访问。终端用户和非账户管理人员在日常工作中不需要访问密码数据库。安全专业人员应该对任何未经授权的密码数据库访问进行及时调查。

加密密码文件。对可用操作系统的密码文件进行强加密有助于保护它们免受未经授权的访问。散列法(如前所述)是一种常见的加密方法。此外，在进行密码散列之前，对密码加盐(salting)可以提供更强的保护。对包含密码数据库文件副本的所有介质进行严格控制也非常重要，如备份磁带或磁盘修复。最后，在传输过程中对敏感数据进行加密也是很重要的，包括通过网络发送密码。

创建强密码策略。通过编程的密码策略可以强制使用强密码，确保用户定期更改密码。攻击者在破解多种字符类型的长密码时需要用更长的时间。如果有足够的时间，攻击者可以通过离线暴力攻击找到所有的密码，所以要保持安全性，就需要定期更换密码。很多安全或敏感环境需要更强的密码，并且会要求用户频繁更改密码。许多组织对特权账户实行单独的密码策略，如管理员账户，以确保这些账户的密码更强且管理员与普通用户相比，会更加频繁地修改密码。

使用密码掩码。确保应用程序在任何屏幕上都没有以明文方式显示过密码，而且在显示密码时以替代性字符表示密码，如星号(*)。这能减少肩窥，但用户应该意识到，攻击者能够通过观察用户在键盘上的按键方式获得密码。

配置多因素身份认证。配置多因素身份认证，比如使用生物识别技术或令牌设备。当某组织使用多因素身份认证时，攻击者就算发现了密码，也无法访问网络。许多在线服务，比如谷歌，现在

提供的就是多因素身份认证，作为额外的保护措施。

使用账户锁定控制。账户锁定控制有利于防止在线密码攻击。在密码输入不正确超过预先设定的次数后，账户就会被锁定。账户锁定控制通常使用阀值水平(clipping levels)，虽然会忽略一些用户错误，但在达到某个阈值后就会采取行动。例如，通常会允许用户发生 5 次的错误输入，之后就会锁定账户。对于不支持账户锁定控制的系统和服务，比如大多数的 FTP 服务器，会在登录时附加入侵检测系统以保护服务器的安全。

提示：

账户锁定控制有助于防止攻击者猜测网上账户的密码。然而，这并不能阻止攻击者使用密码破解工具对偷来的数据库文件进行密码破解。

使用最后一次登录通知。许多系统会显示一条消息，包含最后一次成功登录的时间、日期和地点(如计算机名或 IP 地址)。如果用户关注此消息，则可能会注意到是否有其他人登录自己的账户。例如，如果用户是在上周五登录账户，但最后一次登录通知显示周六时有人访问该账户，则表明存在问题。怀疑别人登录自己账户的用户可以更改密码或向系统管理员报告这个问题。

对用户进行安全教育。获得恰当训练的用户对安全性和使用强密码有着更好的理解。警告用户他们不应该分享或写下自己的密码。管理员可能会对最敏感的账户，如管理员账户或根账户，设置又长又复杂的密码，并把这些密码存储在库或保险箱中。提示用户如何创建强密码，如密码短语，以及如何预防肩窥。让用户知道在所有网上账户(如银行账户和游戏账户)上使用相同密码的危险。当用户对所有这些账户使用相同的密码时，对游戏系统的成功攻击可以让攻击者访问用户的银行账户。用户也应该知道常见的社会工程学手段。

14.3 本章小结

本章涵盖了许多访问控制模型相关的概念。权限是指对客体的访问权，并决定着用户(主体)能够对客体做什么。权利主要是指对客体采取行动的能力。特权包括权利和权限。隐式拒绝确保对客体的访问被拒绝，除非访问权被明显地授予主体。

访问控制矩阵是一个关注客体的表，包括客体、主体以及分配给主体的特权。表中的每一行代表单个客体的 ACL。ACL 关注客体，并识别为任何特定客体而授予主体的访问权。功能表关注主体，并识别主体可以访问的客体。

限制接口基于用户的特权限制他们可以做什么或者可以看到什么。内容有关的控制基于客体的内容限制访问。情境有关的控制在授予用户访问权之前需要进行特定的活动。

最小特权原则确保主体只被授予执行工作任务和工作职能所需的特权。职责分离有助于防止欺诈，因为它确保敏感功能会分别由两名或两名以上的员工负责。

书面安全策略定义了组织的安全需求、安全控制的实施和执行安全策略。深度防御策略实现了多级安全控制以对资产进行保护。

在有自主访问控制时，所有客体都有一个所有者，所有者对客体具有完全控制权。管理员集中管理不可任意支配的控制。基于角色的访问控制使用通常与组织层级结构相匹配的角色和组。管理员为用户设定角色，并基于工作或任务为角色分配权限。基于规则的访问控制使用适用于所有主体的全局规则。强制访问控制要求所有客体都有标签，访问基于主体是否有相匹配的标签。

重要的是要理解评估访问控制攻击潜在损失时的基本风险元素。风险是威胁利用漏洞带来损失的可能性。资产估值确定资产的价值，威胁建模识别潜在威胁，脆弱性分析识别漏洞。这些都是在实施控制以防止访问控制攻击时需要理解的重要概念。

常见的访问控制攻击试图绕过身份认证机制。访问聚合是收集和聚合非敏感信息以便推断出敏感信息的行为。

密码是一种常见的身份认证机制，存在几个不同的攻击类型试图破解密码。密码攻击包括字典攻击、暴力攻击、生日攻击、彩虹表攻击和嗅探攻击。套路攻击是针对智能卡的被动攻击。

社会工程学技术经常在为了得到密码和其他数据时使用。网络钓鱼使用电子邮件试图让用户放弃有价值的信息(比如凭证)、单击链接或打开恶意附件。鱼叉式网络钓鱼针对的是一群人，比如在某个组织工作的人。捕鲸针对的是高层管理人员。

14.4　考试要点

识别常见授权机制。考虑到分配给已认证身份的权限，授权确保请求的活动或客体访问是可能的。例如，可以确保具有适当权限的用户可以访问文件和其他资源。常见的授权机制包括隐式拒绝、访问控制列表、访问控制矩阵、功能表、限制接口、内容有关的控制和情境有关的控制。这些机制应实施安全原则，如“知其所需”、“最小特权原则”和“职责分离”。

了解每个访问控制模型的细节。在自主访问控制模型中，所有客体都有所有者，所有者可以修改权限。管理员集中管理不可任意支配的控制。基于角色的访问控制模型使用基于任务的角色，当管理员为账户分配角色后，用户获得特权。基于规则的访问控制模型使用一套规则、限制或过滤器来确定访问。强制访问控制使用标签来识别安全域。主体需要匹配标签来访问客体。

理解基本的风险元素。风险是威胁利用漏洞、破坏资产的可能性。资产估值确定资产的价值，威胁建模识别对这些资产的威胁，脆弱性分析识别组织有价值资产的弱点。访问聚合是一种结合、聚合非敏感信息以获取敏感信息的攻击，用于侦察攻击。

理解暴力攻击和字典攻击的运行方式。暴力攻击和字典攻击针对的是被盗密码数据库文件或系统的登录提示。设计它们是为了发现密码。暴力攻击使用的是键盘字符所有可能的组合，而字典攻击中使用的是可能密码的预定义列表。账户锁定控制能阻止它们对网络攻击的有效性。

理解强密码的必要性。强密码会使密码破解工具失效。强密码包括多个字符类型，而不是字典中的单词。密码策略确保用户创建强密码。密码在存储时应被加密，通过网络发送时也应进行加密。身份认证可以通过使用密码以外的额外因素进行增强。

理解嗅探攻击。在嗅探攻击(或窃听攻击)中，攻击者使用数据包捕获工具(如嗅探器或协议分析器)来获取、分析和读取通过网络发送的数据。攻击者可以很容易地读取在网络上以明文发送的数据，但是在传输中加密数据就可以防止这种类型的攻击。

理解电子欺骗攻击。电子欺骗指的是假装成别的东西或其他人，被用在许多类型的攻击中，包括访问控制攻击。攻击者通常试图获得用户的凭据，以便可以诱骗用户的身份。欺骗攻击包括邮件欺骗、电话欺骗、IP 欺骗。许多钓鱼攻击都使用欺骗的方法。

理解社会工程学。社会工程学攻击是指攻击者试图说服某人提供信息(如密码)或执行他们通常不会执行的动作(如单击恶意链接)，从而导致安全性损害。社会工程师经常试图获得对 IT 基础设施或物理设施的访问权限。用户教育是一种用来阻止社会工程学攻击的有效工具。

理解网络钓鱼。网络钓鱼攻击常用来诱使用户放弃个人信息(如用户账户和密码)、单击恶意链接或打开恶意附件。鱼叉式网络钓鱼的目标针对特定的用户群，捕鲸针对高层管理人员。电话钓鱼使用 VoIP 技术。

14.5 书面实验室

1. 描述自主和非自主访问控制模型之间的主要区别。
2. 列出在识别和阻止访问控制攻击时可利用的三个识别要素。
3. 说出三种用于发现密码的攻击类型。

14.6 复习题

1. 以下哪一项最能描述隐式拒绝原则?
   A. 未明确否认的所有动作都被允许。
   B. 未明确允许的所有操作都被拒绝。
   C. 所有行动必须明确否认。
   D. 以上都不是。
2. 最小特权的目的是什么?
   A. 由用户运行系统进程需要的最严格的权利。
   B. 由用户运行系统进程需要的最少限制的权利。
   C. 由用户完成指定任务所需的最严格的权利。
   D. 由用户完成指定任务所需的最少限制的权利。
3. 一个表包括多个客体和主体，并确定了每个主体具体访问时都有不同的客体。这个表被称为什么?
   A. 访问控制列表
   B. 访问控制矩阵
   C. 联合
   D. 蠕变特权
4. 谁或什么根据自主访问控制模型授予权限给用户?
   A. 管理员
   B. 访问控制列表
   C. 分配标签
   D. 数据监管者
5. 以下哪个模型也被称为基于身份的访问控制模型?
   A. 自主访问控制
   B. 基于角色的访问控制
   C. 基于规则的访问控制
   D. 强制访问控制

6. 集中式授权确定哪些文件用户可以访问。以下哪一项最能说明这一点？
   A. 访问控制列表(ACL)
   B. 访问控制矩阵
   C. 自主访问控制模型
   D. 非自主访问控制模型
7. 集中式授权确定用户可以根据组织层级结构来访问哪些文件。以下哪一项最能说明这一点？
   A. 自主访问控制模型
   B. 访问控制列表(ACL)
   C. 基于规则的访问控制模型
   D. 基于角色的访问控制模型
8. 以下哪一项涉及基于角色的访问控制模型？
   A. 基于角色的访问控制模型允许多个组中的用户成员资格
   B. 基于角色的访问控制模型允许单个组中的用户成员资格
   C. 基于角色的访问控制模型是非分层的
   D. 基于角色的访问控制模型使用标签
9. 以下哪一项对于在组织内部使用基于角色的访问控制模型是最佳选择？
   A. Web 服务
   B. 应用程序
   C. 数据库
   D. 开发人员
10. 以下哪一项最能说明基于规则的访问控制模型？
   A. 采用本地规则应用于单个用户
   B. 采用全局规则应用于单个用户
   C. 采用本地规则平等地应用于所有用户
   D. 采用全局规则平等地应用于所有用户
11. 什么类型的访问控制模型被用于防火墙？
   A. 强制访问控制模型
   B. 自主访问控制模型
   C. 基于规则的访问控制模型
   D. 基于角色的访问控制模型
12. 什么类型的访问控制依赖于使用标签？
   A. 自主访问控制模型
   B. 非自主访问控制模型
   C. 强制访问控制模型
   D. 基于角色的访问控制模型
13. 以下哪一项最能说明强制访问控制模型的特点？
   A. 采用显式拒绝理念
   B. 宽松的
   C. 基于规则
   D. 静止

14. 以下哪一项不是有效的访问控制模型？

A. 自主访问控制模型

B. 非自主访问控制模型

C. 强制访问控制模型

D. 基于 Lettuce 的访问控制模型

15. 组织会做什么来识别弱点？

A. 资产评估

B. 威胁模型

C. 脆弱性分析

D. 访问审查

16. 以下哪一项可以帮助缓解网上蛮力攻击的成功率？

A. 彩虹表

B. 账号锁定

C. 撒盐密码

D. 密码加密

17. 试图检测智能卡中的缺陷是什么攻击？

A. Whaling

B. 旁路攻击

C. 暴力攻击

D. 彩虹表攻击

18. 什么类型的攻击使用电子邮件，试图诱骗高层管理人员？

A. 网络钓鱼

B. 鱼叉式钓鱼

C. 捕鲸

D. 语音钓鱼

在回答问题 19 和 20 时，参考以下情境：

一个组织最近遭受了一系列安全漏洞，声誉大大受损。多次成功袭击后，可以通过公司的一台 Web 服务器获得被盗用的客户数据库文件。此外，一名员工能从先前的工作权限分配中获得对机密数据的访问。这名员工对数据进行复制，并卖给竞争对手。该组织已聘请安全顾问，帮助他们减少未来攻击的可能风险。

19. 顾问会用什么来识别潜在的攻击者？

A. 资产评估

B. 威胁模型

C. 脆弱性分析

D. 访问审查和审计

20. 为确保顾问具有正确的关注点，需要完成什么？

A. 资产评估

B. 威胁模型

C. 脆弱性分析

D. 审计跟踪的建立

第 15 章

安全评估和测试

本章中覆盖的 CISSP 考试大纲包含：

6. 安全评估和测试(设计、执行和分析安全测试)
- A. 设计与验证评估和测试策略
- B. 进行安全控制测试
  - B.1 漏洞评估
  - B.2 渗透测试
  - B.3 日志审核
  - B.4 综合事务
  - B.5 代码审核和测试(如手动测试、动态测试、静态测试、模糊测试)
  - B.6 误用情况测试
  - B.7 测试覆盖分析
  - B.8 接口测试(如 API 测试、UI 测试、物理测试)
- C. 收集安全处理数据(如管理和操作控制)
  - C.1 账户管理
  - C.2 管理审核
  - C.3 关键性能和风险指标
  - C.4 备份验证数据
- D. 分析和报告测试输出(如自动、手动)
- E. 实施或促进内部审计和第三方审计

在这本书中，你已经了解了很多信息安全专家用来确保信息机密性、完整性和数据可用性的不同控制。其中，技术性控制在保护服务器、网络和其他信息处理资源方面发挥着重要的作用。一旦安全专家创建并配置了这些控制，就必须定期地测试这些控制以便确保持久地保障信息安全。

安全评估和测试程序要进行定期检查，以确保安全控制数量足够、部署到位并且能够有效地执行它们的指定功能。在本章，你将学习世界各地的安全专家们所使用的各种评估和测试控制方法。

15.1 创建安全评估和测试程序

信息安全团队维护活动的基石就是他们的安全评估和测试程序。这个程序包括测试、评估和审计，它们用来定期核实机构有充足的安全控制以及这些安全控制可以正常运作以便有效地保护信息资产。

在本节，你将学习安全评估程序的三大主要构成：

- 安全测试
- 安全评估
- 安全审计

15.1.1 安全测试

安全测试能够验证控制运行正常。这些测试包括自动扫描、工具辅助渗透测试和手动测试。安全测试应该定期进行，需要关注保护组织的每个关键安全控制。安排对安全控制进行审查时，信息安全管理人员应考虑以下因素：

- 安全测试资源的可用性
- 由被测控制保护的系统和应用程序的危急程度
- 被测系统和应用所包含信息的敏感度
- 实现控制机制出现技术故障的可能性
- 会危及安全的错误配置的可能性
- 系统遭受攻击的风险
- 控制配置的变化率
- 可能影响控制性能的技术环境中的其他变化
- 执行控制测试的难度和所需时间
- 测试对正常业务运行的影响

完成对这些因素的评估后，安全团队可设计和验证一个综合的评估测试策略。这一策略可包括频发的自动测试并辅以较少的手工测试。例如，信用卡处理系统可在夜间进行自动漏洞扫描，并且在扫描检测到新漏洞时立即提醒管理员。一旦配置了自动扫描，就不再需要管理员做此工作，所以频发运行就相对容易很多。安全团队可能希望以手动渗透测试作为自动扫描的补充，手动渗透测试需要雇佣外部顾问来进行。这些测试最好在每年年检的基础上进行，如此可降低成本、减少业务中断。

警告：

许多安全测试程序开始时比较随意，安全专家只是用新奇的工具测试他们首先遇到的系统，而不管这个系统是什么。实验新工具固然很好，但安全测试程序应该精心设计，这个设计要使用风险优先法来包含严格的和常规的检测系统。

当然，只进行安全测试是不足够的。安全专家也必须仔细审核这些测试的结果，确保每个测试是成功的。某些情况下，这些审核要包括手动阅读测试的输出结果并验证测试已成功完成。还有些测试需要人工解释，这些解释必须由训练有素的分析师进行。

其他审核可以由安全测试工具自动执行，该工具能够验证测试的成功完成、记录结果并保持沉默直到有重大发现。当系统检测到需要引起管理员注意的问题时，会触发警报、发送电子邮件或短信，甚至根据预警的严重性和管理员的偏好自动打开故障单。

15.1.2　安全评估

安全评估是对系统、应用程序或其他测试环境的综合评价。在进行安全评估的过程中，受过培训的信息安全专家会执行风险评估以识别受测环境的漏洞，由此可根据需要做出折中处理和提出修复建议。

安全评估通常包括使用安全测试工具，但不只是自动扫描和手动渗透测试，还包括彻底审核威胁环境、当前和未来面临的风险以及目标环境的价值。

安全评估工具的主要产物通常是一份用于管理的评估报告，这份报告以非技术性的语言描述了评估结果，并且以具体建议作为结论，从而提高被测环境的安全性。

15.1.3　安全审计

安全审计会使用与安全评估期间相同的许多技术，但必须由独立的审计员执行。虽然组织的安全人员可能经常进行安全测试和评估，但并不适用于审计。评估和测试结果仅供内部使用，旨在评估控制以求发现需要改进之处。从另一方面来说，审计就是评估，目的是向第三方展示控制的有效性。为组织设计、实施和监测控制的员工在评估这些控制的有效性时存在固有的利益冲突。

审计员对安全控制的状态做出的评判应公正、无偏见。他们编写的报告与安全评估报告非常类似，但这些报告的阅读对象不同，可能是公司的董事会、政府的监管人员和其他第三方。审计的类型主要有两种：内部审计和外部审计。

政府审计员发现空中交通管制的安全漏洞

美国联邦、州和地方政府也使用内部和外部审计员执行安全评估。美国政府审计总署(GAO)受国会要求执行审计，而 GAO 审计通常关注的是信息安全风险。2015 年，GAO 发布了一份审计报告，题为“信息安全：美国联邦航空管理局(FAA)需要解决空中交通管制系统的安全漏洞。”

这份报告的结论不太乐观：“尽管美国联邦航空管理局(FAA)已经采取措施保护其空中交通管制系统不受基于网络的威胁及其他威胁，但其仍然存在重大的安全控制弱点，影响了该机构保证国家空管系统(NAS)可以不间断安全运行的确定性。这些控制弱点体现在对计算机资源未经授权访问的防止、限制和检测上。例如，关于保护系统边界的控制、识别和验证用户、授权用户访问系统、加密敏感数据以及对 FAA 系统的审计和监测活动。”

接着这份报告提出 17 个建议，建议 FAA 如何提高其信息安全控制以便更好地保护国家空中交通管制系统的完整性和可用性。GAO 报告全文可从下面的链接找到：http://gao.gov/assets/670/668169.pdf。

内部审计由组织的内部审计人员执行且通常也是为了内部使用。执行这些审计的内部审计人员通常有一套报告流程，这套流程完全与他们评估的功能一致。在许多组织中，首席审计执行官向总裁、首席执行官或类似角色的人员进行直接汇报。首席审计执行官也可直接向组组的董事会进行汇报。

外部审计由外部审计公司执行。这些审计的外部效度(degree of external validity)很高，因为理论上执行评估的审计员与机构本身没有利益冲突。可以进行外部审计的公司有很多，但人们最信赖的当属“4 大”审计公司：

- 安永
- 德勤
- 普华永道
- 毕马威

由这 4 大公司执行的审计通常受多数投资者和机构成员接受和认可。

信息安全专家往往被要求参与内部和外部审计。他们通常必须提供相关的安全控制信息给审计人员，这里可采用面谈和书面文档的形式。审计员也可要求主管安全的工作人员参与控制评估的过程中。通常情况下，审计员有得知组织所有信息的权利，而且主管安全的工作人员应当依从这些请求，如有需要应作为管理层顾问。

当审计出现错误时

4 大审计公司直到 2002 年才最终形成。在这之前，其实是 5 大审计公司，还包括备受人们推崇的安达信会计师事务所。然而，始料未及的安然事件让安达信再也无法立足。安然是一家能源公司，在其系统化的财务造假行为受到指控而引发监管机构和媒体的广泛关注后，安然于 2001 年突然申请破产。

安达信是当时世界最大的审计公司之一，曾执行对安然公司的财务审计，并签字认为安然的欺诈行为具有合法有效性。后来，该公司被指控妨碍司法公正，虽然最高法院随后宣告其罪名不成立，但由于该公司在安然丑闻和其他欺诈行为的指控中信誉严重受损，因此很快就倒闭了。

15.2 执行漏洞评估

漏洞评估是信息安全专家工具箱中的一个重要测试工具。漏洞扫描和渗透测试为安全专家提供的视角是系统或应用在技术控制方面的弱点。

注意：

从术语角度更清晰的解释是，本章描述的漏洞评估其实就是安全测试工具而非安全评估工具。为保持语言的一致性，它们应该被称为漏洞测试，但我们继续沿用(ISC)^{2}在官方 CISSP 知识体中的描述。

15.2.1 漏洞扫描

漏洞扫描会自动对系统、应用程序和网络进行探测，寻找可能会被攻击者利用的弱点。用于这些测试的扫描工具能提供快速、仅通过点击操作的测试，并执行这些单调乏味的任务，而无须手动干预。大多数工具允许以循环为基础的预定扫描，并且能够提供报告，显示不同时间各项扫描之间的差异，向管理员提供安全风险环境的变化情况。

漏洞扫描的类型主要有三种：网络发现扫描、网络漏洞扫描和 Web 应用程序漏洞扫描。每种类型的扫描都由多个工具执行。

警告：

记住，信息安全专家并不是唯一有漏洞测试工具的人。攻击者通过使用“好人”同样的工具，在尝试入侵前对系统、应用程序和网络运行漏洞进行测试。这些扫描能够帮助攻击者瞄准漏洞系统，重点攻击他们最可能得手的系统。

1. 网络发现扫描

网络发现扫描使用多种技术对一系列 IP 地址进行扫描，搜索配有开放网络端口的系统。网络发现扫描器实际上不能探测系统的漏洞，只是提供一份网络检测的系统显示报告和一份端口清单，这份清单通过网络和服务器防火墙公开了隐藏在扫描器和扫描系统之间网络路径中的端口。

网络发现扫描器使用许多不同技术识别远程系统中的开放端口。一些比较常见的技术如下：

TCP SYN 扫描　向每个被扫描的端口发送带有 SYN 标志设置的单个数据包，这代表打开一个新连接的请求。如果扫描器收到了 SYN 和 ACK 标志设置的响应包，则表明该系统正以 TCP 三次握手方式移至第二阶段，且端口是开放的。TCP SYN 扫描也被称为“半开放”扫描。

TCP 连接扫描　向指定端口的远程系统打开一个全连接。这种扫描的使用情景是：扫描用户没有运行“半开放”扫描的必要权限。

TCP ACK 扫描　发送带有 ACK 标志设置的单个数据包，指明它是开放连接的一部分。

Xmas 扫描　发送带有 FIN、PSH 和 URG 标志设置的数据包。这个数据包带有很多标志设置，被称为“点亮的圣诞树”，因而给这种扫描起了这个名字。

提示：

如果忘了 TCP 三次握手是如何实现功能的，可以在第 11 章“网络安全架构与保护网络组件”中找到关于这一内容的全部解释。

用于网络发现扫描的最常见工具是一个名为 nmap 的开源工具。nmap 最初在 1997 年发布，现如今依然在维护和使用。它是一款很受欢迎的网络安全工具。绝大多数安全专家在其职业生涯中或是定期使用 nmap，或是在某种情况下使用 nmap。可以通过下面的链接下载免费的 nmap 或了解关于此工具的更多内容：http://nmap.org。

当 nmap 扫描系统时，它能够识别系统上每个网络端口的当前状态。当 nmap 检测到结果时，会给出该端口的当前状态：

开放　端口在远程系统上是开放的，有一个应用程序正在连接该端口。

关闭　端口在远程系统上可用，意味着防火墙允许接入，但是没有开放应用程序与该端口的连接。

过滤　nmap 无法确定端口是开放还是关闭，因为防火墙对连接请求有干扰。

图 15.1 显示的是正在工作的 nmap 示例。使用者在 Linux 系统中执行下列命令：

```
nmap -vv 52.4.85.159
```

nmap 软件对 IP 地址 52.4.85.159 开始系统端口扫描。指定-vv 标志只是告知 nmap 使用详细模式，对报告结果做出详细输出。扫描结果出现在图 15.1 的底部，表明 nmap 发现系统的三个活动端口：22、80 和 443。端口 22 和 80 是开放的，表明系统正在这些端口上接受连接请求。端口 443 是关闭的，意味着防火墙包含允许在该端口进行连接的请求规则，但系统没有运行适配于接受这类连接的应用程序。

```
Sun May 03 scanner $ nmap -vv 52.4.85.159

Starting Nmap 6.40 ( http://nmap.org ) at 2015-05-03 16:06 UTC
Initiating Ping Scan at 16:06
Scanning 52.4.85.159 [2 ports]
Completed Ping Scan at 16:06, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:06
Completed Parallel DNS resolution of 1 host. at 16:06, 0.00s elapsed
Initiating Connect Scan at 16:06
Scanning ec2-52-4-85-159.compute-1.amazonaws.com (52.4.85.159) [1000 ports]
Discovered open port 22/tcp on 52.4.85.159
Discovered open port 80/tcp on 52.4.85.159
Completed Connect Scan at 16:06, 4.71s elapsed (1000 total ports)
Nmap scan report for ec2-52-4-85-159.compute-1.amazonaws.com (52.4.85.159)
Host is up (0.00090s latency).
Scanned at 2015-05-03 16:06:24 UTC for 5s
Not shown: 997 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
443/tcp closed https

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.73 seconds
Sun May 03 scanner $
```

图 15.1　nmap 扫描 Linux 系统的 Web 服务器

要想解释这些结果，必须了解常见网络端口的使用方法，如在第 12 章中所述。现在来看一下 nmap 的这次扫描结果：

- 端口列表第 1 行，22/tcp open ssh，表示系统在 TCP 端口 22 上接受连接。SSH 服务使用此端口允许管理员连接服务器。
- 端口列表第 2 行，80/tcp open http，表示系统在端口 80 上接受连接请求，使用 HTTP 发送 Web 页面。
- 端口列表最后一行，443/tcp closed https，表示防火墙允许使用端口 443，但没有该端口提供的服务。端口 443 使用 HTTPS 协议接受加密的 Web 服务器连接。

从这些结果中，我们能学到什么？被扫描的系统很可能是一台 Web 服务器，能公开接受来自扫描系统的连接请求。扫描器和系统之间的防火墙配置允许安全(端口 443)和非安全(端口 80)的连接，但实际上并没有对服务器进行加密交易的设置。该服务器也有一个开放的管理员端口，允许命令行连接。

阅读这些结果的攻击者可能会对系统进行如下观测，以便进行进一步的探索：

- 在此服务器上指定 Web 浏览器能很好地观测该服务器能做什么以及谁在操作。在浏览器地址栏中简单输入 http://52.4.85.159 能显示出可用信息。图 15.2 显示了进行此操作的结果：该网址正在运行 Apache Web 服务器的默认安装。
- 指向该服务器的连接没有加密。窃取这些连接，如有可能，会泄露一些敏感信息。
- 开放的 SSH 端口是个有趣的发现。攻击者可能试图在这个端口上对管理员账户进行暴力密码攻击以便进一步访问系统。

在这个例子中，我们用 nmap 扫描单个系统，但是该工具也允许扫描带有开放端口系统的整个网络。图 15.3 显示了对 192.168.1.0/24 网络的扫描，包括 192.168.1.0~192.168.1.255 范围内的全部地址。

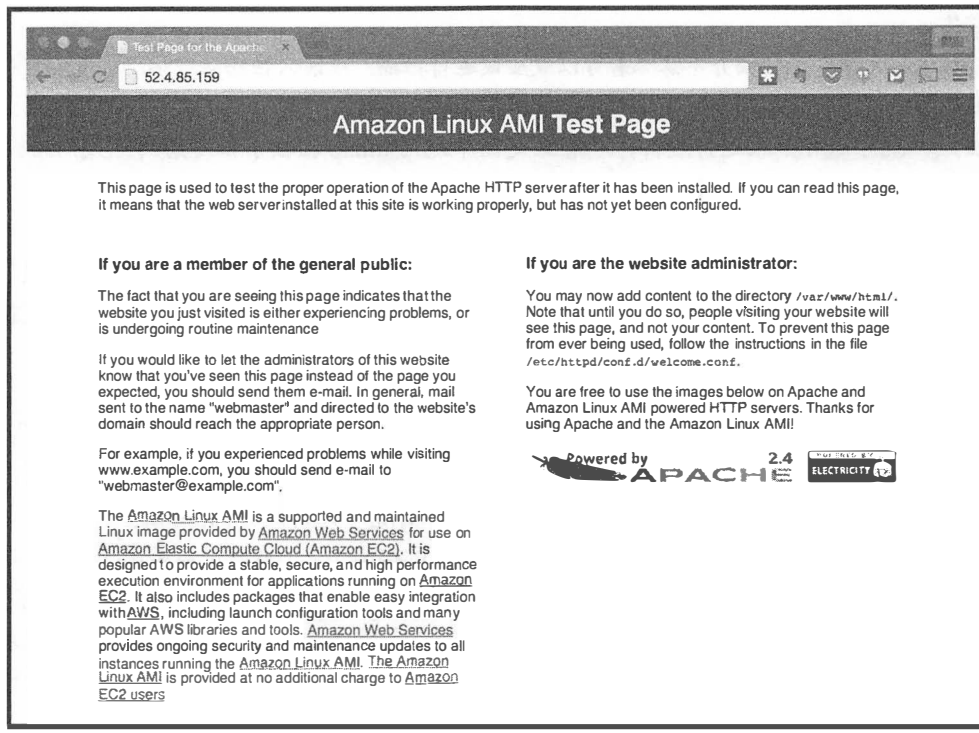


图 15.2　在图 15.1 所示的扫描服务器上运行的默认 Apache 服务器页面

```
MacBook$ nmap 192.168.1.0/24

Starting Nmap 6.01 ( http://nmap.org ) at 2015-05-09 15:50 EDT
Strange error from connect (65):No route to host
Nmap scan report for 192.168.1.65
Host is up (0.036s latency).
All 1000 scanned ports on 192.168.1.65 are closed

Nmap scan report for 192.168.1.69
Host is up (0.0017s latency).
All 1000 scanned ports on 192.168.1.69 are closed

Nmap scan report for 192.168.1.73
Host is up (0.021s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
80/tcp   open  http
515/tcp  open  printer
631/tcp  open  ipp
8080/tcp open  http-proxy
8290/tcp open  unknown
9100/tcp open  jetdirect

Nmap scan report for 192.168.1.94
Host is up (0.00089s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
5009/tcp  open  airport-admin
10000/tcp open  snet-sensor-mgmt

Nmap scan report for 192.168.1.114
Host is up (0.0015s latency).
Not shown: 962 closed ports, 37 filtered ports
PORT     STATE SERVICE
4242/tcp open  vrml-multi-use
```

图 15.3　在 Mac 系统的终端应用上运行大网络范围的 nmap 扫描

警告：

能够运行网络发现扫描并不意味着可以或应该运行扫描。应该只扫描从网络所有者那里得到明确许可的网络，从而进行安全扫描。一些司法机构认为，未经授权的扫描违反了计算机滥用方面的法律法规，就可以对个人进行起诉，尽管只是简单地用 nmap 扫描了咖啡店的无线网络。

2. 网络漏洞扫描

网络漏洞扫描远比网格发现扫描深入。它们不会在检测到开放端口后就停止扫描，而是继续调查目标系统或网络来查找已知的漏洞。这些工具包括数以千计已知漏洞的数据库，它们还能执行一些测试，来确定系统是否易受系统数据库中每个漏洞的影响。

当扫描器测试系统漏洞时，它使用数据库中的测试来确定一个系统是否可能包含漏洞。在某些情况下，扫描器可能没有足够的信息来最终确定一个漏洞的存在，也可能会在没有问题时报告漏洞。这种情况被称为假性正面报告，有时会成为系统管理员的麻烦。更危险的是，漏洞扫描器可能会漏掉漏洞，从而无法提醒管理员危险情况的存在。这种情况被称为假性负面报告。

默认情况下，网络漏洞扫描器会进行未经身份认证的扫描。它们在测试目标系统时，不需要密码，也不需要其他授予扫描器特权的信息。这可以使得扫描从攻击者的角度运行，而且限制了扫描器全面评估可能漏洞的能力。一种提高扫描准确性并减少假性正面和假性负面报告的方法是对系统执行身份认证的扫描。在这种方法中，扫描器可以对被扫描的服务器进行只读访问，可以使用此访问从目标系统读取配置信息，并在分析漏洞测试结果时利用这些信息。

图 15.4 展示了使用 Nessus 漏洞扫描器对系统进行网络漏洞扫描的结果，此系统与本章之前用网络发现扫描器进行扫描的系统是同一系统。

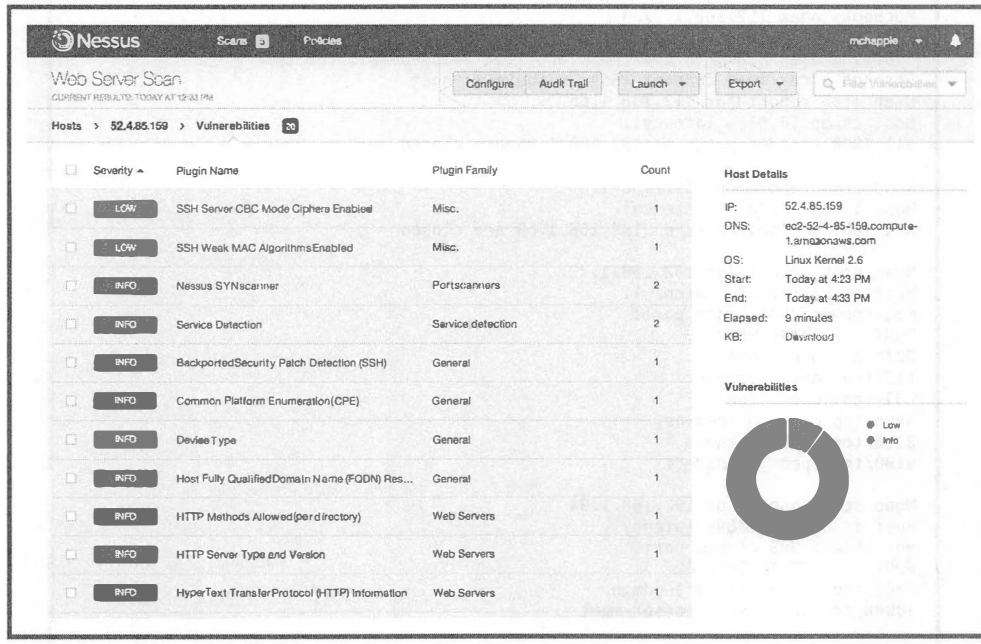


图 15.4　对同一台 Web 服务器的网络漏洞扫描，此服务器在图 15.1 中已进行端口扫描

图 15.4 所示的扫描结果是非常干净的，代表着一个运行良好的系统。没有严重的漏洞，只有两个低风险漏洞，与被扫描系统上运行的 SSH 服务相关。系统管理员可能希望调整 SSH 密码设置，

以删除那些低风险的漏洞，因此这对管理员来说是一份很好的报告，证实了系统管理良好。

学习 TCP 端口

解释端口扫描结果需要对一些常见 TCP 端口有所了解。以下是在准备 CISSP 考试时必须记住的一些 TCP 端口：

FTP	21
SSH	22
Telnet	23
SMTP	25
DNS	53
HTTP	80
POP3	110
NTP	123
HTTPS	443
Microsoft SQL Server	1433
Oracle	1521
H.323	1720
PPTP	1723
RDP	3389

3. Web 漏洞扫描

Web 应用程序对企业安全构成重大风险。就其本质而言，许多运行 Web 应用程序的服务器必须向互联网用户公开服务。防火墙和其他安全设备通常包含一些规则，可以允许网络流量通过 Web 服务器而不受约束。运行在 Web 服务器上的应用程序是复杂的，经常对底层数据库有访问特权。攻击者通常使用 SQL 注入和其他针对 Web 应用程序安全设计缺陷的攻击来发现这些情况。

提示：

在第 9 章“安全脆弱性、威胁和对策”中可以找到有关 SQL 注入攻击、跨站脚本(XSS)、跨站请求伪造(XSRF)和其他 Web 应用程序漏洞的全部讲解。

Web 漏洞扫描器是在 Web 应用程序中搜寻已知漏洞的专用工具。它们在所有安全测试项目中都扮演着重要的角色，因为它们可能会发现网络漏洞扫描器发现不了的缺陷。当管理员进行一次 Web 应用程序扫描时，工具会使用自动化技术探测 Web 应用程序，这些技术会操纵输入和其他参数来识别 Web 漏洞。然后工具会提供一份发现报告，通常包括所建议的漏洞修复技术。图 15.5 还展示了使用 Nessus 漏洞扫描工具进行的 Web 漏洞扫描示例。此扫描针对的运行 Web 应用程序的服务器与图 15.1 和图 15.4 中的服务器相同。阅读图 15.5 中的扫描报告时注意，发现了网络漏洞扫描中没有出现的漏洞。

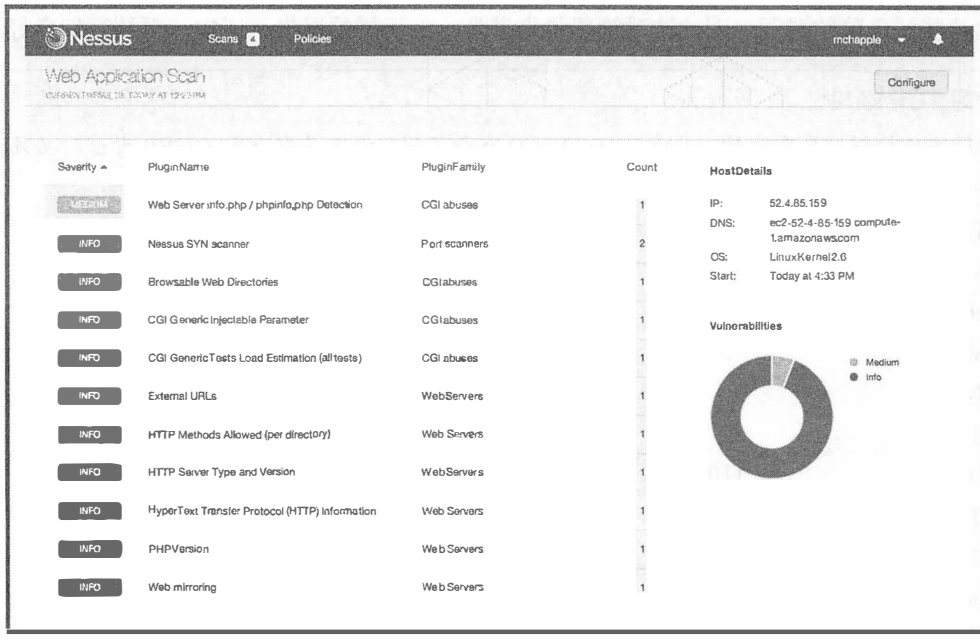


图 15.5　Web 应用程序漏洞扫描，扫描的服务器与图 15.1 和图 15.4 中的服务器相同

注意：

是不是感觉网络漏洞扫描和 Web 漏洞扫描听起来差不多呢？这是因为它们确实差不多！它们是两个运行在一台服务器上的探测服务，用于检测已知的漏洞。所不同的是，网络漏洞扫描通常不会深入到 Web 应用程序的结构，而 Web 应用程序扫描不会查看那些支持 Web 服务以外的服务。许多网络漏洞扫描器也会执行基本的 Web 漏洞扫描任务，但是深入的 Web 漏洞扫描需要专门的、专用的 Web 漏洞扫描工具才行。

你可能已经注意到，Nessus 漏洞扫描器既可以执行图 15.4 所示的网络漏洞扫描，又可以执行图 15.5 所示的 Web 漏洞扫描。Nessus 是一个可以进行两种类型扫描的混合工具。

对于大多数工具，各种漏洞扫描器的功能各异。使用扫描器前，应该先研究一下，以确保符合你的安全控制目标。

Web 漏洞扫描是组织的安全评估和测试程序的一个重要组成部分。在下列情况下运行扫描是很好的：

- 当开始执行第一次 Web 漏洞扫描时，扫描所有的应用程序。这将检测到应用程序的遗留问题。
- 将任何新的应用程序第一次移交生产环境之前进行扫描。
- 在代码更改进入生产环境之前扫描任何修改的应用程序。
- 在循环的基础上扫描所有的应用程序。有限的资源可能需要在基于应用程序优先级的情况下安排这些扫描。例如，可能希望扫描那些经常需要与敏感信息交互的 Web 应用程序。

在某些情况下，可能需要 Web 应用程序扫描来满足合规要求。例如，第 4 章“法律、法规和合规”中讨论的支付卡行业数据安全标准(PCIDSS)要求组织至少每年进行一次 Web 应用程序漏洞扫描，或者安装专用的 Web 应用程序防火墙来增加对 Web 漏洞的额外保护层。

15.2.2　渗透测试

渗透测试超越了漏洞测试技术，因为它实际上试图利用系统漏洞。漏洞扫描只是调查漏洞的存在，通常不会对目标系统采取进攻行动(也就是说，一些漏洞扫描技术可能会破坏系统，尽管这些选项通常在默认情况下是禁用的)。另一方面，安全专家进行渗透测试是为了试图让安全控制失效，进入目标系统或应用程序来展示缺陷。

渗透测试需要训练有素的安全专家集中注意力来应对比漏洞扫描更广的范围。当执行渗透测试时，安全专家通常的目标是一个系统或一组系统，并使用许多不同的技术来访问。这个过程可能包括：

- 执行基本侦察来确定系统功能(如访问托管在系统上的网站)
- 执行网络发现扫描以识别开发端口
- 执行网络漏洞扫描以识别没有应用补丁的漏洞
- 执行 Web 应用程序漏洞扫描以识别 Web 应用程序缺陷
- 使用开发工具自动试图破坏系统安全
- 尝试手动探测和攻击

渗透测试人员通常使用一个名为 Metasploit 的工具来自动对目标系统执行攻击。如图 15.6 所示，Metasploit 使用一门脚本语言来允许自动执行常见的攻击，以节省测试人员(和黑客!)大量的时间，因为执行攻击时涉及的许多烦琐步骤被省略了。

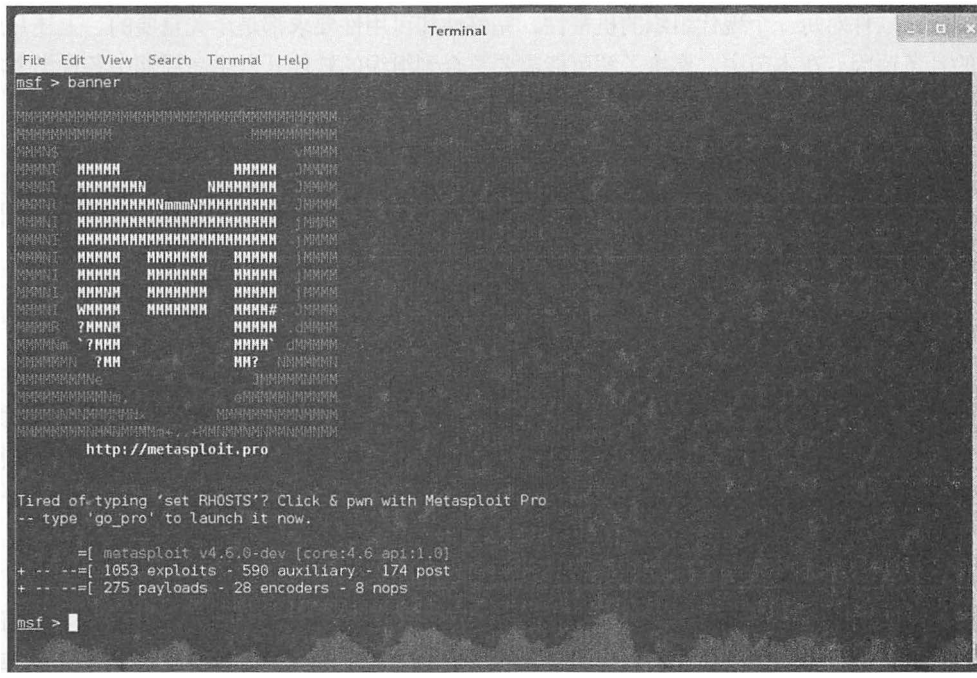


图 15.6　Metasploit 自动系统漏洞发现工具允许攻击者迅速执行对目标系统的常见攻击

渗透测试人员可能是公司员工，他们执行这些测试作为职责的一部分，也可能是由聘请的外部顾问执行渗透测试。测试通常分为三组：

白盒渗透测试 为攻击者提供了目标系统的详细信息。这绕过了攻击之前经常会有的许多侦察步骤，缩短了攻击时间并增加了发现安全漏洞的可能性。

灰盒渗透测试 也称为部分知识测试，有时会选择这些来平衡白盒和黑盒渗透测试的优缺点。如果想要黑盒渗透测试结果，但是成本或时间有限，就意味着需要一些知识来完成测试，这种情况特别常见。

黑盒渗透测试 攻击之前不为攻击者提供任何信息。这模拟了外部攻击者在进行攻击之前试图获取业务和技术环境信息的情况。

渗透测试耗时较长，并且需要专门的资源，但它们在良好的信息安全测试程序的持续运行中扮演着重要角色。

15.3 测试你的软件

软件是系统安全的一个关键组成部分。考虑在整个现代企业中使用的许多应用程序的常见特点：

- 软件应用程序通常有特权进入操作系统、硬件和其他资源。
- 软件应用程序经常处理敏感信息，其中包括信用卡号码、社会保障号和专利业务信息。
- 许多软件应用程序都依赖于也包含敏感信息的数据库。
- 软件是现代企业的核心，执行关键业务功能。软件故障可以扰乱企业业务，带来非常严重的后果。

仔细测试软件对每一个现代组织的机密性、完整性和可用性要求都是至关重要的。上述几点只是集中的几条原因。在本节中，你将了解可能需要整合到组织的软件开发生命周期中各种类型的软件测试。

注意：

本章主要讲解软件测试主题。在第 20 章“软件开发安全”中可以找到更深层次的软件开发生命周期(SDLC)和软件安全问题。

15.3.1 代码审查和测试

软件测试项目的最关键部件之一是进行代码审核和测试。这些程序在将代码移交生产环境之前由第三方对开发人员执行的工作进行评审。代码审核和测试可能会在缺陷生效并对经营产生负面影响之前发现安全、性能或可靠性缺陷。

1. 代码审查

代码审查是软件评估项目的基础。在代码审查(也称为“并行审核”)期间，由除了写代码的人以外的开发人员进行审查、查找缺陷。代码审查的结果可能是应用程序被批准进入生产环境，或他们可能把代码发回最初的开发人员，并对审查中发现的问题提供返工建议。

代码审查可能会有许多不同的形式，不同组织之间的形式也是不同的。最正式的代码评审过程称为 Fagan 检查，遵循如下严格的审查和测试过程，有 6 个步骤：

(1) 规划

(2) 概述
(3) 准备
(4) 检查
(5) 返工
(6) 后续行动

对 Fagan 检查的概述见图 15.7。每个步骤都有明确定义的进出标准，从一个阶段过渡到下一个阶段时必须满足这些标准。

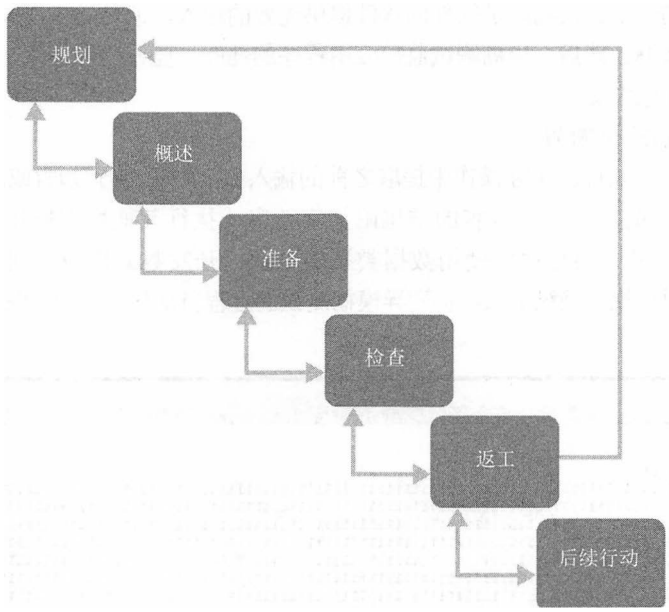


图 15.7　Fagan 检查遵循严格的正式流程，各阶段之间的转换必须满足明确定义的进出标准

正式的 Fagan 检验通常只存在于高度受限的环境中，其中代码缺陷可能产生灾难性影响。大多数组织都使用那些代码并行审查措施不太严格的流程，包括：

- 开发人员在会见一个或多个其他团队成员时走查他们的代码
- 高级开发人员执行手工代码审查，在转入生产环境之前签署所有代码
- 在转入生产环境之前，使用自动审核工具检测常见的应用程序缺陷

每个组织都应该采取一种适合自身业务需求和软件开发文化的代码审查流程

2. 静态测试

静态测试在不运行软件的情况下通过分析源代码或编译的应用程序对软件进行评估。静态分析通常涉及用来检测常见软件缺陷(如缓冲区溢出)的自动化工具。在成熟的开发环境中，应用程序开发人员能够使用静态分析工具，并在设计、开发和测试过程中使用它们。

3. 动态测试

动态测试是在运行环境中评估软件安全，对于部署别人写的应用程序的组织来说通常是唯一选择。在这种情况下，测试人员经常不能访问底层的源代码。动态软件测试的一个常见例子是使用 Web 应用程序扫描工具来检测 Web 应用程序中的跨站脚本、SQL 注入或其他缺陷的存在。对生产

环境的动态测试应该进行小心协调，以避免意外中断服务。

动态测试可能包括使用综合事务来验证系统的性能。这些是具有已知预期结果的脚本事务。测试人员针对测试代码运行综合事务，然后将事务输出与预期状态进行比较。实际结果和预期结果之间的任何偏差都代表代码中可能的缺陷，必须进一步研究。

4. 模糊测试

模糊测试是一项专门的动态测试技术，向软件提供了许多不同类型的输入，来强调其局限性并发现先前未被发现的缺陷。模糊测试软件向软件提供无效的输入，或是随机生成，或是特别制作，以触发特殊的软件漏洞。然后，模糊测试监控应用程序的性能，监视软件崩溃、缓冲区溢出或其他不良和/或不可预知的结果。

有两个主要类别的模糊测试：

变异模糊测试　从软件的实际操作中提取之前的输入值，对其进行处理(或改变)以创建模糊输入。它可能改变内容的字符，为内容的结尾附加字符串或执行其他数据操作技术。

智能模糊测试　基于对程序所使用数据类型的理解，开发数据模型并创建新的模糊输入

zzuf 工具根据用户规范操纵输入，将变异模糊测试的过程自动化。例如，图 15.8 显示了一个包含一系列 1 的文件。

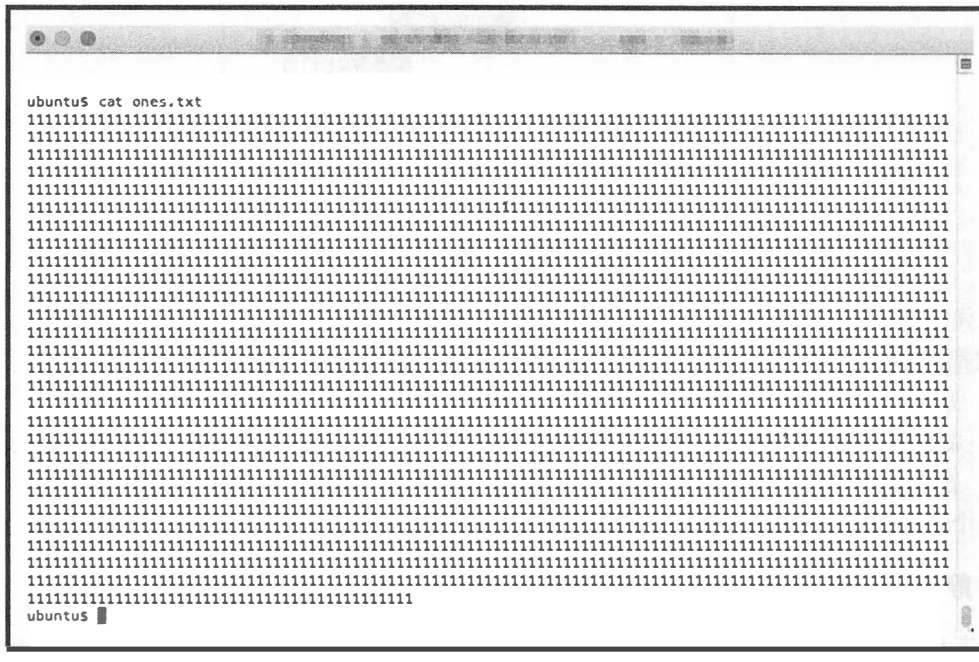


图 15.8　对包含一系列 1 的输入文件进行预模糊测试

图 15.9 显示了应用于这种输入的 zzuf 工具。产生的被模糊文本几乎与原始文本是相同的。尽管还是主要包含 1，但现在文本有几个变化，可能会与期望原始输入的程序相混淆。这个稍微操纵输入的过程被称为翻转。

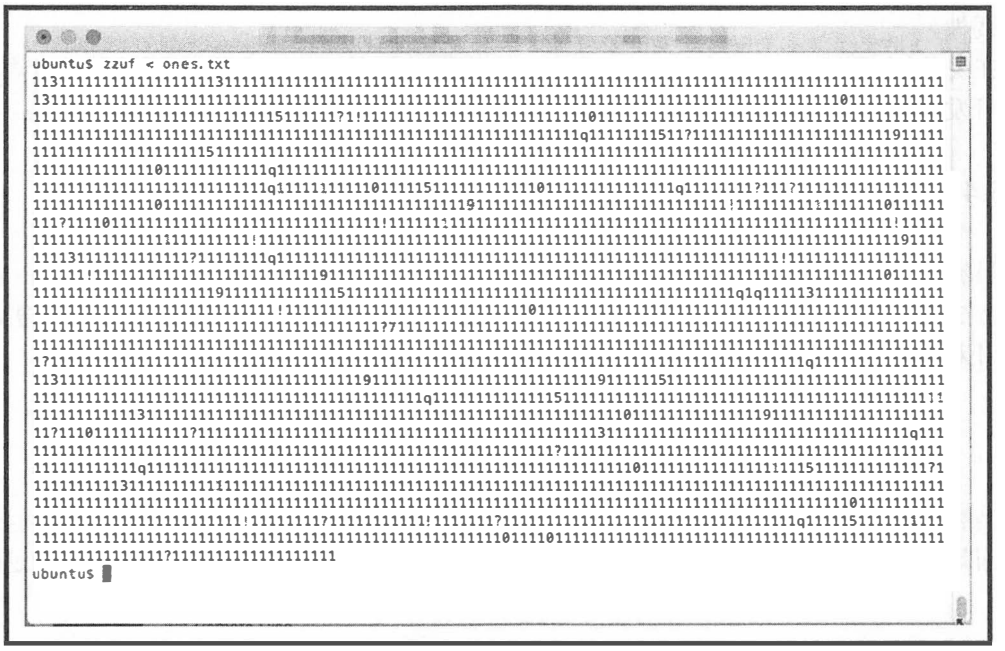


图 15.9　图 15.8 所示的输入文件经过 zzuf 变异模糊测试工具后的结果

15.3.2　接口测试

接口测试是开发复杂软件系统的一个重要组成部分。在许多情况下，多个团队的开发人员必须在复杂应用程序的不同部分进行工作，他们必须相互合作以实现业务目标。这些被分别开发的模块之间的传递使用定义良好的接口，以便团队可以独立工作。接口测试评估模块针对接口规范的性能，以确保所有开发工作完成后模块能正常工作。

在软件测试过程中，应对三种接口进行测试：

应用编程接口(API)　为代码模块提供一种标准化的方式进行交互，可以通过 Web 服务向外部公开。开发人员必须测试 API 来确保它们执行所有安全需求。

用户界面(UI)　例子包括图形用户界面(GUI)和命令行接口。UI 为终端用户提供与软件交互的能力。界面测试应包括审查所有的用户界面来验证它们能否正常运作。

物理接口　在一些操作机器、逻辑控制器或物理世界中其他对象的应用程序中存在。软件测试人员应该注意物理接口，因为如果它们失效，会带来一些潜在后果。

接口为复杂系统的计划或未来互连提供重要的机制。Web 2.0世界取决于这些接口的可用性，以方便不同软件包之间的相互作用。然而，开发人员必须小心，因为接口提供的灵活性不会带来额外的安全风险。接口测试对接口满足组织的安全需求提供了一种更高程度的保证。

15.3.3　误用案例测试

在某些应用程序中，关于软件用户可能试图滥用应用程序有明确示例。例如，银行软件的用户可能会试图操纵输入字符串来获取其他用户的账户。他们也可能试图从一个已经透支的账户取出资金。软件测试人员使用称为误用案例测试或滥用用例测试的过程来评估他们的软件对这些已知风险

的脆弱性。

在误用案例测试中，测试人员首先列举已知的误用案例。然后他们试图使用手动和/或自动攻击技术开发这些用例。

15.3.4 测试覆盖率分析

虽然测试是软件开发过程的重要组成部分，但遗憾的是，不可能对全部软件都进行测试。有太多的方法会造成软件故障或用于对它们进行攻击。软件测试专业人员经常进行测试覆盖率分析，进行估计对新软件进行测试的程度。使用以下公式计算测试覆盖率：

$$\text{测试覆盖率} = \frac{\text{使用的测试用例数}}{\text{使用的用例总数}}$$

当然，这种计算非常主观。准确计算测试覆盖率要求列举可能的用例，这是一项非常艰巨的任务。因此，任何人在使用测试覆盖率计算时都应该理解在解释研究结果时用于开发输入值的过程。

15.4 实现安全管理过程

除了进行评估和测试，有效彻底的信息安全项目还包括各种管理流程，用来监督信息安全程序的有效运行。这些过程在安全评估过程中是关键的反馈回路，因为它们提供管理监督，并对内部攻击的威胁起到震慑作用。满足这一需求的安全管理评审包括日志审核、账户管理、备份验证、关键性能指标和风险指标。

15.4.1 日志审核

在第 16 章“管理安全运营”中，你将学习存储日志数据的重要性，并进行自动和手动日志审核。安全信息和事件管理(SIEM)系统在这些过程中发挥重要作用，将日志审查的大部分日常工作自动化。信息安全管理人员还应该定期进行日志审查，特别是对于敏感功能来说，以确保特权用户不滥用特权。例如，如果一支信息安全团队访问了 eDiscovery 工具，能够搜索个人用户文件的内容，那么安全管理人员应定期检查这些管理用户的行动日志，以确保他们的文件访问与合法 eDiscovery 相关方案并不侵犯用户隐私。

15.4.2 账户管理

账户管理审核确保用户只保留授权权限，而没有发生未经授权的修改。账户管理审核可能是信息安全管理人员或内部审计师的职责之一。执行账户管理审核的方法之一是对所有账户进行全面的审核。通常只对高特权账户这样做，因为审核全部账户太耗时间。具体过程可以根据组织的不同而不同，但这里有一个例子：

(1) 管理人员要求系统管理员提供具有访问特权的用户列表及其被授予的特权。他们可能会对管理员进行监控，同样他们还会检索该列表来避免篡改。

(2) 管理人员要求特权批准机构提供授权用户的列表及其他们应被分配的特权。

(3) 然后管理人员比较这两个列表，以确保只有授权用户可以访问系统且每个用户的访问不超出他们的授权。

这个过程可能包括许多其他检查，如验证终止用户不保留对系统的访问，检查特定账户的书面记录或其他任务。

没有时间执行整个过程的组织可以使用抽样。在这种方法中，管理人员抽出账户的随机样本，对授予这些账户权限的过程执行一次完整的验证。如果在样本中未发现明显的缺陷，就可以认为它们代表所有账户。

警告：

只有随机抽样才是有效的！不允许系统管理员生成样本或使用非随机的标准选择要审核的账户，否则有可能错过存在错误的所有用户类别。

15.4.3　备份验证

在第 18 章“灾难恢复计划”中，将学习维护一致的备份程序的重要性。管理人员应该定期检查备份的结果，以确保过程有效执行，并满足组织的数据保护需要。这可能涉及审核日志、检查散列值或请求对系统或文件的实际恢复。

15.4.4　关键性能指标和风险指标

安全管理人员还应该持续监视关键性能指标和风险指标。他们所监视的确切指标将根据组织的不同而不同，但可能包括以下：

- 开放漏洞的数量
- 解决漏洞的时间
- 被盗账户的数量
- 在生产前扫描(preproduction scanning)中发现的软件缺陷数
- 重复审计发现
- 访问恶意网站的用户尝试

一旦组织识别了希望跟踪的关键安全度量，管理人员可能希望开发一个仪表板，以清楚地显示这些指标的值随时间推移的变化，并将其放在管理人员和安全团队能够经常看到的地方。

15.5　本章小结

安全评估和测试程序在确保组织的安全控制随时间保持有效性方面发挥着重要作用。业务操作、技术环境、安全风险和用户行为的变化，可能会改变用于保护信息资产的机密性、有效性、完整性和可用性的控制的有效性。评估和测试程序监控这些控制，并强调要求管理员干预的那些变化。安全专家应该仔细设计评估和测试程序，并根据业务需求的变化进行修改。

安全测试技术包括漏洞评估和软件测试。在漏洞评估中，安全专家执行各种各样的测试，以确

定系统和应用程序中的配置错误和其他安全缺陷。网络发现测试确定网络上带有开放端口的系统。网络漏洞扫描能够在这些系统上发现已知的安全漏洞。Web 漏洞扫描对 Web 应用程序的操作进行探测，以寻找已知的漏洞。

软件在任何安全基础设施中都发挥着至关重要的作用，因为它处理敏感信息并与关键资源进行交互。组织应该使用代码审核过程，在移交生产环境之前进行并行代码验证。严格的软件测试项目还包括使用静态测试、动态测试、接口测试和误用案例测试，以有力地评估软件。

安全管理过程包括日志审查、账户管理、备份验证和跟踪关键性能指标和风险指标。这些流程帮助安全管理人员验证信息安全项目的持续有效性。第三方不太频繁地进行的正式内部审计和外部审计可作为补充。

15.6 考试要点

了解安全评估和测试程序的重要性。安全评估和测试程序为验证安全控制的持续有效性提供了一个重要的机制。它们包括各种工具，包括漏洞评估、渗透测试、软件测试、审计工具以及旨在验证控制的安全管理任务。每个组织都应该有明确定义和可操作的安全评估和测试程序。

进行漏洞评估和渗透测试。漏洞评估使用自动化工具来搜索系统、应用程序和网络中的已知漏洞。这些缺陷可能包括缺失的补丁、配置错误或错误的代码，它们会使组织暴露于安全风险中。渗透测试也使用相同的工具，但以攻击技术作为补充，评估人员试图利用漏洞并访问系统。

执行软件测试来验证进入生产环境的代码。软件测试技术能验证代码功能符合设计，并不包含安全缺陷。代码审核使用并行评审过程在代码部署到生产环境之前进行正式或非正式的验证。接口测试利用 API 测试、用户界面测试和物理接口测试评估组件和用户之间的交互。

理解静态和动态软件测试的区别。静态软件测试技术，如代码审核，通过分析源代码或所编译应用程序，在软件未运行时对软件安全进行评估。动态测试在软件运行时评估软件安全，对于部署由别人写的应用程序的组织来说通常是唯一选择。

解释模糊测试的概念。模糊测试使用修改过的输入来测试软件在意外情况下的性能。变异模糊测试修改已知输入来生成合成输入，这可能会引发意想不到的行为。智能模糊测试基于预期输入模型来开发输入，以执行相同的任务。

执行安全管理任务以提供对信息安全项目的监管。安全管理人员必须执行各种活动，以保证对信息安全项目的适当监督。日志审核，特别是对于管理员的活动来说，能够确保系统不被滥用。账户管理审核确保只有授权用户具有对信息系统的访问权限。备份验证保证了组织的数据保护过程正常运作。关键性能指标和风险指标提供了安全计划有效性的高级视图。

执行或促进内部和第三方审计。当第三方对用于保护组织信息资产的安全控制进行评估时，安全审计便会出现。内部审计由组织的内部员工进行，仅用于管理。外部审计由第三方审计公司进行，通常用于组织的治理机构。

15.7 书面实验室

1. 描述 TCP SYN 扫描和 TCP 连接扫描的区别。

2. nmap 网络发现扫描工具返回的三个端口状态值是什么？
3. 静态和动态代码测试技术的区别是什么？
4. 变异模糊测试和智能模糊测试的区别是什么？

15.8　复习题

1. 以下哪个工具主要用于网络发现扫描？
   A. nmap
   B. Nessus
   C. Metasploit
   D. lsof
2. Adam 最近对组织内运行的 Web 服务器进行了一次网络端口扫描。他从外部网络进行扫描，以获得攻击者的扫描角度。下列哪个结果是引起警报的最大原因？
   A. 80/open
   B. 22/filtered
   C. 443/open
   D. 1433/open
3. 在为某个特定系统规划安全测试计划时不应考虑下列哪个因素？
   A. 存储在系统上的信息的敏感度
   B. 执行测试的难度
   C. 利用新测试工具进行试验的意愿
   D. 系统对攻击者的吸引力
4. 以下哪一项一般不包括在安全评估中？
   A. 漏洞扫描
   B. 风险评估
   C. 漏洞缓解
   D. 威胁评估
5. 谁是安全评估报告的阅读对象？
   A. 管理人员
   B. 安全审计师
   C. 安全专家
   D. 客户
6. Beth 想在组织的私有网络上对所有系统运行 nmap 扫描，包括处于 10.0.0.0 私有地址空间中的系统。她想要扫描整个私有地址空间，因为她不确定使用的是哪个子网。Beth 应该以哪个网络地址作为扫描目标？
   A. 10.0.0.0/0
   B. 10.0.0.0/8
   C. 10.0.0.0/16
   D. 10.0.0.0/24

7. Alan 对服务器运行 nmap 扫描，确定服务器上的端口 80 是开放的。什么工具可能会给他带来有关服务器目的和服务器操作者身份的最好附加信息？

A. SSH

B. Web 浏览器

C. telnet

D. ping

8. 什么端口通常用于使用 SSH 实用工具接受管理连接？

A. 20

B. 22

C. 25

D. 80

9. 下列哪个测试提供有关服务器安全状态的最准确和最详细信息？

A. 未经身份认证的扫描

B. 端口扫描

C. 半开式扫描

D. 经验证的扫描

10. 什么类型的网络发现扫描只遵循 TCP 握手的前两个步骤？

A. TCP 连接扫描

B. Xmas 扫描

C. TCP SYN 扫描

D. TCP ACK 扫描

11. Matthew 想在网络上测试系统的 SQL 注入漏洞。下列哪个工具最适合这个任务？

A. 端口扫描器

B. 网络漏洞扫描器

C. 网络发现扫描器

D. Web 漏洞扫描器

12. Badin Industries 运行着一个处理电子商务订单和信用卡交易的 Web 应用程序。因此，它应遵守支付卡行业数据安全标准(PCI DSS)。该公司最近对应用程序执行了 Web 漏洞扫描，没有得到不满意结果。Badin 应多久后重新扫描应用程序？

A. 只能在应用程序发生变化时

B. 至少每月

C. 至少每年

D. 没有再次扫描的要求

13. Grace 对客户的网络执行渗透测试，并且愿意使用工具协助自动执行常见的漏洞利用。下列哪个安全工具能最好地满足她的需要？

A. nmap

B. Metasploit

C. Nessus

D. Snort

14. Paul 想用之前使用的输入的稍微修改版来测试应用。Paul 打算进行什么类型的测试？

A. 代码审核

B. 应用程序漏洞审核

C. 变异模糊测试

D. 智能模糊测试

15. 银行应用程序的用户可能试图从不存在资金的账户中取出资金。开发人员意识到这种威胁，并实现代码进行防范。如果开发人员还没有矫正，那么什么类型的软件测试最有可能捕捉到这种类型的漏洞？

A. 误用案例测试

B. SQL 注入测试

C. 模糊测试

D. 代码审核

16. 哪种接口测试能够识别程序命令行接口的缺陷？

A. 接口测试中的应用编程

B. 用户接口测试

C. 物理接口测试

D. 安全接口测试

17. 在什么类型的渗透测试期间，测试人员总是访问系统配置信息？

A. 黑盒渗透测试

B. 白盒渗透测试

C. 灰盒渗透测试

D. 红盒渗透测试

18. 在运行未加密 HTTP 服务器的系统上，什么端口通常是开放的？

A. 22

B. 80

C. 143

D. 443

19. 下列哪一项是 Fagin 检验过程的最后一步？

A. 检验

B. 返工

C. 后续行动

D. 以上均不是

20. 什么信息安全管理任务能够确保有效地满足组织的数据保护需求？

A. 账户管理

B. 备份验证

C. 日志审核

D. 关键性能指标

第 16 章

管理安全运营

本章中覆盖的 CISSP 考试大纲包含：

安全运营

- D. 保护资源的配置
  - D.1 资产清单(例如，硬件、软件)
  - D.2 配置管理
  - D.3 物理资产
  - D.4 虚拟资产(例如，软件定义网络、虚拟 SAN、宾客操作系统)
  - D.5 云资产(例如，服务、VM、存储、网络)
  - D.6 应用(例如，负载或私有云、Web 服务、SaaS)
- E. 理解和应用基本的安全操作原则
  - E.1 知其所需/最小特权(例如，权利、聚合、传递信任)
  - E.2 职责和责任分离
  - E.3 监控专有特权(例如，操作、管理)
  - E.4 岗位轮换
  - E.5 信息生命周期
  - E.6 服务级别协议
- F. 采用资源保护技术
  - F.1 介质管理
  - F.2 硬件和软件资产管理
- I. 执行和支持补丁及脆弱性管理
- J. 参与和理解变更管理流程(例如，版本、基线、安全影响分析)
- P. 参与解决人身安全问题(例如，胁迫、旅行、监控)

安全运营域包括范围广泛的安全基础概念和最佳实践。该域包含许多核心概念，任何组织都需要这些概念来提供基本的安全保护。本章的 16.1 节将讨论这些概念。

资源保护确保在资源整个生命周期内的介质和其他有价值的资产都得到保护。类似地，配置管

理确保系统在整个生命周期内都被配置，并且变更管理流程使系统免受外部未授权改变导致的运行中断。补丁和漏洞管理控制确保系统是最新的，并使其免受已知漏洞的攻击。

16.1 应用安全运营的概念

安全运营实践的主要目的是保障系统中信息资产的安全性。这些实践有助于确定威胁和漏洞，并实施控制来降低整个组织资产的风险。

在 IT 安全环境中，应尽关注和应尽职责依靠不断演进的基本原则，采取合理的关注来保护组织的资产。高级管理人员对执行应尽关注和应尽职责有直接责任。实施的通用安全运营概念包括如下几个部分：执行周期性的审计和检验，验证应尽关注和应尽职责的级别(这将减少损失发生时高级管理部门的责任)。

16.1.1 知其所需和最小特权

知其所需和最小特权是值得在任何 IT 安全环境中采纳的两条标准原则。通过限制对有价值资产的访问来提供保护。虽然这两个术语之间有关联，且许多人都交换地使用这两个术语，但是它们之间仍然有一些明显的差异。知其所需关注权限和访问信息的能力，而最小特权关注特权。

第 14 章“控制和监控访问”对许可、权限和特权做了对比。提醒一下，许可允许访问客体，如文件。权限涉及采取行动的能力。访问权限和许可是同义词，但是权限涉及操作操作系统的能力，例如改变系统时间。特权是权限和许可的结合。

1. 知其所需访问

知其所需原则利用需求来给用户授权，仅仅根据为完成所分配任务而授权访问需要操作的数据或资源。主要目的是保持秘密信息的机密性。如果想保守一个秘密，最佳方式是不告诉任何人。如果你是唯一知道该秘密的人，你能确保守口如瓶。但如果你告诉一个可信朋友，他或许会保守秘密，也或许会告诉其他人——例如其他可信朋友。然而，越多的人了解该秘密，机密泄露的风险越高。限制知道秘密的人将增加保守秘密的可能性。

知其所需一般与安全许可相关，例如有安全许可的个人。然而，安全许可不能自动为数据授予访问。例如，假设 Sally 有安全许可。这表明她被允许访问某些机密数据。然而，该许可不能自动授权她访问所有的机密数据，因为高级管理员仅仅授权她访问在工作中需要知道的机密数据。

虽然知其所需经常与军事和政府机构中使用的安全许可相关，但也能应用在民用组织中。例如，数据库管理员需要访问数据库服务器来执行维护，但不需要访问服务器数据库中的所有数据。基于知其所需的访问限制有助于抵御未授权访问导致的机密性丧失。

2. 最小特权原则

最小特权原则表明主体仅仅被授予执行已分配工作任务的特权，不会拥有超出其工作任务的特权。记住这里所讲的特权包含了数据的许可权和执行系统任务的权限。针对数据，包含了数据的控制能力，如阅读、创建、修改、删除操作，基于最小特权原则的限制和特权控制就可以保障数据的机密性和完整性。如果用户仅仅能修改为完成工作所需要修改的这些数据文件，那么这将保护环境

中其他文件的完整性。

注意：

最小特权原则依靠如下假设：全体用户都有每个人都能理解的明确定义的工作描述。如果没有确定的工作描述，将不可能知道用户需要什么样的特权。

但是最小特权原则不仅仅延伸到数据访问，也应用到了系统访问中。例如，网络中的普通用户能够使用一个网络账户登录网络中的任何一台计算机。然而，组织通常通过阻止普通用户登录服务器或限制用户登录单个工作站来限制这些特权。

组织违背最小特权原则的通常方式是增加所有用户到本地管理员组或者授予某台计算机的根访问权限。这将给予用户对计算机的完全控制权。然而，普通用户很少需要这么多的访问。当他们有这么多的访问时，他们能意外地(或故意地)导致系统内部的破坏，例如访问或删除有价值的数据。

此外，如果用户使用完整的管理员特权登录，并无心安装了恶意软件，恶意软件就能获取用户账户的整个管理员特权。相比之下，如果用户使用普通用户账户登录，恶意软件仅仅能够获取普通账户的有限特权。

最小特权确保用户的特权是受到约束的，但最小特权也被应用在其他主体中，如应用或进程。例如，服务和应用经常运行在一个账户的上下文中，该账户是由特定的服务或应用创建的。从历史观点来讲，管理员经常授予这些服务账户整个管理员特权，而不考虑最小特权原则。如果攻击者获取了该应用，他们能潜在地获得服务账户的特权，授予攻击者整个管理员特权。

当知其所需和最小特权被授予、聚合和传递信任时，额外的人员概念需要被考虑。

授予　授予特权涉及一系列用户获取的特权，典型地是当第一次开通账户时。换句话说，当管理员创建用户账户时，他们应确保该账户被分配了适量的资源，并且包括特权。用户服务开通的过程应该采用最小特权原则。

聚合　最小特权环境下的聚合涉及用户随着时间而收集到的一系列特权。例如，如果一个用户从一个部门转到另一个部门，但同时还是在一家公司任职，这个用户会终止每个部门的特权。为了避免访问的聚合问题，管理员在用户转到不同部门时应该收回特权，使其不再拥有前一个部门的特权。

传递信任　非传递信任出现在两个安全域中，这两个安全域可能在同一个组织也可能在不同的组织之间。这允许一个域中的主体访问另一个域中的客体。传递信任扩展了两个安全域以及它们的所有子域之间的信任关系。在最小特权环境中，检查这些域的信任关系非常重要，尤其是在不同的组织间创建域。非传递信任实施了最小特权原则并在某一时刻授予信任给单个域。

16.1.2　职责和责任分离

职责和责任分离确保没有单个人能控制某个关键功能或整个系统。这很有必要，能确保没有单个人能危害到系统或系统的安全性。相反，两人或更多人必须共谋或串通违反组织，这对于这些人增加了被发现的风险。

职责分离策略建立了一个相互制约和平衡的系统，在这个系统中，多个主体可以相互校验操作，并且必须一起完成必要的工作任务。职责分离使得恶意的、欺诈的犯罪或其他未授权的活动变得更加困难，并且拓宽了检测和报告的范围。相比之下，如果他们认为可以侥幸成功，那么执行未授权活动是十分容易的，但是涉及两人或更多人，那么被发现的风险将会增加，这通常会作为一种有效

威慑。

有一些简单的例子。电影院使用职责分离来预防欺诈。一人卖票，另外的人收票，并且不允许没有票的人进入。如果同一个人既能收钱又能授权进入，那么这个人就可能允许没有票的人进入电影院，或者将收到的钱放入自己口袋而不发票。当然，也有可能卖票的人和收票人合谋，并图谋从电影院偷票。这就是合谋，因为在两人或更多人之间必须达成某个协议来执行某些未授权的活动。然而，合谋将花费更多的精力且增加了每个人的风险。职责分离策略能减少未授权共谋欺骗的实施。

类似地，组织经常将一个过程分解为多人任务或职责，并且分配这些职责到不同的人来预防欺骗。例如，某人批准有效的账单付款，而其他人执行实际上的付款。如果某人控制整个付款批准和付款过程，那么他将很容易批准伪造的发票来欺骗公司。

另一种方式的职责分离是通过在多个可信个体中划分安全职责或管理能力来实施。当组织在许多用户间划分管理和安全职责时，个人不可能有足够的访问权限来规避或禁用安全机制。

1. 特权分离

特权分离类似于任务和职责分离的概念，建立在最小特权原则之上并应用到应用程序和进程中。特权分离策略要求使用颗粒状的权限和许可。

管理员为每种类型的特权操作分配不同的权限和许可。他们仅仅授予必需的特权给特定进程来执行一定的功能，而不是授予他们对系统无限的访问权。

正像最小特权原则一样能应用到用户和服务账户中，特权分离的概念也能应用到用户和服务账户中。

许多服务器应用有一些支持应用的潜在服务，并且作为早期的描述，这些服务必须运行在一个账户环境中，通常称为服务账户。针对服务器的应用拥有多个服务账户在今天是很常见的。管理员授予每个服务账户唯一的特权，该特权需要在应用程序中才能执行相应的功能。这样就支持了特权分离策略。

2. 职责划分

职责划分类似于任务和职责分离策略，但也结合了最小特权原则。职责划分的目标是确保个人没有可能导致利益冲突的额外系统访问。当职责被完全分离时，单个雇员将没有能力制造欺骗或犯错误，并且也没有能力来掩盖错误。在职责被划分时，类似于职责分离，也类似于在特权被限制时的最小特权原则。

职责划分策略对于任何一家必须遵守 2002 萨班斯-奥克斯利法案(SOX)的公司都是高度相关的，因为 SOX 明确指出需要进行职责划分。然而，在任何 IT 环境中执行职责划分策略也是有可能的。

注意：

SOX 被应用于所有的上市公司，上市公司都已经在证券交易委员会(SEC)那里注册了抵押和欠债状况。美国政府通过 SOX 法案作为对许多知名度较高的金融丑闻的一种响应，这些金融丑闻曾经导致股东数以亿计美元的损失。

其中，在组织内部实施职责划分最常见的是确保安全职责从其他职责中分离出来。换句话说，负责审计、监控和安全审查的个人没有其他操作职责，这些操作职责与他们正在执行的审计、监控和审查活动有关联。无论任何时候，安全职责都将结合其他操作职责，因此个人能使用他们的安全特权来掩盖与他们的操作职责相关的活动。

图 16.1 给出了一个基本的职责划分控制矩阵，它在组织内部对比不同的角色和任务。使用 X 标识的区域表明了要避免潜在的冲突。例如，考虑个应用程序员和安全管理员。程序员能对应用执行未授权的修改，但是安全管理员将通过审计或审查检测出未授权的修改。然而，如果某人拥有这两项工作的职责(和特权)，此人将修改应用并掩盖修改来防止被检测到。

角色/任务	应用程序员	安全管理员	数据库管理员	数据库服务器管理员	预算分析师	应收账款	应付账款	补丁部署	验证补丁
应用程序员		X	X	X					
安全管理员	X		X	X	X	X	X	X	
数据库管理员	X	X		X					
数据库服务器管理员	X	X	X						
预算分析师		X				X	X		
应收账款		X			X		X		
应付账款		X			X	X			
补丁部署		X							X
验证补丁								X	
	冲突的潜在区域								

图 16.1　职责分离控制矩阵

注意：

职责划分控制矩阵中的角色和任务不是所有组织使用的标准。一般组织会裁剪角色和职责，使其更适用于组织内部。例如，图 16.1 中的这个矩阵为我们提供了确定潜在冲突的指引。

理论上，一般个人将不会被分配两个有利益冲突的角色。然而，如果环境需要分配有利益冲突的角色，我们将实施补偿控制来缓解风险。

3. 双人控制

双人控制类似于职责划分，需要两个人认同关键任务。例如，需要两把钥匙才能打开银行的安全存款箱。银行的一个雇员控制着一把钥匙，顾客控制着另一把钥匙。要开箱，需要两把钥匙，且银行雇员允许一个顾客访问箱子仅仅是在验证了该顾客的身份之后。

在组织内使用双人控制确保了并行互审并减少了共谋和欺骗的可能性。例如，组织能够要求公司内的两个人(例如首席财务官和首席执行官)来批准关键业务决策。此外，配置某些特权活动以便需要两个管理员来共同完成一个任务。

分解知识结合职责分离和双人控制概念到单个解决方案中。基本思想是信息或权限需要执行一个操作，该操作在两个或多个用户间被划分。这就确保没有任何个体有充足的特权来危害环境的安全性。

16.1.3　岗位轮换

通过使用岗位轮换来执行进一步控制和限制特权能力。岗位轮换简单来讲就是轮换职责，或者至少某些工作职责被轮换到不同的雇员。使用岗位轮换作为安全控制可以提供并行审查、减少欺骗

并促进交叉培训。交叉培训使得环境很少依赖任何单个个体。

岗位轮换既能作为威慑，也能作为检测机制。如果雇员知道在将来的某些时点，将由其他人担负他们的工作职责，他们最不可能做的就是参与欺诈行为。如果他们依然选择欺骗，担负工作职责的他人很容易发现他们的欺骗行为。

16.1.4 强制休假

许多组织要求雇员在一周或两周以上时间强制休假。这将提供一种并行互审的形式，并且有助于检测欺诈和共谋。该策略确保了其他雇员接替一个人的工作职责至少一个星期的时间。如果一个雇员涉及欺诈，接替该职责的人将会发现其欺诈行为。

这类似于岗位轮换带来的好处。强制休假既能作为威慑，也能作为检测机制，就如岗位轮换策略一样。尽管其他人也就接替一个人的职责一周或两周时间，但这足够来检测到一些违规行为。

注意：

金融组织存在因雇员的欺骗行为导致重大损失的风险。他们常常使用岗位轮换、职责分离和强制休假策略来减少风险。结合这些策略有助于预防事件，也有助于在事件发生时进行检测。

16.1.5 监控特殊的特权

特殊的特权操作是一项需要特殊访问或较高的权限来执行许多管理员和敏感工作任务的活动。这些任务包括创建新用户账户、增加新路由到路由表、修改防火墙配置、访问系统日志和审计文件。使用通用的安全实践，例如最小特权原则，确保数目有限的人才能有这些特殊的特权。监控确保授予这些特权的人不能滥用特权。

有较高特权的账户经常作为特权实体，特权实体能访问特殊的、对普通用户来说不可访问的高级功能。如果误用，这些较高的权限能导致组织资产的机密性、完整性和可用性受损。基于此，监控特权实体及其访问是非常重要的。

在大部分情况下，这些高级特权都仅限于管理员和某些系统操作员。在该环境中，系统操作员是需要额外特权来执行特定工作职能的用户。普通用户(或普通系统操作员)仅仅需要最基本的特权来完成他们的工作。

拥有这些特权角色的雇员常常是可信雇员。然而，存在许多原因会使一个雇员从可信雇员变为心怀不满的雇员或恶意的内部人员。改变可信雇员行为的原因可能和低于预期的奖金、负面的绩效评审或者仅仅因为个人对其他雇员的怨恨一样简单。然而，通过监视特殊特权的使用，组织能够防止雇员滥用特权，并检测可信雇员是否存在滥用行为。

通常，任何类型的管理员账户都有高级特权并应该被监控。也能授予用户较高的特权但不给用户授予所有的管理访问权。按照这个思路，当某个用户有特定的高级特权时，监控用户的行为也是重要的。下面的列表包含某些监控特权操作的例子：

- 访问审计日志
- 改变系统时间
- 配置接口
- 管理用户账户

- 控制系统重启
- 控制通信路径
- 备份并恢复系统
- 运行脚本/任务自动化工具
- 配置安全机制控制
- 使用操作系统控制指令
- 使用数据库恢复工具和日志文件

许多自动化工具能够监视这些特权操作活动，当管理员或特权操作员执行以上这些活动时，该工具能记录日志并发送警告。此外，访问审查审计能检测这些特权的滥用。

注意：

特定的特权监控任务与其他基本原则可以一起协同使用，例如最小特权原则和职责分离。换句话说，最小特权原则和职责分离有助于阻止安全策略的违反活动，且不管是否使用了预防控制，监控活动都有助于阻止并检测任何违规行为的发生。

16.1.6　管理信息生命周期

第 5 章“保护资产的安全”讨论了各种保护数据的方法。当然，不是所有的数据都受到同样级别的保护。然而，组织将给数据分类下定义，并基于分类来确定保护数据的方法。组织定义数据分类，并在安全策略内发布该分类。某些通用的数据分类被政府使用，包括绝密、机密、秘密和未分类。民用分类包含机密(或专有)、私有、敏感和公开。

安全控制保护了整个生命周期内的信息。通用方法包括标记、处理、存储和恰当销毁数据。

标记数据　数据标记(或标签)确保用户能很容易地识别数据的价值。用户应该在创建数据后不久就标记它们。例如，绝密数据的备份应该被标记为绝密。类似地，如果一个系统处理敏感数据，该系统应该使用合理的标签来标记。除了外部系统的标记外，组织经常配置壁纸和屏幕保护来清晰地表明在系统中处理数据的等级。例如，处理机密数据的系统必须有壁纸和屏幕保护，目的是清晰地表明系统在处理机密数据。

处理数据　数据处理主要涉及数据的传输，并且关键是在传输过程中提供与数据存储时相同级别的保护。例如，在数据中心，存储在一台服务器上的敏感数据有许多安全控制来保护它们。在敏感数据存储位置之外时，数据的备份需要得到保护。保护的级别依赖于数据的价值。类似的，传输中的数据(网络上的传输)需要基于数据的价值提供保护。在发送数据之前对其进行加密以提供这种数据保护。

存储数据　数据存储的位置需要得到保护以防止丢失。数据主要存储在磁盘驱动上，并且需要有人去周期性地备份有价值的数据。存储敏感信息的备份位于一个位置，而其拷贝存放在另一个位置。物理安全机制防止这些备份被偷盗。有关环境的安全控制能防止数据由于腐蚀而丢失。

销毁数据　当数据不再需要时销毁数据，且以一种数据不可读的方式来销毁。简单地删除文件不能完全删除数据，而只是标记数据为删除，所以这不是一种删除数据的有效方式。当需要时，技术人员和管理员使用不同种类的工具来移除所有的可读文件元素。常常使用 1 和 0 序列的模式来覆盖文件或磁盘，或者使用其他的方法来粉碎文件。当删除敏感数据时，许多组织需要专人来销毁磁盘，目的是确保数据不可访问。

16.1.7 服务级别协议

服务级别协议(SLA)是组织和外部实体(如供应商)之间的一份协定。SLA 保证对性能的期望被满足，也常常包含如果供应商不能满足这些期望会受到的处罚。

举个例子，许多组织使用基于云的服务来租用服务器。供应商提供对服务器的访问，并对服务器进行维护来确保服务器是可用的。组织能使用 SLA 来确定诸如最大故障时间的可用性。沿着这个思路，公司在与第三方合作时，应该清晰地知道自己的需求，并确保 SLA 中包含这些需求。

除了 SLA 之外，公司常常使用备忘录协议(Memorandum of Understanding，MOU)和/或互联安全协议(Interconnection Security Agreement，ISA)。MOU 记录了两个实体朝着共同目标在一起工作的意图。虽然 MOU 类似于 SLA，但它是非正式的，且不包含对其中某个合作方不负责时的处罚。

如果用双方或多方计划来传输敏感数据，他们能使用ISA来确定连接的技术需求。ISA提供了通信双方如何建立、维持和断开连接的信息。也能使用最小加密方法来确保数据安全。

注意：

NIST 专业出版物 800-47“互联信息技术系统的安全指南”中包括详细的关于 MOU 和 ISA 的信息。

16.1.8 关注人员安全

关注人员安全是安全运营中非常重要的安全因素。代替数据、服务器甚至整个建筑物等物体是有可能的。但对比之下，不可能代替人。顺着这个思路，公司应该实施安全控制来增强人员安全。

举个例子，考虑在数据中心的安全出口用电子加密锁来控制。如果火灾导致电力故障，安全门会自动解锁还是继续维持锁住状态？公司认为服务器机房中的资产价值比人员安全价值高，所以决定保持安全门处于锁住状态。这保护了数据中心的物理资产。然而，也在冒着危及房间内人员生命安全的风险，因为人们不容易逃出房间。对比之下，当没电时，因为公司认为人员安全价值比服务器机房中的资产价值高，所以决定保持安全门处于解锁状态。

当人员单独工作时胁迫系统是有用的。例如，下班后的单名保安还在守护着大楼。如果一群人破门而入大楼，保安可能无法独自阻止他们。然而，保安能使用胁迫系统报警。简单的胁迫系统仅仅需要按一下按钮就能发出求救信号。监控机构收到求救信号后根据常规程序做出响应。监控机构可能给发出求救信号的人打电话或发送一条文本消息。在这个例子中，保安通过确认现状做出响应。

安全系统常常包括密语或人们用来确认一切事物都 OK 的短语，或者验证存在问题。例如，一条代码短语表明一切都 OK，这可能表示“一切都是好的”。如果保安不小心激活了胁迫系统，并且监控机构也做出了响应，保安说“一切都是好的”，然后解释所发生的一切。然而，如果犯罪分子看透保安的意图，就可能会略过该短语并且通过虚构保安是如何意外激活胁迫系统的故事来代替。监控机构将识别保安发过的密语并提供帮助。

另一种安全需要关注雇员出差时的安全问题，因为罪犯最有可能将出差的公司雇员作为他们的袭击对象。对员工进行安全实践培训，可以使得这些员工在旅游时能增加他们的安全性并阻止安全事件的发生。这包含一些较为简单的事情，例如在打开旅馆房门之前检查个人的身份。如果房间的服务包含免费赠送的食物，给前台打个电话确认酒店是否提供了该项服务，以防欺诈。

16.2　提供和管理资源

安全运营知识域的另一个元素是整个生命周期中的资源配置及管理，这包括多种类型的资产，如硬件、软件、物理资产、虚拟资产和基于云的资产。保护数据资产也很重要。第 5 章已深入剖析对数据资产的保护。

16.2.1　管理硬件和软件资产

本书中，硬件指信息技术资源，如计算机、服务器和外设。软件包括操作系统和应用程序。组织经常清点库存以便对软硬件进行跟踪。

1. 硬件清单

贯穿设备的整个生命周期，许多组织使用数据库和库存应用程序来清点库存和跟踪硬件资产。例如，条形码系统可以打印条形码并放置在设备上。条形码数据库中包含硬件的相关细节，如型号、序列号和位置。定期使用条码阅读器对所有条码进行人工扫描来验证组织是否仍对硬件可控。

类似的方法还有使用无线射频识别(RFID)标签，它可以将信息传送到几英里以外的射频识别阅读器。将射频识别标签人工放置在设备上，并使用射频识别阅读器来清点所有的设备。射频识别标签和射频识别阅读器比条形码和条形码阅读器更贵。然而，射频识别方法显著减少了清点库存的时间。

在设备进行处理之前要进行人工净化。清除设备中的所有数据，以确保未授权的人员不会访问到敏感信息。生命周期即将结束时，设备中的数据很容易丢失，所以使用清单来净化系统往往是有价值的。检查表可清理硬盘、非易失性存储器和可移动介质，如系统中的 CD、DVD 和 USB。

保存敏感数据的便携式介质设备也被视为一种资源。例如，组织可以在便携式介质设备上使用条形码标签，并使用条形码库存系统定期完成库存清点。这使他们能够对含有敏感数据的介质设备进行定期盘点。

2. 软件许可

组织购买软件，并经常使用许可证密钥来激活软件。激活过程通常需要在互联网上连接一台许可证服务器，以防止盗版。如果许可证密钥泄露，该服务器能够使密钥失效。

例如，一个组织购买了可以安装 5 个软件产品的许可证密钥，但只立即安装并激活了一个。如果该密钥被盗，被安装在其他组织的 4 个系统上并成功激活。当该组织尝试在内部系统上安装时，激活就会失败。因此，对于组织来说任何类型的许可证密钥都是非常重要的，需要加以保护。

软件许可也能够确保系统没有未授权的软件被安装。许多工具都可用来对系统进行远程监控以便检测到系统的详细数据。例如，微软的系统中心配置管理器(ConfigMgr)是一款服务器产品，可监控每个系统。ConfigMgr 具有广泛的功能，包括识别安装的操作系统和应用程序。这使得它能够识别系统中运行的未授权软件，并帮助组织确保符合软件许可规则。

注意：

ConfigMgr 等工具需要定期扩充功能。例如，ConfigMgr 现在已具有连接到移动设备的能力，包括那些运行 Windows 操作系统、苹果 iOS 和 Android 操作系统的设备。除了识别操作系统和应用程

序外，还可以根据预定义的要求，确保客户设备状态良好，如运行防病毒软件或具有特定的安全设置的配置功能。

16.2.2 保护物理资产

物理资产在 IT 硬件之外，包括所有的物理设施，如组织的办公建筑及其内部设施。保护物理资产的方法包括栅栏、路障、门锁、安保、闭路电视(CCTV)系统等。

组织在规划布局时，通常把敏感的物理资产定位到建筑物的中心。这就使得组织能够实施逐步加强的物理安全控制。例如，组织会把装有多个服务器的数据中心定位在更靠近建筑物中心的房间。如果数据中心坐落在靠近外墙的位置，攻击者可能驾驶卡车穿过墙壁并窃取服务器。

类似的，任何人可以经常进入建筑物的公共入口。但是附加的物理安全控制限制对内部工作区域的进出。密码锁、陷阱、安全徽章和保安是用来控制进出的常用方法。

16.2.3 管理虚拟资产

为了大幅度节约成本，组织逐步使用越来越多的虚拟化技术。例如，组织可以将 100 台物理服务器减少到 10 台，托管 100 台虚拟服务器。这降低了供暖、通风、空调、电力和整体运营成本。

虚拟化不仅仅针对服务器。软件定义一切(SDx)是指以软件代替硬件的虚拟化趋势。在此概念下的虚拟资产包括：

虚拟机(VM) 虚拟机类似于物理服务器上的客户操作系统。物理服务器具有计算能力、内存和磁盘存储能力，能够满足虚拟机的需求。

软件定义网络(SDN) SDN能够将控制平面从数据平面(或转发平面)中分离出来。控制平面使用协议来决定向哪里发送信息，而载有规则的数据平面决定是否转发信息。不同于传统的网络设备，如路由器和交换机，SDN控制器使用能够接收控制器指令的简单网络设备。这消除了一些与传统的网络协议相关的复杂性。

虚拟存储区域网络(VSAN) SAN是含有多个存储设备的专用高速网络。它们经常与需要高速访问数据的服务器一起使用。很久以来，由于复杂的硬件要求，SAN的价格居高不下。VSAN通过虚拟化绕过了这些复杂性。

虚拟化中的主要软件组件是管理程序。虚拟机管理程序管理虚拟机、虚拟数据存储和虚拟网络组件。作为物理服务器上附加的一个软件层，它也是另外的一个攻击面。如果攻击者能够破解物理机，那么就可以访问托管在物理服务器上的所有虚拟系统。管理员往往格外小心，以确保虚拟主机不被侵入。

虽然虚拟化可以简化许多 IT 概念，但我们仍要牢记：许多相同的安全基本要求仍然适用。例如，每个虚拟机仍然需要单独更新。更新主机系统不能更新虚拟机。此外，组织应保留虚拟资产的备份。许多虚拟化工具都具有内置的工具来创建虚拟系统的完整备份，并创建定期快照，以便及时进行较为方便的数据恢复。

16.2.4 管理基于云的资产

基于云的资产包括组织使用云计算访问的任何资源。云计算是指几乎可从任何地方提供按需访

问的计算资源，且云计算资源高度可用、易于扩展。组织通常从其他组织租用基于云的资源，但也可在组织内部管理云资源。其中面临的一个主要的挑战是，这些资源是在组织的直接控制之外，这使得组织更难以管理风险。

一些基于云的服务只提供数据存储和访问。当在云中存储数据时，组织必须确保安全控制能防止未授权的数据访问。此外，组织应正式定义存储和处理存储在云中的数据的要求。举一个例子，在对计算资产的使用进行评估时，美国国防部的云计算安全要求指南为美国政府机构定义了特定要求。这个文档为资产定义了计算需求，用 6 个独立的信息影响级别标记了机密及其以下级别。

根据服务模式，可分为不同程度的资产责任。其中包括维护资产，以确保它们维持功能，并保持系统和应用程序更新补丁。在某些情况下，云服务提供商(CSP)对这些步骤负责。在其他情况下，由消费者负责。

软件即服务(SaaS)　SaaS模型经常通过Web浏览器提供全功能的应用程序。例如，谷歌的Gmail是一个 SaaS 应用。CSP 负责所有 SaaS 服务的维护。消费者不管理或控制任何基于云的资产。

平台即服务(PaaS)　PaaS 模型为消费者提供了一个计算平台，包括硬件、操作系统和应用程序。在某些情况下，用户通过 CSP 提供的清单安装应用。消费者管理他们的应用程序，并可以在主机上设置一些配置。然而，CSP 负责主机和底层的云基础设施的维护。

基础设施即服务(IaaS)　IaaS 模型为消费者提供基本的计算资源，这包括服务器、存储和某些情况下的网络资源。消费者安装操作系统和应用程序，并执行所有必要的操作系统和应用程序的维护。CSP 维护基于云的基础设施，确保消费者获得租赁系统。当对公共服务进行评估时，IaaS 和 PaaS 模式之间的区别并不是很清晰。然而，当租赁基于云的服务时，理解 CSP 使用的标签，没有理解执行不同维护和安全措施的负责人所使用的标签那么重要。

提示：

NIST SP 800-145 “NIST 云计算的定义” 提供了许多云服务的标准定义，包括服务模型(SaaS、PaaS、IaaS)的定义和部署模型的定义(公共、私人、社区和混合)。NIST SP 800-144 “公共云计算中的安全和隐私原则” 提供了与云计算相关的更深层次、更细致的安全问题。

云部署模型也影响云计算资产的责任。4 种可用的云模型分别为公共型、私有型、混合型、社区型。

- 公共云模型包括可用于任何消费者租用的资产并由外部 CSP 管理。服务水平协议可以有效地保证 CSP 提供组织可接受水平的云服务。
- 私有云部署模型包括组织的基于云计算的资产。组织可以使用自己的资源创建和管理私有云。组织负责所有维护工作。然而，组织也可以从第三方租赁资源并按照服务模型(SaaS、PaaS 或 IaaS)分割维护要求。
- 社区云部署模型为两个或多个组织提供云基础资产。维护责任根据对资产和服务模型的管理来分配。
- 混合云部署模型包括两个或两个以上的云组合。类似于社区云部署模型，基于对资产和服务模型的管理，维护责任共享。

16.2.5　介质管理

介质管理是指采取措施保护介质和存储在介质上的数据。本书中，介质是指可以保存数据的任

何事物，包括磁带、CD 和 DVD 光盘、便携式 USB 或 FireWire 驱动器、外部 SATA(eSATA)驱动器、内部硬盘、固态硬盘、USB 闪存驱动器。许多便携式设备，如智能手机，包括存储卡，因为可以容纳数据，故它们也属于这一类。介质还包括任何类型的硬拷贝数据。磁带常用于备份，所以介质管理直接涉及磁带。然而，介质管理的扩展范围则超出了备份磁带，可延伸到任何类型的可保存数据的介质。

当介质设备包含敏感信息时，信息应被存储在安全的位置，加以严格的访问控制，以防止由于未经授权的访问造成损失。此外，用于存储介质设备的任何位置都应该有温度和湿度控制，以防止因腐蚀而引起的损失。

介质管理还可以包括使用技术控制来限制来自于计算机系统的设备访问。例如，由 USB 驱动器引发的风险。许多组织使用技术控制来阻止他们使用并且/或在用户使用时进行检测和记录。在某些情况下，通过书面安全策略禁止 USB 闪存驱动器的使用，并使用自动检测方法检测，如有违反行为立刻报告。

注意：

USB 闪存驱动器的主要风险是感染恶意软件和窃取数据。当用户插入 USB 驱动器时，感染病毒的操作系统可以检测并感染该 USB 驱动器。当用户将这个被感染的 USB 驱动器插入到另一个系统中时，恶意软件将试图感染第二个系统。此外，恶意用户可以很容易地复制和传输大量的数据，并把驱动器隐藏在他们的口袋中。

正确管理介质可保持信息的机密性、完整性和可用性。正确标记、处理、存储介质信息能够防止未经授权的披露(保密性的缺失)、未经授权的修改(完整性的缺失)和未经授权的破坏(可用性的缺失)。

闪存驱动器控制

许多组织将 USB 闪存驱动器限制在组织提供和购买的特定品牌范围内。这使得组织能够对 USB 闪存驱动器上的数据进行保护，并确保驱动器不被用来在系统之间传输恶意软件。使用 USB 闪存驱动器对于用户来说仍有益处，此方法在不妨碍用户使用的同时降低了组织的风险。

例如，Imation 销售的 IronKey 闪存驱动器内置了多个保护级别。应用多种认证机制以确保只有授权用户可以访问驱动器上的数据，并且内置 AES 256 位硬件加密设备来保护数据。闪存驱动器的主动反恶意软件有助于防止恶意软件感染驱动器。IronKey 企业版中含有“银弹”服务，用来保护丢失或被盗的数据设备。这项服务可以远程拒绝所有的数据访问、禁用或启动自毁程序摧毁该设备。“自毁”也许能使我们联想到科幻电影中的一次大爆炸的场景。然而，IronKey 自毁功能不会引起爆炸，而是毁坏设备中的所有数据和设置。

1. 磁带介质设备

组织通常将备份存储在磁带上，但磁带常因腐蚀而很容易损坏。最佳的方法就是保存至少两份备份。一份保存在外部，必要时立即使用。另一份保存在安全的位置。如果发生灾难性的破坏，如火灾破坏了主要备份，仍可用备用备份找到数据。

存储区的清洁度将直接影响磁带介质设备的寿命和实用性。此外，磁场就像消磁器，能够擦除或损坏磁带上的数据。所以，磁带不应暴露于磁场中，如电梯电机、打印机和旧的 CRT 显示器都有磁场。这里是管理磁带介质设备的一些指南：

- 为防止新介质设备沾染灰尘和污垢，应保持它们在原始密封包装中直到使用。
- 打开介质设备包装时要格外谨慎，不以任何方式损害介质设备，这包括使其避免尖锐物体且不扭曲或弯曲介质设备。
- 避免将介质设备暴露于极端温度；不可将其靠近加热器、散热器、空调或其他极端温度源存储。
- 不使用已损坏或暴露在灰尘、污垢中及摔落的介质设备。
- 介质设备应在装有温度控制的车辆中运送。
- 介质设备应避免暴露于外界环境；避免阳光、水分、潮湿、过热、过冷。
- 介质设备应适应 24 小时后再使用。
- 从备份设备的出发点运输到安全的异地存储位置的整个过程应采取适当的安全措施。介质设备在运输过程中的任何一点都容易受到损坏或盗取。
- 基于对介质设备的分类水平标准，应在其整个生命周期采取适当的安全措施。

2. 移动设备

移动设备包括智能手机和平板电脑。这些设备有内部存储器或可移动存储卡，可以容纳大量的数据。数据可以包括含有附件的电子邮件、联系人和计划信息。此外，许多设备都安装了允许用户读取和处理不同类型文档的应用程序。

组织经常为员工购买智能手机，并保存其中的数据。这对于员工来说当然是很好的福利，但也给组织提供了对员工手机以及其所含数据的更多控制。组织常用的控制手段包括手机加密、屏幕锁、全球定位系统(GPRS)和远程擦除。加密能够在手机丢失或被盗时保护数据，屏幕锁可能会拖住偷手机的人，全球定位系统提供手机丢失或被盗后的位置信息。如果手机丢失，远程擦除信号将被发送到丢失的设备，以删除设备上的部分或所有数据。当远程擦除成功时，许多设备会回复一条确认消息。

提示：

远程擦除并不对保护提供完全保证。想要从商务智能手机中偷取数据的人都掌握一定的相关知识，他们会立即移除手机中的用户身份卡(SIM)。此外，当把卡放回手机以获取数据时，他们会使用类似于法拉第笼的屏蔽室。这些技术阻碍了远程擦除信号。如果没有收到远程擦除已成功的短信回复，那么很可能数据已经泄露。

组织有时允许员工使用他们的个人设备，并将它们连接到单位的网络。这也会引发不同的问题。例如，如果是员工的设备，组织应该做些什么才能确保设备保持在安全的状态并且里面存储的数据是受保护的？为了应对这一挑战，组织通常把自带设备(BYOD)策略列入安全策略。BYOD 策略为那些想要将个人设备连入组织网络的员工界定了责任和权利。

16.2.6　管理介质的生命周期

所有介质设备的生命周期对我们都很有帮助，但其生命周期也是有限的。所有介质设备都有平均故障时间，这个时间能够告诉你该设备可使用的次数或年限。例如，一些磁带会有特殊的规格，提示我们该磁带可重复使用 250 次或在理想条件下能保存 30 年。然而，许多因素会影响介质的寿命并会减少预计使用次数。监控备份错误很重要，可以使用它们作为指导来衡量在该环境中介质设备

的生命周期。当磁带开始产生错误时，技术人员应停止使用。

一旦备份介质设备已达到其寿命，就要进行销毁。磁带上数据的分类将决定销毁方法。当磁带达到生命周期时，一些组织会将其消磁，然后存储直到销毁。常用破碎机或焚烧炉销毁磁带。

第 5 章讨论了固态硬盘(SSD)的一些安全问题。具体来说，消磁不能清除 SSD 中的数据，内置擦除命令也不能完全清除数据。许多组织直接销毁 SSD 而不是仅将里面内容清除。

注意：

平均无故障时间(MTTF)不同于平均故障间隔时间(MTBF)。平均无故障时间一般是计算一旦失败就无法修复的时间，比如磁带。相比之下，平均故障间隔时间指故障后直到人员修复好的时间间隔，比如计算机服务器。

16.3 配置管理

配置管理有助于确保系统处于一致安全的状态，并在其整个生命周期维护这种状态。配置管理使用的一种方法是基线。

16.3.1 基线

基线是一个起点。在配置管理中，它是一个系统的启动配置。管理员为了满足不同需求，经常在完成系统部署之后修改基线。然而，当系统被部署在有安全基线的状态下时，系统会更安全。这尤其适用于组织具备有效的执行变更管理计划时。

基线可与检查列表同时产生，但需要人工确认系统以特定的方式或配置部署。然而，手动基线常有人为错误。人很容易遗漏下一个步骤或者错误配置系统。脚本和操作系统工具也被用来实现基线，使用自动方法能够减少手动基线的潜在错误。例如，微软操作系统包括组策略。管理员可以单次配置一个组策略，之后组策略会自动将设置应用到域中的所有计算机。

16.3.2 用镜像创建基线

许多组织使用镜像来创建基线。图 16.2 显示了在一个整体的三步过程中创建和部署基线镜像的过程。这个步骤是：

注意：

在实践中，整个过程中会涉及更多的细节，这取决于使用镜像的工具。例如使用赛门铁克 Norton Ghost 来捕获和部署镜像的步骤，不同于使用微软的部署服务(WDS)的步骤。

(1) 管理员最开始在计算机上安装操作系统和所有所需的应用程序(如图16.2中标记的基线系统)。然后，管理员对系统进行相关的安全配置和其他设置以满足组织的需求。在继续下一步之前，将进行人工测验来确保系统正常运行。

(2) 接着，管理员使用镜像制作软件捕获系统的镜像，并将其存储在图 16.2 所示的服务器上(标记为镜像服务器)。人们经常将镜像存储在外部的硬件设备、USB 驱动器或 DVD 上。

(3) 然后，根据需要，手动将镜像部署到系统中。这些系统通常需要额外的配置来完成，比如给它们取独特的名字。然而，这些系统的整体配置同基线系统是相同的。

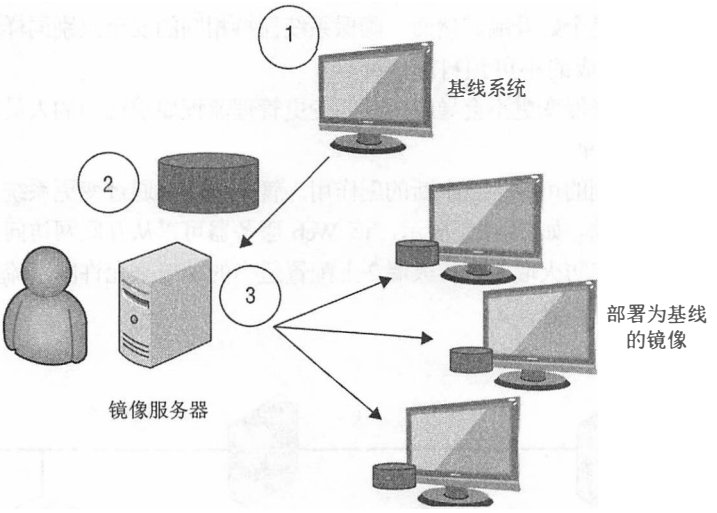


图 16.2　创建和部署镜像

通过确保所需的安全设置始终正确配置，基线镜像提高了系统的安全性。此外，它们减少了部署和维护系统所需的时间，从而降低了整体维护成本。预置镜像的部署只需要花费技术员几分钟的时间。此外，当用户的系统损坏时，技术人员可以在几分钟内重新部署镜像，而不是用几个小时来排除系统故障或试图重建。

在基线中将镜像和其他自动化方法结合起来很常见。换句话说，管理员可以在组织内为所有台式计算机创建镜像。然后使用自动化的方法来添加额外的应用程序、功能或设置(针对特定的计算机组)。例如，通过脚本或其他自动化工具，一个部门的计算机可以安装额外的安全设置或应用程序。

真实场景

用在美国政府中的基线镜像

美国政府认为很多安全问题是由 Windows 系统配置错误引发的。许多 IT 专业人员知道核心安全设置来保护系统，但往往部署系统的人员没有这方面的知识。技术人员部署的系统常常很脆弱，导致安全事件的发生。这些事件都是专业人员所了解且可以预防的。

对此，美国空军和微软合作，创建标准化的镜像作为他们系统的基线。后来，一些政府机构再次与微软合作，创建标准化的镜像作为所有政府机构系统的基线。美国政府配置基线(USGCB)现在包括几个不同的操作系统镜像。

目前，管理和预算办公室(OMB)要求在所有通用的基于 Windows 系统的电脑上使用这种镜像，如用于政府机构的台式机和笔记本电脑。美国国家标准与技术研究所(NIST)维护和更新所需的镜像。如下网站提供了更多细节信息：http://usgcb.nist.gov/。

16.4 变更管理

部署系统处于安全状态是个好开端。然而，确保系统保持相同的安全级别同样重要。变更管理有助于减少由未授权变更造成的不可预料的中断。

变更管理的主要目标是确保变更不会导致中断。变更管理流程要求适当的人员在实施变更前审查和批准变更，并做详细记录。

变更往往会产生意想不到的可能导致中断的副作用。管理员可以通过变更系统来解决问题，但会在其他系统中产生未知问题。如图 16.3 所示，该 Web 服务器可以从互联网访问，并可访问内部网络上的数据库。管理员已在防火墙 1 和防火墙 2 上配置适当的端口来允许网络流量通过，进而允许 Web 服务器访问数据库服务器。

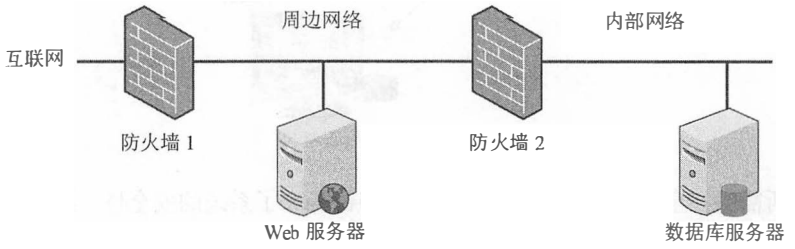


图 16.3 Web 服务器和数据库服务器

有能力的防火墙管理员可能会在防火墙 2 上看到一个无法识别的开放端口，并出于安全考虑决定将其关闭。遗憾的是，Web 服务器需要此端口打开来与数据库服务器进行通信，所以当端口被关闭时，Web 服务器将出现问题。很快，帮助台如洪水般的请求打开，人们开始修复服务器。他们向 Web 服务器的程序员寻求帮助，并在一些故障排除后，开发人员意识到数据库服务器无响应。然后，他们呼叫数据库管理员来对数据库服务器进行故障排除。在一阵大喊大叫、指责和责骂后，有人意识到防火墙 2 的一个需要开放的端口被关闭了。他们打开端口并解决了这个问题。至少直到这个端口被再次关闭或者有人开始研究防火墙 1 之前，这个问题解决了。

提示：

组织不断寻求安全性和易用性之间的最佳平衡。有实例证明，组织会做出这样的决定：想要通过削弱系统的安全性来提高性能。然而，变更管理有助于确保组织花时间评估削弱安全性带来的风险，并与由此增加的易用性回报进行比较。

未授权的变更直接影响到 CIA 三要素中的可用性。然而，变更管理过程给不同的 IT 专家提供了机会，让他们在技术人员做出变更之前审查意料之外的副作用的变化。同时，它们给了管理员时间，在生产环境变化之前检查其工作是否在可控范围内。

此外，一些变更可能会削弱安全性。例如，如果组织没有使用有效的访问控制机制来授予用户访问权限，管理员可能会无法跟上额外的访问请求。技术差的管理员可能会决定将一组用户添加到网络的管理员组中。用户将拥有他们需要的所有访问权，并且他们的网络使用能力提高了，不用再向管理员提出访问请求。然而，以这种方式授予管理员访问权直接违反了最小特权原则，并明显削弱了安全性。

注意：

如今使用的许多配置和变更管理概念已经不同于最初发表的英国信息技术基础架构库(ITIL)。ITIL 的核心包括 5 个出版物，阐述了系统的整个生命周期。ITIL 作为整体定义了组织确定可以采取的用于提高整体可用性的最佳实践，并且出版物 Service Transition 说明了配置管理和变更管理流程。虽然许多概念来自 ITIL，但组织不需要采用 ITIL 来实施变更和配置管理。

16.4.1　安全影响分析

变更管理过程确保人员可以进行安全影响分析。在生产环境中，专家对变更进行评估并识别安全影响之后，工作人员才开始实施变更。

变更管理控制提供一个过程来控制、文档化、跟踪和审计所有系统的变化。其中包括系统任何一方面的变更，包括硬件和软件配置。组织在任何系统的生命周期中都能够实现变更管理过程。

变更管理过程中的常见任务如下：

1) 请求变更。一旦所需变更确定下来，工作人员就会请求变更。一些组织使用内部网站，允许员工通过网页提交变更请求。内部网站自动记录数据库中的请求，并允许工作人员跟踪更改。任何人都可查看更改请求的状态。

2) 审查变更。单位内的专家会审查变更。审查变更的人员通常来自同一单位的不同领域。在某些情况下，他们可能会很快完成审查并决定批准或拒绝变更。在其他情况下，通过广泛的测试之后，变更可能需要正式的变更审查委员会批准。

3) 批准/拒绝变更。在审查的基础上，这些专家随后批准或拒绝变更。他们还记录了变更管理文档的响应。例如，如果组织使用内部网站，有人会在网站的数据库中记录结果。在某些情况下，变更审查委员会可能需要创建回滚或退出计划。这将确保如果变更失败，管理人员可以将系统还原。

4) 计划和实施变更。变更是有时间计划的，以确保变更对系统及用户产生的影响能够降到最小。这可能需要将变更时间调整到下班时间或非高峰期。

5) 记录变更。最后一步是记录变更以确保所有相关人员熟悉变更。这往往需要改变配置管理文档。如果不相关的灾难需要管理员重建系统，变更管理文档为他们提供相关信息。这确保他们可以还原系统。

有一些需要紧急变更的情况。例如，如果攻击或恶意软件感染了一个或多个系统，管理员可能需要做出变更来处理该事件。在这种情况下，管理员仍然需要记录变更。这确保变更审查委员会可以观察潜在问题的变化。此外，记录的紧急情况下的变更也可确保系统在需要重建时有最新配置。

在执行变更管理的过程中，将为系统的所有变更创建文档。如果技术人员需要修改变更，这就为其提供了相关信息。如果人员需要在其他系统上实现相同的变更，文档还提供了一个流程图以供遵循。

在 ISO 通用标准中变更管理控制对于一些安全保证要求是强制性元素。然而，在许多组织中实现变更管理控制都不需要符合 ISO 标准。它提高了环境的安全性，预防了因未授权的变更而导致的损失。

16.4.2　版本控制

版本控制通常是指软件配置管理中使用的版本控制。标签或编号系统将多台机器上或处于不同

时间点的软件集与配置在一台机器上区分出来。例如，应用程序的第一个版本可能被标记为 1.0。第一次小更新将被标记为 1.1，第一个主要的更新将被标记为 2.0。这有助于随着时间的推移跟踪变更。

虽然大多数软件开发商都意识到对应用程序版本进行识别与控制的重要性，但许多新的 Web 开发人员没有认识到这一点。这些 Web 开发者已经掌握了能够创建优秀网站的技能，但他们总是意识不到一些基本原则，比如版本控制的重要性。如果他们不能通过某种类型的版本控制系统来控制变更，就可能引发由于变更导致的网站瘫痪。

16.4.3 配置文档

配置文档确定当前系统的配置。它定义了系统负责人及系统目标，并且列出了所有应用于基线的变更。几年之前，许多组织使用简单的纸笔记本记录这些服务器信息，但如今，将这些信息存储在文件或数据库中更常见。当然，将信息存储在数据队列中面临的一个问题就是断电时没办法获得信息。

16.5 补丁管理和减少漏洞

补丁管理和漏洞管理同时用于保护企业的系统免受威胁。在操作系统和应用程序中经常发现错误和安全漏洞。一经发现，供应商就会编写和测试补丁去消除该漏洞。补丁管理能够确保应用适当的补丁，并且漏洞管理有助于验证系统免受已知威胁的干扰。

16.5.1 补丁管理

补丁是用于任何类型代码编写的笼统术语，写补丁能够纠正错误或修复漏洞，或提高现有软件的性能。软件可以是操作系统或应用程序。补丁有时被称为更新、快速修复或热修复。在系统安全的状态下，管理员主要关心的是安全补丁，这是影响系统漏洞的补丁。服务包是补丁的集合，携带着系统当前最新的补丁。

即使供应商经常发布补丁，这些补丁也只有在被应用时才是有用的。这个道理显而易见，但是仍然会发生很多安全事件，这是由于很多组织并不执行补丁管理策略。有效的补丁管理程序能够确保系统安装当前最新的补丁。如下是有效补丁管理程序中共同的步骤：

评估补丁：当供应商发布补丁后，管理员会进行评估，以确定补丁适用于他们的系统。例如，用于修复配置了 DNS 服务器的 Unix 系统漏洞的补丁，经评估不适用于配置了 DNS 服务器的 Windows 系统。类似地，如果 Windows 系统中的某个功能被禁用，则用于修补该功能的补丁也同样不需要了。

测试补丁：管理员随时都要测试单一系统的补丁，以确定该补丁不会带来其他副作用。最糟糕的情况就是，当使用补丁后，系统无法启动。例如，修补程序经常会引起系统开始无休止的重新启动周期。它们引发一个停止错误，并重复尝试重新启动后从错误中恢复。如果在单一系统上进行测试，那么只影响一个系统。然而，如果组织将未测试的补丁程序应用到一千台计算机上，就可能会有灾难性的结果。

注意：

较小的组织往往不会自行评估、测试和批准补丁，而是采用一种自动化的方法来应用补丁。Windows 系统包括 Windows 更新，这使得自动更新补丁变得简单。然而，更大的组织通常选择自己控制整个过程，以防止更新过程的意外中断。

批准补丁：管理员测试补丁并确定其安全性后，就会批准补丁的部署。批准程序中常用到变更管理过程(在本章前面叙述过)。

部署补丁：经过测试和批准，管理员部署补丁。许多组织使用自动化的方法部署补丁。自动化方法可以是第三方产品或由软件供应商提供。

确认补丁已部署：部署补丁后，管理员定期测试和审计系统，以确保系统补丁仍然有效。许多部署工具都有审计系统的功能。此外，许多漏洞评估工具也具有检查系统的功能，以确保随时有合适的补丁。

补丁星期二和漏洞星期三

微软经常在每月的第二个星期二发布补丁，通常被称为补丁星期二。固定的时间能够帮助管理员做计划，以便他们有足够的时间去测试和部署补丁。许多与微软有合作的组织在星期二发布补丁之前收到补丁版本通知。一些补丁很重要，微软会有“例外”。换句话说，微软会提早发布补丁，而不是等到下个星期二。

攻击者发现很多组织并没有立即修补补丁。一些攻击者会逆向补丁，用来确定有潜在的漏洞，然后使用某些方法来利用漏洞。这些攻击者一般会在星期二发布补丁之后的一天之内完成动作，所以就有了词组“漏洞星期三”。

然而，许多攻击者都是在厂商发布补丁之后的几周、几月甚至几年之后才破解未安装补丁的系统。换句话说，许多系统仍然没有安装补丁，攻击者也是在供应商发布补丁之后超过一天的时间之后才破解补丁。例如，微软在 2008 年 10 月份发布了一个修补名为 Conficker 的漏洞的补丁。Conficker 含有许多恶意功能，是很大的威胁。然而，到 2011 年，在全球范围内，仍有 180 多万台电脑感染了 Conficker，这意味着至少这些计算机都没有更新补丁以修补漏洞。

16.5.2　漏洞管理

漏洞管理是指定期检测漏洞，评估并采取相应措施来减少相关风险。但消除风险是不可能的。同样，也不可能消除漏洞。然而，有效的漏洞管理程序能够帮助组织定期检测评估漏洞，并及时修补高危漏洞。漏洞管理程序的两个常见要素是例行漏洞扫描和定期脆弱性评估。

注意：

组织中未安装补丁的系统最容易出现漏洞，所以一般漏洞管理程序会同补丁管理程序分工协作。通常情况下，两个程序由不同的人员负责。一人或一组人负责确定补丁的更新，而另一人或另一组人负责确定漏洞已经被修补。责任分离确定了检查方法并保证组织内部的平衡。

16.5.3　漏洞扫描

漏洞扫描器是用来测试系统和网络有无已知安全问题的软件工具。攻击者利用漏洞扫描器来检

测系统和网络中的漏洞，如补丁丢失或密码等级较弱。当他们发现弱点时，就会发动攻击并利用这些漏洞。许多组织中的管理员使用相同类型的漏洞扫描器来检测他们网络中的漏洞。他们的目标是检测漏洞，并在被攻击之前修补漏洞。

正如防病毒软件使用特征文件来检测已知病毒，漏洞扫描器有个已知安全问题的数据库，并能够根据数据库检测系统。供应商定期更新这个数据库，并向订购的用户出售。如果管理员不定期更新漏洞扫描器，他们将无法检测到新的威胁。这类似于如果防病毒软件不知道最新型的病毒，就不能检测到该病毒。

Nessus 是 Tenable 网络安全公司管理的一款非常受欢迎的漏洞扫描器，它结合多种技术来检测各种各样的漏洞。Nessus 能够分析由系统发送出的数据包，以检测其操作系统和关于系统的其他细节。它使用端口扫描来检测打开的端口，并识别可能在这些系统上运行的服务和协议。一旦 Nessus 发现系统的基本细节，它接下来就会跟踪查询检测系统中已知的漏洞，例如系统的补丁是否是最新的。它还可以发现网络中使用 IP 探针和 ping 扫描的潜在恶意系统。

认识到漏洞扫描器不仅用来检查未打补丁的系统是很重要的。例如，如果系统正在运行数据库服务器应用程序，它可以检查该数据库默认账户的默认密码。同样，如果系统是托管的网站，它可以检查网站是否使用输入验证技术来防止不同类型的注入攻击，如 SQL 注入和跨站脚本。

在一些大的组织中，会有专业安全团队使用扫描工具进行定期的漏洞扫描。在较小的组织中，IT 或安全管理委员会把扫描工作当成兼职来完成。但需要谨记一件事情：如果负责部署补丁的人也负责运行扫描和检查补丁，将会产生潜在冲突。如果管理员因一些事情不能部署补丁，管理员也会直接跳过检测未打补丁系统的扫描步骤。

扫描器能够生成详细说明被其发现的系统漏洞情况的报告。报告可能会建议应用补丁或进行特定的配置，或进行安全设置变更，以改善安全性。显然，只是推荐使用补丁并不能减少漏洞的存在。管理员需要完成很多个步骤才能将补丁应用成功。

然而，可能会有补丁不可行或不满足的情况发生。例如，如果补丁在修复一个小的安全问题时中断了系统中的一个应用，管理程序可以决定在开发人员创建工作区之前停止该补丁的修复工作。即使组织已经处理了风险，漏洞扫描器也会定期报告漏洞。

注意：

相对于减少风险，管理层可以选择接受风险。施加控制后仍然存在的任何风险都是剩余风险。剩余风险产生的任何损失都是管理层的责任。

相比之下，从未执行漏洞扫描的组织可能会有许多漏洞。此外，这些漏洞将保持未知状态，且管理层也没有机会决定缓解哪个漏洞或接受哪个漏洞。

16.5.4 漏洞评估

漏洞评估通常包含漏洞扫描结果，但真正的评估将涵盖更多的东西。例如，每年的漏洞评估可能会分析过去一年中的所有漏洞扫描报告，以确定组织是否正在修复漏洞。如果在每一份漏洞扫描报告上都有相同的漏洞，我们脑海中就会自然而然产生一个问题，为什么这个漏洞没有被修复？能接受的原因有：可能管理层选择接受漏洞，或是一直有对漏洞的扫描，但没有对漏洞采取修复措施。

漏洞评估往往是风险分析或风险评估的一部分，以确定某个时间点的漏洞。此外，漏洞评估还检测其他领域，以确定风险。例如，漏洞评估通过检测敏感信息在整个生命周期中如何被标记、处

理、存储和销毁，来解决潜在风险。

提示：

术语漏洞评估有时被用来表示风险评估。在这种情况下，漏洞评估将包括与风险评估相同的元素。这在第 2 章“人员安全和风险管理概念”中有所描述。其中包括确定资产的价值，确定漏洞和威胁，并进行风险分析，以确定整体风险。

第 15 章“安全评估和测试”中包括渗透测试。许多渗透测试以漏洞评估开始。此外，许多渗透测试人员将社会工程学作为他们整体测试的一部分。

16.5.5　常见漏洞和披露

根据通用漏洞披露(CVE)列表来看，漏洞很常见。CVE 列表提供了一个标准的公约，用来找出漏洞。MITRE 维护 CVE 漏洞库，可以单击网址 www.cve.mitre.org 来查看。

提示：

MITRE 看起来像缩写，但其实不是，其创始人是美国麻省理工学院(MIT)的研究工程师，这个名字是为了让人们记住创始人作为工程师的那段历史。然而，MITRE 不是麻省理工学院的一部分。MITRE 从美国政府获得资金来维护 CVE 漏洞库。

在 CVE 列表中，补丁管理和漏洞管理程序是标准的漏洞扫描工具。例如，前面我们提到过 Conficker。Conficker 利用没有打补丁的 Windows 系统中的漏洞。微软发布了微软安全公告 MS08-067 并不断更新以修复漏洞。同样的 Conficker 漏洞也被 MITRE 认定为 CVE-2008-4250 或 CVE 兼容产品。

CVE 数据库为组织创建补丁管理和漏洞管理工具提供了方便。他们不必花费任何资源去命名或定义漏洞，而更加专注于研究检查系统漏洞的方法。

16.6　本章小结

一些基本的安全原则是任何环境中安全运营的核心。这些原则包括知其所需、最小特权、职责和责任分离、岗位轮换和强制休假。将它们结合使用，有助于防止安全事故的发生，并限制发生的范围。根据安全原则，管理员和运营者有特殊的特权去完成他们的工作。除了实施原则，监控特权活动以确保特权实体不滥用他们的访问权限也是非常重要的。

介质设备或其他含有数据的资产在其整个生命周期都受保护。介质设备包括任何可以保存数据的设备，例如磁带、内部驱动器、便携式驱动器(USB、FireWire 和 eSATA)、CD 和 DVD、移动设备、存储卡和打印输出设备。带有敏感信息的介质设备会被组织以相应的处理办法标记、处理、存储和销毁。资产管理延伸到组织内部除介质以外的任何资产——物理资产，如计算机和软件资产(如购买的应用程序和软件许可密钥)。

虚拟资产包括虚拟机、软件定义网络(SDN)和虚拟存储区域网络(VSAN)。虚拟机管理程序是管理虚拟组件的主要软件构件，但虚拟机管理程序也增加了额外的攻击面，所以确保它被部署在安全的状态并持续更新补丁显得尤为重要。此外，每个虚拟组件需要单独更新。

基于云的资产包括存储在云中的任何资源。当与云服务提供商谈判时，必须明确谁是维护安全的负责人。一般情况下，云服务提供商作为服务资源提供方承担大部分责任，平台即服务(SaaS)产品提供商承担小部分责任。基础设施即服务(IaaS)产品提供商承担最少的责任。当洽谈云服务时，许多组织使用服务级别协议(SLA)。SLA 保证满足性能预期，并且通常包括供应商不满足这些预期的处罚措施。

变更和配置管理是有助于减少中断的两个额外控制手段。配置管理确保系统部署以一致且安全的方式进行。镜像是一种常见的配置管理技术，能够确保系统以已知基线运行。变更管理有助于减少未授权的更改而导致意外中断，也可以帮助阻止弱化安全性的变更。

补丁和漏洞管理程序同时工作，以保持系统免受已知漏洞的威胁。补丁管理保持系统能够及时更新最新的相关补丁。漏洞管理包括漏洞扫描，以检查各种已知的漏洞(包括未打补丁的系统)，也包括作为风险评估一部分的漏洞评估。

16.7 考试要点

理解知其所需和最小特权原则。知其所需和最小特权原则是在安全网络中实现的两条标准的信息安全保护原则。它们限制访问数据和系统，使用户和其他使用方只访问他们所需的数据。这种有限的访问有助于防止非安全事件的发生，并有助于限制事件发生时的范围。一旦不遵守这些原则，安全事件会给组织带来更大的损失。

理解职责分离和岗位轮换制度。职责分离是一条基本的安全原则，能够确保单人不能完全控制关键的功能或系统的所有元素。随着岗位轮换，员工被轮换到不同的工作岗位或者任务被分配给不同的员工。共谋是一种在多人之间达成的协议，目的是完成一些未授权或非法的行为。通过限制单个人行为来执行这些策略有助于防止没有同谋下的欺诈。

理解监控特权操作的重要性。特权实体应该被信任，但他们也可以滥用特权。正因为如此，才要监控所有的特权分配和特权使用操作。目标是确保值得信赖的员工不滥用他们被授予的特权。

理解信息生命周期。数据在整个生命周期中都需要加以保护。首先要正确地分类和标记数据，还包括适当的处理、存储和销毁数据。

理解服务级别协议。组织与外部实体(如供应商)使用服务级别协议(SLA)。此协议约定了预期值(如最大停机时间)，并且如果供应商未能在预期内完成，协议中还规定了相应的处罚措施。

理解虚拟资产。虚拟资产包括虚拟机、软件定义网络(SDN)和虚拟存储区域网络(VSAN)。虚拟机管理程序是管理虚拟组件的主要软件构件，但虚拟机管理程序也增加了额外的攻击面，所以确保它被部署在安全的状态并持续更新补丁显得尤为重要。此外，每个虚拟组件需要单独更新。

认识云资产的安全问题。云资产包括通过云访问的任何资源。云存储增加了数据的风险，所以需要采取更多的措施保护数据。采取何种措施取决于数据的价值。当租赁云服务时，必须了解哪方负责执行维护和安全措施。在 IaaS 模型中，供应商提供的维护和保障最少。

解释配置和变更控制管理。有效的配置和变更管理程序能够预防许多中断和错误事件的发生。配置管理确保系统的配置相似，系统配置已知且记录在案。基线保证系统的部署处于相同基线或相同起点。镜像是一种常见的基线法。变更管理有助于减少中断或由于未授权变更而引起的安全性削弱。变更管理过程需要变更被请求、批准和记录。版本管理使用标签或编号系统来跟踪变化，更新软件版本。

理解补丁管理。补丁管理确保系统保持当前补丁的最新状态。应该明确，有效的补丁管理程序包括评估、测试、批准和部署补丁几部分。此外，系统审计会验证已批准补丁在系统中的部署情况。补丁管理通常与变更和配置管理交织在一起，以确保文档能真实反映变更情况。如果组织没有有效的补丁管理程序，就会经常遇到由未知问题引发的中断或错误，这些本是可以避免的。

解释漏洞管理。漏洞管理包括常规的漏洞扫描和定期的漏洞评估。漏洞扫描可以检测已知的安全漏洞和弱点，如补丁缺失或弱密码。扫描能够生成关于系统的技术漏洞报告，且对于补丁管理程序是很有效的一种检查方法。漏洞评估不仅仅是技术性扫描，还包括审查和审计以检测漏洞。

16.8　书面实验室

1. 说明知其所需和最小特权原则的区别。
2. 列出用来管理敏感信息的常用方法的名称。
3. 列出三个主要的基于云计算的服务模型，并确定由每个模型的云服务提供商提供的维护水平。
4. 在系统配置中，什么控制用来防止因未授权修改而带来的中断？

16.9　复习题

1. 组织确保用户被授予仅需要执行具体工作任务的数据访问权。它们是以下哪些原则？
   A. 最小特权原则
   B. 职责分离
   C. 知其所需原则
   D. 基于角色的访问控制
2. 管理员正在为数据库授予权限。管理员应该授予新用户什么默认级别？
   A. 读
   B. 修改
   C. 完全访问
   D. 禁止访问
3. 为什么对于安全目标来说职责分离是重要的？
   A. 确保了多个人可以做同样的工作
   B. 当他们失去重要的人时，可以防止组织失去重要的信息
   C. 可以防止任何单个安全人员做出重大安全更改而不涉及其他个人
   D. 可以帮助员工集中他们的聪明才智，他们将是最有用的人
4. 岗位轮换和职责分离策略的主要好处是什么？
   A. 防止合谋
   B. 防止欺诈
   C. 促进合谋
   D. 纠正事件

5. 金融机构通常让员工每半年轮换一次岗位。他们采用了什么安全原则？
   A. 岗位轮换
   B. 职责分离
   C. 强制休假
   D. 最小特权
6. 以下哪一项是组织实施强制性休假制度的主要原因？
   A. 为了轮转工作职责
   B. 为了发现欺诈
   C. 为了提高员工生产力
   D. 为了减轻员工的压力
7. 组织想要减少针对恶意欺诈员工的漏洞。下列哪些选项能达到这个目标？(选择所有适用的)
   A. 岗位轮换
   B. 职责分离
   C. 强制休假
   D. 基线
8. 下列选项中，对于特殊权限什么是不相关的有效安全做法？
   A. 监控特权分配
   B. 授予管理员和操作员同等访问权
   C. 监控特权使用
   D. 只授予受信任员工访问权限
9. 如果供应商不担负规定的责任，以下哪一项确定供应商的责任，包括罚款？
   A. 服务级别协议(SLA)
   B. 签署备忘录(MOU)
   C. 互联安全协议(ISA)
   D. 软件定义服务(SaaS)
10. 在设备生命周期结束且正在捐献给慈善机构时，应该做什么？
   A. 删除所有 CD 和 DVD
   B. 删除所有软件
   C. 净化设备
   D. 安装正版软件
11. 组织正在规划新的将容纳数据中心建筑的布局。数据中心最合适放置在什么地方？
   A. 在大楼中心
   B. 临近进入大楼的电源，靠近外墙位置
   C. 靠近供热、通风和空调系统的位置
   D. 在楼的后面
12. 以下哪一项是关于运行在物理服务器上作为客户机操作系统的虚拟机的正确描述？
   A. 通过更新物理服务器自动更新虚拟机
   B. 通过更新任意 VM 自动更新虚拟机
   C. 虚拟机不用更新，只更新物理机就可以了
   D. 虚拟机必须单独更新

13. 一些基于云计算的服务模型需要组织来执行维护，并担负一些安全责任。以下哪个模型承担组织租用基于云资源的主要职责？

A. 基础设施即服务(IaaS)

B. 平台即服务(PaaS)

C. 软件即服务(SaaS)

D. 云即服务(CaaS)

14. 组织使用的是软件即服务(SaaS)这种基于云的服务来与其他组织共享。这种描述是以下哪种类型的部署模型？

A. 公有

B. 私有

C. 共同

D. 混合

15. 需要对已达到生命周期的备份磁带进行处理。以下哪一项是最合适的处理方法？

A. 把它们扔掉。因为它们的生命周期结束了，所以不可能从它们读出数据

B. 对它们进行处理之前清除磁带上的所有数据

C. 对它们进行处理之前擦除磁带上的数据

D. 把磁带存储在存储设施里

16. 以下哪一项是使用基线的一种有效的配置管理方法？

A. 实施变更管理

B. 使用镜像

C. 实施漏洞管理

D. 实施补丁管理

17. 以下哪个步骤将不包括在变更管理流程中？

A. 如果能提高性能，立即实施变革

B. 请求更改

C. 为变更创建回滚计划

D. 文档变更

18. 在解决网络问题时，技术员意识到该问题能够通过在防火墙上打开一个端口得到解决。技术员打开了端口，并检查了系统的工作状态。然而，网络攻击者访问了这个端口，并发起了一次成功的攻击。怎样才能预防该问题的发生？

A. 补丁管理流程

B. 漏洞管理流程

C. 配置管理流程

D. 变更管理流程

19. 以下哪一项不是补丁管理过程的一部分？

A. 评估补丁

B. 测试补丁

C. 部署所有补丁

D. 审计补丁

20. 管理员会用什么来检查系统，攻击者可以利用系统的已知漏洞？

A. 版本跟踪

B. 漏洞扫描

C. 安全审计

D. 安全审查

第 17 章

事件预防和响应

本章中覆盖的 CISSP 考试大纲包含：

安全运营

- C. 管理日志和监控行为
  - C.1 入侵检测和防御
  - C.2 安全信息和事件管理
  - C.3 持续监控
  - C.4 出口监控(例如，数据防泄露、隐写术、数字水印)
- G. 实施事件管理
  - G.1 检测
  - G.2 响应
  - G.3 缓解
  - G.4 报告
  - G.5 恢复
  - G.6 纠正
  - G.7 经验教训
- H. 操作和维护预防措施
  - H.1 防火墙
  - H.2 入侵检测和防御系统
  - H.3 白名单/黑名单
  - H.4 第三方安全服务
  - H.5 沙箱
  - H.6 蜜罐/蜜网
  - H.7 防恶意软件

CISSP 认证考试的安全运营域包含了与事件管理直接相关的多个目标。有效的事件管理有助于组织在攻击发生时做出适当的响应来限制攻击范围。组织实施预防性措施来对抗、检测和防止攻击，

本章涵盖了许多这方面的控制和对策。日志记录、监视和审计提供了安全控制的保证，并提供了所需要的保护。

17.1 管理事件响应

任何安全程序的主要目标之一是防止安全事件发生。然而，IT和安全专业人员尽了最大努力，事件还是会发生。当它们发生时，组织必须能够响应以限制或遏制安全事件。事件响应的主要目标是尽量减少事件对组织的影响。

17.1.1 事件界定

在进入事件响应之前，重要的是要了解对事件的界定。虽然这看起来很简单，但你会发现根据不同的背景，会有不同的界定。

事件是任何对组织资产的保密性、完整性或可用性有负面影响的事故。IT基础设施库第3版(ITIL v3)定义事件为：“对于 IT 服务来说的、非计划的中断或质量的降低。”这些定义涵盖多种直接攻击形式，例如自然事件，如飓风或地震；以及人为故障，如不小心割断一条在用的网络电缆。

相反，计算机安全事件(有时被称为安全事件)通常是指攻击结果，或指对部分用户来说是恶意或故意行动的结果。例如，RFC 2350“对计算机安全事件响应的预期值”定义安全事件和计算机安全事件为：“任何破坏某些计算机或网络安全方面的不良事件。”美国国家标准与技术研究所(NIST)专业出版物(SP)800-61“计算机安全事件处理指南”对计算机安全事件的定义是：“违反或即将威胁违反计算机安全策略、可接受的使用策略或标准的安全实践。”(NIST SP 文档，包括 SP 800-61，可从 NIST 专业出版物网址下载：http://csrc.nist.gov/publications/PubsSPs.html)

在事件响应的背景下，事件是指计算机安全事件。往往，你只会看到事件。例如，在安全操作域的 CISSP 考生信息公告(CIB)中，“进行事件管理”针对的显然是计算机安全事件。

注意：

在本章中，任何关于事件的引用都是指计算机安全事件。组织处置一些特别事件时，如天气事件或自然灾害，可以使用其他方法，如业务连续性计划(可参考第 3 章内容)或灾难恢复计划(可参考第 18 章内容)。

组织通常将计算机安全事件的含义包含在他们的安全策略或事件响应计划中。定义通常是一到两条句子，还包括安全事件分类及常见事件案例，如下所示：

- 任何网络入侵企图
- 任何拒绝服务攻击企图
- 对任何恶意软件的检测
- 任何未经授权的数据访问
- 任何违反安全策略的行为

17.1.2　事件响应步骤

有效的事件响应管理分为几个步骤或处理阶段。图 17.1 显示了 CISSP CIB 中概括的事件响应管理涉及的 5 个步骤。重要的是要认识到，事件响应是正在进行的活动和吸取的经验教训，可用来提高检测方法或有助于防止事件重复发生。下面的章节将更深入地描述这些步骤。

图 17.1　事件响应

注意：

你可能会发现在不同文档中，这些步骤会有所不同。例如，SP 800-61 是学习更多关于事件处理知识的极好资源，但将事件响应生命周期分为以下 4 个步骤：1)准备，2)检测和分析，3)遏制、消除和恢复，4)事后恢复。然而，无论文档如何列出步骤，它们都包含了许多相同的元素，并以有效管理事件响应为相同目标。

重要的是要强调，事件响应不包括对攻击者的反击。对别人发动攻击往往适得其反并且非法。如果技术人员能够识别攻击者并发动攻击，则很可能导致攻击者的攻击升级。换言之，攻击者可能会考虑周期性地发动怨恨攻击。此外，很可能攻击者隐藏在一个或多个无辜受害者的背后。攻击者经常使用欺骗的方法来隐藏自己的身份，或在僵尸网络上通过僵尸发动攻击。反击很可能会殃及无辜的受害者，而不是针对攻击者本身。

17.1.3　检测

IT 环境包括多种检测潜在事件的方法。下面的列表列出了用于检测潜在事件的许多常用方法，还包括报告这些事件的方法：

- 当相匹配的事项发生时，入侵检测和防御系统(将在本章后面描述)会发送警告给管理员。
- 当检测到恶意软件时，反恶意软件往往会显示弹出窗口来加以提示。
- 许多自动化工具定期扫描审计日志，寻找预定义的事件，如使用特殊特权。当它们检测到特定的事件时，通常会向管理员发送警告。
- 最终用户有时会发现不规则的活动，并联系技术人员或管理员寻求帮助。当用户报告事件时，比如无法访问网络资源，会提醒 IT 人员存在潜在的安全事件。

仅仅因为 IT 专业人员从自动化工具或用户投诉那里收到警告，并不能判定安全事件的发生。入侵检测和防御系统往往给人发出虚假的报警，而最终用户容易出现简单的用户错误。IT 人员需要调查这些事件，以确定它们是否是真实事件。

许多 IT 专家被归类为事件的第一响应者。他们是第一批到达现场并具有如何区分典型 IT 问题和安全事件知识的人。他们类似医疗急救人员，具有突出的技术和能力，在事故现场提供医疗援助，并帮助患者在必要时获得医疗设施。医疗急救人员有专项培训，以帮助他们确定轻微和重大伤害之

间的区别。此外，当遇到重大伤害时他们知道该怎么做。同样，IT 专业人员需要专门培训，使得他们能够对典型问题进行处理和对安全事件进行升级。

在调查一个事件，并确定是安全事件后，IT 人员转向下一个步骤：响应。在许多情况下，个人初始调查后进行事件升级，以便其他 IT 专业人士进行响应。

17.1.4 响应

检测和验证事件后，下一步是响应。响应程度取决于事件的严重程度。许多组织有指定的事件响应团队——有时被称为计算机事件响应小组(CIRT)或计算机安全事件响应小组(CSIRT)。组织通常不会在小事件中激活该团队，而在重大的安全事件发生后才激活该团队。一个正式的事件响应计划会描述谁会在什么条件下能激活该团队。

团队成员应该对事件响应和组织的事件响应计划进行培训。通常情况下，团队成员将协助调查事件、评估损害、收集证据、报告事件和恢复程序。他们还将参与修复和吸取经验教训，并帮助做根本原因分析。

组织如果能较快地响应一个事件，就可以有更好的机会来减少损害。另一方面，如果一个事件持续了几小时或几天，损害可能会更大。例如，攻击者可能试图访问客户数据库。快速的响应可以防止攻击者获得任何有意义的数据。然而，如果让攻击者持续通畅地访问数据库几个小时或几天，攻击者就有可能会得到整个数据库的副本。

在调查结束后，管理层可能决定起诉责任人。正因为如此，重要的是要在调查过程中保护所有的数据作为证据。第 19 章“事件与道德规范”，涵盖事件处理以及在响应背景下支持调查。如果有任何起诉的可能性，团队成员会采取额外的步骤来保护证据。这保证证据可以在法律程序中使用。

注意：

控制事件时，计算机不应该被关闭。如果计算机断电，临时文件和易失性随机存取存储器(RAM)中的数据将丢失。只要系统保持供电，取证专家可以用工具检索临时文件和易失性内存中的数据。然而，如果有人将电脑关闭或将电源拔掉，这些证据就会丢失。

17.1.5 缓解

缓解措施尝试遏制事件。有效的事件响应的主要目标之一是限制事件的影响或范围。例如，如果受感染的计算机通过网卡(NIC)发送数据，技术人员可以禁用网卡或断开网卡连接的网线。有时候，包括断开到其他网络的连接以控制问题在单个网络之中。当问题被隔离之后，安全人员可以解决它，而不必担心它会蔓延到网络的其余部分。

17.1.6 报告

报告是指向组织内部，同时向组织外部报告事件。虽然没有必要报告轻微的恶意软件感染事件给公司的首席执行官(CEO)，但高层管理人员确实需要知道严重的安全破坏事件。

2014 年 11 月 24 日，当索尼员工登录到自己的电脑时，他们看到了一幅布满头骨和来势汹汹、瘦骨嶙峋的手指的怪异的红色图像。伴随着一个警告：“我们已经获得了你所有的内部数据”，并警

告索尼要满足他们的要求。到了当日 11:00，新闻报道表明，作为预防措施，位于洛杉矶的索尼的所有电脑被关闭，但没有通知高级管理人员这些步骤。第二天，索尼的一位发言人发表了一份公开声明，表示他们正在调查。第二周，索尼的首席执行官兼联席主席发布了一个关于公司范围内的被攻击警告。索尼的响应表明，他们明显有面向高层管理人员的报告机制。

组织往往有法律要求，对组织以外报告事件。大多数国家(和许多较小的司法管辖区，包括州和城市)已经制定了监管合规法律来治理安全破坏，特别适用于保留在信息系统中的敏感数据。这些法律通常包括报告事件的要求，特别是如果安全漏洞暴露了客户数据的话。法律根据地域不同而不同，但都寻求保护个人记录和信息隐私，以保护消费者的身份，并建立财务实践和公司治理标准。每个组织都有责任知道什么法律适用于自身并遵守这些法律。

许多管辖区具有保护个人身份信息(PII)的法律。如果 PII 数据泄露，组织必须报告。不同的法律有不同的报告要求，包括通知受事件影响的个人的要求。换句话说，如果针对系统的攻击导致攻击者获得 PII 信息，系统的拥有者有责任通知这个攻击以及哪些数据被攻击者访问。

针对严重的安全事故，组织应考虑到报告事件给官方机构。在美国，这可能意味着告知联邦调查局(FBI)、区检察长办公室和(或)州立及当地执法机构。在欧洲，组织可以报告事件给国际刑事警察组织(INTERPOL)或基于事件和地区的其他一些机构。这些机构可能协助调查，他们收集的数据可能会帮助防止针对其他组织的未来攻击。

许多事件没有被报道，因为它们不被确认为事件。这往往是专业知识不够的结果。实际的解决办法是确保人员有相关的培训。培训应该教会个人如何识别事件，在最初的反应中做什么，以及如何报告事件。

17.1.7　恢复

调查人员从系统收集所有适当的证据后，下一步是恢复系统或将系统恢复到完全正常的状态。对小事件而言这非常简单，可能只需要重新启动。然而，重大事件可能需要完全重建系统。重建系统包括从最近的备份中恢复所有的数据。

当受损的系统重建时，重要的是要确保配置正确，至少和事件发生前一样是安全的。如果组织具备有效的配置管理和变更管理程序，这些程序将提供必要的文档，以确保重建的系统配置正确。有些事情要做双重检查，包括访问控制列表(ACL)，确保不必要的服务和协议被禁用或删除，安装所有最新的补丁，还有用户账户的默认值被修改。

注意：

在某些情况下，攻击者可能在攻击过程中，在系统上安装了恶意代码。如果没有做详细检查，这可能无法觉察。从头开始完全重建系统是事件恢复的最安全方法。如果调查人员怀疑攻击者可能在系统上修改了代码，重建系统可能是最好的选择。

17.1.8　修复

在修复阶段，人员观察事件并确定什么原因导致事件发生，然后实施措施以防再次发生，这包括执行根本原因分析。

执行根本原因分析是为了确定什么原因导致事件发生。例如，如果攻击者通过网站成功访问了

一个数据库，人员将检查系统所有元素以确定是什么让攻击者获得成功。如果根本原因分析确定一个漏洞可以缓解，这时建议进行变更。

可能是 Web 服务器没有安装最新的补丁，允许攻击者获得服务器的远程控制。补救措施可能包括实施补丁管理程序。也可能是网站应用程序没有使用足够的输入验证技术，允许进行成功的 SQL 注入攻击。补救将涉及更新应用程序，包括输入验证。还可能是数据库位于 Web 服务器而不是后端数据库服务器。修复意味着将数据库移到位于另一个防火墙后面的服务器上。

17.1.9 经验教训

在吸取经验教训阶段，人们检查事件和响应，看看有没有任何经验教训可以吸收。事件响应小组将参与这个阶段，但是其他了解该事件的员工也将参与。

在检查事件响应时，人们可以寻找改进响应的任何方面。例如，如果响应团队需要很长时间来遏制事件，应确定原因。可能是因为人们没有得到足够的培训，没有足够的知识和技能来有效响应。当收到第一个警告时，他们可能没有认识到这是安全事件，允许攻击持续的时间比需要的更长。第一响应者可能没有认识到需要保护证据，并在响应过程中不经意地破坏了证据。

记住，这个阶段的输出可以反馈到事件管理的检测阶段。例如，管理员可能会意识到，攻击未被发现，需要增加检测能力并建议对入侵检测系统进行升级。

完成经验教训审查后，通常需要事件响应团队编写一份报告。根据发现，事件响应团队可能会建议程序变更，增加安全控制，甚至改变策略。管理层将决定哪些建议予以实施，并为他们因拒绝建议而遗留的风险负责。

真实场景

授权事件响应给用户

在组织中，计算机入侵响应的职责需要扩展到用户。针对每台电脑应有一个检查表，以鉴别恶意软件感染的常见症状。如果用户怀疑自己的电脑感染了病毒，检查表将指导他们断开网卡和联系服务台报告该问题。通过断开网卡，可以迅速限制恶意软件，并阻止进一步的传播。

但这不可能在所有组织中得以实施。在该案例中，用户是一个非常庞大的网络运营中心的一部分，他们参与了某种形式的计算机支持。换言之，他们已不是典型的最终用户，而是大量的技术专家。

17.2 部署预防措施

理想情况下，组织完全可以通过实施预防措施避免事故。本节介绍许多用于预防常见攻击的安全措施。你可能会注意到术语“预防”和“防御”都会使用。虽然大多数文档目前只使用“预防”，但 CIB 包括这两种用法。例如，第 1 知识域提到了预防性控制。本章覆盖了第 7 知识域的目标和第 7 知识域提到的预防措施。为了简单起见，我们将在本章中使用“预防”，除了当引用 CIB 时。

17.2.1　基本的预防措施

虽然没有可以防止所有攻击的单一步骤，但可以采取一些能抵御大多数典型攻击的大有帮助的步骤。这些步骤中的大多数在本书的其他领域有更深入描述，但在本节中也被作为介绍列出来了。

保持系统和应用程序最新。供应商定期发布补丁以纠正错误和安全漏洞，但这些补丁需要被部署才会有效。补丁管理(见第 16 章“管理安全运营”)能确保在系统和应用程序上安装最新的相关补丁。

删除或禁用不必要的服务和协议。如果系统不需要某个服务或协议，它就不应该运行。攻击者不可能利用没有在系统上运行的服务或协议中的漏洞。作为极端对比，想象一台 Web 服务器正在运行所有可用的服务和协议，它很容易受到任何这些服务和协议的潜在攻击。

使用入侵检测和防御系统。入侵检测和防御系统观察活动，试图检测攻击，并提供警报。它们往往可以阻止或停止攻击。这些系统在本章后面会有深入介绍。

使用最新的反恶意软件。第 21 章“恶意代码和应用攻击”涵盖各种类型的恶意代码，如病毒和蠕虫。主要对策是反恶意软件，在本章后面会覆盖到。

使用防火墙。防火墙可以阻止许多不同类型的攻击。基于网络的防火墙保护整个网络，基于主机的防火墙保护个人系统。第 11 章“安全网络架构和保护网络组件”包括在网络中使用防火墙的信息，并且本章包括描述防火墙如何阻止攻击的内容。

注意：

为了防止攻击者破坏系统安全性，应确保系统及时更新补丁，并正确配置。防火墙、入侵检测和防御系统往往能帮助检测并收集证据，并起诉破坏系统安全性的攻击者。

17.2.2　理解攻击

安全专业人员需要了解常见的攻击方法，采取有效措施预防攻击，在攻击发生时能够识别出来，并采取适当方法做出响应。本节对一些常见的攻击方法进行了概述。下面的部分讨论了许多用于阻止这些或其他攻击的预防措施。

注意：

本书较为全面地概述了不同的攻击方法，并尽量避免了对某一特定方法的重复赘述。除本章外，在其他章你也会了解到不同的攻击类型，例如，第 14 章“控制和监控访问”讨论了一些与访问控制相关的攻击方法；第 12 章“安全通信和网络攻击”描述了不同类型的基于网络的攻击；第 21 章描述了几种与恶意代码和应用程序相关的不同类型的攻击方法。

1. 拒绝服务攻击

拒绝服务(DoS)攻击能够阻止系统处理或响应来自资源和客体的合法数据或请求。拒绝服务攻击的最常见形式是向服务器传输使其无法全部处理的过多数据包。其他拒绝服务攻击形式关注于对操作系统、服务或应用程序中已知故障或漏洞的利用。利用系统的故障进行攻击往往会导致系统崩溃或 100%的 CPU 使用率。无论实际攻击的形式如何，任何造成受害系统无法执行正常活动的攻击都可以被认为是拒绝服务攻击。拒绝服务攻击会导致系统崩溃、系统重启、数据损坏、服务被阻断等

后果。

注意：

对于任何一种面向互联网的系统，拒绝服务(DoS)攻击都很常见。换句话说，如果攻击者可以通过互联网访问一个系统，它就很容易受到 DoS 攻击。相比之下，对于不直接访问互联网的内部系统来说，DoS 攻击并不常见。

另一种形式的 DoS 攻击是分布式拒绝服务(DDoS)攻击。DDoS 攻击发生时，多个系统在同一时间攻击单个系统。例如，一组攻击者可以发动针对同一个系统的协同攻击。然而今天，攻击者会将几个系统联合起来，并将其作为平台，以便对想要攻击的系统采取行动。攻击者通常使用僵尸网络(在本章稍后描述)发动 DDoS 攻击。

一种变体的 DoS 形式被称为分布式反射拒绝服务(DRDoS)攻击，它利用反射方式发起攻击。换句话说，它不是直接攻击受害者，而是代替操纵流量或网络服务，以使攻击反射回来自其他来源的受害者。域名服务(DNS)投毒攻击(第 12 章中有介绍)和 smurf 攻击(本章后面有介绍)就是这样的例子。

SYN 泛洪攻击

SYN 泛洪攻击是一种常见的 DoS 攻击，它通过破坏 TCP/IP 启动通信会话的三步握手标准来实施攻击。通常，客户端向服务器发出 SYN(同步)数据包，服务器向客户端发送 SYN/ACK(同步/应答)响应数据包，随后客户端向服务器回应 ACK(应答)数据包。这样的三步握手建立起了两个系统间的一个用于数据传输的会话，这个会话直到出现 FIN(结束)或 RST(重置)数据包才会断开。

然而，在 SYN 泛洪攻击发生时，攻击者发送多个 SYN 数据包但 ACK 不完全。这类似于一个喜欢开玩笑的人伸出手去握手，但是当其他人做出回应，伸出手准备握手时，那人却将手缩了回来，留下对方的手悬在半空中。

图 17.2 为我们展示了一个例子。在这个例子中，攻击者已发出三个 SYN 数据包且服务器对每个都做出了回应。对于这些请求，服务器保留系统资源等待系统正确应答(ACK)。服务器通常在等待 ACK 三分钟后放弃尝试，但管理员可以调整这个时间。

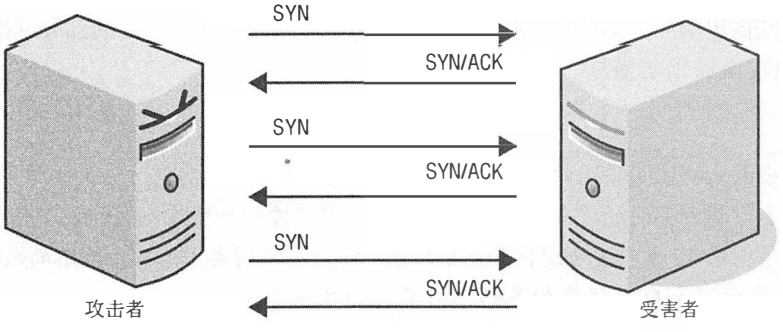


图 17.2 SYN 泛洪攻击

三个不完整的会话并不会引发问题。但是，攻击者会给受害者发送数百或数千个 SYN 数据包。每一个不完整的会话都会消耗资源，然后，在某一点，受害者变得不堪重负，无法回应合法请求。攻击可以消耗可用的内存和处理能力，导致受害系统变慢甚至崩溃。

对于攻击者来说伪造源地址很简单，每个 SYN 数据包都具有不同的源地址。正是因为这样，阻止攻击者使用源 IP 地址很困难。攻击者还会协调，对同一受害者同时发起攻击，这就是 DDoS

攻击。限制允许开放的会话的数量并不能有效加以防御，因为一旦系统达到了限制，就会阻止合法用户的会话请求。增加服务器上所允许会话的数量，会导致攻击消耗更多的系统资源，服务器的内存和处理能力也是有限的。

使用 SYN Cookie 是阻断这类攻击的一种方法。这些小记录消耗小部分系统资源。当系统接收到 ACK 应答时，检查 SYN Cookie 并建立会话。防火墙通常能够通过检测和防御系统检测 SYN 攻击。

阻断这种攻击的另一种方法是降低 TCP 重置攻击，服务器通常会等待一段时间以接收 ACK 应答。默认时间是三分钟，但在正常操作中合法系统发送 ACK 应答并不需要这么长时间。通过减少时间，半开放的会话在系统内存中的刷新会更快。

TCP 重置攻击

另一种通过操纵 TCP 会话的攻击方式叫作 TCP 重置攻击，会话通常由 FIN(完成)或 RST(复位)数据包终止。攻击者可以在 RST 包中伪造源 IP 地址并断开活动会话。两个系统之间则需要重新建立会话。这对系统来说是一个很大的威胁，系统之间需要持续的会话以保持数据。当会话重建时，系统就需要重建数据，所以这不仅仅是来回发送三个数据包以建立会话的问题。

2. smurf 和 fraggle 攻击

smurf 和 fraggle 攻击都属于 DoS 攻击。smurf 攻击是另一种类型的泛洪攻击，但使用网络控制消息协议(ICMP)回应数据包而不是 TCP SYN 数据包来攻击其他系统。更具体地说，是使用受害者的 IP 地址作为源 IP 地址的伪造广播 ping。

ping 使用 ICMP 检查与远程系统的连接。通常情况下，ping 发送一个回包请求到单一的系统，该系统用回包做出响应。然而，在 smurf 攻击中，攻击者将回应请求作为广播发给网上的所有系统，并伪造 IP 地址。所有系统通过响应回包到伪 IP 地址做出回应，这样就阻碍了受害者网络的流畅性。

smurf攻击利用放大网络(也称为 smurf 放大器)，通过路由器发送定向广播。然后，放大网络上的所有系统对受害者发起攻击。然而，在 1999 年发行的 RFC 2644 改变了路由器的标准，路由器不能转发定向广播。当管理员使用 RFC 264 正确配置路由器之后，网络便不能被放大。这给 smurf 攻击单一网络带来了限制。此外，在防火墙上禁用 ICMP 的情况越来越普遍，甚至许多服务器能够防止利用 ICMP 的任何类型的攻击。在使用标准安全的措施之后，现如今，smurf 攻击已经很少见了。

fraggle 攻击类似于 smurf 攻击。然而，fraggle 攻击使用 UDP 端口 7 和 19 而不是 ICMP。fraggle 攻击能够使用伪造的 IP 地址将 UDP 数据包发送给受害者。所有的系统就都会将其转发给受害者，这类似于 smurf 攻击。

3. ping 泛洪攻击

ping 泛洪攻击通过给受害者发送洪水般的请求来达到攻击目的，在 DDoS 攻击中给僵尸网络发送僵尸信息的效果很明显。如果成千上万的系统同时给一个系统发送 ping 请求，该系统将在试图回应 ping 请求时发生混乱。受害者便没有时间来回应合法请求。今天常见的一种处理方式就是阻断 ICMP 流量。主动入侵检测系统能检测到 ping 泛洪攻击，然后通过修改系统环境来阻断 ICMP 流量。

4. 僵尸网络

今天僵尸网络相当普遍。僵尸网络中的计算机就像机器人(通常称为僵尸)，并将会按照攻击者的要求执行命令。僵尸牧人通常是指通过一个或多个命令控制所有计算机和服务器的罪犯。僵尸牧人在服务器中输入命令，僵尸定期执行命令并控制服务器接收指令。僵尸牧人通常使用僵尸网络中的计算机来发起大范围攻击，发送垃圾邮件和钓鱼邮件，或向其他罪犯租用僵尸网络。

计算机通常在被一些恶意代码或恶意软件感染后，加入僵尸网络。计算机一旦被感染，就往往能够让僵尸牧人远程访问系统或使得额外的恶意软件得以安装。在某些情况下，僵尸安装恶意软件，这些软件能够为攻击者搜索他们需要的密码或信息。有时，这些恶意软件含有键盘记录器，能够记录用户击键信息。

僵尸网络感染 4 万台计算机很常见，并且在过去，僵尸网络控制数以百万计的系统也很常见。有些僵尸牧人控制多个僵尸网络。

防止计算机加入僵尸网络最好的办法，就是确保反恶意软件的正常运行和定期更新。因为恶意软件往往利用操作系统和应用程序未打补丁的漏洞，所以保持系统定期更新补丁，有助于对系统的保护。

许多恶意软件基于浏览器感染系统，用户在上网时，系统就会被感染。保持浏览器及插件的更新是极其重要的。此外，大多数的浏览器安全性较强，这些功能不应被禁用。例如，大多数浏览器支持 Web 应用程序沙箱隔离，但一些浏览器能够禁用该功能。禁用可能会改善浏览器的性能，但同时也具有较大风险。

真实场景

近期的一些僵尸网络

不法分子利用 Gameover Zeus 僵尸网络(GOZ)收集财务系统的凭证并进行银行诈骗。他们还用 GOZ 来分发 CryptoLocker 勒索软件。CryptoLocker 加密用户数据，然后要求用户支付一定金额以获得解密密钥。在 2014 年 6 月份，GOZ 感染了 50 万到 100 万个系统。Operation Tovar(几个执法机构之间的国际合作机构)能够暂时切断 GOZ 命令和控制服务器之间的通信线路。然而，犯罪分子已经开始使用不同的战术，且 GOZ 感染的数量还在不断增长。

Simda 是另一个僵尸网络，罪犯能够用它窃取银行认证并安装额外的恶意软件。在 2015 年 4 月，一名来自国际联合会的执法人员将其破解时，Simda 已经控制了超过 770 000 台电脑。这是个相对较新的僵尸网络，但在 6 个月中，每个月感染了约 128 000 台新电脑。

Esthost 僵尸网络(也称为 DNSChanger)感染了约 400 万台计算机。它操纵 DNS 设置以使用僵尸牧人控制的 DNS 服务器，还操纵广告。该僵尸网络造成了至少 1400 万美元的非法支付，并阻止用户更新反恶意软件或操作系统。在这种情况下，无法更新系统是很严重的问题，但许多用户都忽略了。执法人员在 2011 年手工破解该网络。

这些都是一些著名的大型僵尸网络，但这个名单肯定是不完整的。没有人知道有多少小型僵尸网络正在运行，但也有控制着几万台主机的较为活跃的僵尸网络清单。

5. 死亡 ping

死亡 ping 攻击采用一个超大的 ping 数据包。ping 数据包通常是 32 或 64 字节，但不同的操作系统可以使用其他的大小。死亡 ping 攻击将 ping 数据包的大小改到超过 64KB，这比许多系统可以处理的大小都要大。当系统收到的 ping 数据包大于 64 KB 时，就会出现问题。在某些情况下，系统就会崩溃。在其他情况下，将导致缓冲区溢出错误。现今，死亡 ping 攻击很少能够成功，因为补丁和更新改善了系统的脆弱性。

注意：

尽管现今死亡 ping 攻击已经构不成威胁，但很多其他类型的攻击也能够造成缓冲区溢出错误(在第 21 章中讨论)。当供应商发现可能导致缓冲区溢出的错误时，他们会发布修补程序来修复它们。对任何缓冲区溢出攻击的最好的保护手段之一是保持系统更新当前最新补丁。此外，生产系统不应该包括未测试的代码，也不能允许系统或根级权限的使用。

6. 泪滴攻击

在泪滴攻击中，攻击者阻碍传输，系统无法将数据包一起发回。大数据包通常被分成较小的碎片，当它们被发送到网络上时，接收系统把数据包碎片还原到原来的状态。然而，泪滴以一种系统无法将文件还原在一起的方式分割数据包。旧的系统无法处理这种情况，并且会崩溃，但补丁解决了这个问题。目前的系统不容易受到泪滴攻击，但需要强调保持系统更新的重要性。此外，入侵检测系统可以检查畸形数据包。

7. land 攻击

land 攻击是指攻击者使用受害者的 IP 地址作为源 IP 地址和目的 IP 地址，并发送伪造的 SYN 数据包给受害者。这使系统不断地对自己做出应答，并最终可能会冻结、崩溃或重新启动。这种攻击在 1997 年被第一次发现，它几次攻击不同的端口。保持系统更新并使用过滤和检测相同的源和目的 IP 地址的流量，有助于防止 land 攻击的发生。

8. 零日攻击

零日攻击是指利用他人未知的系统漏洞对系统发起攻击。然而，安全专业人员在不同的情况下使用该术语，并且在本书中也有一些小差异。这里有一些例子：

攻击者首先发现了一个漏洞　当攻击者发现一个漏洞时，他可以很容易地利用它，因为攻击者是唯一意识到漏洞的人。在这一点上，供应商是不知情的，所以并没有开发或发布补丁。这是零日漏洞的常见定义。

供应商了解漏洞的存在　供应商了解漏洞的存在，他们会对威胁进行评估，并优先发布补丁。软件补丁很复杂，需要大量测试，以确保补丁不会引起其他问题。供应商可能会在几天内开发和发布高危漏洞补丁，而他们可能需要几个月的时间来开发和发布小漏洞补丁。在这个时候，利用该漏洞的攻击通常被称为零日漏洞，因为公众不知道该漏洞。

供应商发布补丁　一旦补丁被开发和发布，修补过的系统就不再容易受到攻击。然而，在安装补丁之前，组织往往需要时间来评估和测试，从而导致在供应商发布补丁和管理员应用补丁之间有一定的时间差。微软通常在每个月的第二个星期二发布补丁，通常被称为“补丁星期二”，攻击者往往使用逆向工程来破解补丁，然后在第二天利用它们，通常被称为“漏洞星期三”。一些人把在供应

商发布补丁第二天进行攻击的行为称为零日攻击。然而，这种用法并不常见。相反，许多安全专家认为这是对未安装补丁系统的攻击。

注意：

如果组织没有一个有效的补丁管理系统，他们的系统就很容易受到已知漏洞的威胁。如果在供应商发布补丁之后的几个星期或几个月后发生了系统攻击，这不叫做零日漏洞。相反，这是对未安装补丁系统的攻击。

用于保护系统免受零日漏洞的方法包括许多基本的预防措施。确保系统不运行不需要的服务和协议可以减少系统的攻击面，使基于网络和基于主机的防火墙能够限制潜在的恶意流量，并使用入侵检测和防御系统检测和阻止潜在的攻击。此外，蜜罐和填充单元使得管理员有机会观察攻击并可能揭示使用零日漏洞攻击的原理。蜜罐和填充单元在本章后面会做出解释。

9. 恶意代码

恶意代码是指在计算机系统上执行不必要的、未授权的或未知活动的脚本或程序。恶意代码可以采取多种形式，包括病毒、蠕虫、特洛伊木马、具有破坏性的宏文件和逻辑炸弹。它们通常被称为恶意软件或恶意代码。恶意代码存在于每一种类型的计算机或计算设备上，它们是现今最常见的安全问题。第 21 章将详细介绍恶意代码。

传播病毒的方法不断发展。几年前，最流行的方法是通过软盘，手动完成系统与系统之间的传播。后来，最流行的方法是通过电子邮件的附件或嵌入式脚本。今天，许多专业人士认为，偷渡式下载是最流行的方法。

偷渡式下载可以未经用户许可就将恶意软件下载并安装在用户的系统中。攻击者修改网页上的代码，当用户访问时，代码未经用户许可就在用户系统中下载和安装恶意软件。攻击者有时会利用合法的网站，并向其添加恶意代码以便实现偷渡式下载。他们还拥有自己的恶意网站，并使用网络钓鱼或重定向的方法使用户进入网站。大多数偷渡式下载利用的是未安装补丁的系统的漏洞，所以保持系统更新能起到保护作用。

注意：

最近的一些偷渡式下载程序包括 Zeus 和 Gumblar。Zeus 通过偷渡式下载和网络钓鱼尝试来传播，并且一旦安装后，就会窃取银行站点的凭证。感染了 Gumblar 的网站会将用户重定向到另一个网站，然后下载并打开受感染的 PDF 文件。

安装恶意软件的另一种流行方法是使用付费的安装方法。罪犯支付网站运营商一定费用购买他们的恶意软件，这通常是假冒的反恶意软件程序。网站运营商从每一个由其网站发起的安装中获利。根据赛门铁克公司调查，每次安装获利金额从 13 美分到 30 美元不等，这取决于安装软件的类别及安装位置。

虽然大多数恶意软件来自于互联网，但也有些是通过 USB 闪存驱动器传输的。当用户在系统中插入 USB 闪存驱动器时，许多病毒都能检测到，然后感染驱动器。当用户将其插入另一个系统时，恶意软件会感染另一个系统。

10. 中间人攻击

当恶意用户能够逻辑上获得正在进行通信的两个端点之间的位置时，中间人攻击就会产生。中

间人攻击有两种。一种涉及复制或嗅探双方通信，这基本上算是嗅探攻击，如第 14 章所述。另一种类型是攻击者在通信线路上定位自己，将本身作为存储和转发或代理机制，如图 17.3 所示。客户端和服务器认为它们是直接连接的。然而，攻击者捕获和转发这两个系统之间的所有数据。攻击者可以收集登录凭据和其他敏感数据，以及改变两个系统之间交换的消息内容。

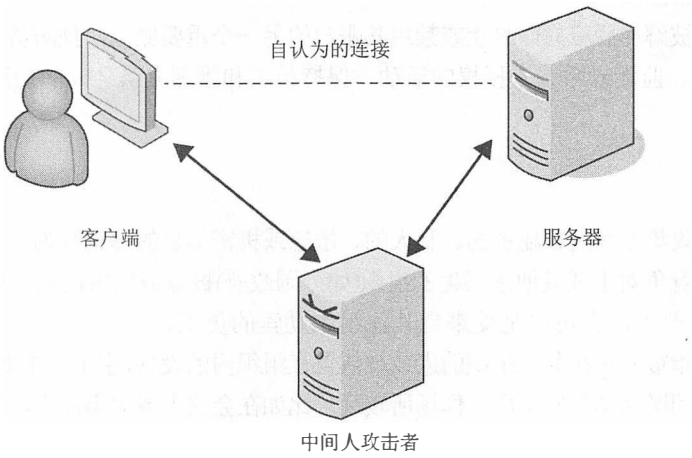


图 17.3　中间人攻击

中间人攻击比其他许多攻击需要更多技术，因为从客户角度出发，攻击者需要冒充服务器，从服务器的角度来看，攻击者还要冒充客户端。中间人攻击往往需要组合多种攻击。例如，作为攻击的一部分，攻击者可能会改变路由信息和 DNS 值，或伪造地址解析协议(ARP)查找。

通过保持系统更新最新补丁，能够预防一些中间人攻击。入侵检测系统通常无法检测到中间人或劫持人攻击，但可以检测到通信线路上的异常活动并对可疑活动提高警惕。

11. 战争拨号

战争拨号是一种使用调制解调器搜索接受入站连接尝试的系统的行为。战争拨号器通常是附有调制解调器以及运行战争拨号程序的计算机，也可以是一台单独的设备。不管采用哪种形式，战争拨号器都被用于系统地拨打电话号码，并且能够侦听计算机载波音。一旦检测到某个计算机载波音，战争拨号器就会在搜索过程结束时，在生成的报告中添加相应的电话号码。战争拨号器能够被用于搜索任意号码段，例如特定前缀内的所有 10 000 个号码或特定电话区号内的所有 10 000 000 个号码。

虽然对调制解调器的使用已大幅减少，但仍有组织在使用。对于那些没有访问互联网权限的员工来说，调制解调器为他们提供了远程访问的途径。同时，员工已经掌握了通过在工作系统上安装调制解调器，并避开组织的监控工具来访问互联网的方法。

一种新的战争拨号形式能够在不使用调制解调器的情况下，使用互联网协议电话(VoIP)拨号，这样攻击者就能够扫描到更多的电话号码，并发现除了调制解调器以外的其他设备，如传真机、语音信箱、拨号音和人的声音。例如，Metasploit 纳入了 WarVOX 的更新版本(一种使用 VoIP.Metasploit 的战争拨号工具)，是一款众所周知的被攻击者和测试者使用的渗透测试工具。

抵御恶意战争拨号攻击的对策包括：实施强大的远程访问安全性(主要依靠强的身份认证)，确保不存在未授权的调制解调器，以及使用回叫安全机制、协议约束与呼叫登入。

12. 破坏

破坏指的是员工对组织的破坏行为。如果员工对组织的资产足够了解，且有足够的机会来操作环境的关键位置，破坏将会构成风险，破坏通常发生在员工自身怀疑将被无故解雇或被解雇员工仍对系统有访问权的情况下。

这也是员工被解雇后应立即终止或禁用其账户的另一个重要原因，预防员工破坏的其他保障措施还有定期审计、监测异常或未授权的活动、保持员工和管理人员之间的沟通开放，并适当奖励员工。

13. 间谍

间谍是一种收集专有的、秘密的、私人的、敏感或机密信息的恶意行为。攻击者经常从事间谍活动，目的是向竞争对手或其他感兴趣的组织(如外国政府)披露或出售信息。攻击者可以是不满的员工，在某些情况下，也可以是受来自其他组织勒索的员工。

间谍也可以指被安排在某一组织的人或被放置在组织内的设备，用于为主要秘密雇主提供信息。在某些情况下，间谍活动的发生离工作场所较远，比如在会议上或大事件中，这些人专门利用员工的流动性进行间谍活动。

反间谍活动指严格控制访问所有的非公开数据，彻底筛选新的员工，并有效地跟踪所有员工活动。

17.2.3 入侵检测和防御系统

入侵发生时，攻击者能够绕过或破坏安全机制，并获得组织的资源。入侵检测是一种特定形式的监测，通过监控记录信息和实时事件来检测潜在事件或入侵的异常活动。入侵检测系统(IDS)通过自动检测日志和实时系统事件以检测入侵和系统故障。

入侵检测系统能够有效检测许多DoS和DDoS攻击。它们可以识别来自外部连接的攻击，如来自互联网的攻击，以及通过内部传播的攻击，如恶意蠕虫。一旦发现可疑的事件，便会通过发送或响起警报的方式来做出回应。在某些情况下，它们可以修改环境来阻止攻击。入侵检测系统的主要目标是提供能够及时和准确应对入侵的方法。

注意：

入侵检测系统是纵深防御安全计划的一部分，将与其他安全机制(如防火墙)共存，并相互补充，但并不会取代它们。

入侵防御系统(IPS)具有入侵检测系统的所有功能，而且还可以采取额外的措施来阻止或防止入侵。如果需要的话，管理员可以禁用 IPS 中的这些额外功能，使之成为入侵检测系统。

你会经常看到入侵检测和防御系统的结合(IDPS)。例如，NIST SP 800-94 “入侵检测和防御系统指南” (NIST 特别出版物下载页面：http://csrc.nist.gov/publications/PubsSPs.html)，详细且全面介绍了入侵检测和防御系统，但在本书中简化使用 IDPS 代替两者。在本章中，我们描述了使用 IDS 检测攻击的方法，它们如何应对攻击，以及 IDS 所支持系统的类型。我们会在 IPS 的适当位置添加信息。

CISSP 目标的历史

CISSP 认证在 1994 年被首次建立并推出，并经历了多年的变化。同样，随着新威胁的出现以及安全人员对安全控制的创建和改进，IT 安全性也经历了一些变化。

$(ISC)^2$ 发布的应试者信息公告(CIB)中确定了 8 个领域，还列出了域内主要的主题和副主题。CIB 提供有限的考试蓝图。在 2002 年，$(ISC)^2$ 称该文档为 CISSP CBK 学习指南。尽管学习指南中的内容更详尽，但它和目前的 CIB 很相似。

入侵检测是一个已在 CISSP 的 CBK 和 CIB 中存在多年的话题。在 2002 年的 CBK 学习指南中，入侵检测内容包括访问控制系统的方法论域和业务安全域两部分(目前 CIB 将这两个域分别命名为身份与访问管理、安全运营)。

然而，2009 和 2012 年的 CIB 中并没有包含任何有关入侵检测的信息。入侵检测仍在测试中，但并没有被列出来。在本书的最新版本中，我们将入侵检测列入“实施预防攻击措施”的一部分。在这个版本的 CIB 中，$(ISC)^2$ 在预防措施的目的中，再次提及入侵检测和防御系统。随着这一话题不断出现，我们能确定入侵检测是考试的重要考点。

1. 基于知识和基于行为的检测

入侵检测系统(IDS)能够通过监控网络流量和检查日志来检查有无可疑活动。例如，入侵检测系统使用传感器或代理设备来监控路由器和防火墙等关键设备。这些设备有可以记录活动的日志，传感器可以将这些日志条目转发给入侵检测系统，以便分析。一些传感器将所有的数据发送到入侵检测系统，而另一些传感器检查条目，只发送特定的日志条目。具体方式取决于管理员对传感器的控制。

入侵检测系统对数据进行评估，并使用如下两种常见方法对恶意行为进行检测：基于知识的检测和基于行为的检测。总之，以知识为基础的检测使用签名，这种签名类似于反恶意软件中使用的签名定义。基于行为的检测不使用签名，而是将活动同正常性能的基线进行对比，以检测异常行为。许多入侵检测系统采用两者相结合的方法。

基于知识的检测　最常用的检测方法是基于知识的检测(又称为模式匹配检测或基于签名的检测)。它使用由入侵检测系统供应商开发的已知攻击的数据库。例如，一些自动化工具可以启动 SYN 泛洪攻击，而这些工具的模式和特点均已在签名数据库中定义。流量数据实时与数据库相匹配，如果入侵检测系统发现匹配，则发出警告。基于知识的入侵检测系统的主要缺点是，只对已知的攻击方法有效。新的攻击或已知攻击被稍微修改版本，入侵检测就会失效。

IDS 中基于知识的检测类似于反恶意软件应用中基于签名的检测。反恶意软件应用有已知恶意软件的数据库，并在数据库中检索，寻找匹配的文件。正如反恶意软件应用必须从软件供应商那里获得更新，入侵检测数据库也必须定期更新攻击签名。大多数的入侵检测系统供应商提供自动更新签名的方法。

基于行为的检测　第二种检测类型是基于行为的检测(也被称为统计入侵检测、异常检测和基于启发式的检测)。基于行为的检测最开始在系统中创建正常活动和事件的基线。一旦积累足够多的能够确定正常活动的基线数据，便可以检测恶意入侵或恶意事件的异常活动。

基线通常在有限的时间内建立起来，例如一个星期。如果网络被修改，基线需要更新。否则，入侵检测系统可能会提醒存在异常活动，但其实是正常的。一些产品继续监测网络，以了解更多的正常活动，并且会根据监测更新基线。

基于行为的入侵检测系统使用基线、活动数据、启发式评估技术将当前活动同先前活动进行比较，以检测潜在恶意事件。许多可以执行状态包分析，这类似于通过状态检测防火墙(第 11 章中有相关介绍)检测基于网络流量的状态。

正常的分析能够使入侵检测系统识别下列情况，并作出相应反应。具体情况有：流量及活动的激增，多次失败的登录尝试，在正常工作时间以外的登录或程序活动，或突然增加的错误或失败信息。所有这些都代表发生了以知识为基础的检测系统所无法识别的攻击。

基于行为的入侵检测系统可以被认为是专家系统或伪人工智能系统，因为它可以学习并对事件做出假设。换言之，入侵检测系统可以像人类专家一样，能够通过已知事件对当前事件进行评估。基于行为的入侵检测系统的正常活动和事件的信息越多，检测到异常情况的概率就会越高。不同于基于签名的检测，基于行为的入侵检测系统的一个明显好处是可以不使用签名，便能检测到新的攻击。

基于行为的入侵检测系统的主要缺点是，往往会发起大量的假警报，也被称为虚假警报或误报。在正常操作过程中，用户和系统活动的模式可能会有很大的不同，使得难以准确地定义正常和异常活动的边界。

真实场景

虚假警报

许多入侵检测系统管理员面临的一个挑战是在入侵检测系统发送的错误警报或警报的数量之间找到一个平衡点，以确保入侵检测报告的真实性。在我们所了解的一个组织中，其入侵检测系统在几天内发出了一系列警告，调查后发现是虚假警报。管理员对系统失去信心，后悔在这些虚假警报上浪费了时间。

之后，入侵检测系统在发生真实攻击时发送了报告。然而，管理员正在积极解决另一个他们认为是真实攻击的问题，所以并没有花时间去检查他们认为的假警报。管理员只是简单地驳回了入侵检测系统的警报，直到几天之后才发现攻击发生了。

2. IDS 响应

虽然基于知识和基于行为的入侵检测系统使用的方法不同，但是它们都使用警报系统。当入侵检测系统检测到事件时，便会触发报警。然后，可以使用被动或主动的方法做出响应。被动响应是指系统记录事件并发送通知。主动响应是指系统通过改变环境来阻止活动而不是做记录和发送通知。

注意：

在某些情况下，可以在防火墙的前后各放置一个被动式入侵检测系统，以检查防火墙的有效性。通过检查两个 IDS 警报，便能确定被防火墙阻挡的攻击类型而不是仅仅确定正在进行的攻击类型。

被动响应 系统能够通过电子邮件、文本、寻呼消息或弹出消息的方式将信息发送给管理员。在某些情况下，如有必要，警报可以生成一份报告，详细说明事件和日志活动，可为管理员提供更多的信息。许多 24 小时的网络运营中心(NOC)都有中央监控屏幕，主要支持中心的所有人员都能看到。例如，一面墙上有多个大屏幕，实时监测并显示 NOC 中的不同网络元素数据。IDS 警报会显示在一个屏幕上，以确保工作人员及时了解事件。这些即时通知帮助管理员快速有效地对未知行为

做出响应。

主动响应　主动响应可以使用几种不同的方法来修改环境。典型的一些回应有通过修改 ACL 以阻止基于端口、协议和源地址的流量输出，甚至可以禁用某段电缆上的所有通信。例如，如果 IDS 检测到来自某一 IP 地址的 SYN 泛洪攻击，IDS 可以通过改变 ACL 以阻止来自该 IP 地址的所有流量输入。同样，如果 IDS 检测到来自多个 IP 地址的 ping 泛洪攻击，可以改变 ACL 以阻止所有的 ICMP 流量输入。入侵检测系统也可以阻止可疑或非法用户的资源访问。安全管理员事先对这些活动配置合适的响应方式，并可以根据环境的变化做出调整。

注意：

使用主动响应方式的 IDS，通常被称为 IPS(入侵防御系统)。在某些情况下，这样说是准确的。然而，IPS(在本节后面介绍)应与系统流量相一致。如果某个主动 IDS 与系统流量相一致，它就是 IPS。如果不一致，就不能称之为 IPS，因为它只有在进程中检测到攻击之后才能做出反应。NIST SP 800-94 建议将所有主动 IDS 与系统一起安装，以便它们能发挥 IPS 功能。

3. 主机型和网络型 IDS

IDS 一般根据信息来源进行分类。目前主要有两类 IDS：主机型与网络型。主机型 IDS(HIDS)监视单个计算机或主机上的可疑活动，网络型 IDS(NIDS)则监视在网络介质上进行的可疑活动。

基于应用程序的入侵检测系统很少使用，它是一种特定类型的基于网络的入侵检测系统。它监视两个或多个服务器之间的特定应用程序流量。例如，基于应用程序的入侵检测系统可以监视 Web 服务器和数据库服务器之间的流量，以寻找可疑活动。

主机型 IDS　HIDS 监视单个计算机上的活动，包括过程调用和日志，这些日志记录在系统、应用、安全和基于主机的防火墙中。它检测的事件比 NIDS 更详细，并且可以在攻击中找到特定的文件，同时还可以跟踪攻击者采用的进程。

HIDS 优于 NIDS，是因为它可以检测到主机系统上的异常。例如， HIDS 能够检测到攻击者进入系统并进行远程监控的感染点。你可能会注意到，这听起来类似于电脑上的反恶意软件，确实是这样。许多 HIDS 都拥有反恶意软件的能力。

虽然很多厂商建议在所有系统中安装基于主机的 IDS，但该行为仍不常见，因为 HIDS 也有缺点。相反，许多组织选择在关键的服务器上安装 HIDS 作为附加保护。HIDS 的缺点是费用和相关的可用性。HIDS 比 NIDS 更昂贵，因为它们需要对每个系统进行监视，而 NIDS 通常支持集中式管理。HIDS 不能检测到其他系统的网络攻击。此外，它还将消耗大量的系统资源，降低主机系统的性能。虽然限制 HIDS 所使用的系统资源也是可以做到的，但这样通常会导致对一次活跃攻击的遗漏检测。此外，HIDS 更容易被攻击者发现，并且日志将会保存在系统中，这更方便入侵者修改日志。

网络型IDS　NIDS监测并评估网络活动来检测攻击事件或异常。它不能检测加密流量的内容，但可以监测其他数据包的信息。NIDS系统通过使用远程传感器来收集关键网络位置的数据，以监测大型网络。在关键网络位置能够将数据发送到中央管理控制台，这些传感器可以监视路由器、防火墙、支持端口镜像的网络交换机和其他类型的网络端口流量。

提示：

交换机通常被用于阻止恶意嗅探。如果 IDS 被连接到交换机上一个正常的端口，它将只捕获网络流量的一小部分，这样就不会产生太大作用。相反，交换机被配置到能够监测 IDS 上特定端口的

所有流量(通常被称为端口镜像)。在思科交换机上，用于端口镜像的端口被称为交换端口分析器(Switched Port Analyzer，SPAN)端口。

中央控制台通常被安装在单一用途的计算机上，以防止攻击。这减少了 NIDS 漏洞，并可以让它的运行透明，使得攻击者难以发现并做出攻击。网络型入侵检测系统对网络整体性能的负面影响很小，当它被安装在单一的系统上时，不会对其他任何计算机的性能产生不利影响。在大流量的网络中，NIDS 可能无法跟上数据流量，但可以添加额外的系统以平衡负载。

通常情况下，网络型入侵检测系统可以通过反向地址解析协议攻击源(RARP)或反向域名系统(DNS)查找攻击源。然而，攻击者往往使用虚拟 IP 地址或僵尸网络发起攻击，这需要做更深入的调查以确定攻击源。该过程很困难，并且已经超出了入侵检测系统的检测范围。然而，可以通过一些调查手段找到虚假 IP 源。

警告：

对入侵者发起反击或试图反黑客入侵是不道德的，也是有风险的。相反，可以依靠日志记录和嗅探收集功能，来收集足够的数据以起诉罪犯或改善环境安全。

NIDS 通常能够检测到攻击或将要进行的攻击，但它们往往不能提供有关攻击成功的信息。如果攻击感染了特定的系统、用户账户、文件或应用程序，NIDS 就不会检测到。例如，NIDS 可能会发现通过网络发送的缓冲区溢出攻击，但不一定了解该攻击是否成功感染了系统。然而，管理员收到警报后，他们会检查相关的系统。此外，调查人员可以将 NIDS 日志作为审计线索的一部分以了解入侵防御系统中发生的攻击。

4. 入侵防御系统

入侵防御系统(IPS)是一种特殊类型的主动入侵检测系统，能够在攻击到达目标系统之前进行检测并阻止攻击，有时也被称为入侵检测和防御系统(IDPS)。两者之间最主要的区别就是 IPS 同流量保持一致，如图 17.4 所示。换句话说，所有流量必须通过 IPS，IPS 可以在分析之后选择将流量通过或阻止。这使得 IPS 能够阻止攻击到达目标。

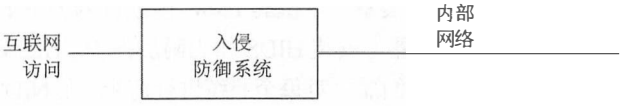


图 17.4　入侵防御系统

相反，与流量不一致的 IDS 只有在攻击到达目标之后才能检测到。主动 IDS 能够在攻击开始之后采取措施阻止攻击，但不能预防攻击。

就像其他的 IDS 一样，IPS 可以使用基于知识的检测和/或基于行为的检测。此外，可以记录活动，并像 IDS 一样给管理员发出警报。

5. 理解黑暗网络

在入侵检测环境中，黑暗网络使用已分配的、不使用的 IP 地址网络空间的一部分，包括一台已配置的、为捕获所有进入黑暗网络的流量的设备。由于 IP 地址没有被使用，黑暗网络没有任何其他主机并且也应该根本没有任何流量。但是，如果正在探测网络的攻击者或恶意软件正在试图扩散，那么黑暗网络中的主机将会探测和捕捉到这项活动。这样的好处是很少有误报信息。合法流量不会

出现在黑暗网络中，除非有网络配置错误，否则出现在黑暗网络中的流量是不合法的。

17.2.4　特殊的防御措施

虽然入侵检测和防御系统对于保护网络需要走很长的路，但是管理员通常可以使用额外的安全控制措施来保护他们的网络。以下部分描述了其中几个额外的预防措施。

1. 蜜罐/蜜网

蜜罐通过创建独立的计算机作为陷阱来捕获入侵者。可通过两个或多个联网蜜罐一起来模拟网络。它们看起来像是合法的系统，但它们对于攻击者不存放任何真实的有价值的数据。管理员通常配置带有漏洞的蜜罐，诱使入侵者攻击他们。它们可能是未打的补丁或管理员有意打开的安全漏洞。目标是抓住入侵者的注意力，并使入侵者远离保存有价值资源的合法网络。合法用户无法访问蜜罐，因此对蜜罐的任何访问都很可能是未授权的入侵者。

除了使攻击者远离生产环境之外，蜜罐也为管理员提供了机会，使他们在不破坏真实环境的情况下观察攻击者的活动。在某些情况下，蜜罐可以用来延迟入侵者的侵入时间，以便 IDS 尽可能多地检测和收集有关入侵者的信息。攻击者在蜜罐中花费的时间越长，管理员调查和识别入侵者的时间就越多。许多安全专家认为蜜罐能够有效防范零日攻击。

通常情况下，管理员将蜜罐和蜜罐网络放置在虚拟网络中。在被攻击之后重建也很简单。例如，管理员可以配置蜜罐，然后给蜜罐虚拟机拍快照。如果攻击者修改了环境，管理员可以将机器恢复到拍快照时的状态。

蜜罐的使用引出了有关引诱与诱捕问题的讨论。如果入侵者不是在蜜罐所有者对外公开时发现蜜罐，那么蜜罐就可以作为合法的引诱设备使用。在互联网上放置安全脆弱性开放的系统并用已知的方法激活服务就是引诱，引诱提供从事非法或未授权活动的机会但是由犯罪者自己决定是否执行活动。当蜜罐的所有者积极地唆使访问者访问蜜罐所在站点，然后控诉访问者的未授权入侵，这就是非法诱捕。换句话说，当哄骗或怂恿犯罪者执行非法的或未授权活动时，就应该考虑到这是诱捕。

2. 理解伪漏洞

伪漏洞是被故意植入系统中，试图引诱攻击者的虚假漏洞或明显漏洞。它们通常作为已知的操作系统漏洞被用在蜜罐系统中。试图寻找已知漏洞的攻击者可能会被伪缺陷迷惑，并认为他们已经成功穿透了系统。更复杂的伪缺陷机制能够完全模拟渗透效果并向攻击者证明，他们已经成功获得系统的访问权。然而，当攻击者破解系统时，监测和报警机制已经被触发，并向管理员发出威胁警报。

3. 理解填充单元

填充单元系统与蜜罐类似，但使用不同的方式来隔离入侵。当入侵者被 IDS 检测到时，入侵者被自动转移到填充单元。填充单元具有实际网络的结构和布局，但是在填充单元里，入侵者既不能执行任何恶意活动，也不能访问任何机密数据。

填充单元是模拟环境，类似蜜罐，通过提供伪造数据来吸引入侵者。但是，将入侵者转移到填充单元时，并不会告知入侵者环境已经发生变化。相比之下，攻击者选择攻击蜜罐。填充单元被管理员严密监控，并且用它们跟踪和收集可能发生的诉讼证据。

4. 警告框

警告框将基本安全策略准则通知给用户和入侵者。通常他们会提示在线活动被审计和监控，并提供受限制的活动提醒。在大多数情况下，从法律的角度来看，警告框中的措辞很重要，因为这些警告框可以将用户合法地束缚到一组活动、行为或过程中。

能够登录到系统的未经授权人员也能看到警告框。在这种情况下，警告框可以被看作“禁止入内”的牌子的电子等价物。当所有活动被监测并记录，且警告框清楚表明禁止未经授权的访问时，可以对入侵者和攻击者发起起诉。

提示：

警告框对授权和未经授权的用户同时发出通知。警告框通常提示授权用户可接受使用协议的内容。

5. 反恶意软件

阻止恶意代码最重要的措施是使用带有最新签名文件的反恶意软件。攻击者定期发布新的恶意软件，并经常修改现有的恶意软件来阻止反恶意软件的检测。反恶意软件供应商寻找这些变化，并开发新的签名文件来检测新的恶意软件并对其进行修改。几年前，反恶意软件供应商建议每周更新一次签名文件。然而现今，在没有用户干预的情况下，大多数的反恶意软件每天会检查更新数次。

注意：

最初，反恶意软件将注意力集中在病毒上。然而，恶意软件不断扩展，最终含有其他恶意代码，如木马、蠕虫、间谍软件和 rootkit，供应商也随之扩展了他们的反恶意软件的功能。现在，大多数的反恶意软件都能够检测并阻止大多数恶意行为，所以在技术上可以称之为 anti-malware 软件。CISSP CIB 中使用 anti-malware 作为专业术语。

许多组织使用多种方法来阻止恶意软件并进行检测。含有内容过滤功能的防火墙(或内容过滤应用程序)通常被用在互联网和内部网络之间的边界上，以过滤恶意代码。专业的安装在电子邮件服务器上的反恶意软件，能够检测并过滤出电子邮件中的恶意代码。此外，在每个系统上安装反恶意软件以检测和阻止恶意软件的侵入。组织经常使用一台中心服务器来部署反恶意软件和下载更新，以及将更新推送到客户端。

在每个系统中，多方式并重的反恶意软件除了能过滤系统内容之外，还有助于保护系统免受感染。举个例子，在每个系统中使用最新版的反恶意软件能够检测并阻止员工的 USB 闪存驱动器中的病毒。

反恶意软件供应商通常建议在一个系统上只安装一个反恶意软件应用程序。当系统中有多个反恶意软件应用程序时，它们之间会互相干扰，有时会导致系统出现问题。此外，有多个扫描器会消耗过多的系统资源。

遵循最小特权原则也有帮助。用户没有系统管理权限，无法安装可能是恶意的应用程序。如果有病毒感染系统，就可以模拟登录用户。当该用户的权限有限时，病毒的能力也是有限的。此外，增加额外的应用程序也会增加与恶意软件相关的漏洞。每一个额外的应用程序都为恶意代码提供了一个潜在的攻击点。

培训用户以了解恶意代码的危险性，了解攻击者如何欺骗用户安装恶意软件，了解如何控制风

险，这也是一种保护措施。很多情况下，用户只要不点开链接，或不打开电子邮件的附件，就可以避免感染。

第 14 章“控制和监控访问”讨论了社会工程学，包括网络钓鱼、鱼叉式网络钓鱼和捕鲸。当用户了解这些攻击类型时，便很难上当。尽管用户了解了这些风险的有关知识，钓鱼邮件仍然充斥着整个网络，并被发送到用户的收件箱。攻击者继续发送邮件的唯一原因是他们想继续欺骗一些用户。

教育、策略和工具

对于任何使用 IT 资源的组织来说，恶意软件都是要面临的一个持续不断的挑战。想想 Kim，他通过邮件向 Larry 的账户转发了一个看似无害的办公室笑话。Larry 打开文件，它实际上包含源代码段，该源代码段能够在 Larry 的系统中进行有害行动。之后 Larry 向其工作站报告了许多“性能问题”和“稳定性问题”，而这些在之前从来没有报告过。

在这种情况下，Kim 和 Larry 没有意识到他们看似无害的活动所造成的危害。毕竟，通过公司的电子邮件分享轶事和笑话是一种联络和社交的常见方式。怎么会有害处呢？真正的问题是，我们应如何教育 Kim、Larry 和所有其他用户谨慎处理共享文件？

关键是教育、策略和工具的结合。应教育 Kim，使他明白给公司网络转发与工作无关的材料违反策略和道德。同样，Larry 应该认识到，打开与工作无关的附件会导致各种各样的问题。策略中应该清楚地写明 IT 资源可使用的范围和未授权材料的危险性。像反恶意软件这样的工具，应被用来预防和检测环境中任何类型的恶意软件。

6. 白名单和黑名单

白名单和黑名单可以有效阻止用户运行未授权的应用程序。它们还有助于预防恶意软件感染。白名单有助于识别系统中经过授权的软件，黑名单能够识别系统中未经过授权的软件。白名单中不含有恶意软件，但能阻止其运行。一些白名单识别应用程序使用哈希算法来创建哈希。然而，如果一个应用程序感染了病毒，该病毒可以有效地改变哈希，因此白名单也能阻止这类被感染的应用程序运行(第 6 章“密码学与对称加密算法”讨论了更深入的散列算法)。

在 iPhone 和 iPad 上运行的 iOS 是一个极端的白名单例子。用户只能从苹果的应用程序商店安装应用程序。苹果的工作人员对商店的所有程序进行检查和批准，并及时消除不良行为。虽然用户可以将 iOS 设备越狱以绕过其安全保护，但大多数用户为了质量而选择拒绝越狱。

注意：

越狱的 iOS 设备，允许对操作系统根级别的访问，类似于在运行安卓操作系统的设备上刷机。

如果管理员能够确定想阻止的应用程序，黑名单是很好的选择。例如，如果管理层想确保用户不在他们的系统上运行游戏，管理员可以使用工具来阻止这些游戏的安装。

7. 防火墙

防火墙通过过滤流量为网络提供保护。正如在第 11 章中讨论的，防火墙已经历多年变化。

基本的防火墙使用协议号过滤基于 IP 地址、端口和一些协议的流量。防火墙含有 ACL 中的一些规则，能够允许特定的流量，以及以隐式拒绝规则结束。隐式拒绝规则阻止以前的规则所不允许的所有流量。例如，防火墙可以分别通过允许使用 TCP 端口 80 和 443 的流量来允许 HTTP 和 HTTPS 流量(第 11 章详细叙述了逻辑端口的有关细节)。

ICMP 使用 1 号协议，所以防火墙通过允许带有协议号 1 的流量允许 ping 流量。同样，防火墙可以通过分别允许带有协议号 50 和 51 的流量来允许 IPSec 封装安全协议(ESP)流量和 IPsec 认证头(AH)流量。

注意：

互联网地址分配机构(IANA)维护一组与协议相关的已知端口。IANA 同时也维护 IPv4 和 IPv6 中的指定 IP 号码列表。

第二代防火墙添加了额外的过滤功能。例如，应用级网关防火墙能够过滤基于特定应用需求的流量，而电路级网关防火墙能够过滤基于通信电路的流量。第三代防火墙(也称为状态检测防火墙和动态包过滤防火墙)能够过滤基于流量状态的流量。

下一代防火墙含有统一威胁管理(Unified Threat Management，UTM)装置的功能，并将几个过滤功能结合在一起。它包括传统的功能，如数据包过滤和状态检测。然而，它能够执行数据包检测技术，使其能够识别和阻止恶意流量。它可以过滤使用定义文件和/或白名单和黑名单的恶意软件。它还包括入侵检测和/或入侵防御功能。

8. 沙箱

沙箱为应用提供了一个安全边界，以防止应用程序与其他应用程序交互。反恶意软件应用程序使用沙箱技术来检测未知的应用。如果应用程序显示可疑特征，沙箱技术能够防止应用程序感染其他应用程序或操作系统。

应用程序开发人员经常使用虚拟化技术来测试应用程序。他们创建一台虚拟机，接着将其与主机和网络隔离，并且他们能够在不影响虚拟机外部环境的情况下在沙箱中对软件进行检测。同样，许多反恶意软件厂商使用虚拟化作为沙箱技术来观察恶意软件的行为。

9. 第三方安全服务

一些组织将安全服务外包给第三方，这是该组织以外的个人或组织。其中可以包括许多不同类型的服务，如检测和渗透测试。

在某些情况下，组织必须向外部实体提供保证，第三方服务提供商必须符合特定的安全要求。例如，组织进行主要信用卡交易时必须符合支付卡行业数据安全标准(PCI DSS)。这些组织经常外包一些服务，PCI DSS 要求组织保证服务方也能遵守 PCI DSS。换言之，组织不能外包责任。

一些 SaaS 提供商通过云提供安全服务。例如，Barracuda Networks 提供基于云的解决方案，类似于下一代防火墙和 UTM 设备。例如，它们的网络安全服务为 Web 浏览器充当代理。管理员配置代理设置以访问基于云的系统，基于组织的需要进行网页过滤。类似的，还有基于云的 email 安全服务，能够执行入站垃圾邮件和恶意软件过滤。

10. 渗透测试

渗透测试是另一种预防性措施，组织可以用来应对攻击。渗透测试(通常简称为 pentest)模仿实际攻击，尝试确定攻击者会使用哪些技术绕过应用程序、系统、网络或组织的安全性，可能包括漏洞扫描、端口扫描、数据包嗅探、DoS 攻击和社会工程学技术。

当进行渗透测试时，安全专家会设法避免中断。但渗透测试有入侵性，可能会影响系统的可用性。因此，安全专家在执行任何测试之前，得到高级管理层批准是非常重要的。

注意：

NIST SP 800-115“信息安全测试和评估技术指南”中包括大量的关于测试的信息，也包括渗透测试。可以从 NIST 专门的下载网页 http://csrc.nist.gov/publications/PubsSPs.html 下载。

定期实施渗透测试是评价组织内部使用的安全控制是否有效的一个好方法。渗透测试可以揭示什么区域的补丁或安全设置不够，哪里的新漏洞被开发出来或已暴露，以及哪些安全策略是无效的或无法跟踪。攻击者可以利用这些漏洞。

渗透测试通常包括漏洞扫描或漏洞评估以发现漏洞。但是，渗透测试会更进一步，试图利用这些弱点。例如，漏洞扫描器会发现有后端数据库的网站没有使用输入验证技术，容易受到 SQL 注入攻击。然后，渗透测试会使用 SQL 注入攻击访问整个数据库。类似地，漏洞评估可以发现员工没有接受关于社会工程学攻击的教育，渗透测试可以使用社会工程学方法访问安全区域或从员工那里获取敏感信息。

这里列出了一些关于渗透测试的目标：

- 确定系统对于攻击有多高的容忍度
- 确定员工检测和实时响应攻击的能力
- 识别可实施以降低风险的额外控制

注意：

渗透测试通常包括社会工程学攻击、网络和系统配置检查以及环境漏洞评估。渗透测试采取漏洞评估和漏洞扫描，并进一步验证漏洞是否可以利用。

渗透测试的风险

对于渗透测试，一个值得注意的危害是有些操作可能会导致中断。例如，如果漏洞扫描发现基于网络的服务器易受缓冲区溢出攻击，渗透测试可以利用该漏洞，这可能导致服务器关闭或重启。

理想情况下，渗透测试应在造成实际损失之前停止。遗憾的是，测试人员往往直到进行某一步骤时才知道会导致损坏。例如，不认真的测试人员会给应用程序或系统发送无效或随机数据来检查响应，但直到运行这些数据时测试者才发现错误。经验丰富的渗透测试人员能够最大限度地减少测试造成损害的风险，但他们不能消除风险。

如果可能的话，测试人员会在测试系统而不是实时的生产系统上进行渗透测试。例如，当测试一个应用程序时，测试人员可以在孤立的环境中运行应用程序，然后在隔离的环境中测试应用程序。如果测试导致损坏，那么只会影响测试系统，不影响实时网络。面临的挑战是，测试系统往往不提供生产环境的真实视图。测试人员能够测试系统中不与其他应用程序交互的简单应用程序。当使用测试系统时，渗透测试人员通常发布一份测试资格声明，该声明中写明测试是在测试系统中进行的，所以结果可能无法提供对生产环境的有效分析。

获得渗透测试权限

经高级管理人员仔细审议和批准后才能进行渗透测试。许多安全专业人员坚持书面批准，并写明风险。执行未经批准的安全测试可能导致生产效率损失和触发应急响应。

故意违反 IT 环境安全性的员工将依法受到处罚。同样，如果内部员工在没有授权的情况下对系统进行非正式的测试，组织可能会将他们的行为视为非法攻击而不是渗透测试。这些员工很可能会失去工作，甚至可能面临法律后果。

渗透测试技术

组织聘请外部顾问进行渗透测试的情况很常见。组织可以控制给这些测试人员提供的信息，组织给予的信息的水平决定了其所要进行的测试类型。

注意：

第 20 章“软件开发安全”叙述了软件测试背景下的白盒测试、黑盒测试和灰盒测试。这些术语往往与渗透测试相关并表达相同含义。

零知识团队黑盒测试 除了公开可用的信息，如域名和公司地址之外，零知识团队不知道任何有关目标网站的信息。似乎他们将目标看成一个黑色的盒子，直到检测才知道盒子里是什么。零知识团队的攻击与真正的外部攻击极其类似，因为所有有关环境的信息必须从零开始。

全知识团队白盒测试 全知识团队可以访问目标环境的所有方面。他们了解所有安装的补丁和升级类型，以及所有相关设备的精确配置。如果目标是一个应用程序，他们将能访问源代码。全知识团队进行白盒测试(有时被称为水晶盒或透明盒测试)。白盒测试通常被认为能够更经济、有效地定位漏洞，因此发现漏洞所需的时间更短。

部分知识团队灰盒测试 对目标有部分但不全面了解的团队进行灰盒测试。他们可能会有网络设计及配置细节方面的相关信息，以便专注于特定目标的攻击和漏洞。

定期保护渗透测试目标的安全管理人员可以被认为是全知识团队。然而，他们不是执行渗透测试的最佳选择。他们往往有盲点，或在对特定安全问题的理解、估计和能力上有差距。如果他们知道一个漏洞会被利用，很可能就会提出一种控制方法以减少发生的可能性。全知识团队知道什么是安全的，所以可能无法依靠虚假的假设去正确地测试每一种可能性。零知识或部分知识团队不太可能犯这些错误。

渗透测试可以采用自动攻击工具和套件，或者手动使用普通的网络工具。自动攻击工具的范围包括从专业的漏洞扫描工具和渗透测试工具，到混乱的、在互联网上发现的地下工具。一些开源和商业工具(如 Metasploit 和 Core Impact)是可用的，安全专业人员和攻击者都使用这些工具。

渗透测试中经常使用社会工程学技术。根据测试的目标，测试人员可以使用技术来突破组织的物理边界或让用户泄露信息。这些测试有助于确定有缺点的员工如何被经验丰富的社会工程学攻击接近，并且也有助于让他们熟悉怎么阻止这些攻击类型的安全策略。

真实场景

渗透测试中的社会工程学

下面的例子是在一家银行进行的渗透测试，但许多不同的组织往往得出同样的结果。测试人员被特别询问了能否访问员工的用户账户或用户系统的问题。

渗透测试人员设计了一封伪造的电子邮件，使之看起来像是来自银行内部人员。它描述了一个网络问题，并要求所有员工尽快回复用户名和密码，以确保他们没有失去访问权限。超过 40%的员工做出了回应。

此外，测试人员在几台 USB 设备中安装了恶意软件并将它们“丢”在停车场和银行内部的不同位置。一名好心的员工看到了一个，并把它捡起插入到一台计算机上，想确定其所有者。然而，USB 驱动器却感染了用户的系统，为测试者提供了远程访问权限。

测试人员和攻击者经常成功地使用类似的方法。教育往往是缓解这些类型的攻击的最有效方法，并且渗透测试也常常强调相关知识教育的必要性。

防护报告

渗透测试人员将提供一份记录测试结果的报告，且该报告应被作为敏感信息而被保护。该报告将概述具体的漏洞，以及这些漏洞将如何被利用。它还经常包括对于如何缓解漏洞的建议。如果测试结果在组织采纳建议之前落入攻击者手中，攻击者将利用报告中的漏洞细节发起攻击。

另外我们还要认识到，渗透测试团队提出了一个建议，但这并不代表组织会采纳该建议。管理层有选择权，可以选择实施建议以减少风险，但如果他们认为成本太高不值得，也可以选择接受风险。换言之，去年的报告可能会列出一个没有被修补的漏洞。这份报告可能就像是昨天刚做完一样，问题还没有得到解决。

道德黑客行为

道德黑客经常被用作渗透测试的另一个名称。道德黑客指的是了解网络安全并知道如何破解安全性，却不利用该知识为自己谋利的人。相反，道德黑客使用这方面的知识帮助组织了解其漏洞并采取行动，从而防止恶意攻击。道德黑客将永远停留在法律允许范围内。

第 14 章“控制和监控访问”中提到了骇客、黑客和攻击者之间的技术差异。黑客的原始定义是指无恶意的科技爱好者，而骇客和攻击者却是有恶意的。黑客一词的原意已逐渐模糊，因为它常常作为攻击者的同义词使用。换言之，大多数人认为黑客就是攻击者，人们觉得道德黑客这个词本身就有矛盾。然而，道德黑客使用黑客的原始含义。

道德黑客将了解并经常同攻击者使用相同的工具。然而，他们不使用这些工具攻击系统。相反，他们使用工具测试系统漏洞，且只有在组织授予他们明确许可时才做测试。

17.3　日志、监控和审计

日志、监控和审计程序有助于组织防止事件发生，并能够在事件发生时做出有效响应。下面的章节将叙述日志和监控等内容，以及用于评估访问控制的有效性的各种审计方法。

17.3.1　日志和监控

日志将事件记录到各种日志中，并监控这些事件。联合、日志和监控体系使得组织能够追踪、记录和审查活动，提供完全的可问责性。

这有助于组织检测可能会对系统机密性、完整性和可用性产生负面影响的不良事件，也有助于在事件发生后重建活动，以确定发生了什么，有时能够为起诉相关负责人员提供证据。

1. 日志技术

日志记录是将事件的信息记录到日志文件或数据库的过程。日志记录捕获的事件、变更、信息通知和其他数据能够描述系统上发生的活动。日志通常会记录细节，如发生了什么事、在什么时候、在哪里、谁做的，有时还记录事件是如何发生的。当需要寻找最近发生的事件时，系统日志是个很好的开始。

例如，图 17.5 显示了微软服务器上的事件查看程序，一些日志条目已被选择和扩展。此日志条目显示一位名为 Darril 的用户在名为 SQL1 的服务器上删除了位于 C:\CISSP Study Notes 目录下的一个名为 CISSP Study Note 的文件夹。它还显示 Darril 在 7 月 14 日上午 10:30 删除了该文件。

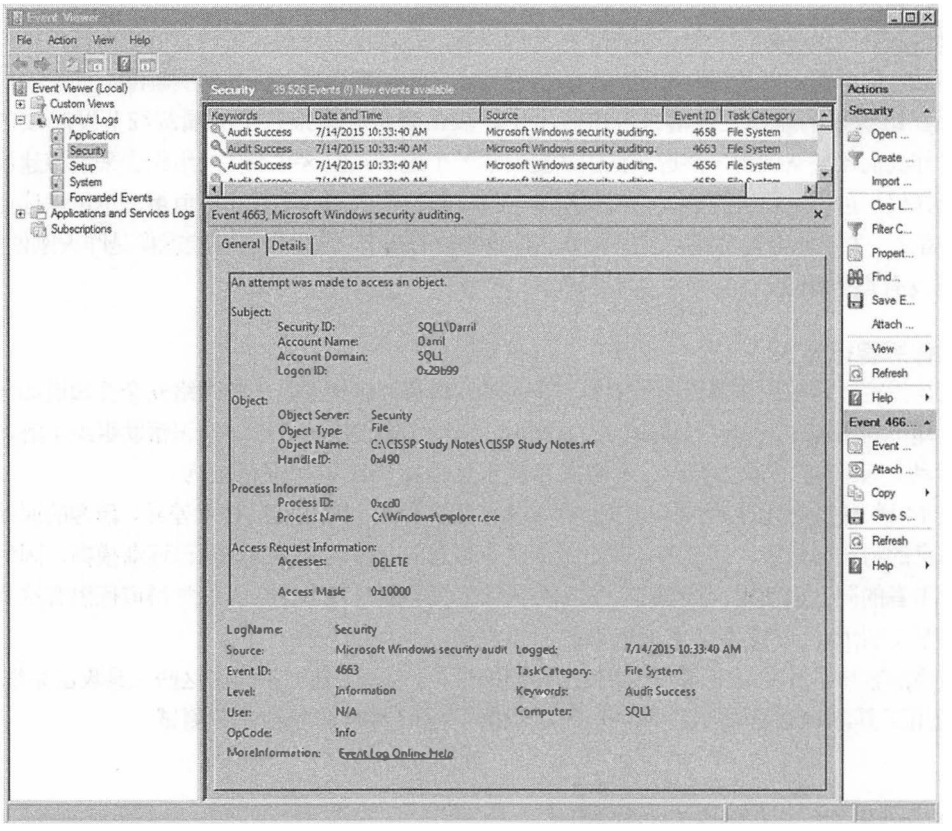


图 17.5　查看日志条目

只要身份识别和认证过程是安全的，Darril 就有权删除文件。另一方面，如果组织不使用安全认证流程，就很可能有其他人冒充另外的用户，Darril 可能面临错误指控。安全识别和认证实施作为可问责性的先决条件，如有要求便需要加强。

注意：

日志通常被称为审计日志，而日志记录通常被称为审计日志记录。然而，我们要认识到：审计(在本章后面会有叙述)不仅仅是日志记录。日志记录是记录事件，而审计会检查所处环境。

2. 通用日志类型

有许多不同类型的日志。下面是一个在 IT 环境中常见日志的短列表。

安全日志　安全日志能够记录对一些资源的访问，如文件、文件夹、打印机等。例如，当用户访问、修改或删除文件时，安全日志能够记录下来，如图 17.5 所示。许多系统能够自动记录对关键系统文件的访问，但需要管理员在登录访问之前启用对其他资源的审计。例如，管理员可能会为专有数据配置日志记录，但不会对发布在网站上的公共数据进行配置。

系统日志　系统日志记录类似于系统或服务器的开启或关闭等事件。如果攻击者能够关闭系统

并使用 CD 或 USB 闪存驱动器将其重启，他们就可以从系统中窃取数据而不留下任何访问记录。同样，如果攻击者能够将正在监视系统的服务停止，他们就可能能够在不产生任何行动日志的情况下访问系统。能够检测出系统重启或服务停止的日志有助于管理员发现潜在恶意行为。

应用程序日志　这些日志记录特定应用程序的信息。应用程序开发人员能够选择要在应用程序日志中做出记录的程序。例如，开发人员可以设置在任何人访问特定的数据对象(如表或视图)时，日志做出记录。

防火墙日志　防火墙日志可以记录与到达防火墙的流量相关的任何事件，包括防火墙允许的流量和阻止的流量。这些日志通常记录主要的数据包信息，如源和目的 IP 地址、源和目的端口，但不记录数据包的实际内容。

代理日志　代理服务器为用户提高了互联网访问性能，并可以控制用户访问的网站的范围。代理日志有记录详细信息的功能，如特定用户访问了哪些网站，以及他们浏览网站花费了多长时间。当用户试图访问已知的禁止访问的网站时，代理日志也能够做出记录。

变更日志　作为整体变更管理过程的一部分，变更日志能够记录变更请求、批准和系统的实际变更。跟踪被批准的变更是很有益处的。作为灾难恢复计划的一部分，变更日志仍大有益处。例如，发生故障之后，灾难管理员或技术人员可以使用变更日志将系统还原，其中包括所有应用的变更。

日志记录通常是操作系统中的本地功能，并用于大多数应用程序和服务。这使得管理人员和技术人员能够相对容易地配置系统来记录特定类型的事件。特权账户的事件，如管理员和根用户账户，应包含在任何日志记录计划中。这有助于防止恶意内部人员的攻击，并能够在必要时提供起诉的活动文件。

3. 保护日志数据

组织内部人员可以使用日志来重新创建事件，但前提是日志没有被修改。如果攻击者可以修改日志，他们便能够擦除自己的活动痕迹，有效地清除有价值的数据。文件便不再含有准确的信息，也不能作为起诉攻击者的证据。所以，保护日志文件免受未授权的访问和修改是很重要的。

在中央系统上存储日志的副本来保护日志的方法很常见。即使攻击者修改或破坏了原始文件，工作人员也仍然可以使用副本查看事件。保护日志文件的一个方法是通过指定权限来限制他们的访问权。

对于实施日志文件备份的组织通常都有严格的管理策略。此外，这些策略都规定了备份保留时间。例如，组织可能会将归档日志文件保存一年、三年或更长时间。一些政府法规要求组织无限期地保存归档日志。能够设置日志只读模式、分配权限、实施物理控制的安全控制可以保护归档日志免受未授权的访问和修改。当不再需要日志时，应及时销毁。

提示：

组织有法律经验的话，就会意识到对不必要日志的过度保存会导致劳动成本的过度使用。例如，如果法规要求组织保存一年内的日志，而组织却保存了十年，法院在检查时就会要求相关人员检索这十年内日志中的相关数据。相比之下，如果组织只保存了一年的日志，相关人员只需要在这一年的日志中检索有价值的信息，这会显著减少所需的时间和精力。

美国国家标准与技术研究所(NIST)发表了大量的与 IT 安全问题相关的信息，包括联邦信息处理标准(FIPS)出版物。联邦信息和信息系统(FIPS 200)的最低安全要求中明确指明了以下信息为审计数据的最低安全要求：

- 建立、保护和保留信息系统审计记录，以使监测、分析、调查和报告非法的、未授权的或不适当的信息系统活动的需求范围扩大。
- 确保个人信息系统用户的行为能够被唯一地追踪到这些用户，以便他们能够为自己的行动负责。

注意：

在准备 CISSP 考试时，你会发现复习 NIST 文件是很有帮助的。对于不同的安全概念，它能为你提供更全面的信息。这些信息都是免费的，下面是网址：http://csrc.nist.gov。也可以点击下面这个网址来下载 FIPS 200 文件：http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf。

4. 角色监控

监控功能为组织带来了很多好处，比如增加可问责性、帮助调查、提供基本的故障排除方法。下面将更深入地描述这些好处。

监控和可问责性

监控是一个必要的功能，能够确保受监控者(如用户和员工)可以对他们的行动和活动负责。用户提供身份(如用户名)并证明自己的身份(通过认证)，然后审计跟踪系统就会在其登录时记录活动。监控和审计跟踪日志使得用户能够承担相应责任。

这直接促进用户的积极行为并能使其遵守组织的安全策略。意识到日志能够记录活动信息的用户，不大可能会尝试绕过安全控制或执行未授权或受限制的活动。

一旦发生违反安全策略的事件，应确定违规的来源。如果确定是个人责任，他们应该依照组织的安全策略承担相应的责任。如果事件严重，可能会终止劳动合同或进行法律起诉。

立法往往需要具体的监督和可问责实践。这包括许多组织都必须遵守的法律，如 2002 萨班斯-奥克斯利法案、健康保险流通与责任法案(HIPAA)和欧盟的隐私法律。

真实场景

监控活动

从一线步兵到监控日常运作的高级指挥官，对于每个层面的业务工作来说，可问责都是相当必要的。如果不对用户及其活动，或者系统中的应用程序进行监控的话，就无法实现可问责性。

Duane 是一家石油钻井数据挖掘公司数据录入部门的质量安全主管。在日常工作中，他能够看到许多敏感文件，其中包括有价值的信息，这些信息可以帮助 Duane 从那些对这些数据感兴趣的人那里获得不菲的小费。他也会纠正一些可能会导致客户严重不满的错误，有时候，一个小的错误就会给客户的整个计划带来非常严重的问题。

Duane 在其工作站中接触或转发这类信息时，就会留下电子追踪证据。他的主管 Nicole，能够使用该线索检查 Duane 的操作是否是在被监控的情况下进行的。她可以在 Duane 访问或修改敏感信息时，监控到 Duane 从哪里获得信息，并将其放置到哪里，同时还能监控到信息从信息源到客户端之间的处理过程。

这种可问责性能够为公司提供保障，以免 Duane 滥用信息。同时也能保护 Duane，以防他人指控自己滥用数据处理职能。

监控和调查

审计跟踪系统使得调查人员在发生事件之后能够对其进行重建。它们可以记录访问权限的滥用、特权侵犯、试图入侵和许多不同类型的攻击。在检测到安全冲突后，通过对审计追踪信息进行检查，安全专业人员可以重建导致事件的条件和系统状态。

确保日志有准确的时间戳很重要，这些时间戳在整个环境中需要保持一致。常用的方法是建立一台内部的网络时间协议(Network Time Protocol，NTP)服务器，该服务器是同步的可信时间源，如公共 NTP 服务器。其他系统可以用此内部 NTP 服务器同步时间。

注意：

系统应保持时间与一台集中或受信任的公共时间服务器同步，这确保所有的审计日志记录事件的准确性和时间的一致性。

监控和问题识别

审计跟踪为管理员提供了一些有用的、与事件相关的详细信息。它们可以记录系统故障、操作系统错误和软件错误，还有恶意攻击。一些日志文件甚至可以捕获应用程序或系统崩溃时内存的内容。这些信息可以帮助查明事件的原因，如果确认是攻击的话，信息还能够帮助消除威胁。例如，如果系统由于内存不足而崩溃，崩溃转储文件可以帮助诊断问题。

为此而使用日志文件通常被称为问题识别。一旦确定了问题，执行解决问题的步骤则需要更多的信息。

5. 监控技术

监控是一种检查信息日志并寻找具体某些细节的过程。工作人员可以手动查看日志，或使用工具来自动处理过程。监控是必要的，以检测恶意行动，以及入侵和系统故障。还可以帮助重建事件，提供起诉证据，并创建分析报告。

日志分析是监测过程中一种详细且系统化的模式，日志分析能够分析监测记录信息的趋势、模式，还能够分析未授权的、非法的、违反策略的活动。日志分析不一定是对事件的响应，而是一项周期性的任务，可以检测潜在的问题。

当手动分析日志时，管理员只需打开日志文件，并查找相关数据。即使使用一些工具，这项工作也是非常烦琐和耗时的。例如，在特定的事件或身份代码中搜索 10 个不同的存档日志会花费很多时间，即便是在使用内置搜索工具的前提下。

在许多情况下，日志产生了太多的信息，以至于重要的细节会丢失，因此管理员经常使用自动化工具来分析日志数据。例如，入侵检测系统(IDS)积极监视多个日志来检测和响应实时的恶意入侵。入侵检测系统可以帮助检测和跟踪来自外部攻击者的攻击，向管理员发送警报，并记录攻击者对资源的访问。

多个供应商销售运营管理软件，积极监控整个网络系统的安全性、健康度和性能。该软件寻找能指明问题的可疑或异常活动，如攻击或未授权的访问。

安全信息和事件管理

许多组织使用集中式应用程序来自动监控网络上的系统。有些术语被用来描述这些工具，包括安全信息和事件管理(Security Information and Event Management，SIEM)、安全事件管理(Security Event Management，SEM)和安全信息管理(Security Information Management，SIM)。这些工具为组织

提供了对系统事件的实时分析。它们具有安装在远程系统上的代理，能够监控特殊事件，被称为触发器。一旦触发警报，代理会将事件报告给中央监控软件。

例如，SIEM 可以监视一组电子邮件服务器。每一次邮件服务器记录事件时，SIEM 代理就会检查该事件以确定它是否和利益有关。如果有关，SIEM 代理会将事件转发到中央的 SIEM 服务器，并根据事件的严重性，依次提高向管理员发出的警报程度。例如，如果电子邮件服务器的发送队列开始备份，SIEM 应用可以检测问题，并在问题变得严重之前，提醒管理员。

大多数的 SIEM 软件都是可配置的，使得组织内部人员能够指定哪些项和利益相关，需要转发给 SIEM 服务器。SIEM 软件几乎有所有服务器和网络设备的代理，在某些情况下，它们能够监控网络流量，提供趋势分析。该工具还可以从目标系统收集所有的日志，并使用数据挖掘技术来检索相关的数据。安全专业人员可以创建报告和分析数据。

一些监控工具也能用于库存及状态方面。例如，一些工具可以查询所有可用的系统和文档的详细信息，如系统名称、IP 地址、操作系统、安装补丁、更新和已安装的软件。这些工具可以根据组织的需要创建系统报告。例如，它们可以确定有多少系统是活跃的，识别系统与未打的补丁，标志有未授权软件安装的系统。

软件监控程序能够监控企图安装或未批准而安装的软件，或未授权软件的使用，或未授权使用合法软件。这样就降低了用户在不经意间安装病毒或木马的风险。

审计跟踪

审计跟踪指的是一些记录，它们在关于事件和突发事件的信息被存储在一个或多个数据库或日志文件中时被创建出来。审计跟踪提供了系统活动的记录，并可以重建导致安全事件的活动。安全专家提取事件的审计线索来证明或反驳责任信息。审计跟踪允许安全专家检查和跟踪事件的正向或反向顺序。当跟踪问题、性能问题、攻击、入侵、安全漏洞、编码错误和其他潜在的策略违规行为时，这种灵活性是很有帮助的。

提示：

审计跟踪提供了全面的系统活动记录，并且可以帮助检测各种各样的安全违规行为、软件缺陷和性能问题。

使用审计跟踪是一种被动的检测性安全控制形式。与闭路电视或保安人员所起的作用一样，审计跟踪只是作为一种威慑手段。如果攻击者知道他们正受到监视，并且他们的活动也被记录下来，那么他们从事违法的、未授权或恶意活动的可能性就会减小(至少理论上是这样，但是某些罪犯要么粗心、要么无视这些措施)。

在起诉罪犯时，审计跟踪也是重要的证据。审计跟踪通常被用于生成资源、系统和资产状态前后对照的镜像。这反过来有助于标识所发生的变化或改变是否由用户的行为、操作系统或软件行为造成，或者是否由其他一些原因(例如，硬件故障)引起。

抽样

抽样或数据抽取是为了构建有意义的整体表示法或概述，而从大量的数据中提取元素的过程。换句话说，抽样是一种数据简化形式，允许审计人员快速地从审计跟踪中确定重要的问题或事件。

使用精确的数学函数从大量数据中抽取有意义信息的审计工具，执行的是统计学抽样。这与进行民意测验时使用的方法一样，不是采访每个人。抽样数据不能准确表示整个数据主体，以至于误

导审计人员和管理人员的风险总是存在，并且统计学上的抽样可以被用于衡量风险。

阀值级别

阀值是一种非统计抽样。它只选择超过阀值平均值的事件，阀值平均值是事件的预定义阈值。事件达到此阈值，系统就会忽略该事件。

例如，登录失败在系统中很常见，因为用户会轻易地输入错误密码一两次。阀值平均值能够设置成只有在 30 分钟内有 5 次或 5 次以上失败登录时才会发出警报，而不是每一次失败登录都报警。许多账户锁定控件使用类似的阀值级别。在一次登录失败后不会将账户锁定。相反，只有在失败登录次数达到预定义的阈值时才锁定账户。

阀值级别被广泛地用在审计事件的过程中，从而建立例行系统或用户行为的基线。如果超过了这条基线，那么就会触发异常事件的警报。换句话说，阀值级别引起系统忽略例行事件，而当监测到严重的入侵行为时，触发报警。

另外，阀值级别往往与名为违规分析的主框架审计形式相关联。在属于较早审计形式的违规分析中，环境中出现的错误会受到监控。错误的基线是预期的和已知的，这种常见错误的级别被标记为阀值级别。超过阀值级别门限而触发违规的任何错误，以及这种事件的相关细节都会被记入违规记录，以便稍后进行分析。

大体上来说，非统计抽样是任意抽样或取样，审计程序有自由裁定权。不提供整体数据的精确值，并将忽略未达到阈值级别的事件。然而，当用于特定事件时，该方法却是很有效的。此外，非统计抽样比统计抽样更便宜、更容易实现。

注意：

统计学意义上的和非统计学意义上的抽样，都被认为是生成大量审计数据主体的概况或归纳的有效机制。不过，统计学意义上的抽样更为可靠和精确。

其他监控工具

虽然日志是审计使用的主要工具，但在组织中也会使用一些额外的工具。例如，闭路电视(CCTV)可以自动将事件记录到磁带上供以后查看。安全人员也可以通过闭路电视实时监控系统的不必要的、未经批准的或非法的活动。该系统可以单独工作或与安全警卫合作，他们由闭路电视监控，并对任何非法或不道德的活动负责。防止数据丢失的工具包括按键监控、流量监控分析、趋势分析和监测监控。

击键监控　击键监控是记录用户在物理键盘上进行击键的行为。记录行为可以通过技术方式(如硬件设备)或软件方法(如键盘记录器)进行。无论如何，视频录屏能执行可视化监控。在大多数情况下，击键监控用于恶意的目的。只有在极端环境中和高度安全的环境中，击键监控实际上才作为一种审计和分析用户键盘操作活动的方法。

击键监控经常被比作搭线窃听。对于击键监控是否应该与电话窃听一样采取相同的限制和控制方式，目前还存在一些争论。许多使用击键监控的组织都通过雇用协议、安全策略和登录区域的警告标题来通知经过授权和未授权的用户存在这样的监控措施。

注意：

公司确实能够以一些原因利用击键监控，但是通常必须通知被监控的员工。

流量分析和趋势分析　流量分析和趋势分析都是监控的形式，它们对数据包的流(而不是数据包

的实际内容)进行检查。这有时被称为网络流量监测。使用流量分析和趋势分析可以对大量的信息进行推断，如主通信路径和备份通信路径、主服务器的位置、网络支持的通信流量、数据流的特有方向、通信的频率等。

这些技术有时可以揭示可疑的流量模式，例如，如果一名员工的账户发送大量的电子邮件给别人，就可能表明该员工的系统是由远程操作的攻击者控制的僵尸网络的一部分。同样，如果有内部人员通过电子邮件的方式将内部信息转发给未授权的人，流量分析程序也会发现这类行为。这些类型的事件通常会留下可检测的签名。

17.3.2 出口监控

出口监测是指监测传出的流量，以防止数据泄露，也就是防止组织数据的未授权传输。防止数据泄露的一些常见方法有：使用数据丢失防护技术，寻找隐藏的企图，以及利用水印检测未经授权的数据。

1. 数据泄露保护

数据丢失防护(Data Loss Prevention，DLP)系统能够检测和阻止数据泄露的企图。这些系统有扫描数据、寻找关键字和数据模式的能力。例如，假如组织使用机密的、专有的、私有的和敏感的数据分类，DLP 系统可以扫描文件来寻找这些关键字并检测。

模式匹配的 DLP 系统寻找特定的模式。例如，美国的社会安全号码是 nnn-nn-nnnn 模式(3 个数字、破折号、两个数字、破折号、4 个数字)。DLP 可以寻找这种模式并检测。管理员可以设置 DLP 系统以根据自己的需要，寻找任意模式。

DLP 系统有两种主要类型：基于网络的 DLP 和基于终端的 DLP。

基于网络的 DLP 基于网络的 DLP 扫描所有网络输出数据以寻找具体的数据。管理员会把它放在负边缘以扫描所有从组织传输出去的数据。如果有用户发送了一个含有限制数据的文件，DLP 系统将检测并阻止该文件从组织发出。DLP 系统会发出警报，比如向电子邮件管理员发出警报。

基于终端的 DLP 基于终端的 DLP 可以扫描存储在系统中的文件以及发送到外部设备的文件，如打印机。例如，基于终端的 DLP 可以防止用户复制敏感数据到 USB 闪存驱动器或发送敏感数据到打印机。管理员可以给 DLP 配置适当的关键字以扫描文件，如果在文件中检测到这些关键字，将阻止复制或打印。也可以配置基于终端的 DLP 系统，使其定期扫描文件(如文件服务器)，以确定是否存在包含特定关键词或图形的文件或未经授权的文件类型，如 MP3 文件。

DLP 系统通常具备进行深层次检查的能力。例如，如果用户将文件压缩成 zip 压缩文件，DLP 系统仍然可以检测到关键词和模式。然而，DLP 系统没有解密数据的能力。

在过去，基于网络的 DLP 系统阻止过重大违规事件。例如 2014 年的索尼攻击，攻击者从索尼员工那里偷得 25GB 以上的敏感数据，包括社会安全号码、医疗和工资信息。如果攻击者在检索之前不对数据进行加密处理，DLP 系统可以检测到在网络上试图传递出来的数据。然而，值得一提的是，高级持续性威胁(比如经 Mandiant 认证的 APT1)在发送之前都对数据进行了加密处理。

2. 隐写术

隐写术指的是在文件中嵌入消息。例如，个人可以通过修改图片文件内的位数来嵌入消息。这种变化对观看图片的人来说是潜移默化的，但如果其他人知道并想要寻找其中的信息，便可以进行

提取。

然而，如果怀疑一个文件有隐藏信息，且有该文件的源文件，就可以检测隐写术。如果使用散列算法，如 MD5 哈希值，就可以为两个文件创建哈希值。如果哈希值是相同的，就说明该文件没有隐藏的信息。然而，如果哈希值是不同的，就表明第二个文件已被修改。Forensic 分析技术能够检索到信息。

在出口监控的背景下，组织可以定期检测很少变化哈希值的内部文件。例如，图形文件(如JPEG和GIF文件)的哈希值通常保持不变。如果安全专家怀疑有内部员工将额外的数据信息嵌入这些文件，并以电子邮件的形式发给其他组织，安全专家便比较原始文件和内部员工发出的文件的哈希值。如果哈希值不同，就说明文件是不同的，可能包含隐藏信息。

3. 水印

水印指的是在纸上嵌入不容易感知的图像或图案，经常被用来防止伪造货币。同样，组织经常使用含数字水印的文件。例如，敏感文档的作者可以用“机密”或“私有”等适当的分类字样来标记它们。任何使用或打印敏感文件的工作人员都能很轻松地分辨它们。

从出口监控的角度来看，DLP 系统能检测到水印。当 DLP 系统从这些水印中识别出敏感数据时，就可以阻止传输并向安全人员发出警报。这样就防止了组织文件的泄露。

数字水印是一种比较先进的水印。数字水印是一种在数字文件中秘密嵌入的标记。例如，一些电影公司对发送给不同分销商的电影嵌入数字水印。每个副本都有一个不同的标记且可以追踪哪个分销商收到了哪份副本。如果有分销商发行盗版电影，制片商便能够确定是哪家分销商。

17.3.4　审计和评估有效性

许多组织都有强大且有效的安全策略。然而，有策略并不意味着工作人员了解或遵守策略。许多时候，组织将会通过审计环境的方式评估其安全策略和相关的访问控制。

审计是对环境有条理地进行检查或审查，目的是确保符合法规，并且还能够检测异常、未授权的事件或犯罪。审计验证了部署在环境中的安全机制是否能够提供足够的安全性。测试过程确保工作人员遵循由安全策略或其他规则制定的要求，并且在部署的安全解决方案中不存在重大漏洞或弱点。

审计人员负责测试和验证安全策略或法规的具体落实过程和程序，并通过检查使它们能够满足组织的安全要求。他们还验证工作人员是否遵循这些过程和程序。总的来说，审计人员执行审计。

审计

术语“审计”在 IT 安全性背景下有两种不同的含义，所以认识这两种含义间的差异是很重要的。

首先，审计是指利用审计日志和监控工具来跟踪活动。例如，当任何用户访问文件时，审计日志可以做出记录，并记录用户的使用过程。

其次，审计也指检查或评估。具体来说，审计是对特定过程或结果的检查或评价，用以确定组织是否遵循特定的规则或准则。

这些规则可能来自于组织的安全策略或外部法律和法规。例如，安全策略可能会规定在员工被解雇之后，应尽快禁用其非活动账户。审计可以检查非活动账户，甚至验证账户被禁用的准确时间是否与员工被解雇的时间相同。检查审计可以在内部进行，也可以由外部审计师进行，他们经常将审计和监控活动创建的日志作为评估过程的一部分。

1. 检验审计

安全 IT 环境很大程度上依赖于审计，将其作为一种检测安全控制来发现和纠正漏洞。本书中访问控制的两个重要审计分别是访问审查审计和用户权限审计。

明确并坚持审计频率是很重要的。组织通常按照风险的大小来决定安全审计的频率。对组织财产的漏洞和威胁进行人工评估，以确定整体风险水平，这有助于组织调整审计费用并决定审计频率。

提示：

审计需要成本和时间，审计的频率与风险有关。例如，潜在的滥用或破坏特权账户比误用或破坏普通账户的风险更大。所以，安全人员执行对特权账户的用户权限审计的频率要高于普通用户。

同其他部署和维护安全的方式一样，安全审计通常被视为维护的关键要素。如果高级管理层未能执行定期的安全审计，那么利益相关方将追究他们的责任，并要求他们承担所有因安全漏洞或策略违规问题而造成的资产损失。不执行审计，就意味着管理层没有履行监察责任。

2. 访问审查审计

许多组织定期进行访问审查和审计，以确保访问对象和账户管理符合安全策略要求。这些审计能够检查用户，确保他们没有过多的权限，并能够适当地管理账户。它们确保安全流程和程序都正常运行，人员会对它们进行跟踪。

例如，对高度有价值数据的访问范围应只限于需要数据的用户。访问审查审计能够验证数据是否已经分类，且用户是否已经知晓分类。此外，将确保任何被授权访问数据的人知道是什么使得他有权访问这些数据。例如，如果一名服务台的专业人员能够被授权访问高级别的分类数据，那么他需要知道是什么使他有资格获得该级别的访问权。

当检查账户管理实践情况时，访问审查审计将根据最佳的实践情况和安全策略来确保账户被禁用或删除。例如，如果员工被解雇，其账户应该尽快被删除。典型的离职策略通常包括以下元素：

- 面谈过程中至少有一个见证人
- 面谈过程中账户被禁用
- 面谈中或面谈后立即收回员工身份徽章和其他凭据物件，如智能卡
- 面谈后立即护送员工离开

访问审查能够验证策略是否存在且验证人员是否正在对其进行追踪。当被解雇的员工在离职后继续访问网络时，就很容易给公司带来损失。例如，管理员可以创建一个单独的管理员账户，即使管理员的原始账户被禁用，也可以使用它来进行访问。

3. 用户权限审计

用户权限是指授予用户的特权。用户需要权利和权限来完成工作，但他们只需要有限数量的特权。在用户权限的背景下，最小特权原则能够确保用户只有他们所需要的用于完成工作的权限，并且没有更多其他权限。

虽然访问控制试图执行最小特权原则，但有些时候，用户会被授予过多的特权。当用户有过多的特权时，用户权限审查能够发现这违反了有关用户权限的安全策略。

4. 特权组审计

许多组织将小组作为基于身份的访问控制模型的一部分使用。限制这些小组中的成员是很重要的。同样重要的是还要确保小组成员只有在必要时才使用他们的高特权账户。审计可以帮助确定这些人员是否遵循这些策略。

5. 高级别管理组

许多操作系统都有特权组，如管理员组。管理员组通常被授予系统的全部权限，当用户账户被放置在管理员组中时，用户就有了这些特权。所以，用户权限审计将经常审查所有特权组的成员，包括不同的管理员组。

一些组有很高的特权，以至于即使是拥有成千上万用户的组织，极高特权组中的成员数量也是很小的。例如，微软域管理有一个企业管理组。这个组中的用户可以在微软森林体系(一组相关域)的任何域上做任何事情。这个组的权利相当高，以至于只有两个或三个高层次的管理人员有访问权。监测和审计组中的成员能够发现添加到该组中的未授权的人。

可以使用自动化的方法来监视特权账户成员，未授权添加用户将会失败。审计日志也将记录此操作，且权限审计能够检查这些事件。审计人员可以检查审计线索，以确定是谁试图添加未授权的账户。

拥有高特权的员工也可以创建其他组。例如，管理员可以给 IT 部门的一些用户创建 IT 管理员组。基于工作需求，这些管理员将会被授予适当的特权，并将其账户放入 IT 管理员组中。只有来自 IT 部门的管理员能够进入组，用户权限审计能够检查是否有其他部门的用户在组中。IT 部门的管理人员应该在组内，用户权限审计可以验证其他部门的用户不在组内。这是一种检测蠕变特权的方式。

注意：

用户权限审计也可以检测当用户不需要时，进程是否能够正常删除其特权，同时也能检测到工作人员是否遵守该过程。例如，如果一个管理员被转岗到组织的销售部门，这个管理员就不应该再拥有管理权限。

6. 双重管理员账号

许多组织要求管理员拥有两个账户。一个账户作为日常使用，另一个账户拥有额外的特权，管理员使用该账户从事管理工作。这减少了特权账户的相关风险。

例如，如果恶意软件在用户登录时感染了系统，恶意软件便可以使用该账户的特权。如果用户登录特权账户，恶意软件便有特权。然而，如果管理员只用工作时间的十分之一使用管理员账户执行特权，那么登录特权账户被恶意软件感染的可能性便会减小。

审计可以验证管理员是否适当地使用特权账户。例如，组织能够估算出管理员在全天中只需要十分之一的时间来使用特权账户，并在其他时间使用普通账户。日志分析可以验证估计的准确性，以及管理员是否遵循了该原则。如果管理员经常使用管理员账户，很少使用常规的用户账户，审计能够对该明显违规行为做出标记。

同样，管理员账户需要等级更高的密码。策略中可以明确规定普通账户的密码长度至少为 8 个字符，而管理员账户的密码长度最少为 15 个字符。密码破解工具可以尝试破解管理员账户的密码，以验证管理员使用的是高级别密码。

7. 安全审计和审查

安全审计有助于帮助组织确定正确实现了安全控制。访问审查审计(本章前面有所介绍)能够评估访问控制的有效性。这些审查确保账户管理适当，没有过多的权限，并在需要时会被禁用或删除。在安全操作域的上下文中，安全审计有助于确保管理控制到位。下面的列表包括一些需要检查的常见条目：

补丁管理 补丁管理审查能够在补丁发布后，尽可能快地对其进行评估。它还确保组织遵循既定的程序来评估、测试、批准、部署和验证补丁。在补丁管理审查或审计中，漏洞扫描报告是很有价值的。

漏洞管理 漏洞管理审查能够确保漏洞扫描和评估按照既定的准则定期执行。例如，组织可能有一份策略性的文件，指出漏洞扫描至少每周进行，并对其进行审查核实。此外，审查将验证在扫描中发现的漏洞问题已经得到解决。

配置管理 系统可以定期进行审核，以确保原始配置不被修改。通常可以使用脚本工具来检查系统的特定配置，并在发生变更时进行确定检查。此外，日志记录可以为许多配置设置记录配置变更。配置管理审计可以检查任何变更的日志，并验证变更是否经过授权。

变更管理 变更管理审计能够确保变更符合组织的变更管理策略。其中通常包括中断审查以确定原因，由未授权变更导致的中断意味着变更管理程序需要改进。

8. 报告审计结果

组织使用的审计跟踪报告在格式上有很大不同。然后，报告中必须列出一些基本的概念或核心概念：

- 审计目的
- 审计范围
- 审计发现或揭示出的结果

除了这些基本概念，审计报告往往包括许多特定于环境的细节，如时间、日期和被审计系统的列表，主要包括如下内容：

- 问题、事件和状态
- 标准和基线
- 诱因、原因及产生的影响和效果
- 推荐的解决方案和保障措施

审计报告应该有清晰、简洁和客观的结构或设计。虽然审计师通常会提出意见或建议，但他们必须明确它们。实际调查结果应以审计记录和其他证据中收集的证据和事实为依据。

9. 保护审计结果

审计报告通常包含敏感信息。它们应该被分配一个分类标签，只有那些有足够特权的人能够访问审计报告，包括高层次的管理人员和参与创建报告或负责更正报告中涉及条目的安全人员。

审计人员有时会为其他人员创建一份独立的审计报告。这份修改后的报告只提供与目标人员相关的细节信息。例如，高级管理人员不需要知道审计报告的所有细节。因此，针对高级管理人员的审计报告更为简洁，更多是提供了调查结果的概述或总结。负责纠正问题的安全管理员的审计报告应该是非常详细的，包括事件的所有详细信息。

另一方面，审计师执行审计往往是公开的。这使得员工了解到，高级管理人员正积极地采取措施维护安全。

10. 发布审计报告

审计报告完成后，审计人员将按照安全策略文档中的规定，将报告提交给指定的收件人。给文件签署确认收据是很常见的。当审计报告包含有关严重的安全违规或性能问题的信息时，就需要升级到更高层次的审查管理，并通知相关人员解决问题。

11. 使用外部审计师

许多组织选择聘请外部安全审计师进行独立审计。此外，一些法律和法规规定组织需要进行外部审计。外部审计提供了内部审计所不能提供的客观评价，相较于内部的策略、做法和程序，外部审计能够提供新的视角。

注意：

许多组织聘请外部安全专家来对他们的系统进行渗透测试。这些渗透测试有助于组织确定漏洞并判断攻击者如何利用这些漏洞。

外部审计师可以访问公司的安全策略并被授权检查 IT 和物理环境的某些方面。因此，审计师必须值得信赖。审计活动的目标是获得含有详细调查结果和建议对策的报告。

在某些情况下，外部审计会花费很多时间——几周或几个月。在审计过程中，审计师可以发布临时报告。临时报告是一份书面或口头报告，能够给组织提供在审计过程中观察到的需要立即加以关注的弱点或策略/程序的不匹配状况。当问题严重到不能等到最终报告一起汇报时，审计师可以发布临时报告。

审计师一旦完成的审计调查，通常会召开退出会议。审计师会在会议上陈述审计中发现的问题，并对问题进行讨论，以寻找解决办法。然而，只有到会议结束，审计师退出之后才会向组织提交最终的审计报告，以保证审计报告不受组织的策略及强制措施干扰。

组织收到最终的审计报告后，内部审计人员对其进行审查，并根据报告向高级管理层提出建议。高级管理层负责选择哪些建议能够采纳，并由内部工作人员实施建议。

17.4　本章小结

CISSP CIB 列出了 6 个具体的事件响应步骤。检测是第一步，可以根据自动化工具或员工的建议执行。工作人员调查警报，以确定是否实际发生了安全事件，如果发生了，下一步是响应。在缓解阶段，遏制事件进一步恶化是很重要的。在应对处理事件的整个过程中，保护证据也是很重要的。根据有关法律或组织的安全策略，很可能需要填写报告。在恢复阶段，系统需要恢复到能够完整地进行操作的阶段，确保系统恢复到攻击发生之前的一个较为安全的状态也是很重要的。整理阶段往往会对问题的根本原因进行分析，且常常包括相应的预防措施。最后，吸取经验教训阶段会对事件及应对措施进行反思，以寻找是否有可以吸取的任何经验教训。

有几个基本步骤可以防止许多常见的攻击。它们包括保持系统和应用程序更新补丁，删除或禁用不必要的服务和协议，使用入侵检测和防御系统，使用含最新签名的反恶意软件，并启用基于主

机和基于网络的防火墙。

拒绝服务(DoS)攻击阻止系统处理或响应对合法服务的请求，常常通过互联网攻击系统。SYN 泛洪攻击能够破坏 TCP 三次握手过程，并且这在现今是很常见的，而其他的攻击往往是在旧的攻击方式上稍作改进。僵尸网络通常被用于分布式 DoS(DDoS)攻击。零日漏洞是以前未知的漏洞。以下基本预防措施有助于防止零日漏洞攻击。

像入侵检测系统这样的自动化工具能够使用日志来监视环境，并检测正在发生的攻击。一些工具还可以自动阻止攻击。IDS 使用的检测方法有两种：基于知识的 IDS 和基于行为的 IDS。基于知识的入侵检测系统使用攻击签名的数据库进行检测，但检测不到新的攻击方式。基于行为的入侵检测系统使用正常活动的基线标准，然后将基线同非正常活动的基线进行比较。被动响应将会记录攻击活动，对于和利益相关的条目，被动响应还会发出警报。主动响应会通过变更环境的方式阻止攻击活动。基于主机的系统会被安装在单一主机上，并对其进行监控；而基于网络的系统会被安装在网络设备上，并监测网络的整体活动。入侵防御系统与流量保持一致，能够在恶意流量到达之前进行阻止。

蜜罐、蜜网和填充单元是防止在生产网络中发生恶意活动，并引诱攻击者的有力工具。它们常常含有用来引诱攻击者的伪漏洞和假数据。管理员和安全人员也使用这些工具来收集证据，以便起诉攻击者。

反恶意软件的及时更新能够防止许多恶意代码攻击。反恶意软件通常安装在互联网和内部网络之间的边界、电子邮件服务器和每个系统上。限制用户安装软件的权限有助于防止用户意外地安装恶意软件。此外，让用户了解不同类型的恶意软件，以及犯罪分子如何试图欺骗用户等知识，能够帮助他们避免危险行为。

渗透测试对于检测安全措施和组织的安全策略的强度和效率很有益。渗透测试通常以漏洞评估或扫描开始，然后尝试利用漏洞。渗透测试只有在得到管理批准的情况下才能进行，且只能在测试系统而不是生产系统中执行。组织经常聘请外部顾问进行渗透测试，并可以控制这些测试人员对系统的了解程度。零知识测试通常被称为“黑盒测试”，全知识测试通常被称为“白盒”或“水晶盒测试”，而部分知识测试通常被称为“灰盒测试”。

当日志记录和监测与有效的认证和识别方法结合在一起时，便能够提供详细的细节。日记记录包含对日志和数据文件中事件的记录。安全日志、系统日志、应用程序日志、防火墙日志、代理日志和变更管理日志都是常见的日志文件。日志文件包含有价值的数据，故应加以保护，以确保它们不会被修改、删除或受到损坏。如果不对日志施加保护，攻击者常常会试图修改或删除日志，这样就没有了起诉攻击者的证据。

监控包括实时审查日志，这也是审计的一部分。将事件或突发情况的有关信息记录到一个或两个数据库或文件中，就创建了审计跟踪记录。它们可以用来重建事件，提取关于事件的信息，并证明或反驳罪责。审计跟踪提供了一种被动形式的检测安全控制，就像 CCTV(闭路电视)和安全警卫一样，审计跟踪也被认为是一种威慑手段。此外，在起诉犯罪时也需要审计跟踪。日志可能会很大，所以人们会使用不同的方式来分析日志，或减小日志的大小。抽样是用来分析日志的统计学方法，使用阀值级别对和利益相关的条目进行统计。

使用不同的审计和审查方式能够对访问控制的有效性进行评估。审计是一种针对环境的有条理的审查方式，能够确定环境符合规定，并检测异常和未经授权的事件或犯罪。访问审查确保访问和账户管理操作符合组织的安全策略。用户权限审计确保工作人员遵守最小特权原则。

审计报告以文档形式记录审计结果。应对这些报告加以保护，仅限于组织内特定的人才能查看

报告。高级管理人员和安全专家需要了解安全审计的结果，但是如果攻击者得到了审计报告，他们将会利用报告寻找可以利用的漏洞。

审计报告能够用来保证控制措施和工作正确开展。审计能够用来检查补丁管理、漏洞管理、变更管理和配置管理程序。

17.5　考试要点

了解事件响应的步骤　CISSP CIB 将事件响应分为以下几个步骤：检测、响应、缓解、报告、恢复、整理和吸取经验教训。在检测和验证事件的发生之后，第一反应是限制事件的扩散范围，并同时做好证据保护工作。根据管理法规的要求，组织需要向上级报告事件。如果对 PII 产生影响，则需要通知到个人。整理和吸取经验教训阶段包括执行根本原因分析，以确定成因和建议的解决方案，防止复发。

了解基本的预防措施　基本的预防措施可以防止许多事件的发生。这些措施包括保持系统更新，删除或禁用不必要的协议和服务，使用入侵检测和防御系统，使用含最新签名的反恶意软件，并使用基于主机和基于网络的防火墙。

了解拒绝服务(DoS)攻击　拒绝服务(DoS)攻击能够阻止系统对合法服务的请求的回应。最常见的 DoS 攻击有 SYN 泛洪攻击，该攻击能够破坏 TCP 三次握手过程。尽管现今由于预防措施的阻止，旧的攻击方式不是很常见，但我们仍然需要对它们进行检测，因为许多新的攻击方式往往是从旧的攻击方式演变而来的。使用放大网络的 smurf 攻击能够向众多受害者发送大量的回应数据包。ping 死亡攻击向受害者发送大量的 ping 数据包，导致受害者系统被冻结、崩溃或重新启动。

理解僵尸网络、僵尸网络控制器和僵尸牧人　由于能够发动攻击的电脑数量庞大，因此僵尸网络是重大威胁。所以，了解它们是什么很重要。僵尸网络是网络上由名为僵尸牧人的犯罪分子控制的受损个人电脑(常被称为僵尸)的集合。僵尸牧人使用口令，控制服务器远程控制僵尸，且通常使用僵尸网络对其他系统发起攻击，或者发送垃圾邮件或钓鱼邮件。僵尸牧人也从其他犯罪分子那里租用僵尸网络。

理解零日漏洞　零日漏洞指的是利用除了攻击者或一小部分人以外没有人知道的漏洞，进行攻击的一种方式。表面上看，似乎我们并不能保护未知的漏洞，但是基本安全策略一直在努力预防漏洞的产生。删除或禁用不必要的协议和服务能够减少攻击面，使用防火墙能够屏蔽多数攻击点，且使用入侵检测和防御系统有助于检测和阻止潜在的攻击。此外，类似于蜜罐和填充单元这样的工具也能够保护网络。

理解中间人攻击　当恶意用户能够在通信链路的两端之间获得逻辑位置时，中间人攻击就会发生。虽然对攻击者来说完成中间人攻击很复杂，但是从攻击中获得的数据量是相当可观的。

理解破坏行为和间谍行为　如果组织的内部员工因某些原因对组织产生了不满，可能会实施破坏行为。当组织的竞争对手试图偷取信息时，他们通常会买通该组织的内部员工以实施间谍行为。一些基本安全原则(如最小特权原则、及时解雇原则)的实施有助于限制不满员工的行为，并减少因攻击受到的损失。

理解入侵检测和入侵防御　IDS 和 IPS 是重要的检测和预防攻击的方法。应了解基于知识(使用类似于反恶意软件签名的数据库)的检测和基于行为的检测方式之间的区别。基于行为的检测首先确定一个正常情况下的基线，并使用该基线同活动基线作对比，以检测有无非正常活动。如果网络环

境被修改，基线就会失效，所以在系统环境发生变更之后应更新基线。

识别 IDS/IPS 响应 入侵检测系统可以通过日志记录和发送通知做出被动响应，也可以通过变更环境做出主动响应。一些人将之称为 IDS 和 IPS。然而，IPS 与流量相一致，包含在恶意流量到达目标之前做出阻止响应的功能。

理解 HIDS 和 NIDS 之间的差异 主机型 IDS(HIDS)可以监测单一系统上的活动。缺点是攻击者能够发现并将其禁用。网络型 IDS(NIDS)可以监测网络上的活动，且对攻击者不可见。

理解蜜罐、填充单元和伪缺陷 蜜罐是一种含有伪缺陷和假数据，用来引诱入侵者的系统。管理员可以观察蜜罐中的攻击者的活动。只要攻击者在蜜罐中，他们就没有对真实网络造成攻击。经过检测，一些 IDS 具有将攻击者转移到填充单元中的功能。虽然蜜罐和填充单元相似，但蜜罐用来引诱攻击者，而攻击者会被转移到填充单元中。

理解阻止恶意代码的一些方法 将几种工具组合在一起能够破解恶意代码。最常见的就是拥有最新补丁包的反恶意软件。这些程序被安装在每个系统中、网络边界或电子邮件服务器上。然而，一些策略要求遵守基本的安全原则，如最小特权原则，这能够有效防止普通用户安装恶意软件。此外，对用户进行攻击风险及攻击手段方面的知识教育能够帮助用户了解并避免危险行为。

理解渗透测试 渗透测试从发现漏洞开始，然后模仿攻击，以确定什么样的漏洞可以被利用。没有管理层明确的同意通知是不能进行渗透测试的。此外，因为渗透测试可能会导致损坏，所以应尽可能在孤立系统中执行。同时还应该了解黑盒测试(零知识测试)、白盒测试(全知识测试)和灰盒测试(部分知识测试)之间的差异。

了解日志文件类型 日志数据记录在数据库或不同类型的日志文件中。常见的日志文件包括安全日志、系统日志、应用程序日志、防火墙日志、代理日志和变更管理日志。日志文件应通过集中存储和限制访问权限的方法来保护，日志文件的格式应设置为只读，以防他人更改。

理解监控和监控工具的使用 监控是一种审计形式，侧重于对日志文件数据进行主动审查。监控用来保持受试者并使他们对自己的行动负责，同时监控能够检测到异常或恶意的活动。监控也被用来监视系统性能。监控工具(如 IDS 或 SIEM)能够提供对事件的实时分析。

理解审计跟踪 将事件信息记录到一个或更多个数据库或日志文件中，就创建了审计跟踪记录。审计跟踪能够用来重建事件、提取事件信息、证明或反驳罪责。使用审计跟踪是侦查安全控制的一种被动形式，也是起诉犯罪分子的重要证据。

理解抽样 采样或数据提取是从大量的数据中提取所需要素，以构建能够代表整体的总结的过程。统计抽样使用精确的数学函数，从大量的数据中提取有意义的信息。阈值是一种非统计抽样，只记录超出阈值的事件。

理解问责方式 通过对审计的使用，问责能够详细到个人。日志记录了用户活动，用户也能够为记录的行动负责。这使得用户不执行违规行为，并遵守组织的安全策略。

理解安全审计和审查的重要性 安全审计和审查有助于确保管理程序有效且被记录。它们通常与账户管理联系在一起，以防止用户违反最小特权或知其所需原则。然而，它们也可以用于监督补丁管理、漏洞管理、变更管理和配置程序管理。

理解审计和频繁安全审计的必要性 审计是对环境有条理地进行检查或审查，以确保其符合法规，并能够检测异常、未经授权的事件或犯罪。安全 IT 环境在很大程度上依赖于审计。总体而言，在安全环境中，审计是一种很重要的检测控制手段。IT 设施安全审计或安全审查的频率取决于风险。组织会对风险进行评估，以决定补充经费或终止审计。风险等级还影响着审计方式。明确并坚持审计频率是很重要的，从而验证部署在环境中的安全机制能否提供足够的安全性。

理解审计是维护的一方面　安全审计和有效审查是维护的关键要素。高级管理人员必须依照规定执行定期的安全审查，否则他们将可能对发生的任何资产损失负责。

理解控制审计报告访问的必要性　审计报告通常具有相同的概念，如审计目的、审计范围、审计发现或揭示出的结果。审计报告中通常还有环境的具体信息，以及一些敏感信息，如问题、标准、起因和建议。含有敏感信息的审计报告应被单独分类标签，并妥善处理。只有具有访问权限的人才能查看审计报告。提供给不同人的审计报告可以有不同的版本，里面只提供该份报告的目标读者所需要的信息。例如，提供给高级安全管理员的报告应详细说明所有细节，提供给普通管理人员的报告只含有概括性的信息。

了解访问审查和用户权限审计　访问审查确保用户访问和账户管理行为符合安全策略中的规定。用户权限审计确保最小特权原则能够实施，并能够对特权账户加以监控。

控制审计访问　定期审查访问控制有助于确保访问控制的有效性。例如，审计可以记录账户的登录成功或失败。入侵检测系统可以监控这些日志，轻松地识别攻击，并通知管理员。

17.6　书面实验室

1. 列出 CISSP CIB 中定义的事件响应的不同阶段。
2. 描述主要的入侵检测系统类型。
3. 描述审计和审计跟踪之间的关系。
4. 组织应该怎样验证账户是否妥善管理？

17.7　复习题

1. 下列哪一项是在检测和确认事件发生后最好的响应？
   A. 控制它
   B. 报告它
   C. 修复它
   D. 收集证据
2. 在事件响应的修复阶段，安全人员会做下列哪件事？
   A. 控制事件
   B. 收集证据
   C. 重建系统
   D. 执行根本原因分析
3. 以下哪些是拒绝服务攻击？(选择三项)
   A. 泪滴攻击
   B. smurf 攻击
   C. 死亡 ping
   D. 欺骗

4. SYN 泛洪攻击是如何工作的？

A. 利用 Windows 系统中的数据包处理漏洞

B. 使用放大网络产生大量数据包并发送给受害者

C. 扰乱 TCP 使用的三次握手过程

D. 发送超大 ping 数据包给受害者

5. 在互联网上托管的 Web 服务器最近被攻击者利用操作系统中的漏洞攻击了。操作系统供应商在事件协助调查并证实该漏洞以前并不知道。什么类型的攻击是这样的？

A. 僵尸网络

B. 零日漏洞攻击

C. 拒绝服务攻击

D. 分布式拒绝服务攻击

6. 以下哪个选项是散播恶意软件的最常见方式？

A. 偷渡式下载

B. USB 闪存驱动器

C. 勒索

D. 未经批准的软件

7. 在下列选项中，哪一项指出了入侵检测系统(IDS)的主要目的？

A. 检测异常活动

B. 诊断系统故障

C. 评估系统性能

D. 测试系统漏洞

8. 关于主机型入侵检测系统(HIDS)，以下哪一项描述是正确的？

A. 可以监控整个网络

B. 监控单个系统

C. 对于攻击者和用户是无形的

D. 不能检测恶意代码

9. 下列哪一项描述了以未打补丁和未受保护的安全漏洞和错误数据设计虚假网络以吸引攻击者？

A. IDS

B. 蜜网

C. 填充单元

D. 伪缺陷

10. 下列选项中，反恶意软件保护的最佳方式是什么？

A. 每个系统上多个解决方案

B. 整个组织一个解决方案

C. 在不同的位置部署反恶意软件保护

D. 在所有边界网关不折不扣地过滤内容

11. 当使用渗透测试验证安全策略的强度时，下列哪一项是不受推荐的？

A. 模仿以前发生过的对系统的攻击

B. 在没有管理常识的情况下执行攻击

C. 使用手动和自动攻击工具

D. 重新配置系统去解决任何发现的漏洞

12. 什么用于保持主体为他们的行为负责，同时他们的身份已由系统认证？

A. 认证

B. 监控

C. 账户锁定

D. 用户权限审查

13. 审计跟踪是什么类型的安全控制？

A. 行政管理性安全控制

B. 检测性安全控制

C. 纠正性安全控制

D. 物理性安全控制

14. 下列哪些选项能在环境中有条不紊地检查或审查以确保符合法规，并且检测异常、未授权的事件或犯罪？

A. 渗透测试

B. 审计

C. 风险分析

D. 陷阱

15. 什么可以用来减少使用非统计方法的日志或审计数据量？

A. 阀值级别

B. 取样

C. 日志分析

D. 报警触发器

16. 下列哪一项比实际内容更侧重于模式和数据的趋势？

A. 击键监控

B. 流量分析

C. 事件日志

D. 安全审计

17. 当用户拥有不必要的特权时需要进行哪项活动？

A. 账户管理

B. 用户权限审计

C. 日志记录

D. 报告

在回答问题 18 至 20 时请参考下面的场景：

一个组织有一份需要核实后报告事件的响应计划。为了安全目的，该组织并没有公布这份计划。只有事件响应团队的少数几个成员知道这份计划及其内容。近日，服务器管理员发现自己管理的 Web 服务器运行比平时慢。快速调查后，他发现攻击来自某个特定 IP 地址。他立即重新启动 Web 服务器以重置连接，攻击停止了。然后，他使用从互联网上找到的专门针对此 IP 地址的工具进行了数小时的反击。因为来自这个 IP 地址的攻击停了下来，他没有报案。

18. 在重新启动 Web 服务器之前应该做什么？

A. 审查事件

B. 执行补救措施

C. 采取恢复步骤

D. 收集证据

19. 以下哪一项指出了服务器管理员在此事件中做出的严重错误？

A. 重新启动服务器

B. 不报案

C. 攻击 IP 地址

D. 重置连接

20. 在这起事件中完全丧失了什么？

A. 经验教训

B. 检测

C. 响应

D. 恢复

第 18 章

灾难恢复计划

本章中覆盖的 CISSP 考试大纲包含：

安全评估与测试

- C. 收集安全过程数据(例如，管理和运营控制)
  - C.5 培训和意识
  - C.6 灾难恢复与业务连续性

安全运营

- K. 实施恢复策略
  - K.1 备份存储策略(例如，异地存储、电子传送、磁带循环)
  - K.2 站点恢复策略
  - K.3 多站点(例如，操作冗余系统)
  - K.4 系统恢复能力、高可用性、服务质量和容错能力
- L. 执行灾难恢复过程
  - L.1 响应
  - L.2 人员
  - L.3 通信
  - L.4 评估
  - L.5 恢复
  - L.6 培训和意识
- M. 测试灾难恢复计划
  - M.1 通读测试
  - M.2 结构化演练
  - M.3 模拟测试
  - M.4 并行测试
  - M.5 完全中断测试

在第 3 章“业务连续性计划”中，你已经学习了业务连续性计划(BCP)的基本内容，也就是帮助组织避免因紧急事件或灾难而使业务中断的技术。但是业务连续性计划并不力图去阻止每个可能的灾难。

灾难恢复计划(DRP)在 BCP 中止时开始。当灾难发生且业务连续性计划无法防止业务中断时，灾难恢复计划开始生效，并且指导紧急事件响应人员的工作，直至达到最终目标，也就是业务被还原到主要运营设施的全部运营能力。

阅读本章时，你可能会注意到在BCP和DRP处理过程之间有很多重叠的地方。实际上，我们对特定灾难的讨论，是从BCP和DRP的角度，从如何处理这些灾难中提供信息。事实上，虽然(ISC)^{2}的CISSP课程对两者进行了区分，但是大多数组织都只有单个团队和计划，同时涉及业务连续性和灾难恢复所关注的内容。在许多组织里，单一学科被称为业务连续性管理(BCM)，包括BCP、DRP以及单独保护下的事件管理。

18.1 灾难的本质

灾难恢复计划围绕组织正常运营被中断，为混乱的事件带来正常的工作秩序。灾难恢复计划理所当然要在高度紧张和冷静的头脑可能不容易占优势时得以执行。对可能发现有必要实施 DRP 措施的环境进行描述，如飓风破坏了主运营设施、火灾烧毁了主运营中心、恐怖行为阻碍进入城市的主要区域。停止、阻止或中断组织执行其工作任务的任何事件都被视为灾难。一旦 IT 无法支持关键任务进程，就需要通过 DRP 来管理还原和恢复过程。

灾难恢复计划应该被配置为几乎是自动执行的。DRP 还应当被设计为在灾难期间尽可能排除决策活动。必要的人员应该就灾难发生时他们的责任和任务进行良好培训，并且了解他们需要采取的措施，从而尽可能快地使组织恢复运营。我们将从分析可能影响组织的一些灾难开始，进而对它们所造成的特殊威胁进行分析。前面在第 3 章中已经提到过其中很多威胁，但是我们将在本章对它们进行更深入研究。

为了针对自然和非自然灾难进行计划编制，必须首先理解灾难的各种形式，下面将详细讨论这个问题。

18.1.1 自然灾难

自然灾难反映了我们生存环境的狂怒(由于地球表面或大气变化超出人类的控制，因此会出现强烈的变化)。在某些情况下(如飓风)，科学家已经开发出了成熟的预报技术，在灾难发生之前能够提供充分的警示。其他某些情况(如地震)则可能会在瞬间带来不可预测的破坏。灾难恢复计划应当针对灾难的两种类型提供相应的机制，这两种机制可以是响应力的逐渐形成，也可以作为对突然出现的紧急危机的立即响应。

1. 地震

地震由大陆板块的移动引发，可能会在全世界的任何地方发生，而且没有预警。然而它们更有可能在已知的断层上发生，这样的断层在世界的很多地方都存在。San Andreas 断层就很有名，它给美国西部的部分地区带来了相当大的危险。如果住在地震可能出现的断层附近区域，那么 DRP 应当

说明在地震导致正常操作中断时业务将要执行的程序。

你可能会对这样的事实感到惊奇：全球有一些地区被认为可能会发生地震。表 18.1 中列出了美国联邦紧急事件管理机构(FEMA)认为会出现中级、高级或很高级别地震风险的美国部分地区。可以注意到，表中列出了 50 个州中 82%的州(41 个)，这意味着美国的大部分地区都会出现至少属于中级的地震事件。

表 18.1　美国地震风险等级

中等地震风险	高地震风险	极高地震风险
Alabama	American Samoa	Alaska
Colorado	Arizona	California
Connecticut	Arkansas	Guam
Delaware	Illinois	Hawaii
Georgia	Indiana	Idaho
Maine	Kentucky	Montana
Maryland	Missouri	Nevada
Massachusetts	New Mexico	Oregon
Mississippi	South Carolina	Puerto Rico
New Hampshire	Tennessee	Virgin Islands
New Jersey	Utah	Washington
New York		Wyoming
North Carolina		
Ohio		
Oklahoma		
Pennsylvania		
Rhode Island		
Texas		
Vermont		
Virginia		
West Virginia		

2. 洪水

每年在全球的任何地方都可能随时发生洪水灾害。一些洪水是由于河流、湖泊和其他水体中的雨水逐渐增多，然后溢出堤坝淹没乡镇、村落造成的。某个地区的地表在短时间内无法容纳比雨水更多的突然发生的大暴雨时，就会出现另一些类型的洪水，如山洪暴发。洪水也可能在堤坝受损时发生。由地震活动导致的大浪或海啸会形成令人畏惧的洪水般的力量和破坏性，例如 2011 年日本大海啸灾难。海啸彻底展示了洪水的破坏力，并且会对各种业务和经济造成影响。

根据美国政府的统计数据，在美国每年由于洪水灾害而对商业和家庭造成的危害损失超出 10 亿美元。对于洪水袭击业务设施的事件，DRP 能够做出恰当的响应计划是非常重要的。

警告：

为了开发业务连续性和灾难恢复计划而对公司进行洪水破坏风险的评估时，最好请一些认真负责的人进行检查，并且确信为了降低洪水带来的经济影响，组织买了足够的保险。在美国，大多数常规业务保险合同没有涵盖洪水破坏，因此应当对 FEMA 的国家洪水灾害保险计划中那些获得政府财政专项支持的洪水灾害保险进行研究。

尽管理论上洪水灾害可能会在全球各地发生，但是在某些特定的区域发生的可能性更高。FEMA 的国家洪水灾害保险计划负责对全美国的洪水灾害风险进行评估，为国民提供地理形式的数据。可以从 http://msc.fema.gov/portal 联机查看洪水灾害地图。

这个站点还提供有关地震、飓风、暴风雨、冰雹和其他自然灾害的有价值的历史信息，从而帮助准备组织的风险评估。

在查看洪水灾害地图(如图 18.1 所示)时，你会发现有两种风险常常被定义到地图中，它们就是“百年洪泛区”和“五百年洪泛区”。这些评估说明政府预计这些地区至少每 100 年或 500 年出现一次洪水。关于洪水灾害地图的更多详细指导信息，读者可以查看 www.fema.gov/media/fhm/firm/ot_firm.htm。

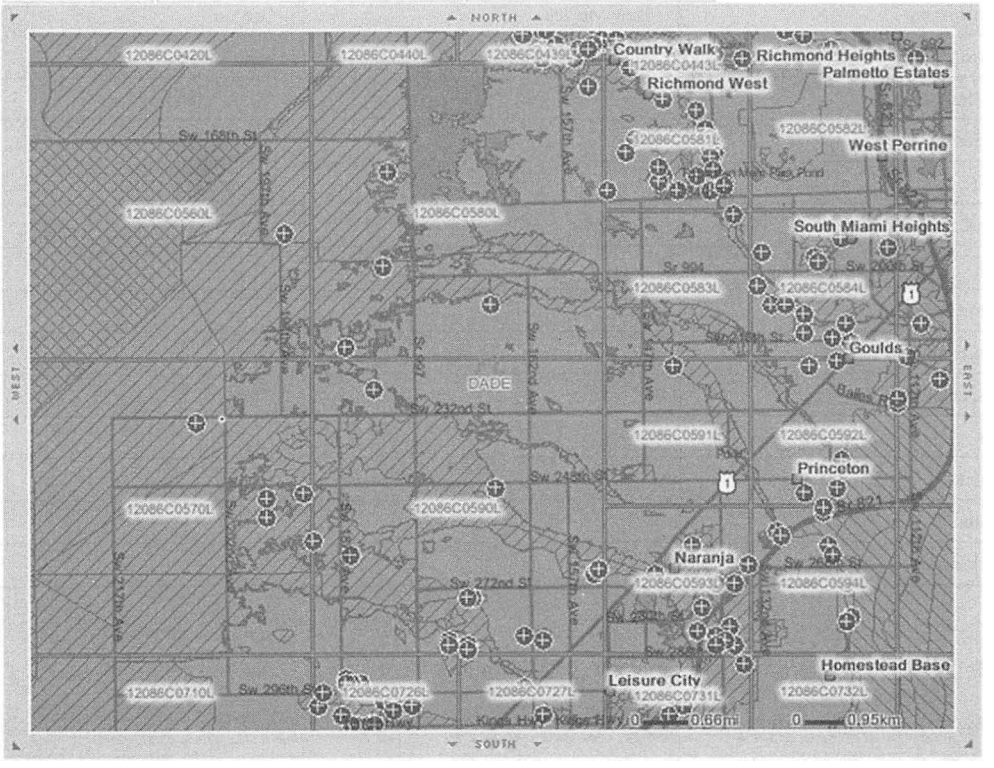


图 18.1　佛罗里达州迈阿密戴德郡的洪患图

3. 暴风雨

暴风雨有很多形式，并且会对业务带来很多不同的风险。长期的强降雨会导致山洪暴发的风险，这在前面的内容中已经进行过描述。具有严重威胁的飓风和龙卷风的风速都超过了每小时 100 英里，这对建筑物结构的完整性造成了威胁，并且将普通的物体(如树木、割草机甚至汽车)变成了致命的

飞弹。冰雹带来了从天而降的破坏性冰块的迅猛袭击。很多暴风雨还会伴随闪电，这可能会对敏感的电子设备带来严重的毁坏。因此，业务连续性计划应该详细描述防护闪电危害的恰当机制，并且灾难恢复计划应当为可能在闪电袭击中出现的电力中断和设备损坏提供足够的防护。永远都不要低估暴风雨可能导致的破坏程度。

2005 年，有史以来造成损失最大、最致命和最强的大西洋 5 级飓风 Katrina 横扫美国大陆，破坏的范围从阿拉巴马州直至路易斯安那州，几乎毁坏了整个范围内所有自然的和人造的物体。这次暴风雨导致的大规模破坏的经济损失估计超过 810 亿美元，毁坏了墨西哥海湾沿岸公路的主要设施，导致商品出口困难，更不必说新奥尔良城近 80%的地区被淹没。

提示：

如果居住在容易受到某种特定类型的强暴风雨影响的地区，那么定期查看相关政府机构发布的天气预报是非常重要的。例如，在飓风出现的季节里，灾难恢复专家应定期查看美国国家气象服务预报中心的站点(www.nhc.noaa.gov)。这个站点使你能够在本地新闻播报前监视可在本地造成危害的大西洋和太平洋风暴，从而能够在灾难到来之前开始对暴风雨逐步做出响应。

4. 火灾

火灾的发生可能会有很多原因，既可能是人为的，又可能是自然的，但是这两种形式的火灾所带来的危害是相等的。在 BCP 和 DRP 处理过程中，应当评估火灾带来的风险，并且采取最基本的措施来缓解这些风险，在关键性设施发生灾难性火灾后恢复业务。

世界上的一些地区在温暖的季节容易发生燎原大火。这些火灾一旦发生，根据可预测的一些蔓延模式，火灾专家会同气象学家一起对大火的可能蔓延路径进行相对准确的预报。

提示：

与其他很多类型的大型自然灾难一样，可以从网上获得与即将出现的威胁相关的有价值信息。在美国，国家机构火灾中心在其网站 http://www.nifc.gov/fireInfo/fireInfo_maps.html 上显示每天的火灾更新信息和预报信息。其他的国家也有类似的警报系统。

5. 其他的地区性事件

世界上某些地区具有地区性的自然灾难。在 BCP/DRP 处理过程中，评估团队应当分析组织的所有运营地区，并且估计这些类型的事件可能会对业务造成的影响。例如，世界上的很多地区都会出现火山爆发。如果在靠近活火山或休眠火山的地区进行业务的运营，那么 DRP 或许就应当说明这种可能性。其他的地区性灾难事件包括亚洲的季风、南太平洋的海啸、高山地区的雪崩和美国西部的泥石流。

如果业务分布在不同的地区，那么就应当明智地在策划团队中包括地区政府。最起码，采用像政府紧急事件预备队、城市防御组织和保险索赔办公室这样的当地资源有助于指导工作。这些组织拥有大量的知识，通常更愿意帮助组织对意外事件进行准备。毕竟，每个成功经受住自然灾害的企业都是灾害发生后较少需要恢复资源的企业。

18.1.2 人为灾难

人类几个世纪以来所建立的先进文明变得越来越依靠技术、逻辑和自然系统之间复杂的相互作用。形成的成熟社会的复杂交流还可能造成很多潜在的、有意和无意人为灾难的脆弱性。在这一节中，我们将研究几个较为常见的灾难，从而帮助你在准备业务连续性计划和灾难恢复计划时对企业的脆弱性进行分析。

1. 火灾

在本章前面部分，我们探讨了由于自然原因造成的燎原大火带来的危害。很多较小的火灾是由于人为原因造成的，例如粗心、错误的电线连接、不正确的防火措施或其他一些原因。来自保险信息协会的研究显示,每天在美国至少有 1000 幢建筑物发生火灾。如果其中一处火灾袭击了你的企业，那么你会有足够的预防措施快速遏制火灾吗？如果火灾破坏了你的设施，那么你的灾难恢复计划多快才能使企业在其他地方恢复经营？

2. 恐怖行为

自 2001 年 9 月 11 日的恐怖袭击发生以来，业务活动对恐怖威胁带来的风险越来越关注。由于缺乏足够的确保企业持续生存的业务连续性计划/灾难恢复计划，9 • 11 恐怖袭击使得很多小型企业最终关门。很多较大的企业都经历过由长期破坏导致的极大损失。保险信息协会在恐怖袭击发生后一年发布了一份研究报告，这份报告对纽约市由于恐怖袭击造成的全部破坏进行了评估，破坏的损失高达 400 亿美元！(是的，那只是开始！)

警告：

组织可能无法选用适当的普通保险业务来应对恐怖行为造成的损失。在 2001 年 9 • 11 恐怖袭击以前，大多数保单要么包括恐怖行为，要么没有明显地提及恐怖行为。在遭受惨痛的损失之后，许多保险公司很快做出相应的修改方案，从而不再包括恐怖活动造成的损失。保单附加条款有时列出，但常常具有极高的保费成本。如果业务连续性或灾难恢复计划包括保险并将之作为经济补偿的一种手段(因为可能应该这样做)，那么应当会被劝告查看保险合同并联系专属客服，以确保你始终包括在保险范围内。

恐怖行为由于不可预测性，为 DRP 团队带来了特殊的挑战。在 2001 年 9 • 11 恐怖袭击以前，很少有 DRP 团队认为飞机撞击总部的威胁大到值得去缓解的程度。现在很多公司正在自问很多新的关于恐怖行为的“如果…会怎样”的问题。通常，这些类型的问题在促进业务成员之间提出有关潜在威胁的对话方面是有益的。相反，灾难恢复计划的策划者必须强调稳健的风险管理原则，并且确保没有针对恐怖威胁过度分配资源，以免对那些为防护更可能发生的威胁而进行的 DRP/BCP 行为造成影响。

3. 爆炸/煤气泄漏

煤气泄漏可能来自很多人为因素。煤气泄漏可能使得房间里/建筑物里充满爆炸性的气体，随后被点燃引发破坏性的爆炸。在很多区域发生的爆炸还会引发担忧。从灾难计划的观点出发，爆炸和煤气泄漏与那些大型火灾引发的灾害有着相似的结果。然而，计划避免爆炸的影响更为困难，并且

依赖于物理安全措施，如第 10 章“物理安全需求”中讨论的那些措施。

4. 电力中断

即使最基本的灾难恢复计划也包括了对短时间电力中断威胁的应对方法。关键业务系统常常由不间断电源设备(UPS)进行保护，这些电源使你至少有足够长的时间关闭系统或启动并运转应急发电机。然而，企业是否具有应对长时间电力中断的能力呢？

在 2005 年 Katrina 飓风登陆美国本土之后，据报道，密西西比州、路易斯安那州和阿拉巴马州有 240 万人遭遇停电。业务连续性计划能够在这样长时间没有电力的情况下保持业务连续进行吗？即使在商业输电网仍然无法运行时，灾难恢复计划也具有及时恢复电力的充分准备吗？

警告：

定期检查 UPS！这些关键设备常常直到它们必须使用时才被重视。很多 UPS 包括自动报告问题的自测机制，但是对其定期进行测试仍是不错的措施。此外，要确保审计每个 UPS 中插入的设备数量/类型。很多人认为向 UPS “多增加一个系统”没有问题，这简直太让人惊讶了。如果设备在电力中断期间无法处理负载，就不应该感到惊讶！

当今的技术型组织对电力的依赖程度越来越高，BCP/DRP 团队应当考虑备用电源，从而能够在不确定的时间段内为业务系统的运行提供电力。一台足够胜任的备用电机可能就意味着在生死攸关的时刻对业务的持续运营产生很大的影响。

18.1.3　其他公共设施和基础设施故障

当计划编制者考虑公共设施停止运转可能对企业造成的影响时，他们自然首先会想到电力中断造成的影响。但是，还应该考虑其他的公共设施。是否有依赖于水、污水管、天然气或其他公共设施的关键业务系统呢？当然还要考虑地区性的基础设施，如公路、机场或铁路。这些系统中的任何一个都可能出现故障，而这些故障与本章中提到的天气或其他条件并不相关。很多业务依赖于这些基础设施中的一个或多个来调动人员或搬移物品。故障可能会使你的业务持续运行能力瘫痪。

注意：

在被询问是否具有依赖于水、污水管、天然气或其他公共设施的关键业务系统时，如果很快回答没有，那么就需要再仔细考虑一下。考虑过关键业务系统中的人吗？如果一场大暴风雪破坏了设施和保持这些设施运行所需要的供水，那么能够为员工提供足够的饮用水以满足他们的生理需求吗？

你的防火系统怎么样？如果它们都需要用水，那么在公共供水系统出现故障时，是否有提供充足水源的储水系统能够扑灭严重的建筑物大火呢？在经受暴风雪、地震和其他可能中断水力传输的自然灾害破坏的地区，火灾常常会造成严重的破坏。

1. 硬件/软件故障

不管喜欢不喜欢，计算机系统都会出现故障。硬件组件可能受到磨损且无法继续运行或受到物理损坏。软件系统含有 bug，或者被给予不正确/意想不到的操作指令。因此，BCP/DRP 团队必须在系统中提供足够的冗余度。如果强制要求零宕机时间，那么最好的解决方案是在具有不同通信链路

和基础设施的不同地方使用全冗余故障恢复服务器。如果一台服务器被破坏或损坏，那么另一台将立即接管正在处理的负载。更多的相关信息，读者可以参见本章稍后的“远程镜像”部分。

由于财务上的限制，维持全冗余系统并非总能实现。在这些情况下，BCP/DRP 团队应该说明如何很快获得和安装被替换的部分。在本地零件库中应该保存尽可能多的零件以备进行快速替换，这对于很难找到而必须进口的零件来说尤为重要。毕竟，在关键 PBX 组件从国外进口并在现场安装的那些天里，能有多少企业可以在三天内不接听电话呢？

真实场景

纽约大停电

2003 年 8 月 14 日，由于一系列连锁故障引发主要电网瘫痪，纽约以及美国东北部和中西部的大部分地区遭遇了大停电。

幸运的是，纽约地区的安全专家早已有所防备。经历 2001 年 9 • 11 恐怖袭击后，许多业务都更新了灾难恢复计划，并且采取措施确保在出现其他灾难时仍然能够持续运营。这次大停电提供了一次测试机会，许多业务都能够通过采用备用电源或将控制无缝转向外部数据处理中心来实现持续运营。

全世界的 BCP/DRP 团队能够从纽约大停电得到下列教训：

- 确保作为替代的处理场所位于与主场所足够远的地方，从而不容易受到相同灾难的影响。
- 需要记住的是，组织会面对来自内部和外部的威胁。下一个灾难可能来自恐怖袭击、建筑物火灾或者在网络上自由运行的恶意代码。采取某些措施，确保作为替代的场所与主设施隔离，从而防护上述所有威胁。
- 灾难往往不会伴随着预先警告。如果实时操作对于组织来说是关键的，那么必须确认备份场所已经做好准备，一接到通知，就能接替主要状态。

2. 罢工/示威抗议

在设计业务连续性计划和灾难恢复计划时，不要忘记在紧急事件计划中指出人为因素的重要性。经常被忽视的一种人为灾难形式可能是罢工或其他劳工危机。如果大部分员工在同一时间罢工，那么将会对业务产生什么影响？能承受在某个区域没有固定的专职员工工作的时间有多长？BCP 和 DRP 团队应该解决这些问题，从而提供在劳工危机出现时的备选计划。

3. 盗窃/故意破坏

在前面的内容中，我们看到了恐怖行为给组织带来的威胁。偷窃、故意破坏与恐怖行为具有相同点，只是规模小得多。但是，在大多数情况下，组织有更大的可能性会受到偷窃或故意破坏的影响，而不仅仅是恐怖袭击的影响。保险为这些事件提供了一些经济保护(受限于免责和限制条款)，但是这些行为可能会长期和短期对业务带来严重破坏。业务连续性计划和灾难恢复计划应当包括充分的预防性措施，以便控制这些事件的发生频率，此外还应当包括紧急事件计划来减轻偷窃和故意破坏对正在进行的工作的影响。

注意：

盗窃基础设施的情况变得越来越普遍，因为小偷的目标是空调系统、管道工程和电源子系统中的铜金属。认为固定基础设施不会被盗的想法是错误的。

真实场景

安全性面临的外部挑战

偷窃和故意破坏的持续威胁是全世界范围内信息安全专家的克星。针对个人身份信息(PII)、专业或商业秘密以及其他形式的机密数据，直接竞争者或其他未授权方与这些信息的创建者和所有者具有相同的兴趣。

作为一家著名的、引人注目的计算机公司的安全人员，Aaron 了解相关工作的第一手资料。他的主要职责是保证敏感信息不被泄露给各类人员和实体。Bethany 是一名非常令人头疼的员工，这是因为她经常在没有正确保护内容安全的情况下将笔记本电脑带出工作场所。

即使偶然的破窗盗窃企图也会使数千客户的联系方式及其机密的业务交易存在泄露的风险，而且这些信息可能会被出卖给恶意方。Aaron 知道这些潜在的风险，但是 Bethany 似乎对此漠不关心。

这就引发了一个问题：如何更妥善地通知、培训或建议 Bethany，从而使 Aaron 不会由于笔记本电脑被盗而被解除职务？Bethany 必须理解和意识到保证敏感信息安全的重要性。我们有必要强调这样的事实：潜在的损失和泄漏会导致敏感数据被泄漏给坏人、竞争者或其他未授权的第三方。员工手册清楚地规定了其行为导致未授权泄漏或信息资产损失的员工会被扣工资或解雇，向 Bethany 指出这一点可能已经足够。如果在警告之后仍然出现这样的行为，那么 Bethany 应当受到指责，并且在未被立即解雇的情况下为其重新分配不会泄漏敏感或专有信息的岗位。

注意：

在计划零件库存时，应当考虑盗窃对企业的影响。对具有高被窃率的物品(如内存和笔记本电脑)保持额外的库存是明智的。同样，在安全的位置存放零件并且要求员工在使用这些零件时签名，也是不错的主意。

18.2　理解系统恢复和容错能力

作为 CIA 安全三要素(机密性、完整性和可用性)的核心目标之一，增加系统应变能力和容错能力的技术控制会直接影响到可用性。系统恢复和容错能力的主要目标是消除单点故障。

单点故障可以发生在任何组件上，能够导致整个系统崩溃。如果计算机的单一磁盘上含有数据，那么该磁盘发生故障就会导致计算机崩溃，所以磁盘是故障发生的单点。如果基于数据库的网站有多台 Web 服务器，而这些服务器又是由单一数据库服务器支持的，那么该数据库服务器就是故障发生的单点。

容错能力是指系统在发生故障的情况下仍然继续运行的能力。容错能力是通过添加冗余组件实现的，如廉价冗余磁盘阵列(RAID)中的额外磁盘或故障转移群集配置中的额外服务器。

系统恢复能力指的是系统在发生不利事件时保持可接受的服务水平的能力。这可能是容错组件管理的硬件错误，也可能是其他控制管理的攻击，如有效的入侵检测和防御系统。在某些情况下，

指的是在发生不利事件后系统还原的能力。例如，如果故障转移群集中的一台主服务器崩溃，容错能力能够使得系统故障转移到另外的服务器上，而系统恢复能力能够保障在原系统修复后，该集群能够返回原服务器。

18.2.1 保护硬盘驱动器

在计算机中添加容错和系统恢复组件的常见方法是增加冗余磁盘阵列(RAID)。冗余磁盘阵列包括两个或两个以上的磁盘，即使其中一个磁盘损坏，大多数的 RAID 配置也都能够继续运行。一些常见配置如下：

RAID-0　也被称为条带。它使用两个或两个以上的磁盘，并提高了磁盘子系统的性能，但不提供容错能力。

RAID-1　也被称为镜像。它使用两个磁盘，并含有相同的数据信息。如果一个磁盘损坏，另一个磁盘仍含有数据，这样在单一磁盘损坏后，系统仍能继续运行。系统可能会在不干扰的情况下继续运行或需要手动配置以使用没有损坏的磁盘，这取决于使用的硬件以及损坏的驱动器。

RAID-5　也叫作奇偶校验。它使用三个或更多个磁盘，相当于一个磁盘，其中包含奇偶校验信息。如果单一磁盘损坏，磁盘阵列将继续运行，但速度会变慢。

RAID-10　也被称为 RAID 1+0 或条带镜像，是在条带(RAID-0)配置上再配置两个或两个以上的镜像(RAID-1)。它使用至少 4 个磁盘，但可以支持更多个磁盘，磁盘可添加数应为偶数。即使多个磁盘损坏，只要在每个镜像中至少有一个驱动器继续运行，它就能继续运行。例如，如果有三个镜像集(称为 M1、M2、M3)，则共有 6 个磁盘。如果 M1、M2、M3 中分别有一个驱动器损坏了，该阵列将继续运行。然而，如果在任何镜像集中两个驱动器都损坏了，如 M1 的两个驱动器，整个阵列将无法继续运行。

注意：

容错同备份不同。有时，管理者可能会因为备份磁带的价格问题转而考虑用 RAID 进行备份。然而，如果发生了灾难性的硬件故障，并破坏了一个磁盘阵列，除非数据有备份，否则其中的数据将会全部丢失。同样，如果没有备份，意外使得数据发生损坏，也不能恢复。

RAID 可基于软件，也可基于硬件。基于软件的系统需要操作系统来管理阵列中的磁盘，而且这会降低系统的整体性能。它们相对便宜，因为不需要除额外磁盘以外的任何其他硬件。基于硬件的磁盘阵列系统通常更有效、更可靠。虽然基于硬件的磁盘阵列更昂贵，但当使用这种阵列以增加其个关键组件的可用性时，益处大于成本。

基于硬件的磁盘阵列通常含有可以在逻辑上添加到磁盘阵列中的备用驱动器。例如，基于硬件的 RAID-5 可能含有 5 个磁盘，在 RAID-5 阵列中有 3 个磁盘，另外还有两个备用磁盘。如果一个磁盘损坏，硬件检测出了故障，便能够在逻辑上将发生故障的磁盘替换为备用磁盘。此外，大多数基于硬件的阵列支持热交换，使得技术人员在不给系统断电的情况下能够更换损坏的磁盘。冷交换的 RAID 要求系统关机后才能更换损坏的驱动器。

18.2.2 保护服务器

可以通过故障转移集群将容错功能添加到关键服务器中。故障转移集群含有两个或两个以上的

服务器，如果其中一台服务器出现故障，集群中的其他服务器可以通过称为故障转移的自动化过程接管其负载。故障转移集群可以含有多台服务器(不只是两台)，它们还可以为多个服务或应用程序提供容错功能。

作为故障转移集群的一个例子，如图 18.2 所示。图中多个组件组合在一起，为使用数据库的大量网站访问提供了可靠的 Web 访问方式。DB1 和 DB2 是配置在故障转移集群中的两台数据库服务器。在任何给定的时间内，只有一台服务器将作为活动数据库服务器，而另一台服务器将处于不活动状态。例如，如果 DB1 是活动服务器，它将执行网站所有的数据库服务。DB2 监视 DB1 以确保其正常运行。如果 DB2 检测到 DB1 损坏，集群中的故障将自动转移到 DB2。

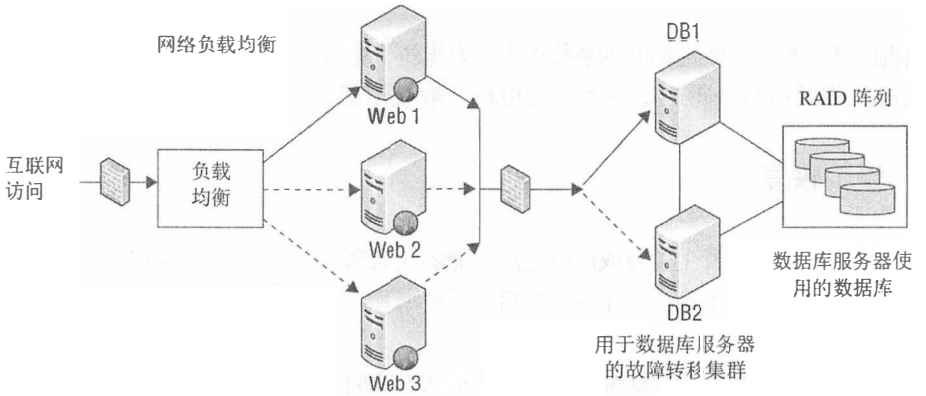


图 18.2　网络负载均衡下的故障转移集群

如图 18.2 所示，DB1 和 DB2 都能访问数据库中的数据。这些数据存储在 RAID 磁盘阵列上，这为磁盘提供了容错能力。

此外，三台 Web 服务器被配置在网络负载均衡集群中。负载均衡器可以基于软件，也可基于硬件，它平衡了三台服务器上的客户端负载。可以添加额外的 Web 服务器来处理增加的负载，同时也平衡所有服务器之间的负载。如果服务器发生故障，负载均衡器可以感知故障并停止向服务器发送数据。虽然网络负载均衡主要用来增加系统的可扩展性，使它可以处理更多的数据，但也提供了容错功能。

注意：

故障转移集群不是服务器容错的唯一方法。一些系统为服务器提供了自动容错功能，允许服务器发生故障而不失去继续提供服务的能力。例如，在具有两个或两个以上的域控制器的微软域中，每个域控制器将定期与其他域控制器复制数据，以便所有的域控制器都具有相同的数据。如果一个域控制器产生故障，域内的计算机仍然可以找到另一个(多个)域控制器且网络可以继续运行。同样，许多数据库服务器含有复制其他服务器数据的方法，以便所有的服务器都具有相同的内容。其中三种方法是电子传送、远程日志记录和远程镜像，它们将在本章稍后讨论。

18.2.3　保护电源

可以为不间断供电电源(UPS)、发电机或它们两者提供容错能力。一般情况下，不间断供电电源提供 5 到 30 分钟的短时间供电，而发电机提供长期电力。使用 UPS 的目的是为完成系统的逻辑性关闭提供足够的时间，或在发电机发电提供稳定电源之前维持电力供应。

理想情况下，电力是稳定的、无波动的。但在现实中，商业供电面临各种各样的问题。激增指的是电压快速增高，而下滑指的是电压突然快速降低。如果电力长时间维持在高压状态，则被称为电涌而不是激增。如果长时间处于低压状态，则被称为电力不足。偶尔，电源线会有噪音，这种情况被称为瞬变，瞬变有许多种来源。所有这些问题都可能会导致电力设备故障。

最基本的不间断电源(也被称为离线或备用电源)提供电涌保护和电池备份。它被插入到商业电源中，比较关键的系统会被插入到 UPS 系统中。如果电源发生故障，备用电池会为系统短时间供电。在线互动式的不间断电源越来越受欢迎，除了基本功能外，它们还增加了其他功能。它们含有可变电压互感器，能够在不使用电池电量的情况下对高低电压做出调整。在断电时，电池能为系统短时间供电。

发电机能够在长时间断电期间为系统供电。发电机供电时间的长短取决于燃料，只要发电机有燃料，就能依靠发电机获得稳定电力。发电机一般使用柴油、天然气或丙烷作为燃料。

18.2.4 受信恢复

受信恢复保证系统在发生故障或崩溃之后，能够还原到之前的状态。根据故障的类型，还原可以分为自动还原和管理员手动干预还原。然后，不论哪种还原方式，系统应该被预置，以确保还原的安全性。

系统可以被预置，在损坏时能够处于故障防护状态或应急开放状态。处于故障防护状态的系统会在故障发生时保持在防护状态，并禁止所有访问。应急开放的系统会在发生故障前保持在开放状态，并授权所有访问。对二者的选择取决于在系统故障之后安全性和可用性的重要程度。

例如，防火墙通过控制网络的访问和拒绝来维持安全性。防火墙配置了隐式否认体系，只允许规定中明确指出可以进入的流量信息进入。防火墙通常被设计为故障防护状态，支持隐式否认体系。如果防火墙发生故障，所有的流量都会被禁止。虽然这消除了防火墙通信的可用性，但很安全。相比之下，如果通信的可用性比安全性更重要的话，防火墙可以被配置为应急开放状态，允许所有的流量通过，这是不安全的，但网络通信不会被禁止。

注意：

在具有电子硬件锁的物理安全体系中，使用术语“故障防护状态”和“应急开放状态”。具体而言，应急开放状态的电子锁在断电时就会解锁，而故障防护状态的电子锁在断电时会保持锁定状态。例如，紧急出口的门将被设置为应急开放状态，以便在火灾或其他紧急情况下，人员不会被锁在内部。这种情况下，如果发生事故，主要考虑的是人员能安全离开。相反，银行的金库会被设置为故障防护状态，以便于在断电时，门能保持锁定状态。因为在这种情况下，主要考虑的是安全金库门不被打开。

恢复过程的两个要素能够确保可信解决方案的实施。第一个要素是失败准备。除了可靠的备份解决方案之外，还包括系统恢复及容错方法。第二个要素是系统恢复的过程。系统必须重新启动到单用户、非特权状态。这意味着系统应该重新启动，以达到正常账户能够登录系统且系统不在授权非授权用户登录的状态。系统恢复还包括在发生故障或崩溃时，恢复在系统中使用的所有受影响的文件和服务。恢复所有丢失或受损文件，更正所有变更分类标签，检查所有重要的安全文件的设置。

常见标准(在第 8 章“安全模型的原则、设计和功能”中有所介绍)中有一节是对受信恢复的叙述。恢复过程与系统恢复能力及容错能力相关。具体而言，定义了 4 种类型的受信恢复：

手动式恢复　如果系统崩溃，系统并没有处于故障防护状态。相反的是，在系统故障或崩溃后，管理员需要手动执行必要措施以实现系统恢复。

自动式恢复　对于至少一种类型的系统故障，系统能够自动执行受信恢复。例如，RAID 硬盘能够恢复硬盘驱动器故障，但是不能恢复整个服务器故障。一些类型的故障需要手动恢复。

无过度损失的自动式恢复　这类似于自动式恢复，对于至少一种类型的系统故障，系统能够自动执行恢复过程。然而，其中包括一些能够保护特定对象免受损失的机制。无过度损失的自动式恢复的方法包括对数据及其他对象的恢复。可能含有其他机制，以恢复受损文件、重建日志数据和验证密钥系统和安全组件的完整性。

功能恢复　支持功能恢复的系统能够自动恢复某些特定功能。这种状态能够确保系统成功地完成功能恢复，否则系统将会回到变更前的故障防护状态。

18.2.5　服务质量

服务质量(Qos)控制能够保护负载下的数据网络的完整性。许多不同的因素有助于提升最终用户体验的质量，服务质量对这些要素进行管理，以创造能够满足商业需求的环境。

有助于服务质量提升的一些因素如下：

宽带　可供通信的网络容量。

延迟时间　数据包从源到目的地所需的时间。

抖动　不同数据包之间的延迟变化。

数据包丢失　一些数据包可能会在源和目的地之间传送的过程中丢失，需要重传。

干扰　电噪声、故障设备等因素可能会损坏数据包的内容。

除了控制这些因素之外，服务质量系统往往优先考虑某些业务类型，其中包括对干扰容忍度较小和/或有高业务需求的业务类型。例如，QoS 设备可能会被编程，行政会议室的视频流会优先于实习生电脑的视频流。

18.3　恢复策略

当灾难中断公司业务时，灾难恢复计划应该能够几乎全自动起到作用并开始为恢复操作提供支持。灾难恢复计划应该以下面这种方式进行设计，即使正式的 DRP 团队成员还未到达现场，灾难现场的第一位员工能够以有组织的方式立刻开始恢复工作。接下来，我们将讨论精心设计有效的灾难恢复计划时所涉及的关键子任务，它们将对迅速恢复正常业务过程和重新开始主要业务地点的活动进行指导。

除了提高响应能力之外，购买保险也能够减少经济损失。选择保险时，一定要购买足够责任范围的保险，以便能够从灾难中恢复过来。简单的定额责任范围可能不足以包括实际的更换成本。如果财产保险包括实际现金价值(ACV)条款，受损日该受损财产的公平市场价值减去从购买之日起的累计折旧价值就是能够得到的补偿。这里有一个很重要的关键点，就是除非在保险合同中有关于更换费用的条款，否则组织将要自掏腰包。

有效凭证保险责任范围为记名的、打印的和书面的文档与手稿，以及其他打印的业务记录提供了保护。不过，这种保险的责任范围并不包括对钞票和印刷的安全证书的损坏。

18.3.1 确定业务单元的优先顺序

为了尽可能最有效地恢复业务运营，就必须精心策划灾难恢复计划，以至于优先级别最高的业务单元能被最先恢复。必须识别和优化重要业务功能，以及定义在发生灾难或错误之后，想恢复哪个功能或以什么顺序恢复。

要完成这一目标，DRP 团队必须首先标识那些业务单元并决定它们的优先级顺序，在业务功能方面也需如此(注意主要业务单元并不需要执行所有的业务功能，所以最终分析结果可能含有主要业务单元和其他选择单元的集合)。

该过程应该听起来很熟悉！因为这与第 3 章讨论过的在业务影响评估期间由 BCP 团队执行的优先级划分任务非常相似。事实上，大多数组织将完成业务影响评估(BIA)作为业务连续性规划过程的一部分。这种分析能够检测漏洞、建立策略来降低风险，并最终生成一份 BIA 报告以描述组织面临的潜在风险并确定重要的商业单元和功能。BIA 还确定故障造成的损失，其中包括现金流损失、更换设备的相关费用、加班费、利润损失、无法获得新业务的损失等。根据财务状况、人员、安全、法律合规性、合同履行、质量保证以及货币条款等方面的潜在影响对这些损失进行评估，同时进行评估比较以设置预算。拥有所有的 BIA 信息，便可以使用生成的文件作为优先级任务的基础。

作为最低要求，这个任务完成后的结果应该是一张简单的业务单元优先级列表。然而，更加有用的可交付使用的应该是一张非常详细的、被拆分为具体业务过程的按优先级排序的列表。这个面向业务过程的列表更加真实地反映了现实状况，但需要付出相当大的额外努力。无论如何，它在恢复工作中会给予巨大帮助，但毕竟不是所有最高优先级的业务单元所执行的每个任务都具有最高的优先级别。在试图开始完全恢复工作之前，在组织内最好先恢复最高优先级业务单元 50%的运营能力，然后继续恢复优先级别较低的业务单元，使之达到最小限度的运营能力。

同样的道理，关键的业务流程和功能也必须完成同样的步骤。这其中不仅涉及多个业务单元，还定义了在发生系统崩溃或其他业务中断后，必须恢复的操作要素。在这里，最后的结果应按照优先级顺序列出清单，并列出风险和成本评估，同时还应列出最小恢复时间及相关恢复目标。

18.3.2 危机管理

如果灾难袭击了你的组织，那么很可能会引起恐慌情绪。与之进行斗争的最好方法是使用组织的灾难恢复计划。对于公司中很可能首先注意到发生了紧急情况的个人(也就是保安、技术人员等)，应该对他们进行完整的灾难恢复措施培训，并且让他们知道适当的通知措施和立即响应机制。

许多事情可能看起来属于常识性的问题(如在美国发生火灾时拨打电话 911)，但在紧急情况下，惊恐的员工想到的只是迅速逃离。处理这种情况的最好方法是进行连续的灾难恢复职员培训。回到火灾的例子，应该培训所有的员工在发现火灾时，启动防火警报装置或与紧急情况办公室联系(当然，在这之后，应该采取适当的措施来保护自己的安全)。毕竟，即使消防队接到了组织中 10 个不同人员拨打的报告火灾电话，也比每个人都假设其他人会关注火灾，自己不必打电话的情况好得多。

危机管理是一门科学和技术。如果培训预算支出允许，那么对主要员工进行危机培训是个好主意。这样做能够确保至少有一些员工知道如何使用正确的方法处理紧急情况，并对那些受到灾难恐吓的同事起到重要的现场领导作用。

18.3.3　应急通信

当灾难来袭时，组织能够在内部与外部之间进行通信是很重要的。任何重大的灾难很容易被注意到，如果组织无法与外部保持联系，向外面的人告知恢复状况，公众很容易感到害怕并往最坏处想，进而认为组织无法恢复正常状态。灾难期间，组织内部进行沟通也是很重要的，这样员工就知道他们应该做些什么，例如：是回去工作，还是向另一个地点汇报情况？

在某些情况中，引起灾难发生的环境可能使一些或所有的正常通信手段遭到损坏。猛烈的暴风雨或地震可能已经毁坏了通信系统，此时再试图找到与内部和外部进行通信的其他方法已为时太晚。

18.3.4　工作组恢复

在设计灾难恢复计划时，记住目标是让工作组恢复到正常状态并且重新开始他们在日常工作地点的活动是非常重要的。很容易把工作组恢复变为次要目标，并认为灾难恢复纯粹是 IT 人员的工作，IT 部门重点负责将系统和过程恢复正常。

为了推动这项工作，有时候为不同的工作组开发独立的恢复设施是最好的方法。例如，如果在不同的地点有几家子公司，并且执行的任务与你所在办公室的工作组的任务类似，那么可能希望临时重新安置这些工作组到其他设施工作，并使他们通过电子通信和电话与其他业务单元联系，直至他们准备好回到主运营设施中来。

较大的组织找到能够处理整个业务运营的恢复设施可能很困难，因此这也是不同的工作组适合独立恢复环境的另外一个例子。

18.3.5　可替代的工作站点

灾难恢复计划中最重要的要素之一是：在主要的工作站点无法使用时选择可以替代的工作站点。在考虑恢复设施时，有许多可供选择的方案，方案的多少只会受到灾难恢复计划编制人员和服务提供人员创新能力的限制。接下来，我们将会讨论在灾难恢复计划中经常使用的几类站点：冷站点、温站点、热站点、移动站点、服务局以及多站点。

注意：

选择任何可替代的工作站点时，一定要确认该场所远离主站点，从而使其不会与主站点一起受到相同灾难的影响。但是也要近一些，至少在一天内能开车到达那里。

1. 冷站点

冷站点只是备用设施，它有足够大的地方处理组织的运营工作，并带有适当的电子和环境支持系统。冷站点可能是大的仓库、空的办公大楼或其他类似的建筑物。然而，站点内没有预先安装计算设施(硬件或软件)，并且没有可以使用的宽带通信链接。许多冷站点内确实有一些铜质电话线，某些站点可能还具有备用链接，从而可以使用最低限度的通知设备。

真实场景

冷站点设置

小说《开水房》对冷站点设置做了最好的描述，书中涉及某个脏车店投资商行向期望的客户电话推销伪造的制药投资。当然，在这个虚构的场景中，“灾难”是人为的，但是概念大致相同。

在随时会暴露并遭受执法查抄的威胁之下，这个投资商行在附近建造了一座空的建筑，并且在伪装的冷恢复站点的布满灰尘的水泥地板上摆放了几部银行电话。虽然这些工作是虚构的和非法的，但却说明为了保证业务连续性而维护冗余故障转移恢复站点的真实与合理原因。

研究各种恢复站点，然后考虑哪一种最适合你的特定业务需求和预算。冷站点是最便宜的选择，并且可能是最实用的。温站点包含数据链接，并且为了开始还原操作而对设备进行了预先配置，但是不存在可用的数据或信息。最昂贵的选择是热站点，它完全复制现有的业务基础设施，并且随时准备立即接管主站点。

冷站点的主要优点是成本相对便宜，也就是说没有需要维护的计算基础设备，如果站点未被使用，那么就没有每月的通信费用。然而，这种站点的缺点也是显而易见的，即在制定决策启用该站点到该站点实际准备好能够支持业务运营之间，存在巨大的时间滞后问题。必须先购买服务器和工作站，然后进行安装配置。数据必须从备份磁带中还原。通信链接必须被启动或建立。启动使用冷站点的时间通常需要数个星期，因此及时地完成恢复过程是不可能的，并且经常会产生安全假象。所需的大量时间、精力和费用来激活冷站点和传输操作是值得观察的，这使得这种方法最难测试。

2. 热站点

热站点恰好与冷站点相对。这种类型的建筑布局中具有固定的被维护的备用工作设施，并且附带完备的服务器、工作站和通信链接设备，准备承担主要的运营职责。服务器和工作站都是预先配置好的，并且已经装载了适当的操作系统和应用软件。

主站点服务器上的数据会被定期或持续地复制到热站点中相对应的服务器上，从而确保热站点中所有的数据都是最新的。根据两个站点之间可以使用的带宽，热站点中的数据可以立刻被复制。如果能够做到这一点，那么操作人员一接到通知就可以移到热站点进行操作。如果无法做到这一点，那么灾难恢复管理人员通过下列三种可选择的方法来启用热站点：

- 如果在主站点被关闭之前有充足的时间，那么他们可以在操作控制转换之前强制在两个站点之间进行数据复制。
- 如果这样做不可能，那么他们可以从主站点搬运事务日志的备份磁带到热站点，并以手工方式应用自上次复制以来发生的事务。
- 如果没有任何可用的备份并且无法强制进行复制，那么灾难恢复团队只能接受部分数据的损失。

热站点的优点是相当明显的，这种类型的场所能提供的灾难恢复保护程度是非常好的，然而成本也是极高的。一般来说，为了维护热站点，会使组织购买硬件、软件和服务的预算增加一倍，而且需要额外的人力进行维护。

警告：

如果使用了热站点，那么一定不要忘记那里具有产品数据的副本。同时，要确认热站点与主站点提供了相同级别的技术和物理安全控制。

如果组织希望维持一个热站点，但是又想减少设备和维护费用的支出，那么可以选择使用由外部承包商管理的共享的热站点设施。然而这些设施内在的危险是在灾难普遍发生时，它们可能不堪重负，从而不能为全部用户同时提供服务。如果组织考虑这种安排方式，那么双方一定要在签署合同之前、合同期间定期地彻底调查这些问题。

3. 温站点

温站点介于热站点和冷站点之间，是灾难恢复专家可以选择的中间场所。这种站点往往包含快速建立运营体系所需的设备和数据线路。与热站点一样，这些设备通常是预先配置好的，并准备就绪可以运行合适的应用程序，以便支持组织的业务运作。然而，与热站点不同的是，温站点一般不包含客户数据的备份。使温站点完全处于运营状态的主要要求是将合适的备用介质运送到温站点，并在备用服务器上还原关键数据。

在崩溃后，重新激活站点至少需要 12 个小时。这并不意味着能够在 12 个小时激活的站点就是热站点。然而，大多数热站点的切换时间都在几秒或几分钟之内，完成交接时间也很少超过一个或两个小时。

温站点能够避免在维护操作环境的实时备份方面耗费的电信及人工费用。有了热站点和冷站点，也可以通过共享基础设施得到温站点。如果选择这种方式，请确保在无锁定政策中写明，及时在高需求时期，仍对合适的设备有使用权。深入了解此概念并检查合伙人操作计划，以确定设备能够备份“无锁定”保证。

4. 移动站点

对于传统的恢复站点而言，移动站点属于非主流的替代方案。它们通常由设备齐全的拖车或其他容易重新安置的单元组成。这些场所拥有为维持安全计算环境所需的所有环境控制系统。较大的公司有时候以“移动方式”维护这些站点，随时准备通过空运、铁路、海运或地面运输，在全世界任何地点部署它们。小一些的公司可以在本地与移动站点的供应商联系，这些供应商提供的服务是以客户的随时需求为基础的。

提示：

如果灾难恢复计划依赖于工作组的恢复策略，那么移动站点可能是实现这一过程的好方法。移动站点的空间通常足够大，以至于能容纳整个小型的工作组。

根据要支持的灾难恢复计划，移动站点一般可以被配置为冷站点或温站点。当然，移动站点还可以被配置为热站点，但并不经常这样做，原因在于通常不会提前知道移动站点会部署在哪里。

硬件替换选项

一般而言，确定移动站点和恢复站点时要考虑的一件事情是硬件替换储备。本质上，硬件替换储备具有两个选项。一个选项是利用“内部”替换，此时额外和重复的设备被存放在不同但是很近的位置(也就是城镇另一端的某个仓库)。这里的“内部”意味着已经拥有替换的设备，但是并非意味着必须存放在生产环境中。如果出现硬件故障或灾难，那么可以立即从隐藏处取出适当的设备。另一个选项是与供应商的 SLA 类型约定，从而在发生灾难时能够提供快速的响应和交付。然而，即使与供应商签署了 4、12、24 或 48 小时的替换硬件合同，也不能保证进行可靠的交付。如果将第二个选项作为唯一的恢复选项，那么恢复工作将依赖于太多的不可控可变因素。

5. 服务局

服务局是租借计算机时间的公司。服务局拥有很大的服务器群，并且通常具有大量工作站。任何组织都可以与服务局签署购买合同，以便使用部分处理能力。访问可以是联机的，也可以是远程的。

在发生灾难时，服务局的工作人员通常能够为你的所有 IT 需求提供支持，甚至工作人员还能够使用台式机。与服务局签署的合同往往包含测试和备份以及响应时间和可用性。不过，服务局往往投机于不会同时履行所有合约而超卖实际容量。因此，在出现严重的灾难时存在潜在的资源竞争。如果公司位于行业密集的区域，那么这个因素一定要想到。为了确保有权使用处理设施，可能需要同时选择本地的和远距离的服务局。

6. 云计算

许多组织现在将云计算作为首选的灾难恢复选项。基础设施即服务(IaaS)提供商，如亚马逊网络服务、微软的 Azure、谷歌云计算，以较低的成本按需提供服务。希望保留自己数据中心的公司，可以选择使用这些 IaaS 服务作为备份服务提供商。在云中存储准备运行的镜像是经济实惠的，在云站点被激活之前能够避免大部分的操作成本。

18.3.6 相互援助协议

相互援助协议(Mutual Assistance Agreement，MAA)也被称为互惠协议，在灾难恢复的文学作品中非常流行，但是在真实世界的实践中很少被实施。理论上，相互援助协议提供了优秀的可供选择的工作方案。在 MAA 下，两个组织保证在灾难发生时通过共享计算设施或其他技术资源彼此相互援助。这个协议似乎相当具有成本效益，即任何一个组织都无须维持昂贵的替代工作场所(如在前面讨论的热站点、温站点、冷站点和移动站点)的费用。事实上，许多 MAA 被构造成能够提供 18.3.5 节“可替代的工作站点”中描述的其中一种服务级别。在冷站点的情况中，每个组织可能只是维护他们工作设施中的一些开放的空间，其他组织在发生灾难时可以使用这些空间。在热站点的情况中，组织可能会通过完全冗余的服务器为彼此提供服务。

然而，相互援助协议存在许多缺点，这阻碍了它的广泛使用：

- MAA 很难强制实施。协议参与各方要彼此信任，在灾难发生时能够给予实际的支持。但是，当真的出现灾难时，非受害方可能会拒绝履行协议。受害方只能通过法律手段取得赔偿，但是这样做对于立即进行灾难恢复工作没有帮助。
- 相互合作的组织的地理位置应该相对接近，以便于不同场所之间员工的交通便利。但是，地理位置靠近意味着两个组织很可能遭受相同的威胁。如果你所在的城市发生了地震，协议双方的工作场所都遭到了破坏，那么 MAA 也就没有任何作用了。
- 出于对机密性的考虑，经常会阻止公司将自己的数据放置在其他公司手里。这是出于法律考虑(如医疗或财务数据的处理)或商业考虑(如贸易机密或其他情报财产问题)。

除去这些需要关心的问题，对于组织来说，MAA可能是一种很好的灾难恢复解决方案，尤其当成本成为最重要的考虑因素时。如果对于任何一种类型的替代工作设施的实施费用都无法负担，那么在业务遭到灾难袭击时，MAA能够提供一定程度的有价值的保护措施。

18.3.7　数据库恢复

许多组织依靠数据库来处理和跟踪对于持续运行的非常关键的运营、销售、物流和其他活动。出于这个原因，在灾难恢复计划中包括数据库恢复技术是很重要的。在 DRP 团队中包含数据库专家，他们可以对各种不同的意见提供技术可行性分析，这样做是十分明智的。毕竟，在技术上至少需要大半天时间才能完成还原工作时，肯定不希望分配好几个小时的时间用于还原数据库备份。

接下来，我们将讨论用于创建远程数据库内容备份的三种主要技术手段：电子链接、远程日志处理和远程镜像。每一种技术都有各自的优缺点，这需要分析组织的计算需求和可获得的资源，然后选择最适合公司的方法。

1. 电子链接

在电子链接这种情况中，数据库备份通过批量传送的方式被转移到远处的某个场所。远处的这个场所可以是专用的替代性恢复场所(如热站点)，也可以只是由公司或承包商管理的、用于维护备份数据的远程场所。

如果使用了电子链接，那么需要记住的是，从宣布灾难开始到数据库准备好当前的数据准备运营，可能存在着相当长的时间延迟。如果决定启用恢复站点，技术人员需要从电子链接中检索到适当的备份数据，并应用到恢复站点中即将投入使用的生产服务器上。

警告：

在考虑与供应商签订电子链接合同时，一定要小心。在业内，对电子链接的定义非常广泛。不要满足于“电子链接容量”这样的含糊承诺。一定要坚持提供此项服务的书面定义，包括存储容量、通往电子链接的通信链接带宽，以及在灾难发生时检索到保险库数据所需的时间。

无论哪种类型的备份场景，一定要定期测试电子链接设置。测试备份解决方案的一种好方法是让灾难恢复人员进行一次“突然测试”，即要求他们从某一天开始还原数据。

2. 远程日志处理

远程日志处理以一种更加迅速的方式完成数据的传输。数据传输仍然以批量传输的方式进行，但是发生的更加频繁，通常每小时一次或间隔时间更短。与电子链接不一样的是，在数据库备份文件被转移时，远程日志处理设置传输数据库事务日志的副本，其中包括从上次批量传输以来发生的事务。

远程日志处理与电子链接类似，传输到远程站点的事务日志不是应用于实时数据库服务器，而是使用备份设备进行维护。当宣布发生灾难时，技术人员找到合适的事务日志并将其应用于生产数据库。

3. 远程镜像

远程镜像是最先进的数据库备份解决方案。当然，不必惊讶，也是费用最昂贵的！远程镜像使用的技术水平超过了远程日志处理和电子链接。使用远程镜像时，实时数据库服务器在备份站点进行维护。将数据库修改应用于主站点的生产服务器时，远程服务器同时收到修改副本。因此，镜像服务器准备好在接到通知时，接管运营服务器的角色。

远程镜像是组织寻求实施热站点时一种流行的数据库备份策略。然而，在衡量远程镜像解决方案的可行性时，一定要考虑所需要的支持镜像服务器的基础设施和人员成本，以及附加在镜像服务器上的每个数据库事务的处理开销。

18.4 恢复计划开发

一旦为组织建立业务单元优先级并获得合适的替代恢复场所的办法，就该起草实际的灾难恢复计划了。不要指望一坐下来就能写出全部的计划。在形成最终的书面文档之前，DRP 团队很有可能要经历许多次反复修改草稿文档的过程，以满足关键业务单元的运营需求。计划中要考虑灾难恢复预算对资源、时间和费用的限制，以及可以获得的人力资源。

接下来，我们将会讨论灾难恢复计划中应该包括的一些重要条目。根据组织的规模大小和参与 DRP 工作的人员数量，维护几种针对不同读者的不同类型的计划文档是一个不错的主意。下面列出了一些需要考虑的文档类型：

- 行政部门的总结，提供对计划的高度概括
- 具体部门的计划
- 针对负责实现和维护关键备份系统的 IT 技术人员的技术性指导
- 灾难恢复团队的人员清单
- 为重要灾难恢复团队成员准备的完整计划的副本

在灾难发生或即将来临时，使用特别定制的文档变得尤为重要。在波及组织各个部门的灾难恢复过程中，想要使自己保持头脑清醒的人员能够参考他们所在具体部门的计划。灾难恢复团队的重要成员有一份清单，这份清单在混乱的灾难环境中能够指导他们的行为。IT 人员有一份技术指南，以帮助他们建立和启用替代场所。最后，经理和公关人员有一份简单的文档，不用与灾难恢复工作直接相关的团队成员解释，这份文档的内容能使他们大致了解当前的灾难恢复工作是如何协调在一起的。

提示：

单击如下网址以浏览专业实践图书馆：https://www.drii.org/certification/professionalprac.php，查看工作方法相关文件，并记录 BCP 过程计划及灾难恢复计划。该领域的其他标准文件有 BCI 良好实践指南、(http://thebci.org/index.php/resources/the-good-practice-guidelines)、ISO 27001(www.27001-online.com)和 NIST SP 800-34(http://csrc.nist.gov/publications/PubsSPs.html)。

18.4.1 紧急事件响应

灾难恢复计划中应当包含重要人员在识别出灾难或灾难即将来临时应立即遵守的、简单但内容全面的指令。根据灾难的性质、对事件做出响应的人员种类，以及在需要撤离设施和/或关闭设备之前可用的时间，这些指令千差万别。例如，对于大规模火灾的指令，就要比准备迎接预计将在 48 小时后，在运营地点附近着陆的飓风袭击的指令更加简明。紧急事件响应计划通常以提交给响应者的清单的形式放在一起。当设计这些清单时，需要记住一条重要的设计原则：对清单的任务进行优先级安排，最重要的任务应当放在第一位！

记住这些清单将在危机发生时被执行是很有必要的。响应者无法完成整个清单中的任务是非常

有可能的，特别是在很仓促地通知有灾难发生时。出于这个原因，应该把最重要的任务(例如，“触发火警”)放在清单中的第一位。列表中级别越低的条目，在撤离/关闭之前未被完成的可能性就越大。

18.4.2　人员通知

灾难恢复计划中还应该包括一份人员列表，以便在发生灾难时进行联络。通常，这些人员包括 DRP 团队的重要成员和那些在整个组织内执行关键灾难恢复任务的人员。这份响应清单应该包括可选的联系方式(如呼机号码、手机号码等)，每一位角色还要有一位后备联系人，以防主要联系人无法联系上或出于某种原因不能到达恢复场所的情况。

清单的重要作用

在面对灾难时，清单是非常宝贵的工具。在灾难引发的混乱事件中，清单提供了一系列条理。花费一定的时间确保响应清单为最初的响应者提供清晰的计划，从而保护生命与财产的安全并确保操作的连续性。

针对建筑物火灾的响应清单包括下列步骤:

(1) 启动建筑物警报系统。

(2) 确保有序地进行撤离。

(3) 离开建筑物后，使用移动电话呼叫 911(在美国范围内)，以确保应急机构接收到警报通知。为必需的紧急响应提供额外的信息。

(4) 确保受伤人员接受适当的医疗救护。

(5) 启动组织的灾难恢复计划，以确保业务操作的连续性。

在收集和分发电话通知列表之前，出于对隐私的尊重，一定要询问组织内个人的意见。有关在清单中使用家庭电话号码和其他个人信息时，可能需要遵守特殊的策略。

通知清单应该提供给所有可能对灾难做出响应的人员。这样做能够迅速通知到主要人员。许多公司用“电话树”的形式组织他们的通知清单，即树上的每一个成员联系他下面的人，这样就把通知任务分散到团队的成员之中，而不是只靠一个人拨打许多电话。

如果选择使用电话树通知方案，一定要添加安全网。让每个链中的最后一个人联系第一个人，以确定整个链条上的人都被通知到位。这能够让你放心，证明灾难恢复团队的激活正在顺利进行中。

18.4.3　评估

当灾难恢复团队到达现场时，他们的首要任务之一就是评估现状。这通常以旋转的方式进行:第一响应者进行非常简单的评估、分类活动并启动灾难响应。随着事件的发展，更加详细的评估将用于衡量灾难恢复工作的有效性以及资源分配的优先级。

18.4.4　备份和离站存储

灾难恢复计划(尤其是技术指南)应该完整地说明组织要求的备份策略。实际上，这是任何业务连续性计划和灾难恢复计划中最重要的要素之一。

许多系统管理员已经熟悉各种不同的备份类型，在 BCP/DRP 团队中有一位或几位在这方面拥

有技术专长的专家会使组织受益匪浅。目前存在下列三种主要的备份类型：

完整备份 顾名思义，完整备份存储着受保护设备上包含的数据的完整副本。无论归档比特的设置如何，完整备份都会复制系统中的所有文件。一旦完整备份完成，每个文件的归档比特都会被重置、关闭或设置为 0。

增量备份 增量备份只存储那些自从最近一次完整备份或增量备份以来被修改过的文件。增量备份只复制归档比特被打开、启用或设置为 1 的文件。一旦增量备份完成，所有被复制的文件的归档比特都会被重置、关闭或设置为 0。

差异备份 差异备份存储那些自从最近一次完整备份以来被修改过的所有文件。差异备份只复制归档比特被打开、启用或设置为 1 的文件。不过，与完整备份和增量备份不同的是，差异备份过程并不改变归档比特。

增量备份和差异备份之间最重要的差异在于发生紧急事件时还原数据所需的时间。如果组合使用完整备份和差异备份，那么只需要还原两个备份，也就是最近的完整备份和最近的差异备份。另一方面，如果组合使用完整备份和增量备份，那么就需要还原最近的完整备份以及最近一次完整备份以来完成的所有增量备份。要根据创建备份所要求的时间做出权衡：差异备份的还原时间短，但是生成时间比增量备份长。

备份介质的保存同样至关重要。我们可以方便地将备份介质保存在主操作中心内部或附近，以便轻易满足备份数据的请求，但肯定需要至少在一个离站位置保管备份介质的副本，从而在主操作位置突然受到破坏的情况下能够提供冗余。

使用备份

在系统出现故障时，许多公司都使用两种常用方法之一从备份中还原数据。在第一种情况中，公司在周一晚上进行完整备份，然后在一星期内每隔一个晚上都进行差异备份。如果故障发生在星期六早晨，那么公司需要先还原周一的完整备份，然后只需还原周五的差异备份。在第二种情况中，公司在周一晚上进行完整备份，然后在一星期内每隔一个晚上都进行增量备份。如果故障发生在星期六早晨，那么公司需要先还原周一的完整备份，然后按照时间顺序依次还原每个增量备份(也就是周三、周五的增量备份等)。

大多数组织采取的备份策略都会使用一种以上的备份，并有介质循环使用计划。这允许备份管理人员充分访问备份数据以满足用户的请求，并在尽量减少购买备份介质支出的同时提供容错能力。比较常用的一种备份策略是：每个周末进行一次完整备份，每天晚上进行增量备份或差异备份。具体的备份方式和所有详细的备份流程取决于组织的容错要求。如果无法容忍少量的数据丢失，那么容忍故障的能力比较低。然而，如果数小时或数天的数据丢失都没有严重的后果，那么容忍故障的能力是比较高的。

真实场景

经常被忽略的备份

对于已知的计算灾难而言，备份可能是最少实践和最容易忽视的预防措施。工作站上所有操作系统和个人数据的综合备份频率小于针对服务器或关键任务计算机的备份频率，但是它们都具有同样的和必要的用途。

Damon 是一位信息专家，在导致一家信息经纪公司一楼毁坏的一次自然灾难中，他数月的工作成果付之东流，此时他才真正认识到备份的重要性。Damon 从未利用系统中内建的备份设施或由管理员 Carol 建立的任何共享设备。

作为管理员，Carol 对备份解决方案比较了解。她在生产服务器上建立增量备份，在开发服务器上建立差异备份，并且从未遇到过还原丢失数据的问题。

固定备份策略面对的最棘手的障碍是人类的天性，因此简单的、透明的和综合的策略是最实用的。差异备份只要求两个容器文件(最新的完整备份和最新的差异备份)，并且可以计划在某些特定的时间间隔定期更新。因此，Carol 选择实现这种方式，并且她随时准备在需要时还原备份。

1. 备份介质格式

物理特征和轮换周期是有价值的备份解决方案应当跟踪和管理的两个因素。物理特征是使用中的磁带驱动器的类型，它定义了介质的物理形状。轮换周期是备份的频率和受保护数据的保留时间。通过查看这些特征，可以确保有价值的数据被保存在可用的备份介质上。备份介质具有最大使用限制；统计表明，在开始丧失可靠性之前，备份介质可能被重写 5、10 或 20 次。介质格式存在下列广泛类型：

- 数字数据存储(DDS)/数字音频磁带(DAT)
- 数字线性磁带(DLT)和超强 DLT
- 线性磁带开放式技术(LTO)

2. 磁带到磁带(D2D)备份

在过去的 10 年中，磁盘存储变得越来越便宜。现今，驱动能力已经开始使用百万兆字节(TB)来测量，磁带和光盘已无法应付数据量的要求。现在很多企业将磁盘到磁盘(D2D)备份方式应用于灾难恢复策略。

一个重要的注意事项：采用完整的磁盘到磁盘备份方法的组织，必须确保地理多样性。一些磁盘需要异地保存。许多组织通过租用托管服务提供商来管理远程备份位置。

提示：

随着传输和存储成本的下降，基于云的备份解决方案正在变得更具成本效益。可能会选择类似服务而不是使用物理传输方式将备份发送到远程位置。

3. 最佳备份做法

无论采用哪一种备份解决方案、介质或方法，都必须解决一些常见的备份问题。例如，备份和还原活动可能庞大和缓慢。这样的数据移动会显著影响网络的性能，在日常的工作时间内更是如此。因此，备份应当被调度在空闲时间(如晚上)进行。

备份数据量会随着时间的推移而增加，这会导致每次的备份(和还原)过程都比之前花费更长的时间，并且占用备份介质上的更多空间。因此，需要在备份解决方案中设计足够的容量来处理合理时间段内备份数据的合理增长。在这里，是否合理完全取决于具体环境和预算。

在使用定期备份的情况下(也就是说每隔 24 小时进行一次备份)，总是有可能存在备份以来的数据丢失的现象。Murphy 定律表明服务器在成功备份之后不会立即崩溃，而是往往在下一次备份开始前发生。为了避免定期备份存在的问题，需要部署某些实时连续的备份形式，例如 RAID、群集或

服务器镜像。

最后，请记住测试组织的恢复流程。企业往往出现的事实就是备份软件报告备份成功而恢复尝试却失败，然而检测到有问题时已经太晚了。这是备份失败的最大原因之一。

4. 磁带轮换

备份常用的几种磁带轮换策略包括：祖父-父亲-儿子(Grandfather-Father-Son，GFS)策略、汉诺塔策略以及六磁带每周备份策略。这些策略相当复杂，尤其在使用很大的磁带组时更是如此。可以通过使用一支铅笔和一本日历来人工实现这些策略，也可以通过使用商用备份软件或全自动分层存储管理(Hierarchical Storage Management，HSM)系统来自动实现这些策略。HSM 系统是自动化的机械备份换带机，由 32 或 64 个光学或磁带备份设备组成。HSM 系统中的所有驱动器元素都被配置为单个驱动器阵列(有些像 RAID)。

注意：

有关各种磁带轮换的细节超出了本书的讨论范围，如果读者想了解更多的信息，那么可以在互联网上搜索相关的内容。

18.4.5 软件托管协议

软件托管协议是一种特殊的工具，可以对公司起到保护作用：避免公司受软件开发商的代码故障的影响，以便为产品提供足够的支持，还可以防止出现由于软件开发商破产而造成产品失去技术支持的情况。

提示：

集中精力与那些规模大小有可能破产的软件供应商商谈软件托管协议。当然，不可能与像微软这样的公司讨论这种协议，除非负责的是一家非常大的公司并且拥有讨价还价的能力。另一方面，像微软这么大的公司也不大可能破产，不会导致终端用户孤立无援。

如果组织依赖于定制开发的或小公司生产的软件产品，那么可能需要考虑开发这种类型的协议，从而将其作为灾难恢复计划的一部分。在软件托管协议下，软件开发商将应用程序源代码的副本提供给独立的第三方组织。然后，第三方用安全的方式维护源代码副本备份的更新。终端用户和开发商之间的协议具体说明了什么是“触发事件”，如开发商满足服务级别协议(SLA)条款失败或开发商的公司破产。当触发器事件发生时，第三方会向终端用户发布应用程序源代码的副本。随后，终端用户可以通过分析源代码来解决应用程序的问题或实现软件的升级。

18.4.6 外部通信

在灾难恢复期间，与组织外部不同的实体进行通信是很有必要的。需要联系供应商提供供应物资，以便在需要时他们能够支持灾难恢复工作。客户会与你联络，从而确认仍在运营。负责公关的领导可能需要联系媒体或投资公司，经理可能需要与政府的管理局进行会谈。出于这些原因，灾难恢复计划中必须包括数量充足的与外部联络的通信渠道，以便满足公司的运营需求。通常，在灾难期间由 CEO 作为发言人不是合理的业务实践或恢复实践。公司应当雇用和培训媒体联络人员，以

便随时准备担负此责任。

18.4.7　公用设施

如本章前面所述，组织要依靠一些公用设施来提供自身基础设施的关键要素，如电力、水、天然气和管道服务等。因此，灾难恢复计划中应该包括解决这些服务在灾难发生过程中出现问题的联系信息和措施。

18.4.8　物流和供应

灾难恢复操作过程中有关物流的问题是值得关注的。此时，你会突然面对调拨大量人员、设备和供应物资到备用恢复场所的问题。人员可能会在那些场所内生活很长一段时间，并且灾难恢复团队会负责给他们提供食物、水、避难所和适当的设施。如果这些情况恰好发生在预期操作范围之内，那么灾难恢复计划中就应该包括这样的条款。

18.4.9　恢复与还原的比较

有些时候，区分灾难恢复任务和灾难还原任务是很有用的。在估计恢复工作要花费很长时间时，这尤为重要。在灾难恢复团队被指派执行和维护恢复场所工作时，一支救助团队被指派还原主要场所的运营能力，这些任务分配的制订应当依据组织的需要和灾难的类型。

注意：

恢复与还原是不同的概念。在这里，恢复涉及将业务操作和过程还原至工作状态；还原涉及将业务设施和环境还原至可工作状态。

灾难恢复团队成员可以操作的时间范围很短，他们必须尽可能迅速地应用 DRP 和还原 IT 能力。如果灾难恢复团队不能在 MTD/RTO 内还原业务过程，那么公司就会遭受损失。

一旦人们相信原有场所是安全的，那么抢救团队成员就会开始工作。他们的工作是将公司还原至最初的全部能力，并且在必要时还原至原始位置。如果原始位置不再存在，那么就需要为公司选择新的地点。抢救团队必须重构或修复 IT 基础设施。因为这个活动基本上与构建新的 IT 系统相同，所以从可替代的恢复场所返回至最初的主要场所的活动本身具有风险。此外，抢救团队的工作时间多于恢复团队的工作时间。

抢救团队必须确保新的 IT 基础设施的可靠性。通过将最小关键任务进程返回至被还原的原有场所，进而对重构的网络进行压力测试，抢救团队就可以实现这个目标。一旦被还原的场所展现了自己的恢复能力，那么更重要的进程会被转移至原有场所。关键任务进程返回原有场所时存在严重的脆弱性。返回原有场所的动作可能导致自身的灾难。因此，只有在全部的正常操作都返回至被还原的原有场所后，才能宣告紧急状态结束。

在结束所有灾难恢复工作之后，就需要在原有场所执行还原操作，并且终止灾难恢复约定下的任何处理场所操作。DRP 应当指定能够确定何时适合返回原有场所的标准，并且指导 DRP 恢复和抢救团队进行有序转移。

18.5 培训、意识与文档记录

与业务连续性计划一样，对所有涉及灾难恢复工作的人员进行培训是十分重要的。培训所要求的程度根据个人在公司中的职位和工作角色而有所不同。当设计培训计划时，应该考虑下面这些要素：

- 对全体新员工进行定向培训。
- 对第一次担任新的灾难恢复角色的员工进行基本培训。
- 对灾难恢复团队的成员进行详细的复习培训。
- 对所有的其他员工进行简要的复习培训(可以作为会议的一部分完成培训或通过像电子邮件的时事通讯这样的介质发送给所有员工)。

提示：

活页夹为灾难恢复计划提供了一种良好的存储选择，这样可以不破坏整个计划而单独修改一页纸上的计划。

灾难恢复计划还应该进行完整的文档记录。在本章的前面，我们讨论了几种可供使用的文档记录方式。一定要实现必要的文档记录程序，并在计划发生改变后修改文档。因为灾难恢复计划和业务连续性计划快速改变的本质，所以可以考虑在组织的内部网上发布有保证的部分。

DRP 应当被视为极其敏感的文档，并且只在有分类和“需知”的基础上提供给个人。参与计划的人员应当完全理解其角色，但是不必知道或访问完整的计划。当然，确保 DRP 团队关键成员和高级管理人员知晓整个计划和理解高级实现细节是必不可少的。完全不必让每位参与计划的人员都了解所有的内容。

警告：

需要记住的是，灾难可能导致内部网不可用。如果选择通过内部网分发灾难恢复计划和业务连续性计划，那么一定要确保在主要场所和替代场所都保存足够数量的打印副本，并且只保存最新的副本。

18.6 测试与维护

每一种灾难恢复计划都必须定期进行测试，以确保计划的条款是可行的并且符合组织变化的需要。可以实施的测试类型依赖于能够使用的恢复设施的类型、组织的企业文化和灾难恢复团队成员的可用性。本章余下的部分将讨论 5 种主要的测试类型：通读测试、结构化演练、模拟测试、并行测试和完全中断测试。

18.6.1 通读测试

通读测试是其中一种最简单的测试，但也是最重要的一种测试。在这种测试类型中，只需向灾难恢复团队成员分发灾难恢复清单的副本，并要求他们审查清单。这样就允许同时实现下列三个目标：

- 清单确保关键人员意识到他们的职责并定期复习知识。
- 清单为人员提供了审查清单中过时信息的机会，并根据组织的变化更新需要修改的条目。
- 在大型组织中，清单能够帮助标识这样的情况：重要的人员已经离开公司，并且没有人为重新分配他们的灾难恢复职责而负责！这也是为什么灾难恢复职责应该包含在工作描述中的原因。

18.6.2　结构化演练

结构化演练进一步进行了测试。在这种经常被称为“桌面练习”的测试类型中，灾难恢复团队成员聚集在一间大会议室中，不同的人在灾难发生时扮演不同角色。通常，确切的灾难情景只有主考官知道，他在会议上向团队成员描述具体的情况。然后，团队成员通过参考他们的灾难恢复计划对特定的灾难类型进行讨论，进而得出适当的响应办法。

18.6.3　模拟测试

模拟测试与结构化演练类似。模拟测试为灾难恢复团队成员呈现情景并要求他们产生出适当的响应措施。与前面讨论的测试不同，其中某些响应措施随后会被测试。这种测试可能涉及中断非关键的业务活动并使用某些操作人员。

18.6.4　并行测试

并行测试表示下一个层次的测试，并涉及将实际人员重新部署到替换的恢复场所和实现场所启用措施。被重新部署到该场所的员工，以灾难实际发生时的方式执行他们的灾难恢复职责。唯一的差别在于主要设施的运营不会被中断，这个场所仍然处理组织的日常业务。

18.6.5　完全中断测试

完全中断测试与并行测试的操作方式类似，但涉及实际关闭主场所的运营并将其转移到恢复场所。出于很明显的原因，完全中断测试安排起来极其困难，并且经常会遇到来自管理层的阻挠。

18.6.6　维护

需要记住的是，灾难恢复计划是一份灵活的文档。随着组织需求的变化，必须对灾难恢复计划进行修改以符合变化的需要。通过使用组织好的和协调一致的测试计划，我们会发现灾难恢复计划中需要修改的地方。微小的变化经常会通过一系列的电话交谈或电子邮件而进行，然而重大的变化可能需要整个灾难恢复团队进行一次或几次会议商讨。

灾难恢复计划编制人员应当将组织的业务连续性计划借鉴为恢复工作的模板。这个模板和所有支持性素材都必须遵守美国联邦的法规和反映当前的业务需求。业务过程(如薪水和订单生成)应当包含映射到支持性 IT 系统和基础设施的特定度量。

大多数组织都应用正式的变更管理过程，这样在 IT 基础设施发生更改时能够更新和检查所有相关的文档，以便反映更改。通过调度常规的消防训练和演练来确保 DRP 的所有元素都被正确地使用，从而对所有职员进行培训，并且也是将变更集成到日常维护和变更管理措施中的一次极佳机会。每次设计、实现和记录更改时，都需要重复这些过程和实践。一定要了解所有设施的位置，并且正确地维护 DRP 工作的所有元素，在出现紧急情况时，就需要使用恢复计划。最后，要确保所有职员经过培训，从而提高现有支持人员的技能，并且确保新员工尽快了解相应的工作。

18.7 本章小结

灾难恢复计划是完整的信息安全计划的关键。无论业务连续性计划有多全面，当业务被一场灾难中断时，都将面临快速而有效地恢复运营的问题。

在本章中，你了解了不同类型的可能会影响业务的自然和人为灾害，你还探索了恢复场所的类型和提高恢复能力的备份策略。

组织的灾难恢复计划是安全专业人员监管下的一份最重要的文件，能够为在发生灾难时负责确保操作连续性的工作人员提供保障。在将主场所恢复到运行状态的同时，DRP 能够提供激活交替处理场所事件的有序序列。一旦成功地开发了 DRP，就要培养相应的使用人才，以确保准确记录，并定期进行检查以确保响应人员对计划有清晰的概念。

18.8 考试要点

了解可能威胁组织的常见自然灾难。经常威胁组织的自然灾难包括地震、洪水、暴风雪、火灾、海啸和火山爆发。

了解可能威胁组织的常见人为灾难类型。常见的人为灾难包括爆炸、电气火灾、恐怖行为、电力中断、其他公共设施故障、基础设施故障、硬件/软件故障、罢工、盗窃和故意破坏。

熟悉常见的恢复设施类型。常见的恢复设施包括冷站点、温站点、热站点、移动站点、服务局以及多站点。必须理解每种设施的优点和缺陷。

解释相互援助协议的潜在优点及其不能在当今的商业活动中普遍实现的原因。虽然相互援助协议(MAA)提供了相对廉价的灾难恢复替代场所，但是由于它们无法强制实施而不能被普遍使用。参与 MAA 的组织可能会由于相同的灾难而被迫关闭，并且 MAA 还会引发机密性问题。

了解可以帮助数据库备份的技术。数据库得益于三种备份技术。电子传送用于将数据库备份传输到远程站点，作为批量传输的一部分。远程日志则用于更频繁的数据传输。借助远程镜像技术，数据库事务在实时备份站点镜像。

了解灾难恢复计划测试的 5 种类型和每种测试对正常业务运营的影响。灾难恢复计划测试的 5 种类型是通读测试、结构化演练、模拟测试、并行测试和完全中断测试。通读测试完全是文书工作练习，而结构化演练涉及项目组会议。两者都不会影响业务运营。模拟测试可能会使非关键的业务停止运作。并行测试涉及重新部署人员，但不会影响日常运作。完全中断测试包括关闭主要系统以及将责任转移到恢复设施。

18.9　书面实验

1. 当企业考虑采用相互援助协议时有哪些主要担忧？
2. 列出并解释 5 种类型的灾难恢复测试。
3. 解释本章讨论的三类备份策略之间的差异。

18.10　复习题

1. 什么是灾难恢复计划的最终目标？
   A. 防止业务中断
   B. 建立临时业务运营
   C. 恢复正常的业务活动
   D. 最小化灾难影响
2. 下列哪一项是人为灾难的例子？
   A. 海啸
   B. 地震
   C. 停电
   D. 雷击
3. 根据美国联邦紧急事务管理局的统计，美国各州至少有地震活动的中等风险的比例大概是多少？
   A. 20%
   B. 40%
   C. 60%
   D. 80%
4. 下列哪一种灾难类别不受通常的商业标准或房主保险覆盖？
   A. 地震
   B. 洪水
   C. 火
   D. 盗窃
5. 在 9 • 11 恐怖袭击事件以后，什么行业的剧烈变化直接影响到 DRP/BCP 活动？
   A. 旅游
   B. 银行
   C. 保险
   D. 航空公司
6. 下面有关业务连续性计划和灾难恢复计划的描述中哪一个是不正确的？
   A. 业务连续性计划的重点是当灾难发生时保持业务功能不间断
   B. 企业可以选择是否制定业务连续性计划或灾难恢复计划
   C. 业务连续性计划弥补了灾难恢复计划的不是
   D. 灾难恢复规划指导组织恢复主站点的正常运营

7. “百年一遇洪水”对于应急准备的官员是什么意思?
   A. 最后一次袭击该区域的任何类型的洪水超过 100 年之久
   B. 在任何一年洪水发生的可能性在 1/100 的级别
   C. 预计该区域由洪水带来的问题至少 100 年是安全的
   D. 对该地区最后一次严重洪水袭击已过 100 年之久
8. 下列哪种数据库恢复技术之一是准确的、数据库保持在备选位置的最新副本?
   A. 事务记录
   B. 远程日志
   C. 电子传送
   D. 远程镜像
9. 什么灾难恢复原则能最好地保护组织避免硬件故障?
   A. 一致性
   B. 效率
   C. 冗余
   D. 首要
10. 什么业务连续性计划技术可以帮助准备灾难恢复计划的业务单元优先任务?
   A. 脆弱性分析
   B. 业务影响评估
   C. 风险管理
   D. 连续性规划
11. 下列哪个备选处理场所需要的激活时间最长?
   A. 热站点
   B. 移动站点
   C. 冷站点
   D. 温站点
12. 灾难声明后估计激活温站点的标准时间是多长?
   A. 1 小时
   B. 6 小时
   C. 12 小时
   D. 24 小时
13. 下列哪一项是热站点的特征而不是温站点的特征?
   A. 通信电路
   B. 工作站
   C. 服务器
   D. 当前数据
14. 哪种数据库备份策略类型包括在远程站点维护实时的备份服务器?
   A. 事务记录
   B. 远程日志
   C. 电子传送
   D. 远程镜像

15. 什么类型的文件能够帮助公关专家和其他需要灾难恢复工作的高度概括总结的人？

A. 执行摘要

B. 技术指南

C. 具体部门计划

D. 清单

16. 什么灾难恢复计划工具可以用来防止为所提供产品提供相应支持的重要软件公司破产？

A. 差异备份

B. 业务影响评估

C. 增量备份

D. 软件托管协议

17. 什么类型的备份包括所有文件自最近一次完整备份以来存储修改文件的拷贝？

A. 差异备份

B. 部分备份

C. 增量备份

D. 数据库备份

18. 什么样的备份组合策略能提供最快的备份创建时间？

A. 完整备份和差异备份

B. 部分备份和增量备份

C. 完整备份和增量备份

D. 增量备份和差异备份

19. 什么样的备份组合策略提供最快的备份还原时间？

A. 完整备份和差异备份

B. 部分备份和增量备份

C. 完整备份和增量备份

D. 增量备份和差异备份

20. 什么类型的灾难恢复计划测试在备份设施中充分评估运营，但不转移主站点业务的主要运营责任？

A. 结构化演练

B. 并行测试

C. 全中断测试

D. 模拟测试

第 19 章

事件与道德规范

本章中覆盖的 CISSP 考试大纲包含：

1. 安全和风险管理
- E. 理解职业道德
  - E.1 实践(ISC)^2 职业道德准则
  - E.2 支持组织的道德准则

7. 安全运营
- A. 理解和支持调查
  - A.1 证据收集和处理(例如，监管链、采访)
  - A.2 报告和文档
  - A.3 调查技术(例如，根本原因分析、事故处理)
  - A.4 数字取证(例如，介质、网络、软件和嵌入式设备)
- B. 理解调查取证类别的要求
  - B.1 操作型调查
  - B.2 犯罪调查
  - B.3 民事调查
  - B.4 监管调查
  - B.5 电子发现(eDiscovery)

本章中，我们探讨事件处理过程，包括计算机犯罪是否已被提交的调查技术以及适当时证据的收集技术。本章还包括对道德问题及信息安全从业人员行为准则的完整讨论。

决定如何应对计算机攻击的第一步是要了解攻击是否发生或何时发生。在选取合适的应对措施之前，应了解如何确定攻击正在发生或攻击已经发生。一旦发现攻击已经发生，下一步就是进行调查和收集证据，找出发生了什么，并确定损害程度。必须确保调查方式遵守当地的法律法规。

19.1 调查

所有信息安全专家迟早都会遇到需要调查的安全事件。在很多情况中，这种调查将是简短的、

非正式的确定事件，不足以严重到授权进一步的行动或执法机构的介入。然而在一些情况中，产生的威胁或造成的破坏将足以严重到需要进行更正式的调查。当这种情况出现时，调查人员必须仔细调查，确保执行正确的步骤。违背正确的步骤可能会侵犯被调查者的公民权利，并且可能导致失败的诉讼，甚至导致被调查者采取合法的抵抗措施。

19.1.1 调查的类型

安全实践人员发现他们执行的调查有各种理由。一些调查涉及法律法规且调查证据必须严格遵守法院可接受的标准，还有一些调查由于必须支持内部业务流程，因此要求更严格。

1. 操作型调查

操作型调查研究涉及组织的计算基础设施问题，且首要目标为解决业务问题。例如，如果 IT 团队在 Web 服务器上发现性能问题，就会执行有关确定性能问题起因的调查。

提示：

操作型调查可能会迅速过渡到另一种类型的调查。比如，对性能问题的调查可能会发现一些可能成为犯罪调查的系统入侵证据。

操作型调查对信息收集标准是比较宽松的。因为目标仅仅是完成内部业务目标，所以不倾向找出证据。因为解决问题是首要目标，所以管理员进行操作型调查时只进行必要的分析，得出他们的操作结论而不需要拿出特别详细且充分的调查证据。

除了解决操作问题，操作型调查需要执行旨在识别操作出现问题的根本原因分析。执行根本原因分析是为了找出修复措施，以防止今后类似事件再次发生。

2. 犯罪调查

犯罪调查通常由法律执行者进行，是针对违法行为进行的调查。犯罪调查的结果是指控犯罪和在刑事法庭上控诉。

多数犯罪案件必须满足超越合理怀疑的证据标准。根据这个标准，控方必须证明被告犯罪，凭借事实而不是其他逻辑结论。为此，犯罪调查必须遵循非常严格的证据收集和保存过程。

3. 民事调查

民事调查通常不涉及执法，而涉及内部员工和外部顾问代表法律团队的工作。他们会准备必要的证据来解决双方之间的纠纷。

大多数的民事案件不会遵循超出合理怀疑证据的标准。相反，它们使用较弱的证据标准。要达到这一标准，只需要证据能够说明调查结果是可信赖的。因此，民事调查的证据收集标准并不像犯罪调查要求那么严格。

4. 监管调查

政府机构在他们认为个人或企业可能违反法律时会执行监管调查。监管机构通常会在他们认为可能发生的地点进行调查。监管调查范围比较广泛，几乎总是由政府工作人员执行。

5. 电子发现

在诉讼过程中，任何一方有责任保留与案件相关的证据，并在发现过程中在控诉双方之间分享信息。这个发现过程应用纸质档案和电子记录及电子发现(eDiscovery)的过程促进电子信息披露的处理。

电子发现参考模型描述了发现的标准过程，共需如下 9 步：

(1) **信息治理**　确保信息系统针对将来的发现有良好的组织。

(2) **识别**　当组织相信起诉很有可能时，要指出电子发现请求信息的位置。

(3) **保存**　确保潜在的发现信息不会受到篡改或删除。

(4) **收集**　将敏感信息收集起来用于电子发现过程。

(5) **处理**　过滤收集到的信息并进行无关信息的“粗剪”，减少需要详细检查的信息。

(6) **检查**　检查留下的信息，以确定哪些信息是敏感的请求并移除那些律师与客户之间保护的任何信息。

(7) **分析**　对留下来的内容和文档执行更深层次的检查。

(8) **产生**　用需要分享他人的信息标准格式产生信息。

(9) **呈现**　向证人、法院和其他当事方演示信息。

进行 eDiscovery 是一个复杂的过程，需要在 IT 专业人员和法律顾问之间仔细协调。

19.1.2　证据

为了成功地检举犯罪，起诉律师必须提供足够的证据来证实某个人的罪行超出合理的怀疑。接下来，我们将研究证据在法庭上被许可之前要满足的要求、可以使用的不同类型的证据，以及处理和记录证据的需求。

提示：

NIST 的指南把司法鉴定技术整合到了事件响应(SP 800-86)中，大量资料可以查询 www.csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf。

1. 可接纳的证据

在法庭上采纳的证据有三种基本要求。要成为可接纳的证据，必须满足下列所有三个要求(在法庭公开讨论之前由法官确定)：

- 证据必须与确定事实相关。
- 证据要确定的事实必须对本案来说是必要的(即相关的)。
- 证据必须有法定资格，这意味着必须合法获得。通过非法搜查获得的证据由于不具备法定资格，是不可接纳的。

2. 证据的类型

在法庭上可能使用的证据有 4 种类型：实物证据、文档证据、言辞证据以及可论证的证据。每一种证据都有稍许不同的额外可接纳要求。

实物证据　实物证据也被称为客观证据，包括那些可能会被实际带到法庭上的物品。在常见的犯罪行动中，这可能包括谋杀凶器、衣物或其他有形物体。在计算机犯罪中，实物证据可能包括没

收的计算机设备，如带有指纹的键盘或黑客计算机系统中的硬盘。根据具体的环境，实物证据还可能是无可辩驳的结论性证据，如 DNA。

文档证据 文档证据包括所有带到法庭上用于证明事实的书面内容。这种证据类型也必须经过验证。例如，如果律师希望将计算机日志作为证据，那么必须将证人(即系统管理员)带到法庭上，以证明日志是作为常规的商业活动收集的，并且是系统实际收集的真实日志。

下列两种额外的证据规则被特别应用于文档证据：

- 最佳证据规则声明，当文档作为法庭处理的证据时，必须提供原始文档。除了规则应用的某些例外之外，原始证据的副本或说明(被称为次要证据)不会被接受为证据。
- 口头证据规则声明，当双方的协议被以书面的形式记载下来时，书面文档被假设包含所有协议的条款，并且口头协议不可以修改书面协议。

如果文档证据满足必要、有作证能力以及关联要求，并且还符合最佳证据和口头证据规则，那么就可能被法庭采纳。

证据链

像所有类型的证据一样，实物证据必须在提交给法庭之前满足关联、必要和有作证能力的要求。此外，实物证据必须经过验证。这可以通过能够实际确认目标唯一的证人来完成(如“刀柄上有我名字的那把刀就是闯入者从我房中的桌子上拿起并刺伤我的那把刀”)。

在很多案件中，证人在法庭上唯一确认物品是不可能的。在这些案件中，就必须建立证据链(chain of evidence，也被称为监管链(chain of custody))。这涉及所有处理证据的人，包括收集原始证据的警员、处理证据的证物技术人员以及在法庭上使用证据的律师。对证据的位置必须从被收集的时刻到出现在法庭上的时刻进行完整记录，以确保是同一证据。这需要对证据进行彻底标记，记录谁在特定的时间接触过这个证据，以及要求接触证据的原因。

当标记证据以维护监管链时，标签应当包含下列与证据收集相关的信息：

- 证据的一般性描述
- 证据收集的时间和日期
- 证据收集源自的确切位置
- 证据收集人员的名字
- 证据收集的相关环境

处理证据的每个人都必须签署监管日志链，以表明直接负责处理证据的时间以及交予监管链中的下一个人的时间。监管链必须提供完整的事件序列，从而说明从证据收集开始到审问之间的过程。

言辞证据 言辞证据十分简单，是包括证人证词的证据，证词既可以是法庭上的口头证词，也可以是记录存储的书面证词。证人必须宣誓同意讲真话，并且他们必须了解证词的根据。此外，证人必须记得证词的根据(他们可以参考书面注释或记录来协助记忆)。证人可以提供直接证据：基于自己的直接观察来证明或驳斥某个断言的口头言辞。大多数证人的言辞证据都被严格地限定为基于证人的事实观察的直接证据。不过，如果法庭认为证人是特定领域的专家，那就不应采用这种方法。在这种案件中，证人可以基于其他存在的事实及其个人的专业知识来提供专家观点。

言辞证据不得是所谓的传闻证据。证人不可能证实其他人在法庭外告诉他的内容。没有经过系统管理员验证的计算机日志文件也可能被认为是传闻证据。

3. 证据收集和司法取证

收集数字证据是一个复杂的过程，并且应当只由专业的司法技术人员进行。计算机证据国际组织(IOCE)概述了指导数字证据技术人员的 6 条原则：

- 处理数字证据时，必须应用所有通用的司法和程序原则。
- 收集数字证据后，不能对证据有所修改。
- 某人有必要使用原始数字证据时，应当接受有针对性的培训。
- 与收集、访问、存储或转移数字证据有关的所有活动都应当被完整地记录和保留，并且可供审查。
- 在数字证据被某人掌握之后，他应当对与数字证据有关的所有活动负责。
- 所有负责收集、访问、存储或转移数字证据的机构都负责遵守上述原则。

进行取证时，保留原来的证据也很重要。请记住，调查行为可能会改变正在评估的证据。因此，在分析数字证据时，最好使用副本。例如，当对硬盘驱动器上的内容进行调查时，制作驱动器镜像，并将原始驱动器密封在证据袋中，然后使用镜像进行调查。

介质分析　介质分析是计算机取证分析的一个分支，涉及存储介质中信息的识别和提取。可能包括：

- 磁介质(如磁盘、磁带)
- 光学介质(如 CD、DVD、蓝光光盘)
- 存储器(如内存、固态存储)

用于介质分析的技术可能包括从物理磁盘的未分配扇区恢复已删除文件，对连接到计算机系统的存储介质的分析(检查加密介质设备时会有益处)，以及存储介质的法医图像的静态分析。

网络取证分析　调查人员常对发生在网络上的安全事件感兴趣。由于网络数据的波动性，事件很难重建。除非是在事件发生时有意记录，否则事件记录并不会被保存。

因此，网络取证分析往往取决于对事件发生的预先了解，或使用记录网络活动的已经存在的安全控制。这些措施包括：

- 入侵检测和防御系统日志
- 通过流量监测系统捕获的网络流量数据
- 事件发生过程中有意收集的数据包
- 日志、防火墙和其他网络安全设备

网络取证分析师的任务是收集不同来源的信息，并将它们关联起来，然后完成一份尽可能全面的网络构图。

软件分析　网络取证分析师也会对软件及其活动进行检查。在某些情况下，当内部人员被怀疑时，网络取证分析师可能会要求对软件代码进行审查，以寻找后门、逻辑炸弹或其他安全漏洞。有关这些主题的更多内容，请参见第 21 章“恶意代码与应用攻击”。

在其他情况下，网络取证分析师可能也会被要求对应用程序或数据服务器的日志文件进行检查并做出解释，也会寻找恶意活动，如 SQL 注入攻击、特权升级或其他应用程序攻击。这些问题在第 21 章中有所讨论。

硬件/嵌入式设备分析　最后，网络取证分析师还要对硬件和嵌入式设备的内容进行分析。这可能包括对个人电脑、智能手机、平板电脑、嵌入汽车/安全系统/其他设备的电脑和其他设备的审查。

进行这些审查的分析师必须具有专业的相关知识。这往往需要熟悉内存、存储系统以及操作系

统和相关设备的专家顾问。由于软件、硬件和存储设备之间复杂的相互交互，硬件分析需要掌握介质分析和软件分析技能。

19.1.3 调查过程

当启动计算机安全调查时，应该首先召集一支有能力的分析师团队，以协助调查。该团队应根据组织现有的事件响应策略进行操作，同时应给予该团队一份章程手册。其中应清楚概述调查范围；调查人员的权力、角色和责任；以及调查过程中必须遵守的参与制度。这些规则能够规定并指导调查人员在不同阶段采取的行动，比如遵守法律、审讯犯罪嫌疑人、收集证据以及破坏系统访问。

1. 请求执法

在调查中必须做出的首要决定是：是否要请求执法机构介入。这实际上是一个相当复杂的决定，应当涉及资深管理官员。请求专家协助有很多因素。例如，FBI 现在有一个美国国家计算机犯罪小组，组里包括具有下列资质的人：

- 计算机科学学位
- 在业界和学术机构有领先的工作经验
- 受过基本的和高级的商业培训
- 具备基本的数据和通信网络知识
- 拥有 Unix 和其他计算机操作系统的使用经验

另一方面，还有两个主要因素可能使公司回避请求官方的协助。首先，调查将更可能公开化，并且可能给公司带来麻烦。其次，执法机构一定要采取遵从第四修正案和其他合法要求的调查方式，而如果公司自我实施私下调解，则不需要这么做。

搜查证

即使很少观看美国警匪电视剧的观众也都熟悉这样的话："你有搜查证吗？"美国国会通过的第四修正案概述了调查人员在进行特定搜查之前应当取得有效的搜查证以及取得搜查证时应当克服的法律障碍：

"人们的人身、房屋、文件和财产具有受保护而不被不合理地搜查和获取的权利，在没有获得法律许可的情况下，这个权利不可剥夺。但是基于可能由誓言或批准的原因，被特别描述的场所会被搜查，人员或物品会被逮捕或扣押。"

这个修正案包括下列重要条款，这些条款能够指导执法人员的活动：

- 如果存在合理的理由希望了解个人的隐私，那么调查人员在搜查个人私有物品之前必须取得搜查证。这个要求的例外规定有很多，如个人同意搜查、明确的犯罪证据或威胁生命的紧急情况迫使进行搜查。
- 只能基于可能的动机发放搜查证。必须存在某种罪行已发生的证据，并且当前考虑的搜查会取得与该罪行相关的证据。要求取得搜查证的"可能动机"标准明显弱于要求确定有罪的证据标准，大多数搜查证只基于调查人员的言辞而"发出"。
- 搜查证必须指定搜查范围。搜查证必须包含对搜查和扣押的合法范围的详细说明。

如果调查人员未能遵守这些条款的一丁点儿细节，那么他们就会发现搜查证是无效的，并且搜查结果不被认可。这就引出了另一句人们常提到的话："由于技术上的原因，他逃脱了惩罚。"

2. 实施调查

如果选择不请求执法机构的协助，那么还应当试图遵守合理的调查原则，以确保调查的准确和公平。记住下列几个主要的原则十分重要：

- 永远不要对被破坏的实际系统实施调查。将系统脱机，进行备份，并且使用备份进行事件的调查。
- 永远不要试图“反黑”并对犯罪进行报复。否则，可能会无意中攻击无辜的第三方，并且发现自己会受到计算机犯罪的指控。
- 如果有疑问，那么就请求专家的协助。如果不希望请求执法机构的协助，那么就联系一家在计算机安全调查领域具有特殊经验的私人调查公司。
- 通常，最好使用非正规的口头会谈技术开始调查过程。这些方法被用于收集事实和确定案件的实质。当明确的嫌疑犯被确定时，就应当使用审问技术对他们进行盘问。此外，如果没有具体的法律建议，那么最好不要涉及这个领域。采访通常涉及开放式问题，用于收集信息。审讯通常涉及封闭式提问，考虑到具体的目标，在本质上更具对抗性。同样，这没有具体法律建议，最好保持不变。

19.2　计算机犯罪的主要类别

攻击计算机系统有很多种方式，同时对计算机系统进行攻击的动机也有很多种。信息系统安全从业人员通常会将计算机犯罪分为几类。简单来说，计算机犯罪是与计算机相关的违反法律或法规的犯罪行为。犯罪可能针对计算机，或者计算机可能已经被用在实际的犯罪活动中。每种计算机犯罪类型都代表了攻击的目的及预期结果。

任何违反了一个或多个安全策略的个人都被认为是攻击者。攻击者使用不同的技术达到特殊的目的。了解目标有助于分辨不同攻击类型。需要记住的是，犯罪就是犯罪，计算机犯罪的动机与其他类型的犯罪动机没有任何差别。唯一的不同可能是攻击者进行攻击的方法有所不同。

计算机犯罪通常分为下面几种类型：

- 军事和情报攻击
- 商业攻击
- 财务攻击
- 恐怖攻击
- 恶意攻击
- 兴奋攻击

理解计算机犯罪类型之间的区别，对于更好地理解如何保护系统并在攻击发生时如何响应来说是十分重要的。攻击者留下的证据的类型和数量常常取决于他们的专业程度。在下面的内容中，我们将讨论计算机犯罪的不同类型以及在攻击发生后可能找到的证据的类型。证据可以帮助确定攻击者做了些什么，以及攻击的预计目标是什么。你可能发现自己的系统只是到达真正受害者网络连接链中的一个链接，这使得对攻击者的跟踪变得更难。

19.2.1　军事和情报攻击

军事和情报攻击主要用于从执法机关或军事和技术研究机构获得秘密和受限的信息。这些信息

的暴露可能使研究泄密、中断军事计划甚至威胁国家安全。收集军事信息或其他敏感信息的攻击常常是其他更具破坏性攻击的前兆。

攻击者可能在寻找下列类型的信息：

- 任何类型的军事说明信息，包括部署情报、就绪情报以及战斗计划指令
- 为军事或执法目的收集的秘密信息
- 在犯罪调查过程中获得的证据的说明和存储位置
- 任何可能被用在后续攻击中的秘密信息

由于军事和情报机构收集和使用的信息的敏感特性，因此他们的计算机系统常常成为富有经验的攻击者的目标。为了保护存储此类信息的系统不受更多和更有经验的攻击者的攻击，系统中通常存在更正规的安全策略。正如第 1 章中所述，数据可以根据敏感度进行分类并且被存放在支持所需安全级别的系统中。通常，你会发现强有力的边界安全以及内部控制被用于限制对军方和情报机构的系统中机密文档的访问。

可以确信的是，获取军方或情报信息的危险攻击都是由专业人员进行的。专业的攻击者在掩盖攻击痕迹时常常是非常彻底的。在这样的攻击发生后，通常几乎收集不到证据。如果无人能够感觉到攻击的发生，这种类型的攻击者会取得最成功、最满意的结果。

高级持续性威胁

近年来，被称为高级持续性威胁(Advanced Persistent Threat，APT)的复杂攻击崛起。攻击者拥有资金，并拥有先进的技术技能和资源。他们代表民族国家、犯罪组织、恐怖组织或其他发起人，对非常集中的目标进行有效攻击。

19.2.2 商业攻击

商业攻击专门非法获取公司的机密信息。这种信息可能是对公司经营很关键的信息(如秘方)，或者一旦泄漏便可能损害公司形象的信息(如员工的个人信息)。对竞争者机密信息的收集也称工业间谍活动，这并不是一种新的事物。商业活动使用非法的手段获得竞争信息已经有很多年了。下列两种原因令这种攻击类型很具吸引力：偷取竞争者机密信息的诱惑，精明的攻击者可以轻易破坏一些计算机系统。

商业攻击的目的只是获得机密信息。使用通过攻击收集到的信息通常会比攻击本身更危险。遭受这种攻击的商业系统可能永远都无法恢复。确保包含机密数据的系统安全取决于安全专家所做的工作。此外，必须制定控制这种入侵的策略(有关安全策略的更多信息，读者可以参看第 2 章“个人安全和风险管理概念”)。

19.2.3 财务攻击

财务攻击被用于非法获得钱财和服务。这是人们经常在新闻中听到的计算机犯罪类型。财务攻击的目标可能会是增加银行账户中的存款，或是免费打长途电话。你可能听说过个别人闯入电话公司的计算机，并且设置免费电话。这种类型的财务攻击被称为电话线路盗用。

入店行窃和入室行窃都是财务攻击的例子。总是可以根据破坏造成的经济损失来描述攻击者的技巧。缺乏经验的攻击者会寻找较为简单的目标，尽管破坏通常极小，但是随着时间的推移，破坏

会越来越大。

由经验丰富的攻击者发起的财务攻击可能会导致相当大的破坏。虽然电话线路盗用会使电话公司损失被设定呼叫的收入，但是严重的财务攻击可能会导致数百万美金的损失。正如我们在前面的攻击描述中讲到的，能够检测到攻击并跟踪攻击者的难易在很大程度上依赖于攻击者的技能水平。

19.2.4　恐怖攻击

恐怖攻击实际上存在于我们这个社会的很多领域。对信息系统日益增长的依赖使得信息系统对于恐怖分子越来越具有吸引力。这种攻击有别于军事和情报攻击，恐怖攻击的目标在于中断正常的生活和制造恐怖气氛，而军事和情报攻击被用来获取秘密信息。情报收集一般先于恐怖攻击进行。恰好成为恐怖攻击的受害者系统可能已经在之前的情报收集攻击中被损害。对攻击检测得越认真，对更加严重攻击的防护准备将越好。

计算机恐怖攻击的目的可能是控制电厂、控制电信或造成电力中断。很多这样的控制和管理系统都是计算机化的，并且容易受到恐怖分子的攻击。实际上，同时进行物理的恐怖攻击和计算机化的恐怖攻击的可能性是存在的。对于这样的攻击，如果针对电力和通信的物理攻击与计算机攻击同时发生，那么我们的反应能力将大大下降。

大多数大型电力和通信公司都有专门的安全保卫人员确保系统的安全，但是很多较小的公司具有连接到互联网的系统，它们更容易受到攻击。为了确定攻击，必须认真地监视系统，并且在发现攻击后即刻做出反应。

19.2.5　恶意攻击

恶意攻击可以对组织或个人造成破坏。破坏可能是信息的丢失或信息处理能力的丧失，也可能是组织或个人名誉的损害。恶意攻击的动机通常来自于不满，并且攻击者可能是现在的或以前的员工，也可能是希望组织不能正常运作的人。攻击者对受害者不满，进而以恶意攻击的形式发泄他们的不满。

最近被解雇的员工是可能对组织进行恶意攻击的主要人员。另一种攻击者是被拒绝与其他员工建立个人关系的人。被拒绝的人可能对受害者的系统发起一次攻击，并且破坏受害者系统中的数据。

真实场景

内部人员威胁

安全专家通常更关注来自组织外部的威胁。事实上，许多安全技术都被设计用于阻挡外部的未授权人员。我们往往不太注意防范组织内部的恶意人员，但他们常常对计算资产带来最大的风险。

本书的一位作者最近参与了与某大型知名企业的普通子公司进行的协商讨论。这家公司遭受了严重的安全违规事件，事件造成数千美元被盗以及企业敏感信息被蓄意破坏。组织内部的IT 负责人需要专家与他们一起对该事件进行研究，从而能够找出事件的原因，并且能够防止在未来发生类似的事件。

仅仅通过少量的调查工作，我们很快发现面对的是内部人员攻击。入侵者的动作说明他了解公司的 IT 基础设施，并且掌握对公司持续运营而言最重要的数据类型。

进一步的调查表明罪犯是由于待遇问题离开公司的前员工。他离开公司时心怀不满，并且心怀叵测。遗憾的是，作为曾经的系统管理员，这位员工能够访问公司的许多系统，并且公司的防备措施不够完善，从而在他离开公司时没有删除其所有访问权限。该员工轻易就发现一些自己可用的活动账户，并且使用这些账户通过 VPN 来访问公司的网络。

这个故事对我们有何启示？千万不要低估内部人员威胁。花费一定的时间来评估控制措施，以便缓解恶意的在职员工和离职员工给组织带来的风险。

安全策略应当解决心怀不满的员工可能引发的潜在攻击。例如，员工一旦被解雇，这名员工所有的系统访问都应该被终止。这种操作降低了恶意攻击的可能性，并且删除了当前未使用的访问账户，以免它们会被用在未来的攻击中。

虽然大多数恶意攻击者只是具有有限攻击和破坏能力的人，但是一些人所具有的一些技能会导致巨大的破坏。不高兴的破坏者对于安全专家来说可能是件棘手的事。当一名具有已知的破坏能力的人离开公司时，需要对此高度重视。至少，应当对这个人可能访问的所有系统进行漏洞评估。你可能会惊讶地发现系统中有一个或多个“后门”(有关后门的更多信息，读者可以参看第 21 章)。但是即使缺少后门，一名熟悉组织的技术体系结构的离职员工也仍然可能知道如何利用系统的漏洞。

如果恶意攻击未受到抑制，那么可能会是毁灭性的。认真地对系统漏洞进行监控和评估，是应对大多数恶意攻击的最佳防护措施。

19.2.6 兴奋攻击

兴奋攻击是由具有很少技能的破坏者发起的攻击。缺乏自己设计攻击的能力的攻击者常常会下载某些程序来进行攻击。这些攻击者常常被称作“脚本小子”，因为他们只运行他人的程序或脚本而发起攻击。

这些攻击的动机是闯入系统的极度兴奋。如果是兴奋攻击的受害者，那么所遭受的最常见打击就是服务中断。虽然这种类型的攻击者可能会破坏数据，但是他们的主要动机还是破坏系统，并且可能使用该系统对其他受害者发起拒绝服务攻击。

兴奋攻击的一种常见类型涉及 Web 站点被破坏，此时攻击者会危害 Web 服务器，并且将组织的合法 Web 内容替换为通常炫耀自己技术的其他页面。例如，匿名为 iSKORPiTX 的攻击者在 2006 年造成两万个以上的 Web 站点被破坏，这些站点的合法内容都被替换为包含“Hacked by iSKORPiTX”文本的页面。

最近，我们能够看到“黑客行动主义”的兴起。这些被称为“黑客行动主义者”(黑客和激进分子的结合)的袭击者，常常将政治动机与黑客的快感结合在一起。他们自己组织松散的群体，并将群体命名为同 Anonymous 或 Lolzsec 相似的名字。他们使用 Low Orbit Ion Cannon 这样的小工具，并且还拥有一点点相关知识，制造了大规模的拒绝服务攻击。

19.3　事故处理

在事故发生时，必须根据安全策略中描述的，并且符合当地法律和法规的方法来处理事故。正确处理事故的首要步骤是在事故发生时发现它。必须理解下列两个与事故处理相关的术语：

事件　在特定时间周期内发生的任何事情。

事故　对组织数据的机密性、完整性和可用性具有负面影响的事件。

事故没有被报告的最常见原因是它们从未被发现。每天都可能有很多违反安全策略的事件发生，但是如果没有办法发现它们，那么永远不会知道这些事故的发生。因此，安全策略应当确定并列出所有可能违规的事情和检查它们的方法。根据出现的违规和攻击的新类型对安全策略进行更新，这也是十分重要的。

当发现事故已经发生时该做些什么，这取决于事故的类型和破坏程度。法律规定一些事故必须报告，如那些影响政府或美国联邦利益的计算机(美国联邦利益的计算机是由金融机构和水力、电力系统这样的基础设施系统使用的计算机)或某些金融交易的事故，无论破坏程度如何都需要报告。如今，美国大多数州的法律都要求：如果组织的事故涉及特定的个人标识信息(信用卡号、社会保险号和驾照号)，那么就必须通知相关人员。

除了法律条文之外，许多公司都具有向业务伙伴通知各类不同事故的合约责任。例如，支付卡行业数据安全标准(PCI DSS)要求所有处理信用卡信息的商家向开卡银行和执法部门报告涉及相应信息的事故。

接下来，我们将介绍一些不同类型的事故及典型反应。

19.3.1　常见的事故类型

当针对系统实施的攻击或其他违反安全策略的事情发生时，事故便随之而来。有很多种方法能够区分事故的类型，下面给出了常规的一些类别：

- 扫描
- 泄密
- 恶意代码
- 拒绝服务

这 4 个领域是攻击者影响系统的基本切入点。必须针对每个领域建立有效的监控策略，以便检测系统事故。每个事故领域都具有向安全管理员发送事故发生警报的典型特性。一定要确保理解操作系统环境以及每种事故类型的警告信号。

1. 扫描

扫描攻击通常是先于其他更严重的攻击进行的侦察攻击。这种攻击类似于入室盗窃者先冒充邻居围绕目标进行查看，从而发现未锁的屋门或无人守护的房屋。攻击者在发起定向攻击之前将收集尽可能多的系统信息。寻找任意端口上的不寻常操作或者来自任意单一地址的不寻常操作。例如，端口 22 上的大量 SSH 包可能表明发生了针对网络的系统扫描。

需要记住的是，根据当地法律法规，仅仅扫描系统可能并不违法。扫描可以指出其后的行为是非法的，因此将扫描视为事故，并且收集扫描活动的证据是一个很好的主意。你可能会发现，为了找到随后发生攻击的当事人的责任，在系统被扫描时收集到的内容可能会成为所需的重要证据。

由于扫描是这样一种普遍现象，因此一定要自动收集证据。设置防火墙以记录丢弃的通信数据，并且对这些日志记录文件进行归档。日志记录可能会变得相当大，但是存储设备十分廉价，应当为保留证据付出一定的成本。

2. 泄密

泄密指的是对系统或系统存储的信息进行的未授权访问。泄密可能源自组织的内部或外部。更糟糕的是，泄密可能来自一名合法用户。合法用户 ID 的未授权使用所造成的泄密事故，与有经验的破坏者从外部闯入所造成的损害是相当的。

泄密可能难以检测。通常，数据管理员会注意到数据有些不寻常。这可能会是数据的丢失、更改或移动，可能是时间标记有所不同，还有可能是其他一些内容完全不对。对于系统的正常运作了解得越多，对于检测系统非正常行为的准备工作越充分。

3. 恶意代码

提到恶意代码时，可能会想到病毒和间谍软件。虽然病毒是恶意代码的常见类型，但只是其中一种类型(在第 21 章中，我们讨论恶意代码的不同类型)。这种类型的恶意代码事故的察觉源自由恶意代码引起的终端用户的报告，或者源自自动报告已经发现被扫描的代码包含恶意内容。

保护系统不受恶意代码攻击的最有效方法是使用病毒和间谍软件扫描程序，并且使特征数据库保持最新。另外，安全策略应当解决外部代码的引入问题，要具体到准许终端用户安装的代码。

4. 拒绝服务

最后一种事故类型是拒绝服务(DoS)。通常，这种事故类型最容易检测到。用户或自动化工具能够报告一种或多种服务(或整台机器)是不可用的。尽管拒绝服务很容易被检测，但是避免其发生总比采取措施应对好得多。虽然从理论上讲，动态改变防火墙规则可以拒绝 DoS 网络信息传输，但近几年更加完善和复杂的 DoS 攻击使得它们很难被防范。因为 DoS 攻击的变化太多了，实施这项策略是一项艰巨的任务。

有关 DoS 和 DDoS 攻击的更多信息，可以参看第 21 章。

19.3.2 响应团队

现在许多组织都有负责调查计算机安全事故的专门团队。这些团队通常被称为计算机事故响应团队(CIRT)或计算机安全事故响应团队(CSIRT)。当发生事故时，响应团队具有下列 4 个主要职责：

- 确定事故导致的破坏程度和范围
- 确定事故期间是否有机密信息出现泄密
- 实现任何必要的恢复措施，以便在遭到与事故相关的破坏后还原安全性并进行恢复
- 针对改善安全性和防止相同事故再次出现的其他所有必要的安全措施，进行监督管理工作

真实场景

来自 Gibson 的研究：拒绝服务攻击是出于乐趣还是恶意？

Steve Gibson 在 IT 行业是知名的软件开发商和个人，他的高知名度不仅仅源于与其公司 Gibson 相关的高度受到重视的产品，还有他作为 *Computer World* 杂志的自由和直言专栏的作家身份。近几年，他在计算机安全领域非常活跃，并且他的网站提供免费的针对操作系统漏洞的漏洞扫描服务以及各种补丁程序和修补程序。由他运营的网站 http://grc.com 上有很多文档记录了全面的关于拒绝服务攻击的主题。探讨这种攻击是因为怀有恶意(也就是那些通过闯入明显和估计有很好防范措施的攻击点来提升个人声名的人)还是出于乐趣(也就是那些有很多闲暇时间来寻找向知名对手证明自己能力的人，他们这样做不是为了出名)，这是一件非常有趣的事情。

事实上，Gibson 的网站上有两篇文档记录了全面的拒绝服务攻击的课题，从下列网址可以查到文档的详细信息：

- “分布式反射拒绝服务”：http://www.cs.washington.edu/homes/arvind/cs425/doc/drdos.pdf
- “针对GRC.COM的拒绝服务攻击的奇特故事”：http://www.crime-research.org/library/grcdos.pdf

尽管后来 Gibson 与其中一位参与此次攻击的犯法者进行过匿名讨论，表明某些类型的拒绝服务攻击的动机是出于乐趣而不是商业破坏或恶意行为，但这些报告还是很吸引人的，因为它们为事故处理和报告提供了极好范例。

这些文档中包含了攻击发生前的征兆和发生时间顺序的概要，还有为了阻止攻击再次发生而进行了短期的和长期的修订和变更。文档中还强调了服务提供者之间通信的重要性(在进行通信的过程中，他们的基础设施可能正在遭受攻击)。Gibson 的关于拒绝服务攻击的报告强调，他曾经历过 17 个小时的故障时间，因为他无法与自己的服务提供商的拥有丰富知识的、称职的工程师取得联系，工程师能够帮助确定通信过滤器的正确类型，以便阻止具有典型拒绝服务攻击特点的通信泛洪。

Gibson 的分析还表明，他彻底分析了分布式拒绝服务攻击的源，并对被他称为“在这些攻击发动期间收集的恶意通信的精确概述”进行了文档记录。这些信息可以让他的互联网服务供应商确定一系列过滤器，以便用于进一步阻止通信数据从互联网服务供应商最后的 T1 链接传输至他的服务器。Gibson 的经验证明：识别、分析和特征化攻击对于确定过滤器以及阻止或击败拒绝服务攻击的其他对策来说，绝对是必不可少的。

作为这些责任的一部分，响应团队应当在事故发生一周内对事故进行事后回顾，从而确保事故的关键当事人共享了解的情况并提出最佳的做法，进而为将来的响应工作提供借鉴。

当组建事故响应团队时，一定要保证设计功能交叉的人员组合，以便涵盖管理、技术和受安全事故影响最直接的职能领域。潜在的团队成员包括如下：

- 来自高层管理部门的代表
- 信息安全专业人员
- 法律代表
- 来自公共事务/通信部门的代表
- 来自系统和网络工程领域的代表

19.3.3 事故响应过程

许多组织都采用三步骤的事故响应过程，这个过程由下列三个阶段组成：

(1) 检测和确认

(2) 响应和报告

(3) 恢复和补救

接下来，我们将概述标准的事故响应过程的这三个阶段。

步骤 1：检测和确认

事故确定过程具有两个主要目标：确定事故以及通知适当的人员。为了成功地确定事故，安全团队必须监控发生的所有相关事件，并且在事件达到组织为安全事故定义的阀值时发出通知。确定事故的关键是要确定出所有异常的或可疑的活动，这些活动可能构成事故的证据。虽然根据攻击的典型特征可以检测到攻击，但是有经验的攻击者知道如何“在雷达下飞行(也就是隐藏特征)”。因此，必须清晰地了解系统是如何正常工作的。异常的或可疑的活动指的是在系统中发生的任何不正常的系统活动。

应当通过下列一些工具和技术来监控表明安全事故的事件：

- 入侵检测/防御系统
- 反病毒软件
- 防火墙日志
- 系统日志
- 物理安全系统
- 文件完整性监控软件

在调查事故时，始终要使用多个数据源。对任何不合理的活动都要有所怀疑，确保自己能够阐明系统中任何不正常的活动。如果只是“感觉”不正常，那么这可能成为成功阻止正在发生的事故的唯一线索。

一旦最初的评估员确定事件满足组织的安全事故标准，评估员就必须通知事故响应团队。通知总结了事故的检测阶段、确定阶段、初步响应和报告阶段。

步骤 2：响应和报告

一旦确定事故已经发生，下一步就是选择执行恰当的行动。安全策略应当指定针对各类事故应采用的步骤。始终都要认定事故最终会诉诸法律。收集证据时，要保证证据能够达到出庭标准。如果证据受损，那么就无法追回。因此，必须确保证据链得到维护。

隔离与抑制 采取的第一个行动应当致力于限制组织泄密和阻止进一步破坏。在系统可能泄密的情况中，应当断开其与网络的连接，这样不仅可以阻止入侵者访问受到危害的系统，而且也可以防止受害的系统影响网络中的其他资源。

警告：

使受害系统保持运行状态至关重要。切记：不要关闭受害系统！关闭计算机会毁坏易失性存储设备中的内容，从而可能破坏证据。

收集证据 为了执行适当的调查，没收设备、软件或数据是常见的事情。没收证据的行为十分

重要，一定要以恰当的方式来进行。目前有下面三种基本的选择方案。

首先，拥有证据的人可能自愿交出证据。这种方法通常适用于当攻击者不是所有者时。但是；有罪的人很少会自愿交出控告他们犯法的证据。经验较少的攻击者可能认为，他们已经成功地掩盖了自己的痕迹并自动交出重要的证据。一名优秀的法庭调查员能够从计算机上提取“被隐藏”的信息。在大多数情况下，从可疑的攻击者那里寻找证据，就是为了警告嫌疑犯正在进一步采取法律行动。

提示：

就内部调查而言，你会通过自愿交出方式收集到的绝大多数证据。通常情况下，你在某位高级管理人员的支持下进行调查，这位高管会授权你访问完成调查所需的组织内的任何资源。

其次，可以让法院发出一张传票或法令，强迫个人或组织交出证据，并由执法部门强制执行传唤。同样，这种做法也会引起某些人的充分注意，并且导致更改证据使之在法庭上无效。

最后，可以选择申请搜查证。这种选择只有必须在不惊扰证据的所有者或其他当事人的情况下获取证据时使用。必须通过合理可信的强烈怀疑使法官同意采取这样的行动。

这三种选择方案适用于没收组织内部和外部的设备，但是我们还可以采取另一个步骤，以便确保恰当实施没收属于组织的设备的行为。让所有新员工签署协议，使其同意在调查期间可搜寻和没收任何必要的证据，这已经变得越来越常见。通过这种方式，同意条款被作为雇用协议中的一个条件，这使得没收措施更容易执行，并减少了等待法律许可获取证据而导致证据丢失的可能性。确保安全策略涉及这个重要的主题。

当决定收集何种证据时，应该考虑下列数据源：

- 涉及事故的计算机系统(服务器和工作站)
- 来自安全系统(例如入侵检测、文件完整性监控和防火墙)的日志
- 来自网络设备的日志
- 物理访问日志
- 与被调查事故相关联的其他数据源

分析与报告　一旦完成证据收集工作，就应当分析证据以便确定导致事故的一系列事件。在提交给管理部门的书面报告中概述这些发现。在报告中，应当慎重地描述事实并给出意见。对可能的原因进行推断是可接受的，但是应该确信结论陈述完全依赖于事实，并且需要一定程度的估计判断。

步骤 3：恢复与补救

在完成调查之后，还要执行两个任务：将工作环境还原至正常的运营状态，以及完成“总结经验教训”过程，从而提高应对未来事故的能力。

恢复　恢复过程的目标是修正针对组织的所有已发生破坏，并且限制将来由于类似事故导致的破坏。这个过程应当采取下列一些关键行动：

- 重构受到危害的系统，注意纠正可能导致事故的任何安全漏洞。
- 在必要时还原备份数据，以替代完整性出现问题的数据。
- 在必要时增补现有的安全控制，以弥补事故分析期间确定的缺陷。

一旦完成恢复过程，业务就应当回到事故前的状态并重新运营(不过采用了更安全的方式)。

总结经验教训　事故响应过程的最后一个阶段是召开“总结经验教训”会议。在这个重要的过

程中，事故响应团队的成员会回顾他们在事故期间的活动，并且寻找行动中和事故响应过程中是否还有改进之处。通过分析现实事故期间的效力，这种事后反思的行为能够为今后成功的事故响应提供重要参考。

19.3.4 约谈个人

事故调查期间，你会发现有必要与可能掌握相关信息的人员进行谈话。如果只是为了获取有助于调查的信息，那么这种谈话被称为约谈。如果怀疑某人涉嫌犯罪并希望收集在法庭上可用的证据，那么这种谈话被称为审问。

约谈和审问是一种专门的技巧，并且应当只由训练有素的调查人员进行。不恰当的方法可能会损害执法部门成功起诉嫌疑人的能力。此外，许多法律都涉及对人员的限制或拘留。如果打算进行私下审问，那么就必须严格地遵守这些法律。在进行任何约谈之前，始终要与律师商讨相应的对策。

19.3.5 事故数据的完整性和保存

无论证据的说服力如何，如果在证据收集的过程中发生变更，那么就会被法院拒绝受理。一定要确保能够维护所有证据的完整性，但在进行数据收集之前要了解什么是数据的完整性。

我们不可能检测到所有正在发生的事故。有时，调查结果会揭示出以前存在未被发现的事故。如果在跟踪证据时，发现包含攻击者相关信息的重要日志文件已经被清除，将令人沮丧。一定要认真地考虑日志文件的作用或其他可能存在证据的地方。简单的归档策略有助于确保能够在需要时获得证据，无论事故已经发生了多长时间。

因为许多日志文件中都包含了有价值的证据，攻击者时常在攻击成功之后试图清除这些证据。要采取措施保护日志文件的完整性并防止被修改。有一种技术被用于实现远程日志记录，采用这种技术时，网络中所有的系统将日志记录发送到一台中央日志服务器，这台中央日志服务器被锁定，以免受到攻击，从而使数据免于修改；这起到了保护日志文件在事故发生之后不被清除的作用。此外，系统管理员经常使用数字签名来证明日志文件在最初获取之后未被篡改。要了解更多的相关信息，读者可以参看第 7 章“PKI 和密码学应用”。

由于涉及安全计划的各个方面，因此无法实现统一的解决方案。一定要熟悉系统并采取措施，使组织采用最合理方式对其进行保护。

19.3.6 事故报告

应该何时报告事故？应该向谁报告？通常这些问题很难回答。安全策略中应当包含回答这两个问题的指导方针。在报告事故时有一条基本原则。如果每个事故都进行报告，那么就会承担被认为是麻烦制造者的风险。当发生严重事故时，报告就会被人忽略。同样，报告不重要的事故会给人这样的印象：组织非常容易受到攻击。这会对实施严格安全措施的组织产生不利影响。例如，在每天都听说银行发生事故之后，公众对银行的安全实践措施就无法保持信心。

另一方面，如果在发现事故之后不及时报告，那么自动调整和法律制裁就变得更加困难。如果延迟向管理机构通知发生的严重事故，那么很可能就要回答有关延迟通知动机的质疑，甚至无辜的人可能看起来像是通过不及时报告发生的事故来试图隐瞒某些情况。

与大多数安全主题一样，回答这个问题并不容易。事实上，对某些事故的报告要被迫受到法律或法规的限制。必须确信自己了解所要上报的事故。例如，存储信用卡信息的组织必须对发生信息泄露的事故予以上报。

在事故发生之前，与公司的法律人员和适当的执法代理机构建立良好的关系是非常明智的。找到适合组织的执法联络人并同他们商讨。在应该报告事故时，提前努力建立关系的工作将会见到成效。如果已经了解了正在与你谈话的人，那么会减少用于介绍和解释的时间。预先确定一名联系人作为组织与执法部门的联络人员是一个不错的主意。这种做法有下列两点好处：首先，能够确保执法部门从固定的联络人那里了解组织的想法并知道通过何人进行调查；其次，允许预先指示联络人与执法人员建立良好的工作关系。

注意：

与执法部门建立技术联系的一个好方法是参与 FBI 的 InfraGard 计划。InfraGard 覆盖了美国绝大部分大城市区域，并且为执法人员和业务安全人员提供了一个在封闭环境中共享信息的论坛。要了解更多的信息，访问 www.infragard.org 站点。

一旦决定报告事故，就要保证报告尽可能多地包含下列信息：

- 事故的性质是什么？如何开始和由谁开始？
- 事故何时发生(日期和时间要尽可能精确)？
- 事故是在哪里发生的？
- 如果知道，那么攻击者使用的是什么工具？
- 这个事故会造成什么损害？

你可能还会被要求提供更多的信息。准备尽可能及时地提供这些信息。此外，你还可能被要求对系统进行隔离。

与采取的任何安全措施一样，对所有的通信过程进行日志记录，并对作为事故报告提供的任何文档进行复制备份。

提示：

关于事件处理的更多信息，请阅读NIST SP 800-61计算机安全事件处理指南，网址为 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf，*也可阅读计算机安全事件响应小组手册(CSIRTs)，网址为*http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=6305。

19.4　道德规范

因为安全专家处理敏感信息，需要赢得信任，所以安全专家自身及相互之间负有高标准的行为职责。管理个人行为的规则被统称为道德规范。一些组织已经认识到需要标准的道德规范或准则，并且为道德行为设计了指导原则。

本节将讨论两种道德规范。这些规范不是法律。它们是对专业人士行为的最低标准。它们为你提供了合理的道德判断标准。无论其专业领域是什么，受雇于何人，我们期望所有的安全专家都应该遵守这些指导原则。你一定要理解并遵守本节列出的道德规范。除了这些代码，所有信息安全专业人士也应该支持他们组织的道德准则。

19.4.1 (ISC)^2 的道德规范

管理 CISSP 认证考试的机构是国际信息系统安全认证协会，也就是(ISC)^2。(ISC)^2 的道德规范被用于提供 CISSP 行为的基准，是包含一个序言和 4 条标准的简单准则。接下来我们将简要概述(ISC)^2 的道德规范的主要概念。

提示：

所有 CISSP 应试者都应当熟悉(ISC)^2 的整个道德规范，这是因为他们必须签字同意遵守这个规范。本书不会深入介绍这个规范，不过可以在 www.isc2.org/ethics 站点上查看(ISC)^2 的道德规范的详细信息。必须访问这个站点并阅读规范全文。

道德规范的序言

道德规范的序言如下：

- 社会安全和福利、公益、对委托人的责任，以及要遵守的其他要求，还有需要去遵守的要求，这些是要遵守的行为的最高道德标准。
- 因此，严格遵守这些标准是认证考试的要求。

道德规范的标准

道德规范包括如下准则:

保护社会、公益、必需的公信与自信，以及基础设施 安全专业人员具有很大的社会责任。我们担负着确保自己的行为使公众受益的使命。

行为得体、诚实、公正、负责和遵守法律 对于履行我们的责任来说，诚实正直是必不可少的。如果组织、安全团体内部的其他人或一般公众怀疑我们提供的指导不准确，或者质疑我们的动机，那么我们就无法履行自己的职责。

为委托人提供尽职的、胜任的服务工作 尽管要对整个社会负责，但是也会专门对雇用我们来保护其基础设施的人负责。我们必须确保为组织提供无偏见的、完全胜任的服务。

发展和保护职业 我们选择的这个职业也在不断变化。作为安全专业人员，我们必须确保掌握最新的知识并且应用到社会的公共知识体系中。

19.4.2 道德规范和互联网

在 1989 年 1 月，互联网顾问委员会(IAB)认识到快速扩张的互联网范围超出了当初创建网络的可信团体。考虑到互联网发展中出现的滥用情况，IAB 发布了一份有关正确使用互联网的政策声明。这份声明的内容直到今天仍然有效。了解这个名为“道德规范和互联网(RFC 1087)”的文档的基本内容是十分重要的，这是因为大多数的道德规范都能在这个文档中追根溯源。

这份声明被认为是不道德行为的概括列表。道德规范告诉人们应该怎样做，而此列表概括了不应该做什么。RFC 1087 说明了怀有下列目的的任何行为都是不可接受和不道德的：

- 试图获得未经授权访问 Internet 资源的权利
- 破坏 Internet 的正常使用
- 通过这些行为耗费资源(人、容量、计算机)

- 破坏以计算机为基础的信息的完整性
- 危害用户的隐私权

计算机道德规范的 10 条戒律

计算机道德规范(Computer Ethics)协会制定了自己的道德规范。下面列出了计算机道德规范的 10 条戒律:

1) 不准使用计算机危害他人。
2) 不准妨碍他人的计算机工作。
3) 不准窥探他人的计算机文件。
4) 不准使用计算机进行偷盗。
5) 不准使用计算机作伪证。
6) 不准私自复制未付费的专用软件。
7) 不准在未被授权或未适当补偿的情况下使用他人的计算机资源。
8) 不准盗用他人的知识产品。
9) 必须考虑所编写程序或所设计系统的社会后果。
10) 必须总是以确保关心和尊重同事的方式使用计算机。

IT 行为可选择的道德规范有很多种。普遍接受的系统安全准则(GASSP)是可以考虑选择的一个系统。可以在 www.infosectoday.com/Articles/gassp.pdf 网页中找到 GASSP 系统的完整文本。

19.5　本章小结

信息安全专业人员必须熟悉事件响应过程。这涉及收集和分析所需的证据，以便进行调查。安全专业人员应该熟悉证据的主要类别，包括实物证据、书面证据、言辞证据。电子证据往往通过对硬件、软件、存储介质和网络的分析，进行收集。使用适当的程序收集证据很必要，不能改变原始证据，并应对证据链进行保护。

计算机犯罪被归结为几种主要的类别，每个类别中的犯罪行为有共同的动机和期望的结果。理解攻击者所寻找的内容，对于恰当地保护系统是很有帮助的。

例如，军事和情报攻击被用于获得秘密信息，这些信息通过合法的方式是无法获得的。除了目标为民用系统以外，商业攻击几乎与军事和情报攻击是相同的。其他类型的攻击包括财务攻击(电话线路盗用是财务攻击的一个例子)和恐怖攻击(在计算机犯罪中，这是一种用来中断正常生活的攻击)。最后是恶意攻击和兴奋攻击。恶意攻击的目的是通过销毁数据或运用使组织或个人感到困窘的信息进行破坏。兴奋攻击由缺乏经验的攻击者发起，进而使系统受到损害或被禁用。尽管通常缺乏经验，但是兴奋攻击可能会令你非常烦恼，并且付出高昂的代价

事故是违反安全策略的行为或对安全策略的威胁。当事故被怀疑时，应当立即开始调查，并收集尽可能多的证据。这是因为，如果决定报告这个事故，那么就必须具备足够多的、可接受的证据来支持你的观点。

道德规范是管理个人行为的一组规则。实际上，从一般到特殊存在几种道德规范，安全专家可以将它们用作指导准则，$(ISC)^2$ 将道德规范作为认证要求。

19.6 考试要点

了解计算机犯罪的定义。计算机犯罪是指违反法律或法规的任何行为，直接针对或直接涉及使用计算机。

能够列出并解释计算机犯罪的 6 个类别。计算机犯罪被分为 6 个类别：军事和情报攻击、商业攻击、财务攻击、恐怖攻击、恶意攻击和兴奋攻击。能够解释每种攻击的动机。

了解证据收集的重要性。只要发现事故，就必须开始收集证据并尽可能多地收集事故的相关信息。证据可以在后来的法律活动中使用，或者被用于确定攻击者的身份。证据还可以帮助确定损失的范围和程度。

理解事故是任何违反安全策略的行为或对安全策略的威胁。事故应该在安全策略中加以定义。即使特殊的事故没有被概括出来，策略的存在也仍然为系统的使用设立了标准。有任何负面影响的事件(影响到组织的数据的机密性、完整性或可用性)都是事故。

能够列出 4 种常见的事故类型并了解每种事故的征兆。当针对系统的攻击或其他违反安全策略的行为出现时，就会发生事故。事故可以被分为下列 4 种类型：扫描、泄密、恶意代码和拒绝服务。一定要能够解释每种事故所涉及的内容和出现的征兆。

了解识别异常和可疑活动的重要性。攻击总会产生一些不正常的活动。识别出异常和可疑的活动是检测出事故的第一步。

知道如何调查入侵事件以及如何从设备、软件和数据中收集充分的信息。必须拥有设备、软件或数据的所有权，以便进行分析并使用它们作为证据。必须获得没有被修改的证据，或者不允许其他任何人修改证据。

了解三种基本的没收证据的选择方案，并知道每种方案适用的情况。第一种，拥有证据的人可能会自愿提交证据。第二种，使用法院传票强迫嫌疑人交出证据。第三种，如果需要没收证据，但不给嫌疑人修改证据的机会，搜查证是最有用的。

了解保存事故数据的重要性。因为在事故发生之后，总会发现某些事故迹象，所以除非保证关键的日志文件被保存一段合理的时间，否则将会失去有价值的证据。可以在适当的地方或档案文件中保留日志文件和系统状态信息。

熟悉如何报告事故。第一步是要与公司和法律从业人员建立工作关系，与他们一起处理发生的事故。当确实需要报告事故时，应当尽可能多地收集描述性信息并及时上交报告。

理解法庭可接纳证据的基本要求。能够被接纳的证据必须与案件事实相关，事实必须以材料形式呈现，证据的收集方式应在能力范围内，且符合法律规定。

解释各种可能在刑事或民事审判中使用的证据。实物证据由可以被带进法庭的事实物件组成。书面证据由能够说明事实的书面文件组成。言辞证据包括证人陈述的口头证据或书写的言论证据。

理解安全人员职业道德的重要性 安全从业者被赋予非常高的权利和责任，以执行其工作职能。这便会存在权利滥用的情形。没有严格的准则对个人行为进行限制，我们可以认为安全从业人员具有不受限制的权利。遵守道德规范有助于确保这种权利不被滥用。

了解(ISC)^2 的道德规范和 RFC 1087“道德规范和互联网”。所有参加 CISSP 考试的人都应该熟悉(ISC)^2 的道德规范，这是因为他们必须签署遵守这一准则的协议。除此之外，他们还应当熟悉 RFC 1087 的基本要求。

19.7　书面实验室

1. 计算机犯罪的主要类别是什么？
2. 兴奋攻击背后的主要动机是什么？
3. 约谈和审问之间的差异是什么？
4. 事件与事故之间的差异是什么？
5. 事故响应团队的一般成员有哪些？
6. 事故响应过程的三个阶段是什么？
7. 证据能够被法庭采纳的三个基本要求是什么？

19.8　复习题

1. 什么是计算机犯罪？
   A. 在安全策略中具体列出任何攻击
   B. 任何损害受保护计算机的非法攻击
   C. 任何涉及计算机的法律或法规违反行为
   D. 未能实行计算机的安全尽职调查
2. 军事和情报攻击的主要目的是什么？
   A. 为了攻击军事系统的可用性
   B. 为了获得军事或执法来源的秘密和限制信息
   C. 为了利用军事或情报机构系统来攻击其他非军事网站
   D. 为了破坏用于攻击其他系统的军事系统
3. 什么类型的攻击目标是存储在民用组织系统中的专有信息？
   A. 业务攻击
   B. 拒绝服务攻击
   C. 财务攻击
   D. 军事和情报攻击
4. 什么目标不是金融攻击的目的？
   A. 还没有购买的接入服务
   B. 透露机密的个人员工信息
   C. 从不法来源转移资金到你的账户
   D. 从其他组织窃取金钱
5. 以下哪些攻击是最明显的恐怖袭击？
   A. 涂改敏感的贸易秘密文件
   B. 破坏通信能力和物理攻击应对能力
   C. 窃取机密信息
   D. 转移资金到其他国家
6. 下列哪一项不是怨恨攻击的主要目的？
   A. 披露令人尴尬的个人信息

B. 启动组织系统中的病毒
C. 用受害组织的虚假地址发送不恰当电子邮件
D. 使用自动化工具扫描组织系统以找出易受攻击的端口

7. 什么是攻击者进行兴奋攻击的主要原因？(选择所有适用选项)
A. 耀武扬威
B. 出售被盗的文档
C. 以征服安全系统为荣
D. 对个人或组织报复

8. 收集证据时要遵循的最重要的规则是什么？
A. 直到拍摄了画面才关闭计算机
B. 列出目前同时收集证据的所有人
C. 在收集过程中从来不修改证据
D. 将所有设备转移到一个安全的存储位置

9. 当事故被发现时不能立即关闭设备电源，什么是正确的观点？
A. 所有的损害已经完成。关闭设备不会停止额外的伤害
B. 如果被关闭，没有其他的系统可以代替
C. 太多的用户登录并使用系统
D. 在内存中有价值的证据都将丢失

10. 黑客行动主义者由以下哪些因素驱使？(选择所有适用选项)
A. 财务收益
B. 快感
C. 技能
D. 政治信仰

11. 什么是事故？
A. 任何导致系统损坏的主动攻击
B. 对任何道德规范的违反
C. 涉及计算机的任何罪行(对法律或法规的违反)
D. 任何对数据的机密性、完整性和可用性产生不利影响的事件

12. 如果端口扫描不会对系统造成损害，为什么通常还被认为是事故？
A. 所有端口扫描表明敌对行为
B. 端口扫描是造成损害的预先攻击，是未来进一步攻击前奏
C. 扫描端口会损坏端口
D. 端口扫描使用了能更好服务于用户的系统资源

13. 什么类型的事故的特点是获得更多的特权级别？
A. 危及
B. 拒绝服务
C. 恶意代码
D. 扫描

14. 什么是识别系统中异常和可疑行为的最好方法？
A. 要注意最新攻击

B. 配置 IDS 检测并报告所有的异常流量
C. 知道正常系统活动的样子
D. 研究主要攻击活动类型的特征

15. 如果需要没收一台疑似不为组织工作的攻击者计算机，什么法律渠道最合适？
A. 员工签订同意协议
B. 搜查令
C. 没有合法渠道是必要的
D. 自愿同意

16. 为什么要避免删除每天的日志文件？
A. 事故可能好几天不会被发现，有价值的证据可能会丢失
B. 磁盘空间便宜，日志文件被频繁使用
C. 日志文件被保护，不能被改变
D. 日志文件中的任何信息是无用的，几个小时后就旧了

17. 以下哪些情况可能需要报告事故？(选择所有适用选项)
A. 政府法规保护的机密信息可能被披露
B. 赔偿超过$1500
C. 事故发生之前
D. 事故导致违反法律的行为发生

18. 什么是道德？
A. 强制要求履行的工作要求行动
B. 专业操守的法律
C. 由专业机构规定的条例
D. 个人行为的准则

19. 根据$(ISC)^2$的道德规范，CISSP 考试人员应该如何行动？
A. 诚实、勤奋、负责和守法
B. 值得尊敬、诚实、公正、负责和守法
C. 支撑安全策略和保护组织
D. 守信、忠诚、友善、礼貌

20. 下列哪个操作被认为是不可接受的，并根据 RFC 1087“道德规范与互联网”是不道德的？
A. 行动危及机密信息的保密性
B. 行动损害了用户隐私
C. 扰乱组织活动的行为
D. 一台被用于执行违反规定的安全策略操作的计算机

第 20 章

软件开发安全

本章中覆盖的 CISSP 考试大纲包含：

- A. 在软件开发生命周期中理解应用安全
  - A.1 开发方法论(例如，敏捷开发、瀑布模型)
  - A.2 成熟度模型
  - A.3 运行和维护
  - A.4 变更管理
  - A.5 集成产品开发团队(如 DevOps)
- B. 在开发环境中执行安全控制
  - B.1 软件环境安全
  - B.3 安全编码中的配置管理
  - B.4 代码仓库的安全说明
  - B.5 API 安全
- C. 评估软件安全的有效性
  - C.1 审计和记录变更
  - C.2 风险分析和缓解
  - C.3 验收测试
- D. 评估软件获取的安全性影响

软件开发是由许多拥有不同技能和不同安全意识的开发者实施的一项复杂和具有挑战性的任务。这些开发人员创建和修改的应用程序通常会使用敏感数据，还会和公众交互。这给企业安全带来了巨大的风险，并且信息安全专家必须理解这些风险，对风险和业务需求做出平衡，并且实施适当的风险缓解机制。

20.1 系统开发控制概述

为了实现灵活的操作目标，很多公司都使用定制开发的硬件和软件系统。由于恶意的和/或粗心

的开发人员创建后门、缓冲区溢出漏洞或其他导致系统被恶意人员利用的弱点，因此这些定制解决方案可能存在巨大的安全漏洞。

为了防范这些漏洞，在整个系统开发的生命周期内引入安全性是至关重要的。有组织、有条理的过程可以帮助确保解决方案满足功能需求以及安全性指导原则。安全性关注应当是从事解决方案开发的信息安全专家的重点考虑事项，接下来将针对这些关注内容对一系列系统开发行为进行讨论。

20.1.1 软件开发

在系统开发的每个阶段都应当考虑安全性，这些阶段包括整个软件开发过程。开发人员应该力求在他们开发的所有应用程序中构建安全性，并且为关键的应用程序和拥有敏感信息的应用程序提供更高的安全级别。因为在软件开发项目的初期，给系统构建安全性比在现有系统中添加安全性容易得多，所以在初期就考虑安全性是极为重要的。

1. 编程语言

你可能已经知道，软件开发人员需要使用编程语言来开发软件代码。你可能不知道同一个系统能够同时使用好几种编程语言。本章简要介绍不同类型的编程语言以及每种编程语言的安全影响。

计算机能够理解二进制代码。计算机语言中只有 1 和 0，而二进制代码正是这样的语言。计算机接受的指令由一长串二进制数字组成，这些二进制数字使用的语言被称为机器语言。每个 CPU 芯片集都具有自己的机器语言，事实上，如果不借助专门的软件，那么人们连最简单的机器语言代码都无法理解。汇编语言是一种使用记忆符号来表示 CPU 基本指令的语言，但是仍然要求人们了解硬件专用的、相对模糊的汇编语言。此外，汇编语言还要求进行大量乏味的编程工作，将两个数字相加这样的简单任务就需要 5 行或 6 行汇编代码才能完成。

编程人员当然不希望使用机器语言或汇编语言来编写代码，他们更喜欢使用高级编程语言，例如 C++、Ruby、Java 和 Visual Basic。这些语言允许编程人员以更接近人际交流的方式编写代码，从而缩短了编写应用程序的时间，可能减少项目所需的编程人员数量，并且还允许不同操作系统和硬件平台之间的某些可移植性。一旦编程人员准备执行设计的应用程序，那么他们就有两种可用的选项：编译型和解释型。

某些语言(例如，C、Java 和 FORTRAN)是编译型语言。使用编译语言时，编程人员可以使用被称为编译器的工具将高级语言转换为在特定操作系统中使用的可执行文件。可执行文件随后被分发给终端用户，终端用户会在认为合适时使用这些文件。一般而言，在可执行文件中不可能查看或更改软件指令。

其他语言(例如，JavaScript 和 VBScript)是解释型语言。使用这些语言时，编程人员会分发源代码，源代码中包含以高级语言编写的指令。终端用户随后在系统中使用解释器来执行这些源代码。此时，用户能够查看编程人员编写的原始指令。

每种方式都具有各自的安全性优点和缺点。编译代码通常不易被第三方操纵。然而，因为终端用户无法查看原始指令，所以恶意的(或不熟练的)编程人员也更容易在编译代码中嵌入后门和其他安全缺陷并逃避检测。不过，编程人员不易在解释型代码中插入恶意代码，原因在于终端用户可以查看代码和检查代码的准确性。另一方面，接触软件的任何人都能够更改编程人员的原始指令，并且可能在解释型软件中嵌入恶意代码。你将在第 21 章“恶意代码与应用攻击”中的“应用攻击”一节中学到攻击者常常如何利用漏洞来破坏软件。

编程语言的发展

在 CISSP 考试中，还应当熟悉编程语言的发展，各代编程语言的定义如下：

- 第 1 代语言(1GL)包括所有机器语言。
- 第 2 代语言(2GL)包括所有汇编语言。
- 第 3 代语言(3GL)包括所有编译语言。
- 第 4 代语言(4GL)试图接近于自然语言，包括数据库使用的 SQL。
- 第 5 代语言(5GL)允许编程人员创建使用可视接口的代码。

2. 面向对象编程

许多现代编程语言(例如，C++、Java 和.NET 语言)都支持面向对象编程(OOP)的概念。较早的编程风格(例如，函数式编程)关注程序流本身，并且试图将希望的行为设计为一系列步骤。面向对象编程关注交互所涉及的对象。可以将这些对象视为被请求执行特定操作或显示特定行为的一组对象。对象一起工作，从而提供系统的功能或能力。OOP 可能更为可靠，并且能够减少程序变化错误的传播。作为一种编程方法，OOP 更适合建模或模拟现实生活。例如，某个银行业务程序可能具有三个对象类，这三个对象类分别对应于账户、账户所有人和员工。在系统中添加一个新账户时，就会创建适当对象的一个新实例或副本，这个实例或副本包含新账户的详细信息。

在 OOP 模型中，每个对象都有对应其特定操作的方法。例如，账户对象可以有方法去增加资金、扣除资金、关闭账户和转移所有权。

对象也可以是其他对象的子类，并且继承父类的方法。例如，账户对象可能有相关特定账户类型的子类，比如储蓄、检查、抵押和汽车贷款。子类可以使用父类的所有方法，并且有额外的特定类方法。比如，检查对象可能有一个方法名叫 write_check()，而其他子类则没有。

从安全的角度来看，面向对象编程提供了一个抽象的黑盒方法。用户需要知道对象的接口细节(通常关于每个对象方法的输入、输出和动作)，但不一定需要知道对象内部如何有效地使用它们来工作。为了提供面向对象系统要求的特性，对象会被封装(独立的)，以及它们只能通过特定消息被访问(换句话说就是输入)。对象也可以表现出替换的属性，允许不同对象提供兼容操作来彼此替换。下面是一些可能会在工作中遇到的常见的面向对象编程术语：

消息　消息是对象的通信或输入。

方法　方法是定义对象执行响应消息操作的内部代码。

行为　由对象呈现的结果或输出是一种行为。行为是通过方法处理消息的结果。

类　定义对象行为的一组对象的公共方法的集合就是类。

实例　对象是包含对象方法的类的实例或例子。

继承　某个类(父类或超类)的方法被另一个子类继承时就会出现继承性。

委托　委托是某个对象将请求转发给另一个对象或委托对象。如果某个对象没有处理特定消息的方法，那么就需要委托。

多态性　多态性是对象的特性，当外部条件变化时允许以不同的行为响应相同的消息或方法。

内聚　内聚描述相同类中方法目的之间关系的强度。

耦合　耦合是对象之间的交互级别。低耦合意味着较少的交互。因为对象更为独立，所以低耦合提供了更优的软件设计。低耦合更易于检测故障和更新。内聚程度较低的对象需要大量来自其他对象的帮助才能完成任务，并且具有高耦合的特点。

3. 保证

为了确保在新应用程序中构建的安全控制机制能够在系统的整个生命周期内正确地实现安全策略，管理员会使用保证过程。保证过程只是据此在系统生命周期内构建信任的正规过程。可信计算机系统评估标准(TCSEC)橘皮书将这个过程称为生命周期保证。

4. 避免和缓解系统故障

无论开发团队多么高级，系统在某些时候都可能出现故障。实施软件和硬件控制时，应该为这种故障类型做好准备，从而确保系统做出适当的响应。我们可以通过许多方法来避免故障，包括使用极限检查和创建故障防护或应急开放过程。下面将详细讨论这些方法。

输入验证 当用户与软件交互时，他们通常以输入的形式向应用程序提供信息。这里可能包括程序后续要用到的值的类型。开发者经常希望这些值在一定的参数范围内。例如，如果程序员要用户输入月份，程序可能希望看到 1~12 之间的某个整数值。如果用户输入的值在该范围之外，写得差的程序最好的情况是崩溃，最糟糕的情况是允许用户对底层操作系统进行控制。

输入验证核实用户提供的值是否匹配程序员的期望，之后才允许进一步的处理。例如，输入验证会检查月份值是否是 1~12 之间的一个整数。如果值在这个范围之外，程序将不会作为日期处理这个数字，而是会通知用户希望输入的值。这种类型的输入验证，通过代码检测确保数字落在一个可接受的范围，被称为限制检测。

输入验证也可以检测不寻常的字符，如文本字段中的引号，这可能是攻击的象征。在某种情况下，输入验证程序可以改变收入，移除风险特征序列，以及用安全的值来替换。这个过程被称为换码输入。

输入验证应该经常存在于事务处理的服务器端。任何发送给用户浏览器的代码容易受到用户的操作，因此这些代码很容易被绕开。

提示：

在大多数组织内，安全专家具有系统管理背景，但是并不具备软件开发的专业经验。如果没有此类经验，那么一定不能放弃学习，并且要教育组织的开发人员，使他们了解安全编码的重要性。

故障防护和应急开放 即使编程人员、产品设计人员和项目管理人员以最佳的状态全身心投入工作，被开发的应用程序也仍然会遭遇不可预测的或无法完全理解的情况和环境。其中，某些状况会导致出现故障。因为故障是不可预测的，所以编程人员应当在代码中设计如何响应和处理故障的常规方法。

当应对系统故障做计划时有两个基本选择：

- 故障防护状态将系统置入高级别安全性(甚至可能完全禁用)，直至管理员能够诊断问题并将系统还原至正常操作状态。
- 应急开放状态允许用户绕开失败的安全控制，此时用户获得的特权过高。

在大多数环境中，因为能够防止对信息和资源的未授权访问，所以故障防护是恰当的故障状态。

软件应当恢复故障防护状况，这意味着只关闭应用程序或停止整个主机系统的操作。Windows 操作系统中出现的蓝屏死机(BSOD)就是这种故障响应方式的一个示例，不过它实际上被称为 STOP 错误。尽管操作系统努力防止 STOP 错误，但是在出现不安全的和非法的活动时仍然会发生 STOP 错误。不安全的和非法的活动可能包括：应用程序直接访问硬件，企图绕开安全控制检查，或者一

个进程擅自使用其他进程的内存空间。一旦出现非法操作，系统环境就不再可信。因此，此时 OS 不会继续支持不可靠和不安全的操作环境，而是启动作为安全防护响应的 STOP 错误。

一旦出现安全防护操作，编程人员就应当考虑接下来发生的活动。此时，可能的选项是：停留在安全防护状态，或者自动重启系统。前一个选项要求管理员人工重启系统并监督这个过程，通过使用启动密码就可以实施这个动作。后一个选项并不要求人工干预，系统能够自己还原至正常运作状态，但仍存在自身特有的问题。例如，必须约束系统重启至非特权状态。换句话说，系统的重启应当不执行自动的登录操作，而是提示用户提供授权的访问凭证。

警告：

在有限的一些环境中，实现应急开放的故障状态可能更为合适。这种方式有时适用于多层安全系统中较低层的组件。应急开放系统的使用应当极为谨慎。部署使用这种故障模式的系统之前，必须明确验证用于该模式的业务要求。如果验证通过，那么在系统故障时需要确保能够采用其他适当的控制来保护组织的资源。希望所有安全控制都利用应急开放方式的情况是极为罕见的。

即使正确设计了安全性并将之嵌入软件，但是为了支持更简单的安装，所设计的安全性往往会被禁用。因此，IT 管理员负责打开和配置与特定环境需求匹配的安全性是非常普遍的。如图 20.1 所示，维护安全性常常需要权衡用户友好性与功能性。此外，如果添加或增加安全性，那么也会增加成本、增加行政管理开销和降低生产率/吞吐量。

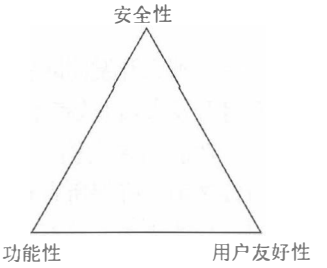


图 20.1　安全性、用户友好性和功能性之间的关系

20.1.2　系统开发生命周期

如果在系统或应用程序的整个生命周期内都进行计划和管理，那么安全性是最有效的。管理员利用项目管理使项目的开发遵循目标，并且逐步实现整个产品的目的。通常，项目管理使用生命周期模型进行组织，以便指导开发过程。使用正规化的生命周期模型有助于确保良好的编程实践以及在产品开发的每个阶段都嵌入安全性。

所有系统开发过程都应当具有几个共用的活动。虽然可能没有必要共享相同的名字，但是这些核心的动作对于开发健全的、安全的系统来说都是必不可少的。下面列出了这些动作：

- 概念定义
- 功能需求确定
- 控制规范的开发
- 设计审查
- 代码审查走查
- 用户验收测试

- 维护和变更管理

本章稍后的“生命周期模型”部分将分析两个生命周期模型，并且说明如何在实际的软件工程环境中应用这些活动。

注意：

注意到下面这一点十分重要：系统开发生命周期中使用的术语在不同的模型、不同的发行产品之间是有区别的。不必花费太多的时间担心本书或可能遇到的其他文献中使用的术语是否有区别。参加 CISSP 考试时，深入理解处理过程如何工作以及支撑安全系统开发的基本原理是极其重要的。也就是说，与任何规则一样，都可能存在一些例外。

1. 概念定义

系统开发的概念定义阶段涉及为系统创建基本的概念声明。简而言之，是由所有利益相关方(开发人员、客户和管理人员)协商的简单声明，规定了项目用途以及系统大体需求。概念定义是一份非常高级的用途声明，仅包括寥寥一两段话。如果阅读项目的详细总结，那么会看到概念声明是一个摘要或简介，它使得外行可以在短时间内对项目具有高度概括性的理解。

在系统开发过程的所有阶段参考概念声明是很有帮助的。开发过程错综复杂的细节常常使项目的最高目标变得模糊不清。简单地定期阅读概念声明能够帮助开发团队重新瞄准自己的目标。

2. 功能需求确定

一旦所有的利益相关方都同意概念声明，那么开发团队就该着手开始功能需求确定过程。在这个阶段，具体的系统功能会被列出来，并且开发人员开始考虑系统的这些部分应当如何互相协作，以便满足功能需求。从这个阶段得出的是功能需求文档，它们列出了具体的系统需求。

与概念声明一样，在工作进入下一阶段之前，确保所有利益相关方都同意功能需求文档是十分重要的。当功能需求确定过程最终完成时，功能需求文档不应当被简单地束之高阁而且落满尘土，整个开发团队都应该在全部阶段不断地参考这份文档，以确保项目正常进行。在最后的测试和评估阶段，项目管理者应当使用这份文档作为核对清单，确保所有功能需求得到满足。

3. 控制规范的开发

树立起安全意识的组织还会确保从最早的开发阶段开始就将恰当的控制设计到所有系统中。在生命周期模型中，具有控制规范的开发阶段常常是非常有用的。这个阶段在功能需求开发阶段后不久开始，并且往往在设计和审核阶段继续进行。

在控制规范的开发过程中，从许多安全角度对系统进行分析是很重要的。首先，恰当的访问控制必须被设计到所有的系统中，从而确保只有授权的用户被准许访问系统，并且不允许他们超出授权级别。其次，系统必须通过使用正确的加密和数据保护技术来维护关键数据的机密性。再次，系统不仅应当提供审计跟踪来强制实施个人的可问责性，而且应当提供对非法活动的检测机制。最后，根据系统的危险程度，必须解决可用性和容错问题。

需要记住的是，将安全性设计到系统中不是一次性过程，并且必须主动进行。系统经常在设计时缺乏安全性计划，并且随后开发人员试图利用正确的安全机制更新系统。遗憾的是，这些机制慢了一拍，并且没有完全与系统设计集成在一起，这就造成了裂口性的安全漏洞。此外，在每次对设计规范进行重大改动时应当再次参考安全需求。如果系统的主要组件发生了变化，那么很可能也要

对安全性需求进行改动。

4. 设计评审

一旦完成功能需求确定和控制规范开发过程，那么系统设计人员就可以开始工作了！在这个漫长的过程中，设计人员要正确地确定系统的不同部分将如何相互操作以及如何布置模块化的系统结构。此外，在这个阶段，设计管理团队通常为不同的团队设置具体的任务，并且布置编码里程碑的初步完成时间。

设计团队完成正式的设计文档后应当与利益相关方召开评审会议，确保每个人都同意此过程在按部就班地进行，在向着成功开发具有所期望功能的系统的方向迈进。

5. 代码审查走查

一旦利益相关方为软件设计提供了支持，那么软件开发人员就可以开始编写代码。在编码过程的不同里程碑，项目经理应该安排几次代码审查走查会议。这些技术性会议通常只涉及开发人员，他们根据特定模块的代码副本进行走查，寻找逻辑流中的问题或其他设计/安全性缺陷。这些会议有助于确保不同开发团队开发的代码依据规范执行。

6. 用户验收测试

在经过多次代码审查和漫长时间之后，就会到达开发人员写下最后一个分号并表示系统完成的结束点。很多经验丰富的软件工程师都知道，系统永远不可能完成。现在要进入的是系统测试复审阶段。最初，大多数组织由开发人员执行系统的初始测试，从而找出一些明显的错误。

一旦这个阶段完成，代码可能会转移到部署。与任何关键的开发过程一样，保存一份书面的测试计划和测试结果是非常重要的，可供将来审查。

7. 维护和变更管理

一旦系统可以操作，面对操作、数据处理、存储和环境需求的改变，为了确保持续运作，有必要进行多样的维护工作。拥有一支有经验的、能够处理常规或意外维护任务的支持队伍是必不可少的。同样重要的是，任何代码的变更都要通过正式的变更管理流程来进行，如第 1 章所述的“通过原则和策略来进行安全治理”。

20.1.3　生命周期模型

你会从许多较为成熟的工程学科(例如，土木工程、机械工程和电子工程)从业者那里听到很多意见，其中一种说法就是软件工程根本不是工程学科。事实上，他们坚持认为，软件工程仅仅是一些混沌过程的组合，有时由于某种原因经过管理成为可工作的解决方案。实际上，在目前的开发环境中出现的一些软件工程只是依靠“胶带和鸡肉丝”组合在一起的引导编码。

然而，可以从采用更正式的生命周期管理过程中看到主流软件工程行业的成长。毕竟，把一门古老的学科，如土木工程的过程，和一门只有几十年历史的产业学科进行比较是不公平的。在 20 世纪 70 年代和 80 年代，先驱者(如 Winston Royce 和 Barry Boehm)提出软件开发生命周期(SDLC)模型来帮助指导软件开发实践走向形式化的过程。在 1991 年，软件工程研究所介绍的能力成熟度模型，描述了过程的组织保证，因为他们朝着将固体工程原则纳入软件开发的过程。在下面的章节中，

我们将看看这些研究产生的成果。合适的管理模型应该能够改善最终的产品。然而，仅仅有 SDLC 方法论是不够的，项目可能无法满足企业和用户的需求。所以，验证软件开发生命周期模型是否正确实施以及是否适合环境是非常重要的。此外，实施 SDLC 模型的初始步骤之一包括获得管理层的批准。

1. 瀑布模型

瀑布模型最初是由 Winston Royce 在 1970 年开发的，它试图将系统开发的生命周期看作一系列反复活动。如图 20.2 所示，传统的瀑布模型有 7 个开发阶段。在每个阶段完成时，项目会进入下一个阶段。正如相反箭头所示，现代的瀑布模型准许开发返回到先前的阶段，从而纠正在后续阶段发现的错误。这通常被称为瀑布模型的反馈循环特征(feedback loop characteristic)。

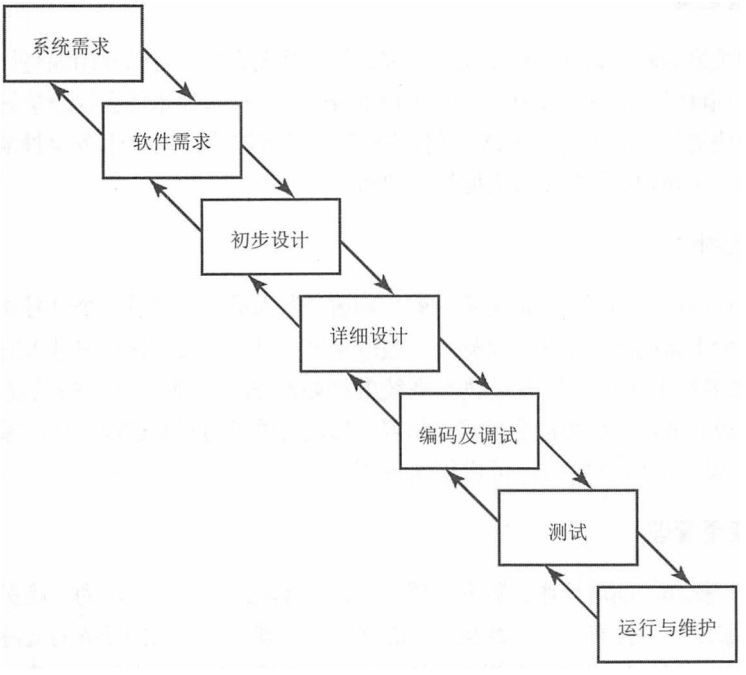


图 20.2　瀑布生命周期模型

瀑布模型是在考虑返回先前阶段以纠正系统错误的必要性的情况下，建立软件开发过程的模型的第一次全面尝试。然而，这个模型受到的一个主要批评是：只准许开发人员后退一个阶段。瀑布模型并没有对开发周期后期发现错误做出相应规定。

注意：

近来，人们通过为每个阶段都添加确认和验证步骤改进了瀑布模型。验证针对规范评估产品，而确认则评估产品满足实际需求的程度。这种改进的模型被标记为改良瀑布模型。不过，在螺旋模型统治项目管理领域之前，改良瀑布模型并未得到广泛应用。

2. 螺旋模型

1988 年，TRW 的 Barry Boehm 提出了一种替代的生命周期模型，允许瀑布类型处理过程多次反复。图 20.3 说明了这种模型。因为螺旋模型封装了许多迭代的其他模型(也就是瀑布模型)，所以

被称为元模型或“模型的模型”。

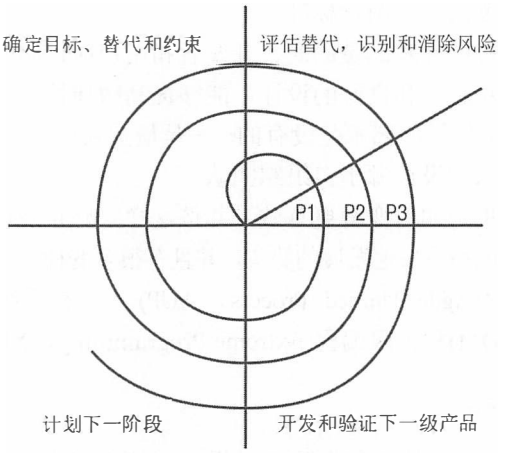


图 20.3　螺旋生命周期模型

可以注意到，螺旋的每次“回路”都导致新系统原型的开发(在图 20.3 中用 Pl、P2 和 P3 表示)。理论上，系统开发人员为每个原型的开发应用完整的瀑布处理过程，由此逐渐得到满足所有功能要求(经过全面验证)的成熟系统。Boehm 的螺旋模型为瀑布模型受到的主要批评提供了一个解决方案，也就是说，如果技术需求和客户需求发生变化，需要改进系统，就允许开发人员返回到计划编制阶段。

3. 敏捷软件开发

最近，软件开发的敏捷模型已经在软件工程界越来越受欢迎。从 20 世纪 90 年代中期开始，开发者越来越接受避开过去僵化模式的软件开发方法，喜欢采用替代的、强调客户需求的和快速开发的新功能，并以迭代的方式满足这些需求。

17 位敏捷开发方法的先驱在 2001 年聚集在一起，制作了一份名为“敏捷开发宣言”的文档(http://agilemanifesto.org)，这份文档声明了这种敏捷开发方法的核心理念：

我们正在发现更好的方法以开发软件，通过这样做和帮助他人这样做。通过这项工作，我们可以获得以下价值:

个体与交互重于过程和工具

有效的软件重于完整的文档

客户合作重于合同谈判

响应变更重于遵循计划

也就是说，虽然有价值的条目在右边，但我们更重视条目的左边。

“敏捷宣言”还定义了基础理念的 12 条原则，可查看 http://agilemanifesto.org/principles.html。

在“敏捷宣言”中所说的 12 条原则是：

- 我们的最高优先级是通过早期和持续交付有价值的软件来满足客户。
- 欢迎不断变化的需求，甚至在开发后期。敏捷过程利用变化为客户取得竞争优势。
- 在几星期到几个月的时间里以较短的时间，频繁地提供能用的软件。
- 业务人员和开发人员在整个项目过程中，每天都要在一起工作。
- 围绕着积极的个人建立项目。给他们所需要的环境和支持，并且相信他们能够完成这项工作。

- 在开发团队中传递信息的最有效率和最优效果方法是面对面交谈。
- 有效的软件是进度的首要衡量标准。
- 敏捷过程促进可持续开发。赞助商、开发者和用户应该始终保持同一个步调。
- 持续关注技术的卓越性和良好的设计，能够提高敏捷性。
- 简单——最大化工作量的艺术是没有的——是最重要的。
- 最好的架构、需求和设计源于自组织团队。
- 在团队内部定期思考如何变得更有效，并按这样来修正及优化自身的行为。

敏捷开发方法在软件圈里有快速发展的势头，并且有很多变种，包括 Scrum(迭代式增量软件开发过程)、敏捷统一过程(Agile Unified Process，AUP)、动态系统开发模型(Dynamic System Development Model，DSDM)和极限编程(Extreme Programming，XP)。

4. 软件能力成熟度模型

Carnegie Mellon 大学的软件工程学院(SEI)提出了软件能力成熟度模型(Software Capability Maturity Model，缩写为 SW-CMM、CMM 或 SCMM)，这种模型主张所有从事软件开发的组织都依次经历不同的成熟阶段。SW-CMM 描述了支持软件过程成熟度的原则与惯例，目的是：通过实现从特别混沌的过程到成熟的、有纪律的软件过程的发展路径，从而帮助软件组织改善软件过程的成熟度和质量。SW-CMM 背后的思想是软件的质量依赖于其开发过程的质量。

SW-CMM 具有下列阶段：

第 1 阶段：初始级 在这个阶段，常常可以发现在无组织的工作模式中有很多努力工作的人。通常，这个阶段几乎没有或完全没有定义软件开发过程。

第 2 阶段：可重复级 在这个阶段，出现基本的生命周期管理过程。开始有组织地重用代码，而且类似的项目期望具有可重复的结果。SEI 将用于这个级别的主要处理范围定义为：需求管理、软件项目计划编制、软件项目跟踪和监督、软件转包合同管理、软件质量保证和软件配置管理。

第 3 阶段：定义级 在这个阶段，软件开发人员依照一系列正式的、文档化的软件开发过程进行操作。所有开发项目都在新的标准化管理模型的制约下进行。SEI 将用于这个级别的主要处理范围定义为：组织处理中心、组织处理定义、培训计划、综合的软件管理、软件产品工程、团体之间的协调和对等复审。

第 4 阶段：管理级 在这个阶段，软件处理过程的管理进入下一个级别。定量衡量被用来获得对开发过程的详细了解。SEI 将用于这个级别的主要处理范围定义为：定量处理管理和软件质量管理。

第 5 阶段：优化级 在优化的组织中，会采用一个继续改进的过程。成熟的软件开发过程已经确立，可以确保为了改善未来的结果将一个阶段的反馈返回给前一个阶段。SEI 将用于这个级别的主要处理范围定义为：缺陷预防、技术更改管理和过程更改管理。要了解有关软件能力成熟度模型的更多信息，可以参见 SEI 的 Web 站点 www.sei.cmu.edu。

5. IDEAL 模型

SEI 还为软件开发确立了 IDEAL 模型，这种模型实现了许多 SW-CMM 属性。IDEAL 模型具有下列 5 个阶段：

1：启动 在 IDEAL 模型的启动阶段，概述更改的业务原因，为举措提供支持，以及准备好恰当的基础设施。

2：诊断　在诊断阶段，工程师分析组织的当前状态，并且为更改给出一般性建议。

3：建立　在建立阶段，组织采用诊断阶段的一般建议，并且开发帮助实现这些更改的具体动作计划。

4：行动　在行动阶段，停止“讨论”开始“执行”。组织开发解决方案，随后测试、改进和实现解决方案。

5：学习　与任何质量改进过程一样，组织必须不断分析其努力的结果，从而确定是否已实现期望的目标，必要时建议采取新的行动，使组织重返正轨。

IDEAL 模型如图 20.4 所示。

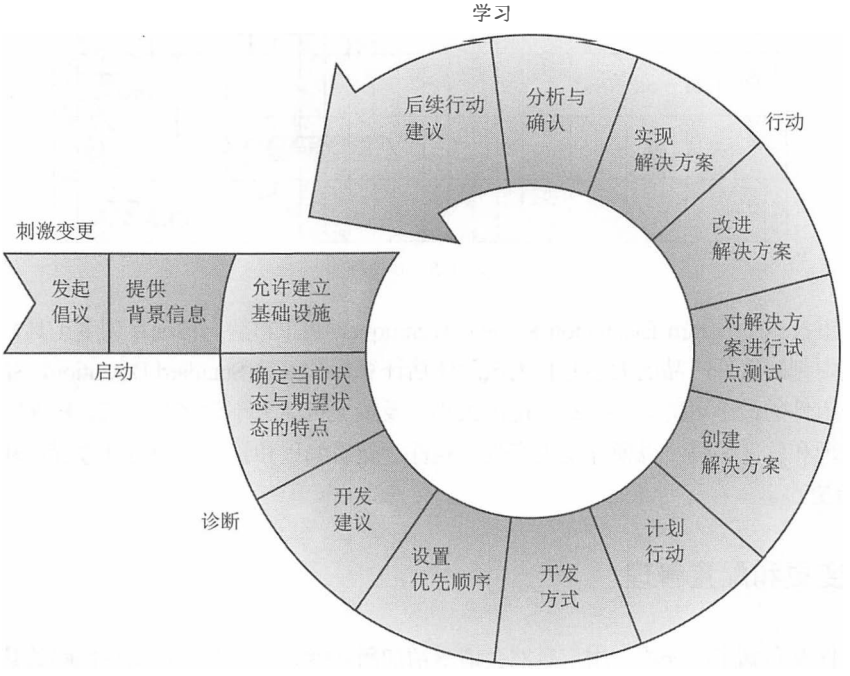


图 20.4　IDEAL 模型

SW-CMM 和 IDEAL 模型的记忆方法

为了帮助记忆 SW-CMM 和 IDEAL 模型的 10 个级别名的首字母(ll DR ED AM LO)，可以想象一下正坐在精神病医生办公室的长沙发上说着：“I...I，Dr.Ed，am lo(w)”。如果能够记住这条短句，那么就可以抽取这些级别名的首字母。如果将这些字母排成两列，那么就可以按照顺序重构两个系统的级别名。如下所示，左边一列字母是 IDEAL 模型，右边一列字母则表示 SW-CMM 各级别的首字母：

Initiating(初始	Initiating(初始)
Diagnosing(诊断)	Repeatable(可重复)
Establishing(建立)	Defined(定义)
Acting(行动)	Managed(管理)
Learning(学习)	Optimized(优化)

20.1.4 甘特图与 PERT

甘特图是一种显示不同时间项目和调度之间相互关系的条形图，提供了帮助计划、协调和跟踪项目中特定任务的调度图表。图20.5给出了甘特图的一个示例。

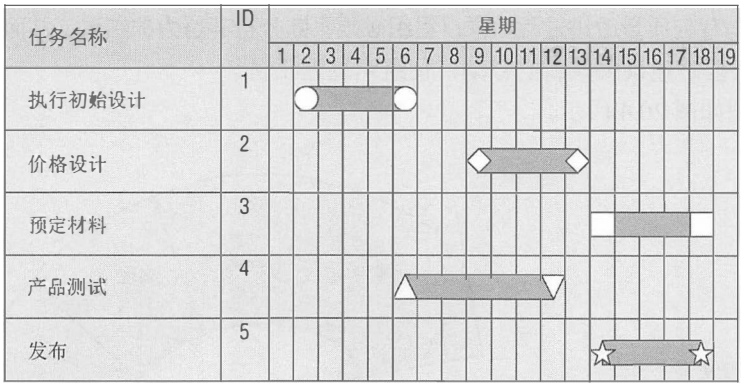


图 20.5 甘特图

计划评审技术(Program Evaluation Review Technique，PERT)是一种项目调度工具，这种工具被用于在开发中判断软件产品的大小并且为风险评估计算标准偏差(Standard Deviation，SD)。PERT 将估计的每个组件的最小可能大小、最可能的大小以及最大可能大小联系在一起。PERT 被用于直接改进项目管理和软件编码，以便开发更有效的软件。随着编程和管理能力得到改善，软件的实际生成大小应当更小。

20.1.5 变更和配置管理

一旦软件发布到生产环境，用户必然会请求增加新功能、修正 bug 以及对代码的其他更改。正像组织开发软件的严密过程一样，同样也必须以有组织的方式管理所请求的更改。这些变更必须被记录到中央存储库，以支持将来的审计、调查和分析需求。

将变更管理作为安全工具

在受控的数据中心环境中监视系统时，变更管理(又称为控制管理)扮演了重要的角色。本书的一位作者最近与一个组织一起工作，将变更管理作为一种能够检测对计算系统进行非授权更改的主要组件来使用。

在本章中，你将会了解到文件完整性监控工具(例如，Tripwire)如何允许监控系统的变化。这个组织使用 Tripwire 来监控数百台生产服务器。然而，该组织很快发现难以应付由于正常活动导致的文件修改警告。该作者与组织一起工作，希望调整 Tripwire 监控策略并集成它们到变更管理流程中。此时，所有的 Tripwire 警告都被集中至监控中心，监控中心的管理员将这些警告与变更许可联系在一起。只有在安全团队确定某个变更并不关联任何认可的变更请求时，系统管理员才会接收到警告。

这种方式大大减少了管理员检查文件完整性所花费的时间，并且为安全管理员改进了安全工具的有效性。

这种变更管理流程有三个基本组件：

请求控制　请求控制过程提供了一个有组织的框架，在这个框架内，用户可以请求变更，管理者可以进行成本/效益分析，开发人员可以优化任务。

变更控制　开发人员使用变更控制过程来重新创建用户遭遇的特定情况并且分析能够进行弥补的适当变更。变更控制过程也提供了一个有组织的框架。在这个框架内，多个开发人员可以在部署到生产环境之前创建和测试某个解决方案。变更控制包括：遵守质量控制约束，开发用于更新或更改部署的工具，正确记录任何编码变化，以及将新代码对安全性的负面影响最小化。

发布控制　一旦完成变更，它们就必须通过发布控制过程来进行发布认可。发布控制过程中一个必不可少的步骤是：复核并确保更改过程中作为编程辅助设计插入的任何代码(例如，调试代码和/或后门)，在发布新软件产品之前都已被删除。发布控制还应当包括验收测试，从而确保对终端用户工作任务的任何更改都是可理解的和有用的。

除了更改控制过程之外，安全管理员还应当意识到配置管理的重要性。配置管理过程用于控制整个组织范围内使用的软件版本，并且正式跟踪和控制对软件配置的更改。这个过程具有下列 4 个主要组件：

配置标识　在配置标识过程中，管理员记录整个组织范围内的软件产品的配置。

配置控制　配置控制确保对软件版本的更改要与更改控制和配置管理策略一致。只有符合这些策略的授权分发才能够执行更新操作。

配置状态统计　用于跟踪所有发生的授权更改的正规过程。

配置审计　进行定期的配置审计能够确保实际的生产环境与统计记录一致，以及确保没有发生未授权的配置变更。

总之，变更控制与配置管理技术一起构成了软件工程体系的重要部分，并且能够防止组织遭遇与开发相关的安全性问题。

20.1.6　DevOps 方法

最近，许多技术专业人士意识到，在软件开发、质量保证和技术操作这些主要的 IT 职能之间存在脱节的情况。这些职能，通常配备给不同类型的个人，并且还位于不同的组织，通常彼此冲突。这种冲突导致在创建代码、测试和部署到生产环境中的长时间延迟。当问题出现时，团队不是一起合作解决问题，而是经常“踢皮球”，这导致官僚作风。

DevOps 方法通过将三种职能集中在一个操作模型中来解决这些问题。DevOps 这个词是开发(Development)和操作(Operations)的组合，表示这些功能必须合并和合作才能满足业务需求。图 20.6 中的模型说明了软件开发、质量保证和 IT 操作的重叠性。

DevOps模型与敏捷开发方法紧密配合，旨在显著地缩短开发、测试和部署软件更改所需的时间。虽然传统方法常常导致主要软件部署很少，或许每年一次，但是使用DevOps模型的组织通常每天部署代码多次。一些组织甚至努力实现连续部署的目标，其中代码可以每天部署几十甚至几百次。

注意：

如果有兴趣学习关于 DevOps 更多的内容，作者极力推荐一本书给大家，书名叫作 *The Phoenix Project: A Novel about IT,DevOps,and Helping Your Business Win* (IT Revolution Press,2013)。这本书以引人入胜的小说形式呈现了 DevOps 案例，分享了 DevOps 战略。

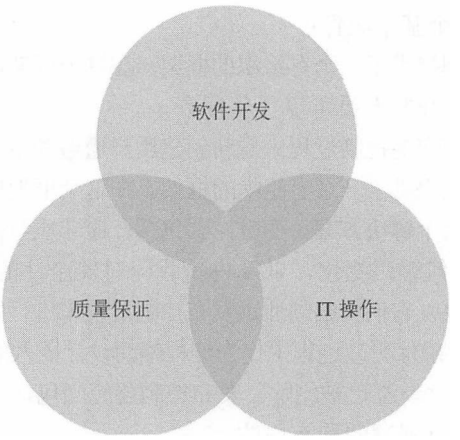


图 20.6　DevOps 模型

20.1.7　应用编程接口

尽管早期的 Web 应用程序通常是处理用户请求和提供输出的独立系统，但现代的 Web 应用程序越来越复杂，它们通常包括多个不同的 Web 服务之间的交互。例如，一个零售网站可能会利用一个外部信用卡处理服务，允许用户在社交媒体上分享他们的采购信息，与运输供应网站集成，并在其他网站上提供推荐计划。

为了使这些跨站点功能正确工作，网站必须相互交互。许多组织为了这个目标提供应用编程接口(API)。API 允许应用程序开发人员绕过传统的网页，并通过函数调用直接与底层服务进行交互。例如，一个社交媒体 API 可能包括以下一些 API 函数调用：

- 发布状态
- 关注用户
- 取消关注的用户
- 喜欢/喜爱的发布

提供和使用 API 为服务提供商创造了巨大的机会，但也带来了一些安全风险。开发人员必须意识到这些挑战，并在创建和使用 API 时解决这些挑战。

首先，开发人员必须考虑认证要求。一些 API，比如允许检查天气预报或产品库存的 API，可以向公众提供，并且不需要任何认证就可以使用。其他 API，例如那些允许修改信息、下订单或访问敏感信息的 API，只限于特定用户并且依赖于安全认证。API 开发人员必须知道何时需要身份认证，并确保他们认证每个 API 调用的凭据和授权。这种认证通常通过为授权的 API 用户提供一个被每一个 API 调用通过的复杂 API 密钥来完成。后端系统在处理请求之前验证此 API 密钥，确保进行请求的系统被授权进行特定的 API 调用。

警告：

API 密钥就像密码，应该被视为非常敏感的信息。它们应该总是存储在安全位置，并且仅在加密的通信信道上传输。如果有人获得对 API 密钥的访问权限，他们就可以与 Web 服务进行交互，就像他们是你一样！

API 也必须彻底测试安全缺陷，就像任何 Web 应用程序一样。将在下一节中了解更多信息。

20.1.8　软件测试

作为开发过程的一部分，组织在内部分发(或市场发布)任何软件之前都应当对其进行彻底测试。进行测试的最佳时间是设计模块之时。换句话说，用于测试某个产品的机制和用于研究该产品的数据集应当与产品本身同时进行设计。编程团队应当开发特殊的数据测试组以及预先知道正确的输出结果，通过这些数据测试组能够测试软件所有可能的执行路径。

应该执行的多个测试的其中一个是合理性检查。合理性检查确保匹配的符合指定指标的返回值在合理的范围内。例如，一个程序计算一个人的最佳体重，并返回 612 磅的值，这肯定是一次失败的合理性检查！

此外，在进行软件测试时，应该测试软件产品如何处理正常和有效的输入数据、不正确的类型、越界值以及其他界限和/或条件。真实的工作量可能提供最佳的压力测试。但是，因为一个缺陷或错误就会导致违背测试数据的完整性或机密性，所以不应该使用真实的或实际的现场数据进行测试，在早期开发阶段尤其如此。

测试软件时，应该应用与组织其他方面所使用的相同的责任分离规则。换句话说，应当指定编程人员以外的人员进行软件测试，从而避免利益冲突，并且能够保证最后的产品更成功。在第三方测试软件时，必须确保第三方执行客观的和无偏见的检查。第三方测试允许更广泛和更彻底的测试，并且能够防止由于编程人员的偏见和爱好而影响测试结果。

可以使用下列三种软件测试方法：

白盒测试　白盒测试检查程序的内部逻辑结构并逐行执行代码，从而分析程序是否存在潜在的错误。

黑盒测试　通过提供广泛的输入场景和查看输出，黑盒测试从用户的角度检查程序。黑盒测试人员并不访问内部的代码。在提交系统之前进行的最终验收测试就是黑盒测试的常见示例。

灰盒测试　灰盒测试组合了上述两种测试方式，并且是一种流行的软件验证方式。在这种测试方式中，测试人员着手从用户的角度处理软件，分析输入和输出。测试人员也会访问源代码，并且使用源代码来帮助设计测试。不过，测试人员在测试期间并不分析程序的内部工作原理。

除了评估软件的质量，程序员和安全专业人员应仔细评估软件的安全性，以确保满足组织的安全要求。这对于暴露给公众的 Web 应用程序尤其关键。有两种专门用于评估应用程序安全性的测试类别：

静态测试　静态测试通过分析源代码或编译的应用程序来评估软件的安全性，而不需要运行软件。静态分析通常涉及使用自动化工具来检测常见的软件缺陷，如缓冲区溢出(关于缓冲区溢出的更多内容，请参见第 21 章“恶意代码与应用攻击”)。在成熟的开发环境中，应用程序开发人员可以访问静态分析工具，并在整个设计/构建/测试过程中使用它们。

动态测试　动态测试在运行时环境中评估软件的安全性，并且通常是部署了由其他人编写的应用程序的组织的唯一选择。在这些情况下，测试人员通常无法访问基础的源代码。动态软件测试的常见示例是使用 Web 应用程序扫描工具来检测是否存在跨站脚本、SQL 注入或 Web 应用程序中的其他缺陷。在生产环境下的动态测试应始终仔细考虑以避免意外中断服务。

正确地实施软件测试是项目开发过程中的一个关键要素。通常在商业和内部软件中发现的许多常见错误和疏忽都可以消除。保持测试计划和结果作为系统永久性文档的一部分。

20.1.9 代码仓库

软件开发需要共同的努力，大型软件项目需要开发人员团队可以同时承担代码的不同部分的工作。使情况进一步复杂化的事实是，这些开发者可能在地理上分散在世界各地。

代码仓库提供了支持这些协作的几个重要功能。首先，它们作为开发人员放置源代码的中心存储点。此外，代码仓库(如 GitHub、Bitbucket 和 SourceForge)还提供版本控制、错误跟踪、Web 托管、发布管理和支持软件开发的通信功能。

代码仓库是促进软件开发的出色的协作工具，但它们也有自己的安全风险。首先，开发人员必须适当地控制对仓库的访问。一些仓库，如支持开源软件开发的仓库，可能允许公众访问。其他仓库，如托管含有商业机密信息的代码，可能受到更多限制，并限制对授权开发者的访问。仓库所有者必须仔细设计访问控制，仅允许适当的用户读取和/或写入访问权限。

敏感信息和代码仓库

开发人员必须注意不要在公共代码仓库中包含敏感信息，这尤其适用于 API 密钥。

许多开发人员使用API来访问基础设施服务提供商的基础功能，例如Amazon Web Services(AWS)、Microsoft Azure和Google Compute Engine。这提供了巨大的好处，使开发人员能够快速配置服务器、修改网络配置和使用简单的API调用来分配存储。

当然，IaaS 提供商对这些服务收费。当开发人员准备一台服务器时，就会触发该服务器每小时收费，直到它被关闭。用于创建服务器的 API 密钥将服务器绑定到特定的用户账户(和信用卡！)。

如果开发人员编写包含 API 密钥的代码，然后将 API 密钥上传到公共存储库，则世界上的任何人都可以访问他们的 API 密钥。这允许任何人创建 IaaS 资源，并且费用由原开发者的信用卡支付。

在进一步恶化的情况下，黑客已经写了机器人，四处搜索公共代码仓库中泄露的 API 密钥。这些机器人可以在几秒钟内检测到无意中发布的密钥，并允许黑客在开发人员甚至知道他们的错误之前快速提供大量的计算资源！

20.1.10 服务等级协议

使用服务等级协议(SLA)是越来越流行的方式，是被服务提供商和服务供应商都认同的确保组织向内部和/或外部客户提供服务，并保持适当服务水平的一种方法。对于组织的持续生存能力，把所有的数字电路，应用程序、信息处理系统、数据库或其他关键组件都置入 SLA 是明智的，也是至关重要的。SLA 中通常涉及以下问题：

- 系统正常运行时间(如总工作时间的百分比)
- 最大连续停机时间(以秒/分钟为单位等)
- 高峰负荷
- 平均负荷
- 责任诊断
- 故障切换时间(如冗余到位)

如果不能维持协议，服务级别协议通常还包括财务和其他合约商讨好的补救措施。例如，如果关键电路停机超过 15 分钟，服务提供商可能同意放弃该电路上的所有费用一周。

20.1.11　软件采购

企业使用的大多数软件都不是内部开发的，而是从供应商那里采购。这些软件中的一些被购买并运行在组织管理的服务器上，无论是在内部还是在基础设施即服务(IaaS)环境中。其他软件是以软件即服务(SaaS)方式通过 Web 浏览器从互联网购买和提供的。大多数组织根据业务需求和软件可用性，结合使用这些方法。

例如，组织可能会以两种方式来使用电子邮件服务。他们可能购买物理或虚拟服务器，然后在上面安装电子邮件软件，如 Microsoft Exchange。在这种情况下，组织从 Microsoft 购买 Exchange 许可证，然后安装、配置和管理电子邮件环境。

作为一种替代方案，组织可能会选择将电子邮件完全外包给 Google、Microsoft 或其他供应商。然后，用户通过他们的 Web 浏览器或其他工具访问电子邮件，直接与供应商管理的电子邮件服务器进行交互。在这种情况下，组织只负责创建账号和管理某些应用程序级的设置。

在任何一种情况下，安全都应该被关注。当组织购买和配置软件本身时，安全专业人员必须了解软件的正确配置以满足安全目标。他们还必须对安全公告和补丁保持警惕，以纠正新发现的漏洞。不履行这些义务可能会导致不安全的环境。

在 SaaS 环境中，大多数安全责任由供应商负责，但是组织的安全人员也不能逃脱责任。虽然他们可能不负责同样多的配置，但他们现在负责监控供应商的安全。这可能包括审计、评估、漏洞扫描和旨在验证供应商是否保持适当控制的其他措施。

20.2　创建数据库和数据仓储

几乎所有的现代型公司都维护着一些类别的数据库，它们包含操作的关键信息，例如用户的联系信息、订单跟踪数据、人事和福利信息或一些敏感的商业机密。许多这样的数据库一般都包含属于用户秘密的个人信息，如信用卡使用活动、旅行习惯、商店购物和电话记录。由于对数据库系统依赖程度增加，因此信息安全专家必须确保具备适当的安全控制，从而保护数据免受未授权的访问、篡改或破坏。

接下来，我们将讨论数据库管理系统(DBMS)的体系结构、各种不同的 DBMS 类型及特性。随后还会讨论数据库安全特性，包括多实例、ODBC、聚合、推理以及数据挖掘。

20.2.1　数据库管理系统的体系结构

尽管目前存在多种可用的数据库管理系统(DBMS)，但当今的大多数系统都使用一种被称为关系型数据库管理系统(RDBMS)的技术。因此，下面的内容主要关注于关系数据库。不过，我们首先要讨论两个重要的 DBMS 体系结构：层次式数据库和分布式数据库。

1. 层次式和分布式数据库

层次式数据模型将关联的记录和字段组合为一个逻辑树结构。这会导致一个“一对多”数据模型，其中的每个节点可能不具有子节点，也可能具有一个或多个子节点，但是都只具有一个父节点。

图 20.7 说明了一个层次式数据模型。

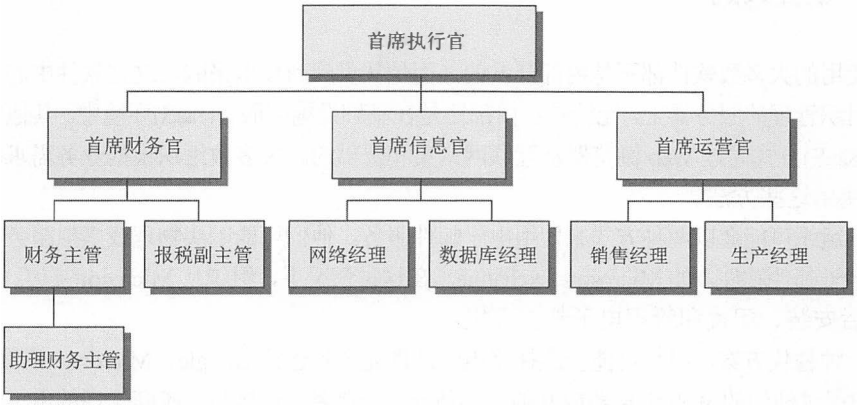


图 20.7 层次式数据模型

图 20.7 中的层次式数据模型是一家公司的组织结构图。注意，这个示例适用“一对多”数据模型。某些员工拥有一名部下，某些员工拥有多名部下，另外一些员工则没有部下。然而，每位员工都只拥有一位经理。层次式数据模型的其他模型包括 NCAA 的“三月疯”对垒系统以及在互联网上使用的域名系统(DNS)记录的层次化分布。层次数据库以一种分层的方式来存储数据，并且对于适合该模型的专用应用程序是有用的。例如，生物学家可能会使用一个层次数据库存储标本数据，在那个领域内根据 kingdom/phylum/class/order/family/genus/species 层次模型。

分布式数据模型将数据存储在多个数据库中，不过这些数据库是逻辑连接的。即使数据库由通过互联网相互连接的许多部分组成，用户也仍然将数据库理解为单个实体。每个字段都具有许多子字段和父字段。因此，分布式数据库的数据映射关系是多对多。

2. 关系数据库

关系数据库是由行和列组成的平面二维表。实际上，每个表看起来类似一个电子表格文件。行列结构提供了一对一数据映射关系。关系数据库的主要构件是表(也被称为关系)。每个表都包含一组相关的记录。例如，某个销售数据库可能包含下列表：

- Customers 表，包含组织中所有客户的联系信息。
- Sales Reps 表，包含组织中销售人员的身份信息。
- Orders 表，包含每个用户所下订单的记录。

面向对象编程和数据库

对象-关系数据库结合了关系数据库和面向对象编程功能。在真正的面向对象数据库(OODB)中，由于方便了代码重用和故障处理分析，并减少了整体维护工作量，因而带来了好处。此外，与其他数据库类型相比，OODB 更适合支持涉及多媒体、CAD、视频、图形和专家系统的复杂应用程序。

上述每个数据表都包含许多属性或字段(field)。每个属性都对应表中的某个列。例如，Customers 表可能包含用于公司名、地址、城市、州、邮政编码和电话号码的不同列。每个用户都具有自己的记录或元组(tuple)，这些记录或元组由表中的某行表示。关系中行的数量被视为基数(cardinality)，列的数量被视为度(degree)。关系的域(domain)是一组属性可以采用的允许值。图 20.8 说明了某个关系数据库中 Customers 表的示例。

Company ID	Company Name	Address	City	State	ZIP Code	Telephone	Sales Rep
1	Acme Widgets	234 Main Street	Columbia	MD	21040	(301) 555-1212	14
2	Abrams Consulting	1024 Sample Street	Miami	FL	33131	(305) 555-1995	14
3	Dome Widgets	913 Sorin Street	South Bend	IN	46556	(574) 555-5863	26

图 20.8　关系数据库的 Customers 表

在这个示例中，Customers 表的基数为 3(对应于表中的 3 行)，度为 8(对应于表中的 8 列)。在正常业务过程中，例如当销售代表添加新客户时，表的基数发生变化是很常见的。表的度通常不会频繁改变，通常需要数据库管理员的干预才能变。

提示：

为了记住基数(cardinality)的概念，可以想象一下摆在桌上的一副纸牌，每张牌(card 是 cardinality 的前 4 个字母)就是一行。为了记住度(degree)的概念，可以想象一下挂在墙上的温度计(换句话说，作为温度计测量单位的度数 degree)。

定义表之间的关系以标识相关记录。在此例中，Customers 表和 Sales Rep 表之间存在关系，因为每个客户都被分配了一个销售代表，而每个销售代表被分配给一个或多个客户。此关系由 Customers 表中的 Sales Rep 字段/列反映，如图 20.8 所示。此列中的值指的是 Sales Rep 表中包含的销售代表 ID 字段(未显示)。此外，Customers 表和 Orders 表之间也可能存在关系，因为每个订单必须与客户相关联，并且每个客户与一个或多个产品订单相关联。Orders 表(未显示)可能包含一个包含客户 ID 值的客户字段。

记录可以使用多种键进行标识。简单地说，键是表中字段的子集，可以用于唯一标识记录。在希望相互引用这些信息时，它们还被用于连接表。你应当熟悉下列三种键：

候选键　可以被用于唯一标识表中记录的属性子集。在同一个表中，对于组成一个候选键的所有属性而言，任何两条记录的这些属性值都不完全相同。每个表都可能有一个或多个候选键，它们从列的头部选出。

主键　从表的这组候选键中选出的用来唯一标识表中记录的键被称为主键。每个表都只有一个主键，由数据库设计者从这组候选键中选出。通过不准许利用相同主键插入多个记录，RDBMS 强制实施了主键的唯一性。在图 20.8 所示的 Customers 表中，CompanyID 很可能就是主键。

外键　外键被用于强制在两个表之间建立关系(也称为参照完整性)。参照完整性确保：如果一个表包含一个外键，那么它对应于关系中另一个表内仍然存在的主键。需要弄清楚的是，没有任何记录/元组/行包含对不存在的记录/元组/行的主键的引用。根据前面的描述。图 20.8 中的 Sales Rep 字段是参照 Sales Reps 表中主键的外键。

所有关系数据库都使用一种标准语言，即结构化查询语言(SQL)，从而为用户存储、检索和更改数据，以及管理控制 DBMS 提供了一致的接口。每个 DBMS 供应商实现的 SQL 版本略有不同(如 Microsoft 公司的 Transact-SQL 和 Oracle 公司的 PL/SQL)，但是都支持一个核心特性集。SQL 的主要安全特性是其授权的粒度。这意味着 SQL 允许为每个极细的级别设置许可。能通过表、行、列，甚至是些情况下单独的单元来限制用户访问。

数据库范式

数据库开发人员致力于创建组织有序的、有效的数据库。为了帮助完成这个目标，开发人员定义了若干被称为范式的数据库组织级别。使数据库表遵从范式的过程被称为规范化。

尽管存在许多范式，但是其中最常见的三种形式是：第一范式(1NF)、第二范式(2NF)以及第三范式(3NF)。这三种形式都添加了下面的需求：减少表中的冗余，消除错误放置的数据，执行其他许多内置处理任务。范式是渐进的，换句话说，要采用 2NF 格式，首先必须遵从 1NF 格式；要采用 3NF 格式，首先必须采用 2NF 格式。

数据库表的范式细节超出了 CISSP 考试的范围，但是某些 Web 资源能够帮助更详细地理解范式范式需求。例如，读者可以参考站点 http://databases.about.com/od/specificproducts/a/ normalization.htm 上“Database Normalization Basics”的相关内容。

SQL 为管理员、开发人员和终端用户与数据库交互提供了必需的完整功能。事实上，目前流行的图形数据库界面只不过是对 DBMS 的标准 SQL 接口进行了修饰。SQL 本身被分为两个截然不同的组件：数据定义语言(DDL)，允许创建和更改数据库的结构(数据库的结构被称为模式)；数据操纵语言(DML)，允许用户与模式内包含的数据交互。

20.2.2 数据库事务

关系数据库支持事务的显式和隐式使用，从而确保数据的完整性。每个事务都是 SQL 指令的离散集，作为一个组的这些 SQL 指令要么成功，要么失败。事务的一部分成功而另一部分失败的情况不可能出现。以银行内两个账户之间的转账为例。使用下面的 SQL 代码，可以先在账户 1001 中增加 250 美元，然后在账户 2002 中减少 250 美元：

```
BEGIN TRANSACTION
UPDATE accounts
SET balance = balance + 250
WHERE account_number = 1001;

UPDATE accounts
SET balance = balance - 250
WHERE account_number = 2002

END TRANSACTION
```

设想一下这两条语句未作为事务的部分被执行而是被分别执行的情况。如果数据库在第一个事务完成和在第二个事务完成之间的某个时间点出现失败，那么账户 1001 中增加了 250 美元，但是账户 2002 中的资金没有被相应减少。这 250 美元就是凭空多出的！这个简单的示例强调了面向事务的操作的重要性。

一个事务成功完成时，这个事务已被提交给数据库，并且不能取消。事务的提交可以是显式的，也就是使用 SQL 的 COMMIT 命令；可以是隐式的，也就是成功到达事务结束进行提交。如果必须中止事务，那么可以显式地使用 ROLLBACK 命令进行回滚操作，也可以是硬件或软件故障引起的隐式回滚。当一个事务被回滚时，数据库会将自身还原至这个事务开始前的状态。

所有的数据库事务都具有 4 个必需的特征：原子性、一致性、隔离性以及持久性。这些属性合称为 ACID 模型，这是数据库管理系统开发中的一个关键概念。下面简要介绍了这 4 种需求：

原子性 数据库事务必须是原子的，也就是说，必须是“要么全有，要么全无”的事务。如果事务的任何部分失败，那么整个事务都会被回滚，就像什么也没发生一样。

一致性 所有事务都必须在与数据库所有规则(例如所有记录都具有唯一的主键)一致的环境中

开始操作。事务结束时，无论事务本身操作期间是否违反了数据库的规则，数据库都必须再次与这些规则一致。其他任何事务都不能利用某个事务执行期间可能产生的任何不一致数据。

隔离性　隔离性原则要求事务彼此之间独立操作。如果数据库接收到两个更改相同数据的 SQL 事务，那么在一个事务被允许更改相同数据之前，另一个事务必须完全结束。隔离性能够防止一个事务处理另一个事务中途生成的无效数据。

持久性　数据库事务必须是持久的，也就是说一旦被提交给数据库，就会被保留下来。数据库通过使用备份机制(例如事务日志)确保持久性。

接下来将对数据库开发人员和管理员所关心的多种具体安全问题进行讨论。

20.2.3　多级数据库的安全性

你曾经在第 1 章学习过，基于分配给数据客体和单独用户的安全性标签，很多组织使用数据分类方案强制实施访问控制限制。当得到组织安全策略的委托授权时，这种分类概念还必须被延伸至组织的数据库。

多级安全性数据库包含大量不同分类级别的信息，它们必须对分配给用户的标签进行验证，并且根据用户的请求只提供适当的信息。然而，考虑到数据库的安全性，这种概念显得稍微复杂了一些。

要求多级安全性时，管理员和开发人员致力于使数据满足各种不同安全需求是必不可少的。将分类级别和/或“知其所需”需求不同的数据混合在一起被称为数据库污染，这是一个重大的安全风险。通常，管理员会通过部署可信前端为旧式的或不安全的 DBMS 添加多级安全性。

真实场景

使用视图限制访问

在数据库中实现多级安全性的另一种途径是使用数据库视图。视图只不过是将数据库表提供给用户的 SQL 语句。视图能够被用于整理来自多个表的数据、聚合单独的记录或限制用户访问数据库属性和/或记录的有限子集。

在数据库中，视图被存储为 SQL 语句而不是被存储为数据表。这样可以显著减少所需的数据库空间，并且允许视图违反应用于数据表的规格化规则。另一方面，因为 DBMS 可能需要通过执行计算来确定每条记录特定属性的值，所以从复杂的视图中检索数据的时间要明显长于从表中检索数据的时间。

因为视图非常灵活，所以许多数据库管理员将视图作为一种安全工具使用，就是允许用户只与受限的视图交互，而非与作为视图基础的原始数据表交互。

1. 并发性

并发性或编辑控制是一种预防性的安全机制，这种机制试图使数据库中存储的数据始终是正确的，或者至少使其完整性和可用性受到保护。不论数据库是多级的还是单级的，我们都可以使用这个特性。并发性使用“锁定”功能允许已授权用户更改数据，但是同时拒绝其他用户访问以查看或更改数据元素。更改完成后，“解锁”功能就允许其他用户执行自己所需的访问操作。在某些实例中，

管理员会使用具有审计的并发性机制来跟踪文档和/或字段的变化。检查已记录的数据时，并发性就成为一种检测性控制。

2. 其他安全机制

使用 DBMS 时，管理员可以部署其他一些安全机制。这些特性的实现相对简单，并且在业内是常见的。例如，与语义完整性相关的机制就是 DBMS 的一种常见安全特性。语义完整性确保用户的动作不会违反任何结构上的规则。此外，还检查存储的所有数据类型都位于有效的域范围内，确保只存在逻辑值，并且确认系统遵守任何和所有的唯一性约束。

管理员可能通过时间和日期标记来维护数据的完整性和可用性。时间和日期标记常常出现在分布式数据库系统中。在所有更改事务上添加时间标记，然后将这些更改分发或复制至其他数据库成员时，所有变化会应用于所有成员，但是需要按照正确的时间顺序实现变化。

DBMS 的另一个常见安全特性是在数据库内能够细粒度地控制对象，这也改善了安全控制。内容相关的访问控制就是细粒度对象控制的一个示例。内容相关的访问控制重点基于要访问对象的内容或有效载荷进行控制。因为必须在逐个访问对象的基础上做出决定，所以内容相关的访问控制增加了处理开销。细粒度控制的另一种形式是单元抑制。单元抑制的概念是对单独的数据库字段或单元隐藏或强加更安全的约束。

因为名字类似，所以上下文相关的访问控制与内容相关的访问控制经常被放在一起讨论。上下文相关的访问控制通过宏观评估来制定访问控制决策。上下文相关的访问控制的重要因素是每个对象、数据包或字段如何与总体的活动或通信相联系。任何单个元素本身看上去无关紧要，但是在较大的上下文环境中就会表露出是有益的还是有害的。

管理员可以使用数据库分区技术来防止聚合、推理和污染漏洞。数据库分区是将单个数据库分解为多个部分的过程，其中每个部分都具有唯一的和不同的安全级别或内容类型。

在同一个关系数据库表中，两行或更多行具有相同的主键元素，但是包含在不同分类级别使用的不同数据时，就会出现多实例(polyinstantiation)。多实例常常被用作针对某些推理攻击类型的防范措施(稍后将讨论推理攻击)。

以一个数据库表中包含巡逻的不同海军舰艇的位置为例。正常情况下，这个数据库包含每艘舰艇的准确位置，这属于秘密级信息。然而，一艘特殊的舰艇 UpToNoGood 正在暗中执行到达绝密位置的任务。海军指挥官不希望任何人知道这艘舰艇未处于正常的巡逻状态。如果数据库管理员简单地将 UpToNoGood 的位置分类更改为绝密，那么属于秘密级的用户在不能查询这艘舰艇的位置时就会知道发生了一些不正常的事情。然而，如果应用了多实例方法，那么表中可能会插入两个记录。第一条属于绝密级分类，将反映这艘舰艇的实际位置，并且只对属于绝密安全级的用户可用。第二条记录属于秘密级，将指出舰艇正在进行例行巡逻，并且向属于秘密安全级的用户显示这一内容。

最后，管理员可以利用噪声和干扰在 DBMS 中插入错误的或欺骗的数据，从而重定向或阻挠信息机密性攻击。这是一个被称为噪声和扰动的概念。在使用此技术时，必须非常小心，确保插入数据库中的噪声不会影响业务操作。

20.2.4 ODBC

开放数据库互连(ODBC)是一种数据库特性，也就是在不必分别针对交互的每种数据库类型直接进行编程的情况下，允许应用程序与不同数据库类型通信。ODBC 扮演了应用程序和后端数据库驱动程序之间代理的角色，使应用程序编程人员能够自由创建解决方案，而不必考虑后端的数据库系

统。图 20.9 说明了 ODBC 与 DBMS 之间的关系。

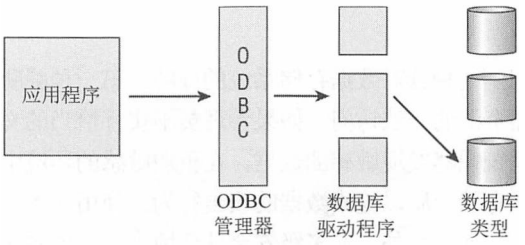


图 20.9　作为应用程序与 DBMS 之间接口的 ODBC

20.3　存储数据和信息

数据库管理系统已经帮助加强了数据的力量，并且获得了对可以访问数据的人和可以对数据执行的操作所进行的少量控制。然而，安全专家必须记住的是，DBMS 安全性只适用于通过传统的“前门”渠道访问信息。数据还通过计算机的存储资源(内存和物理介质)进行处理。为了确保这些基本的资源免受安全漏洞的威胁，就必须采取预防措施。毕竟，我们永远都不会将大量的时间和金钱花费在只保护前门而令后门大开，是吗？

20.3.1　存储器的类型

现代计算机系统使用几种类型的存储器来保存系统和用户的数据。为了满足组织对计算的要求，系统要在各种存储类型间进行平衡处理。目前常用的存储类型包括：

- 主(或实际)存储器由系统的 CPU 可以直接访问的主要存储资源组成。主存储器通常由易失性的随机访问存储器(RAM)组成，并且一般是系统可以使用的性能最高的存储资源。
- 辅助存储器由许多较廉价的、非易失性的、可供系统长期使用的存储资源组成。典型的辅助存储资源包括磁性的和光学的介质，如磁带、磁盘、硬盘和 CD/DVD 存储器。
- 虚拟内存准许系统利用辅助存储器模拟额外的主存储器资源。例如，系统缺少昂贵的 RAM，可能会利用硬盘的一部分作为直接 CPU 寻址使用。
- 虚拟存储器准许系统利用主存储器模拟辅助存储器的资源。虚拟存储器的最常见例子是作为辅助存储器提供给操作系统的“RAM 磁盘”(但是实际上在易失性 RAM 中实现)。这为多种应用程序的使用提供了极快的文件系统，但是没有提供恢复能力。
- 随机访问存储器准许操作系统请求介质上任意位置的内容。RAM 和硬盘都是随机访问存储器的例子。
- 顺序访问存储器需要从头到指定地址对整个介质进行扫描。磁带是常见的顺序访问存储器的例子。
- 易失性存储器在资源断电时会丢失上面的存储内容。RAM 是最常见的易失性存储器类型。
- 非易失性存储器不依赖于电源的供电来维持存储内容。磁性的/光学的介质和非易失性 RAM (NVRAM)都是非易失性存储器的例子。

20.3.2 存储器威胁

信息安全专家应当意识到两种针对数据存储系统的威胁。第一种威胁是无论正在使用哪种类型的存储器，都存在对存储器资源的非法访问。如果管理员不实行恰当的文件系统访问控制，那么入侵者就可能通过浏览文件系统偶然发现敏感的数据。在更加敏感的环境中，管理员还应当防止绕过操作系统控制直接访问物理存储介质以检索数据的攻击行为。使用加密文件系统是最好的办法，只有通过主操作系统才可以被访问。此外，在多级安全性环境中运作的系统应当通过提供恰当的控制来确保共享内存和存储器资源时提供故障安全(fail-safe)控制，从而使某个分类级别的数据对于较低分类级别的使用者来说是不可读取的。

隐蔽通道攻击是对存储器资源的第二种主要威胁。隐蔽存储通道准许通过直接或间接地操纵共享存储介质，在两个分类级别之间传输敏感的数据。这可能与向不经意间共享的内存或物理存储器的一部分写入敏感数据一样简单。更复杂的隐蔽存储通道可能操纵磁盘的可用空间或文件大小，在安全级别之间偷偷地传送信息。要了解隐蔽通道分析的更多信息，请参看第 8 章“安全模型的原则、设计和能力”。

20.4 理解基于知识的系统

自计算机问世以来，工程师和科学家们一直致力于开发能够执行常规操作的系统，这些操作将会耗费人力和消耗大量时间。这方面的大部分成就都集中于减轻计算密集型任务的负担。然而，研究人员也在开发“人工智能”系统方面取得了巨大进步，可以(在一定程度上)模拟纯粹的人类推理能力。

接下来的部分研究了两种类型的以知识为基础的人工智能系统：专家系统和神经网络。我们也将看到它们潜在的计算机安全问题。

20.4.1 专家系统

专家系统试图具体化人类在某个特殊学科累积的知识，并且以一致的方式将它们应用于将来的决定。一些研究已经表明：在正确开发和实现专家系统之后，专家系统常常能够做出比人类的常规决策更好的决定。每个专家系统都有两个主要的组件：知识库和推理引擎。

知识库包含专家系统已知的规则。知识库试图以一系列“if/then”语句对人类专家的知识进行编码。让我们考虑一个简单的专家系统，它被设计用于帮助房主们决定在面临飓风的威胁时是否应该撤离某个区域。知识库可能包含下列一些语句(这些语句只是一些例子)：

- 如果飓风是 4 级或更高级别的风暴，那么洪水一般会达到海拔 20 英尺高。
- 如果飓风的风速超过了每小时 120 英里，那么木质结构的建筑物将被毁坏。
- 如果是在飓风季节末期，那么飓风在到达海岸时会变得更强。

在实际的专家系统中，知识库将包含成百上千个如上所示的断言。

专家系统的另一个主要组件是推理引擎，它对知识库中的信息进行分析，从而得到正确的决策。专家系统用户使用一些种类的用户接口将当前环境的具体内容提供给推理引擎，并且推理引擎使用

逻辑推理和模糊逻辑技术的组合，基于过去的经验做出结论。仍然以飓风为例，用户可能通知专家系统，4 级飓风已经接近海岸，风速为平均每小时 140 英里。推理系统将随后分析知识库中的信息，并且基于以前的知识做出撤离建议。

专家系统并非万无一失，它们的优劣完全取决于知识库中的数据和推理引擎实施的决策制订算法。不过，专家系统在紧迫的情况下有一个主要的优点，它们的决策不涉及情绪影响。专家系统可能在一些情况中扮演重要的角色，例如紧急事件、股票交易和其他有时因情绪因素妨碍做出合理决策的情况。由于这些原因，很多贷款机构现在采用专家系统来做出信用决策，而不是相信贷款主管所说的话："好，虽然 Jim 一直没有准时付账，但是他看起来是个相当不错的人。"

模糊逻辑

前面提到，推理引擎通常使用一种被称为模糊逻辑的技术。与利用"黑白"数据归类的代数方式或集合论的严格数学相比，这种技术的设计更接近于人类的思维模式。通过替换使用模糊的界限，模糊逻辑允许算法思考控制人类思维的"灰度梯度"。专家系统通过下列 4 个步骤或阶段使用模糊逻辑：模糊化、推理、合成以及逆模糊化。

以确定某个 Web 站点是否能够经受拒绝服务攻击的任务为例。传统的数学技术可能创建基本的规则，例如"如果每秒钟的连接超过 1000 次，那么就在遭受攻击"。另一方面，模糊逻辑可能定义一条模糊的界线：每秒钟的连接为 1000 次表示受攻击的几率为 80%，每秒钟的连接为 10000 次表示受攻击的几率为 95%，而每秒钟的连接为 100 次则表示受攻击的几率为 5%。对这些可能性的解释则留给后面的分析师来做。

20.4.2　神经网络

在神经网络中，计算单元链被用来尝试模仿人脑的生物学推理过程。在专家系统中，一系列规则被存储在知识库中，而在神经网络中则建立了互相插入和最终合计生成预期输出结果的计算决策长链。

需要记住的是，所设计出的神经系统要想达到实际的人类推理能力还有待时日。尽管如此，神经网络仍然在推动人工智能领域超越当前的状态，在这方面显示出了巨大的潜力。神经网络的优点包括线型、输入-输出映射和自适应性。在用于语音识别、脸部识别、天气预报以及关于意识与思考模型研究的神经网络实现中，这些优点十分明显。

典型的神经网络涉及很多层次的合计，每一层的合计都需要加权信息以反映在整个决策制定过程中计算的相对重要性。针对期待神经网络做出的每种决策，这些权值必须是被定制的。这可以在培训阶段实现，在这个阶段，网络被提供正确决策已知的输入信息。这个算法随后进行这些决策的逆向工作，从而为计算链中的每个节点确定正确的权值。这种活动被称为 Delta 规则或学习规则。通过使用 Delta 规则，神经网络就能够从经验中学习知识。

20.4.3　决策支持系统

决策支持系统(Decision Support System，DSS)是一种知识型应用，它分析业务数据并且以更容易做出业务决策的形式提供给用户。决策支持系统更多被视为信息型应用而不是操作型应用。DSS 常常被知识型员工(例如服务台人员或客户支持人员)和销售服务人员(例如电话推销员)所使用。这种

应用可能以图形方式提供信息，从而链接概念和内容并指导操作者。通常，DSS 得到了控制某个数据库的专家系统的支持。

20.4.4 安全性应用

专家系统和神经网络都在计算机安全领域具有很多应用。这些系统提供的一个主要优点是它们快速做出一致决策的能力。计算机安全性方面的一个主要问题是，系统管理员没有能力为了寻找异常而对大量的日志记录和审计跟踪数据进行一致的、彻底的分析。这似乎是天生的一对矛盾！

对于计算机安全领域来说，这种技术的一个成功应用是 Philip Porras 及其团队在 SRI 国际信息和计算科学系统设计实验室开发的下一代入侵检测专家系统(NIDES)。这个系统提供了一个推理引擎和知识库，它从网络的多种审计日志中提取信息，并且在单个用户的操作与他们的标准应用描述不同时向安全管理员发出通知。

20.5 本章小结

数据很快成为许多组织拥有的最有价值的资源。因此，信息安全从业人员了解保护数据自身以及有助于处理数据的应用程序和系统的必要性是十分重要的。在每个充分了解相关技术的组织中，都必须实现针对恶意代码、数据库脆弱性和系统/应用程序开发缺陷的防护。

恶意代码对象给组织的计算资源带来威胁。在非分布式环境中，这样的威胁包括病毒、逻辑炸弹、特洛伊木马和蠕虫。

此时，你一定认识到了为这些有价值的信息资源设置充分的访问控制和审计跟踪的重要性。数据库安全性是一个快速增长的领域，如果数据库在安全责任中扮演重要的角色，那么我们就应当花一些时间请教数据库管理员并学习相关课程、书籍和基础理论。这是一项颇有价值的投资。

最后，在系统和应用程序的开发过程中，为了确保这些过程的最终产品与安全环境中的操作兼容，可以使用多种控制手段。这些控制手段包括进程隔离、硬件划分抽象和服务等级协议。始终应当在所有开发项目的早期计划编制阶段引入安全性，并且在产品的设计、开发、部署和维护阶段持续进行监控。

20.6 考试要点

解释关系数据库管理系统(RDBMS)的基本体系结构。了解关系数据库的结构。能够解释表(关系)、行(记录/元组)和列(字段/属性)的功能。知道如何在表和各种键类型的角色间定义关系。描述由聚合和推理形成的数据库安全威胁。

知道各种存储器类型。解释主存储器、虚拟存储器、辅助存储器和虚拟存储器、随机访问存储器和顺序访问存储器、易失性存储器和非易失性存储器之间的区别。

解释专家系统和神经网络如何工作。专家系统包括两个主要的组件：包含一系列“if/then”规则的知识库；使用知识库信息得到其他数据的推理引擎。神经网络模拟人类大脑的运作，在有限的范围内通过安排一系列的分层计算来解决问题。神经网络需要针对特定的问题进行大量的训练，才

能够提供解决方案。

理解系统开发的模型。瀑布模型描述了一个连续的开发过程，导致最终产品的开发。如果发现错误，那么开发人员只能回退一个阶段。螺旋模型反复使用了几个瀑布模型，从而生成许多详细说明的和完全测试的原型。敏捷开发模型将重点放在客户的需求上，并快速开发新的功能，以迭代的方式满足这些需求。

描述软件开发成熟度模型。知道成熟度模型能帮助组织通过实施从临时的、混乱的过程到成熟的、有纪律的软件开发过程的进化路径，从而提高软件开发过程的成熟度和质量。能够描述 SW-CMM 和 IDEAL 模型。

理解变更和配置管理的重要性。知道变更控制的三个基本组件——请求控制、变更控制、发布控制，以及它们对安全的贡献。解释配置管理如何控制在组织中使用的软件版本。

理解测试的重要性。软件测试应当被设计为软件开发过程的一部分。软件测试应当作为改善设计、开发和产品化过程的管理工具。

20.7　书面实验室

1. 数据库表中的主键的主要目的是什么？
2. 什么是多实例？
3. 解释应用程序代码的静态和动态分析的区别？
4. 在瀑布模型中，当发现开发缺陷时允许回退多远？

20.8　复习题

1. 以下哪个选项不属于 DevOps 模型的三个组件之一？
   A. 信息安全
   B. 软件开发
   C. 质量保证
   D. IT 运维
2. Bob 正在开发一个应用软件，该应用软件有一个区域，用户可以在这里输入日期。他想要确保用户提供的值是准确的日期，以防止安全问题。下面哪一项技术应该是 Bob 要采用的？
   A. 多实例
   B. 输入验证
   C. 污染
   D. 筛选
3. 变更管理过程中的哪一部分允许开发人员优先考虑任务？
   A. 发布控制
   B. 配置控制
   C. 请求控制
   D. 变更审计

4. 下列哪一种故障失效管理方法将系统置于比较高层次的安全状态？

A. 故障开放

B. 故障减轻

C. 故障保护

D. 故障清除

5. 什么软件开发模型使用 7 阶段的方法和一个反馈回路，允许返回到上一步？

A. Boyce-Codd

B. 瀑布型模型

C. 螺旋型模型

D. 敏捷开发

6. 什么形式的访问控制主要与字段存储的数据有关？

A. 内容相关

B. 上下文相关

C. 语义完整性机制

D. 扰动

7. 以下哪一种键被用来执行数据库表之间的完整性引用？

A. 候选键

B. 主键

C. 外键

D. 超级键

8. Richard认为，一个数据库用户滥用其权限进行查询，并结合大量记录中的数据来获取公司整体业务的趋势信息。该数据库用户利用的过程是什么？

A. 推理

B. 污染

C. 多实例

D. 聚合

9. 什么样的数据库技术可以阻止“未授权用户通过正常无权访问信息的提示来确定信息级别”这样的事情发生？

A. 推理

B. 操纵

C. 多实例

D. 聚合

10. 以下哪一项不是敏捷开发的原则？

A. 通过早期和持续地交付来满足用户需求

B. 业务人员和开发者一起工作

C. 持续关注卓越的技术

D. 在其他需求之上有限地考虑安全

11. 什么样的信息被用来形成专家系统的决策过程的基础？

A. 一系列加权分层计算

B. 结合大量的人类专家的输入，根据过去的表现加权

C. 一系列被编入知识库的“if/then”规则

D. 一个模拟人类思维所使用的推理过程的生物决策过程

12. 在软件成熟度模型 SW-CMM 中，组织达到哪个阶段就可以使用定量的方法获得组织开发过程的详细理解？

A. 初始化

B. 可重复

C. 可定义

D. 可管理

13. 以下哪个选项可以作为应用程序和数据库之间的代理，以支持交互和简化程序员的工作？

A. SDLC

B. ODBC

C. DSS

D. 抽象

14. 在哪一种软件测试类型中，测试人员可以访问底层的源代码？

A. 静态测试

B. 动态测试

C. 跨站脚本测试

D. 黑盒测试

15. 哪个类型的图表提供了一个时间表，有助于计划、协调和跟踪项目任务的图形说明？

A. 甘特图

B. 维恩图

C. 柱状图

D. RERT

16. 当数据从一个较高分类级别到达一个较低分类级别时，数据库会发生以下哪类安全风险？

A. 聚合

B. 推理

C. 污染

D. 多实例

17. 什么数据库安全技术涉及创建两行或更多行记录，它们具有看起来相同的主键，这些主键为用户包含不同安全许可的不同数据？

A. 多实例

B. 单元抑制

C. 聚合

D. 视图

18. 以下哪一项不是变更管理过程的一部分？

A. 请求控制

B. 发布控制

C. 配置审计

D. 变更控制

19. 什么事务管理原则确保两个事务在操作相同的数据时不会相互干扰？

A. 原子性

B. 一致性

C. 隔离性

D. 持久性

20. Tom 建立了一个数据库表，这个表包含名字、电话号码、业务相关的客户 ID。这个表还包含 30 个客户的信息，请问这个表的度是多少？

A. 2

B. 3

C. 30

D. 未定义

第 21 章

恶意代码与应用攻击

本章中覆盖的 CISSP 考试大纲包含：

3. 安全工程
- E. 评估和缓解安全架构、设计和解决方案组件中的漏洞
- F. 评估和缓解基于 Web 系统(例如，XML、OWASP)的漏洞

8. 软件开发安全
- B. 在开发环境中实施安全控制
  - 软件环境中的安全
  - 安全弱点和源代码级别的漏洞(例如，缓冲区溢出、特权扩大、输入/输出验证)

在前面的章节中，你已经学习了很多能帮助安全从业者开发针对恶意个体进行保护的常规安全原则、策略处理机制。本章将深入探讨这个领域的管理员在日常工作中所面对的一些具体威胁。

这些内容不仅对于 CISSP 考试很关键，而且还是计算机安全专业人员为了有效开展工作而必须理解的一些最基本信息。本章首先介绍恶意代码对象带来的威胁，这些恶意代码对象包括病毒、蠕虫、逻辑炸弹和特洛伊木马。接着，我们将研究其他一些安全性应用，黑客会利用它们试图获取对系统的未授权访问或者阻止合法用户获得这样的访问。

21.1 恶意代码

恶意代码对象包括广泛的代码形式的计算机安全威胁，这些威胁利用各种网络、操作系统、软件和物理安全漏洞对计算机系统散播恶意载荷。某些恶意代码对象(例如，计算机病毒和特洛伊木马)依靠用户对计算机的不当使用在系统之间成功地传播。其他一些恶意代码对象(例如，蠕虫)则依靠自身的力量在脆弱的系统间快速传播。

所有计算机安全从业人员都必须熟悉由各种恶意代码带来的风险，这样才能够采取适当的对策来保护所关注的系统，以及在系统受到破坏时做出适当的响应。

21.1.1 恶意代码的来源

恶意代码源自哪里？在计算机安全的早期，恶意代码的编写者都是相当有经验(尽管误入歧途)的软件开发人员，他们会为自己精心构思的、富有创意的恶意代码技术感到骄傲。的确，他们揭露了流行软件包和操作系统中的安全漏洞，从而提高了人们对计算机安全性的意识，这确实起到了一点有用的作用。对于这种类型的代码编写者，可以在本章后面的“RTM 和网络蠕虫”补充内容中找到示例。

如今这个时代出现了一些脚本小子，他们并不理解安全漏洞内在的技术，但是从互联网上下载了随时可用的软件(或脚本程序)，并且利用这些软件对远程系统进行恶意攻击。这种趋势导致了一种新的病毒制造软件，它准许任何具有极少技术知识的人制造病毒并在互联网上传播。到现在为止，大量的病毒被反病毒机构证明属于这种类型。这些业余的恶意代码开发人员常常只是在尝试他们所下载的新工具，或者试图为一两个对手制造麻烦。遗憾的是，这些恶意代码有时会快速传播，并且通常会对互联网用户带来很多麻烦。

此外，脚本小子使用的工具可以免费提供给那些犯罪意图更加危险的人。事实上，国际组织犯罪集团在恶意软件扩散中发挥了作用。这些犯罪分子都在执法机制薄弱的国家，使用恶意软件窃取来自世界各地的钱财和人们的身份信息，特别是美国居民的。事实上，宙斯特洛伊木马被广泛认为是东欧有组织犯罪团伙的产品，试图感染尽可能多的系统，并记录击键信息和收获网上银行密码。宙斯木马爆发始于 2007 年，至今依然横行。这只是恶意软件发展趋势的一个例子。

21.1.2 病毒

计算机病毒可能是最早的令安全管理员苦恼的恶意代码形式。实际上，病毒如今相当普遍，病毒大爆发会引起大众媒体的关注，并且在一般的计算机用户中引起轻度恐慌。根据 Symantec 公司(一家主要的反病毒软件供应商)的报告，在 2010 年大约有 2 亿 8600 万种病毒的变形在全球网络中传播，并且这种趋势在继续。 一些消息来源表明，每一天大概有 200 000 个新的恶意软件样本出现在互联网上。每天都会有数十万的病毒变种对大意的计算机用户进行着攻击。许多病毒都带有恶意有效载荷，它们导致的破坏包括从屏幕上自始至终显示亵渎信息，直至导致本地硬盘上的所有存储数据被完全破坏。

与生物病毒一样，计算机病毒具有两个主要的功能：传播和破坏。那些制造病毒的卑劣家伙精心地设计代码以创新的方法执行这些功能，他们希望利用这些方法使病毒可以躲避检查并绕过日益完善的反病毒技术。可以这样说，在病毒编写者和反病毒专家之间正在展开竞赛，每一方都希望开发出的技术高出对手一筹。传播功能定义了病毒如何在系统之间扩散，从而感染激发每一台计算机。病毒的有效载荷通过执行病毒作者预谋的恶意行为来释放它的破坏力。这些都能产生任何针对系统或数据的机密性、完整性或可用性的负面影响。

1. 病毒传播技术

根据定义，病毒必须包含能够使其在系统之间进行传播的技术，有时会借助于无疑心的计算机用户通过交换磁盘、共享网络资源、发送电子邮件或其他手段试图共享数据的活动。一旦病毒到达新的系统，它们会使用某种传播技术来感染新的受害者以及扩展其触及范围。接下来，我们将介绍

4 种常见的传播技术：主引导记录感染、文件感染、宏感染和文件注入。

主引导记录病毒　主引导记录病毒(Master Boot Record，MBR)是已知的最早的病毒感染形式。这些病毒攻击 MBR——可启动介质(例如，硬盘、软盘或 CD/DVD)上计算机用于在启动过程中加载操作系统的部分。由于 MBR 非常小(通常只有 512 字节)，因此它不能包含实现病毒传播和破坏功能所需的所有代码。为了避开空间的限制，MBR 病毒将主要的代码存储在存储介质的其他部分。在系统读取受感染的 MBR 时，病毒会引导系统读取并且执行在另一个地方存储的代码，从而将全部的病毒加载到内存中，并且可能触发病毒有效载荷的传播。

引导扇区和主引导记录

你经常看到，“引导扇区”和“主引导记录”被用于描述存储设备上用来加载操作系统和攻击这个加载过程的病毒类型的部分，这在技术上是不正确的。MBR 是一个单独的磁盘扇区，通常是在启动过程的初始阶段读取的介质的第一个扇区。MBR 决定介质的哪个部分包含操作系统，并且随后指导系统读取对应部分的引导扇区，以便加载操作系统。

病毒可能攻击 MBR 和引导扇区，结果实质上类似。MBR 病毒将系统重定向到被感染的引导扇区，在从合法引导扇区加载操作系统之前将病毒加载到内存中。引导扇区病毒实际上感染合法的引导扇区，并且在操作系统加载过程中被加载到内存中。

大多数MBR病毒在系统之间通过用户不经意地共享被感染的介质进行传播。如果在启动过程中被感染的介质在驱动器中，那么目标系统就会读取被感染的MBR、将病毒加载到内存中、感染目标系统硬盘的MBR，并且还会感染其他计算机。

文件程序感染病毒　许多病毒感染不同类型的可执行文件，并且在操作系统试图执行这些文件时被触发。对于基于 Windows 的系统来说，可执行文件以扩展名.exe 和.com 为后缀。文件程序感染病毒的传播程序可能只是对可执行程序进行了少许改动，从而植入了病毒需要复制并毁坏系统的技术。在某些情况下，病毒可能实际上用被感染的版本替换了整个文件。标准的文件程序感染病毒没有使用障眼法技术，例如隐形或加密(参见本章稍后的“病毒技术”部分)，通过比较感染前后的文件特性(如大小和修改日期)或散列值，常常可以很容易地检查出这种病毒。本章后面的“反病毒机制”部分会介绍与这些技术相关的技术细节。

文件程序感染病毒的一个变种是同伴病毒。这种病毒是自包含的可执行文件，利用与合法的操作系统文件类似但又稍有不同的文件名来躲避检查。同伴病毒依靠基于 Windows 的操作系统在执行程序文件时关联在命令上的默认文件扩展名(.com、.exe 和.bat，并且按照这个顺序)进行操作。例如，如果在硬盘上有一个名为 game.exe 的程序,那么同伴病毒可能会使用名字 game. com。如果你随后打开一个命令行工具并简单地键入“game”，那么操作系统将执行这个病毒文件 game.com，而不是实际要执行的文件 game.exe。对于在命令行工具下执行文件时要避免快捷方式并且使用具体的文件名来说，这的确是一个很好的理由。

宏病毒　许多常用的软件应用程序为了协助重复任务的自动执行而实现了某些脚本功能。这些功能常常使用简单却有效的编程语言，例如 Visual Basic for Applications(VBA)。虽然宏的确为计算机用户提供了巨大的提高生产率的机会，但是它们也将系统暴露给了另一种感染手段——宏病毒。

宏病毒最早出现在 20 世纪 90 年代中期，它采用拙劣的技术感染流行的 Microsoft Word 环境中生成的文档。虽然宏病毒相对简单，但是由于反病毒机构没有预见到，反病毒软件没有提供对它们的任何防护，因此这些病毒得到了快速传播。宏病毒很快就变得越来越普遍，供应商匆忙地修改他

们的反病毒平台，使之能够对应用文档进行宏病毒扫描。1999 年，Melissa 病毒通过 Word 文档传播，利用 Microsoft Outlook 中的安全漏洞进行复制。在 2000 年初，臭名昭著的 I Love You 病毒很快步其后尘，也利用相似的漏洞进行传播。

警告：

因为很容易采用现代生产性应用程序使用的脚本语言(例如，VBA)编写代码，所以宏病毒会大量传播。

在 20 世纪后期出现了一系列宏病毒之后，生产力软件开发人员对宏开发环境进行了重大改变，限制了不受信任的宏在没有明确用户许可的情况下运行的能力。结果就是导致宏病毒的数量急剧减少。

服务注入病毒 最近爆发的恶意代码使用另一种技术感染系统和逃脱检测——将自己注入到操作系统的可信运行进程中，如 svchost.exe、winlogin.exe 和 explorer.exe。通过成功地破坏这些受信进程，恶意代码能够绕过主机上运行的任何防病毒软件的检测。保护系统免受服务注入的最好技术之一是确保允许浏览 Web 内容的所有软件(如浏览器、媒体播放器、帮助应用程序)接收当前的安全补丁。

2. 容易受到病毒攻击的平台

如同大多数宏病毒感染那些运行流行的 Microsoft Office 应用程序套件的系统一样，大多数计算机病毒被设计成破坏在世界上最流行的操作系统 Microsoft Windows 上运行的活动。据估计，今天世界上只有不到百分之一的病毒被设计为影响其他操作系统，例如 Unix 和 Mac OS。

首先，实际上已经没有单一的“Unix”操作系统。相反，一系列很相似的操作系统以类似的方式实现了与 Unix 相同的功能，并且由大量的开发人员独立设计。大规模企业开发的软件在与无数免费的由公众随意开发的 Linux 操作系统一直在进行竞争。Unix 版本的严格编号以及它们在完全不同的内核(操作系统的核心代码)上进行开发的事实，使得难以编写病毒，从而对 Unix 系统产生大范围的影响。

也就是说，Macintosh 和 Unix 用户不应该安于现状。只有几个病毒对他们的系统带来威胁，这并不意味着其中的病毒不能对他们的系统随时产生影响。任何人都有责任确保计算机系统的安全性，并应该实施适当的反病毒机制以确保其资源的持续安全。

3. 反病毒机制

今天，几乎每台工作中的台式计算机都运行着某种反病毒软件包。流行的计算机反病毒软件包括微软的 Security Essentials、McAfee 的 VirusScan 和 Norton 的 AntiVims，但是市场上还存在其他很多产品能够提供从单一系统到整个企业的保护；有的被设计用于防范指定的常见病毒威胁类型，例如入站电子邮件。

这些软件包中的大多数都使用一种被称为特征型检测的方法来识别系统中潜在的病毒感染。实质上，反病毒软件包维护着一个极大的数据库，这个数据库中包含所有已知病毒的指示特征。依赖于反病毒包和配置设置，反病毒软件包能够定期扫描存储介质，对所有包含与标准匹配的数据的任何文件进行检查。一旦检测到任何问题，反病毒软件包就会采取下列措施中的某种措施：

- 如果软件可以消除这些病毒，那么就对这些被感染的文件进行杀毒，并且将系统还原到安全的状态。

- 如果软件识别了病毒但是不知道如何为文件杀毒，那么可能会隔离这个文件，直至用户或管理员可以人工进行分析。
- 如果安全设置/策略没有提供隔离或者文件超出了预定义的危险阈值，那么反病毒软件包可能删除这些被感染的文件，以试图保持系统的完整性。

使用特征型反病毒软件包时，必须记住的是，软件包的有效性只依赖于基础性的病毒定义文件的有效性。如果不经常更新病毒定义(通常需要每年订购的费用)，那么反病毒软件将不能检测新出现的病毒。互联网上每年新出现成千上万个病毒，过期的病毒定义文件将很快使反病毒防护失效。

许多防病毒软件包还使用基于启发式的机制来检测潜在的恶意软件感染。这些方法分析软件的行为，寻找病毒活动的迹象，例如试图提高特权级别、掩盖电子踪迹，以及更改不相关的或操作系统的文件。

大多数现代反病毒软件产品能够检测、删除和清除系统上的大量不同类型的恶意代码。换句话说，反病毒解决方案不仅仅限于防范病毒。这些工具往往能够提供针对蠕虫、特洛伊木马、逻辑炸弹以及其他电子邮件或 Web 承载代码的防护。在怀疑互联网上存在新的恶意代码时，最佳的做法是联系反病毒软件供应商并咨询当前针对新威胁的防护状态。不要坐等下一次定期或自动特征字典更新。此外，不要相信第三方关于反病毒解决方案所提供保护状态的言论。始终牢记与反病毒软件供应商直接联系。大多数负责的反病毒软件供应商都会在确定新的重大威胁的第一时间向客户发出警报，因此客户也一定要保证关注这样的警报。

其他安全软件包(例如，流行的 Tripwire 数据完整性保证软件包)也提供了辅助的反病毒功能。Tripwire 被设计用于警示管理员发生未授权的文件修改，常常被用来检测对 Web 服务器的破坏和类似的攻击。不过，如果关键的系统可执行文件(如 command.com)被突然修改，那么 Tripwire 也可能提供某些病毒感染的警告。这些系统通过维护系统所有存储文件的散列值的数据库进行工作(对用于创建这些散列值的散列函数的详细讨论，可以参看第 6 章“密码学与对称加密算法”)。通过比较这些归档的散列值与当前计算的文件散列值，就可以检测出两个时间段之间所有被修改的文件。在最基本的层面上，散列是用来汇总文件内容的数字。只要文件保持不变，散列将保持不变。如果文件被修改，即使是轻微的，散列也将发生明显的变化，表明文件已被修改。除非该操作似乎可解释，例如，如果发生在安装新软件、操作系统补丁程序的应用或类似的更改之后，在可执行文件中的突然更改可能是恶意软件感染的迹象。

4. 病毒技术

当病毒检测和消除技术得到提高以便战胜恶意开发人员设计的新威胁时，新类型的病毒被设计用于挫败使用这些技术的系统。接下来我们将分析病毒的 4 种具体类型，它们使用卑鄙的技术企图逃避检测，这 4 种类型是：复合病毒、隐形病毒、多态病毒和加密病毒。

复合病毒　复合病毒使用多种传播技术试图渗透只防御其中一种方法的系统。例如，在 1993 年发现的 Marzia 病毒通过为每个文件添加 2048 个字节的恶意代码来感染关键的 COM 和 EXE 文件，最明显的就是系统文件 command.com。这个特征说明它是一种文件程序感染病毒。此外，在 Marzia 病毒感染系统两个小时后，它会向系统的主引导记录写入恶意代码，这说明它也是一种引导扇区病毒。

隐形病毒　隐形病毒通过对操作系统的实际篡改来欺骗反病毒软件包认为所有事情都工作正常，从而将自己隐藏起来。例如，隐形的引导扇区病毒可能利用恶意代码覆盖系统的主引导记录，随后还通过修改操作系统的文件访问功能来覆盖自身痕迹。当反病毒软件包请求 MBR 的副本时，

被修改的操作系统代码提供它所期望看到的版本：也就是没有任何病毒特征的未被感染的 MBR 版本。然而，系统启动时会读取被感染的 MBR，并且将病毒加载到内存中。

多态病毒 在系统间传输时，多态病毒实际上会修改自己的代码。这种病毒的传播和破坏技术保持完全相同，但是每次感染新的系统时病毒的特征略有不同。多态病毒制造者的希望就是，通过连续改变特征使得特征型反病毒软件包失效。然而，反病毒软件供应商识破了许多多态病毒技术的代码，因此目前使用的反病毒软件版本都能够检测出已知的多态病毒。剩下的唯一担心是，为了阻止多态病毒的攻击而生成必要的特征文件，这会花费供应商较长的时间，因此可能导致多态病毒在更长时间范围内在互联网上肆无忌惮地运行。

加密病毒 加密病毒使用密码术(参看第 6 章的内容)来躲避检测。在加密病毒的外部表现中，它们实际上很像多态病毒，每个被感染的系统都有不同特征的病毒。然而，加密病毒不是通过改变代码来生成这些修改过的特征，而是修改在磁盘上的存储方式。加密病毒使用一个很短的、被称为病毒解密程序的代码段，这个代码段包含必要的密码学信息，用于对存储在磁盘上其他地方的主病毒代码进行加载和解密。每个感染过程都使用不同的密钥，这使得主代码在每个系统上都呈现出完全不同的样子。不过，病毒解密程序往往包含指示特征，因此加密病毒很容易被最新的反病毒软件包识破。

5. 骗局

如果缺少对病毒骗局(hoax)导致的损害和资源浪费的讨论，那么对病毒的研究就不算完整。几乎每个电子邮件用户都曾经收到过朋友转发来的邮件信息或者有关 Internet 存在最新病毒威胁的警告。这个传闻中的“病毒”总是那些目前尚未发作但是最具破坏性的病毒，没有任何反病毒软件包能够检测和/或删除它们。有关这种骗局的一个著名示例是欢乐时光(Good Times)病毒警告，它最早在 1994 年出现在互联网上，直到今天依然在传播。

如果想获得关于这个主题的更多信息，myth-tracking 网站 Snopes 保存了一份病毒骗局列表，网址如下：http://www.snopes.com/computer/virus/virus.asp。

21.1.3 逻辑炸弹

你曾经在第 20 章“软件开发安全”中学过，逻辑炸弹是感染系统并且在达到一个或多个满足的逻辑条件(例如，时间、程序启动、Web 站点登录等)前保持休眠状态的恶意代码对象。大多数逻辑炸弹被软件开发人员编入用户定制的应用程序中，这些开发人员的目的是在被突然解雇时破坏公司的工作。第 20 章已经介绍了几个这类逻辑炸弹的例子。

然而，必须记住的是，像所有恶意代码对象一样，逻辑炸弹具有许多形式和大小。事实上，许多病毒和特洛伊木马都包含一个逻辑炸弹组件。著名的米开朗其罗病毒在 1991 年被发现时曾导致介质混乱，它就是由其包含的逻辑炸弹触发启动的。这个病毒通过共享被感染的软盘来感染系统的主引导记录，并且随后将自己隐藏起来，直到 3 月 6 日(即著名的意大利艺术家米开朗其罗的生日)这一天启动，从而重新格式化被感染系统的硬盘并且破坏硬盘包含的所有数据。

21.1.4 特洛伊木马

系统管理员经常警告计算机用户，不要从互联网上下载并安装软件，除非能够绝对保证来源可

靠。事实上，许多公司严格地禁止安装任何非 IT 部门预筛选的软件，这样的策略能够最小化组织的网络被特洛伊木马破坏的风险。特洛伊木马是一种软件程序，这种软件程序表面上友善，但是实质上承载恶意有效载荷，具有对系统或网络的潜在破坏能力。

不同的特洛伊木马在功能上区别很大。一些木马将破坏系统上存储的所有数据，试图在尽可能短的时间段内产生大规模的破坏。一些木马则可能是无害的。例如，在 2002 年中出现在互联网上的一系列木马，这些木马声称为 PC 用户提供在计算机上运行为 Microsoft Xbox 游戏系统设计的游戏的能力。当用户运行这个程序时，它什么也不做。不过，它还向 Windows 注册表插入一个值，导致每次计算机启动后都打开指定的 Web 页面。该特洛伊木马的制作者们希望通过 Xbox 木马接收到大量的对其 Web 页面的浏览，从而得到广告收入。不过令他们感到遗憾的是，反病毒专家们很快就发现了他们的真实企图，并且相关网站也被关闭了。

最近对安全圈造成重大影响的一类木马是流氓杀毒软件。这类软件欺骗用户安装它，声称是一个防病毒包，通常伪装成一个弹出广告，并模仿成安全警告的外观和感觉。一旦用户安装软件，就会窃取个人信息或提示用户付款以“更新”流氓杀毒软件。“更新”只是禁用木马！

另一个变种——勒索软件，是特别阴险的。勒索软件感染目标计算机，然后使用加密技术来加密存储在系统上的文档、电子表格和其他文件，并使用只有恶意软件创建者知道的密钥。接下来用户无法访问他们的文件，并收到一条不祥的弹出消息警告，文件将被永久删除，除非在短时间内支付赎金。用户然后经常支付这个赎金来重新获得对他们文件的访问。最著名的勒索软件种类之一是 Cryptolocker。

真实场景

僵尸网络

数年以前，本书的一位作者访问了一家组织，这家公司怀疑自己存在安全问题，但是却不具备诊断或解决问题的专业知识。安全问题的主要症状是网络速度缓慢。我们在执行基本的测试时发现，公司网络中的所有系统都没有运行基本的反病毒软件，并且某些系统已经感染了特洛伊木马。

是什么原因导致网络速度缓慢呢？是的，特洛伊木马使所有被感染的系统都成为某个僵尸网络(botnet)的成员，僵尸网络由 Internet 上被僵尸牧人(botmaster)控制的众多计算机(有时是数千台)组成。

这个特定僵尸网络的僵尸牧人使组织网络中的系统参与针对某个 Web 站点(由于某个原因或其他原因，僵尸牧人不喜欢相应的站点)的拒绝服务攻击。僵尸牧人指示僵尸网络中的所有系统都反复检索相同的 Web 页面，从而使受攻击的 Web 站点由于负荷过高导致出现故障。组织网络中存在大约 30 个被感染的系统，僵尸网络的攻击几乎占用了所有带宽！

解决这个问题非常简单。我们在所有系统中都安装了反病毒软件并删除了特洛伊木马。进行这些操作之后，一切都恢复正常了。

21.1.5　蠕虫

蠕虫给网络安全带来了空前的风险。它们包含的破坏潜力与其他恶意代码对象相同，并且还具有额外的手段，也就是不需要任何人为干预就可以传播自己。

互联网蠕虫是互联网上发生的首例主要的计算机安全事件。从那时起，成百上千个新的蠕虫(带有成千上万个变种)开始在互联网上散播它们的破坏力量。

1. Code Red 蠕虫

在 2001 年夏天，当 Code Red 蠕虫在未安装补丁程序的 Microsoft Internet Information Server(IIS) Web 服务器之间快速传播时，受到了媒体的极大关注。Code Red 在被其渗透的系统中执行下列三种恶意动作：

- 随机选择成百上千的 IP 地址，并且随后探测这些主机，查看这些主机是否运行存在漏洞的 IIS 版本。任何被找出的系统都很快被破坏。因为每个被感染的主机继续寻找很多新目标，Code Red 的破坏范围也就随之显著扩大了。
- 破坏本地 Web 服务器上的 HTML 页面，并且将正常的内容替换为如下所示的文本：

```
Welcome to http: //www.worm.com!
HackedBy Chinese!
```

- 向系统植入一个逻辑炸弹，这个逻辑炸弹将向 IP 地址 198.137.240.91 发起拒绝服务攻击，该地址在当时属于驻留白宫主页的 Web 网站服务器。反应敏捷的政府 Web 站点管理员在实际攻击发生之前便改变了白宫的 IP 地址。

互联网蠕虫、Code Red 及其许多变种的破坏力量给现代互联网带来了极大的风险。系统管理员必须确保他们为连接 Internet 的系统使用了软件供应商所发布的适当的安全补丁。针对 Code Red 利用的 IIS 漏洞的安全补丁在蠕虫攻击互联网之前一个月左右就已由 Microsoft 发布，如果安全管理员迅速地安装了这个补丁，那么 Code Red 将会是一种失败的病毒。

RTM 与互联网蠕虫

1988 年 11 月，一位年轻的名叫 Robert Tappan Morris 的计算机专业学生，仅仅利用几行计算机代码就使得刚刚起步的互联网遭受重创。他宣称由他作为实验制造的一个恶意蠕虫被意外地释放到了互联网上，很快这个蠕虫就传播并破坏了大量的系统。

如下所示，这个蠕虫通过利用 Unix 操作系统 4 个特殊的安全漏洞进行传播：

Sendmail 调试模式 当时流行的 Sendmail 软件包的最新版本被用于在互联网上对电子邮件进行路由，但是它却包含一个安全漏洞。这个漏洞准许蠕虫通过向远程系统上的 Sendmail 程序发送特殊的、包含蠕虫代码的破坏性电子邮件来传播自己。远程系统在处理邮件时就会被感染。

密码攻击 这个蠕虫还使用了字典攻击，通过使用一个有效系统用户的用户名和密码来试图获得对远程系统的访问权限(本章后面部分将介绍字典攻击的更多内容)。

finger 漏洞 流行的互联网实用程序 finger 准许用户决定谁可以登录到远程系统。当时流行的 finger 软件的最新版本包含一个缓冲区溢出漏洞，这个漏洞使得蠕虫能够进行传播(本章稍后部分将对缓冲区溢出进行详细讨论)。自此，finger 程序就从大多数连接互联网的系统上被删除了。

信任关系 在感染系统后，这个蠕虫分析了网络中该系统与其他系统之间存在的信任关系，并且试图通过可信路径传播至这些系统。

多分支的方式使得互联网蠕虫变得极为危险。幸运的是，计算机安全组织很快组织了一个研究小组，他们解除了互联网蠕虫的危险，并且为受影响的系统开发了补丁程序。由于互联网蠕虫存在一些低效的代码，进而限制了自身的传播速度，因此研究小组的工作变得容易了许多。

由于法律执行机构和法院系统在处理计算机犯罪方面缺少经验，因此 Morris 只为其犯罪行为受到轻微控诉。根据 1986 年的计算机违法犯罪法案(Computer Fraud and Abuse Act)，他被判三年缓刑、400 小时的社区服务和一万美元的罚款。具有讽刺意味的是，在事件发生时，Morris 的父亲 Robert Morris 是国家安全机构(NSA)下属国家计算机安全中心(NCSC)的主管。

2. 震网病毒

在 2010 年年中，名为震网(Stuxnet)的蠕虫在互联网上出现。这种高度复杂的蠕虫使用各种高级技术来传播，包括多个以前未记录的漏洞。震网病毒使用以下传播技术：

- 在本地网络上搜索未受保护的管理共享系统
- 利用零日漏洞攻击 Windows 服务器上的服务和打印机后台处理程序
- 使用默认的数据库密码连接系统
- 使用共享的 USB 设备进行传播

震网病毒在从一个系统传播到另一个系统的过程中，系统本身不受伤害，它实际上是在寻找一种特殊类型的系统——使用由西门子制造的控制器系统，据称是用于生产核武器材料的系统。当发现这样的系统时，它会执行一系列旨在摧毁连接到西门子控制器离心机的动作。

震网病毒似乎从中东开始传播，特别是位于伊朗的系统。据称，它是由西方国家设计的，意图破坏伊朗核武器计划。根据《纽约时报》的一个故事，以色列的一个设施包含用于测试蠕虫的设备。故事说：“以色列已经开发了与伊朗几乎完全相同的核能离心机”，并继续说：“那里的运行以及在美国的相关努力都是——该病毒被设计为美国和以色列项目的线索，意图破坏伊朗核方案”。

如果这些指控是真实的，震网病毒标志着恶意代码世界里的两个主要演变：使用蠕虫对设施造成严重的物理损坏，以及在国家之间的战争中使用恶意代码。

21.1.6　间谍软件与广告软件

在正常使用计算机时，我们还会遇到其他两种不希望的软件干预类型。间谍软件会监控你的动作，并且向暗中监视你活动的远程系统传送重要的细节。例如，间谍软件可能等待你登入某个银行站点，随后将你的用户名和密码传送给间谍软件的创作者。此外，间谍软件也可能等待你在某个电子商务站点输入信用卡号，然后将卡号传送给在黑市进行贩卖交易的骗子。

广告软件在形式上与间谍软件极为相似，只是具有不同的目的。广告软件使用多种技术在被感染的计算机上显示广告。最简单的广告软件形式会在你连接 Web 时在屏幕上显示弹出式广告。更恶毒的广告软件版本可能会监控你的购物行为并将你重定向至竞争者的 Web 站点。

注意：

广告软件和恶意软件的作者通常利用流行的互联网工具的第三方插件(如 Web 浏览器)来传播其恶意内容。他们发现插件已经具有强大的用户基础，这些插件被授予权限在他们的浏览器内运行和/或获取他们的信息。然后他们用原始插件代码补充恶意代码，这些代码散布恶意软件、窃取信息或执行其他不必要的活动。

21.1.7 对策

针对恶意代码的主要防护手段是使用反病毒过滤软件。这些软件包主要是特征型系统，它们被设计用于检测在系统中运行的已知病毒。如下所示，至少在三个关键区域考虑实现反病毒过滤是非常明智的。

客户端系统：网络中的每个工作站都应当通过更新的反病毒软件在本地文件系统中查找恶意代码。

服务器系统：服务器应当具有类似的防护。因为公用服务器上的一个病毒会迅速在整个网络内传播，所以保护服务器系统比保护客户端系统更为重要。

内容过滤器：目前的大多数病毒都通过互联网传播。继续在网络上根据恶意代码的特征，对入站和出站电子邮件以及 Web 流量进行内容过滤，是非常明智的做法。

注意：

利用当前的反病毒软件，往往能够在发现恶意代码后的数个小时内执行去除操作。去除操作会删除恶意代码，但是并不修复恶意代码导致的损坏。往往能够在发现恶意代码数天之后使用清除功能。清除操作不仅能够删除恶意代码，而且还能够修复恶意代码导致的损坏。

警告：

需要记住的是，大多数反病毒过滤器都是特征型软件。因此，反病毒过滤软件只有在病毒定义文件是最新时才能有效运作。定期更新这些文件至关重要，尤其在互联网上出现新的高风险恶意代码特征时更是如此。

特征型过滤器依赖于软件开发人员提供的对已知病毒的描述。因此，任何指定病毒从第一次现身网络到更新过滤器之间存在一定的时间周期。目前，有两种常用的解决方案能够解决这个问题：

- 使用完整性检查软件(例如 Tripwire，在 www.tripwire.org 站点上有可用的开放源码)扫描文件系统中意外的更改并定期报告。
- 应当严格地维护和实施访问控制，从而限制恶意代码破坏数据和在网络上传播的能力。

此外，下列三种额外的技术能够专门防止系统受到活动内容内嵌的恶意代码的感染：

- Java 的沙箱技术为 applet 提供了一个隔离的环境，在这个环境中，applet 不需要访问关键的系统资源就能够安全地运行。
- ActiveX 控件签名技术利用数字签名系统来确保代码来自可信源。最终用户需要确定通过身份认证的来源是否可信。
- 操作系统级别的应用程序白名单要求管理员指定批准的应用程序。操作系统使用此列表，仅允许已知的良好应用程序运行。

要对数字签名进行深入理解，请查看第 7 章“PKI 和密码学应用”中的内容。

许多形式的恶意代码利用零日漏洞——被黑客发现的安全漏洞，这些漏洞尚未得到彻底解决。系统受到这些漏洞影响的两个主要原因是：

- 在发现新型恶意代码和发布补丁及更新病毒特征库之间的时间拖延
- 在系统管理期间应用更新缓慢

零日漏洞的存在，使得必须在组织中拥有强大的补丁管理程序，确保应用及时更新。此外，可

能希望使用漏洞扫描程序定期扫描系统来查找已知的安全问题。

21.2　密码攻击

攻击者用于获得对系统的非法访问的最简单技术之一是：获悉已授权系统用户的用户名和密码。一旦作为正常用户获得访问权限，那么攻击者就会在系统中具有立足之地。此时，攻击者可以使用其他技术(包括 rootkit 软件包)自动获取增强级别的系统访问权限(参看本章稍后的“权限提升和 rootkit”部分)。攻击者还可能将受到危害的系统作为跳板，从而攻击相同网络中其他更加诱人的目标。

下面几节分析了攻击者用于获悉合法用户密码并访问系统的三种方法：密码猜测攻击、字典攻击和社会工程学攻击。很多这些类型的攻击依赖于脆弱的密码存储机制。例如，许多 Unix 操作系统在/etc/passwd 文件中存储用户密码的加密版本。

21.2.1　密码猜测攻击

在这种最基本的密码攻击类型中，攻击者只是试图猜测用户的密码。无论进行了多少次安全性教育，用户还是常常使用极为脆弱的密码。如果攻击者能够获得授权系统用户的列表，那么他们常常能够快速找出正确的用户名(在大多数网络中，用户名包含用户名字的第一个字母，后面紧跟着他们的姓氏部分)。利用这些信息，攻击者就能够开始对用户的密码进行某些猜测。最常用的用户密码形式是用户姓氏、名字或用户名。例如，为了容易记忆，用户 mchapple 可能会使用脆弱的密码 elppahcm。遗憾的是，这个密码也很容易被猜到。如果猜测企图失败，那么攻击者会转向互联网上最常见密码的普通列表。“最常见的密码”部分列出了其中一些密码。

最常见的密码

攻击者常常使用互联网分发常被使用的用户密码列表，这些密码通过系统被攻破时收集到的数据建立。列表中的很多内容并不使人惊讶。在互联网上检索到的攻击者列表包含 815 个密码，下面列出了其中一小部分：

Password
Secret
sex
money
love
computer
football
hello
morning
Ibm
work
office

online
terminal
Internet
除了这些常见的单词外，密码列表里包含超过 300 个第一名字，其中 70%是女性的名字。

最后，对某人稍有了解就可以为其密码提供极佳的线索。很多人使用配偶、孩子、宠物、亲友或喜欢的演员的名字作为密码。常见的密码还包括生日、周年纪念日、社会保险号、电话号码和(不管你是否相信)ATM PIN。

21.2.2 字典攻击

前面曾经提到过，许多 Unix 系统在所有系统用户可访问的/etc/passwd 文件中存储用户密码的加密版本。为了提供某些安全性级别，这个文件并不包含实际的用户密码；但包含了通过单向加密函数获得的加密值(参看第 7 章对加密函数的讨论)。当用户试图登入系统时，访问验证程序使用相同的加密函数加密用户输入的密码，然后与/etc/passwd 文件中存储的实际密码进行比较。如果这两个值匹配，那么用户就被准许访问系统。

密码攻击者使用自动化工具(例如，John the Ripper)运行自动的字典攻击，字典攻击利用了这种机制的一个简单漏洞。攻击者采用一个包含成千上万词汇的大型字典文件，然后针对这些词汇运行加密函数，以获得加密的等值效果。接着，John the Ripper 程序在密码文件中查找与加密字典相匹配的加密值。查找到某个匹配时，John the Ripper 程序会报告用户名和密码(明文形式)，攻击者便获得了对系统的访问权限。

密码破解

JohntheRipper 是一个密码破解程序。在互联网上有许多其他可用的攻击技术，这些包括 Cain & Abel、Ophcrack、Brutus、THC Hydra、L0phtCrack、Pwdump 和 RainbowCrack。每个工具都有专门的不同的操作系统和密码类型。

这听起来像是一种简单的安全机制，并且安全教育将会防止用户使用那些容易被破解程序猜到的密码，但是这种工具对于攻击实际的系统来说惊人有效。随着新版破解工具的发布，更多的高级特性被用于战胜用户常用的技术以及战胜密码复杂度规则。下面列出了其中一些高级特性：

- 重新排列字典词汇的字母
- 为字典词汇附加数字
- 将字典词汇中出现的每个字母 O 都替换为数字 0(或用数字 1 替换字母 L)
- 采用某些形式组合两个字典词汇

21.2.3 社会工程学攻击

社会工程学是攻击者用于获得系统访问权限的最有效工具之一。在其最基本的形式中，社会工程学攻击包括简单地通过电话询问用户的密码，就像技术支持人员或其他权威机构声明他们立即需要这些信息一样。幸运的是，大多数当代计算机用户都已意识到这些花招，通过简单询问用户密码的有效性如今已经有所降低。相反，这些攻击依赖于网络钓鱼电子邮件，提示用户使用他们真实的

用户名和口令登录到一个假冒的网站，然后攻击者捕获这些用户信息，并用于登录实际的网站。网络钓鱼往往针对金融服务网站，用户凭据可以用来快速转移现金。除了欺骗用户放弃他们的密码，网络钓鱼攻击通常用来让用户安装恶意软件或提供其他敏感的个人信息。

虽然用户变得越来越精明，但对于密码(通常针对网络)的安全性来说，社会工程学仍然是个严重的威胁。攻击者常常可以通过与计算机用户、办公室中的饶舌者和行政管理人员的“闲谈”获得敏感的个人信息。在进行密码猜测攻击时，这些信息可以提供极好的攻击素材。此外，攻击者有时可以获得敏感的网络拓扑图或配置数据，在计划对组织进行其他类型的电子攻击时，这些信息也非常有用。

21.2.4　对策

所有安全措施的基石是教育。安全人员应该经常提醒用户选择安全密码进行保密的重要性。用户应该在他们首次加入组织时接受培训，并且应当定期接受最新的培训，即使这种培训只是来自管理员提醒他们相关威胁的电子邮件。

为用户提供建立安全密码所需要的知识，告诉他们攻击者在猜测密码时所使用的技术，并且为用户提供一些有关如何建立强密码的建议。最有效的密码技术之一是使用某种记忆手段，如设想一个容易记忆的句子并利用每个词的首字母建立密码。例如，将句子“My son Richard likes to eat 4 pies”变为密码 MsRlte4P，这是一个极难破解的密码。你可能也希望考虑为用户提供一个安全工具，允许存储这些强密码。Password Safe 和 LastPass 是两个常见的例子。这些工具允许用户为他们使用的每个服务创建独特的、强大的密码，而不承担他们所有的负担。

提示：

防止基于密码的攻击的最好方法之一是采用其他认证技术作为密码技术的补充。这种方法被称为多因素认证，已在第 13 章讨论。

由过分热心的管理员导致的一种最常见错误是建立一系列强密码，并且将它们分发给用户(用户随后会被禁止改变为他们分发的密码)。乍一看，这是一个听起来十分安全的策略。然而，用户在收到像 lmfOA8flt 这样的密码时，他们将要做的第一件事是将密码写在便签上并将其粘贴在计算机键盘的下面。这下可好，安全保护彻底破产了！

如果网络包括使用/etc/passwd 文件的 Unix 操作系统，那么请考虑使用其他的访问验证机制来增强安全性。在很多版本的 Unix 和 Linux 上都可用的一种流行技术是使用影子密码文件/etc/shadow。这个文件包含每个用户的实际加密密码，但是除了管理员外，任何人都不能访问这个文件。可公共访问的文件/etc/passwd 只是包含用户名的列表，它并不包含发起字典攻击所需的必要数据。

21.3　应用程序攻击

在第 20 章中，学习了在开发操作系统和应用程序时使用可靠的软件工程过程的重要性。在下面几节，你将会简要学习一些特殊的技术，攻击者可以使用这些技术来利用由于编码过程疏忽大意而留下的漏洞。

21.3.1 缓冲区溢出

缓冲区溢出漏洞存在于当开发人员不正确地验证用户的输入，以确保以适当的大小输入时。输入太大，可以“溢出”一个数据结构，影响存储在计算机内存中的其他数据。例如，如果一个 Web 表单有一个域与后端的变量关联，该变量仅允许输入 10 个字符，但表单的处理器不验证输入的长度，操作系统可能会简单地将数据写入留给该变量的空间，对存储在内存中的其他数据可能造成损害。在最坏的情况下，该数据可以用来覆盖系统代码，允许攻击者利用缓冲区溢出漏洞在服务器上执行任意代码。

当编写软件时，开发人员必须对允许用户输入的变量给予特别关注。许多编程语言对变量的长度不强制实施固有的限制，这就要求编程人员对代码进行边界检查。因为许多编程人员认为参数检查是一种不必要的、会减缓程序开发速度的负担，所以这就成了程序开发的一个固有的漏洞。作为安全行业的从业人员，必须负责确保组织的开发人员意识到由缓冲区溢出漏洞引起的风险，并且应当采取适当的措施来保护编程人员开发的代码免遭这种类型的攻击。

只要允许用户输入程序变量，编程人员就应当采取有效措施，从而确保满足下列各项条件：

- 用户输入的值的长度不能超过任何存放它的缓冲区的大小(例如，将一个具有 10 个字母的单词输入到最多容纳 5 个字母的字符串变量中)。
- 用户不能向保存输入值的变量类型输入无效的值(例如，将一个字符输入到一个数字型变量中)。
- 用户输入的数值不能超出程序规定的参数操作范围(例如，用“也许”来回答结果只能为“是”或“否”的问题)。

如果没有执行对上述条件的简单检查，那么就可能造成缓冲区溢出漏洞，这种漏洞会导致系统崩溃，甚至可能允许用户运行 shell 命令并获得对系统的访问权限。缓冲区溢出漏洞在使用 CGI 或其他语言进行快速代码开发的过程中尤其普遍，这是因为快速代码开发允许没有经验的编程人员快速生成交互式的 Web 页面。

21.3.2 检验时间到使用时间

检验时间到使用时间(Time-Of-Check-To-Time-Of-Use，TOCTTOU 或 TOC/TOU)的问题是一个时间型漏洞，当程序检查访问许可权限的时间大大早于资源请求的时间时，就会出现这种问题。例如，如果操作系统针对用户登录建立了一个综合的访问许可权限列表，并且在整个登录会话期间查询这个列表，那么就存在 TOCTTOU 漏洞。如果系统管理员取消了某个特殊的权限，那么这个限制只有在用户下次登录时才会起作用。如果在用户登录时正好发生取消访问许可权限的操作，那么用户是否能够访问资源就是不确定的。用户只需保留会话打开数天之久，新的限制就永远不会被应用。

21.3.3 后门

后门是没有被记录到文档中的命令序列，它们允许软件开发人员绕过正常的访问限制。在开发和调试过程中，后门常常被用于加快工作流程并避免强制程序开发人员不断地对系统进行身份认证。有时候，开发人员在系统达到生产要求之后仍在系统中留下这些后门，从而既可以在出现意外故障

时使用，也可以在系统处理他们没有访问权限的敏感数据时进行“偷看”。除了开发商的后门外，许多类型的恶意代码感染系统并创建后门，允许恶意代码的开发者远程访问受感染的系统。

无论怎样，后门不被记录到文档中的性质使其成为系统安全的严重威胁，尤其在后门未被记录到文档中却又被遗忘时更是如此。如果开发人员离开了公司，那么他们可以利用后门访问系统、检索机密信息或参与行业破坏活动。

21.3.4　权限提升和 rootkit

一旦攻击者在一个系统上站稳脚跟，他们通常会迅速进入第二个目标——将他们的访问权限从正常的用户账户扩展到更全面的管理访问权限。他们通过权限提升攻击来实现。

攻击者权限提升攻击的最常见方法之一是通过使用 rootkit。rootkit 可以从互联网上免费获得，并且能够利用各种操作系统的已知漏洞。攻击者经常通过使用密码攻击或社会工程学攻击获得标准的系统用户账号，然后使用 rootkit 将他们的访问权限提高到 root(或系统管理员)级别。这种从标准到管理特权访问的提升被称为权限提升攻击。

系统管理员可以采用一种简单的预防措施来保护他们的系统不会遭受大量的 rootkit 攻击，这其实并不新鲜。系统管理员必须关注针对其环境所使用操作系统而发布的新的补丁程序，而且要始终坚持应用这些修正措施。这是一种加强网络以应对几乎所有 rootkit 攻击和许多其他潜在漏洞的简单方法。

21.4　Web 应用的安全性

Web 应用让你足不出户地购买在线机票、查看电子邮件、支付账单以及买卖股票。今天，几乎所有交易都可以在 Web 站点上完成，许多站点更是允许人们通过其管理重要的事务。

Web 应用具有便利的优点，随之而来的则是一系列新的攻击，这些攻击使提供 Web 应用的机构可能面临安全风险。接下来，我们将介绍两种常见的 Web 应用程序攻击。另外关于更多 Web 应用安全的细节，可以查看第 9 章“安全脆弱性、威胁和对策”。

21.4.1　跨站脚本(XSS)攻击

当 Web 应用程序包含反射式输入类型时，就容易出现跨站脚本(XSS)攻击。例如，某个简单的 Web 应用程序只包含一个请求用户输入用户名的文本框，用户单击“Submit”按钮后，Web 应用程序就会加载新的页面，该页面显示消息“Hello, name”。

正常情况下，这个 Web 应用程序会按照设计运行。但是，怀有恶意的人可以利用该应用程序来欺骗毫无疑心的第三方。读者可能已经知道，通过使用“<SCRIPT>”与“</SCRIPT>” HTML 标记，就可以在 Web 页面嵌入一些脚本。假设在 Name 字段中不输入名字“Mike”，而是输入下面的文本：

```
Mike<SCRIPT>alert('hello')</SCRIPT>
```

Web 应用程序以 Web 页面形式“反射”这个输入，浏览器进程像处理其他任何 Web 页面一样进行处理：显示 Web 页面的文字部分以及执行脚本部分。此时，脚本只是打开一个显示“Hello”

的弹出式窗口。不过，完全可以嵌入更复杂、更恶意的脚本，比如请求用户提供密码并将密码传送给恶意的第三方。

此时，你可能存在困惑：某人是如何不幸落入这种攻击陷阱的？毕竟，在完成反射操作的 Web 应用程序所提供的输入文本框中，你并不希望嵌入攻击自己的脚本。XSS 攻击的关键在于能够将表单输入嵌入一个链接。恶意攻击者可以创建一个 Web 页面，该页面具有一个标题为“Check your account at First Bank”的链接，并且该链接嵌入了表单输入。用户访问这个链接时，Web 页面显示看似可信的 First Bank Web 站点，该站点能够通过有效的 SSL 认证，同时工具栏中显示正确的站点地址。但是，这个站点随后会执行恶意攻击者在表单输入中嵌入的脚本，并且看上去似乎是有效 Web 页面内的正常操作。

如何防御跨站脚本攻击？在创建允许存在各种用户输入的 Web 应用程序时，必须保证执行输入验证。最基本的做法是：一定不允许用户在可反射输入字段中输入<SCRIPT>标记。然而，这种做法并不能完全解决问题。对于乐此不疲的攻击者来说，总是能够找到其他一些巧妙的方法来攻击 Web 应用程序。最佳的解决方案应当是：首先确定许可的输入类型，然后通过验证实际输入来确保其与指定模式匹配。例如，如果 Web 应用程序具有一个允许用户输入年龄的文本框，那么应当只接受一到三位数字作为输入，其他输入则被视为无效。

提示：

更多关于规避跨站脚本的过滤方法，请查看 https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet。

21.4.2 SQL 注入攻击

从组织的角度看，SQL 注入攻击甚至比 XSS 攻击更加危险。与 XSS 攻击一样，SQL 注入攻击也使用了 Web 应用程序不期望的输入。不过，SQL 注入攻击并不试图使用这样的输入来欺骗用户，而是用于获得对内在数据库的未授权访问。

1. 动态 Web 应用程序

在 Web 早期，所有 Web 页面都是静态或无变化的。Web 站点管理员创建了含有信息的 Web 页面并将其放置在 Web 服务器上，用户则可以使用各自的 Web 浏览器在 Web 服务器上检索到 Web 页面。Web 很快跳出了上述静态模型，这是由于用户希望能够根据自己的具体需要来访问定制的信息。例如，某个银行站点的访问者不仅仅关心显示银行位置、营业时间以及服务等信息的静态页面，而且还希望检索到包含个人账户相关信息的动态内容。显然，Web 站点管理员不可能在 Web 服务器上为不同用户创建包含个人账户信息的 Web 页面。对于一家大型银行来说，使用静态 Web 技术需要维护数百万具有最新信息的页面。因此，动态 Web 应用程序应运而生。

在用户发出请求时，Web 应用程序利用数据库创建符合要求的内容。仍然以银行为例，某位用户通过输入账户与密码登入 Web 应用程序，Web 应用程序随后从银行数据库中检索当前的账户信息，并且使用检索到的信息立即生成一个 Web 页面，这个页面包含该用户的当前账户信息。如果用户在一个小时后再次登录，那么 Web 服务器会重复上述过程，并且从数据库获得最新的账户信息。图 21.1 说明了这个模型。

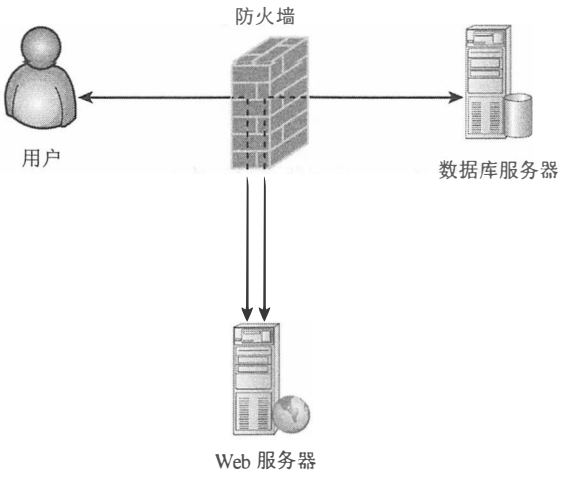


图 21.1　典型的数据库驱动的 Web 站点的体系结构

对于安全人员来说，上述例子说明了什么？ Web 应用程序在传统安全模型中加入了复杂性。如图 21.1 所示，作为可轻易访问的公共服务器，Web 服务器归属于隔离区(DMZ)；另一方面，数据库服务器并非用于公共访问，所以归属于内部网。Web 应用程序需要访问数据库，因此防火墙管理员必须创建一条允许从 Web 服务器访问数据库服务器的规则。这条规则为互联网用户创建了能够有权使用数据库服务器的潜在路径(要想了解防火墙与 DMZ 的更多知识，可以参看第 11 章“网络安全架构和保护网络组件”)。如果 Web 应用程序正常运行，那么就只接受授权用户对数据库的请求。但是，如果 Web 应用程序存在缺陷，就可能导致某些使用 SQL 注入攻击的用户能够以不期望和未授权的方式篡改数据库。

2.SQL 注入攻击

SQL 注入攻击使恶意攻击者能够违反如图 21.1 所示模型的隔离性，从而直接完成攻击内在数据库的 SQL 事务。

提示：

要想了解数据库与 SQL 的更多知识，读者可以参看第 20 章。

在前面的示例中，银行客户可能输入账户号码，从而有权使用检索当前账户细节的动态 Web 应用程序。Web 应用程序则可能使用下面的 SQL 查询形式获取账户信息，这里的<number>是客户在 Web 表单中输入的账户号码：

```
SELECT *
FROM transactions
WHERE account_number = '<number>'
```

此时，还需要明白另一个重要事实：只要每条语句都以分号结束，数据库就能够同时处理多条 SQL 语句。

如果 Web 应用程序并不执行适当的输入验证操作，用户完全可能在由 Web 服务器执行的语句中插入自己的 SQL 代码。例如，假设用户的账户号码为 145249，那么可以输入下面的语句：

```
145249';DELETE * FROM transactions WHERE 'a' = 'a
```

Web 应用程序随后自然地将这些输入嵌入先前 SQL 语句的<number>字段中，从而得到下面这样的语句：

```
SELECT *
FROM transactions
WHERE account_number ='145249'; DELETE * FROM transactions WHERE 'a' = 'a'
```

调整格式之后的语句如下所示：

```
SELECT *
FROM transactions
WHERE account_number ='145249';
DELETE *
FROM transactions
WHERE 'a' = 'a'
```

这是一个包含两条语句的有效 SQL 事务。第一条语句从数据库检索被请求的信息；第二条语句则删除数据库中存储的所有记录，真是令人难以置信！

3. 防御 SQL 注入攻击

可以通过下列三种技术使 Web 应用程序不遭受 SQL 注入攻击的危害：

- **执行输入验证**。与前面讨论的跨站脚本攻击的防御方法一样，输入验证操作能够限制用户在表单中输入的数据类型。具体到上面的 SQL 注入攻击示例，从输入中去除单引号字符就能够成功地防御 SQL 注入攻击。
- **限制用户特权**。Web 服务器使用的数据库账户应当具有尽可能最小的权限集。如果 Web 应用程序只需要检索数据，那么数据库账户就应当仅具有检索能力。在具体的示例中，如果账户只具有 SELECT 权限，那么 DELETE 命令就会失败。
- **使用存储过程**。Web 应用程序的开发应该利用数据库存储过程来限制应用程序执行任意代码的能力。使用存储过程，SQL 语句驻留在数据库服务器上并且仅仅可由数据库管理员修改。调用存储过程的 Web 应用程序可以传递参数，但不改变 SQL 语句的基本结构。

21.5 侦察攻击

恶意代码往往依靠欺骗用户打开或访问恶意软件，其他攻击则直接攻击目标机器。执行侦查可以让攻击者找到弱点，利用他们的攻击代码直接攻击。为了达到这个目标，攻击工具的开发人员开发了许多执行网络侦察的自动化工具。我们将会讨论三种自动侦察技术：IP 探测、端口扫描和漏洞扫描，然后阐述这些技术如何得到更实用的密集型垃圾搜寻技术的辅助。

21.5.1 IP 探测

IP 探测(也被称为 IP 扫描或 ping 扫描)通常是针对目标网络而实施的第一种网络侦察类型。通过这种技术，自动化工具只是试图 ping 某个范围内的所有地址。对 ping 请求进行响应的系统被攻击者记录下来以便进一步分析。没有产生响应的地址被认为不能加以利用并被忽略。

提示：

Nmap 工具是一个用来对 IP 和端口进行扫描的最常见工具，可以免费从 www.nmap.org 网站上下载。

如今，IP 探测在互联网上非常流行。事实上，如果使用公共的 IP 地址来配置系统并连接到互联网，那么在计算机启动后的几个小时内就可能至少遭受一次 IP 探测攻击。这种技术的广泛应用使得禁用 ping 功能成为保护系统安全的强有力理由，至少应当针对网络外部的用户禁用这个功能。

21.5.2　端口扫描

在完成 IP 探测攻击之后，攻击者就会获得一个指定网络中工作系统的列表。攻击者的下一个任务是选择一个或更多个系统作为其他攻击的目标。通常，攻击者已经确定了攻击目标的类型，其中 Web 服务器、文件服务器或其他执行关键操作的服务器是主要目标。

为了缩小搜索范围，攻击者会使用端口扫描软件来探测网络中的所有工作系统并确定每台计算机上运行的公共服务。例如，如果攻击者将 Web 服务器作为攻击目标，那么他们就运行端口扫描软件来定位使用 80 端口(80 端口是 HTTP 服务的默认端口)提供服务的系统。

21.5.3　漏洞扫描

第三种技术是漏洞扫描。一旦攻击者确定了成为攻击目标的系统，他们就需要找到这个系统上可以利用的特定漏洞来获得希望的访问许可权限。从互联网上可以获得的多种工具都能协助完成这个任务。其中，为达到这个目的有许多比较流行的工具，包括 Nessus、OpenVAS、Qualys、Core Impact 和 Nexpose。这些软件包中包含已知漏洞的数据库，并可以通过探测目标系统来定位安全缺陷。随后，它们会生成非常吸引人的报告，报告对所发现的每个漏洞都进行了详细说明。此时，攻击者面对的问题只是找出利用具体漏洞的脚本文件以及对受害系统发动攻击。

认识到漏洞扫描程序是高度自动化的工具十分重要。漏洞扫描程序可以被用于对特定的系统发起攻击，不过攻击者可能使用一系列 IP 探测、端口扫描和漏洞扫描技术来缩小潜在受害系统的列表。不过，入侵者也可能运行漏洞扫描程序来对整个网络进行探测，从而找出可以被利用的漏洞。

需要再次强调的是，只有将操作系统升级到最新的安全补丁级别，才有可能几乎完全修复漏洞扫描程序报告的所有漏洞。此外，明智的系统管理员要学会像他们的敌人那样思考问题，下载并运行这些针对自己网络的漏洞扫描程序(当然要经过上层管理者的许可)，从而了解潜在的攻击者会利用哪些安全漏洞。这样可以快速集中资源以强化网络中最薄弱的环节。

21.5.4　垃圾搜寻

每个组织都会产生垃圾，通常每天的日常工作会产生大量的垃圾。你曾经花时间对自己的垃圾进行过分类吗？查看过是否将敏感资料投入了垃圾箱吗？试着这样做一次，结果会让你大吃一惊。当你将每天分析的工作文件到处乱扔时，试着从攻击者的角度看待这个问题。能够从这些文件中收集到什么样的信息，可以帮助发动一次攻击吗？那些文件里存在有关网络配置或已安装软件版本的敏感数据吗？特殊部门员工的生日列表能够被用于社会工程学攻击吗？一本策略手册中可能包含生

成新账户的详细规范吗？随便丢弃的软盘或其他存储介质可能存有重要数据吗？

不要低估琐碎的公司文档对于社会工程学攻击的价值。著名的社会工程师 Kevin Mitnick 曾经被允许使用公司的简报作为攻击的关键组件。他很快注意到包含新员工列表的部分，并且意识到这些人是最合适的受害者：这些新员工在接到来自“高层”对机密信息的电话请求时都会十分热情。

垃圾搜寻是本书提到的最古老的攻击方法之一，直到今天还在被使用。针对这种攻击的最佳防御措施相当简单，就是使攻击者的行动变得更困难。为主要部门购买碎纸机并鼓励员工使用这种计算机。将垃圾保存在一个安全的地方，直到收拾垃圾的人到来。这些小细节的培养需要经历漫长的过程。

21.6 伪装攻击

为了获得对没有访问资格的资源的访问权限，最简单的方法之一就是假冒具有适当访问许可权限的人。在现实生活中，十几岁的青少年经常借用自己兄长或姐姐的驾驶证开车，在计算机的安全领域中也会发生相同的事情。攻击者借用合法用户和系统的身份得到第三方的信任。在本节中，我们将介绍两种常见的伪装攻击：IP 欺骗和会话劫持。

21.6.1 IP 欺骗

在 IP 欺骗攻击中，怀有恶意的人只是重新配置他们的系统，使其具有可信任系统的 IP 地址，然后试图获得访问其他外部资源的权限。在许多没有安装阻止这种通信类型发生的适当过滤器的系统中，你会惊奇地发现 IP 欺骗非常有效。系统管理员应该在每个网络的边缘配置过滤程序，从而确保数据包至少符合下列标准：

- 具有内部源 IP 地址的包不能从外部进入网络。
- 具有外部源 IP 地址的包不能从内部离开网络。
- 具有私有 IP 地址的包不能从任何一个方向通过路由器(除非被允许作为内部配置的一部分)。

这三条简单的过滤规则能阻止绝大多数的 IP 欺骗攻击并大大提高网络的安全性。

21.6.2 会话劫持

会话劫持攻击指的是怀有恶意的人中途拦截已授权用户与资源之间通信数据的一部分，然后使用劫持技术接管这个会话并伪装成已授权用户的身份。下面列出了一些常见的技术：

- 捕获客户端与服务器之间身份认证的详细信息，并使用这些信息伪装成客户端的身份。
- 欺骗客户端，使其认为攻击者的系统是与之通信的服务器，并在客户端与服务器建立合法连接时作为中间人，然后断开服务器与客户端的连接。
- 使用没有正常关闭连接的用户的 cookie 数据访问 Web 应用程序。

上述所有技术都可能对终端用户造成灾难性的后果，因此必须使用行政管理性控制措施(如防重放身份认证技术)和应用程序控制措施(如在一段适当的时间内使 cookie 数据过期)予以处理。

21.7　本章小结

应用程序开发人员有很多担心！随着黑客使用的工具和技术变得越来越复杂，由于复杂性和多个脆弱点，应用层越来越多地成为他们攻击的焦点。

恶意代码，包括病毒、蠕虫、木马和逻辑炸弹，利用应用程序和操作系统中的漏洞或使用社会工程学感染操作系统，并获得它们的资源和机密信息。

应用程序自身也可能包含许多漏洞。缓冲区溢出攻击利用缺少适当输入验证的代码来影响系统内存中的内容。后门为以前的开发者和恶意代码的作者提供绕过正常安全机制的能力。rootkit 为攻击者提供了一种简单的方法来执行权限提升攻击。

许多应用程序正在转向 Web，从而制造新级别的暴露和漏洞。跨站脚本攻击允许黑客欺骗用户向不安全的站点提供敏感信息。SQL 注入攻击允许绕过应用程序控制直接访问和操纵底层数据库。

探测工具为攻击者提供了自动化工具，他们可以使用它们来确定后面要攻击的带有脆弱性的系统。IP 探测、端口扫描和漏洞扫描都是使用自动化的方法来检测组织的安全控制中的薄弱点。伪装攻击使用隐形技术来模拟用户和系统。

21.8　考试要点

理解病毒使用的传播技术。病毒使用 4 种主要的传播技术来渗透系统并传播恶意有效载荷，这三种技术是文件感染、服务注入、引导扇区感染和宏感染，从而渗透系统和扩散它们的病毒载体。需要理解这些技术以有效地保护网络上的系统免受恶意代码侵犯。

知道反病毒软件包如何检测已知病毒。大多数反病毒程序使用特征型检测算法寻找已知病毒的指示模式。为了维持对新产生病毒的防护，定期更新病毒定义文件是必不可少的。

解释攻击者使用的损坏密码安全的攻击技术。密码是目前最常见的访问控制机制，也是必不可少的，所以需要知道如何保护以防止攻击者破坏它们的安全性。知道如何进行密码破解、字典攻击和社会工程学攻击也可以打败密码的安全性。

熟悉各种类型的应用程序攻击，攻击者使用这些攻击来攻击编写拙劣的软件。应用程序攻击是现代计算的最大威胁之一。攻击者还利用后门、检查时间到使用时间漏洞以及 rootkit 来获得对系统的非法访问。安全专家必须对每种攻击和相关控制措施有清晰的理解。

理解常见 Web 应用程序的漏洞及对策。由于许多应用程序转移到 Web 上，开发人员和安全专业人员必须了解存在于当今环境中的新的攻击类型，以及如何防护它们。两个最常见的例子是跨站脚本(XSS)攻击和 SQL 注入攻击。

知道攻击者准备攻击网络时使用的网络侦察技术。在发起攻击之前，攻击者使用 IP 扫描来找出网络中运行的主机。这些主机随后会遭到端口扫描和其他漏洞探测，从而使攻击者能够定位在目标网络中可能被攻击的脆弱之处。应该在理解这些攻击后帮助网络抵御这些攻击，限制攻击者可能收集的信息量。

21.9 书面实验室

1. 病毒和蠕虫之间的主要区别是什么？
2. 阐述 Robert Tappan Morris 设计的互联网蠕虫所使用的 4 种传播方法。
3. 当反病毒软件包发现被感染的文件时，可以采取什么操作？
4. 解释数据完整性保证软件包(如 Tripwire)如何提供一些辅助的病毒检测能力。

21.10 复习题

1. 以下哪一项技术被普遍采用以应对病毒攻击？
   A. 特征码检测
   B. 启发式检测
   C. 数据完整性保证
   D. 自动重建
2. 你是一家电子商务公司的安全管理员，并且正在部署新的 Web 服务器到生产环境中，应该使用什么网络区域？
   A. 互联网
   B. DMZ
   C. 内部网
   D. 沙盒
3. 以下哪一种类型的攻击依赖于两个事件之间的时间差异？
   A. smurf
   B. TOC/TOU
   C. Land
   D. Fraggle
4. 以下哪一项技术需要管理员确定适当的应用程序环境？
   A. 沙盒
   B. 控制签名
   C. 完整性监控
   D. 白名单
5. 以下什么先进的病毒技术在其感染的每个系统上修改病毒的恶意代码？
   A. 多态
   B. 隐身
   C. 加密
   D. 多分体
6. 下列哪个工具提供了一个忘记复杂密码情况下的解决方案？
   A. LastPass
   B. 破解工具
   C. 影子密码文件

D. Tripwire

7. 以下哪一种应用程序漏洞直接允许攻击者修改系统内存中的内容？

A. rootkit

B. 后门

C. TOC/TOU

D. 缓冲区溢出

8. 以下哪个密码最不可能在字典攻击中被攻破？

A. mike

B. elppa

C. dayorange

D. fsas3aIG

9. 以下哪个文件在 Unix 系统中用于防止字典攻击？

A. /etc/passwd

B. /etc/shadow

C. /etc/security

D. /etc/pwlog

10. 当向 Web 表单中输入数据时，以下哪个字符作为用户输入应该认真对待？

A. !

B. &

C. *

D. '

11. 什么数据库技术，如果执行了 Web 表单，可以限制 SQL 注入攻击？

A. 触发器

B. 存储过程

C. 列加密

D. 并发控制

12. 什么类型的侦察攻击为攻击者提供了关于系统上运行的服务的有用信息？

A. 会话劫持

B. 端口扫描

C. 垃圾回收

D. IP 扫描

13. 在网页上使用跨站脚本攻击，什么条件是必需的？

A. 反射输入

B. 数据库驱动的内容

C. .NET 技术

D. CGI 脚本

14. 什么类型的病毒利用一种以上传播技术，以最大限度地加大渗透系统的数量？

A. 隐形病毒

B. 伴随病毒

C. 多态病毒

D. 多分体病毒

15. 哪种方法是防御跨站脚本攻击的最有效防御方法？

A. 限制账户权限

B. 输入验证

C. 用户认证

D. 加密

16. 以下哪个蠕虫首次对设施造成重大物理损害？

A. 震网病毒

B. 红色代码

C. Melissa

D. RTM

17. Ben 的系统感染了恶意代码，修改了操作系统，允许恶意代码的作者访问他的文件，这个攻击者利用了什么类型的攻击技术？

A. 权限提升

B. 后门

C. rootkit

D. 缓冲区溢出

18. 哪一种技术是 Java 语言采用的用来最小化 applet 带来的威胁？

A. 保密

B. 加密

C. 隐身

D. 沙盒

19. 哪个 HTML 标签常常作为跨站脚本(XSS)攻击的一部分？

A. <Hl>

B. <HEAD>

C. <XSS>

D. <SCRIPT>

20. 为了防止 IP 欺骗而设计防火墙规则时，以下哪条规则需要遵守？

A. 具有内部源 IP 地址的数据包不能从外部输入网络

B. 具有内部源 IP 地址的数据包不从内部退出网络

C. 具有公共 IP 地址的数据包不能从任一方向通过路由器

D. 具有外部源 IP 地址的数据包不从外部输入网络

附录 A

复习题答案

第 1 章　通过原则和策略的安全治理

1. B. 安全性的主要目标和目的是 CIA 三元组中的机密性、完整性和可用性。

2. A. 对脆弱性和风险的评估依据是它们对 CIA 三元组中一条或多条安全原则的威胁程度。

3. B. 可用性意味着经过授权的主体被授权及时地、不间断地访问客体。

4. C. 硬件的毁坏是对可用性和完整性的破坏。对机密性的破坏包括：捕获网络通信数据、窃取密码文件、社会工程学、端口扫描、肩窥、偷听以及嗅探。

5. C. 对机密性的破坏不仅限于直接针对机密性的攻击。许多未授权的敏感或机密信息泄露都是由于人为错误、疏忽或失职造成的。

6. D. 披露不是 STRIDE 的元素。STRIDE 的元素是欺骗、篡改、否认、信息披露、拒绝服务和特权提升。

7. C. 数据、对象和资源的可访问是可用性的目标。如果安全机制提供了可用性，那么它就提供了经过授权的主体能够访问数据、对象和资源的高级别保证。

8. C. 隐私是指保持信息的机密性，这些信息可以是个人身份信息，或者如果泄露，就可能会对他人造成伤害、尴尬或丢人的信息。隔离是将东西存储在一个位置的方式。隐瞒是隐藏或阻止披露的行为。信息对应关键业务的水平是对其重要性的衡量。

9. D. 用户应当意识到电子邮件信息已被保留，但是没有必要向用户泄漏用于执行这个操作的备份机制。

10. D. 所有权授予实体对其拥有的对象全部的功能和特权。获取所有权的能力通常被授予操作系统中最强大的账户，因为它可以用于超越其他实现的任何访问控制限制。

11. C. 不可否认性确保事件或活动的主体不能否认已经发生的事件。

12. B. 分层法是以连续的方式部署多层安全机制。当连续实施安全限制时，它们以线性方式依次被执行。因此，单个安全控制的失败不会使整个解决方案失效。

13. A. 防止经过授权的客体读者删除客体只是一种访问控制，而不是数据隐藏。如果能够阅读客体，那么客体就未被隐藏。

14. D. 防止安全受到威胁是变更管理的主要目标。

15. B. 数据分类方案的主要目的是：根据分配给数据的重要性和敏感性标签对数据安全保护过程进行规范化和层次化。

16. B. 大小不是建立数据分类的标准。当对一个客体进行分类的时候，应当将价值、生存期和安全含义考虑在内。

17. A. 军方(或政府)和私营部门(或商业企业)是两种通用的数据分类方案。

18. B. 在列出的选项中，秘密是最低级别的军事数据分类。请记住，标记为机密、秘密和最高机密的项统称为分类，机密在列表中低于秘密。

19. B. 商业企业/私营部门中的隐私数据分类用来保护个人的相关信息。

20. C. 分层法是安全机制的一个核心方面，但是并非数据分类的重点。

第 2 章　人员安全和风险管理概念

1. D. 无论安全解决方案中有任何元素，人都是最薄弱的环节。

2. A. 雇用新员工的第一步是要生成工作描述。如果没有工作描述，那么就没有对需要寻找和雇用何种类型人员达成一致意见。

3. B. 离职面谈的主要目的是根据雇佣协议和任何其他与安全相关的文件，来检查保密协议(NDA)和对前雇员的其他责任和限制。

4. B. 在员工得到合同终止通知之前或同一时间，就应当删除或禁用此员工的网络用户账号。

5. B. 第三方治理是你的组织所依赖的第三方安全监督的应用。

6. D. 文档审查的一部分是对业务流程和组织策略的逻辑和实际调查。

7. C. IT 基础设施的风险并非都是基于计算机的。事实上，许多风险来自非计算机。当为组织执行风险评估时，应考虑所有可能的风险。假如没有适当评估和对各种形式风险的响应，公司仍然脆弱。

8. C. 风险分析包括：分析环境中存在的风险，评估每种风险发生的可能性和造成的损失是多少，评估各种风险的各种对策的成本，以及生成防护措施的成本/效益报告并呈交给上层管理者。选择防护措施是上层管理者根据风险分析的结果进行的一项任务。这是风险管理中的一项任务，不是风险分析过程的一部分。

9. D. 用户的个人文件不是组织的资产，因此不在风险分析中予以考虑。

10. A. 威胁事件是意外或故意地利用漏洞。

11. A. 脆弱性指的是防护措施或对策不存在或很薄弱。

12. B. 任何能够消除脆弱性或阻止一种或多种特定威胁的方法被称为防护措施或对策，而不是风险。

13. C. 防护措施每年的成本不应该超过资产损失的年度预计成本。

14. B. SLE 是使用公式 SLE=资产价值($)*暴露因子(SLE =AV * EF)来计算的。

15. A. 防护措施对于组织的价值使用下面的公式计算：实现防护措施前的 ALE-实现防护措施后的 ALE-防护措施每年的成本[(ALE1 – ALE2) – ACS]。

16. C. 合作者愿意参与非法或攻击性计划的可能性被降低，这是因为组合使用责任分离、限制工作职责和岗位轮换使得这些活动被发现的风险更高。

17. C. 培训是教育员工执行他们的工作任务和遵守安全策略。培训通常由组织主持，并针对具有类似工作职能的员工群体。

18. A. 安全功能管理通常包括对预算、指标、资源、信息安全策略的评估，以及评估安全程序的完整性和有效性。

19. B. 火灾的威胁和缺少灭火器的脆弱性会导致设备破坏的风险。

20. D. 对策直接影响年发生比率，这主要是因为对策被设计用于阻止风险的发生，从而减少每年发生风险的频率。

第 3 章 业务连续性计划

1. B. 业务结构分析可以帮助最初的计划编制者选择合适的 BCP 团队成员，然后指导整个 BCP 过程。

2. B. BCP 团队的第一个任务应该是审查和确认业务结构分析，业务结构分析最初是由那些负责开拓 BCP 工作的人执行。这样做能够确保由一小组人员承担的初始工作反映整个 BCP 团队的看法。

3. C. 公司的领导和主管在尽职尽责地实施活动方面受到法律的约束。这一概念保证了管理层具有实施适当的业务连续性计划的不可推卸的责任。

4. D. 在计划编制期间，最重要的资源利用是 BCP 团队成员专门进行计划编制本身所花费的时间。这体现了业务资源使用的重要性，也是高层管理人员必须参与进来的另外一个原因。

5. A. 确定优先级的定量分析部分应该用货币单位分配资产价值。

6. C. 年度损失期望(ALE)是指每一年由于特定风险所导致的业务货币损失值。按定量方式确定业务连续性资源分配的优先顺序时，这个数值相当有用。

7. C. 最大可容忍故障时间(MTD)是指业务功能无法获得而不会引起无法挽回的业务损失的最长时间。这个数值在确定分配给特殊功能的业务连续性资源的级别时，非常有用。

8. B. SLE 是 AV 和 EF 的乘积。在本题中，AV 是 3 000 000 美元，并且 EF 是 90%，根据相同土地可以被用与重新构建设施这一事实，因此 SLE 是 2 700 000 美元。

9. D. 这个问题要求计算 ALE，它是 SLE 和 ARO 的乘积。在本题中，ARO 为 0.05(或 5%)。从第 8 题得知，SLE 是 2 700 000 美元，因此 ALE 是 135 000 美元。

10. A. 这个问题要求计算 ALE，它是 SLE 和 ARO 的乘积。在本题中，ARO 为 0.10(或 10%)。由假设场景得知，SLE 是 750 万美元，因此 ALE 是 75 万美元。

11. C. 通过分析在 BIA 期间开发的风险优先级列表和确定在 BCP 中处理哪些风险，策略开发任务在业务影响评估和连续性计划编制之间架起了桥梁。

12. D. 人的生命安全在业务连续性计划中必须始终是最为重要的关注内容。确保你的计划反映了这个优先级，特别在记录文档中更是如此，这份文档会分发给组织中的所有员工！

13. C. 计算负面宣传对业务造成的损失非常困难。因此，这种类型的关注通过定性分析更容易估计。

14. B. 单一损失期望(SLE)是单一风险发生后导致的破坏程度。在本题中，SLE 是 1 千万美元，这是一次龙卷风的破坏期望值。每百年才发生一次的龙卷风不在 SLE 的反映范围内，但在年度损失期望(ALE)的范围内。

15. C. 年度损失期望(ALE)是单一损失期望(SLE，本题中为 1 千万美元)和年度发生率(ARO，本题中为 0.01)的乘积，最后得到结果为 10 万美元。

16. C. 在预备和处理阶段，BCP 团队实际上为缓解在策略开发阶段被认为不可接受的风险设计了规程和机制。

17. D. 这是替换系统的一个例子。冗余通信链路是备用系统的一种形式，它在主通信链路出现故障时提供了备份链路。

18. C. 灾难恢复计划在业务连续性计划中止时开始。在灾难发生后，业务被中断，灾难恢复计划指导响应团队快速地将业务运营恢复到正常水平。

19. A. 单一损失期望是资产价值(AV)和暴露因子(EF)的乘积。其他公式并没有真实反映这个计算过程。

20. C. 你应当致力于尽可能使公司最高主管签署 BCP 的重要性声明。在给出的选项中，首席执行官级别最高。

第 4 章　法律、法规和合规性

1. C. 《计算机诈骗和滥用法案(修正案)》针对那些使用病毒、蠕虫、特洛伊木马和其他类型恶意代码进行犯罪，从而造成计算机系统损坏的个人制定了刑事和民事惩罚。

2. A. 《计算机安全法案》要求强制性地对涉及管理、使用或操作包含敏感信息的联邦计算机系统的所有人定期进行培训。

3. D. 行政法不需要立法机构的法案在联邦一级实施。行政法由政府执行机构颁布的策略、规程和措施组成。虽然不需要国会的法案，但是这些法律要受到司法审查而且必须遵守由立法机构制定的刑法和民法。

4. C. 美国国家标准技术研究所(NIST)负责联邦政府以下所有计算机系统的安全管理，这些系统不用于处理敏感的国家安全信息。美国国家安全局(国防部的一部分)负责管理那些处理机密和/或敏感信息的系统。

5. C. 最初的《计算机诈骗和滥用法案》(1984 年)只包括政府和金融机构使用的系统。该法案在 1986 年被扩展，包括了所有的涉及联邦利益的系统。《计算机滥用修正案》(1994 年)进一步修正了 CFAA，包括了在州间贸易中使用的所有系统，这覆盖了美国大部分(但不是全部)的计算机系统。

6. B. 美国宪法的第四修正案建立了执法官员在执行搜查和/或没收私有财产时必须遵循的“可能动机”标准。它还声明这些官员必须在获得对这些财产的非自愿访问之前获得搜查证。

7. A. 版权法是 Matthew 可以使用的知识产权的唯一类型。它只包括了 Matthew 使用的具体软件的代码，不包括软件背后的思维过程或想法。商标法不适合这种情况。专利权不适用于数学算法。Matthew 不能寻求商业秘密法的保护，这是由于他打算在公共技术杂志上发表该算法。

8. D. Mary 和 Joe 应当将他们的原油处方作为商业秘密。只要他们不公开透露这个处方，那么他们将长期拥有它并作为公司的商业秘密。

9. C. Richard 的产品名称应该受到商标法的保护。在商标注册得到授权前，他可以在名称旁边使用符号™，以通知其他人此名称受到商标法的保护。一旦他的申请被批准，名称就变成一个注册的商标，并且 Richard 可以开始使用®符号了。

10. A. 美国的《隐私法案》(1974 年)限制了政府机构使用公民在某种情况下透露给他们的信息

的方法。

11. B. 《美国统一计算机信息处理法案》(UCITA)试图实施一个有关所有州都采纳的计算机处理的标准法律架构。UCITA 处理的一个问题是不同软件许可证协议类型的合法性。

12. A. 《儿童联机隐私保护法案》(COPPA)对未经父母许可而收集小孩的信息处以严厉的处罚。COPPA 声明如果孩子的年龄小于 13 岁，那么在收集信息前，必须获得孩子父母的允许(除了基本信息要求获得这种许可以外)。

13. A. 《数字千禧年版权法案》对于“暂时性行为”免除的保护不包括任何地理位置的要求。其他选项是 5 个强制性要求中的 3 个。另外两个要求是服务提供商不能决定数据的接收者以及不能对传输数据的内容进行修改。

14. C. 《美国爱国者法案》在 9 • 11 恐怖袭击后被采纳。它扩大了政府监视私人间通信的能力，并且因此实际上削弱了消费者和互联网用户的隐私权。其他被提到的法律都包含用于增强个人隐私权的规定。

15. B. 收缩性薄膜包装的许可证协议在用户打开软件包装时生效。单击包装许可证协议要求用户在安装过程中单击一个按钮，以接受许可证协议的条款。标准的许可证协议要求用户在使用软件之前签署一份书面协议。口头协议通常不用于软件许可，而且还要求软件用户在一定程度上积极参与。

16. B. Gramm-Leach-Bliley法案提供了有关商业机构可能处理属于客户的个人信息方法的规定。

17. C. 美国专利权法从专利申请提交到专利和商标局的时候开始提供 20 年的独家使用权。

18. C. 根据欧盟隐私指令的定义，市场销售需求不是处理个人信息的有效基础。

19. C. 支付卡行业数据安全标准(PCI DSS)适用于涉及信用卡信息的存储、传输和处理的组织。

20. A. 2009 年的《经济和临床卫生健康信息技术法》(HITECH)修订了 HIPAA 的隐私和安全要求。

第 5 章　保护资产的安全

1. A. 信息分类过程的主要目的是识别敏感数据的安全分类，并定义保护敏感数据的需求。信息分类过程通常包括保护静态敏感数据(备份和存储在介质上)的需求，但不包括备份和存储任何数据的需求。类似地，信息分类过程通常包括保护传输中敏感数据的要求，但不包括任何数据。

2. B. 数据根据其对组织的价值进行分类。在某些情况下，如果未授权人员可以访问它们，则是基于潜在负面影响进行分类的，这表示负值。它不是基于系统的处理进行分类，而是基于处理数据的系统进行分类。类似地，基于数据分类来对存储介质进行分类，但是不基于数据被存储在何处来对数据进行分类。可访问性受分类影响，但可访问性不确定分类。人员实施控制来限制敏感数据的可访问性。

3. D. 在网站上不发布敏感数据，但 PII、PHI 和专有数据都是敏感数据。

4. D. 分类是标记介质最重要的方面，因为它清楚地标识介质的价值，用户知道如何基于分类来保护介质。包括诸如日期和内容描述的信息不像标记分类那样重要。可以使用电子标签或标记，但是当使用它们时，最重要的信息仍然是数据分类。

5. C. 清洗介质通过多次写入现有数据来删除所有数据，以确保使用任何已知方法都无法恢复数据。然后，清洗的介质可以在不太安全的环境中重复使用。擦除介质执行删除，但数据仍然保留

且可以轻松恢复。清除或覆盖会将未分类的数据写入现有数据，但某些复杂的取证技术仍然可能恢复原始数据，因此此方法不应用于减少介质的分类。

6. C. 净化可能不可靠，因为人员可能不适当地执行清洗、消磁或其他过程。正确完成后，使用任何已知方法无法恢复已清洗的数据。数据无法从已焚烧或已烧毁的介质中恢复回来。数据不会被物理蚀刻到介质中。

7. D. 清洗是给定选项中最可靠的方法。清洗用随机位多次覆盖介质，并包括附加步骤以确保数据被删除。然而这不是很有效的答案选择，驱动器的破坏才是一种更可靠的方法。擦除或删除进程不可能从介质中删除数据，而是将其标记为删除。固态驱动器(SSD)没有磁通，因此消磁 SSD 不会破坏数据。

8. C. 物理破坏是在诸如 DVD 等光学介质上删除数据方面最安全的方法。格式化和删除处理很少不能从任何介质中删除数据。DVD 没有磁通，因此消磁 DVD 不会破坏数据。

9. D. 数据剩余是指作为剩余磁量保留在硬盘驱动器上的数据残余。消除、清洗和覆盖是擦除数据的有效方法。

10. C. Linux 系统使用 bcrypt 加密密码，bcrypt 基于 Blowfish。bcrypt 添加 128 个附加位作为盐，以防止彩虹表攻击。高级加密标准(AES)和三重 DES(或 3DES)是单独的对称加密协议，没有一个是基于 Blowfish 的，或直接与防止彩虹表攻击相关。安全复制(SCP)使用安全 Shell(SSH)加密通过网络传输的数据。

11. D. SSH 是对 Telnet 的安全替代，因为它加密通过网络传输的数据。相反，Telnet 以明文传输数据。SFTP 和 SCP 是通过网络传输敏感数据的好方法，但不用于管理目的。

12. D. 数据保管者执行日常任务来保护数据的完整性安全，这包括备份它们。用户访问数据。所有者对数据进行分类。管理员为数据分配权限。

13. A. 管理员基于最小特权原则分配权限和知其所需权限。保管者保护数据的完整性和安全性。所有者对数据负有最终责任，确保其被正确分类，并且所有者为管理员提供有权访问的权限，但所有者不分配权限。用户只是访问数据。

14. C. 行为规则识别适当使用和保护数据的规则。最小特权确保用户只能访问他们所需要的数据。数据所有者确定谁有权访问系统，但这不是行为规则。行为规则适用于用户，但不是系统或安全控制。

15. A. 欧盟数据保护法将数据处理器定义为“仅代表数据控制器处理个人数据的自然人或法人”。数据控制器是控制数据处理并指示数据处理器的实体。在欧盟数据保护法中，数据处理器不是计算系统或网络。

16. A. 这些是安全港原则的前 4 条原则，它们适用于保护数据隐私。它们不涉及数据的识别或保留。它们主要涉及隐私数据，如个人身份信息(PII)。虽然这可能被视为分类，但分类不是 7 条安全港原则的主要目的。

17. D. 范围定制和定制过程允许组织根据需要定制安全基线。不需要实施不适用的安全控制，并且不需要识别或重新创建不同的基线。

18. D. 备份介质应该受到与其包含的数据相同保护级别的保护，并且使用安全的异地存储设施来确保这一点。介质应该被标记，但是如果被存放在无人仓库中，那就无法保护它。备份副本应存放在异地，以确保在灾难影响主要位置时可用。如果数据副本未在场外存储或异地备份被破坏，则由于风险的可用性而牺牲了安全性。

19. 如果磁带在离开数据中心之前被标记，员工就会认识到他们的价值，而且更有可能有人会

在无人仓库中挑战他们的存储方式。在使用之前对磁带进行清洗或消磁将会擦除先前保存的数据，但是如果敏感信息在清洗或消磁后备份到磁带中，则无济于事。将磁带添加到资产管理数据库将有助于跟踪它们，但不会防止此类事件。

20. B. 人员没有遵守记录保留策略。该方案声明管理员清洗 6 个月以上的现场电子邮件以符合组织的安全策略，但异地备份包含过去 20 年的备份。当组织不再需要介质时，人员应遵循介质销毁策略，但需要一些备份。配置管理确保使用基线正确配置系统，但这不适用于备份介质。版本控制应用于应用程序，而不是备份磁带。

第 6 章　密码学与对称加密算法

1. C. 要确定密钥空间中的密钥数，可用 2 的密钥空间位数的乘方。例如，2^4=16。

2. A. 不可否认性防止消息的发送者否认曾经发送过消息。

3. A. DES 使用一个 56 位的密钥。这被认为是该密码系统的主要缺点。

4. B. 换位密码使用多种技术重新排列消息中的字符。

5. A. Rijndael 密码准许用户根据特定的应用安全要求选择一个长度为 128、192 或 256 位的密钥。

6. A. 不可否认性要求使用公钥密码系统，从而防止用户错误地否认他们生成了消息。

7. D. 假设使用正确，那么一次性填充是唯一已知的不易攻击的密码系统。

8. B. 选项 B 是正确的，因为 16 被 3 除等于 5，余数为 1。

9. A. 美国的密码分析人员发现了苏联用于生成一次性填充的方法中的一个模式。发现这个模式之后，大多数编码最终都被破译了。

10. C. 分组密码对消息的“组块”进行操作，而不是对单个字符或比特进行操作。选项中提到的其他密码都属于流密码类型，这种密码对消息的单个比特或字符进行操作。

11. A. 对称密钥密码学使用共享的密钥。所有的通信方在任何方向的通信上都使用相同的密钥。

12. B. N 分之 M 的控制要求在代理总数(N)中的最小数量的代理(M)一起工作以执行高安全性任务。

13. D. 输出反馈(OFB)模式防止早期错误干扰未来的加密/解密。密码块链接和密码反馈模式将在整个加密/解密过程中携带错误。电子代码本(ECB)操作不适合大量数据。

14. C. 单向函数是一种数学运算，可以为每个可能的输入组合轻松地生成输出值，但无法检索输入值。

15. C.对称算法所需的密钥数量由公式(n *(n−1))/2决定。在这种情况下，如果n = 10，则密钥数量为45。

16. C. 高级加密标准使用 128 位大小的块，尽管事实上它基于的 Rijndael 算法允许可变块大小。

17. C. 凯撒密码(以及其他简单的替代密码)容易遭受频率攻击，这种攻击会分析特定字母在密文中出现的频率。

18. B. 滚动密钥密码(或“书籍”密码)会将常见书籍中的一段话作为加密密钥。

19. B. 由 Bruce Schneier 开发的 Twofish 算法使用预白化和后白化技术。

20. B. 在非对称算法中，每个通信方都需要两个密钥：公钥和私钥。

第 7 章　PKI 和密码学应用

1. B. 数字 n 是两个大质数 p 和 q 的乘积。因此，n 肯定总是比 p 和 q 大。此外，算法对 e 的选择进行限制，e 要小于 n。因此，在 RSA 密码学中，n 在这个问题的 4 个变量选项中总是最大的。

2. B. El Gamal 密码系统扩展了 Diffie-Hellman 密钥交换协议的功能，从而支持消息的加密和解密。

3. C. Richard 必须使用 Sue 的公钥加密消息，这样 Sue 可以使用自己的私钥解密消息。如果 Richard 使用自己的公钥加密信息，那么接收方就需要知道 Richard 的私钥才能够解密这条消息。如果 Richard 使用自己的私钥加密消息，那么任何用户都可以通过自由获得的 Richard 的公钥来解密消息。因为 Richard 无法取得 Sue 的私钥，所以他无法使用 Sue 的私钥来加密此消息。如果 Richard 做到了，那么任何用户都可以自由获得 Sue 的公钥来解密消息。

4. C. El Gamal 密码系统的主要缺点是：它会将加密的任何消息的长度都增加一倍。因此，当使用 EL Gamal 加密消息的时候，2048 位的明文消息将会产生一条 4096 位的密文消息。

5. A. 椭圆曲线密码系统只需要足够短的密钥就能达到与 RSA 加密算法同样的加密强度。1024 位的 RSA 密钥的加密强度等价于 160 位的椭圆曲线密码系统密钥的加密强度。

6. A. 无论输入消息的大小，SHA-1 散列算法总是生成 160 位的消息摘要。事实上，这种固定长度的输出结果是所有安全散列算法的一个要求。

7. C. WEP 算法已被书面证明存在易被破解的弱点，这种算法应当不能再被用于保护无线网络。

8. A. Wi-Fi 安全访问(WPA)使用临时密钥完整性协议(TKIP)保护无线通信。WPA-2 使用 AES 加密。

9. B. Sue 会使用 Richard 的公钥加密消息。因此，Richard 需要使用密钥对中的互补密钥(即他自己的私钥)来解密消息。

10. B. Richard 应当使用自己的私钥加密消息摘要。当 Sue 接收信息的时候，她会使用 Richard 的公钥解密消息摘要，然后计算出自己的消息摘要。如果这两个消息摘要匹配，那么就能确认此信息的确来自 Richard。

11. C. 数字签名标准允许美国联邦政府使用数字签名算法、RSA 或椭圆曲线 DSA 结合 SHA-1 散列函数一起生成安全的数字签名。

12. B. X.509 管理数字证书和公钥基础结构(PKI)。它为数字证书定义了适当的内容以及证书授权机构生成和撤消证书的过程。

13. B. 可靠隐私使用数字签名验证的“信任 Web”系统，加密技术基于 IDEA 私钥密码系统。

14. C. 安全套接字利用 TCP 端口 443 进行加密的客户端/服务器通信。

15. C. 中间人攻击证明其使用击败标准 DES 同等的计算能力就能够击败 2DES，这导致采用三重 DES(3DES)作为政府通信的标准。

16. A. 彩虹表包含常用密码的预计算哈希值，并且可用于提高密码破解攻击的效率。

17. C. WiFi 保护访问协议加密在移动客户端和无线接入点之间传递的流量。它不提供端到端加密。

18. B. 因为证书撤消列表(CRL)的分发存在时间间隔，所以 CRL 在证书到期过程中引入了固有的延迟。

19. D. 密码分析已能破解Merkle-Hellman背包算法，这种算法依赖于因式分解超增序列的困难性。

20. B. IPSec 是一种安全协议，它为在两个实体之间建立交换信息的安全信道定义了一个架构。

第 8 章　安全模型的原则、设计和功能

1. B. 系统认证是从技术角度进行评估。选项 A 描述的是系统鉴定。选项 C 和 D 指的是制造厂商的标准，而不是实现标准。

2. A. 鉴定是正式验收的过程。选项 B 不是正确的答案，因为它指的是制造厂商的标准。选项 C 和 D 之所以不正确的原因是：没有方法能够证明这种配置实施了安全策略，并且鉴定过程不需要安全通信规范。

3. C. 封闭式系统主要使用专用或不公开的协议和标准。选项 A 和 D 没有描述出任何具体的系统，选项 B 描述的是一个开放式系统。

4. C. 受约束的进程只能访问特定的内存位置。选项 A、B 和 D 描述的不是受约束的进程。

5. A. 客体是用户或进程希望访问的资源。选项 A 描述的是一个访问客体。

6. D. 控制通过限制对某个客体的访问来保护这个客体免遭未经授权的用户的滥用。

7. B. 为 DITSCAP 和 NIACAP 站点鉴定评估独立的特定位置的应用程序和系统。

8. C. TCSEC 定义了 4 种主要类别：类别 A 是经过验证的保护，类别 B 是强制性的保护，类别 C 是自主性的保护，类别 D 则是最小化的保护。

9. C. TCB 是你信任的可以支持和实施安全策略的系统部分。

10. A 和 B. 虽然根据本章介绍的内容，此处最正确的答案是选项 B，但是选项 A 在物理安全上下文中也是正确答案。

11. C. 引用监视器在授予请求访问权之前验证对每个资源的访问。选项 D——安全内核——是协力工作以实现引用监控器功能的 TCB 组件的集合。换句话说，安全内核是引用监控器概念的实现。选项 A 和 B 不是有效的 TCB 概念组件。

12. B. 选项 B 是唯一一个正确定义安全模型的选项。选项 A、C 和 D 分别定义了部分安全策略、认证和鉴定过程。

13. D. Bell-LaPadula 模型和 Biba 模型都建立在状态机模型的基础之上。

14. A. 只有 Bell-LaPadula 模型解决了数据的机密性问题。Biba 和 Clark-Wilson 模型解决的是数据的完整性问题。Brewer and Nash 模型则防止利益冲突。

15. C. 不能向上读的属性也被称为简单安全策略，它禁止主体读取位于更高安全级别的客体。

16. B. 隐蔽通道是用于秘密传送数据的任何方法，此类通道通常不用于通信。其他所有选项描述的都是一般的通信通道。

17. D. 解除分类是一旦确定不再被证明被放置在较高级别时，将对象移动到较低级别分类的过程。只有受信任的主体才能执行解除分类，因为此操作违反 Bell-LaPadula 的星属性规则，而不是违反精神或意图，这是为了防止未授权的泄露。

18. B. 访问控制矩阵将来自多个对象的 ACL 组合到单个表中。该表的行是这些对象主体的 ACE，因此是功能列表。

19. C. 可信计算基(TCB)在理论上具有被称为引用监视器的组件，其在实现中被称为安全内核。

20. C. Clark-Wilson 模型的访问控制关系的三个部分(即访问三元组)是主体、客体和程序(或接口)。

第 9 章　安全脆弱性、威胁和对策

1. C. 多任务处理指同时处理多个任务。在大多数情况下，多任务处理实际上是由操作系统模拟出来的，即使处理器不支持这种技术也是如此。

2. B. 移动设备管理(MDM)是一种软件解决方案，用于管理无数员工使用的访问公司资源的移动设备，这个任务是具有挑战性的。MDM 的目标是提高安全性，提供监控、启用远程管理和支持故障排除。并非所有移动设备都支持可移动存储，甚至只有少量的支持加密可移动存储。地理标记用于标记照片和社交网络帖子，而不是用于 BYOD 管理。应用程序白名单可能是 BYOD 管理的一个元素，但仅是完整的 MDM 解决方案的一部分。

3. A. 单处理器系统一次只能处理一个线程。此题中一共有 4 个应用程序线程(忽略由操作系统创建的线程)，但是操作系统会负责决定任意给定时间在处理器上所运行的线程。

4. A. 在专用系统中，所有用户都必须具有最高级别的、由系统处理的信息的有效安全许可，每个用户都必须被批准访问系统所处理的全部信息，并且都必须具有有效的、对系统所处理全部信息的“知其所需”权限。

5. C. 由于嵌入式系统是控制物理世界的一种机制，因此安全漏洞可能会对人和财产造成伤害。这通常在标准 PC 中不会发生。电源丢失、访问互联网和软件缺陷是嵌入式系统和标准 PC 都有的安全风险。

6. B. 可编程只读存储器(PROM)芯片由终端用户写入一次数据，但是无法再被擦除。在工厂的时候，只读存储器(ROM)芯片的内容就已被“烧入”，而且不允许终端用户写入数据。EPROM 和 EEPROM 芯片都允许终端用户通过某种方法擦除存储设备上的内容并向芯片重新写入新的数据。

7. C. 通过暴露在高强度的紫外线下，EPROM 上的数据可以被擦除。ROM 和 PROM 芯片不提供可擦写的功能。通过对芯片的插脚应用电流，EEPROM 芯片的数据可以被擦除，并且在擦除数据之前不需从计算机上卸下芯片。

8. C. 辅助存储器是一个用于描述磁性和光学介质的术语。这些设备从计算机上拆除后仍然保留着数据内容，并且可以被其他用户读取。

9. B. 笔记本电脑丢失或被盗的风险是数据丢失，而不是系统本身的损失。因此，保持系统上只有最小敏感数据是降低风险的唯一方法。硬盘加密、电缆锁和强密码虽然是好的想法，但只是预防工具，而不是降低风险的手段。它们不会阻止故意和恶意数据泄漏的发生；相反，它们鼓励诚实的人保持诚实。

10. A. 动态 RAM 芯片上有很多电容器，每个电容器上都存有电荷。为了保存芯片上的内容，这些电容器必须不断地被 CPU 刷新。当电源被切断的时候，存储在芯片中的数据就会丢失。

11. C. USB 闪存设备很容易被卸下，并且操作系统往往不太可能对其应用访问控制。因此，加密通常是除了物理安全之外的唯一安全措施，并且费用也完全能够承担。硬盘和 RAM 芯片一般通过操作系统的访问控制来实现安全性。

12. B. 在系统高级模式中，所有用户都必须具有对系统处理的所有信息的适当安全许可和访问特权，但是只需对系统处理的部分信息具有“知其所需”权限。

13. C. 移动电话窃听最常被忽视的方面与在附近偷听对话(至少在他们的一方)的人有关。组织经常考虑和解决无线网络、存储设备加密和屏幕锁定的问题。

14. B. 为了便于将来固件的更新，BIOS 和设备固件通常被存储在 EEPROM 芯片上。

15. C. 寄存器是很小的、直接位于 CPU 芯片上的存储位置。CPU 能够直接使用存储在寄存器上的数据，并且可以很快进行存取。

16. B. 在立即寻址中，CPU 实际上并不需要从存储器中检索任何数据。数据就包含在指令本身中，并且可以被立刻处理。

17. D. 在间接寻址中，提供给 CPU 的存储位置包含了一个内存地址。CPU 通过从这个内存地址进行读取得到操作数(这就是称为“间接”的原因)。

18. C. 进程隔离为在系统中运行的每个进程都提供独立的内存空间。这就阻止进程覆盖其他进程的数据，并确保该进程不会读取另外一个进程的数据。

19. D. 最小特权原则描述的是，只有完全需要内核级别访问特权的进程才能在监管模式中运行。其余的进程应当在用户模式中运行，以便减少潜在安全脆弱性的数量。

20. A. 硬件分隔与进程隔离所要达到的目的是相同的，但硬件分隔是在硬件上使用物理控制方法实现更高级别的安全性。

第 10 章　物理安全需求

1. A. 物理安全是整体安全最重要的方面。如果缺乏物理安全，那么安全性的其他方面都无法得到保证。

2. B. 关键路径分析可以被用于制定组织对新设施的需求。关键路径分析是确定关键任务应用、处理、操作和所有支撑要素之间的关系的过程。

3. B. 配线间是经常位于跨多个楼层相同位置的基础设施部件，以便提供将基于楼层的网络连接和集中一起以提供便利的方法。

4. D. 对于设施内所有场所的等同访问并不是安全所关注的设计要素。每个包含不同重要程度、价值和机密性的资产或资源的区域应当具有相应的安全限制等级。

5. A. 为了保持有效性和安全性，计算机机房不需要与人相协调。与人不协调的服务器机房提供了对攻击的更高的保护等级。

6. C. 散列不是关于包含可重用移动介质存储设施实现的典型安全措施。当需要验证数据集的完整性时可以使用散列，而应该删除不保留可重用移动介质上的数据。通常，介质存储设施的安全特性包括使用库管员或保管人，使用存入/取出过程，以及在返回的介质上使用净化工具。

7. C. 陷阱是通常由保安保护的双重门设置，被用来限制主体，直至其身份得到确认与验证。

8. D. 照明是最常见的一种边缘安全设备或机制。你的整个场所都应该被照亮。照明使得对人员的身份标识更容易，并且更容易注意到入侵行为的发生。

9. A. 保安通常不知道设施内的工作范围，这种做法可以提供机密性，并且有助于降低保安涉及机密信息泄漏的可能性。

10. B. 基于水的灭火系统最常见的故障原因是人为错误。如果在火灾后关闭了水源，随后又忘记再次打开水源，那么在将来发生火灾时就会遇到麻烦。此外，在没有火灾时触发放水也会使办公场所遭受损失。

11. C. 钥匙锁是物理访问控制设备的最常见和最廉价形式。照明、保安和栅栏的费用要高得多。

12. D. 电容运动探测仪对被监控物体周围区域的电场或磁场的变化进行探测。

13. A. 不存在预防性的警报。警报通常由于探测到入侵或攻击而被触发。

14. B. 无论使用何种形式的物理访问控制，都必须部署保安或其他监控系统，以便防止滥用、伪装和混入事件的发生。间谍不能通过物理访问控制进行阻止。

15. C. 人员的安全是所有安全解决方案中最重要的目标。

16. B. 计算机房的理想湿度应该为 40%~60%。

17. D. 1500 伏静电电压可以破坏存储在硬盘驱动器上的数据。

18. A. 因为 B 类灭火器用于液体火灾，所以不能将水用作灭火抑制介质。

19. C. 对于计算机设施来说，预先响应系统是最好的基于水的防火系统。

20. D. 光对于大多数计算机设备来说，通常并无危害，但是火、烟和灭火介质(通常是水)都是有害的。

第 11 章　网络安全架构与保护网络组件

1. D. 传输层是第 4 层。表示层是第 6 层。数据链路层是第 2 层。网络层是第 3 层。

2. B. 封装是指在 OSI 栈中向下传送数据时，向数据添加报头和报尾。

3. B. 第 5 层是会话层，管理着单工(单向)、半双工(双向，但是一次只有一个方向可以发送数据)和全双工(双向，数据可以同时沿两个方向传递)通信。

4. B. 由于 10Base-T 非屏蔽双绞线是非屏蔽的，因此对电磁干扰的阻挡最小。细缆(10Base2)和粗缆(10Base5)都是同轴电缆类型，对电磁干扰具有屏蔽作用。

5. D. VPN 用于在潜在不安全的中间网络之间建立连接的安全隧道。内联网、外联网和 DMZ 是网络分段的例子。

6. B. UDP 是作为 IP 分组的有效载荷操作的传输层协议。虽然不是 IP 本身，但依赖于 IP。IPX、AppleTalk 和 NetBEUI 都是 IP 的替代品，因此被标记为非 IP 协议。

7. C. bluejacking 攻击是针对蓝牙的无线攻击，在这种攻击中，最容易受到危害的设备是移动电话。

8. A. 以太网建立在 IEEE 802.3 标准的基础上。

9. B. TCP 包装是一种应用程序，可以作为基本的防火墙来使用，能够对基于用户 ID 或系统 ID 的访问进行限制。

10. B. 封装是多层协议具备的优点，同时也是潜在的危害。

11. C. 状态检测防火墙能够为已授权的用户和活动授予更广泛的访问权限，并且可以积极地监视和阻止非授权的用户和活动。

12. B. 状态检测防火墙被认为是第三代防火墙。

13. B. 大多数防火墙提供了扩展的日志记录、审计和监控功能以及警报和基本的 IDS 功能。防火墙不能阻止借助其他已授权通信信道传送的病毒或恶意代码，不能防止未授权的、但是由用户无意或有意造成的信息泄漏，不能防范防火墙之后的恶意用户所进行的攻击，也不能在数据离开或进入专用网络之后对数据进行保护。

14. C. 动态的路由协议有很多，包括 RIP、OSPF 和 BGP，但 RPC 不是路由协议。

15. B. 交换机是智能集线器。由于交换机知道连接到每个出站端口的系统的地址，因此它被认为是智能的。

16. A. 无线应用协议(WAP)是一种与移动电话访问互联网相关联的技术，与 802.11 无线网络连

接没有关联。

17. C. 正交频分复用(OFDM)能够提供很高的吞吐量，而且干扰最小。OSPF 不是无线频率访问方法，而是一种路由协议。

18. A. 端点安全是一种安全概念，鼓励管理员在每台主机上安装防火墙、恶意软件扫描程序和 IDS。

19. C. 逆向地址解析协议(RARP)将物理地址(MAC 地址)解析为逻辑地址(IP 地址)。

20. C. 当无线网络被设计为通过使用单个 SSID 和许多接入点来支持大型物理环境时，就会部署企业外延基础设施模式。

第 12 章　安全通信和网络攻击

1. B. 帧中继是第 2 层连接机制，它使用分组交换技术在通信端点之间建立虚电路。帧中继网络是一种共享介质，提供点对点通信的虚电路就被创建在这种介质中。所有虚电路都是独立的，并且彼此不可见。

2. D. 由于系统之间没有通信发生，并且没有中间网络存在，因此独立系统不需要隧道技术。

3. C. IP 安全性(IPSec)是一种基于标准的机制，它能够为点对点的 TCP/IP 通信传输提供加密。

4. B. 169.254.x.x 子网位于 APIPA 范围内，它未在 RFC 1918 中定义。在 RFC 1918 中定义的是 10.0.0.0~10.255.255.255、172.16.0.0~172.31.255.255 和 192.168.0.0~192.168.255.255。

5. D. 要建立 VPN 链路，中间网络连接是必需的。

6. B. 需要通过静态模式的 NAT 来允许外部实体启动与 NAT 代理之后的内部系统的通信。

7. A、B 和 D. L2F、L2TP 和 PPTP 自身都缺少数据加密。只有 IPSec 自身包含数据加密。

8. D. IPSec 在 OSI 模型的网络层(第 3 层)上工作。

9. A. 地址范围 169.172.0.0~169.191.255.255 不是 RFC 1918 中列出的公共 IP 地址范围。

10. D. NAT 并不预防和阻止穷举攻击。

11. B. 当透明性成为服务、安全控制或访问机制的一种特征时，它对于用户来说是不可见的。

12. B. 虽然可用性通常是安全性的主要方面，但它是用于在互联网上传输电子邮件的安全系统中最不重要的方面。

13. D. 在与终端用户讨论关于电子邮件保留的问题时，备份方法不是重要的因素。

14. B. 邮件炸弹是利用电子邮件发起攻击的机制，通过使系统由于邮件信息而泛洪溢出，进而导致拒绝服务。

15. B. 由于邮件信息的源地址通常是欺骗地址，因此通常难以阻止。

16. B. 永久虚电路(PVC)能够被描述为始终存在的逻辑电路，并且随时等待客户发送数据。

17. B. 更改 PBX 系统上的默认密码能够最有效地增强安全性。

18. C. 社会工程学经常用于避开最有效的物理和逻辑控制。无论实际的活动是什么，攻击者都使受害者相信并指示其做一些事情，通常是指示打开后门，从而使攻击者利用后门获得网络的访问权限。

19. C. 暴力攻击不被视为 DoS。

20. A.密码验证协议(PAP)是 PPP 的标准化认证协议。PAP 以明文的方式传输用户名和密码。它不提供任何形式的加密。它只是提供了一种将登录凭据从客户端传输到身份认证服务器的方法。

第 13 章　管理身份与认证

1. E. 所有的答案都包含在组织尝试使用访问控制保护的资产类型中。

2. C. 主体始终是接收客体相关信息或来自客体数据的实体。主体还是更改客体相关信息或客体内存储数据的实体。客体始终是提供或驻留数据、信息的实体。主体可以是用户、程序、进程、文件、计算机和数据库等。当两个实体为完成任务进行通信时，主体和客体的角色可以切换

3. A. 部署预防性访问控制能够防止发生不必要的或未授权的活动。检测控制在活动发生之后发现它们，纠正控制试图纠正由活动引起的任何问题。权威不是有效的访问控制类型。

4. B. 逻辑/技术性访问控制是用于管理对资源和系统的访问以及为这些资源和系统提供保护的硬件或软件机制。行政控制是管理控制，物理控制使用物理方法来控制物理访问。预防性控制尝试防止安全事件。

5. A. 控制资产获取的主要目标是防范损失，包括任何机密性损失、可用性损失或完整性损失。主体在系统上进行身份认证，但客体不进行身份认证。主体访问客体，但客体不访问主体。识别和认证作为访问控制的第一步很重要，但需要更多的措施来保护资产。

6. D. 用户使用登录 ID 来声明身份。登录 ID 和密码的组合提供身份认证。主体在认证后被授权访问客体。记录和审计提供可问责性。

7. D. 可问责性不包括授权。可问责性需要适当的识别和认证。认证后，可问责制需要日志记录以支持审计。

8. B. 密码历史记录可以防止用户在两个密码之间轮换。它记住以前使用的密码。密码复杂性和密码长度有助于确保用户创建强密码。密码年龄可确保用户定期更改密码。

9. B. 密码短语是一个很容易记住的长字符串，例如 IP@$$edTheCISSPEx@m。它不短并且通常包括所有 4 组字符类型。它的强大和复杂，使它很难破解。

10. A. 类型 2 认证因素基于你拥有什么，例如智能卡或令牌设备。类型 3 认证是基于你是什么，有时是你做的，它使用物理和行为生物测定方法。类型 1 身份认证基于你知道什么，例如密码或 PIN。

11. A. 同步令牌生成并显示与认证服务器同步的一次性密码。异步令牌使用挑战-响应过程来生成一次性密码。智能卡不生成一次性密码，通用访问卡是包含用户图片的智能卡版本。

12. B. 诸如指纹和虹膜扫描的物理生物测定方法为主体提供认证。账户 ID 提供标识。令牌是你拥有的，它创建一次性密码，但它与物理特性无关。个人识别码(PIN)是你知道的。

13. C. 生物特征类型1错误(错误拒绝率)和类型2错误(错误接受率)相等的点是交叉错误率(CER)。较低的 CER 表示较高质量的生物测定设备。它不表示灵敏度太高或太低。

14. A. 当一个有效主体未被认证时，发生类型 1 错误(错误拒绝或错误否定)。当无效主体被认证时，发生类型 2 错误(错误接受或错误肯定)。交叉误差率(也称为相等误差率)将类型 1 错误与类型 2 错误的比率进行比较，并提供生物测定系统的精度测量。

15. C. Kerberos 的主要目的是认证，因为它允许用户证明他们的身份。它还使用对称密钥加密来提供机密性和完整性的度量，但这些不是主要目的。Kerberos 不包括日志记录功能，因此它不提供可问责性。

16. D. SAML 是一个基于 XML 的框架，用于在联合身份管理系统内的组织之间交换单点登录(SSO)的用户信息。Kerberos 在单个组织而不是联盟中支持 SSO。HTML 仅描述数据的显示方式。可以使用 XML，但它需要重新定义已在 SAML 中定义的标记。

17. B. 网络访问服务器是 RADIUS 架构中的客户端。RADIUS 服务器是认证服务器，提供认证、授权和计费(AAA)服务。网络访问服务器可能启用了主机防火墙，但这不是主要功能。

18. B. Diameter 基于 RADIUS，它支持移动 IP 和 IP 语音。诸如联合身份管理系统的分布式访问控制系统不是特定协议，并且它们不一定提供认证、授权和计费。TACACS 和 TACACS +是 AAA 协议，但它们是 RADIUS 的替代，不基于 RADIUS。

19. D. 最小特权原则遭到违反，因为他保留了他以前在不同部门的所有行政职位的特权。隐式拒绝确保只允许明确授予的访问权限，但是明确授予管理员权限。虽然管理员的操作可能导致可用性的损失，但可用性的损失不是一条基本原则。防御性特权不是有效的安全原则。

20. D. 账户审查可以发现用户何时具有比他们所需的更多的权限，并且可以用于发现此员工拥有来自多个位置的权限。强认证方法(包括多因素认证)不会阻止这种情况下的问题。记录可能记录了活动，但需要进行审查以发现问题。

第 14 章　控制和监控访问

1. B. 隐式拒绝原则确保对对象的访问被拒绝，除非已明确允许(或明确授予)对主体的访问权。它不允许所有未被拒绝的操作，并且不要求拒绝所有操作。

2. C. 最小特权原则确保用户(主体)只获得他们执行其工作任务和工作职能所需的最严格的权限。用户不执行系统进程。最小特权原则不强制实施最低限制性的权限，而是最严格的权限。

3. B. 访问控制矩阵包括多个对象，并且其列出主体对每个对象的访问。访问控制矩阵内的任何特定对象的单个主体列表是访问控制列表。联合是指共享用于单点登录的联合身份管理系统的一组公司。蠕变特权是指受试者随着时间过去收集的过度特权。

4. D. 数据保管人(或所有者)在自由访问控制(DAC)模型中向用户授予权限。管理员为其拥有的资源授予权限，但不授予 DAC 模型中所有资源的权限。基于规则的访问控制模型使用访问控制列表。强制访问控制模型使用标签。

5. A. 自主访问控制模型是基于身份的访问控制模型。它允许资源的所有者(或数据保管人)在所有者的判断下授予权限。基于角色的访问控制模型基于角色或组成员资格。基于规则的访问控制模型基于其中规则的 ACL。强制访问控制模型使用分配的标签来标识访问。

6. D. 非自主访问控制模型使用中央权威来确定用户(和其他主体)可以访问哪些对象(例如文件)。相反，自由访问控制模型允许用户授予或拒绝访问他们拥有的任何对象。ACL 是一种基于示例或基于规则的访问控制模型。访问控制矩阵包括多个对象，并且其列出主体对每个对象的访问。

7. D. 基于角色的访问控制模型可以基于组织的层次结构，将用户分组到角色，它是一个非自主的访问控制模型。非自主访问控制模型使用中央权威来确定受试者可以访问哪些对象。相反，自由访问控制模型允许用户授予或拒绝访问他们拥有的任何对象。ACL 是使用规则(而不是角色)的基于规则的访问控制模型示例。

8. A. role-BAC 模型基于角色或组成员资格，用户可以是多个组的成员。用户不仅限于单个角色。role -BAC 模型基于组织的层次结构，因此它们是基于层次结构的。强制访问控制模型使用分配的标签来标识访问。

9. D. 开发者在基于角色的访问控制模型中是有效的角色。管理员可以将开发者的用户账户置于开发者角色，并为该角色分配权限。角色通常用于组织用户，其他答案不是用户。

10. D. 基于规则的访问控制模型使用适用于所有用户和其他主体的全局规则。它不会在本地应用规则，或应用于个人用户。

11. C. 防火墙使用基于规则的访问控制模型，其中规则在访问控制列表中表示。强制访问控制模型使用标签。自主访问控制模型允许用户分配权限。基于角色的访问控制模型按组组织用户。

12. C. 强制访问控制依赖于对主体和客体使用标签。非自主访问控制系统允许客体的所有者控制对客体的访问。非自主访问控制可以集中管理，例如部署在防火墙上的基于规则的访问控制。基于角色的访问控制基于任务相关角色定义主体的访问。

13. D. 强制访问控制模型是禁止的，它使用隐式否认理念(不是显式否认理念)。它不是允许的，以及它使用标签而不是规则。

14. D. 基于 Lettuce 的访问控制模型不是有效类型的访问控制模型。其他答案列出了有效的访问控制模型。基于网格(不基于 Lettuce 的)访问控制模型是一种强制访问控制模型。

15. C. 漏洞分析标识漏洞，可以包括定期漏洞扫描和渗透测试。资产评估决定资产的价值，而不是弱点。威胁建模试图识别威胁，但威胁建模不能识别弱点。访问审查审计账户管理和对象访问实践。

16. B. 账户锁定策略将在用户输入错误的密码太多次后锁定账户，这会阻止在线暴力攻击。攻击者在离线密码攻击中使用彩虹表。密码盐降低彩虹表的效果。加密密码保护密码，但不能防止暴力攻击。

17. B. 旁路攻击是一种被动的、非入侵的攻击，用于观察设备的运行，并且可以用于对某些智能卡的检测。方法包括电源监视、定时和故障分析攻击。捕鲸是一种针对高级管理人员的网络钓鱼攻击。暴力攻击试图通过使用所有可能的字符组合来发现密码。彩虹表攻击用于破解密码。

18. C. 捕鲸是一种针对高级管理人员的网络钓鱼形式。鱼叉式网络钓鱼针对特定群体，但不一定是高级管理人员。钓鱼是一种通常使用 IP 语音(VoIP)的网络钓鱼形式。

19. B. 威胁建模有助于识别、理解和分类潜在的威胁。资产评估确定资产的价值，脆弱性分析确定了可以被威胁利用的弱点。访问审查和审计可确保账户管理实践支持安全策略。

20. A. 资产评估确定资产的实际价值，以便确定优先顺序。这将确保顾问专注于高价值资产。威胁建模识别威胁，但应首先进行资产评估，以便关注高价值资产的威胁。脆弱性分析确定弱点，但应注重高价值资产。审计跟踪可用于重新创建导致事故的事件，但如果尚未创建事件，则现在创建它们将无济于事，除非组织再次受到攻击。

第 15 章　安全评估和测试

1. A. nmap 是一种网络发现扫描工具，它报告远程系统打开的端口。

2. D. 只有开放端口代表潜在的重大安全风险。端口 80 和 443 预先在 Web 服务器上打开。端口 1433 是数据库端口，不应暴露给外部网络。

3. C. 存储在系统上的信息的敏感性、执行测试的难度和攻击者针对系统的可能性都是计划安全测试任务时的有效考虑因素。尝试新测试工具的需求不应影响生产测试计划。

4. C. 安全评估包括旨在识别漏洞的许多类型的测试，评估报告通常包括缓解建议。然而，评估并不包括实际缓解这些漏洞。

5. A. 安全评估报告应提交给组织的管理层。因此，它们应该用简明的语言来写，并避免技术

术语。

6. B. 使用 8 位子网掩码意味着 IP 地址的第 1 个 8 位字节表示网络地址。在这种情况下，这意味着 10.0.0.0/8 将扫描以 10 开头的任何 IP 地址。

7. B. 服务器可能在端口 80 上运行网站。使用 Web 浏览器访问网站可能会提供有关网站意图的重要信息。

8. B. SSH 协议使用端口 22 来接受与服务器的管理连接。

9. D. 经过身份认证的扫描可以从目标系统读取配置信息，并减少假阳性和假阴性的报告实例。

10. C. TCP SYN 扫描发送 SYN 分组并接收 SYN ACK 分组作为响应，但它不发送完成三次握手所需的最终 ACK。

11. D. SQL 注入攻击是 Web 漏洞，并且 Matthew 最好由 Web 漏洞扫描程序提供服务。网络漏洞扫描程序也可能会检测到此漏洞，但是 Web 漏洞扫描程序是专门为此任务设计的，并且更有可能成功。

12. C. PCI DSS 要求 Badin 至少每年并在应用程序发生任何更改后重新扫描应用程序。

13. B. Metasploit 是一个自动化的利用工具，允许攻击者轻松执行常见的攻击技术。

14. C. 变异模糊测试使用比特翻转和其他技术来略微修改程序的先前输入，以试图检测软件缺陷。

15. A. 滥用案例测试识别攻击者可能利用系统并明确测试以查看这些攻击在提议的代码中是否可能的已知方式。

16. B. 用户界面测试包括对软件程序的图形用户界面(GUI)和命令行界面(CLI)的评估。

17. B. 在白盒渗透测试期间，测试人员可以访问有关被测系统的详细配置信息。

18. B. 默认情况下，未加密的 HTTP 通信在 TCP 端口 80 上进行。

19. C. Fagan 检查过程在后续行动阶段结束。

20. B. 备份验证过程确保备份正常运行，从而满足组织保护数据的目标。

第 16 章 管理安全运营

1. C. “知其所需”是获取、了解或拥有以执行特定工作任务所要求的数据，而不是更多数据。最小特权原则包括权限和许可，但是术语“最小特权原则”在 IT 安全中无效。职责分离确保个人不控制所有元素的过程。基于角色的访问控制是基于角色授予对资源的访问权限。

2. D. 默认访问级别应为无访问权限。最小特权原则指示用户应该仅被授予他们完成工作所需的访问级别，并且问题不指引新用户需要任何访问。读取访问、修改访问和完全访问授予用户某种级别的访问，这违反了最小特权的原则。

3. C. 职责分离策略阻止单个人控制所有元素的过程，并且当应用安全设置时，它可以防止单个人在没有援助的情况下进行主要的安全变更。岗位轮换有助于确保多个人执行相同的工作，并可以帮助防止单个人离开时丢失信息。让员工集中聪明才智与职责分离无关。

4. B. 岗位轮换和职责分离策略有助于防止欺诈。共谋是多个人之间执行某些未授权或非法行为的协议，并且实施这些策略有助于防止欺诈。它们不能防止串通，当然不是为了鼓励员工与组织勾结。它们帮助阻止和防止事件，但它们不纠正它们。

5. A. 岗位轮换策略使员工轮换岗位或工作职责，并可帮助检测共谋和欺诈的发生。职责分离

策略确保单个人不控制特定职能的所有要素。强制性休假策略确保员工较长时间离开工作，需要其他人履行工作职责，这增加了发现欺诈的可能性。最小特权确保用户仅具有执行其作业所需的权限，而没有更多的权限。

6. B. 强制性休假策略有助于检测欺诈。他们要求员工较长时间离开工作，要求其他人履行他们的工作职责，这增加了发现欺诈的可能性。它不会轮换工作职责。虽然强制性休假可能有助于员工降低总体压力水平，从而提高生产力，但这并不是强制性休假策略的主要原因。

7. A、B 和 C. 岗位轮换、职责分离和强制性休假策略都有助于减少欺诈。基线用于配置管理，并且不会帮助减少串通或欺诈。

8. B. 不应该向管理员和操作员授予相同特权。相反，应该仅向个人授予他们执行工作所需的特权。特殊权限需要特殊访问或提升权限，以执行管理和敏感工作任务。应该监视这些权限的分配和使用情况，并且只应向受信任的个人授予访问权限。

9. A. 服务级别协议指明诸如供应商的第三方责任，并且如果供应商不担负所述的责任，则可以处以罚金。MOU 是非正式协议，不包括罚款。ISA 定义了建立、维护和断开连接的需求。SaaS 是基于云的服务模型之一，不指定供应商责任。

10. C. 系统在其生命周期结束时应进行净化，以确保它们不包括任何敏感数据。删除 CD 和 DVD 是净化过程的一部分，但是还应检查系统的其他元素(例如磁盘驱动器)，以确保它们不包含敏感信息。除非组织的净化过程需要删除软件许可证或安装原始软件，否则不一定需要。

11. A. 有价值的资产需要多层次的物理安全，并且将数据中心放置在建筑物的中心有助于提供这些额外的保护层。将有价值的资产放置在外墙附近(包括建筑物后部)会消除一些安全层。

12. D. VM 需要单独更新，就像它们在物理服务器上运行一样。对物理服务器的更新不会更新托管的 VM。同样，更新一个 VM 不会更新所有 VM。

13. A. 在租赁 IaaS 云资源时，组织对维护和安全负有最大的责任。云服务提供商提供 PaaS 模型时承担更多责任，提供 SaaS 模型时承担最大责任。CaaS 不是基于云的服务模型的有效名称。

14. C. 社区云部署模型向两个或多个组织提供基于云的资产。公共云模型包括可供任何消费者出租或租赁的资产。私有云部署模型包括单个组织的基于云的资产。混合模型包括两个或多个部署模型的组合。

15. B. 磁带应该被清除，确保无法被任何已知方法恢复数据。即使磁带可能在它们的生命周期结束，它们仍然可以保存数据，并且在将它们丢弃之前应该被清洗。擦除不会从介质中删除所有可用的数据，但是清洗可以。如果磁带在生命周期结束时，则不需要存储磁带。

16. B. 映像可以是使用基线的有效配置管理方法。映像可确保系统以相同的已知配置进行部署。变更管理过程有助于防止擅自更改的中断。漏洞管理过程有助于识别漏洞，补丁管理过程有助于确保系统保持最新。

17. A. 变更管理过程可能需要暂时绕过以应对紧急情况，但不应该只是因为有人认为可以提高性能而绕过它们。即使在紧急情况下实施变更，也应在事件发生后记录和审查。请求更改、创建回滚计划和记录更改都是变更管理过程中的有效步骤。

18. D. 变更管理过程将确保在实施变更之前对变更进行评估，以防止意外中断或不必要地削弱安全性。补丁管理确保系统是最新的，漏洞管理检查已知漏洞的系统，配置管理确保系统被相似地部署，但这些其他流程不会阻止未授权的变更。

19. C. 只应部署所需的补丁程序，组织将不会部署所有补丁程序。相反，组织会评估补丁以确定需要哪些补丁，测试它们并且确保它们不会导致意外问题，部署已批准和已测试的补丁，并审核

系统以确保已应用了补丁。

20. B. 漏洞扫描程序用于检查系统中的已知问题，并且是整体漏洞管理程序的一部分。版本控制用于跟踪软件版本，与检测漏洞无关。安全审计和审查有助于确保组织遵守其策略，但不会直接检查系统的漏洞。

第 17 章　事件预防和响应

1. A. 遏制是检测和验证事件后的第一步。这限制了事件的影响或范围。组织根据策略和治理法律来报告事件，但这不是第一步。修复尝试识别事件的原因和可以采取的步骤来防止事件重复发生，但这也不是第一步。重要的是在试图遏制事件时保护证据，但收集证据将在遏制后发生。

2. D. 安全人员在修复阶段执行根本原因分析。根本原因分析尝试发现问题的根源。在发现原因之后，审查将经常确定一种解决方案，来帮助防止将来发生类似事件。包含事件和收集证据是在事件响应过程的早期完成的。在恢复阶段可能需要重建系统。

3. A、B 和 C. 泪滴、smurf 和死亡 Ping 都是 DDoS 攻击的类型。攻击者使用欺骗在各种攻击中隐藏他们的身份，但欺骗不是攻击本身。

4. C. SYN 泛洪攻击通过从不发送第三个包来中断 TCP 三次握手过程。它不是任何特定的唯一的操作系统，如 Windows。smurf 攻击使用放大网络来泛洪受害者的数据包。死亡攻击使用超大的 ping 数据包。

5. B. 零日漏洞利用了以前未知的漏洞。僵尸网络是由僵尸牧人控制的一组计算机，可以发起攻击，但他们可以利用已知的漏洞和以前未知的漏洞。类似地，拒绝服务(DoS)和分布式 DoS(DDoS)攻击可以使用零日漏洞或使用已知的方法。

6. A. 在提供的选项中，偷渡式下载是最常见的恶意软件分发方法。 USB 闪存驱动器可用于分发恶意软件，但此方法不如偷渡式下载常见。Ransomware 是一种恶意软件感染，不是分发恶意软件的方法。如果用户能够安装未经批准的软件，他们可能会无意中安装恶意软件，但这不是最常见的方法。

7. A. IDS自动检查审计日志和实时系统事件来检测和显示未授权系统访问的异常活动。虽然IDS可以检测系统故障和监视系统性能，但它们不包括诊断系统故障或评估系统性能的能力。漏洞扫描程序用于测试系统的漏洞。

8. B. HIDS 监视单个系统以寻找异常活动。基于网络的 IDS(NIDS)监视网络上的异常活动。HIDS 通常作为系统上正在运行的进程可见，并向授权用户提供警报。HIDS 可以检测恶意代码，类似于反恶意软件如何检测恶意代码。

9. B. 蜜罐是单独的计算机，并且蜜网是被创建用于入侵者的陷阱的整个网络。它们看起来像合法的网络，诱骗入侵者有未打补丁和未受保护的安全漏洞，以及有吸引力和诱人但虚假的数据。入侵检测系统(IDS)将检测攻击。在某些情况下，IDS 可以将攻击者转移到填充单元，这是一个模拟环境，用假数据保持攻击者兴趣。伪缺陷(由许多蜜罐和蜜网使用)是有意植入系统中以诱骗攻击者的错误漏洞。

10. C. 多个解决方案提供了最佳解决方案。这涉及在几个位置(诸如在互联网和内部网络之间的边界处，在电子邮件服务器以及每个系统上)部署反恶意软件。不推荐在单个系统上使用多个反恶意软件应用程序。整个组织的单一解决方案通常是无效的，因为恶意软件可以以多种方式进入网络。

边界网关(互联网和内部网络之间的边界)上的内容过滤是一个很好的部分解决方案，但它不会捕获通过其他方法带入的恶意软件。

11. B. 渗透测试应该在管理人员知情和同意的情况下进行。未经批准的安全测试可能会导致生产力损失，触发应急响应小组，并对测试者采取法律行动，包括失业。渗透测试可以模仿以前的攻击，并使用手动和自动攻击方法。在渗透测试之后，可以重新配置系统以解决发现的漏洞。

12. B. 通过监视主体和客体的活动以及维护操作环境和安全机制的核心系统功能来维护可问责性。有效监控需要认证，但它本身不提供可问责性。如果输入错误的密码次数过多，账户锁定会阻止登录到账户。用户权利审核可以识别过多的权限。

13. B. 审计跟踪是一种被动形式的侦探安全控制。行政控制是管理实践。纠正控制可以纠正与事件相关的问题，物理控制是可以接触的控制。

14. B. 审计是对环境系统检查或审查的方法，确保遵守法规、检测异常、未授权的事件或直接的犯罪。渗透测试试图利用漏洞。风险分析试图基于已识别的威胁和漏洞来分析风险。诱骗是欺骗某人进行非法或未授权的行为。

15. A. 阈值是非统计抽样的一种形式，根据限幅水平阈值减少记录数据的量。抽样是一种从审计日志中提取有意义数据的统计方法。日志分析审查查找趋势、模式和异常或未授权事件的日志信息。警报触发是在发生特定事件或阈值时向管理员发送的通知。

16. B. 流量分析更侧重于数据的模式和趋势，而不是实际内容。按键监视记录特定按键来捕获数据。事件日志记录特定事件以记录数据。安全审计记录安全事件和/或审查日志以检测安全事件。

17. B. 用户权利审核可以检测用户何时具有比所需权限更多的权限。账户管理实践尝试确保权限被正确分配。审计检查是否遵循了管理实践。记录日志活动，但是需要检查日志以确定是否遵循实践。报告是审计的结果。

18. D. 保安应该收集证据，以便可能起诉攻击者。检测和验证事件后的第一个响应是包含事件，但可能已被包含而不重新启动服务器。经验教训阶段包括审查，这是最后阶段。修复包括根本原因分析来确定允许事件的原因，但这在过程的后期完成。在这种情况下，重新启动服务器执行恢复。

19. C. 攻击 IP 地址是最严重的错误，因为它在大多数位置是非法的。此外，由于攻击者经常使用欺骗技术，它可能不是攻击者的实际 IP 地址。重新启动服务器而不收集证据并且不报告事件是错误，但不会对组织产生潜在的持久负面影响。重置连接以隔离事件将是一个很好的步骤，如果没有重新启动服务器的话。

20. A. 管理员没有报告事件，因此没有机会执行经验教训步骤。可能是事件发生了，因为服务器上的漏洞，但没有进行检查，确切的原因不会知道，除非攻击重复。管理员检测到事件并做出响应(虽然不适当)。重新启动服务器是一个恢复步骤。值得一提的是，事件响应计划被保密，服务器管理员无法访问它，因此可能不知道正确的响应应该是什么。

第 18 章　灾难恢复计划

1. C. 一旦灾难中断业务运行，DRP 的目标是尽快恢复正常的业务活动。因此，灾难恢复计划在业务连续性计划停止的地方起作用。

2. C. 电力中断是人为灾难的一种形式。这里列出的其他几种事件(海啸、地震和闪电)都是自然界中的事件。

3. D. 50 个州中的 40 个州被认为具有“中级”、“高级”或“很高”的地震风险。

4. B. 大多数常规业务保险和业主保险策略不提供对洪水或山洪的保护。如果洪水对你的企业构成了风险，那么就应当考虑购买根据 FEMA 的国家洪水灾害保险计划提供的洪水保险。

5. C. 虽然选项中列出的所有行业在 9 • 11 事件后都改变了各自的运营，但是保险业的责任范围被修改为不再包括对 BCP/DRP 过程具有最直接影响的恐怖活动。

6. C. 这个选项的说法反过来就对了：灾难恢复计划在业务连续性计划中止时开始。其他三句话都是业务连续性计划和灾难恢复计划的实际反映。

7. B. 术语“百年洪泛区”被用来描述某个地区每隔一百年出现一次洪水。它还可以被理解为每年只有 1 %的可能性发生洪水。

8. D. 当使用远程镜像的时候，数据库的实际副本是在替代场所进行维护的。通过同时在主场所和远程场所执行所有的事务，可以保持远程数据库副本的实时更新。

9. C. 冗余的系统/组件为某部分硬件出现故障提供了保护。

10. B. 在业务影响评估阶段，必须确定组织业务的优先级，从而帮助进行 BCP 资源的分配。这些相同的信息同样可以用来帮助 DRP 业务单元的优先级排列。

11. C. 冷站点不包含任何恢复运营所需的设备。在开始运营之前，所有的设备都必须进行购买和配置，并且还原其中的数据。这通常需要花费数星期的时间。

12. C. 温站点从宣布灾难开始到启用大约需要 12 个小时的时间。这是为了与立刻就能启用的热站点和使冷站点恢复到运营状态的时间(至少一个星期)进行比较。

13. D. 温站点和热站点都包含恢复运营状态所需的工作站、服务器和通信线路。这两种替代场所之间的主要差别是：热站点中运营数据的副本基本上是实时的，而温站点需要从备份磁带中还原数据。

14. D. 远程镜像是唯一的备份选项，其中远程站点上的活动备份服务器维护主服务器内容的位对位副本，与主系统和远程系统之间链接中的延迟同步一致。

15. A. 执行摘要提供了整个组织灾难恢复工作的高度概括。这份文件对公司的经理和领导以及需要对这种复杂努力有非技术观点的公共关系专家有用。

16. D. 软件托管协议将应用程序的源代码放在独立的第三方手中，这样在开发商不能满足服务级别协议条款或开发商的公司破产时，能够为使用软件的公司提供“安全网”保护。

17. A. 差异备份总是存储那些自从最近一次完整备份以来被修改过的所有文件的副本，无论间隔期内是否创建了增量备份或差异备份，都是如此。

18. C. 任何备份策略都必须包含在备份过程的某一时刻进行完整备份。考虑到每次需要备份的文件数量，增量备份的创建速度比差异备份快。

19. A. 任何备份策略都必须包含在备份过程的某一时刻进行完整备份。如果使用完整备份和差异备份的组合，那么最多还原两份备份。如果使用完整备份和增量备份的组合，那么需要还原的备份数量是无限的。

20. B. 并行测试涉及将人员转移到恢复场所并开始运营，但主运营中心的日常业务仍要保持运作。

第 19 章　事件与道德规范

1. C. 犯罪是任何对法律或法规的违反行为。犯罪条款定义了犯罪的行为。如果违规涉及计算机(作为目标或工具)，那么它就是计算机犯罪。

2. B. 军事和情报攻击针对系统中存在的机密数据。对于攻击者来说，信息的价值证明这样一种攻击是值得的。从这种类型攻击中获得的信息常常被用于计划后续的攻击。

3. A. 与军方或情报机构无关的机密信息是商业攻击的目标，其最终的目标可能是破坏、更改信息，也可能是机密信息的泄漏。

4. B. 财务攻击主要专注于非法获得服务和钱财。

5. B. 恐怖攻击通过营造恐怖的气氛干扰人们的生活。计算机恐怖攻击可以通过降低对同时发生的物理攻击的响应能力来实现这个目标。

6. D. 任何损害组织或个人的行为，不论是直接的还是利用令人为难的事情，都将是恶意攻击的有效目标。这样一种攻击的目标是对某人实行报复。

7. A 和 C. 兴奋攻击除了可以产生骄傲和自负以外，没有任何回报。发动兴奋攻击的兴奋来自于攻击的实际参与(而不是获得利益)。

8. C. 虽然其他答案在单独情况中有一些贴近，但是最重要的规则是永远不要修改或损毁证据。如果修改了证据，那么在法庭上它们是不予承认的。

9. D. 不能拔掉电源的最主要原因是将失去内存中的数据。一定要仔细考虑拔掉电源的正面和负面因素。在考虑所有因素后，才可能是最佳选择。

10. B 和 D. 黑客行动主义者(这个词是黑客和行动主义者的组合)经常将政治动机与黑客的刺激结合在一起。他们将自己松散地组织成名为 Anonymous 和 Lolzsec 的团体，并使用低轨离子炮这样的工具创建大规模的拒绝服务攻击，这只需要很少的知识。

11. D. 事故通常被定义为对数据的机密性、完整性或可用性产生负面影响的任何事件。

12. B. 一些端口扫描是正常的。大量异常的端口扫描行为可能是更危险的攻击之前的侦察活动。当发现异常的端口扫描时，应当始终对其进行调查。

13. A. 在攻击者超越其权限时，这种事故被划分为系统威胁，其中包括合法用户超出自己的权限范围以及非法用户通过使用合法用户的 ID 获得访问权。

14. C. 尽管选项 A、B 和 D 中的行为让你意识到是某种攻击和如何检测它们，但除非你了解自己的系统，否则永远不可能成功地检测出大多数攻击。若你知道你的系统中每天正常的活动是怎样的，就可以立即检测到所有的异常活动。

15. B. 在这道题中，你需要一张搜查证，从而能够在嫌疑人毁掉证据之前没收设备。如果嫌疑人为你的组织工作，并且你拥有所有员工签署的同意协议，那么就能够比较容易地没收这些设备。

16. A. 日志文件中包含了大量无用的信息。但是，当你试图跟踪一个问题或事故的时候，它们的价值可能无法衡量。即使事故在发生的时候被发现，也可能已经被其他事故覆盖。日志文件提供了有价值的线索，并且应当加以保护和归档。

17. A 和 D. 你必须对导致违反法律或规章的事故进行报告。这包括汇报发生的任何损失(以及潜在损失)或者受保护的信息被泄漏。

18. D. 道德规范就是个人行为的规则。许多专业组织都通过制定正规的道德规范来约束自己的员工，但道德规范也是个人用来指导自己行为的规则。

19. B. $(ISC)^2$道德规范准则中的第二个标准描述了 CISSP 应该具有的行为，即行为得体、诚实、公正、负责和遵守法律。

20. B. 在选项 A、C 或 D 中没有明确说明 RFC 1087。尽管列出的每一种类型的行为都是不可接受的，但是只有选项 B 中确定了行为在 RFC 1087 中进行了说明。

第 20 章 软件开发安全

1. A. DevOps 模型的三个要素是软件开发、质量保证和 IT 操作。

2. B. 输入验证确保用户提供的输入与设计参数匹配。

3. C. 请求控制向用户提供请求更改的框架，开发人员有机会优先处理这些请求。

4. C. 在故障保护状态下，系统保持高级别的安全性，直到管理员干预。

5. B. 瀑布模型使用 7 阶段方法进行软件开发，并且包括反馈回路，其允许开发返回到上一阶段以校正在后续阶段发现的缺陷。

6. A. 内容相关的访问控制关注每个字段的内部数据。

7. C. 外键被用于在存在关系的表之间强制实施参照完整性。

8. D. 在这里，数据库用户利用的处理过程是聚合。聚合攻击涉及使用专门的数据库函数组合来自大量数据库记录的信息，最后显示的信息可能比单独记录显示的信息更敏感。

9. C. 多实例准许多条记录的插入，看起来在一个数据库中有相同的主键值(处于不同的分类级别)。

10. D. 在敏捷中，最高优先级通过早期和持续交付有价值的软件来满足客户。

11. C. 专家系统利用包含一系列“if/then”语句的知识库，基于人类专家以前的经验形成决策。

12. D. 在可管理阶段，SW-CMM 的第 4 级，组织使用定量措施来详细了解开发过程。

13. B. ODBC 扮演了应用程序和后端 DBMS 之间代理的角色。

14. A. 为了进行静态测试，测试人员必须访问底层源代码。

15. A. 甘特图是一种条形图，显示项目和计划之间的时间相互关系。它提供了一个时间表的图形说明，这样有助于计划、协调和跟踪项目中的特定任务。

16. C. 污染是来自较高分类级别的数据和/或需知需求与来自较低分类级别的数据和/或需知需求的混合。

17. A. 数据库开发人员使用多实例，创建似乎具有相同主键的多条记录，以防止推理攻击。

18. C. 配置审计是配置管理过程的一部分，而不是更改控制过程的一部分。

19. C. 隔离性原则规定，对相同数据进行操作的两个事务必须在时间上彼此隔离，从而使一个事务不会妨碍另一个事务。

20. B. 表的基数是指表中的行数，而表的度是列数。

第 21 章 恶意代码与应用攻击

1. A. 签名检测机制使用已知的病毒描述来识别驻留在系统上的恶意代码。

2. B. DMZ(非军事区)设计为容纳诸如 Web 服务器的系统，这些系统必须能够从内部和外部网

络访问。

3. B. 检验时间到使用时间(TOCTTOU)攻击依赖于这两个事件的执行时间。

4. D. 应用程序白名单要求管理员指定已批准的应用程序，然后操作系统使用此列表仅允许已知的良好应用程序运行。

5. A. 为了避免基于签名的防病毒软件包的检测，多态病毒在每次感染系统时修改自己的代码。

6. A. LastPass 是一个工具，允许用户为他们使用的每个服务创建独特的、强大的密码，而没有记住它们的负担。

7. D. 缓冲区溢出攻击允许攻击者通过写入超出分配给变量的空间来修改系统内存的内容。

8. D. 除了 D 选项之外，其他选项都是可以在字典攻击中找到的常见词汇。mike 是一个名字，并且很容易被发现。elppa 只是 apple 的反向拼写，而 dayorange 则组合了两个字典词汇。Crack 程序和其他实用程序可以很容易地看穿这些“鬼鬼祟祟的”技术。选项 D 是一个字典攻击不会发现的随机字符串。

9. B. 阴影密码文件将加密的密码信息从公共可读的/etc/passwd 文件移到受保护的/etc/shadow 文件中。

10. D. 单引号字符(')用于 SQL 查询，必须在 Web 表单上仔细处理，以防止 SQL 注入攻击。

11. B. Web 应用程序开发人员应该利用数据库存储过程来限制应用程序执行任意代码的能力。使用存储过程、SQL 语句驻留在数据库服务器上，并且只能由数据库管理员修改。

12. B. 端口扫描能够揭示在计算机上运行的公用服务所使用的端口。

13. A. 只有针对包含反射式输入的 Web 应用程序时，才能成功进行跨站脚本攻击。

14. D. 复合病毒使用两种或更多种传播技术(例如文件感染和引导扇区感染)来最大化它们的传播范围。

15. B. 通过将用户输入限制在预定义的范围内，输入确认能够防御跨站脚本攻击。这种做法能够防止攻击者在输入中包含 HTML <SCRIPT>标记。

16. A. Stuxnet 是一种高度复杂的蠕虫，旨在破坏连接到西门子控制器的核浓缩离心机。

17. B. 后门是未记录的命令序列，允许具有后门知识的个人绕过正常的访问限制。

18. D. Java 沙箱隔离了 applet，并且允许 applet 在受保护的环境内运行，从而限制其可能对系统剩余部分的影响。

19. D. <SCRIPT>标签用于指示可执行的客户端脚本的开头，并用于反射型输入来创建跨站脚本攻击。

20. A. 不允许具有内部源 IP 地址的数据包从外部进入网络，因为它们可能被欺骗。

附录 B

书面实验室答案

第 1 章　通过原则和策略的安全治理

1. CIA 三元组是机密性、完整性和可用性的组合。这个术语用于指示安全解决方案的三个关键组件。

2. 可问责性需要建立在身份标识、身份认证、授权和审计的基础上。为了真正地对某人的行为进行问责，必须合法地支持上述每个组件。

3. 变更控制管理的优点包括：阻止由于非受控变更导致的不希望的安全性降低，记录和跟踪环境、标准化、遵循安全策略中的所有改变，以及在发生不希望的或未预期的事件时能够回滚变化。

4. (1)确定管理人并定义他们的职责。(2)指定如何对信息进行分类和标记的评估标准。(3)对每个资源进行分类和标记。尽管所有者主导这个步骤，但是必须有监督人员进行检查。(4)记录发现的分类策略的所有例外，并且将这些例外集成到评估标准中。(5)选择应用于每个分类级别的安全控制，从而提供必要的保护级别。(6)指定解除资源分类的过程以及将资源的保管权转移给外部实体的过程。(7)创建一个整个企业范围内都知晓的计划，从而指导所有人员对分类系统的使用。

5. 6 种安全角色是：高级管理者、IT/安全人员、数据所有者、数据管理员、操作者/用户以及审计人员。

6. 安全策略的 4 个组成部分是：策略、标准、指导方针以及措施。策略是宏观的安全陈述。标准定义了硬件和软件的安全规范。指导方针在没有适当措施的情况下使用。措施详细指导如何以安全的方式逐步完成工作任务。

第 2 章　人员安全和风险管理概念

1. 可能的答案包括：工作描述、最小特权原则、职责分离、工作职责、岗位轮换/交叉培训、绩效检查、背景调查、工作活动警告、意识培训、工作培训、离职/终止合同面谈、保密协议、竞业禁止协议、雇用协议、隐私声明以及可接受的使用策略。

2. 这些公式是：

SLE = AV * EF

ARO = # / yr

ALE = SLE * ARO

成本/效益= (ALE1 – ALE2) – ACS

3. Delphi 技术是一个匿名反馈和响应过程，用于使组织达成匿名的共识，主要目的是引起所有参与者诚实和不受影响的响应。参与者通常聚集在一间会议室里。对每个请求进行反馈时，每个参与者在纸上匿名写下他们的回答。整理结果并提交给小组进行评估。重复该过程直到达成共识。

4. 风险评估通常涉及使用定量和定性的混合方法。纯粹的定量分析是不可能的；不是所有的分析元素和方面都可以量化，因为一些是定性的，一些是主观的以及一些是无形的。由于不可能进行纯粹的定量风险评估，因此平衡定量分析的结果是必要的。将定量和定性分析结合到组织风险最终评估中的方法被称为混合评估或混合分析。

第 3 章　业务连续性计划

1. 联邦政府、州和地方的许多法律或法规要求业务实现 BCP 预备措施。让法律代表加入 BCP 团队有助于确保遵循法律、规章与合同中的约束。

2. “凭直觉”方式是不愿意花费时间和金钱正常实施 BCP 的人使用的借口。如果没有适当的计划来指导紧急情况下的响应，那么就会导致灾难的发生。

3. 定量风险评估涉及使用数值和公式做出决定。定性风险评估包括非数值因素，例如情感、投资者/客户信心以及员工稳定性。

4. BCP培训计划应当包括针对所有员工的计划概述以及针对直接或间接参与的个人的具体培训。此外，应当为每个关键的BCP角色都培训候补人员。

5. BCP 过程的 4 个步骤为：项目范围和计划编制、业务影响评估、连续性计划、批准/实现。

第 4 章　法律、法规和合规性

1. 个人有权访问与其相关的记录，并且有权知道包括在这些记录中的数据源。他们还有权改正错误的记录。个人有权拒绝处理数据，并且在这些权利被违反时进行法律求助。

2. 组织可能会询问外包服务提供商一些常见问题，如下：

- 由供应商存储、处理或传输什么类型的敏感信息？
- 有什么控制来保护组织的信息？
- 组织的信息如何与其他客户信息隔离？
- 如果依赖加密作为安全控制，使用什么加密算法和密钥长度？如何处理密钥管理？
- 供应商执行什么类型的安全审核，客户对这些审核有什么样的访问？
- 供应商是否依赖任何其他第三方存储、处理或传输数据？与安全相关的合同条款如何扩展到第三方？
- 数据存储、处理和传输发生在哪里？如果在客户和/或供应商的本国以外，这有什么影响？

- 供应商的事件响应流程是什么，客户何时会被通知潜在的安全漏洞？
- 有什么条款来确保客户数据的持续完整性和可用性？

3. 为了通知员工在受到监视，雇主采取的一些常见措施包括：在雇用合同的条款中声明员工在使用公司设备时没有隐私要求；在公司可接受的应用和隐私策略中类似的书面声明；登录界面警示所有的通信都受到监视；计算机和电话上的警示监控标记。

第 5 章　保护资产的安全

1. 个人身份信息(PII)是可以识别一个人的任意信息，包括可用于区分或追踪个人身份的信息，例如姓名、社会安全号码或身份证号码、出生日期和地点、母亲的婚前姓名和生物识别记录。受保护的健康信息(PHI)是可以与特定人相关的任何健康相关的信息。PHI 不只仅适用于卫生保健提供者。任何提供或补充保健策略的雇主都会收集和处理 PHI。

2. 固态硬盘(SSD)应该被销毁(例如用破碎机)以净化它们。传统方法使用硬盘驱动器，并不可靠。

3. 组织可以使用他们想要的任何分类级别。两个示例是类 3、类 2、类 1 和类 0，以及机密(或专有)、私有、敏感和公共。

4. 安全港项目包括以下 7 条原则：通知、选择、向前转移、安全、数据完整性、访问和执行。

第 6 章　密码学与对称加密算法

1. 广泛采用一次性密码本加密系统的主要障碍是，难以建立和分发很长的算法所依赖的密钥。

2. 加密这条消息的第一个步骤需要对秘密密钥的字母分配数字列值：

```
S E C U R E
5 2 1 6 4 3
```

第二步，将消息的字母按顺序在密钥字母的下面进行书写：

```
S E C U R E
5 2 1 6 4 3
I W I L L P
A S S T H E
C I S S P E
X A M A N D
B E C O M E
C E R T I F
I E D N E X
T M O N T H
```

最后，发送者通过对向下读取消息的每一列进行加密。列读取的顺序符合第一步所分配的数字编号。这将产生下面的密文：

```
I S S M C R D O W S I A E E E M P E E D E F X H L H P N M I E T I A C X B C I T L T S A O T N N
```

3. 这条消息通过下面的函数解密：

```
P  = (C - 3) mod 26
C: F R Q J U D W X O D W L R Q V B R X J R W L W
P: C O N G R A T U L A T I O N S Y O U G O T I T
```

被隐含的消息为“Congratulation You Got It”。

第 7 章　PKI 和密码学应用

1. Bob 应当使用 Alice 的公钥加密消息，随后将加密的消息发送给 Alice。

2. Alice 应当使用其私钥来解密消息。

3. Bob 应当使用散列函数生成明文消息的消息摘要。随后，他可以使用自己的私钥加密消息摘要，从而创建数字签名。最后，Bob 会在消息中添加数字签名并发送给 Alice。

4. Alice 会使用 Bob 的公钥解密 Bob 所发送消息中的数字签名。随后，她使用与 Bob 创建数字签名相同的散列算法生成明文消息的消息摘要。最后，Alice 比较两个消息摘要。如果二者完全相同，那么数字签名就是可信的。

第 8 章　安全模型的原则、设计和功能

1. 安全模型包括状态机模型、信息流模型、非干扰模型、Take-Grant 模型、访问控制矩阵、Bell-LaPadula、Biba、Clark-Wilson、Brewer and Nash(又被称为中国墙模型，Goguen-Meseguer、Sutherland 和 Graham-Denning。

2. TCB 的主要组件是：用于实施安全策略的硬件和软件元素(这些元素被称为 TCB)，区别和分隔 TCB 组件与非 TCB 组件的安全边界，以及能够作为穿越安全边界的访问控制设备使用的引用监控器。

3. Bell-LaPadula 安全模型的两个规则是不能向上读的简单规则和不能向下写的星号规则。Biba 安全模型的两个规则是不能向下读的简单规则和不能向上写的星号规则。

4. 开放式系统是一种使用已发布 API 的系统，它允许第三方开发与之交互的产品。封闭式系统是专有的系统，它不支持任何第三方产品。开放源码是一种允许他人查看程序源代码的编码方式。封闭源码是一种相反的编码方式，这种方式保持源代码的机密性。

第 9 章　安全脆弱性、威胁和对策

1. 用于描述允许同时执行多个活动的不同计算机机制的术语有：多任务处理、多重处理、多程序设计、多线程处理以及多态处理。

2. 这 4 种安全模式是：专用模式、系统高级模式、分隔模式以及多级模式。

3. 描述存储器的三对特性是：主存储器和辅助存储器，易失性存储器和非易失性存储器，以及随机存取存储器和顺序存取存储器。

4. 分布式体系结构中存在的某些脆弱性包括：台式机/终端/笔记本电脑中的敏感数据，用户缺乏对安全性的理解，物理组件被盗的风险更大，某个客户端受到威胁会导致整个网络受到危害，由于用户安装软件和可移动介质导致引入恶意软件的风险更大，以及客户端上的数据很少被包含在备份中。

第 10 章　物理安全需求

1. 栅栏是一种极佳的边缘防护措施，有助于阻拦偶然的非法进入。6 到 8 英尺高的栅栏能够完成适度的安全工作，并且通常是回旋(也被称为“链节”)围栏，表面缠绕或带刺，以便阻挡一般的翻越。更加安全的安装方法往往是选择高度在 8 英尺以上的栅栏，并且链节上具有多股带刺或锋利的金属网，从而能够阻止进一步的翻越。

2. 哈龙在 900 华氏度降解成有毒气体，此外还不环保(哈龙是一种消耗臭氧的物质)。虽然哈龙是可重复利用的，但是在 2003 年发达国家已停止生产哈龙。哈龙常常被更加环保和毒性较小的物质替代。

3. 一旦用水来抑制起火、火焰或烟雾，带来的危害就成为一个严重的问题，尤其是在使用电子设备的环境中放水时更是如此。水不仅会危害或破坏计算机和其他电子设备，而且还会使许多种存储介质受到破坏或失效。此外，在寻找火源的时候，为了尽可能快速到达指定位置，消防队员经常会使用斧子破门而入或破坏墙壁。这样也会引起对设备和/或邻近线路的潜在物理破坏或毁坏。

第 11 章　网络安全架构与保护网络组件

1. 应用层(7)、表示层(6)、会话层(5)、传输层(4)、网络层(3)、数据链路层(2)和物理层(1)。

2. 与线缆连接相关的问题及对策包括：衰减(使用中继器或不要超出推荐的距离范围)，使用错误的 CAT 线缆(根据吞吐量要求查看线缆规范和小心谨慎防止出错)，串扰(使用屏蔽线缆，将线缆置于不同的管道内，或者使用每英寸缠绕数不同的线缆)，线缆折断(避免线缆移动)，干扰(使用线缆屏蔽，使用每英寸缠绕数更多的线缆，或者切换使用光缆)，偷听(维护所有线缆的物理安全性，或者切换使用光缆)。

3. 人们开发了一些频谱使用技术，这些技术包括扩频、调频扩频(FHSS)、直接序列扩频(DSSS)和正交频分复用(OFDM)。

4. 保证 802.11 无线网络连接安全性的方法包括：禁止 SSID 广播；将 SSID 修改为独特的标识符；启用 MAC 过滤；考虑使用静态 IP 或有保留地使用 DHCP；启用提供的最高加密形式(例如 WEP、WPA 或 WPA2/802.11i)；将无线通信按照远程访问对待以及利用 802.1X、RADIUS 或 TACACS；使用防火墙隔离无线接入点和 LAN；使用 IDS 监控所有无线客户端的活动；考虑要求无线客户端使用 VPN 进行连接，从而获得访问 LAN 的权限。

5. LAN 共享介质访问技术是：CSMA、CSMA/CA(由 802.11 和 AppleTalk 使用)、CSMA/CD(由以太网使用)、令牌传递(令牌环和 FDDI/CDDI)和使用轮询(由 SDLC、HDLC 以及某些大型机系统使用)。

第 12 章　安全通信和网络攻击

1. IPSec 的传输模式被用于主机到主机链接，并且只加密有效载荷，对头不加密。IPSec 的隧道模式用于主机到 LAN 和 LAN 到 LAN 链接，并且加密整个原始有效载荷以及头，随后会添加一个链接头。

2. 网络地址转换(NAT)允许对外部实体隐藏内部系统的身份。NAT 常用于在 RFC 1918 专用 IP 地址和租用的公共地址之间进行转换。因为只允许响应先前的内部查询的入站通信，所以 NAT 充当单向防火墙。NAT 还允许大量的内部系统使用少量的租用公共地址连接到互联网。

3. 电路交换常常与物理连接相关联。链接本身是为通信物理建立和断开的。电路交换提供已知的固定延迟，支持稳定的通信，这种面向连接的交换只对连接(而不是通信)的丢失敏感，并且最常用于语音传输。因为链接只是在可能路径之间逻辑定义的路径，所以分组交换常常与逻辑连接相关联。在分组交换系统内部，每个系统或链接都可以被其他电路同时使用。通信信息被分为若干小段，每个小段都通过电路到达目的地。因为每个小段都可能采用独特的路径，所有分组交换具有可变的延迟。分组交换通常用于突发的通信，不是面向物理连接的，但是往往会使用虚电路，对数据的丢失比较敏感，并且可以用于任何通信形式。

4. 电子邮件本身是不安全的，原因在于它主要是一种明文通信介质，并且使用非加密的传输协议。因此，电子邮件很容易遭受欺骗攻击、垃圾邮件攻击、洪泛攻击、偷听、干扰和劫持攻击。针对这些攻击的主要对策包括：要求强度更高的身份认证，在传输时使用加密技术保护电子邮件的内容。

第 13 章　管理身份与认证

1. 访问控制类型包括：预防、检测、纠正、威慑、恢复、指示和补偿性访问控制。它们被实现为行政管理性控制、逻辑/技术性控制和/或物理性控制。

2. 类型 1 身份认证因素是“你知道什么”。类型 2 身份认证因素是“你拥有什么”。类型 3 身份认证因素是“你是谁”。

3. 联合身份管理系统允许单点登录(SSO)扩展到单个组织之外。SSO 允许用户一次认证并访问多个资源，而不需要再次认证。SAML 是用于在组织之间交换联合身份信息的公共语言。

4. 身份和访问配置生命周期包括配置账户、定期审查和管理账户以及在账户不再使用时撤销账户。

第 14 章　控制和监控访问

1. 自主访问控制(DAC)模型允许对象的所有者、创建者或数据保管人控制和定义访问。管理员集中管理非自主访问控制，并可以进行影响整个环境的变更。

2. 资产、威胁和漏洞应通过资产评估、威胁建模和漏洞分析来识别。

3. 暴力攻击、字典攻击、嗅探攻击、彩虹表攻击和社交工程学攻击都是用于发现密码的方法。

第 15 章　安全评估和测试

1. TCP SYN 扫描向设置了 SYN 标志的每个扫描端口发送单个数据包。这表示打开新连接的请求。如果扫描器接收到设置了 SYN 和 ACK 标志的响应，则表示系统正在进行三次 TCP 握手中的第二阶段，并且端口已打开。TCP SYN 扫描也称为“半开放”扫描。TCP 连接扫描将打开与指定端口的远程系统的完整连接。当运行扫描的用户没有运行半开放扫描所需的权限时，将使用此扫描类型。

2. nmap 返回的三个可能的端口状态值如下：

- 打开——端口在远程系统上打开，并且有一个应用程序正在主动接受该端口上的连接。
- 关闭——端口可在远程系统上访问，这意味着防火墙正在允许访问，但没有应用程序接受该端口上的连接。
- 过滤——nmap 无法确定端口是打开还是关闭，因为防火墙正在干扰连接尝试。

3. 静态软件测试技术(如代码评审)通过分析源代码或编译应用程序来评估软件的安全性，而无须运行。动态测试在运行时环境中评估软件的安全性，并且通常对于部署了由其他人编写的应用程序的组织来说是唯一选择。

4. 变异模糊测试从软件实际操作中提取之前的输入值，对其进行处理(或改变)以创建模糊输入。它可能改变内容的字符，为内容的结尾附加字符串或执行其他数据操作技术。智能模糊测试基于对程序所使用数据类型的理解，开发数据模型并创建新的模糊输入

第 16 章　管理安全运营

1. 知其所需关注权限和访问信息的能力，而最小特权原则集中于特权。特权包括权限和许可。这两者都限制用户和主体仅访问他们需要的东西。遵循这些原则有助于防止和限制安全事件的范围。

2. 管理敏感信息包括根据信息的分类，对其进行正确标记、处理、存储和销毁。

3. 这三种模型是软件即服务(SaaS)、平台即服务(PaaS)和基础设施即服务(IaaS)。云服务提供商(CSP)使用 SaaS 提供最多的维护和安全服务，其次少的是 PaaS，最少的是 IaaS。虽然 NIST SP 800-144 提供了这些定义，但 CSP 有时在营销材料中使用自己的术语和定义。

4. 变更管理有助于防止由于未授权更改了系统配置，从而导致中断。

第 17 章　事件预防和响应

1. CISSP CIB 中列出的事件响应步骤是检测、响应、缓解、报告、恢复、修复和教训总结。

2. 入侵检测系统可以基于它们的检测方法(基于知识或基于行为)，以及基于它们的响应(被动或主动)而被描述为基于主机或基于网络。

基于主机的 IDS 非常详细地检查各个计算机上的事件，包括文件活动、访问和进程。基于网络的 IDS 通过流量评估来检查一般网络事件和异常。

基于知识的 IDS 使用已知攻击的数据库来检测入侵。基于行为的 IDS 从正常活动的基线开始，

并针对基线测量网络活动以识别异常活动。

被动响应将记录活动以及通常提供通知。主动响应直接响应入侵以停止或阻止攻击。

3. 审计是为了确保遵守各项规章制度和检测异常的、未经授权的活动或公开犯罪，而对涉及广泛活动的环境进行的系统检查或审查。审计跟踪提供支持这种检查或审查的数据，并且实质上使得审计和随后检测攻击和行为不端成为可能。

4. 组织应定期执行访问审查和审核。这些可以检测组织何时不遵循自己与账户管理相关的策略和过程。

第 18 章　灾难恢复计划

1. 在考虑采用相互援助协议的时候，存在三个主要的业务问题。首先，由于 MAA 的内在特点，通常要求相互合作的组织的地理位置应该比较接近。但是，这种要求增加了两个组织成为同一威胁受害者的风险。其次，MAA 在危机发生的时候很难强制实施。如果非受害方在最后时刻不履行协议，那么受害方将是非常不幸的。最后，出于对机密性的考虑(与法律和商业相关)，经常会阻止有敏感业务数据的公司信任其他公司。

2. 灾难恢复测试具有下列 5 种主要类型：

- 清单测试是向灾难恢复人员分发恢复清单从而进行审查。
- 结构化演练是“桌面练习”，包括集中灾难恢复团队的成员讨论灾难情景。
- 模拟测试更加全面，并且可能影响组织的一个或多个不很重要的业务单元。
- 并行测试涉及重新分配人员到替代场所，并在那里开始运作。
- 完全中断测试包括重新分配人员到替代场所，并关闭主要的运营场所。

3. 完整备份是创建存储在服务器上的所有数据的备份。增量备份是生成自从最近一次完整备份或增量备份以来被修改过的所有文件的备份。差异备份生成自从最近一次完整备份以来被修改过的所有文件的备份，而不用考虑以前发生的差异备份或增量备份。

第 19 章　事件与道德规范

1. 计算机犯罪的主要类别是：军事或情报攻击、商业攻击、财务攻击、恐怖攻击、恶意攻击和兴奋攻击。

2. 兴奋攻击背后的主要动机是有人尝试体验成功闯入计算机系统带来的极度兴奋。

3. 约谈是为了收集有助于调查的信息而进行的。审问是为了收集刑事检控所需证据而进行的。

4. 事件是在特定时间周期内发生的任何事情。事故是对组织数据的机密性、完整性和可用性具有负面影响的事件

5. 事故响应团队通常包括：高级管理部门的代表、信息安全专业人员、法律代表、公共事务/通信代表以及技术工程师。

6. 事件响应过程的三个阶段是检测和识别、响应和报告，以及恢复和补救。

7. 可以接受的是，证据必须是可靠的、充足的和案件的材料。

第 20 章　软件开发安全

1. 主键唯一标识表中的每一行。例如，员工标识号可能是包含有关员工信息表的主键。

2. 多实例化是一种数据库安全技术，似乎允许插入多个共享相同唯一标识信息的行。

3. 静态分析执行代码本身的评估，对安全缺陷分析指令序列。动态分析在实时生产环境中测试代码，搜索运行时缺陷。

4. 阶段一

第 21 章　恶意代码与应用攻击

1. 病毒和蠕虫都在系统间传播，并且都企图将它们的恶意有效载荷传播到尽可能多的计算机。然而，病毒需要一些类型的人为干预，如通过共享文件、网络资源或邮件进行传播。另一方面，蠕虫能够找出漏洞，并且依靠自己的力量在系统间传播，因此大大增加了它们的复制能力，特别在精心构思的网络中更是如此。

2. 互联网蠕虫使用了 4 种传播技术。首先，它利用 Sendmail 实用程序中的一个 bug，这个 bug 准许蠕虫通过向远程系统上的 Sendmail 程序发送特别制作的、包含蠕虫代码的破坏性电子邮件来传播自己。第二，它使用了基于字典的密码攻击，通过使用一个有效系统用户的用户名和密码来试图获得对远程系统的访问权限。第三，它利用 finger 程序的一个缓冲区溢出漏洞来感染系统。最后，它分析了网络中该系统与其他系统之间存在的信任关系，并且试图通过可信路径传播至这些系统。

3. 如果可能，反病毒软件可能试着为文件清除病毒，删除病毒的恶意代码。如果都失败了，那么它可能隔离文件以便人工复审，或者可能自动删除文件以免遭受进一步的感染。

4. 数据完整性保证软件包(例如 Tripwire)会为受保护系统上存储的每个文件计算哈希值。如果某个文件感染程序病毒攻击了系统，那么会导致受影响文件的哈希值发生变化，并且因此将触发文件完整性警报。

术 语 表

数字和符号

***(星)完整性公理：(*公理)**

Biba 模型的公理，规定在特定分类级别上的主体不能向较高分类级别写入数据。这通常会被缩略为“不能向上写”。

***(星)安全属性：(*属性)**

Bell-LaPadula 模型的属性，规定在特定分类级别上的主体不能向较低分类级别写入数据。这通常会被缩略为“不能向下写”。

802.11i(WPA-2)

对 802.11 标准的修正，定义了新的身份认证以及类似于 IPSec 的加密技术。迄今为止，还不存在能够危害已正确配置的 WPA-2 无线网络的攻击。

802.1q

IEEE 标准定义了 VLAN 标签。VLAN 标签由交换机和网桥用于管理 VLAN 内和 VLAN 之间的流量。

802.1x

一种无线身份认证保护形式，要求所有无线客户端在被准许网络访问前通过 RADIUS 或 TACACS 服务的防护。

1000Base-T

双绞线的一种形式，在 100 米的距离内支持每秒 1000Mbps 或 1Gbpb 的吞吐量。通常被称为千兆以太网(Gigabit Ethernet)。

100Base-TX

双绞线的另一种形式，与 100Base-T 类似。100Base-TX 是快速以太网的最常见形式。

10Base2

同轴电缆的一种类型。通常被用于连接系统和主干中继线。10Base2 最大的跨度是 185 米，最大的吞吐率是 10Mbps。它也被称为细缆。

10Base5

同轴电缆的一种类型。通常被用作网络的主干。10Base5 最大的跨度是 500 米，最大的吞吐率是 10Mbps。它也被称为粗缆。

10Base-T

网络线缆的一种类型，由 4 对双绞的线缆组成，这 4 对线双绞在一起，然后被包在 PVC 绝缘皮内。它也被称为双绞线。

A

abnormal activity：异常活动

指系统中非正常发生的任何系统活动，也被称为可疑活动。

abstraction：抽取

将相似元素组成的集合放入组、类别或角色中，以便作为集合分配安全控制、限制或权限。

acceptable use policy：可接受使用政策

可接受的绩效水平、员工行为和活动期望的策略。不遵守策略可能导致工作行动警告、惩罚或终止。

acceptance testing：验收测试

这种测试试图验证系统满足指定的功能性标准，并且还可能验证满足产品的安全性能。验收测试被用于判断终端用户或客户是否会接受已完成的产品。

accepting risk：接受风险

管理层对可能采用的防护措施进行成本/效益分析评估，进而确定应对措施的成本远远超过风险可能造成的损失的成本。

access：访问

由客体到主体的信息传输。

access aggregation：访问聚合

收集多个非敏感信息并将其组合或聚合用于学习敏感信息。侦察攻击经常使用访问聚合方法。

access control：访问控制

主体被授权或限制对客体进行访问的机制。它包括标识和验证主体，验证对客体的授权以及监视或记录访问尝试的硬件、软件和组织策略或过程。

Access Control List：访问控制列表(ACL)

访问控制列表指定了每个主体对客体的访问级别。

Access Control Matrix：访问控制矩阵(ACM)

包含主体和客体的一个表，它指明了每一个主体可以对每一个客体执行的操作或功能。矩阵中的每一列都是一个 ACL，每一行都是功能列表。

access control types：访问控制类型

预防性控制尝试防止发生安全事件，侦测性控制尝试在事件发生后发现事件，纠正性控制尝试纠正检测到的事件引起的任何问题。其他控制类型包括恢复、威慑、指令和补偿访问控制。控制是使用管理、逻辑/技术或物理手段实现的。

access tracking：访问跟踪

对主体的访问企图或行为进行审计、记录和监控，也被称为活动跟踪。

account lockout：账户锁定

密码策略程序化控制措施中的一个要素，它可以在失败的登录尝试达到指定的次数后禁用用户账户。账户锁定是一种防止针对系统登录提示的穷举攻击和字典攻击的有效对策。

accountability：可问责性

使某人对某件事情负责的过程。此时，如果主体的身份和行为可以被跟踪和验证，那么就有可能实现可问责性。

accreditation：鉴定

由指定许可机构(DAA)给出的正式声明，指出通过在可接受的风险程度上使用一系列规定的安全措施，IT 系统被准许在特定的安全模式下运行。

ACID：模型

ACID中的这些字母表示数据库事务处理的4个必需特征：原子性、一致性、隔离性以及持久性。

active content：活动内容

这种 Web 程序被下载至用户自己的计算机上执行，而不是消耗服务器端的资源。

ActiveX

Microsoft 公司在 Web 应用程序中使用的组件对象模型(COM)技术。ActiveX 可以使用多种语言

之一实现，这些语言包括 Visual Basic、C、C++和 Java。

ad hoc

两个(或多个)单独系统之间的对等无线网络连接，而不需要无线基站。

Address Resolution Protocol：地址解析协议(ARP)

TCP/IP 协议组的一个子协议，工作在数据链路层(第 2 层)上。ARP 被用于通过 IP 地址的轮询发现系统的 MAC 地址。

addressing：寻址

由处理器访问内存中不同位置的方法。

administrative access controls：行政管理性访问控制

依照组织的安全策略定义的策略和措施，用于实现并加强整体的访问控制。例如，行政性访问控制包括雇用准则、背景调查、数据分类、安全培训、假期历史审查、工作监督、人员控制和测试。

administrative law：行政法

行政法涉及广泛的主题，从美国联邦机构内使用的程序，乃至用来执行美国国会通过的法律的移民政策。行政法被颁布在美国联邦法规(CFR)中。

administrative physical security controls：行政性的物理安全控制

安全控制包括设施构造和选择、场地管理、人员控制、意识培训和紧急事件响应及规程。

admissible evidence：可接纳的证据

证据要与确定事实相关。证据要确定的事实必须对本案是必要的(也就是相关)。此外，证据必须具有法定资格，这意味着必须合法获得证据。由于不具备法定资格，因此非法搜查所获得的证据是不可接纳的。

Advanced Encryption Standard：高级加密标准(AES)

由美国国家标准与技术研究院(NIST)在 2000 年 10 月选择的加密标准，基于 Rijndael 密码。

Advanced Persistent Threat：高级持续性威胁(APT)

一些有组织的攻击者，他们有高度动机、技术和耐心。他们通常由政府赞助，专注于特定的目标，并将继续攻击很长一段时间，直到他们实现目标为止。

advisory policy：建议式的策略

建议式的策略讨论可接受的行为和活动，并且定义破坏安全的后果。它解释了高层管理部门在组织内部对安全和遵守规定的期望。大多数的策略都是建议式的。

adware：广告软件

广告软件使用多种技术在被感染的计算机上显示广告。通常与间谍软件相关或链接到间谍软件。

agent：代理

代表用户执行操作的智能代码对象。代理通常接受用户的指令，然后自动执行其操作，并且可能持续一段预定的时间直至满足某些条件，或者可能持续一段不确定的时间。

aggregate functions：聚合函数

SQL 函数，如 COUNT()、MIN()、MAX()、SUM()和 AVG()，它们可能针对数据库运算得到信息集合。

aggregation：聚合

一组函数，它们将一个或多个表中的记录组合在一起，从而产生可能有用的信息。

agile software development：敏捷软件开发

一组软件开发方法，避开过去的僵化模型，倾向于强调客户需求的方法，以及快速开发以迭代方式满足这些需求的新功能。

alarm：警报

从运动探测仪中分离出的一种机制，可以引发威慑、防护和/或通知。只要运动探测仪显示环境中出现显著的变化，就都会发出警报。

alarm triggers：警报触发器

在发生特定事件时发送给管理员的通知。

algorithm：算法

对输入数据执行的一组规则或过程。通常与加密函数相关，指定加密和解密的排列。

analytic attack：分析攻击

这是一种试图减少密码学算法复杂性的代数运算。分析攻击关注于算法本身的逻辑。

AND

检查两个数值是否都为真的运算(利用符号^表示)。

Annualized Loss Expectancy：年度损失期望(ALE)

ALE 指的是针对某种特定的资产，所有已发生的特定威胁实例每年可能造成的损失成本。计算 ALE 的时候可以使用公式：ALE = 单一损失期望(SLE) * 年发生比率(ARO)。

Annualized Rate of Occurrence：年发生比率(ARO)

ARO 的是特定威胁或风险在一年内将会发生(也就是成为现实)的预计频率。也称为可能性确定

applet

从服务器被送往客户端以执行某些动作的代码对象。applet 是一些独立于发送它们的服务器执行的自包含小型程序。

AppleTalk

AppleTalk 协议是一套由苹果公司开发并使用于 Macintosh 系统网络上的协议，最早版本于 1984 年初发布。在 2009 年，Mac OS X 版本 V10.6 发布后取消了苹果操作系统对 AppleTalk 的支持。

application layer：应用层

开放式系统互联(OSI)的第 7 层。

application-level gateway firewall：应用级网关防火墙

一种防火墙类型，基于用于传送或接收数据的网络服务(也就是应用)来过滤通信数据。应用级网关被称为第二代防火墙。

Application Programming Interfaces：应用编程接口(API)

API 允许应用程序开发人员绕过传统的网页，并通过函数调用直接与底层服务交互。虽然提供和使用 API 为服务提供商创造了巨大的机会，但也带来了一些安全风险。

ARP cache poisoning：ARP 缓存投毒

攻击者将虚假信息插入 ARP 缓存(被发现的 IP 到 MAC 关系的本地存储器)中的攻击。

assembly language：汇编语言

替代机器语言代码的更高级语言。汇编语言使用助记符表示 CPU 的基本指令集，但是仍然要求了解硬件的相关知识。

asset：资产

指环境中应该加以保护的任何事物。资产出现损失或泄漏会危及整体的安全性，造成生产率的损失、利润的降低、额外支出的增加、组织停工以及许多无形的后果。

asset valuation：资产评估

根据实际的成本和非货币性支出而分配给资产的货币价值，其中包括开发、维护、管理、广告、支持、维修和替换的成本，还包括难以计算的价值，如公众信心、行业支持、生产率增加、知识成本和所有者权益。

Asset Value：资产价值(AV)

基于实际的成本和非货币性支出而分配给资产的货币价值。

assurance：保证

满足安全需求的置信度。保证必须被持续地维持、更新和重新验证。

asymmetric key：非对称密钥

每个参与者都使用一对密钥(公钥和私钥)的公钥密码系统。使用这对密钥中的一个密钥进行加密的消息只能通过同一密钥对中的另一个密钥进行解密。

asynchronous dynamic password token：异步动态密码令牌

令牌在用户输入由令牌身份认证服务器提供的 PIN 时，会生成一次性密码。PIN 由服务器作为挑战提供，并且用户输入由令牌创建的一次性密码作为响应。

Asynchronous Transfer Mode：异步传输模式(ATM)

一种信元交换技术，而不是像帧中继这样的数据包交换技术。ATM 利用与帧中继十分类似的虚电路，但是由于它使用固定大小的帧或信元，因此可以保证吞吐率。这使得 ATM 成为适用于语音和视频会议的优秀 WAN 技术。

atomicity：原子性

所有数据库事务处理的 4 个必备特征之一。数据库事务处理必须是“要么全有，要么全无”的事务。如果事务处理的任何部分失败，那么整个事务处理都会被回滚，就像什么也没发生一样。

attack：攻击

具有威胁的主体对某些脆弱性的利用。

Attacker：攻击者

任何企图对系统实施恶意行为的人。

attenuation：衰减

由于线缆具有一定长度，因此信号的强度和完整性在线缆上会有损失。

attribute：属性

关系型数据库表中的一列。

Attribute-Based Access Control：基于属性的访问控制模型(ABAC)

许多软件定义的网络应用程序使用 ABAC 模型。

audit：审计

对环境的系统检查或审查，以确保遵守法规，并检测异常、未授权的事件或直接犯罪。

audit trail：审计跟踪

通过将发生的事件和情况的有关信息记录到数据库或日志文件中而生成的记录。审计跟踪被用于重新构建事件，抽取事故的相关信息，证明或驳斥失职行为等。

auditor：审计人员

负责测试和验证安全策略是否被正确实现、总结出的安全解决方案是否适当的人或小组。

authentication：身份认证

用于验证或检查主体所声明身份合法性的过程。

Authentication Header：身份认证首部(AH)

提供了身份认证、完整性和不可否认性的一种 IPSec 协议。

authenticated scan：验证的扫描

安全扫描器被授予认证权限，对正在扫描的服务器(通常通过用户账户)进行只读访问，并且可以使用该访问从目标系统读取配置信息，并在分析漏洞测试结果时使用该信息。

authentication protocols：身份认证协议

为登录凭证提供传输机制而使用的协议。

Authentication Service：身份认证服务(AS)

Kerberos 密钥分发中心(KDC)的要素之一。AS 验证或拒绝票据的可靠性和时间性。

authorization：授权

用于确保所请求的活动或客体访问能够被授予为经过身份认证的身份(也就是主体)分配的权力和特权。

Automatic Private IP Addressing：自动私有 IP 地址寻址(APIPA)

Windows 的一个特征，一旦 DHCP 分配失败，APIP 就会为系统指派 IP 地址。

auxiliary alarm system：辅助警报系统

一种可以加入本地或集中式警报系统的额外功能。辅助警报系统的目的是在警报触发后通知当地警察或消防队。

availability：可用性

确保经过授权的主体被及时准许和不被打断地访问客体。

awareness：意识

安全教育的一种形式，是开展培训的先决条件。安全意识的目的是要把安全放到首位并让学员/用户认识到这一点。

B

backdoor 或 back door：后门

后门是没有被记录到文档的命令序列，允许软件开发人员绕过正常的访问限制。后门可以由制造商放置和留下，或者由黑客使用漏洞来放置。

badges：员工证

物理身份标识和/或电子访问控制设备的形式。

bandwidth on demand：按需带宽

服务提供商提供的功能/优点是：如果运营商网络具有容量，允许客户在需要时消费更多带宽。这种消耗通常以更高速率收费。

base+offset addressing：基址+偏移量寻址

一种寻址机制，它使用存储在其中一个 CPU 寄存器中的数值作为开始计算的基址。然后，CPU 将指令提供的偏移量与基址相加，并从计算得到的存储器地址中取出操作数。

baseband：基带

一次只能传输一个单独信号的通信介质。

baseline：基线

安全性的最小级别，组织中的所有系统都必须达到这个安全级别。基线可以大于安全基线，也可以是性能基线(用于基于行为的 IDS)或配置基线(用于配置管理)。

Basic Input/Output System：基本输入/输出系统(BIOS)

独立于操作系统的原始指令，用于启动计算机和从磁盘加载操作系统。

Basic Rate Interface：基本速率接口(BRI)

提供了 2 个 B 通道(或数据通道)和 1 个 D 通道(或管理通道)的 ISDN 服务类型。每个 B 通道都提供 64Kbps 的速率，D 通道则提供了 16Kbps 的速率。

beacon frame：信标帧

一种无线网络报文类型，用于通过宣告网络 SSID 或网络名称来广播无线网络的存在。

behavior：行为

在面向对象编程术语和技术中，使用某种方法处理消息后来自客体的结果或输出。

behavior-based detection：基于行为的检测

IDS 使用的一种入侵发现机制。基于行为的检测通过观察和研究找出系统中正常的行为和事件。一旦积累了有关正常行为的足够数据，那么它就可以检测到异常的和可能含有恶意的行为和事件。也被称为统计入侵检测、异常检测或启发型检测。

Bell-LaPadula 模型

一种基于状态机模型、关注机密性的安全模型，采用强制性访问控制和格子模型。

best evidence rule：最佳证据规则

该规则声明，当文档被用作法庭处理的证据时，必须提供原始文档。除了规则所应用的某些例外，副本不会被接受为证据。

Biba 模型

一种基于状态机模型、关注完整性的安全模型，采用强制性访问控制和格子模型。

二进制数学

计算机使用的位和字节的计算规则，也称为布尔运算。

bind variable：绑定变量

用于 SQL 字面值的占位符，例如数字或字符串。

biometric factors：生物识别因素

可用于识别或认证任何人的特征。生理生物识别方法包括指纹、面部扫描、视网膜扫描、虹膜扫描、手掌扫描、手部外形和声音模式。行为生物识别方法包括签字力度和击键模式。

biometrics：生物测定学

将人类的生理或行为特征用作逻辑访问的身份认证因素和物理访问的身份标识。

birthday attack：生日攻击

在这种攻击中，怀有恶意的人在数字化签名的通信中寻找可以生成相同信息摘要的不同信息作为替代，从而维持原有数字签名的有效性。在不规则的统计基础上，如果一个房间中有 23 个人，那么存在两人或更多生日相同的人的概率大于 50%。

bit flipping：位翻转

将位改为相反值的活动。通常用于模糊化以轻微修改输入数据的技术。

bit size：位大小

值中的二进制数字或位的数量，例如键、块大小或哈希值。

black-box testing：黑箱测试

查看程序输入和输出的一种程序测试形式，但是不关心内部的逻辑结构。

black box：黑盒

用于操纵线路电压以窃取长途服务。

blackout：电力中断

电力的完全丧失。

block cipher：分组密码

同时对整个信息分组应用加密算法的密码。换位密码就是分组密码的一个例子。

Blowfish

对 64 位文本分组进行操作的分组密码，并且使用变长密钥，密钥长度的范围从相当不安全的 32 位到相当难破解的 448 位。

blue box：蓝盒

用于模拟与电话网络主干(也就是骨干)系统直接互动的 2600Hz 声音。

blue bugging：蓝牙窃听

一种攻击，允许黑客远程控制蓝牙设备的特性和功能。这可能包括打开麦克风的能力，使用手机作为音频监控。

bluejacking：蓝牙劫持

劫持蓝牙连接，以便进行偷听或者可以从设备中抽取信息。

bluesnarfing：蓝牙侵吞

一种攻击，能够允许黑客在你不知情的情况下配对你的蓝牙设备，并且可以从这些设备中提取信息。这种攻击形式能够使攻击者访问你的联系人列表、数据甚至通话。

蓝牙 802.15

通常用于将配件和蜂窝电话或计算机配对的一种无线标准。

boot sector：引导扇区

被用于加载操作系统以及攻击加载过程的病毒类型的存储设备部分。

bot：代理

连续漫游于多个网站并代表用户执行操作的智能代理。

botmaster：僵尸网络控制器

控制僵尸网络的黑客，也称为僵尸牧人。

botnet：僵尸网络

在被称为僵尸网络控制器的攻击者控制下的互联网上计算机(有时是数千甚至数百万台！)的集合。

bounds：界限

对进程可以访问的内存和资源所做的限制。

breach：破坏

破坏是指发生安全机制被威胁主体绕过或阻挠的事情。

Brewer and Nash 模型(也叫作 Chinese Wall)

设计这种模型的目的是准许访问控制基于用户以前的活动动态改变(这也使其成为一种状态机模型)。

bridge：桥

连接速度、线缆类型或拓扑结构不同但是采用协议仍然相同的网络所使用的网络设备。桥是第 2 层设备。

bridge mode：桥接模式

无线接入点部署的一种形式，用于通过无线桥接将两个有线网络连接在一起。

自带设备(BYOD)

允许员工携带自己的个人移动设备并使用这些设备连接(或通过)公司网络的一项策略。虽然设备是员工自有的财产，但存储在设备上的组织数据仍然是组织的资产。

broadband：宽带

支持同时传输多个通信信号的通信介质。

broadcast：广播

向多个未经标识的接收者进行通信传输的一种形式。

broadcast address：广播地址

指定网络分组或容器内所有接收数据的设备的地址。

broadcast domain：广播域

一组网络系统，当该组中的一个成员发送一个广播包时，该组的其他成员接收到该广播包。

broadcast technology：广播技术

基于或依赖于广播而不是单播信令的通信系统。

brouter：桥式路由器

首先尝试路由，如果路由失败，就默认进行桥接的网络设备。

brownout：降低电压

延长的低电压时间段。

brute force：暴力破解

这种攻击模式的特征是自动尝试使用机械性的顺序或组合输入来确定指定系统的安全属性(通常为密码)。

brute-force attack：暴力破解攻击

为了发现已知身份(也就是用户名)的密码而针对系统发起的攻击。为了找到某个账户的密码，暴力破解攻击会使用所有可能的字符组合进行系统化的测试。

buffer overflow：缓冲区溢出

这种脆弱性会导致系统崩溃，或者允许用户运行 shell 命令并获得对系统的访问权限。缓冲区溢出脆弱性在使用 CGI 或其他语言快速开发的 Web 代码中尤为普遍,快速代码开发允许没有经验的程序设计人员快速生成交互式的网页。

business attack：商业攻击

专门非法获取组织机密信息的攻击。

Business Continuity Planning：业务连续性计划(BCP)

涉及对各种组织过程的风险评估，还有在发生这些风险时，为了让它们对组织的影响降到最小程度而建立的各种策略、计划和措施。

Business Impact Assessment：业务影响评估(BIA)

确定能够决定组织持续发展的资源，以及对这些资源的威胁，并且还评估每种威胁实际出现的可能性以及出现的威胁对业务的影响，也被称为业务影响分析(BIA)。

C

高速缓存 RAM

将数据从速度较慢的设备中取出并暂时存储在高性能设备中的过程，以便在希望的时候可以重复使用。

凯撒密码

Julius Caesar 将字母表中的每个字母都替换为其后的第三个字母。

Campus Area Network：园区网(CAN)

跨越学院、大学或复杂的多建筑物办公环境的网络。

candidate key：候选键

用于唯一标识表中任何记录的属性、列和域的子集。

capability list：功能列表

访问控制表的每一行就是功能列表。功能列表与主体相关，其中列出了可以在每个客体上进行的操作。

captive portal：强制门户

一种认证技术，它将新连接的无线 Web 客户端重定向到强制门户访问控制页面。这个门户页面可能需要用户输入付款信息、提供登录凭据或输入访问代码。

cardinality：基数

关系数据库中行的数量。

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol：计数器模式密码块链接消息认证码协议(CCMP)

设计用于替代 WEP 和 TKIP/WPA，使用 128 位密钥的 AES(高级加密标准)作为密文流。

cell suppression：单元抑制

对数据库内部单独的数据项进行抑制(或隐藏)的操作，以便阻止聚合或推理攻击。

centralized access control：集中式访问控制

一种控制方法，所有授权验证都由系统中的一个单独实体来执行。

centralized alarm system：集中式警报系统

一种警报系统，在警报被触发时会通过信号通知远程或集中式监控站。

certificate：证书

被认可的个人公钥的副本，用于验证他们的身份。

Certificate Authority：证书授权机构(CA)

一个认证和分发数字证书的机构。

Certificate Path Validation：证书路径验证(CPV)

从原始起点或可信根源至相关服务器或客户端的证书路径中的每个证书都应当考虑其是否有效与合法。

Certificate Revocation List：证书撤消列表(CRL)

由证书授权机构在证书到期之前撤消的证书列表。

certification：认证

用于支持鉴定过程，对 IT 系统和其他安全措施的技术和非技术安全性特点进行全面评估，以便确定具体设计和实现满足一系列指定安全性需求的程度。

chain of evidence：证据链

在法庭上唯一标识客体的过程，也被称为监管链。

Challenge Handshake Authentication Protocol：挑战握手验证协议(CHAP)

用在 PPP 链接上的一种身份认证协议。CHAP 对用户名和密码进行加密。

change management：变更管理

为了确保任何变更都不会降低或危及安全性而用于记录和监控环境变化的手段。

Channel Service Unit/Data Service Unit：信道服务单元/数据服务单元(CSU/DSU)

将 LAN 信号转换为 WAN 网络所使用格式的边界连接设备，反之亦然。

checklist test：清单测试

向灾难恢复团队的成员分发灾难恢复清单的副本，供他们审查的过程。

Children's Online Privacy Protection Act：儿童联机隐私保护法案(COPPA)

美国对面向孩子或有意收集孩子信息的网站提出明确要求的法律。

chosen cipher-text attack：选定密文攻击

在这种攻击中，攻击者具有解密所选定的部分密文消息的能力。

chosen plain-text attack：选定明文攻击

在这种攻击中，攻击者具有加密他们所选定的明文消息的能力，然后对加密算法的密文输出结果进行分析。

CIA：三元组

三条主要安全原则的名字，这三条安全原则是：机密性、完整性和可用性。

cipher：密码

隐藏消息真正含义的系统。密码使用不同的技术修改并且/或者重新排列消息中的字母或词语，从而获得机密性。

Cipher Block Chaining：密码分组链接(CBC)

未加密文本的每个分组在使用 DES 算法加密之前都与正好在其前面的密文分组进行异或操作的一种过程。

Cipher Feedback：密码回馈(CFB)

在这种模式中，DES 算法被用于加密之前的密文分组。这个分组随后与下一个明文分组异或，从而生成下一个密文分组。

cipher text：密文

已加密的用于传输的消息。

circuit-level gateway firewall：电路级网关防火墙

用于在可信合作伙伴之间建立通信会话的防火墙。它在 OSI 模型的会话层(第 5 层)上工作。

civil laws：民法

民法形成了美国法律体系的大部分。它们被设计用于维护有秩序的社会，并且管理不属于犯罪行为但需要一位公正的仲裁人来解决个人之间和组织之间存在争议的问题。

Clark-Wilson 模型

采用有限接口或程序控制和维护客体完整性的一种模型。

class：类

在面向对象编程术语和技术中，一组对象中定义对象行为的常用方法的集合就是类。

classification：分类

应用于某资源的标签，从而指示其对于组织的敏感度或价值，因此指定了保护该资源的必要安全级别。

classification level：分类级别

安全标签的另一种术语表示。客体和主体被分配的重要性或价值。

clean power：平稳的电力供应

没有波动的纯电力。

clearing：清除

为了介质能在同等的安全环境中被重复使用而彻底删除介质上保存的所有数据的一种方法，也被称为覆盖。

click-wrap license agreement：单击包装许可证协议

一种软件协议，其中的合同条款或者写在软件包装盒外，或者包括在软件文档中。在安装过程中，你会被要求单击一个按钮，表示你已经阅读了协议条款，并且同意遵守这些条款。

clipping level：阈值级别

违规分析审计中使用的阈值。超过阈值级别就会触发将相关事件数据记录到审计日志中的操作。

Closed-Circuit TeleVision：闭路电视(CCTV)

一种使用了视频摄像机和视频记录设备的安全系统。

cloud computing：云计算

一个计算的概念，即处理和存储是通过网络连接而非本地进行。

clustering：群集(也被称为密钥群集)

密码学中的一个缺点，此时使用相同的算法但密钥不同，明文消息会生成完全相同的密文消息。

coaxial cable 或 coax：同轴电缆

同轴电缆的中心是一根铜线，外面包着一层绝缘物质，再往外是一层导电的编织屏蔽物，并且由最外面的绝缘外皮包裹着。同轴电缆能够抵抗电磁干扰(EMI)，拥有较低的价格并且容易安装。

code：编码

代表词或短语，并且有时是秘密符号的密码系统，但它们不一定意味着提供机密性。

code repository：代码仓库

软件开发需要共同努力，大型软件项目需要开发团队可以同时承担代码不同部分的工作。代码仓库是开发人员放置源代码的中心存储点。

cognitive password：感知密码

密码身份认证因素的一个变体，它会询问一系列的问题，这些问题的事实或预定义的响应应该

只有主体才知道。

cohesive 或 cohesiveness：内聚或内聚性

如果某个对象能够在不需要或只需要少量来自其他对象的帮助的情况下完成任务，那么这个对象就高度内聚。高度内聚的对象不像较少内聚的对象那样依赖其他对象。高度内聚的对象往往更好。内聚程度很高的对象能够独自完成任务，并且具有低耦合。

cold sites：冷站点

备用设施有足够大的地方处理组织的运营工作，并带有适当的电子和环境支持系统。

collision：共谋

许多人之间实施未授权或违法行为的约定。

collision domain：冲突域

冲突域是一个互联系统组，如果组内的任何两个(或多个)系统同时进行传输，那么就会发生冲突。

columnar transposition：换位密码

换位密码使用某种加密算法重新排列明文消息中的字母，从而形成密文消息。

commercial business/private sector classification：商业企业/私营部门分类

安全标签通常用在公司使用的安全系统中。常见的公司或商业安全标签包括秘密、专用、隐私、敏感和公开。

Committed Information Rate：待发信息速率(CIR)

对一条虚电路按合同的最小带宽给予保证。

Common Access Card：通用访问卡(CAC)

美国政府内部人员使用的一种卡，里面包含了所有者的照片和其他识别信息。它可以用作徽章和智能卡。

Common Body of Knowledge：通用知识体系(CBK)

由$(ISC)^2$规定的知识领域，作为 CISSP 考试的知识源。

common mode noise：普通模式噪声

由电源或运转的电子设备的火线和地线之间的电势差产生的电磁干扰噪声。

Common Object Request Broker Architecture：公共对象请求代理体系结构(CORBA)

一个针对分布式计算的国际标准。CORBA 支持在计算机上的代码操作能够定位网络中其他位置的资源。

community cloud：社区云

社区云部署模型，为两个或多个组织提供云基础资产。维护责任根据对资产和服务模型的管理来分配。

companion virus：同伴病毒

文件感染病毒的一种变体。同伴病毒是自包含的可执行文件，它利用与合法的操作系统文件类似但又稍有不同的文件名来躲避检查。

compartmented security mode：分隔安全模式

系统处理两种或更多种类型的分隔信息的安全模式。所有系统用户只有具有恰当的许可才能访问由系统处理的所有信息，但是他们不必知道系统中的所有信息。

compensation access control：补偿访问控制

这种访问控制类型为其他已有的控制提供有助于实施和支持安全策略的各种选项。

competent：法定资格

证据的一种特性要求证据必须具有法定资格，这意味着必须合法获得证据。由于不具备法定资格，因此非法搜查所获得的证据是不被认可的。

compiled language：编译语言

在分发或执行前被转换为机器语言的一种计算机语言。

compiler：编译器

编程人员可以使用将高级语言转换为在特定操作系统中使用的可执行文件的编程工具。

compliance testing：合规性测试

另一种常见的审计应用。验证系统是否遵守法律、规章制度、基准、指导原则、标准和策略，它是维护任何环境安全性的一个重要部分。

Component Object Model：组件对象模型(COM)

它是 Microsoft 的标准，被用于进程内的组件或者在同一系统上运行的多个进程之间的组件。

compromise：破坏

如果系统安全被攻破，那么系统就被认为受到破坏。

computer architecture：计算机体系结构

从逻辑层次考虑的计算系统构造的工程学原理。

computer crime：计算机犯罪

任何利用计算机或针对计算机的犯罪行为。

Computer Fraud and Abuse Act：计算机诈骗和滥用法案

一项美国法律，专门用于跨越州边界的计算机犯罪，避免违反州的权力。

Computer Security Act of 1987：1987 年的计算机安全法案(CSA)

一项美国法律，对所有联邦机构的强制安全要求基准。

computer security incident：计算机安全事件

组织内安全策略或实践的违反，或迫在眉睫的威胁的违反。计算机安全事件是攻击、恶意软件感染或员工不当使用的结果。

conclusive evidence：结论性证据

优先于其他证据形式的无可辩驳的证据。

concurrency：并发性

这种安全机制试图使数据库中存储的数据始终是正确的或者至少其完整性和可用性受到保护。并发性使用“锁定”功能允许已授权用户更改数据，只有在完成所有更改后才能“解锁”数据元素。

confidential：机密的

一种政府/军方用于具有机密特性的数据分类。未经授权而泄露机密数据将会导致重大后果，并导致对国家安全的严重破坏。这个分类级别用于处在“秘密”级别和“敏感但未分类”级别之间的所有数据。

confidentiality：机密性

确保信息不会未经授权而泄露，并且定义的保密级别在整个主体-客体交互过程中都会得到保持。

configuration management：配置管理

随时间推移与安全控制和安全机制相关的日志记录、审计和监控活动。这些数据被用于标识变化的主动者，无论其是客体、主体、程序还是通信路径，甚至是网络本身。

confinement 或 confinement property：限制或限制属性

允许一个进程只能从确定的内存地址和资源中读取和写入数据的原则，也可以被称为 Bell-LaPadula 模型的*(星)安全属性。

confusion：混淆

出现在明文和密钥的关系十分复杂的时候，黑客不能继续通过修改明文和分析产生的密文来确

定密钥。

consistency：一致性

所有数据库事务处理的 4 个必备特征之一(其他 3 个特征是原子性、隔离性和持久性)。所有事务处理都必须在与数据库所有规则一致的环境中开始操作。

contamination：污染

具有不同分类级别和/或“知其所需”要求的数据相混合的结果。

content-dependent access control：内容相关的访问控制

基于客体内容或有效负载的访问控制形式。

Content-Distribution Networks 或 Content Delivery Networks：内容分发网络或内容转发网络(CDN)

资源服务的集合，被部署在互联网的许多数据中心以提供低延迟、高性能、高可用性和承载的内容。CDN 通过分布式数据主机提供客户所需的多媒体性能质量。

context-dependent access control：内容相关的访问控制

基于客体内容或有效负载的访问控制形式。

continuity：连续性

企业可以达到的目标，通过制定计划和程序帮助减轻灾难对其连续性操作的影响，并且加快恢复到正常运营的速度。

contractual license agreement：合同许可证协议

在软件商和用户之间概述双方责任的书面合同。

control：控制

使用访问规则或措施来限制主体对客体的访问。

Control Objectives for Information and Related Technology：信息及相关技术控制目标(COBIT)

是一种安全概念基础架构，用于组织公司的复杂安全解决方案。

controls gap：控制差距

风险总计和剩余风险之间的差值。

converged protocols：汇聚协议

专业或专有协议和标准协议的融合，例如 TCP/IP 协议。一些汇聚协议常见的例子：FCoE、MPLS、iSCSI 和 VoIP。

Copper Distributed Data Interface：铜线分布式数据接口(CDDI)

使用双绞线(也就是铜线)部署的 FDDI。它将最大的跨度减少至 100 米，并且容易遭到干扰。

copyright：版权

保护创作者的“原创作品”不遭受未经授权的复制的法律。

corrective access control：纠正性访问控制

为了在不必要的或未授权的操作发生后将系统还原到正常状态而部署的访问控制。例如，纠正性访问控制包括警报、陷阱和安全策略等。

corrective controls：纠正式控制

使用指导说明、规程或指导原则改变不希望的行为(如攻击或错误)的影响。

countermeasures：对策

针对攻击修补漏洞或保护系统的动作。对策可能包括改变访问控制、重新配置安全设置、安装新的安全设备或机制、增加或删除服务等。

coupling：耦合

耦合是对象之间的交互级别。低耦合意味着较少的交互。因为对象更为独立，所以低耦合提供了更优的软件设计。低耦合更易于检测故障和更新。内聚程度较低的对象需要大量来自其他对象的帮助才能完成任务，并且具有高耦合。

covert channel：隐蔽通道

数据可以不按照常规的、期望的或可检测的方法进行传输的一种手段。

covert storage channel：存储隐蔽通道

通过将数据写入一个其他进程可以读到的公共存储区域来传递信息的通道。

covert timing channel：时间隐蔽通道

以一种可预测的方式，通过改变系统组件的性能或更改资源的时间安排来传递信息的一种通道。

cracker：破坏者

企图对个人或系统发动攻击的恶意用户。破坏者可能受贪婪、权力或成名因素的驱使。他们的行为可能导致财产(数据、计划等)被盗、系统被关闭、安全性受到破坏、负面的公众意见、市场占有份额下降、收益率降低和丧失生产率。

credential management system：证书管理系统

当单点登录(SSO)不可用时，为用户提供存储空间以保留其凭据的解决方案。用户可为需要一套不同凭证的网站和网络资源存储凭证。该管理系统确保这些凭证已加密，从而防止未经授权的访问。

creeping privilege(s)：蠕变的特权

用户账户经过一段时间积累的特权，在这段时间内，用户的作业角色以及被指派的工作任务不断发生变化。

criminal law：刑法

警察和其他执法机构执行的法律主体。刑法包含针对某些行为的禁令，如谋杀、伤害、抢劫、纵火和类似的犯罪。

critical path analysis：关键路径分析

一种系统工作，可以确定关键任务应用、过程和操作以及所有必要的支持要素之间的关系。

criticality prioritization：关键性优先顺序

BCP/DRP 创建期间关键资产和过程的优先顺序。

Cross-Site Request Forgery：跨站请求伪造(CSRF)

利用受信用户通过用户浏览器对易受攻击的服务器执行命令的一种 Web 攻击，也被称为 XSRF。

Cross-Site Scripting：跨站脚本(XSS)

当网站包含某种类型的反射式输入时，存在的一种 Web 应用程序攻击形式。经常利用脚本注入。

Crossover Error Rate：错误率交叉点(CER)

在这一点上，误接受率(FAR)等于误拒绝率(FRR)。为了比较不同生物测定设备的性能，从这一点开始测量性能。

cryptanalysis：密码分析

破解编码和密码的研究方法。

cryptographic key：密码学密钥

密码学密钥为用于加密和解密的密码学算法提供“安全”部分。

cryptography：密码学

应用于数据的算法，用于确保机密性、完整性、身份认证和/或不可否认性。

cryptology：密码学

密码术与密码分析学一起被称为密码学。

cryptosystem：密码系统

通信双方使用共享密钥或公钥和私钥对的系统，用于帮助提供通信的安全保护。

cryptovariable：密码变量

用于执行加密和解密操作的密钥的另一个名字。

custodian：监管者

被分配或委派要对客体进行日常的分类和标记工作，并且负责适当的存储和保护工作的人。监管者常常就是 IT 人员或系统安全管理员。

cyber-physical：物联网

指提供一种计算设备来控制物理世界中事物的术语。在过去，这些可能被称为嵌入式系统，但物联网的类别似乎更侧重于物理世界的结果，而不是计算方面。参见物联网(IoT)。

Cyclic Redundancy Check：循环冗余校验(CRC)

与哈希总数类似的一个数值，它指出信息是否在传输过程中已被修改或破坏。

D

darknet：黑暗网络

未使用的网络空间部分，用于监视基于网络的攻击和流量。

data analytics：数据分析

对原始数据进行检查的科学，检查重点是从大量的信息中提取有用的信息。数据分析的结果可以集中在重要的异常值，或正常之外的例外或标准项，或所有数据项的总结，或一些集中的提取和有兴趣信息的组织。

Data Circuit-terminating Equipment：数据链路终端设备(DCE)

一种网络连接设备，在帧中继上执行实际的数据传输，以及为用户建立和维护虚电路。

data classification：数据分类

按标签组织数据，以便应用安全控制和访问限制。

data controller：数据处理者

在欧盟数据保护法条文中将数据处理者定义为控制数据过程的人或实体。

data custodian：数据监管者

被指派实施安全策略和上层管理部门所规定保护任务的用户。数据监管者执行所有必要的措施，从而为数据提供适当的保护，并完成上层管理部门委派的要求和责任。

Data Definition Language：数据定义语言(DDL)

允许创建和更改数据库结构(也被称为模式)的数据库编程语言。

data dictionary：数据字典

数据元素及其关系的集中存放处。存储与数据用法、关系、源和格式相关的关键信息。

data diddling：数据欺骗

对数据进行小改动的行为，通常意图是恶意的。

Data Encryption Standard：数据加密标准(DES)

1997 年对所有政府通信提出的标准密码系统。尽管它在 2001 年被高级加密标准(AES)所代替，但是很多政府机构今天仍继续在密码学应用中使用 DES。

data extraction：数据抽取

为了构建有意义的表示法或整体数据的概述，从大量的数据中抽取要素的过程。

datagram：数据报

传输层 UDP 报头和有效载荷的组合。

data hiding：数据隐藏

避免让主体知道数据存在的过程。

Data Link Layer：数据链路层

OSI 模型的第 2 层。

Data Loss Prevention：数据丢失防护(DLP)

系统能够检测和阻止数据泄露的企图。

Data Manipulation Language：数据操纵语言(DML)

允许用户与模式内包含的数据交互的数据库编程语言。

data mart：数据集市

用于保护元数据安全的存储设施。

data mining：数据挖掘

准许分析人员对数据仓库进行搜索，从而寻找历史数据中潜在的相关信息的技术。

data owner：数据所有者

负责为安全解决方案内的放置和保护进行信息分类的人。

data processor：数据处理者

欧盟数据保护法将数据处理者定义为“一个自然人或法人，他拥有个人资料，仅代表数据控制者的利益。”

data remanence：数据剩磁

在数据被移除之后仍保留在介质上的数据。清除和清理方法尝试确保从介质中删除所有数据而没有任何数据剩余。

data stream：数据流

来自应用层的数据被发送到协议栈。数据流成为顶层协议的初始有效载荷。

Data Terminal Equipment：数据终端设备(DTE)

一种网络连接设备，像一台路由器或交换机，为用户的网络提供到帧中继网络的接入。

data warehouse：数据仓库

大型数据库，它存储了大量用于专用分析技术的来自多个数据库的信息。

database：数据库

为组织收集到的信息而采用的电子整理汇集系统。大多数数据库由文件、记录和字段组织起来。

database contamination：数据库污染

当不同值、分类、安全域中的数据或记录混合在一起时会发生的事情，可能是一种完整性和机密性形式的违反。

Database Management System：数据库管理系统(DBMS)

可以对数据库中的信息应用存储、修改和抽取。

database partitioning：数据库分区

将一个数据库分为若干更小的部分或单独的数据库，通常用于分隔开具有不同敏感度标签的内容。

dead zone：死区网络

一种网络段，IPX 和 AppleTalk 都可作为 IP 协议网关，替代实现 IP 方案。

decentralized access control：分散式访问控制

一种访问控制系统，其中授权验证由整个系统中的不同实体执行。

Decision Support System：决策支持系统(DSS)

这种应用分析业务数据并且以更容易做出业务决策的形式提供给用户。决策支持系统更多地被

视为信息型应用，而不是操作型应用。DSS 常常被知识型员工(例如服务台人员或客户支持人员)和销售服务人员(例如电话推销员)所使用。

declassification：降低机密等级

在资源的价值不再值得受到更高分类级别的安全保护时将之移至更低分类等级的过程。

decrypting：解密

反向用于加密消息的密码算法过程。

dedicated security mode：专用安全模式

运行在专用安全模式中的系统经过授权每次只处理一个具体的分类级别，并且所有系统用户必须具有许可和了解这些信息的需求。

deencapsulation：拆封

在 PDU 沿 OSI 模型的各层向上传输时，从 PDU 中剥离层的头和尾的过程。

defense-in-depth：深度防御

安全的分层方法。实现了多层安全性，攻击者需要绕过多个安全控制才能成功。

degaussing：消磁

使用磁体恢复介质到最初未被使用的状态。

degree：度

关系数据库中列的数量。

delegation：委托

在面向对象编程环境中，将某个对象的请求转发给另一个对象或代理。如果某个对象没有处理特定消息的方法，那么就需要委托。

Delphi 技术

一个匿名反馈和响应过程，这个过程被用于达成一致意见。

delta 规则

也被称为学习规则。它是专家系统的特性，这种特性允许专家系统从经验中加以学习。

deluge system：洪水系统

干管道(火灾抑制)系统的另外一种形式，它使用较粗的管道，因此能排出大股的水流。洪水系统对于放置了电子设备和计算机的环境不太适合。

Denial of Service：拒绝服务攻击(DoS)

阻止系统对针对资源和客体的合法通信或请求进行处理或响应的一种攻击类型。

detective access control：检测性访问控制

为了发现不必要的或未授权的操作的出现而部署的访问控制。例如，检测性访问控制包括保安、监督用户、事故调查和入侵检测系统(IDS)。

deterrent access control：威慑性访问控制

为了防止安全策略违规的访问控制。

DevOps 方法

DevOps方法通过将三种职能集中在一个操作模式中来解决软件开发、质量保证和技术操作的问题。DevOps这个词是开发和操作的组合，表示这些功能必须合并和合作才能满足业务需求。

dictionary attack：字典攻击

一种攻击系统的形式，用于发现已知身份(也就是用户名)的密码。在字典攻击中，常用密码和字典单词的脚本被用来试图发现账户的密码。

differential backup：差异备份

一种备份类型，存储那些自从最近一次完整备份以来被修改过的所有文件。

Diffie-Hellman：算法

在双方可能需要相互通信但是没有物理手段交换密钥内容，并且没有公钥基础设施便于交换保密密钥时使用的密钥交换算法。

diffusion：扩散

明文的一处变化导致整个密文的多处变化。

Digital Millennium Copyright Act：数字千禧年版权法案

此法律阻止那些挫败由版权所有者用于受保护作品的版权保护机制的企图，并且还限制了互联网服务提供商的线路被罪犯用于违反版权法时应负的责任。

Digital Rights Management：数字版权管理(DRM)

一种使用加密来保护数字介质上版权限制的保护软件。在过去十年中，发布商尝试在包括音乐、电影和书籍的各种介质类型中部署 DRM 方案。

digital signature：数字签名

数字签名可以向接收者保证消息的确来自声明的发送者，消息在发送者和接收者之间进行传输的过程中未被改变。

Digital Signature Standard：数字签名标准(DSS)

这个标准指出联邦政府批准的所有数字签名算法都必须使用安全的散列函数。

direct addressing：直接寻址

向 CPU 提供要被访问的存储器位置的实际地址。

direct evidence：直接证据

通过基于证人五官感知收集信息的言辞证据证明或反驳特定行为的证据。

Direct Memory Access：直接内存访问(DMA)

不需要 CPU 帮助就可以直接交换实际存储器数据(RAM)的机制。

Direct Sequence Spread Spectrum：直接序列扩频(DSSS)

以并行方式同时利用所有可用频率的一种无线技术。

directive access control：指令性访问控制

这种访问控制指示、限制或控制主体的活动，从而强制或鼓励主体服从安全策略。

directory service：目录服务

网络中可用资源的集中化数据库，可以被理解为网络服务与资产的电话号码簿。用户、客户端和进程可以通过查阅目录服务了解所期望系统或资源的驻留位置。

disaster：灾难

给系统或环境带来很大伤害、损失或破坏的事件。

disaster recovery plan：灾难恢复计划

为了尽可能快地将业务还原到正常运营而需要的指导恢复工作的文档。

Disaster Recovery Planning：灾难恢复计划编制(DRP)

描述了组织在灾难发生并打断正常的业务活动之后为恢复正常运营而采取的措施。

discretionary access control：自主访问控制

用于控制对客体访问的一种机制。客体的所有者或创建者控制和定义主体对客体的访问。

discretionary security property：自主安全属性

这个属性规定系统使用访问控制表来实施自主访问控制。

distance vector routing protocol：距离矢量路由协议

一种路由协议，维护目的网络以及距离和方向的跳数的列表(也就是到达目的地所经过的路由器

数量)。

distributed access control：分布式访问控制

访问控制的一种形式，其中授权验证由整个系统的不同实体进行。

distributed architecture：分布式体系结构

网络的客户端/服务器模型，其中客户端可以是本地的或通过 WAN 链路(包括 VPN 和互联网)连接。

Distributed Component Object Model：分布式组件对象模型(DCOM)

扩展了 COM 的概念，从而支持分布式计算。这是 Microsoft 公司针对 CORBA 的解决方案。

Distributed Control Systems：集散控制系统(DCS)

DCS 单元通常可以在工业处理方案中看到，它负责从单个地点的大型网络环境中收集数据和实施控制，它是非常重要的。DCS 系统的一个重要方面是控制分布在所监测环境中的元件，如制造车间或生产线和集中监控场所，向局部控制器发送命令，同时收集状态和性能数据。

distributed data model：分布式数据模型

在分布式数据模型中，数据存储在多个数据库中，不过依然是逻辑连接的。即使数据库由通过网络相互连接的许多部分组成，用户仍然将数据库理解为单个实体。每个字段都具有许多子字段和父字段。因此数据映射关系是多对多关系。

Distributed Denial of Service：分布式拒绝服务攻击(DDoS)

当攻击者对多个系统的安全造成威胁并将它们当作发动对其他一个或多个受害系统攻击的平台时，就会发生分布式拒绝服务攻击。在攻击中使用的受威胁系统通常被称为从属系统或僵尸。DDoS 攻击使用来自多个源的数据导致受害系统泛洪。

Distributed Reflective Denial of Service：分布式反射拒绝服务(DRDoS)

DRDoS 攻击利用了主要互联网服务的常规操作机制，这些服务包括 DNS 和路由器更新协议。通过将受害者的地址用为欺骗的源地址，DRDoS 攻击会向各种互联网服务的服务器或路由器发送众多更新、会话或控制包。DRoS 攻击可能导致过多的通信数据，从而使上游系统受到受害者过量数据的负面影响。

DNS 投毒

改变或伪造 DNS 信息(例如 HOSTS 文件、DNS 缓存服务器或授权 DNS 服务器)以便路由或误导合法通信的行为。

DNS 欺骗

使用一台欺诈的 DNS 服务器更改或伪造 DNS 信息并发送假的 DNS 应答的行为，从而导致路由或误导合法流量。

documentary evidence：文档证据

所有带到法庭上证明事实的书面内容。这种证据类型还必须经过验证。

documentation review：文档审查

阅读交换材料并利用标准和期望对其进行检验的过程。

domain：域或领域

1) 一个信任范围，或者共享共同安全策略的主体和客体的集合。每个域的访问控制与其他域的访问控制是独立维护的。在涉及多个域时会导致分散式访问控制。2)CISSP 考试的一个研究领域。

DREAD

风险评级系统设计用于提供灵活评级解决方案，基于对每个威胁的 5 个主要问题：破坏潜力、可重复性、可利用性、受影响用户和可发现性。

drive-by download：偷渡式下载

在用户不知情的情况下下载代码和安装。攻击者有时会修改合法网站上的代码，以包含偷渡式下载。他们还托管自己的恶意网站，并使用网络钓鱼或重定向方法将用户带到恶意网站。

dry pipe system：干管道系统

包含压缩空气的一种火灾抑制系统。一旦灭火装置被触发、空气泄漏、水阀打开，从而使管道充满水并在环境中放出水来。

due care：应尽关注

确保企业的资产和员工是安全的并已经得到保护，并且高层管理人员已经对所有未得到缓解或转移的风险进行了恰当的评估和假设。

due diligence：应尽职责

通情达理的人在特殊的条件下避免损害他人或财务的努力程度。

dumb cards：无记忆卡

人们可以读取的身份卡，通常含有经过授权的持卡人的照片和手写的信息。无记忆卡通常在无法实施或无法利用自动化控制(但使用保安人员是比较可行的方法)的环境中使用。

dumpster diving：垃圾挖掘

为了发现或推断出有价值的机密信息，在组织或生产过程中的废弃物、剩余物或遗留物中进行挖掘的行为。

durability：持久性

所有数据库事务处理的 4 个必备特征之一(其他三个特征是原子性、一致性和隔离性)。数据库

事务处理必须是持久的，也就是说一旦被提交给数据库，事务处理就会被保留。数据库通过使用备份机制(例如事务处理日志)确保了持久性。

dwell time：按压时间

在键盘上按压某个键的时间。这是击键力度生物测定学因素的一个元素。

Dynamic Host Configuration Protocol：动态主机配置协议(DHCP)

用于在系统启动时为系统指派 TCP/IP 配置设置的一种协议。DHCP 将端口 67 用于服务器点对点响应，将端口 68 用于客户端请求广播。DHCP 支持对网络寻址的集中化控制和管理。

dynamic packet-filtering firewalls：动态数据包过滤防火墙

使得过滤规则的实时修改可以建立在通信内容上的防火墙。动态数据包过滤防火墙被称为第 4 代防火墙。

dynamic passwords：动态密码

无法在延长时间段内保持不变的密码。动态密码可以在每次使用时发生变化或定期改变(如每隔 30 天进行一次改变)。

dynamic testing：动态测试

在运行环境中评估软件安全，对于部署别人写的应用程序的组织来说通常是唯一选择。

E

eavesdropping：偷听

嗅探的另一个术语。然而，偷听不只包括捕获和记录网络通信，还包括记录或监听音频通信、传真和无线电信号等。

Economic Espionage Act of 1996：1996 年的经济间谍法案

该法律规定，任何被发现带有为外国政府或机构获利的意图、从美国公司偷取贸易机密的犯罪者可以被处以高达 50 万美元的罚款和长达 15 年的监禁。任何被发现在其他情况中窃取商业秘密的犯罪者可以处以高达 25 万美元的罚款和长达 10 年的监禁。

education：教育

一项更细致的工作，此时学生/用户学习比他们为完成工作任务实际上需要知道的更多的知识。教育通常与用户参加认证考试或寻求职务晋升联系起来。

El Gamal

对 Diffie-Hellman 密钥交换算法背后的数字原理如何被扩展用于支持信息加密和解密的整个公共密码系统进行了解释。

ElectroMagnetic Interference：电磁干扰(EMI)

一种电噪声，可以引起电气设备的工作出现问题。它还可能干扰通信、传输和回放，导致质量下降。

Electronic Access Control：电子访问控制(EAC)

使用凭证读卡器、电磁体和闭门感应器的一种智能锁。

Electronic Codebook：电子代码本(ECB)

最易于理解的加密模式，但安全性最差。每次这个算法处理一个 64 位分组，它简单地使用所选择的密钥对这个分组进行加密。这意味着如果算法多次遇到相同的分组，那么它将产生完全相同的加密分组。

Electronic Communications Privacy Act：电子通信隐私法案(ECPA)

使得对个人电子隐私的侵犯成为犯罪行为的法律。它对电子邮件和语音邮件通信的监视提供了防护，并且防止这些服务的提供商对这些内容进行未授权的公开。

electronic discovery：电子发现(e-Discovery)

在诉讼过程中，任何一方有责任保留与案件相关的证据，并通过发现过程，在控诉双方之间分享信息。这个发现过程应用纸质档案和电子记录和电子发现(e-Discovery)过程促进电子信息披露的处理。

electronic vaulting：电子保险库

在这种存储环境中，使用批量传送方式将数据库备份转移到远处的一个场所。远程的这个地点可以是一个专用的替代性恢复场所(如完备场所)，或者只是由公司或承包商管理的远程场所，主要是出于维护备份数据的目的。

Electronically Erasable PROM：电可擦除 PROM(EEPROM)

存储系统使用传送到芯片引脚的电压来强制擦除。EEPROM 可以在不从计算机中移除的情况下被擦除，它比标准 PROM 和 EPROM 芯片拥有更大的灵活性。

elliptic curve cryptography：椭圆曲线密码学

公钥密码学的一个新的分支，在减少密钥长度的基础上提供与已建立的公钥密码系统相似的安全性。

elliptic curve group：椭圆曲线组

每条椭圆曲线都有对应的椭圆曲线组，这个组由椭圆曲线上的点和位于无穷大处的点 0 组成。在同一个椭圆曲线组中的两个点(P 和 Q)，可以用椭圆曲线的加法算法加在一起。

embedded system：嵌入式系统

通过计算机实现一个更大系统的一部分。嵌入式系统通常围绕与更大的产品相关的一系列有限和特定的功能进行设计并成为它的一个组成部分。它可能由一个典型计算机系统找到的相同组件组成，或者可能是一个微控制器(集成芯片与主板上的内存和外设端口)。

employee：员工

在讨论 IT 问题时，通常是指用户。

employment agreement：雇用协议

一种文档，用来概略说明组织的规则和限制、安全策略和可接受的使用方法和行为准则，详细描述工作情况，概述破坏活动及其后果，并且确定员工胜任工作要求所需的时间。

Encapsulating Security Payload：封装安全有效载荷(ESP)

为保护传输数据的机密性进行加密的 IPSec 组件，但是也可以进行有限的身份认证。

encrypt：加密

将消息转换为密文的过程。

encrypted virus：加密病毒

加密病毒使用密码学躲避检测。在加密病毒的外部表现中，它们实际上很像多态病毒，每个被感染的系统都有一个不同特征的病毒。然而，加密病毒不是通过改变其代码生成这些修改过的特征，而是修改了在磁盘上的存储方式。

encryption：加密技术

对无意的接收者隐藏通信数据的含意或意图的一种艺术和学科。

endpoint security：终端安全

终端安全的概念是每个单独设备必须维护本地安全，不论其网络或通信通道是否提供安全。有时这被表示为“末端设备应对自己的安全负责”。

end-to-end encryption：端到端加密

一种加密算法，保护双方(也就是客户端和服务器)之间的通信安全，并且可以独立于链路加密技术实施。端到端的加密技术的例子是在发送者和接收者之间使用隐私增强邮件(PEM)传递邮件。这种技术可以阻止加密链路的安全端的通信数据或通过未加密的链路传送的通信数据遭到入侵者的监控。

enrollment：注册

在系统中建立新的用户、身份或身份认证因素的过程。安全注册要求个人身份或身份认证因素的实际证明。通常，如果注册过程超过两分钟，那么身份标识或授权机制(尤其是生物测定设备)是

不被认可的。

enterprise extended mode：企业扩展模式

使用多个无线接入点来支持比单个无线接入点更大地理区域的单个无线网络。

entity：实体

指主体或客体。

Erasable PROM：可擦除 PROM(EPROM)

在这些芯片上有一个很小的窗口，当用一束紫外线光照射的时候，就可以擦掉芯片上的内容。这个过程完成之后，终端用户可以将新的信息烧入 EPROM 内。

erasing：擦除

对一个文件、选中的几个文件或整个介质中的文件执行的一次删除操作。大多数情况下，删除或擦除过程只是删掉了链接数据的目录或分类链接。数据实际上还保留在磁盘上。

escalation of privilege：权限提升

任何攻击者或利用，将他们的访问权限从正常的用户账户扩展到管理员特权。

Escrowed Encryption Standard：托管加密标准

美国政府希望为所有加密解决方案创建后门的失败尝试。这个解决方案利用了Clipper芯片，该芯片使用了 Skipjack算法。

espionage：间谍活动

收集有关组织专有的、秘密的、隐私的、敏感的或机密的信息的恶意行为。这种行为出于明确的揭露目的，通常这些数据会被卖给竞争对手或其他感兴趣的组织(如外国政府)。

ethernet：以太网

一种常见的共享介质 LAN 技术。

ethical hackers：道德黑客

经过培训负责网络安全方法、主要目的是进行非破坏性和非入侵测试的人。道德黑客代表安全系统的所有者攻击安全系统，以便确定和记录系统的脆弱性。这样一来，安全系统的所有者就能够在恶意的黑客利用这些脆弱性之前进行补救。道德黑客与普通黑客使用相同的方法，不过会报告他们所发现的问题，而不是像普通黑客那样牟取自己的利益。

ethics：道德规范

管理个人行为的规则。一些组织已经认识到需要标准的道德规范或准则，并且为道德行为设计了指导方针。这些准则不是法律，它们是对专业人士行为的最低标准。它们应该为你提供可靠的、专业的道德判断基础。

evidence：证据

在计算机犯罪中，可以在法庭上用于证明攻击者身份和行为的任何硬件、软件或数据。

excessive privilege(s)：过度的特权

指的是用户具有比其工作任务所要求的更多的访问权限、特权或许可。如果发现用户账户具有过度的特权，那么应当立即撤消额外的和不必要的特权。

exit interview：离职面谈

中止合同策略的一个方面。为了防止机密和敏感信息的泄漏，提醒被解雇的员工他们应该承担的法律责任。

Expectation Maximization：期望最大化(EM)

一种数据挖掘技术，基于用户与组织的联系、数据中心与用户的物理位置之间的距离、一天中的时间和其他属性来开发正常用户行为的模型。

expert opinion：专家观点

由专家提供的观点和事实组成的一种证据类型。专家是接受过某领域教育的人以及目前从事该领域工作的人。

expert system：专家系统

一种系统，寻找某个特殊主体具体化的人类累计的知识，并用于为将来的决定采取一致的形式。

exposure：暴露

指由于威胁而容易造成资产损失的状况。暴露包括容易被威胁主体或事件利用的脆弱性。

Exposure Factor：暴露因子(EF)

如果已发生的风险危害到某种特殊资产，组织将受到的损失的百分比。

Extensible Access Control Markup Language：访问控制标记语言(XACML)

一种标记语言，用于在 XML 格式内定义访问控制策略，并且它通常实现基于角色的访问控制。它有助于给联盟中的所有成员提供保证，保证他们向不同角色授权相同级别的访问。

Extensible Markup Language：可扩展标记语言(XML)

一种标记语言，定义了人类和机器可读的文档格式和编码规则。

Extranet：外部网

互联网和内部网之间的中间物。外部网是组织网络已经被分开的一部分，这样对于专用网络来说，它是一个内部网，但是它还为公共的互联网提供信息服务。外部网常常用于提供商和用户之间的 B2B 应用。

F

face scan：面部扫描

生物测定学因素的一个例子，它是主体唯一具有的行为或生理特征。面部扫描是使用某个人面部的形状和特征布局的过程，被用于建立身份标识或提供身份认证。

fail-open：应急开放

系统对故障的一种响应，从而默认进入“允许”状态。

fail-safe：故障防护

系统对故障的一种响应，从而默认进入“拒绝”状态。

failover：故障转移

当主系统发生故障时，将工作负载或流量重定向到备份系统。

Fair Cryptosystems：公正密码系统

美国政府希望为所有加密解决方案创建后门的失败尝试。这个技术使用了分派在若干受托人之间的分段密钥。

False Acceptance Rate：误接受率(FAR)

在生物测定设备不够敏感和非法的主体通过身份认证的时候发生的错误。

false negative：假性负面

当漏洞扫描器漏掉漏洞并且未能警告管理员存在危险情况时发生的错误。

false positive：假性正面

可能触发警报的事件，当安全扫描器可能没有足够的信息来最终确定一个漏洞的存在时，也可能会在没有问题的时候报告漏洞。它也被称为将良性问题视为恶意事件。

False Rejection Rate：误拒绝率(FRR)

在生物测定设备太敏感和合法的主体没有通过身份认证的时候所发生的错误，也被称为类型 I 错误。

Family Educational Rights and Privacy Act：儿童教育权利和隐私法案(FERPA)

另一种特殊的隐私法案，它影响所有接受美国联邦政府资助的教育机构(绝大多数学校)。该法案赋予 18 岁以上的学生和未成年学生的父母确定的隐私权。

fault：故障

瞬间失去电力。

fault tolerance：错误容错

一种系统遭受故障但能持续运行的能力。容错是指添加冗余组件，如在廉价磁盘冗余阵列(RAID)中添加额外的磁盘，或在故障转移群集配置中添加额外的服务器。

Federal Information Processing Standard 140：联邦信息处理标准 140(FIPS-140)

FIPS-140 为美国联邦政府使用的密码学模块定义了硬件和软件要求。

Federal Information Security Management Act：联邦信息安全管理法案(FISMA)

在 2002 年通过的联邦信息安全管理法案(FISMA)要求联邦机构实施一个信息安全项目，这个项目要覆盖机构部门的运营。FISMA 同样也要求政府部门(包括承包商)的活动在安全管理项目内。

Federal Sentencing Guidelines：联邦判决指导原则

1991 年颁布的针对违反联邦法律提供判决指导原则的法律。

feedback loop characteristic：反馈循环特征

现代瀑布模型中的能力，允许开发返回到上一阶段，以纠正在后续阶段发现的缺陷。

fence：栅栏

一种外围设备。栅栏被用于明确地区分受到特殊安全级别保护的区域和其他区域。栅栏围墙可以包括广泛的成分、材料和建造方法。

Fibre Channel over Ethernet：以太网光纤通道(FCoE)

一种汇聚协议，用来在以太网网络上封装光纤通道通信。它通常需要 10Gbps 以太网以便支持光纤通道协议。

Fiber Distributed Data Interface：光纤分布式数据接口(FDDI)

一种高速的令牌传递技术，它使用两个环，其中通信流在两个环上沿相反的方向传输。FDDI 提供了 100Mbps 的传输速率，并且常被用作大型企业网络的主干。

fiber-optic：光纤

一种线缆连接形式，它传输光脉冲而不是电子信号。光纤线缆支持 2Gbps 的吞吐率，长度可达两公里。

field：字段

在数据库中，一个字段是表的一列或属性。

file infector virus：文件感染病毒

许多病毒感染不同类型的可执行文件，并且在操作系统试图执行这些文件时触发。对于基于 Windows 的系统来说，可执行文件以扩展名.exe 和.com 为后缀。

filter(s)：过滤

在安全设备上常见的一组规则或限制，例如防火墙和代理，也称为规则和 ACL。

financial attack：财务攻击

非法获得钱财或服务的犯罪形式。

fingerprints：指纹

人类手指上的螺旋图案，通常被用作生物学测定的身份认证因素。

firewall：防火墙

用来过滤通信数据的网络设备。防火墙主要用于专有网络和 Internet 的连接之间，也可以用于公司内的部门之间。防火墙根据已定义好的一组规则对通信数据进行过滤。

firmware：固件

存储在只读存储器芯片中的软件。

flash memory：闪存

EEPROM 的衍生概念，是一种非易失性存储媒介，可以进行电子擦除和重写。EEPROM 和闪存的主要区别是：EEPROM 必须完全擦除后才能重写，闪存可以以块或页的方式进行擦写。闪存是最常见的 NAND 闪存，被广泛用于存储卡、优盘、移动设备和 SSD(固态硬盘)。

flight time：抬指时间

前后两次击键之间的时间，是击键力度这种生物测定学形式的一个要素。

flooding：泛洪

向受害者发送足够多的通信数据从而导致 DoS 的一种攻击形式，也被称为流攻击。

footer：报尾

通过协议，添加从较高层协议接收的有效载荷的末端信息。

foreign key：外键

另一个表中的主键，用于在两个表的内容间建立交联或表达的关系。

Fourth Amendment：第四修正案

美国宪法的修正，防止了美国政府机构在缺少搜查证和合理根据的情况下对私有财产的搜查。一些美国法院已经扩展了其对第四修正案的解释，包括针对搭线窃听和其他侵犯隐私行为的防护。

Fraggle

这种拒绝服务攻击类似于 smurf攻击，但利用的是 UDP 数据包，而不是 ICMP 数据包。

fragment：片段

当网络接收到的数据包比它允许的最大数据包的尺寸大时，它会将这个包拆分为两个或更多个片段。这些片段中的每一个都被分配了大小(根据包的尺寸)和偏移量(根据包的起始位置)。

fragmentation attack：片段攻击

一种利用 TCP/IP 协议栈片段重组功能中脆弱性的攻击。

frame：帧

数据链路层报头、有效载荷和尾部的组合。

Frame Relay：帧中继

使用数据包交换技术为用户建立虚电路的共享连接介质。

frequency：频率

用频率测量波在特定时间内振动的次数(使用单位 Hz 进行确定)或者每秒的振动次数。无线电波的频率在 3Hz 到 300GHz 之间。

frequency analysis：频率分析

在加密消息中查看重复字母并与特定语言的字母使用统计信息(例如英语中字母 E、T、A、0、N、R、I、S 和 H 的出现频率)进行比较的密码分析或攻击。

Frequency Hopping Spread Spectrum：跳频扩频(FHSS)

扩频概念的早期实现。这种无线接入技术并非以并行方式发送数据，而是串行发送数据，同时不断改变所使用的频率。

full backup：完整备份

在备份介质上存储受保护设备上数据的完整副本，也指生成数据完整副本的过程。

full-interruption tests：完全中断测试

涉及实际关闭主要场所的运营并把它们转移到恢复场所的灾难恢复测试。

full-knowledge teams：full 认识水平团队

在安全评估或渗透测试之前，这支团队完全了解所有硬件和软件的操作、配置和用法。

fuzz testing：模糊测试

模糊测试是一项专门的动态测试技术，它向软件提供了许多不同类型的输入，来强调其局限性并发现先前未被发现的缺陷。模糊测试软件向软件提供无效的输入，或是随机生成，或是特别制作以触发特殊的软件漏洞。然后，模糊测试监控应用程序的性能，监视软件崩溃、缓冲区溢出或其他不良和/或不可预知的结果。

fuzzy logic：模糊逻辑

与利用“黑白”数据归类的代数方式或集合论的严格数学相比，这种技术的设计更接近于人类的思维模式。

G

Gantt 图

显示不同时间项目和调度之间相互关系的条形图，提供了帮助计划、协调和跟踪项目中特定任务的调度图表。

gate：门

栅栏的出入控制点。

gateway：网关

连接使用不同网络协议的网络连接设备。

generational fuzzing：智能 fuzzing

基于预期输入的模型开发输入，以执行相同任务的 fuzzing 形式，有时也被称为智能 fuzzing。

geo-tagging：地理标记

具有全球定位系统支持的移动设备，支持在使用设备拍摄照片的时候不仅嵌入拍摄的照片日期/时间信息，还可以嵌入纬度和经度形式的地理位置标记。

GNU Privacy Guard：GNU 隐私保护(GnuPG)

OpenPGP 标准的免费和开源实现，是现在商业 PGP 产品的免费/开源变体。

Goguen-Meseguer 模型

一个完整性模型，基于一个主体可以访问预设的域或客体列表。

Government Information Security Reform Act of 2000：2000 年的政府信息安全改革法案

此法案修正了美国法典，实施了附加的信息安全策略和措施。

government/military classification：政府/军方分类

通常应用于军方的安全系统的安全标签。军方安全标签从高到低的分类为：绝密、秘密、机密、敏感但未分类和未分类(绝密、秘密、机密都被认为是已分类的)。

Graham-Denning 模型

关注主体和客体在创建和删除时安全的一个安全模型。

ActGramm-Leach-Bliley(GLBA)法案

直到 1999 年才成为法律，在商业机构之间形成了严格的政府屏障。银行、保险公司和贷款提供商受到对他们所能提供的服务和相互共享的信息的严格限制。GLBA 稍微放松了涉及每个组织所能提供的服务的规定。

granular object control：粒度对象控制

针对某个对象的安全设置的非常具体的和极为详细的控制级别。

grid computing：网格计算

网格计算是并行分布处理的一种形式，这种形式松散地把大量的处理节点组合在一起，为一个处理目标工作。

ground：接地

电路中接地(即与大地相连)的电线。

group：组

访问控制管理的简化机制，与角色类似。类似的用户成为一个组的成员。为组分配针对某个对象的访问权限。因此，组中的所有成员对此对象具有相同的访问权限。组的使用大大简化了管理用户访问对象的行政性开销。

grudge attack：恶意攻击

通常怀有不满的动机，并且对企业或个人进行破坏。破坏可能是信息的丢失或信息处理能力的丧失，也可能是组织或个人名誉的损害。攻击者可能是现在的或以前的员工，也可能是希望组织不能正常运作的人。

guest OS：宾客操作系统

在虚拟机中运行的操作系统。

guideline：指南

提供了如何实现标准和基准的建议的一套文档。指南概述了一套方法(包括行动建议)，但并非强制性的。

H

hacker：黑客

在历史上，没有恶意倾向的技术狂热者。很多作家和媒体在讨论实际上与破坏者相关的问题时常常使用黑客这个术语。

halon：哈龙

一种非常有效的灭火化合物，但它在华氏 900 度的时候会转化为有毒的气体，会耗尽大气中的臭氧层。因此，哈龙通常被其他介质替代。

hand geometry：手部外形

识别手部物理尺寸的一种生物测定学控制类型，包括手掌和手指的宽度与长度。这种技术可以是机械或图像边缘(也就是可视轮廓)图解法。

handshake：握手

由 TCP / IP 协议栈利用的三次过程，用于建立两个主机之间的连接。

hardware：硬件

实际的物理设备，如硬盘驱动器、网卡和打印机等。

Hardware Security Module：硬件安全模块(HSM)

一个密码处理器，用于管理/存储数字加密密钥、加速加密操作、支持更快的数字签名，并提高身份认证。

hardware segmentation：硬件隔离

在硬件层次上通过实施内存访问限制而实现进程隔离的技术。

hash：散列

从散列函数生成的消息摘要所称的数字。

hash function：散列函数

接收一条完整的消息，然后根据消息的内容生成唯一的输出值的过程。这个数值通常被称为消息摘要。

hash total：散列总数

用于校验传输完整性的校验和。

hash value：散列值

从文本字符串产生的数值，实际上比文本本身要小。某种程度上，其他文本生成相同散列值几乎是不可能的。

Hashed Message Authentication Code：散列信息身份认证代码(HMAC)

这种算法实现了部分的数字签名功能，也就是保证了消息在传输过程中的完整性，但没有提供不可否认性。

header：头部

通过协议添加到从较高层协议接收的有效载荷的前面的信息。

Health Information Technology for Economic and Clinical Health Act：关于经济和临床健康的卫生信息技术法案(HITECH)

在 2009 年，美国国会通过了“关于经济和临床健康的卫生信息技术法案(HITECH)”来修订 HIPAA。这条法律更新了许多 HIPAA 的隐私和安全需求，并于 2013 年通过 HIPAA Omnibus Rule 实施。被新法规强制变化的其中一个方面就是在法律对待商业伙伴的方式上，处理被保护的健康信息(PHI)的组织代表了 HIPAA 覆盖的实体。HITECH 也引入了新的数据泄露通告需求。

Health Insurance Portability and Accountability Act：健康保险易移植性和责任性法案(HIPAA)

1996 年通过的法案，这使得管理健康保险和健康保护组织(HMO)的法律发生了许多变化。在 HIPAA 的规定中，隐私规定要求对医院、医师、保险公司和其他处理或存储个人医疗隐私信息的组织实施严格的安全措施。

hearsay evidence：传闻证据

其他人在庭外告诉证人的内容所形成的证据。没有经过系统管理员验证的计算机日志文件也可能被认为是传闻证据。

heart/pulse pattern：心跳/脉搏模式

生物测定学因素的一个示例，它是主体行为或生理学上的特征，具有唯一性。一个人的心跳/脉搏模式被用于建立身份标识或提供身份认证。

hierarchical：层次

一种 MAC 环境。层次环境按照顺序的结构(从低安全性到中等安全性，再到高安全性)将各种分类标签联系在一起。结构中的每个级别或分类标签都是有关系的。某个级别中的许可授权主体访问同一级别以及所有更低级别中的所有客体，但禁止访问更高级别中的任何客体。

hierarchical data model：层次数据模型

这种数据库将关联的记录和字段组合为逻辑树结构。每个字段可能不具有子字段，也可能具有一个或多个子字段，但是都只具有一个父字段。因此，数据映射关系为“一对多”。

High-Level Data Link Control：高级数据链路控制(HDLC)

一种第 2 层协议，用于在同步通信线路上传输数据。HDLC 是基于 EBM 的 SDLC 的一种 ISO 标准。HDLC 支持全双工通信、点对点和点对多点连接，提供了流控制，并且包括错误检测和纠正。

high-level languages：高级语言

并非机器语言或汇编语言的编程语言。这种语言独立于硬件，并且更容易被人类所理解。在被执行之前或执行期间，高级语言必须被转换为机器语言。

High-Speed Serial Interface：高速串行接口(HSSI)

第 1 层协议用于将路由器和多路复用器连接到 ATM 或帧中继以连接设备。

hijack attack：劫持攻击

在这类攻击中，恶意用户出现在客户端和服务器之间，并且随后中断并接管会话。恶意用户常常假扮客户端从服务器上获取数据，而服务器并未意识到通信另一方已经发生了变化。

hoax(aka virus hoax)：骗局(又称病毒骗局)

一种社会工程学攻击的形式，通过使用恶意代码欺骗用户破坏自己的系统。

honeynet/honeypot：蜜罐

单台计算机或整个网络被作为诱捕入侵者的陷阱。蜜罐系统看上去像是一个合法的网络，但它们 100%都是伪造的。蜜罐系统利用没有修补的程序和没有安全保护的脆弱性来吸引入侵者，还可以使用有吸引力但却是伪造的数据。蜜罐系统被设计用于吸引入侵者的注意力，并引导它们进入已受到限制的地点，从而让它们远离合法的网络和机密资源。

host-based IDS：主机型 IDS(HIDS)

安装在单台计算机上的 IDS，可以监视该计算机上的可疑活动。主机型 IDS 能够准确地发现危及系统安全的文件和进程，或是由怀有恶意的用户执行的未经授权的活动。

hostile applet

试图执行不期望的或恶意的活动的任何移动代码。

hot site：完备场所

在这种配置中，按通常的工作顺序维护备用工作设施，带有完备的服务器、工作站和通信链接设备，准备承担主要的运营职责。

hub：集线器

将多个系统连接在一起成为星型拓扑结构的网络设备。集线器将入站通信在所有出站端口上进行中继。

hybrid attack：混合攻击

一种密码攻击形式，首先尝试字典攻击，然后执行某种穷举攻击。后续的穷举攻击被用于为来自字典的密码添加前缀或后缀字符，从而发现单字符构造不同密码、双字符构造不同密码，依此类推。

hybrid cloud：混合云

一种公共云和私有云的混合部署。

hybrid MAC：混合 MAC

一种 MAC 环境。混合环境结合了分层和隔间区分的概念，以使得每个等级水平可能包含许多细分，与安全域的剩余部分相隔离。主体必须有正确的许可，以及在特定隔间的“需知”数据来获得对隔间区分客体的访问。

hyperlink spoofing：超链接欺骗

这种攻击用于将通信重定向至欺诈系统或冒名系统，或者简单地将通信发送至预定目的地之外的任何地方，通常是通过恶意更改发送到客户端文档的 HTML 代码中的超链接 URL。

Hypertext Transfer Protocol：超文本传输协议(HTTP)

这个协议被用于将 Web 页面元素从 Web 服务器传输至 Web 浏览器(通过众所周知的服务 TCP/UDP 端口地址 80)。

Hypertext Transfer Protocol over Secure Sockets Layer：安全套接层上的超文本传输协议(HTTPS)

一种标准，使用端口 443 在 Web 服务器和浏览器客户端之间协商加密的通信会话。

I

identification：身份标识

身份标识是一个过程，在这个过程中主体声明身份，可问责性从此开始。身份标识的过程可以包含用户提供用户名、登录 ID、个人身份号码(PIN)、智能卡或进程 ID 号。

identification card：身份证

物理身份标识的一种形式，通常包含一张主体的照片和/或带有主体附加信息的磁条。

identity and access provisioning life cycle：标识和访问开通使用周期

账户的创建、管理和删除。开通是指在创建账户时和在账户生命周期内向其授予适当的权限。

Identity as a Service or Identity and Access as a Service：身份和访问即为服务(IDaaS)

一个第三方服务，提供身份和访问管理。IDaaS 为云有效提供单点登录，并在内部客户访问那些基于云的软件即服务(SaaS)应用程序时特别有用。

Identity Theft and Assumption Deterrence Act：身份窃取和冒用阻止法案

这个法案使得窃取个人身份成为犯罪行为，并且规定了对任何违反此法律的人处以严厉的犯罪处罚(最长达 15 年的监禁和/或多达 25 万美元的罚款)。

ignore risk：忽略风险

否认风险存在和希望通过忽略风险来认为风险永远不会发生。

immediate addressing：立即寻址

指向数据的一种方法，这些数据作为指令的一部分提供给 CPU 使用。

impersonation：假冒

假装某人的身份或联机账户，往往借助于欺骗和会话重放机制。假冒攻击被视为比伪装更主动的攻击。

implementation attack：实现攻击

这种攻击类型利用密码学系统实现中的弱点，关注于对软件代码的利用，不仅仅涉及错误与缺陷，而且还涉及编写加密系统所使用的方法学。

inappropriate activities：不恰当的行为

是指发生在计算机或 IT 基础设施上的行为活动，它们虽然不是实际的犯罪，但通常要受到内部的处罚或被开除。一些不恰当的行为类型，包括生成或查看不适当的内容、性骚扰和种族歧视、浪费和滥用。

incident：事故

发生系统入侵的事件。

incremental backup：增量备份

只存储那些自从最近一次完整备份或增量备份以来被修改过的文件，也指创建这种备份的过程。

indirect addressing：间接寻址

作为指令的一部分提供给 CPU 的存储器地址，并不包含 CPU 所使用的作为操作数的真实数值。实际上，存储器地址中包含另一个存储器地址(也许位于不同的页面上)。然后，CPU 处理器从这个地址中取出真实的操作数。

Industrial Control System：工业控制系统(ICS)

一种用于控制工业生产过程和机器的计算机管理设备。ICS 被广泛应用于众多的工业行业，包括制造、装配、发电、配电、供水、污水处理、石油精炼。有几种 ICS，包括集散控制系统(DCS)、可编程逻辑控制器(PLC)和数据采集与监控系统(SCADA)。

industrial espionage：行业间谍活动

利用非法手段获取竞争者信息的行为。

inference：推理

这种攻击利用了几个非敏感信息片的组合，从而获得对应属于更高级分类的信息的访问能力。

inference engine：推理引擎

专家系统的第二个主要构件，它对知识库中的信息进行分析，进而做出正确的决策。

information flow model：信息流模型

专注于信息流的模型，无论信息流是什么样的，都会确保维护和实施安全性。信息流模型以状态机模型为基础。

information hiding：信息隐藏

为了对某个主体隐藏数据，将数据和主体放置在不同的安全域。

informative policy：信息式的策略

此策略被设计用于提供特定主体的信息或知识，如公司目标、任务描述或组织如何与合作伙伴和客户交流。信息式的策略不是强制执行的。

Infrastructure as a Service：基础设施即服务(IaaS)

一种云计算概念，不仅可以提供按需操作的解决方案，而且可以完全外包 IT 基础设施。

infrastructure mode：基础设施模式

无线网络配置，使用无线基站将所有无线设备连接到网络，并可能彼此连接。

inherit(或 inheritance)：继承(或继承性)

在面向对象编程环境中，继承性指的是一个类具有来自另一个类的一个或多个相同方法。因此，当一个类具有来自另一个类的一个或多个相同方法时，就说前者“继承了”这些方法。

Initialization Vector：初始化向量(IV)

许多密码学解决方案使用的一种向量，以便通过增加输入的随机性来增加加密数据的强度。

input validation：输入验证

在处理接收的输入之前，检查、扫描、过滤或清理从用户(特别是通过互联网)接收的输入。

inrush：电涌

电源开始的电涌通常与所连接的电源有关，无论电源是主电源还是替换/辅助电源。

instance：实例

在面向对象编程环境中，实例可以是类的对象、例子或表示。

Instant Messaging：即时消息(IM)

一种机制，允许两个用户在互联网上的任何位置进行实时文字聊天。一些 IM 工具允许文件传输、多媒体、语音和视频会议以及更多的功能。

Integrated Services Digital Network：综合业务数字网(ISDN)

综合业务数字网是一种数字化的端到端的通信机制。ISDN 由电话公司开发，支持在用于承载语音通信的同一设备和基础结构上的高速数字通信。

integrity：完整性

确信修改不是由未授权用户进行的，并且确保授权用户没有进行未授权的修改而表现出的一种状态。

intellectual property：知识产权

无形的资产，如秘方或生产技术。

interface testing：接口测试

接口测试评估模块针对接口规范的性能，以确保所有开发工作完成后模块会正常工作。

International Data Encryption Algorithm：国际数据加密算法(IDEA)

一种分组密码，是针对 DES 算法的密钥长度不够而开发的。DES、IDEA 在 6 4 位明文/密文分组的基础上进行操作，但开始操作时使用 128 位密钥。

International Organization for Standardization：国际标准化组织(ISO)

一个独立的监督组织，它定义和维护计算机、网络连接、技术标准以及 13000 多个其他的商业、政府和协会国际标准。

Internet Key Exchange：互联网密钥交换(IKE)

一种协议，在 IPSec 的参与方之间提供加密密钥的安全交换。

Internet Message Access Protocol：网络消息访问协议(IMAP)

从电子邮件服务器向电子邮件客户端传送电子邮件的协议。

Internet of Things：物联网(IoT)

能够通过互联网彼此通信或与控制台通信，用来影响和监视真实世界里设备的集合。

Internet Security Association and Key Management Protocol：互联网安全协会和密钥管理协议(ISAKMP)

一种协议，为 IPSec 提供后台的安全支持服务。

internet Small Computer System Interface：互联网小型计算机系统接口(iSCSI)

一个基于 IP 的网络存储标准。这项技术可以用来支持位置独立的文件存储、传输和局域网、广域网的检索，或者公共互联网连接。iSCSI 常被认为是光纤通道的一种低成本替代。

Internetwork Packet Exchange：互联网分组交换协议(IPX)

IPX 是 IPX/SPX 网络层协议的一部分，并使用于(虽然没有严格的要求)20 世纪 90 年代的 Novell NetWare 网络中。

interpreted languages：解释语言

被转换为机器语言(执行时每次一条命令)的编程语言。

interrogation：审问

询问涉嫌犯罪的人。

interrupt：中断(IRO)

设备或计算机组件用于获取 CPU 注意的一种机制。

interview：约谈

询问某人去收集协助进行犯罪调查的信息。在约谈中，被询问的人不会被怀疑有罪。

Intranet 内部网

是为拥有与在互联网上发现的相同的信息服务而设计的专用网络。

intrusion：入侵

这种情况下威胁主体通过躲过安全控制措施获得访问组织基础设施的权利，并且直接对资产构成了威胁，也被称为渗透。

intrusion detection：入侵检测

一种具体的监控形式，记录信息和实时发生的事件，以便检查不期望的系统访问。

Intrusion Detection System：入侵检测系统(IDS)

一种使审计日志和实时系统事件的检查自动化的产品。IDS 通常主要被用于检测入侵企图，但是也可以被用于检测系统故障或评价系统总体性能。

IP header protocol field value：IP 报头协议字段值

IP 包头部的一个元素，这个元素确定 IP 数据包净载中使用的协议(通常，这个值为 6 表示 TCP、为 17 表示 UDP、为 1 表示 ICMP、此外还可以是许多有效的路由协议号)。

IP Payload Compression (IPComp) protocol：IP 有效载荷压缩协议

这个协议允许 IPSec 用户通过在加密操作之前压缩数据包来增强性能。

IP probes：IP 探测

使用自动化工具在一个范围内 ping 每个地址的攻击技术。对 ping 请求做出回应的系统被黑客记录，便于做进一步分析。没有产生回应的地址被认为不能利用并被忽略。

IP Security：IP 安全性(IPSec)

IP 安全性是一种基于标准的机制，为点对点的 TCP/IP 通信提供加密。

IP spoofing：IP 欺骗

通过这个过程，怀有恶意的人只是通过重新配置他们的系统就具有可信任系统的 IP 地址，然后试图得到访问其他外部资源的权利。

iris scans：虹膜扫描

生物测定学因素的一个例子，它是主体唯一的行为或生理上的特征。瞳孔周围有色的部分被用于建立身份标识或提供身份认证。

isolation：隔离

用于保证任何行为只影响与进程有关的内存和资源的概念。

J

Jailbreak：越狱

越狱会打破 iOS 设备上的限制，并允许根级别访问底层操作系统。它类似于运行 Android 操作系统的设备。

Java

一种独立于平台的编程语言，由 Sun Microsystems 公司开发。

job description：工作描述

一种详细文档，概括出了组织所需特殊职位的要求。工作描述包括安全分类、工作任务等信息。

job responsibilities：工作职责

要求员工在常规的基础上执行的特殊工作任务。

job rotation：岗位轮换

组织通过让员工在不同的工作中转换职位，从而提高整体安全性的一种方法。岗位轮换有两种

功能。首先，它提供了一种知识冗余的类型。其次，人员流动可以减少欺诈、更改数据、偷盗、怠工和滥用信息的风险。

K

Keccak 算法

在 2012 年，美国联邦政府宣布选择 Keccak 算法作为 SHA-3 算法。

Kerberos

基于票据的身份认证机制，它采用被信任的第三方提供身份标识和身份认证。

Kerchoff 假设/原则

算法应当公开，但是所有密钥都应当保密。大多数算法都遵循 Kerchoff 假设或原则，但不是所有的算法都如此。

kernel：内核

总是驻留在内存中的操作系统部分(因此可以根据需要随时运行)。

kernel proxy firewalls：内核代理防火墙

一种防火墙类型，被集成到操作系统的核心，提供会话和数据包评估的多个层次。内核代理防火墙被称为第 5 代防火墙。

key：密钥

1) 用来加密或解密消息的密值。
2) 数据库的列、属性或字段。

Key Distribution Center：密钥分发中心(KDC)

Kerberos 身份认证系统的一个要素。KDC 维护所有已注册的主体和客体的秘密密钥。KDS 还是一个 COMSEC 机构，负责分配对称密码系统的密钥，特别适用于政府机构。

key escrow system：密钥托管系统

在这种密码学恢复机制中，密钥被存储在数据库中。当密钥丢失或受损的时候，密钥只能由被授权的密钥托管机构恢复。

keyspace 或 key space：密钥空间

能够用作特定算法密钥的有效值的范围。

keystroke dynamics：击键力度

通过分析抬指时间和按键时间来度量主体如何使用键盘的生物测定学因素。

keystroke monitoring：击键监控

记录用户在物理键盘上进行按键的行为。记录行为可以通过图像(如使用录像机)或逻辑/技术方法(如使用捕获硬件设备或软件程序)。

keystroke patterns：击键模式

生物测定学因素的一个例子，它是主体唯一的行为或生理上的特征。个人敲击密码短语的模式和速度被用于建立身份标识或提供身份认证。

knowledge base：知识库

专家系统的一个构件，知识库包括专家系统已知的规则。知识库试图以一系列“if/then”语句对人类专家的知识进行编码。

knowledge-based detection 知识型检测

IDS 使用的入侵发现机制，并且基于已知攻击特征的数据库。知识型 IDS 的主要缺点是：只对已知的攻击方法有效。

known plain-text attack：已知明文攻击

在已知明文攻击中，攻击者具有已加密信息的副本和用于产生密文(副本)的明文信息。知道这些信息可以极大帮助攻击者破解较弱的编码。

KryptoKnight

基于票据的身份认证机制，与 Kerberos 类似，但基于对等身份认证方式。

L

LAN 扩展

LAN 扩展是一种远程访问的多层交换机，被用于通过 WAN 链接连接远距离网络。此设备令人奇怪之处在于，它会创建 WAN，但是营销商却避开使用 WAN 术语，而是只使用 LAN 和扩展的 LAN 术语来称呼这种设备。之所以这样做的原因是：标准的 WAN 设备与复杂的概念和术语联系在一起，采用 LAN 术语能够使人们更容易理解这种设备，并且更容易开展营销工作。

land attack：陆地攻击

一种 DoS 类型。陆地攻击出现在攻击者向受害者发送很多 SYN 数据包的时候，并且这时 SYN 数据包已经被欺骗使用与受害者相同的源、目标 IP 地址和端口号。这会令受害者认为它向自己发送了一个 TCP/IP 会话的启动包，从而使得系统出现故障，常常会导致系统挂起、崩溃或重新启动。

lattice-based access control：格型访问控制

非自主访问控制的一种变化形式。格型访问控制为主体和客体间的所有关系定义了访问的上限

和下限。这个上下限可以是任意的，但是它们常常遵循军方或公司的安全标签级别。

layer 1：第 1 层

OSI 模型的物理层。

layer 2：第 2 层

OSI 模型的数据链路层。

layer 3：第 3 层

OSI 模型的网络层。

layer 4：第 4 层

OSI 模型的传输层。

layer 5：第 5 层

OSI 模型的会话层。

layer 6：第 6 层

OSI 模型的表示层。

layer 7：第 7 层

OSI 模型的应用层。

Layer 2 Forwarding：第 2 层转发(L2F)

Cisco 公司开发的相互验证的隧道机制协议。L2F 不提供加密。

Layer 2 Tunneling Protocol：第 2 层隧道协议(L2TP)

混合 PPTP 和 L2F 的元素而形成的点对点隧道协议。L2TP 缺少内置的加密机制，通常使用 IPSec 作为安全保护机制。

layering：层次法

多个安全控制连续地提供安全部署的最大有效性。

licensing：许可证颁发

说明产品如何被使用的合同。

life cycle assurance：生命周期保证

基于设计、架构、创建、测试和分发的概念对产品的信任或可靠性进行评估。最终，判断一个产品是否被设计以安全性作为核心特征。

lighting：照明

最常见的一种边界安全控制形式。照明的主要目的是阻拦那些偶然的入侵者、侵犯者、小偷和希望在黑暗中实施恶意行为的窃贼。

link encryption：链路加密技术

这种加密技术使用软件或硬件解决方案，通过在两个点之间建立一条安全隧道来保护整条通信线路的安全，也就是对进入隧道一端的所有数据都进行加密，对离开隧道另一端的所有数据都进行解密。

link state routing protocol：链路状态路由协议

一种路由协议，维护一张所有已连接网络的拓扑图，并且使用这张拓扑图确定到达目的地的最短路径。

local alarm systems：本地警报系统

广播可听到的警报信号的警报系统，这个最远信号可以传播 400 英尺。另外，本地警报系统必须受到保护，通常由保安进行保护，以防止受到损害和破坏。为了使警报系统有效，附近必须有安全团队或保安，他们可以在警报触发后立即进行响应。

Local Area Network：局域网(LAN)

一种受地理限制的网络形式，例如通常在一间单独的办公室、一栋建筑物或一条城市街区中。

local cache：本地缓存

暂时存储在客户端上的任意内容，用于将来重新使用。一个典型的客户端上有许多本地缓存，包括 ARP 缓存、DNS 缓存以及互联网文件缓存。

log analysis：日志分析

一种更加详细的、系统化的监控形式，在详细分析过程中，对已记录日志的信息进行趋势和图形分析，还对异常的、未授权的、违法的和破坏安全策略的活动进行分析。

logging：日志记录

将事件或所发生情况的相关信息记录到日志文件或数据库中的活动。

logic bomb：逻辑炸弹

恶意代码客体，在达到一个或多个满足的逻辑条件前保持休眠。在满足逻辑条件时，便被激发。

logical access control：逻辑访问控制

硬件或软件机制，可以用于管理对资源和系统的访问，并且提供对这些资源和系统的保护。逻辑访问控制和技术访问控制相同。逻辑访问控制包括加密、智能卡、密码、生物测定学、受限接口、访问控制列表、协议、防火墙、路由器、入侵检测系统和阈值级别等。

logical topology：逻辑拓扑

一种网络的逻辑运行，定义了设备的部署和组织以及用于彼此通信的方式，也称为信号拓扑。

logon credentials：登录凭证

为建立访问，由主体提供的身份标识和身份认证因素。

logon script：登录脚本

在用户登录时运行的脚本。登录脚本常常被用于将本地驱动器号映射为网络共享、启动程序或者打开与经常访问的系统的链接。

loopback address：回送地址

用于创建通过 TCP/IP 协议连接自身的软件接口的 IP 地址。回送地址只由软件处理。即使网络硬件和相关的设备驱动程序丢失或受损，回送地址也允许执行 TCP/IP 协议栈测试。

Low Water-Mark Mandatory Access Control：低水准强制访问控制(LOMAC)

针对 Linux 的内核模块，被设计用于保护进程和数据的完整性。为安全策略提供灵活支持的是 OS 安全体系结构扩展或增强。

M

M of N 控制

一种保护措施，在总数为N的代理中，最少需要M个代理一起工作才能完成安全性很高的任务。

machine language：机器语言

计算机可以直接执行的编程语言。

macro viruses：宏病毒

采用拙劣的技术感染在流行的 Microsoft Word 环境中生成的文档的病毒。

mail-bombing：邮件炸弹

一种攻击形式，当有足够数量的电子邮件信息被指向某个单一用户的邮箱或通过一台特定的 STMP 服务器时，就可能导致拒绝服务攻击。

maintenance：维护

在面临操作转换、数据处理、存储和环境需求时，为保证持续的运营所需的各种任务。

maintenance hook：维护挂接程序

只有系统开发者知道的系统入口点，也被称为后门。

malicious code：恶意代码

包括广泛的可编程的计算机安全威胁的代码对象，这些威胁针对不同的网络、操作系统、软件和物理安全脆弱性，从而将恶意的内容散播到计算机系统中。

mandatory access control：强制性访问控制

一种访问控制机制，使用安全标签来管理主体对客体的访问。

mandatory vacations 强制性休假

一种安全策略，要求所有的员工一年休假一次，这样可以审计和确认员工的工作任务和权限，通常比较容易检测到滥用、欺骗或疏忽行为。

man-in-the-middle attack：中间人攻击

一种攻击类型，在恶意用户能够将自己置身于通信链接的两个端点之间时发生。客户端和服务器都不知道有第三方正在截取并利用他们的通信会话。

man-made disasters：人为灾难

由人引起的灾难，包括爆炸、电气火灾、恐怖行为、电力中断、其他公共设施故障、基础设施故障、硬件/软件故障、劳工困境、偷窃和故意破坏。

mantrap：陷阱

通常由保安守护的双重门设置。陷阱的目的是牵制主体直到其身份得到确认和认证。

masquerading：伪装

使用他人的安全 ID，获得进入设施或系统的权利。

Massively Parallel Processing：大规模并行处理(MPP)

这种技术被用于建立包含数百个或上千个处理器的系统，每个处理器都有自己的操作系统和存储器/总线资源。

Master Boot Record：主引导记录(MBR)

硬盘驱动器或软盘的一部分，计算机用它在启动过程中装载操作系统。

Master Boot Record (MBR) virus：主引导记录病毒

攻击 MBR 的病毒，在系统读取受感染的 MBR 时，病毒引导它读取并且执行存储在另一个地方的代码，从而加载全部的病毒到内存中，可能会触发病毒有效载荷的传播。

Maximum Tolerable Downtime 或 Maximum Tolerable Outage：最大可容忍故障时间(MTD)或最大容许中断(MTO)

指业务功能无法实施而不会引起无法挽回的业务损失的最长时间。

MD2(消息摘要 2)

由 Ronald Rivest 在 1989 年开发的一种散列算法，为 8 位的处理器提供安全散列函数。

MD4

MD2 算法的一种增强版本，于 1990 年发布。它对消息进行填补，从而确保消息的长度比 512 位的倍数短 64 位。

MD5

MD4 算法的下一个版本，于 1991 年发布。它处理 512 位的消息分组，但是使用 4 轮明显不同的计算来生成与 MD2 和 MD4 算法长度一样的消息摘要(128 位)。一般已经被 SHA-1 或其他更现代的哈希算法所取代。

Mean Time To Failure：平均无故障时间(MTTF)

通常表示某种硬件或介质在可靠性出现问题和应该被替换之前，可以被重复使用的时间或次数。

Media Access Control address：介质访问控制(MAC)地址

一个由 6 个字节组成、以十六进制符号表示的地址。地址中的前三个字节指出了物理网络接口的生产厂商或制造商。后三个字节表示唯一的由制造商分配给接口的号码。没有两个设备会具有相同的 MAC 地址。

media analysis：介质分析

计算机取证分析的一个分支，涉及存储介质中信息的识别和提取。

meet-in-the-middle attack：中间相遇攻击

在中间相遇攻击中，攻击者使用一条已知的明文信息。然后，使用每一种可能的密钥(kl)加密这个明文，同时使用所有可能的密钥(k2)解密对应的密文。

memory：存储器

CPU 可以直接使用的主要内存资源。主存储器通常由易失性随机访问存储器(RAM)组成，通常是系统可以使用的最高性能存储资源。

memory card：存储卡

一种用于存储数据但不能处理数据的设备，通常由一些闪存器件构成。

memory page：存储页面

能够移动出入 RAM 的一大块内存，并且硬盘驱动器上的分页文件是虚拟内存系统的一部分。

memory protection：内存保护

一个核心的安全组件，必须对它进行设计和在操作系统中实现，用于防止一个活动进程与没有

专门指派或分配的内存区域进行交互。

memory-mapped I/O：存储映射 I/O

用于管理系统组件和 CPU 之间输入/输出的技术。

message：消息

针对某个对象的通信或输入(面向对象编程中的术语和概念)。

Message Digest：消息摘要(MD)

一条消息内容的概要(与文件校验和不同)，由散列算法产生。

metadata：元数据

针对数据仓库的数据挖掘操作的结果。

metamodel：元模型

模型的模型。因为螺旋模型封装了另一个模型(瀑布模型)的许多迭代，所以被视为一种元模型。

Metasploit

一种漏洞扫描和渗透测试工具，用于利用应用程序、计算机和网络系统中的缺陷。

methods：方法

在面向对象编程环境中，对象针对输入(消息)生成输出(行为)所执行的动作或功能。

microcode：微码

被用于描述存储在 ROM 芯片中的软件的术语，也称为固件。

military and intelligence attacks：军事和情报攻击

主要用于获得机密的和受限制的执法部门或军事信息和技术研究信息。

MIME Object Security Services：MIME 对象安全服务(MOSS)

可以为电子邮件信息提供真实性、机密性、完整性和不可否认性。

misuse case testing：误用用例测试

软件测试人员用来评估软件脆弱性对应已知风险的过程。测试人员首先列举已知的误用情况，然后尝试利用手动和/或自动攻击技术利用这些用例，也称为滥用用例测试。

mitigated：缓解

削弱风险的过程。

Mobile Device Management：移动设备管理(MDM)

一个管理移动设备的软件解决方案，该方案解决员工使用移动设备访问公司资源的挑战性任务。MDM 的目标是提高安全性，提供监测、远程管理、支持和故障排除。

mobile sites：移动场所

移动场所对于传统的恢复场所而言属于非主流的替代方案。它们通常由设备齐全的拖车或其他容易重新安置的单元组成。

Modem：调制解调器

一个传统的陆线调制解调器(调制器-解调器)是一种通信装置，其在模拟信号和数字信息之间进行覆盖或调制，以支持在公共电话网络(PSTN)线路上进行计算机通信。

modification attack：修改攻击

一种攻击，能够更改被捕获的数据包，然后将其放回到系统中。被修改的数据包被设计为能够避开改良的身份认证机制和会话排序限制。

module testing：模块测试

对存在不同规范的每个独立的或自包含的代码段都进行独立于其他所有模块的测试，也可以被称为组件测试。模块测试可以被视为单元测试的父类或超类。

modulo：模

在除法操作完成后得到的余数。

MONDEX

被设计用于管理智能卡上现金的一种电子支付系统和协议。

monitoring：监控

指手工或利用程序审查已记录的日志的信息，以便寻找特殊情况的活动。

motion detector：运动探测仪

在特殊区域使用的设备，用于感知物体的运动。

multicast：多播

针对多个确定接收者的通信传输方法。

multifactor authentication：多因素认证

使用两个或多个因素认证。多因素身份认证使用多个因素(你知道什么、你拥有什么和你是什么)。相比之下，密码和 PIN 并不能算作多因素身份认证，因为这两种方法都属你知道什么。

multilayer protocols：多层协议

一个协议套件或集合，包括几十个跨越 OSI 模型不同协议栈层的单独协议。TCP/IP 是一个常见的多层协议。

multilevel security mode：多级安全模式

被授权在多种安全级别上处理信息的系统，即使在所有系统用户都没有恰当的许可或需要了解所有系统处理的信息的情况下也是如此。

multimedia collaboration：多媒体协作

多媒体协作是使用不同的多媒体通信解决方案来支持远程协作(人们通过远程在一个项目上一同工作)。通常，协作允许人员跨越不同的时间框架同时工作。协作可以通过多媒体功能用于跟踪变化。协作可以和电子邮件、聊天、VoIP、视频会议、电子白板的使用、在线文档编辑、实时文件交换、版本控制以及其他工具进行合作。

multipartite virus：多歧病毒

这种病毒使用不止一种传播技术，试图穿透只有一种或其他某种防御方法的系统。

multiprocessing：多重处理

这种技术可以使计算系统利用多个处理器的能力完成一个应用程序的处理任务。

multiprogramming：多程序设计

为了达到提高运算效率的目的，多程序设计通过操作系统对一个处理器上的两个任务进行协调，模拟两个任务同时执行的情况。多程序设计被认为是一种相对过时的技术，除了在比较老的系统中能够找到，如今已经很少使用了。

MultiProtocol Label Switching：多协议标签交换(MPLS)

一种高通过、高性能的网络技术，它将数据在网络中以基于最短路径的标签而不是更长的网络地址进行传输。

multistate：多态

这个术语用于描述经过认证、可使用特定安全机制同时处理多个安全级别问题的系统。这些安全机制被设计用来阻止信息跨越不同的安全级别。

multitasking：多任务处理

指同时处理两个或更多个任务的系统。

multithreading：多线程处理

多个用户使用相同的进程而不会彼此影响。

mutation fuzzing：突变 fuzzing

一种修改已知输入以创建可能触发意外的合成输入的 fuzzing 形式，也称为变异 fuzzing。

Mutual Assistance Agreement：相互援助协议(MAA)

两个组织保证在灾难发生的时候通过共享计算设施或其他技术资源彼此相互援助的协议。

N

natural disaster：自然灾难

不是人为灾难，如地震、泥石流、沉孔、火灾、洪水、飓风、龙卷风、天降陨石、暴雪、暴雨、冰灾、潮湿、炎热和极度寒冷等。

need to know：知其所需

为了执行特殊工作任务具有访问、了解或占有数据或资源的要求。为了获得访问数据或资源的权利，用户必须具有“知其所需”权限。即使用户与所请求的信息具有相同的安全级别，或者具有比所请求资源更高的安全级别，如果没有“知其所需”权限，那么也会被拒绝访问。

negligence：疏忽

在特定情况下没有进行适当的关注，从而导致对另一方的无意识伤害。

Nessus

漏洞扫描器。

NetBEUI

NetBIOS 扩展用户界面(NetBEUI，又名 NetBIOS 帧协议或 NBF)是微软最广泛认知的一个协议，在 1985 年被开发用于支持文件和打印机共享。微软已经通过将 NetBIOS 工作于 TCP/IP 上(NBT)使得 NetBEUI 支持现代网络。这反过来又支持服务器消息块(SMB)协议，也被称为通用互联网文件系统(CIFS)。作为一个低层协议，NetBEUI 已不再获得支持；只有 SMB 和 CIFS 仍在使用。

Network Access Control：网络接入控制(NAC)

一种访问控制环境中通过严格遵守和实施安全策略的概念。NAC 领域的目标是预防/减少零日攻击，加强网络通信的安全策略，使用验证完成访问控制。

Network Address Translation：网络地址转换(NAT)

这种机制将信息包头内部的不可路由 IP 地址转换为公共 IP 地址，从而在互联网上进行传输。

network analysis 或 network forensic analysis：网络分析或网络取证分析

收集不同来源的信息，并将其关联起来，然后完成一份尽可能全面的网络构图。

network-based IDS：网络型 IDS

为监视网络而安装在一台主机上的 IDS。网络型 IDS 通过捕获和评估网络数据包来检测攻击或异常事件。

network discovery scanning：网络发现扫描

使用多种技术对一系列 IP 地址进行扫描，搜索配有开放网络端口的系统。网络发现扫描器实际上不能探测系统的漏洞，只是提供一份网络检测的系统显示报告和一份端口清单，这份清单通过网络和服务器防火墙公开了隐藏在扫描器和扫描系统之间网络路径上的端口。

Network Layer：网络层

OSI 模型的第 3 层。

network monitoring 网络监控

获取有关网络的信息的监视流量模式的行为。

network topology 或 physical topology：网络拓扑或物理拓扑

计算机和网络连接设备的物理布局和组织。

neural network：神经网络

在这种系统中，互相插入的和最终合计生成预期结果的计算决策长链被建立起来。

nmap

渗透测试工具，能够执行端口扫描、ping 扫描、banner 抓取、网络发现等。

noise：噪声

稳定的干扰破坏。

nonce：现时

密码学软件中使用的是随机数字发生器变量，每次使用时都会创建一个独特的新值，往往建立在基于种子值的时间标记的基础上。

NonCompete Agreement：竞业禁止协议(NCA)

竞业禁止协议试图阻止格外了解组织秘密的员工加入另一个存在竞争关系的组织，从而使第二个机构不能受益于该员工所了解的秘密。

NonDisclosure Agreement：保密协议(NDA)

被用于保护组织的机密信息不会被以前的员工泄漏的文档。当员工签署保密协议的时候，他们同意不对组织以外的任何人泄露被定义为机密级的信息。如果违反了保密协议，那么常常会遭到严厉的处罚。

nondiscretionary access control：非自主访问控制

一种访问控制机制，使用角色或任务来管理主体对客体的访问。

noninterference model：无干扰模型

以松散的信息流模型为基础。如果一个主体的操作影响了另一个主体的系统状态或操作，无干扰模型会给予关注。

non-IP protocols：非 IP 协议

非 IP 协议是作为一种替代 IP 并工作在 OSI 的网络层的协议。在过去，非 IP 协议被广泛使用。然而，与 TCP/IP 的主导地位和成功相比，非 IP 协议已成为专用网络的范畴。三个最被认可的非 IP 协议是 IPX、AppleTalk 和 NETBUI。

nonrepudiation：不可否认性

一种安全控制或应用的特性，可以确保消息的发送者或者活动或事件的主体不能否认所发生的事件。

nonvolatile storage：非易失性存储设备

不依赖于电源的供电维持存储内容。磁性的/光学的介质和非易失性 RAM (NVRAM)都是非易失性存储设备的例子。

normal forms：规格化形式

组织设计的提高有效数据库的不同级别。

normalization：规格化

删除冗余数据并确保所有特性都依赖于主键的数据库过程。

NOT：非

一种操作(用符号或!来表示)，简单地将输入值取反。这个功能每次只对一个变量进行操作。

O

Oauth：公开认证

一个开放标准，它与 HTTP 协作，允许用户以单一账户登录多个站点/位置。

object：客体

为主体提供信息或数据的被动实体。客体可以是文件、数据库、计算机、程序、过程、打印机或存储介质等。

Object Linking and Embedding：对象链接与嵌入(OLE)

一种 Microsoft 技术，用于将数据对象链接嵌入计算机上的多个文件或资源。

Object-Oriented Programming：面向对象编程(OOP)

这种编程方法使用被称为对象的封装代码集。OOP 最适合消除错误传播和模仿真实场景。

object-relational database：对象关系数据库

组合了面向对象编程环境的关系数据库。

off-boarding：下线

一旦员工离开组织，员工的身份将从身份和访问管理系统中移除。

on-boarding：在线

向组织的身份和访问管理系统添加新员工的过程。当员工的角色或位置改变时，或者当他们被授予额外的特权或访问级别时，也使用在线过程。

one-time pad：一次性填充

一种极强大的替代密码。对每一条消息都使用不同的密钥。密钥的长度与消息的长度一样。

one-time password：一次性密码

每次使用时都会发生改变的一种动态密码。

one-upped constructed password：单字符构造不同密码

只有一个字符与其字典形式有差异的密码。

one-way encryption：单向加密

对密码、消息、CRC 等执行的数学函数，生成一个不可逆转的加密编码。

one-way function：单向函数

一种数学运算，它可以通过所有可能的输入值组合得出结果，但是反向得出输入值却是不可能的。公钥密码系统建立在某种单向函数的基础上。

OpenID

一个开放 SSO 标准，由公司 OpenID Foundation 维护，OpenID 可与 OAuth 连同使用，也可单独使用。

open relay agent：开放中继代理

SMTP 服务器被配置为接受来自任何来源的电子邮件，并将其转发到其他目标。开放中继代理通常被垃圾邮件发送者劫持。

Open System Authentication：开放系统身份认证(OSA)

不要求真正身份认证的无线网络的一种连接模式。只要能够在客户端和 WAP 之间传送无线电信号，那么就允许通信。

OSI 模型

这个标准模型为所有的计算机系统建立了一个通用的通信结构或标准。

Open Web Application Security Project：Web 应用程序安全项目(OWASP)

OWASP 是一个非营利性的安全项目，其重点在于提高在线或基于 Web 的应用程序的安全性。

operational plans：操作计划

一种短期计划，是基于战略和战术计划的非常详细的计划。它们只在很短的时间内有效或有用。为了服从战术计划，操作计划必须经常被更新(如每个月或每个季度)。操作计划是详细的计划，它们清楚地说明了如何完成组织的不同目标。

operations security triple：操作安全三元组

资产、脆弱性和威胁之间的关系。

OR：或

一种逻辑运算(利用符号/来表示)，可以检查是否至少有一个输入值为真。

Orthogonal Frequency-Division Multiplexing：正交频分复用(OFDM)

这种无线技术利用允许传输进行更紧密压缩的数字载波调制模式。

Output FeedBack：输出回馈(OFB)

在这种模式中，DES 将明文与种子值相异或。针对第一个加密分组，一个初始值向量被用来建立种子值。以后的种子值通过在之前的种子值上运行 DES 算法取得。OFB 模式的主要优点是传输的错误不进行传播，从而不会影响以后分组的解密。

overt channel：公开通道

由安全策略说明的一种明显的、可视的、可检测的且已知的通信方法，随后由逻辑性或技术性访问控制进行控制。

owner：所有者

对保护和存储数据负有最终法人责任的人。如果所有者在建立和执行安全策略以便保护和维护敏感数据时没有尽职，那么可能要对疏漏承担责任。所有者常常就是 CEO、董事长或部门领导。

ownership：所有权

对个人或群体(例如使某人成为所有者)正式职责的指定。

P

package：包

在针对信息技术安全评估的通用准则环境中，包是一组能够从目标系统中删除或添加的安全特性。

packet：数据包

包含数据和目标地址的消息的一部分，也被称为数据报，通常位于网络层。

packet sniffing：数据包嗅探

从网络中捕获数据包并期望从信息数据包的内容中抽取出有用信息的行为。

padded cell：填充单元

与蜜罐系统类似，当入侵者被IDS 检测到的时候，入侵者被自动地转移到一个填充单元。填充单元具有实际网络的结构和布局，但是在填充单元里，入侵者既不能执行任何恶意的活动，也不能访问任何机密数据。填充单元是一个模拟环境，通过提供伪造数据来吸引入侵者的兴趣。

pairing：配对

通过蓝牙连接两个设备。

palm geography：手掌特征

生物测定学因素的一个例子，它是主体唯一的行为或生理上的特征。人手的形状被用来建立身份标识或提供身份认证。

palm scan：手掌扫描

物理识别因素的一个例子，对于主体是唯一的。用近红外光测量手掌的静脉模式，这些跟指纹一样，是独一无二的。每个人不需要接触扫描仪，只需要把他们的手掌放在扫描仪的上方。一些手掌扫描识别人的手掌上的凹凸褶皱布局，以建立身份或提供认证。

palm topography：手部外形

生物测定学因素的一个例子，它是主体唯一的行为或生理上的特征。人的手形常被用来建立身份标识或提供身份认证。人的手掌上的凹凸褶皱布局，可用以建立身份或提供认证。这与手掌扫描相同，类似于指纹。

parallel data systems or parallel computing：并行数据系统或并行计算

计算系统设计用于同时进行大量的计算，但并行数据系统往往远远超出了基本的多处理能力。它们通常将包括一个大的任务划分成更小元素的概念，然后将每个子元素分发到不同的子处理系统上进行并行计算。这个实现基于这样一个思路：有些问题如果拆解成更小的任务并同时处理，可以更加有效地得到解决。

parallel run：并行运行

在这种新的系统部署测试中，新系统和旧系统并行运行。

parallel tests：平行测试

涉及将实际人员重新部署到替换的恢复场所和实现场所启用措施的测试。

parole evidence rule：口头证据规则

这条规则说明当双方的协议被以书面的形式记载下来时，书面文档被假设包含协议的所有条款，并且口头协议不可以修改书面协议。

partial-knowledge teams：partial 认识水平团队

在渗透测试之前，这支团队拥有组织资产的详细记录(包括硬件和软件目录)。

passphrase：密码短语

通常是一串字符，其长度要比密码长得多。一旦输入密码短语，系统会为了身份认证过程的使用而将其转换为实际密码。密码短语常常是修改过的母语语句，这样可以简化记忆。

password：密码

由主体输入的作为身份认证要素的字符串。

password Authentication Protocol：密码身份认证协议(PAP)

一种标准的 PPP 验证协议。PAP 以明码的形式传递用户名和密码。PAP 没有提供加密的形式，它简单地提供了一种方法，从客户端向验证服务器传递登录证书。

Password-Based Key Derivation Function 2：基于密码的密钥导出函数 2(PBKDF2)

一个密钥延伸技术的例子。PBKDF2 在输入密码上使用散列操作、加密函数或 HMAC 操作(即在散列过程中使用对称密钥)，该操作与盐组合。然后将这个过程重复数千次。

password policy：密码策略

组织安全策略的一部分，规定了密码的规则、限制和要求。还可以规定部署在系统上的程序化的控制措施，以便加强密码的强度。

password restrictions：密码限制

定义密码最低要求的规则，如长度、字符组成成分和使用时限。

patch management：补丁管理

确保相关补丁应用于系统的程序。理想情况下，会评估、测试和部署补丁，并审核系统以验证补丁是否已应用并且未被删除。

patent：专利

政府允许的、授予发明的创造者在设定好的一段时间内独家制作、使用和销售的权利。

Peer To Peer：点对点(P2P)

网络和分布式应用程序的解决方案，用于在点对点实体间共享任务和工作负载。

P2P network：点对点网络

一种网络架构，单个设备之间不需要或使用主要控制实体或设备。

penetration testing：渗透测试

一种用于检测所采用的安全保护措施的强度和有效性、带有经过授权的入侵攻击企图的操作。渗透测试应该得到管理人员的同意和了解。

period analysis：频率分析

检查基于密钥长度重复模式的加密文本。密钥长度是重复的周期。这通常是多字母替代密码的缺陷或脆弱性，这会导致频率分析的过程。

Permanent Virtual Circuit：永久虚电路(PVC)

一条预定义的虚电路，对帧中继用户始终保持可用。

Personal Identification Number：个人身份号码(PIN)

分配给个人的数字或代码，被用作身份识别的因素。PIN 应该保密。

Personal Identity Verification：个人身份认证(PIV)

美国政府内部个人使用的智能卡，里面包含了所有者的照片和其他识别信息，可以用作徽章和智能卡。

Personally Identifiable Information：个人身份信息(PII)

可以很容易地和/或明显地追溯到源头的人或涉及人员的任何数据项。

personnel management：人员管理

维护操作安全时的一项重要因素。人员管理是行政性控制或行政性管理的一种形式。

phishing：网络钓鱼

一种社交工程陷阱，试图诱骗用户，使之掉以轻心，从而打开附件或链接，获取用户敏感信息。它不加区别地发送给大量用户。

phone phreaking 或 phreakin：电话线路盗用

闯入电话公司的计算机，并且设置免费电话的过程。

physical access control：物理访问控制

作为物理屏障，可以用于阻止对系统的直接访问。例如，物理性访问控制包括保安、栅栏、运动探测仪、带锁的门、密封窗、照明、线缆保护、笔记本电脑锁、刷卡、狗、闭路电视、陷阱和警报器。

Physical Layer：物理层

OSI 模型的第 1 层。

piggybacking：混入

跟随着某个人通过受到安全保护的门或通道，而自身没有接受身份标识或授权。

ping

排除连接故障的实用程序，被用于测试某个 IP 地址是否可以访问。

ping-of-death attack：死亡之 ping 攻击

一种 DoS 类型。死亡之 ping 攻击采用超长的 ping 数据包。利用特定的工具，攻击者可以向一个受害者发送大量的超长 ping 包。在很多情况中，当受害系统试图处理信息包时，错误就发生了。这种攻击可能会导致系统的冻结、崩溃或重新启动。

Plain Old Telephone Service：普通老式电话业务(POTS)

普通的电话服务。

plain text：明文

没有被加密的消息。

Platform as a Service：平台即服务(PaaS)

提供计算平台和软件解决方案作为虚拟的或基于云的服务的云计算概念。从本质上讲，这种类型的云计算解决方案提供了一个平台的所有方面(即操作系统和完整的解决方案)。

Point-to-Point Protocol：点对点协议(PPP)

一种全双工协议，用于各种非 LAN 连接(如调制解调器、综合业务数字网、虚拟专用网和帧中继等)上的 TCP/IP 数据包的传递。PPP 得到了广泛支持，并且是拨号互联网连接的传输协议。

Point-to-Point Tunneling Protocol：点对点隧道协议(PPTP)

它是对 PPP 的增强，在通信的双方节点之间建立加密的隧道。PPTP 用在虚拟专用网中，但是常常会被第 2 层隧道协议代替。

polyalphabetic substitution：多字母替代

使用逐字母变化和来自不同语言或国家的多个字母对消息进行加密的密码转换方法。

polyinstantiation：多实例

发生在同一个表中的两行或更多行上，看似具有相同的主键，但是包含使用在不同分类级别上的不同数据。多实例常常被用于防范某些类型的推理攻击。

polymorphic virus：多态病毒

在系统间传输时实际上会修改自己代码的病毒。这些病毒的传播和破坏技术保持完全相同，但是每次感染新的系统时病毒的特征略有不同。

polymorphism：多态性

在面向对象编程术语和概念中，由于外部条件的变化，对象基于相同消息和方法提供不同行为的特征。

port：端口

协议中的一种连接地址。

Port Address Translation：端口地址转换(PAT)

这种机制将数据包头中的内部不可路由 IP 地址转换为能够用于 Internet 传输的公共 IP 地址和端口号。通过使用端口，PAT 支持内部 IP 地址到外部 IP 地址的多对一映射。

port isolation 或 private ports：端口隔离或私有端口

私有 VLAN 的配置是为了使用一个专用的或预留的上行端口。私有 VLAN 或端口隔离 VLAN 的成员仅可以通过预定的出口或上行端口进行相互通信。一种端口隔离的常见示例是在酒店里。

port scan：端口扫描

由入侵者使用的探查网络上所有工作系统的软件，并且能够确定每台计算机上运行的公共服务。

postmortem review：事后回顾

在活动完成后进行的分析和回顾，以便确定是否成功以及需要改进的地方。

Post Office Protocol：邮局协议(POP)

用于从电子邮件服务器向电子邮件客户端传输电子邮件的协议。

preaction system：预先响应系统

一种干管道/湿管道系统的组合系统。此系统一直是干管道系统，直到检测到有火灾发生(烟、热及其他)，然后向管道中充满水。由于受热，洒水头活动触发器被融化之后释放出水。如果在洒水头被触发之前火被熄灭，那么管道可以被手工排空并重新设置。这种系统还允许在洒水头触发洒水装置之前进行人工干预停止放水。预先响应系统最适用于计算机和人都存在的环境的洒水系统。

Presentation Layer：表示层

OSI 模型的第 6 层。

pretexting：假冒身份

这种攻击通过假冒他人获得你的个人信息。通常与网络钓鱼和其他社会工程学攻击相关。

Pretty Good Privacy：可靠隐私(PGP)

一种公钥-私钥系统，它使用 IDEA 算法对文件和电子邮件报文进行加密。PGP 不是一种标准，而是一种独立开发的产品，并且得到了互联网领域的广泛支持。

preventive access control：预防性访问控制

这种访问控制方法被部署用于阻止不必要的或未经授权的行为发生。预防性访问控制包括保安、安全策略、安全意识训练和反病毒软件。

preventive control：预防性控制

任何可以阻止和减轻不必要的行为或事件的机制、工具或措施。

primary key：主键

从表的一组候选键中选出的用来唯一标识表中记录的键被称为主键。每个表只有一个主键。

primary memory：主存储器

通常由易失性的随机访问存储器(RAM)组成的存储设备，一般是系统可以获得的最高性能的存储资源。

Primary Rate Interface：主速率接口(PRI)

一种 ISDN 服务类型，提供了多达 23 个 B 通道和 1 个 D 通道。因此，一条 PRI ISDN 连接提供了 1.544Mbps 的吞吐率，与 T1 线路的传输速率相同。

primary storage：主存储设备

计算机用来存放必要信息的容易访问的 RAM。

principle of least privilege：最小特权原则

属于访问控制学，描述主体为了完成工作任务被允许获得的最少的访问控制权。

privacy：隐私

机密性的一项内容，用于防止有关个体或企业的个人或敏感信息被泄漏。

Privacy Act of 1974：1974 年的隐私法案

本法律规定，政府机构只能维护完成公务需要的记录，应该销毁合法工作中不再需要的记录。

它还提供了正规的过程，以便个人访问政府维护的与本人相关的记录，并请求修改错误的记录。此法案还严格限制了美国联邦政府处理个人的私有信息的方式。

Privacy Enhanced Mail：增强隐私的邮件(PEM)

电子邮件的一种加密机制，提供了身份认证、完整性、机密性和不可否认性。PEM 是一个第 7 层协议。PEM 使用 RSA、DES 和 X.509。

private：私有的

商业企业/私营部门的一种分类，指私有的或个人特性的数据，只供内部使用。如果私有数据被泄漏，那么会对公司或个人产生重大的负面影响。

Private Branch eXchange：专用分组交换机(PBX)

一种成熟的电话系统，常被企业用于提供接入电话呼叫支持、分机至分机呼叫、电话会议和语言邮件。既可以作为单机电话系统网络使用，也可以与 IT 基础设施集成在一起。

private cloud：私有云

私有云部署模型包括一个组织的基于云计算的资产。组织可以使用自己的资源创建和管理私有云。组织负责所有维护工作。然而，组织也可以从第三方租赁资源并按照服务模型(SaaS、PaaS 或 IaaS)分割维护要求。

private IP addresses：私有 IP 地址

RFC 1918 中定义的地址，不在互联网上路由。

private key：私钥

用于加密或解密信息的秘密值，并且要保持秘密，只有使用者才能知道。在非对称密码系统中与公钥联合使用。

privileged mode：特权模式

这种模式被设计用于给予操作系统访问由中央处理器支持的完整指令的权力。

privileged operations functions：特许操作功能

在受保护的 IT 环境中，需要特殊访问或特权才能执行的活动。在大多数情况下，这些功能只限于系统管理员和系统操作员。

privileges：特权

许可和权限的组合。许可是指用户可以在系统上执行的操作，例如更改系统时间。权限是指用户授予数据(如读取、写入、修改和删除)的访问级别。

problem state：问题状态

主动执行进程的状态。

procedure：措施

在安全环境中，是指详细的、按部就班的指导文档，描述了实施特殊安全机制、控制方法或解决方案所需的精确行动。

process isolation：进程隔离

系统设计过程中出现的基本安全措施之一。基本上，使用进程隔离机制(无论是操作系统的一部分或硬件本身的一部分)能够确保每个进程都具有自己独立的内存空间，以便进行数据的存储和应用程序编码自身的实际执行。

processor：处理器

PC 机的中央处理单元，负责处理系统中所有的功能。

Program Evaluation Review Technique：程序评审技术(PERT)

一种项目调度工具。这种方法被用于在开发阶段判定软件产品规模以及为风险评估计算标准偏差(SD)。PERT 将估计的每个组件的最小可能规模、典型规模和最大可能规模联系在一起。PERT 被用于直接改善项目管理和软件编码，以便生成更有效的软件。随着编程和管理能力的提高，实际生成的软件规模应当更小。

Programmable Logic Controllers：可编程逻辑控制器(PLC)

是一种采用一类可编程的存储器，用于其内部存储程序，执行逻辑运算、顺序控制、定时、计数与算术操作等面向用户的指令，并通过数字或模拟输入/输出控制各种类型的机械或生产过程。

Programmable Read-Only Memory：可编程只读存储器(PROM)

在制造过程中，PROM 芯片的内容没有在出厂前被“烧入”，这一点与标准的 ROM 芯片不一样。相反，PROM 芯片安装了特殊的功能，允许最终用户在芯片中烧入内容。

proprietary：专用

商业企业/私企机密信息的一种形式。如果专用数据被泄漏，那么对企业在竞争优势上将可能受到巨大的影响。

protected mode：保护模式

用户模式的另一个名称。用户应用程序所在的 Windows 操作环境中功能较弱的安全域。用户模式与内核模式(也称为特权模式)不同。用户模式提供受限资源，对硬件的间接和有限访问以及进程之间的隔离。

protection profile：保护轮廓

来自针对信息技术安全评估的通用准则，是主体声明其安全要求的评估元素。

protection rings：环保护

将操作系统中的代码和组件(以及应用程序、实用程序或在操作系统控制下运行的其他代码)组织为同心环的安全设计，每个环具有增加或减少的功能和访问级别。

protocol：协议

一组规则和约束，定义了数据如何在网络介质上(例如双绞线、无线传输等)进行传递。协议使得计算机到计算机之间的通信成为可能。

protocol translator：协议转换器

可在协议之间转换的设备或软件，通常能够在 IP 和 IPX 之间移动有效载荷，也称为网关。

proximity reader：邻近式读卡机

一种无源设备、场源设备或发送应答器，用于检查人员是否得到授权，并允许合法者通过设施的物理入口进入。邻近设备由经过授权的持卡人携带或持有，当持卡人通过邻近式读卡机的时候，邻近式读卡机能够确定持卡人的身份和是否有权访问。

proxy：代理

一种可以将数据包从一个网络拷贝到另一个网络的机制。为了保护内部或专有网络的身份，拷贝过程还改变了源和目标的地址。

prudent man rule：审慎者规则

援自联邦判决指导方针，这种规则要求高级行政长官在履行工作职责时对工作予以应尽关注，关注的程度与普通的做事谨慎的人在类似环境下的关注程度相同。

pseudo-flaws：虚假缺陷

经常被用在蜜罐系统和重要的资源上，模仿众所周知的操作系统脆弱性。

public：公开

最低级别的商业企业/私有部门分类。用于所有不适用于更高级别分类的数据。这些信息并不是要故意泄漏出去，但如果它们被泄漏了，对组织也不会造成严重的负面影响。

public cloud：公有云

云部署模型包括可供任何消费者租用或租赁的资产，并由外部云服务提供商(CSP)托管。服务级协议可以有效地确保 CSP 用可接受的水平向组织提供基于云的服务。

public key：公钥

对信息进行加密和解密的一个值，并且对所有用户公开，与非对称密钥密码系统中的私钥一起使用。

public key cryptosystem/public key cryptography：公钥密码系统/公钥算法

基于使用由公钥和私钥组成的密钥对集合的非对称加密算法的子集。使用这个对中的一个密钥加密消息，仅能用来自同一密钥对的另一个密钥来解密。

Public Key Infrastructure：公钥基础结构(PKI)

信任关系的一种结构，使相互不认识的双方之间的通信变得容易一些。

purging：清洗

删除介质内容的过程，这样介质就可以在较不安全的环境下重复使用。

Q

qualitative decision making：定性的决策制定

决策制定过程通常考虑非数字化的因素，如情感、投资者/用户的信心、劳动力的稳定性和其他关注的方面。这种类型的数据通常导致按优先等级进行分类(如高级、中级、低级)。

qualitative risk analysis：定性的风险分析

根据情景为风险等级和决策使用分类和分级的分析方法。

quality assurance check：质量保证(QA)检查

一种人员管理和项目管理形式，监督产品的开发过程。QA 检查确保开发的产品与规定的标准、实践方法、效率等一致。

quantitative decision making：定量的决策制定

使用数字和公式完成决策。选择根据业务的货币价值来表示。

quantitative risk analysis：定量的风险分析

为资产损失分配实际货币价值(美元)的方法。

R

radiation monitoring：辐射监控

一种特殊的探测或窃听形式，涉及无线电频率信号和其他有辐射的通信方法(包括声音和光线)的检测、捕获和记录。

Radio Frequency IDentification：无线射频识别(RFID)

这种技术使用电磁波频谱无线射频部分的电磁或静电耦合来确定特定的设备。每个 RFID 标记

都包含一个独特的标识符，这样一来，只要附近的天线/收发器激活该标记，那么就会将标识符传送回天线进行记录，或者被用于触发某种动作。例如，大多数现代的道路收费系统都使用司机附着在汽车挡风玻璃上的 RFID 设备，一旦天线“读取”到这种设备，车主的通行费用就会相应增加。在公司进行安全监控的前提下，RFID 设备也可以被用于追踪携带标记的个人、设备等。

Radio Frequency IDterference：射频干扰(RFI)

RFI 是由很多常见的电器(包括荧光灯、电缆、电加热器、计算机、电梯、电动机和电磁铁等)产生的一种噪声。RFI 会与 EMI 一样影响许多系统。

rainbow table：彩虹表

彩虹表提供预先计算的密码散列值。彩虹表通常用于破解以密码散列方式存储在系统中的密码。

Random Access Memory：随机存取存储器(RAM)

可读和可写的存储器，保存计算机在处理过程中使用的信息。只有当电源持续不断供应的时候，RAM 才保存着内容。

random access storage：随机存取存储设备

允许操作系统从介质中的任何一点读取数据的设备，如 RAM 和硬盘。

Read-Only Memory：只读存储器(ROM)

只能读但不能写的存储器。

ready state：就绪状态

准备执行但在排队等待 CPU 的状态。

real evidence：客观证据

那些可能会被实际带到法庭上的物品，也被称为实物证据。

real memory：实际的存储器

通常是计算机可以使用的最大的 RAM 存储资源。一股由许多动态的 RAM 芯片组成，因此，CPU 必须定期对它们进行刷新，也被称为主存储器或第一存储器。

realized risk：已发生的风险

在风险发生并且破坏、攻击或侵入已经出现时，可能或不可能造成资产损失、损害或泄漏的事故、遭遇或事件。

reasonableness check：合理性检查

制定和使用特殊的测试数据集，尽可能地运用软件的所有路径，并将结果与已知正确的预期输出进行比较。

record：记录

关系型数据库中表的内容。

record retention：记录保留

组织的一个策略，对应该保留什么样的信息和保留多长时间进行定义。在大多数情况下，相关的记录是用户活动的审计跟踪，这些记录可能包括对文件和资源的访问、登录模式、电子邮件和特权的使用。

record sequence checking：记录序列校验

与散列总数校验类似。然而，它没有对内容的完整性进行校验，而是对数据包或报文的序列完整性进行校验。

recovery access control：恢复访问控制

在安全策略遭到侵犯以后，用于修复或还原资源、功能和性能的一种访问控制类型。

recovery strategies：恢复策略

恢复某个业务的实践、策略和措施，包括指派最早响应严重事故的人员、执行关键的后续任务以及获得减少财务损失风险的保险费。

red boxes：红盒

用于模拟硬币存入付费电话时的声音。

reducing risk：降低风险

保护措施和应对措施的实施，也被称作缓解风险。

reduction analysis：降低分析

这个任务的目的是更好地理解产品逻辑及其与外部的交互元素。不管是应用程序、系统还是整个环境，都需要被分成更小的容器或隔间。如果关注的是软件、电脑或操作系统，这些可能是子程序、模块或客体；如果关注的是系统或网络，这些可能是协议；如果关注的是企业的整个基础设施，这些可能是部门、任务和网络。应该对识别出的每个子元素进行评估，以便理解输入、处理、安全性、数据管理、存储和输出。这有时也被称为分解应用程序、系统或环境。

Redundant Array of Independent Disks：冗余磁盘阵列(RAID)

一种存储设备技术，采用独特组合的多个硬盘驱动器来生成存储解决方案，从而提供更高的吞吐量以及对设备故障的抵抗力。

redundant servers：冗余服务器

一种容错部署选择，用于在发生灾难时提供各种服务器选择，例如镜像、电子存储、远程日志记录、数据库映射和群集。

reference monitor：引用监控器

安全内核的一部分，根据系统的访问控制机制验证用户的请求。

reference profile：参照轮廓

被存储的生物测定学因素采样。

referential integrity：参照完整性

用来强制两个表建立关系。关系中的一个表包含一个外键，对应于关系中另一个表的主键。

reflected input：反射式输入

当一个易受攻击的网站以通过输入框来欺骗网站的方式反馈脚本命令时，输入被反馈回访问者，就像它是原始的和合法的内容一样。

register：寄存器

CPU 携带的一种有限容量的板上存储器。

register address：寄存器地址

直接安装在 CPU 上的非常小的存储器位置。当 CPU 需要从其中一个寄存器(例如寄存器 1)获得信息来完成运算任务时，可以只使用寄存器地址来访问信息。

Registration Authority：注册授权机构(RA)

只读版本的认证授权机构。能够分发 CRL 和执行证书验证过程，但是不能创建新的证书。RA 被用于分担 CA 的工作量。

regulatory policy：规章式的策略

只要行业或法律标准适合组织，就需要规章式的策略。这种策略讨论了必须遵守的规章制度，并概略说明了被用来让人们遵守这些规章制度的措施。

reject risk：拒绝风险

拒绝风险的存在是希望通过对风险的忽视让风险永不发生。这是对风险的不可接受的反应，也被称作否认风险。

relational database：关系数据库

由包含一系列相关记录的表组成的数据库。

relationship：关系

关系数据库中表内信息的关联。

relevant：相关

证据的一种特性，可以被用于在法庭上确定事实。

Remote Authentication Dial-In User Service：远程验证拨号用户服务(RADIUS)

用于集中远程拨号连接的验证服务。

remote journaling：远程日志处理

传输数据库事务日志的副本，其中包括从上次大量传输以来发生的事务。

remote mirroring：远程镜像

维护备份场所的实时的数据库服务器，这是最先进的数据库备份方案。

remote wipe：远程擦除

一个移动设备安全特征，可以远程删除设备上的所有数据，甚至配置设置。

repeater：中继器

一种网络设备，用于放大网络连线上的信号，允许两个节点之间有更长的距离，也可称为集中器或放大器。

replay attack：重放攻击

一种攻击行为，发生时恶意用户记录下客户端和服务器之间的通信。随后从客户端发往服务器的数据包被重放或重新传递到服务器，并且带有稍许不同的时间戳和源 IP 地址(即哄骗)。在一些情况中，这准许恶意用户重新开始与服务器的旧的通信链接，也被称为回放攻击。

residual risk：剩余风险

对特定资产构成特定威胁的风险，高层管理部门选择不对这些资产实施保护措施。换句话说，剩余风险是管理层选择接受的风险而不是削弱的风险。

restricted interface model：约束接口模型

使用分类基础上的限制的一种模型，只提供主体指定的授权信息和功能。在某个分类级别上的主体将可以看到一系列的数据，并且可以使用一系列的功能；而另一个分类级别上的另一个主体将可以看到不同系列的数据，并且可以使用不同系列的功能。

retina scan：视网膜扫描

生物测定学因素的一个例子，它是主体独有的行为或生理上的特征。眼球后面血管的形状被用来建立身份标识或提供身份认证。

Reverse Address Resolution Protocol：反向地址解析协议(RARP)

TCP/IP 协议组的一个子协议，运作在数据链路层(第 2 层)上。RARP 被用于通过使用轮询系统

的 MAC 地址来发现其 IP 地址。

reverse engineering：逆向工程

这被视为不道德的社会工程学形式。编程人员反编译代码，从而理解其功能的所有细节(特别是在生成类似的、竞争性的或兼容的产品时更是如此)。

reverse hash matching：逆向散列匹配

通过生成可能的消息、对这些消息进行散列运算、比较散列值与原有的散列值，从而发现经过散列运算的原始消息的过程。当 H(M) =H (M')时，那么 M = M'。

revocation：取消

准许一个 PKI 证书被取消的机制，能够有效地从系统中删除用户。

RFC 1918

定义公共和私有 IP 地址的公共标准。

Rijndael 分组密码

被选中代替 DES 的一种分组密码。Rijndael 密码准许使用下列三种密钥强度：128 位、192 位和 256 位。

risk：风险

风险是任何一种特定的威胁利用特定脆弱性从而导致损害资产的可能性，是对可能性、概率或偶然性的评估。风险=威胁+弱点。

risk analysis：风险分析

风险管理的内容，包括：分析风险存在的环境，评估每种风险发生的可能性和造成的损失是多少，评估各种应对风险措施的成本，生成安全措施的成本/效益报告并呈交给上层管理部门。

risk framework 风险框架

关于如何评估风险、解决风险和监管风险的指导或方法。

risk management：风险管理

是识别可能造成数据损坏或泄漏因素的详细过程，根据数据的价值评估这些因素和应对措施的成本，并且为了减轻或降低风险而实施有成本效益的解决方案。

risk tolerance：风险容忍度

组织忍受与所发生风险相关的损失的能力。

RSA

以 Rivest、Shamir 和 Adleman 三位发明人的名字命名的公钥加密算法。

role-based access control：角色型访问控制

非自主访问控制的一种类型，通过使用工作职能角色控制主体对客体进行访问。

root

系统的管理员级用户。

rooting

rooting 会移除 Android 设备上的限制，并允许 root 级别访问底层操作系统。它类似于越狱运行 iOS 操作系统的设备。

rootkit

一种专用软件包，允许黑客获得扩展的系统访问权限。

router：路由器

用于控制网络上通信流的网络设备。路由器常常被用来连接相似的网络，并且控制两者之间的通信流。路由器可以利用静态定义的路由表进行工作，也可以采用动态的路由系统进行工作。

rule-based access control：规则型访问控制

强制访问控制的一种变化形式。规则型的系统使用一系列规则、限制或过滤器决定在系统上可以做什么，不可以做什么，如准许主体对客体进行访问或执行某个操作，或者访问某个资源。防火墙、代理和路由器是规则型访问控制系统的常见例子。

running key cipher：滚动密钥密码

在这种密码学中，密钥被指定为某个变化源，如《纽约时报》的第 3 页。

running state：运行状态

进程被主动执行的状态，也被称为问题状态。

S

sabotage：阴谋破坏

对组织有深入了解的员工对组织实施的犯罪行为。

safe harbor：安全港

它是一个控制机制，包括一系列安全港法则。目标是防止未授权的信息泄露，由数据处理者处理数据，以及在数据处理者和数据控制者之间进行传输。如果他们同意遵守 7 项法规和条款 15 中描述的要求，并且经常提问，美国公司可以自愿选择进入项目。

safeguard：防护措施

是指能消除脆弱性或对付一种或多种特殊威胁的任何方法，也被称为应对措施。

sag：电压不足

瞬间的低电压。

salami 攻击

这种攻击收集少量的数据以构造具有更大价值或更高敏感度的事物。

salt：盐

附加于密码的一个随机数，从而增加了随机性，并且确保最后存储的散列值的唯一性。

sampling：抽样

数据简化的一种形式，允许审计人员从审计跟踪中快速地确定重要的问题或事件。

sandbox：沙箱

Java applet 在其内部执行的安全边界。

sandboxing：沙箱

一种安全技术，为应用提供了一条安全边界，以防止应用程序与其他应用程序交互。反恶意软件应用程序使用沙箱技术来检测未知的应用。如果应用程序显示可疑特征，沙箱技术能够防止应用程序感染其他应用程序或操作系统。

sanitization：净化

实际上是准备销毁介质的任意数量的过程，用于保证不能以任何方式恢复销毁或丢弃的介质上的数据。净化也可以是销毁介质的实际方法。介质可以通过清理或消磁得到净化，而不需要对介质进行物理销毁。

scanning：扫描

很像你的邻居准备对你实施盗窃，这是潜在的入侵者寻找进入你的系统所使用的过程。扫描可能预示着有非法行为将会随后发生，因此我们将扫描视为事故，并且收集扫描操作的证据是个很好的主意。

scavenging：打扫

使用电子设备执行垃圾挖掘的一种形式。联机打扫是从进程或任务完成之后留在上面的剩余数据中搜索有用的信息。这些信息可能是审计跟踪、日志文件、内存转储、变量设置、端口映射和缓存的数据等。

scenario：场景

关于风险评估，对单个主要威胁的书面描述。描述的重心集中在威胁是如何产生的及其对组织、IT 基础设施和特定的资产会产生什么影响。

schema：模式

这个结构拥有定义或描述数据库的数据。模式是使用数据定义语言(DDL)编写的。

screen scraper 或 screen scraping：屏幕抓取/抓取

1) 远程控制、远程访问或远程桌面服务。2) 屏幕抓取这个技术可以让一个自动化的工具和人机接口互动。

script kiddie：脚本小子

恶意的个人不了解安全漏洞背后的技术，但从互联网上下载即用软件(或脚本)，并使用它们对系统发起攻击。

scripted access：脚本访问

使用向系统提供登录凭证的一个脚本自动化登录过程的方法。这种方法被视为一种单点登录。

search warrant：搜查证

通过司法系统获得的文件，它准许执法人员在没有事先警示犯罪嫌疑人的情况下从某个地点获取证据。

secondary evidence：次要证据

最佳证据内容的证据副本或口头说明。

secondary memory：辅助存储器

通常是指保存着 CPU 不能立刻获得的数据的磁性/光学介质和其他存储设备。

secondary storage：辅助存储设备

包括磁性的和光学介质的数据存储设备，如磁带、磁盘、硬盘和 CD/DVD 存储器。

second-tier attack：第二级攻击

这种攻击依赖于通过偷听或其他类似数据收集技术获得的信息或数据。换句话说，这是一种在其他某些攻击完成后才启动的攻击。

secret：秘密

政府/军方的一种分类，用于具有秘密性质的数据。未授权而泄露秘密数据将会有严重后果，并且可能导致对国家安全的重大破坏。

secure communication protocol：安全通信协议

使用加密技术为传输的数据提供安全的协议。

Secure Electronic Transaction：安全电子交易(SET)

互联网上进行交易传输时使用的一种安全保护协议。SET 工作在 RSA 加密以及 DES 的基础上。SET 受到一些主要的信用卡公司的支持，如 Visa 和 MasterCard。

Secure Hash Algorithm(SHA-1、SHA-2、SHA-3)：安全散列算法(SHA)(SHA-1、SHA-2、SHA-3)

由美国国家标准和技术协会(NIST)开发的政府标准散列函数，并在正式的政府出版物——安全散列标准(SHS)中进行了说明。SHA-1 产生一个 160 位的消息摘要输出。SHA-2 系列的成员创建了一系列哈希值输出：224、256、384 或 512。在撰写本书时，SHA-3 仍在开发中，但是已经为该新的标准选择了 Keccak 算法。

Secure HTTP：安全 HTTP(S-HTTP)

另一个重要的协议，用于提供万维网的安全性。

Secure Multipurpose Internet Mail Extensions：安全的多用途互联网邮件扩展(S/MIME)

对电子邮件和附件的传输提供保护的一种协议。

Secure Remote Procedure Call：安全远程过程调用(S-RPC)

这种身份认证服务提供了一种简单的方法，用于防止在远程系统上进行的未授权代码的执行。

Secure Shell：安全外壳(SSH)

一个端到端的加密技术。这是一组程序，提供常见互联网应用服务(如 FTP、Telnet 和 rlogin)的加密可选方案。SSH 实际上有两个版本。SSH1 支持 DES、3DES、IDEA 和 Blowfish 算法。SSH2 不支持 DES 和 IDEA，但是增加了对其他一些算法的支持。

Secure Sockets Layer：安全套接层(SSL)

由 Netscape 开发的用于保护 Web 服务器和 Web 浏览器之间通信的一种加密协议。

Security Assertion Markup Language：安全断言标记语言(SAML)

一种基于 XML 的语言，普遍用于联合组织之间交换认证和授权信息，常为浏览器访问提供单点登录功能。

security assessments：安全评估

对系统、应用程序或被测环境的安全性进行全面审查。在安全评估期间，受过训练的信息安全专业人员执行风险评估，识别被测环境中的漏洞，可以允许破坏并且根据需要提出修复建议。

Security Association：安全关联(SA)

在一个 IPSec 会话中，代表通信会话并记录有关连接配置和状态的所有信息的过程。

security audits：安全审计

评估执行的目的是向第三方展示控制的有效性。安全审计会使用与安全评估期间相同的许多技术，但必须由独立的审计员执行。为机构设计、实施和监测控制的员工在评估这些控制的有效性时存在固有的利益冲突。

security boundary：安全边界

任何两个具有不同安全要求或需求的区域、子网或环境之间的交线。

security control baselines：安全控制基线

一套强制性的安全控制，为实施安全和确保最低安全标准提供起点。

security governance：安全治理

安全治理是与支持、定义和指导组织安全工作相关的实践集合。

security ID：安全证

物理身份标识的一种形式，通常包含照片和/或带有个人附加信息的编码数据磁条。

security kernel：安全内核

操作系统服务的核心设置，这些设置控制着访问系统资源的所有用户/应用请求。

security label：安全标签

为确定保护客体并且防止未授权访问所需要的安全级别，在安全模式中使用的指定分类或敏感级别。

security management planning：安全管理计划编制

彻底和系统地设计程序和策略文档，以便减少风险，随后针对特定环境维持可接受的风险级别。

security mode：安全模式

美国政府为处理分类信息的系统指派了 4 种被批准的安全模式：专用模式、系统高级模式、分隔安全模式和多级模式。

security perimeter：安全边界

一条假想的界限，它把 TCB 与系统的其他部分分开。

security policy：安全策略

一种文档，用于定义组织所需的安全范围，规定了管理安全问题的方案，并讨论需要保护的资

产和安全解决方案应提供的所需保护措施的范围。

security professional：安全专家

受过培训和经验丰富的网络、系统和安全工程师，他们负责执行高层管理部门下达的指示。

security role：安全角色

个人在组织内部的整个安全实施和管理方案中扮演的角色。

security target：安全目标

来自针对信息技术安全评估的通用准则的评估要素，其中供应商声明了其产品的安全特性。

security tests：安全测试

安全测试能够验证控制在正常运行。这些测试包括自动扫描、工具辅助渗透测试和手动测试安全性。安全测试应该定期进行，需要关注保护机构的每个关键安全控件。

segment：段

传输层 TCP 报头和有效载荷的组合。

segmentation：分割

网络分割动作将网络细分成较小的组织单位。这些更小的单位、分组、分段或子网络(即子网)可以用来提高网络的各个方面。分割可以提高性能，减少拥塞，划分通信问题(如广播风暴)，并通过流量隔离提供安全改进。分割可以通过使用基于交换机的 VLAN、路由器或防火墙(以及所有这些组合)创建分段。

semantic integrity mechanisms：语义完整性机制

DBMS 的一种常用安全特性。这个特性确保不会违反任何结构上的规则。此外，它还检查所有存储的数据类型都位于有效的域范围内，确保只存在逻辑值，并且确认系统遵守任何和所有的唯一性约束。

senior management：高层管理者

最终负责组织安全维护和最关心保护资产的人。高层管理者必须对所有策略问题签字。高层管理者对安全解决方案的成功或失败负有全部责任，负责对组织在建立安全性方面予以适度关注，也被称作组织所有者和高层管理者。

sensitive：敏感

商业企业/私营部门的分类，用于分类级别高于公开数据的数据。如果敏感数据被泄漏，那么就会对公司产生负面影响。

sensitivity：敏感度

对于生物测定学设备，被配置成进行扫描的敏感级别。

separation of duties and responsibilities：任务和责任分离

一种常见操作，可以阻止任何一个主体具有阻止或停止安全机制的能力。通过把核心管理或高层责任分配给多个人，使得没有人能够进行严重的恶性行为或绕过实施的安全控制。

separation of privilege：特权分离

建立在最小特权原则之上的原则。它要求使用力度化访问特权，也就是说，给每一种类型的特权操作分配不同的特权。这就允许设计人员给一些进程分配执行某些特殊管理功能的权限，而不需要授予他们不受限制地访问系统的权限。

Sequenced Packet Exchange：顺序分组交换(SPX)

Novell 中 IPX/SPX 协议组的传输层协议。

sequential storage：顺序存储设备

这种设备在到达所要求的位置之前，需要读取(或快速经过)以前实际存储的所有数据。顺序存储设备的常见例子是磁带驱动器。

Serial Line Internet Protocol：网络串行线路协议(SLIP)

互联网串行线路协议是一种较老的技术，用于支持异步串行连接(如串行线缆或调制解调器拨号)上的 TCP/IP 通信。

service bureaus：服务局

这种业务通过合同约定租用计算机时间，并且在某些灾难以及需要实施灾难恢复计划或业务连续性计划的业务中断的情况下提供所有 I T 需求。

Service-Level Agreement：服务级别协议(SLA)

一份针对用户的合约式责任，要求执行可靠的 BCP 工作，还用于确保提供商提供的可靠的 BCP 工作的可接受服务级别。

Service Organization Controls (SOC) Report：服务组织控制(SOC)报告

由审核员生成的报告，其中包含云提供商的安全评估结果。

Service Provisioning Markup Language：服务配置标记语言(SPML)

一种标记语言，出于联合身份单点登录目的，专门设计用于用户信息交换。它源自标准通用标记语言(SGML)、可扩展标记语言(XML)和通用标记语言(GML)。

SESAME

一种票据型验证机制，类似于 Kerberos。

session hijacking：会话劫持

怀有恶意的人中途拦截经过授权的用户和资源之间通信数据的一部分，然后使用劫持技术接管这个会话并伪装成已授权用户的身份。

Session Layer：会话层

OSI 模型的第 5 层。

Shared Key Authentication：共享密钥身份认证(SKA)

在网络通信之前要求某种身份认证的无线网络所使用的连接机制。802.11 标准为 SKA 定义了被称为 WEP 的可选技术。

Shielded Twisted-Pair：屏蔽双绞线(STP)

一种双绞线，线缆的周围包有一层金属箔片，对外部电磁干扰(EMI)提供了额外的保护。

shoulder surfing：偷窥

通过留意显示器或操作者敲击键盘来收集系统中信息的行为。

shrink-wrap license agreement：收缩性薄膜包装许可协议

写在软件包装外面的协议。由于常常包括一个条款而得名，该条款规定，撕开封装软件包的收缩薄膜包装就承认了合同条款。

side-channel attack：边信道攻击

被动非侵入式攻击，去观察一个设备的操作。边信道攻击用于智能卡。常见的边信道攻击是功耗监控攻击、定时攻击和故障分析攻击。

signature-based detection：特征型检测

反病毒软件用于识别系统上潜在的病毒感染的过程。

signature dynamics：签字力度

在作为生物测定学方法使用时，为了建立身份标识或提供身份认证而利用的人签名时的模式和速度。

Simple Integrity Axiom：简单完整性规则(SI Axiom)

Biba 模型的一种规则，规定在特定分类标准上的主体不能读取较低分类标准的数据。这通常会被缩略为“不能向下读”。

Simple Key Management for IP：1P 简单密钥管理(SKIP)

用于保护无会话数据报协议的加密工具。

Simple Mail Transfer Protocol：简单邮件传输协议(SMTP)

用于从客户端向服务器和服务器到服务器移动电子邮件的主要协议。

Simple Security Property：简单安全特性(SS 属性)

Bell-LaPadula 模型的一个属性，指出在明确分类级别上的主体不能读取较高敏感性级别的信息。通常被缩写成“不能向上读”。

simulation tests：模拟测试

这种测试为灾难恢复团队的成员呈现一个情景并要求他们提出适当的响应。其中一些响应措施随后会被测试。这可能涉及不重要的业务活动的中断和某些操作人员的使用。

Single Loss Expectancy：单一损失期望(SLE)

与针对特定资产的单个已发生的风险有关的成本，表示组织发生的某种资产被特定威胁损坏所造成的精确损失值。SLE =资产价值(美元)×暴露因子(EF)。

single point of failure：单点故障

基础架构的任何元素(例如设备、服务、协议或通信链路)，如果受到破坏、侵犯或毁坏，将导致完全或重大的停机时间，从而影响组织成员执行基本工作任务的能力。

Single Sign-On：单点登录(SSO)

准许主体在系统上只进行一次身份认证的机制。利用 SSO，一旦主体通过身份认证，那么他们可能在网络中自由漫游，并且不必再次接受身份认证挑战就可以访问资源和服务。

single state：单一状态

要求使用策略机制来管理不同安全级别信息的系统。在这种类型的方案中，安全系统管理员准许处理器和系统一次只处理一个安全级别的问题。

single-use passwords：专用密码

一种动态密码，每次使用时它们都会发生改变。

site survey：现场勘测

使用 RF 信号检测器对无线信号的强度、质量和干扰的正式评估。

Skipjack

与托管加密标准联合，对 64 位的文本分组进行操作的算法。它使用一个 80 位的密钥，并且支持相同的 4 种 DES 操作模式。Skipjack 由美国政府提议，但从未付诸实践。它提供了支持 Clipperr 和 Capstone 高速加密芯片的密码学程序，这些芯片是为重要商业应用而设计的。

sliding windows：滑动窗口

TCP 基于链路可靠性动态地改变传输窗口大小的能力。

smart card：智能卡

信用卡大小的身份证、员工证或安全通行证，上面有磁条、条形码或植入的集成电路芯片。智能卡上包含了可以用于身份标识和/或身份认证目的的经过授权的持卡人信息。

smurf 攻击

一种 DoS 攻击。放大服务器或网络，用无用数据使受害者遭到泛洪攻击。

sniffer attack：嗅探攻击

任何导致恶意用户获得网络信息或通过网络传输的通信信息的操作。嗅探探测器常常是一个包截获程序，它可以将网络介质上传输的数据包的内容复制到文件中，也称为探听攻击。

sniffing：嗅探

网络数据监控的一种形式。嗅探通常包括网络通信数据的捕捉或复制，用于检查、重建和提取。

sniping：秒杀

使用自动化代理提交在线拍卖的最后一次出价。

social engineering：社会工程学

陌生人使用此技巧获取公司内部人员的信任，并怂恿他们对 IT 系统进行修改，从而获得访问权限。

software analysis：软件分析

对正在运行的应用程序中发生的程序或活动进行取证审查。

Software as a Service：软件即服务(SaaS)

一种云计算概念，提供对特定软件应用程序或套件的按需在线访问，而不用本地安装。

Software-Defined Networks：软件定义网络(SDN)

独特的网络操作、设计和管理方法。该概念基于这样一个理论，即传统网络设备配置的复杂性(如路由器和交换机)经常强迫组织依附于一个单一的设备厂商，如思科，这限制了网络的灵活性而难以应付不断变化的物理和商业条件。SDN 旨在从控制层(即网络服务的数据传输管理)分离基础设施层(即硬件和基于硬件的设置)。

software escrow arrangement：软件托管协议

一种特殊的工具，可以对公司起到保护作用：避免公司受软件开发商的代码故障的影响，以便为产品提供足够的支持，还可以防止出现由于开发商破产而造成产品失去技术支持的情况。

software IP encryption：软件 IP 加密(swiPe)

这是一种第 3 层 IP 安全协议。它通过使用封装协议来提供身份认证、完整性和机密性。

spam：垃圾邮件

指那些多余的电子邮件、新闻组或论坛的消息。垃圾邮件可能像善意的厂商发来的广告一样无害，也可能像大量传递的带有病毒或特洛伊木马附件这样的消息一样有害。

spamming attacks 或 spamming：垃圾邮件攻击或垃圾邮件

向系统发送大量垃圾邮件，以引起 DoS 或大众的愤怒，消耗存储空间或消耗带宽和处理能力。

spear phishing：鱼叉式钓鱼

一种针对特定用户组的钓鱼方式。

spike：脉冲

瞬时高电压。

split knowledge：分割知识

在单个解决方案中责任分离和两人控制概念的特定应用。分割知识的基本思想是执行某个操作所需的知识或特权在多个用户之间分配，这样可以确保任何一个人都没有足够的权限来危害环境的安全性。

spoofing：欺骗

利用假的 IP 地址和节点号替代有效的源和/或目标 IP 地址和节点号的行为。

spoofing attack：欺骗攻击

涉及被欺骗的或被修改的数据包的攻击。

spread spectrum：扩频

通信可以通过多个频率同时发生的一种方式和方法。

spyware：间谍软件

软件会监控你的动作，并且向暗中监视你活动的远程系统传送重要的细节。有时用于恶意和非法目的，例如身份盗用或账户接管。

SQL 注入

针对有漏洞的 Web 应用程序的攻击，其中黑客提交 SQL 数据库表达式和脚本代码，绕过身份认证并与 DBMS 或底层操作系统直接交互。

stand-alone mode：独立模式

一个无线网络使用一个无线接入点连接无线客户端但是没有提供任何有线资源。

standards：标准

定义了强制性的硬件、软件、技术和安全控制方法统一使用的要求的文档。它们提供了行为的过程，在这个过程中技术和措施在整个组织内部被统一实施。标准是战术文档，定义了达到目标和安全策略中制定的总体方向的步骤或方法。

state：状态

系统在某个特定情况下的即时快照。

state machine model：状态机模型

一个无论执行何种功能总是安全的系统。

stateful inspection firewall：状态检测防火墙

一种防火墙，对网络通信的状态或环境进行评估。通过检查源和目标的地址、应用习惯、起源地和当前数据包与同一会话的前一个数据包的关系，状态检测防火墙能够为授权用户和操作授予广泛的访问权限，并且积极地监视和堵塞未授权的用户和操作。状态检测防火墙被称为第 3 代防火墙。

stateful NAT：状态 NAT

NAT 维护有关客户端和外部系统之间的通信会话信息的能力或手段。NAT 通过维护内部客户端做出请求，客户端的内部 IP 地址和所联系的互联网服务的 IP 地址之间的映射来操作。

static packet-filtering firewall：静态包过滤器防火墙

一种防火墙，通过检查报文头部的数据进行通信数据的过滤。通常，规则关注于源、目标和端口地址。静态数据包过滤防火墙被称为第 1 代防火墙。

static password：静态密码

不随时间而改变的密码，或在一段有效时间内保持不变的密码。

static system 或 static environment：静态系统或静态环境

一组不改变条件、事件和周边的环境。理论上，一旦理解，就知道静态环境不提供新的或令人惊讶的元素。静态的 IT 环境可以是任何一个系统，其用户和管理员的目的是保持其不变。整个目标是防止或最小程度减少，一个用户可能导致减少安全性或操作功能性的实施变更。

static testing：静态测试

在不运行软件的情况下通过分析源代码或编译的应用程序对软件进行评估。

static token：静态标记

以物理的手段提供身份，通常不被用作身份认证因素。示例包括磁条卡、智能卡、软盘、USB RAM 软件狗，甚至是像开锁的钥匙一样的简单物品。

Station Set IDentifier：工作站集标识符(SSID)

为了与主接入点通信，每个无线客户端都必须知道的无线网络名。

statistical attack：统计攻击

这种攻击类型利用密码系统的统计缺陷，例如浮点错误或不能产生随机数。统计攻击试图查找驻留密码学应用程序的硬件或操作系统的脆弱性。

stealth virus：隐形病毒

这种病毒通过对操作系统的实际篡改来欺骗反病毒软件包认为所有事情都工作正常，从而将自己隐藏起来。

steganography：隐写术

使用密码技术在另外一条消息内嵌入秘密消息的方法，通常在图像或 WAV 文件内插入。

stop error：停止错误

操作系统的安全响应。例如在 Windows 中，当某个应用程序执行非法操作(如访问硬件或更改/访问另一个进程的存储空间)时，系统做出的响应。

stopped state：停止状态

进程结束或必须终止时就会进入停止状态。此时，操作系统可以恢复所有内存和被分配的其他资源，从而允许其他进程根据需要重用这些内存和资源。

storage segmentation：存储分割

一种设备管理技术，用来人为地在存储介质上划分为不同的类型或数值的数据。在移动设备上，设备制造商和/或服务提供商可以使用存储分割将设备的操作系统及预装应用程序与用户安装程序和用户数据进行隔离。一些移动设备管理系统进一步实施隔离，将公司数据和应用程序与用户数据和应用程序分离。

store-and-forward device：存储转发设备

一种网络设备，使用内存缓冲区来存储数据包，直到它们可以转发到较慢的网段。

strategic plan：战略计划

一个长期计划，它是相当稳定的。用于定义组织的目的、任务和目标。如果战略计划每年都被维护和更新，那么可以使用大约 5 年。战略计划还可以作为计划编制的基准。

stream attack：流攻击

一种 DoS 攻击。在大量的数据包使用随机的源和顺序号发往受害者系统的很多端口时，就会出现流攻击。由受害者系统进行的试图解析数据的处理将导致 DoS，也被称为泛洪。

stream ciphers：流密码

对消息(数据流)中的每个字符或每一位进行操作，每次一个字符/位。

streaming audio：流媒体音频

当基于来自提供商/服务器的正在进行的传输而接收到时，被呈现给终端用户的音频传输。流媒体通常通过互联网实时或按需提供。

streaming video：流媒体视频

当基于来自提供商/服务器的正在进行的传输而接收到时，被呈现给终端用户的视频传输。流媒体通常通过互联网实时或按需提供。

strong password：强密码

对付字典攻击或穷举攻击的密码。

SQL

关系数据库使用的标准语言，用于在关系数据库中输入信息或者从中提取存储的信息。

structured walkthrough：结构化演练

一种灾难恢复测试模式，经常被称为“桌面练习”，灾难恢复团队的成员聚集在一间大的会议室里，不同的人在灾难发生时扮演不同角色。

subject：主体

活动的实体，通过访问操作寻找有关被动实体的信息，或者从被动实体中寻找数据。主体可以是用户、程序、进程、文件、计算机或数据库等。

subpoena：传票

法院的指令，强迫个人或组织交出证据或出庭。

substitution cipher：替代密码

使用加密算法、利用不同的字符代替明文信息中的每一个字符或位，如凯撒密码。

supervisor state 或 supervisory state：管理状态或监管状态

进程在享有特权的全访问模式中运行的状态。

Supervisory Control And Data Acquisition：监控与数据采集系统(SCADA)

一个 ICS 单元可以作为一个独立的设备使用，也可与其他 SCADA 系统组成网络或是与传统 IT 系统组成网络。大多数 SCADA 系统以最小的人机接口设计。通常，它们使用机械按钮和旋钮或者简单的液晶屏接口(类似于你在一台商业打印机或 GPS 导航装置上看到的)。然而，网络 SCADA 设备可能有更复杂的远程控制软件接口。

supervisory mode：监管模式

此模式中的进程在层 0 上运行，层 0 是操作系统本身所在的环。

surge：电涌

长时间的高电压。

Sutherland 模型

一个完整性模型，重点是防止干扰的完整性的支持。

switch：交换机

由于交换机知道连接到每个出站端口的系统的地址，因此这种网络设备常常被称为智能集线器。与在所有出站端口上中继通信数据不同，交换机只在已知目标地址所在的出站端口上对通信数据进行中继。交换机提供了更加有效的通信分发方式，建立了隔离的广播和冲突域，并且提高了数据的整体吞吐量。

Switched Multimegabit Data Service：交换式多媒体数据服务(SMDS)

一种无连接的网络通信服务。SMDS 提供按需带宽服务，并且对于那些通信不频繁的远程 LAN 链接是一种首选的连接机制。

Switched Virtual Circuit：交换式虚电路(SVC)

一种虚电路形式，更像一个拨号连接，每次使用时必须重新建立。

symmetric key：对称密钥

依靠一个“共享的秘密”加密密钥的算法，这个密钥被分发给所有公共通信的成员。这个密钥由所有成员用于消息的加密和解密。

Symmetric MultiProcessing：对称多重处理(SMP)

一种系统类型，处理器不但共享一个公共操作系统，而且还共享公共数据总线和存储器资源。在这种结构类型中，系统可以使用不超过 16 个处理器。

SYN 泛洪攻击

一种 DoS 攻击。SYN 泛洪通过不发送最终的 ACK 包发动攻击，从而破坏 TCP/IP 初始化通信会话的三步握手标准。

Synchronous Data Link Control：同步数据链路控制(SDLC)

一种第 2 层上的协议，运用在使用专线或租用线的网络中。SDLC 由 IBM 公司为 SNA 系统的远程通信而开发。SDLC 是面向比特的同步协议。

synchronous dynamic password token：同步动态密码标记

以固定时向间隔生成密码的标记设备使用的所有标记。时间间隔标记需要验证服务器上的时钟和标记设备上的时钟是同步的。生成的密码由主体随同 PIN、密码短语或密码输入到系统中。

synthetic transactions：综合事务

具有已知预期结果的脚本事务。测试人员针对测试的代码运行综合事务，然后将事务的输出与预期状态进行比较。实际和预期结果之间的任何偏差代表代码中可能的缺陷，必须进一步调查。

system call：系统调用

可信度较低的保护环中某个对象请求访问可信度较高的保护环中的资源或对象功能的过程。

system compromise：系统破坏

系统的安全性被损坏的情况，也称为安全损坏、安全破坏、入侵或违规。

system-high security mode：系统高级安全模式

一种模式，系统被授权只处理所有系统用户批准读取(并且具有有效的“知其所需”权限)的信息。如果系统在这种模式中运行，就不能相信它们维护了安全级别的分离。并且这些系统处理的所有信息必须进行控制，就好像它们被分类成与系统处理的最高分类信息处于同一个级别。

system resilience：系统弹性

系统在发生不利事件时保持可接受服务水平的能力。这可能是容错组件管理的硬件错误，也可能是其他控制管理的攻击，如有效的入侵检测和预防系统。

T

table：表

关系数据库的主要构件，也称为关系。

tactical plan：战术计划

战术计划是中期计划，用于提供更加详细的完成战略计划中提出的目标的计划。战术计划通常一年有效，对实现组织目标所必需的任务进行规定和制定进度表。

Take-Grant 模型

一种模型，采用有向图来指示权限如何从一个主体向另一个主体进行传递，或者如何从一个主

体向一个客体传递。简单地讲，具有授权资格的主体可以向另一个主体或客体授予其拥有的其他任何权限。同样，具有获得权限的主体可以从另一个主体获得权限。

task-based：基于任务

一种访问控制方法，这个方法根据工作任务或操作来进行访问控制。

TCP 模型

从 TCP/IP 衍生出来的网络协议概念模型，也称为 DARPA 模型和 DoD 模型。TCP 模型有 4 层，而不是 OSI 模型的 5 层。这 4 层从下到上是网络接入层、网际层、主机到主机层和应用层。

TCP 包装

通过在用户 ID 或系统 ID 的基础上对访问进行限制，可以作为基本防火墙使用的一种应用程序。

teardrop attack：泪滴攻击

一种 DoS 攻击。在攻击者对操作系统中的一个缺陷加以利用时，就会出现泪滴攻击。这种缺陷存在于对碎片数据包进行重新组织(即重新排序)的常规程序中。攻击者向受害者发送很多特别格式的碎片数据包，这会引起系统冻结或崩溃。

technical access control：技术性访问控制

作为硬件或软件机制，可以用于管理对资源和系统的访问，并且提供对这些资源和系统的保护。例如，逻辑性或技术性访问控制包括加密、智能卡、密码、生物测定学、受限接口、访问控制列表、协议、防火墙、路由器、入侵检测系统和阈值级别。与逻辑性访问控制相同。

technical physical security controls：技术上的物理安全控制

依靠技术实施一些物理安全类型的安全控制，包括入侵检测系统、警报、CCTV、监视、HVAC、电源、火灾检查和排除。

telephony：语音通信

用于向组织提供电话服务的方法或者组织使用电话服务用于语音和/或数据通信的机制的总称。传统上，语音通信结合调制解调器，包括 POTS 与 PSTN 的服务。但是，这也被扩展到了 PBX、VoIP 和 VPN。

TEMPEST

各种不同类型的电子硬件，如计算机、电视和电话等产生的电子信号的研究和控制。它的主要目标是阻止电磁干扰和无线电频率的辐射离开被严格规定的区域，从而消除外部辐射监控、窃听和信号嗅探的可能性。

Terminal Access Controller Access Control System：终端访问控制器访问控制系统(TACACS)

RADIUS 的替换协议。TACACS 有三种可用的版本：TACACS 最初版、XTACACS (扩展的 TACACS)和 TACACS+。TACACS 集成了身份认证和授权过程。XTACACS 保持了身份认证、授权

和记账过程的分离。TACACS+通过增加双因素身份认证增强了 XTACACS。

terrorist attacks：恐怖攻击

这种攻击有别于军事和情报攻击，恐怖攻击的目标在于中断正常的生活，而军事和情报攻击被用来获取机密信息。

test data method：测试数据方法

这种程序测试形式通过检查系统测试的范围，从而定位未测试的程序逻辑。

testimonial evidence：言词证据

由证人证词组成的证据，证词既可以是法庭上的口头证词，也可以是记录存储的书面证词。

thin client：瘦客户端

这个术语被用于描述不具有或几乎不具有本地处理或存储能力的工作站。瘦客户端被用于连接和操作远程系统。

third-party governance：第三方治理

可能由法律、法规、行业标准、合同义务或许可要求规定的监督制度。

threat：威胁

对企业或具体的资产可能会造成不良或有害结果的事件。

threat agents：威胁主体

企图利用安全脆弱性的人、程序、硬件或系统。

threat events：威胁事件

对脆弱性的意外利用。

threat modeling：威胁建模

潜在威胁被识别、理解和分类的安全流程。试图确定对有价值资产的潜在威胁列表，并且对威胁的分析。

thrill attacks：兴奋攻击

是由具有很少技能的破坏者发起的攻击。兴奋攻击的动机是闯入系统的极度兴奋。

throughput rate：吞吐速率

生物测定学设备对主体进行扫描和身份认证的速度。一般具体的生物测定学控制可接受的速度大约是 6 秒或更快。

ticket：票据

由 Kerberos 身份认证系统使用的一种电子身份认证因素。

Ticket-Granting Service：票据授予服务(TGS)

Kerberos 身份认证系统的一部分。TGS 管理票据的分配和过期时间。票据被主体用于获得对客体的访问。

Time Of Check：检查时间(TOC)

主体检查客体状态的时间。

Time Of Check To Time Of Use：检查时间到使用时间(TOCTTOU 或 TOC/TOU)

一个时间型的脆弱性，当程序检查访问许可权限的时间超过资源请求时间过长的时候，就会发生这种问题。

Time Of Use：使用时间(TOU)

为访问客休，主体做出决定的时间。

time slice：时间片

处理时间的一部分或划分。

token device：令牌设备

主体必须携带的一种密码生成设备。令牌设备是类型 2 身份认证因素“你拥有什么”的一种形式。

token ring：令牌环

一种传递令牌的 LAN 技术。

top secret：绝密

最高级别的政府/军方分类。未经授权而泄露绝密数据将会有灾难性的后果，并会导致对国家安全的毁灭性破坏。

topology：拓扑

网络设备和连接电缆连接的物理布局。常见的网络拓扑包括环形、总线、星型和网状。

total risk：风险总计

是指在没有保护措施可以实施的情况下，组织将要面对的风险的总数。威胁*弱点*资产价值=风险总计。

trade secret：商业秘密

对于业务绝对关键的知识产权，如果泄露给竞争对手和/或公开，那么就会导致相当大的损害。

trademark：商标

经过注册的单词、口号和标志语，被用于识别一家公司及其产品或服务。

traffic analysis：流量分析

一种监控形式，对数据包的流而不是数据包的实际内容进行检查，也被称为趋势分析。

training：培训

教导员工完成工作任务和遵守安全策略的任务。所有的新员工都需要进行一定级别的培训，这样他们就能够合理遵守安全策略中规定的所有标准、指导原则和措施。

transferring risk：转移风险

把已实现的风险带来的损失转给另一个实体或组织，如购买保险，也被称为转让风险。

transparency：透明度

服务、安全控制或访问机制的特性，确保用户看不到。透明度通常是安全控制的理想状态。安全机制越透明，用户越不可能避开它，甚至是意识到它的存在。

transient：瞬时现象

短时间线路噪声干扰。

transitive trust：传递信任

如果 A 信任 B，并且 B 信任 C，那么 A 通过传递属性继承 C 的信任，这样的工作方式类似于数学方程式：如果 A = B，B = C，则 A = C。传递信任是一个严重的安全问题，因为它可以允许绕过 A 和 C 之间的限制或制约，特别是在 A 和 C 都支持与 B 的交互的情况下。

Transmission Control Protocol：传输控制协议(TCP)

OSI 模型第 4 层上的一种面向连接的协议。

transmission error correction：传输错误纠正

内置在面向连接或面向会话的协议和服务中的一种能力。如果报文的全部或部分被破坏、修改和丢失，那么可能会生成要求源端对报文的部分或全部内部进行重传的要求。

transmission logging：传输日志记录

集中于通信方面的一种审计形式。传输日志记录对有关源、目标、时间标记、身份标识代码、传输状态、数据包数量和报文大小等的详细信息进行记录。

transmission window：传输窗口

发送确认数据包之前传输的数据包数。

Transport Layer：传输层

OSI 模型的第 4 层。

Transport Layer Security：传输层安全(TLS)

基于 SSL 技术，TLS 包含了许多安全增强功能并最终被大多数应用所采用并替代 SSL。早期版本的 TLS 在通信双方都不支持 TLS 的时候可以降级支持 SSL 3.0。然而，在 2011 年 TLS 1.2 去掉了这个向后兼容性。与 SSL 一样，TLS 使用 TCP 端口 443。

transport mode：传输模式

在 VPN 中使用的一种 IPSec 模式。在传输模式中，对 IP 数据包中的数据进行了加密，但是数据包头没有加密。

transposition cipher：换位密码

使用一个加密算法重新排列明文消息中的字母，形成密文消息。

trap door：陷门

没有被记录到文档中的命令序列，它允许软件开发者绕过正常的访问限制。

traverse mode noise：横向模式噪声

由电源或运转的电子设备的火线和中线之间的电势差产生的 EMI 噪音。

Triple DES：三重 DES(3DES)

使用 3 个重复 DES 的标准，利用 2 个或 3 个不同的密钥将密钥的有效强度增加至 112 位。

trojan horse：特洛伊木马

一种恶意代码对象，看起来是个善意的程序(如游戏或简单的实用程序)。它公开执行“覆盖”功能，而且还带有未知的有效载荷，如病毒。

trust：信任

一种在两个域之间建立的安全桥梁，目的是使一个域共享另一个域的资源。在两个域之间建立信任，以便准许用户从一个域中访问另一个域中的资源。信任可以单向的，也可以是双向的。

Trusted Computing Base：可信计算基(TCB)

硬件、软件和控制的组合，形成信任基础，以加强安全策略。

trusted path：可信路径

由 TCB 用来与系统的其他部分通信的安全通道。

Trusted Platform Module：可信平台模块(TPM)

在主板上加密处理器芯片，用于存储和处理加密密钥，以满足基于硬件支持/实现的硬盘加密系统需求。

trusted recovery process：可信任恢复过程

在受保护的系统上，确保系统在出现错误、故障或重新启动后始终返回到安全状态的过程。

trusted system：可信任系统

一种安全的计算机系统。

tunnel mode：隧道模式

VPN 中使用的一种 IPSec 模式。在隧道模式中，整个 IP 数据包被加密，并且为了控制隧道内的传输向 IP 数据包添加了新的数据包头。

tunneling：隧道

通过将协议数据包的内容封装到其他协议的数据包来实现保护的一种网络通信规程。

tuple：元组

数据库中的一条记录或行。

turnstile：转门

一种门，它每次只可以进一个人，并且常常限制在单方向转动。

two-factor authentication：双因素身份认证

需要两个因素的身份认证。

Type 1 authentication factor：类型 1 身份认证因素

指“你知道什么”，如密码、个人身份证号(PIN)、组合锁、密码短语、母亲的娘家姓和喜欢的颜色等。

Type 2 authentication factor：类型 2 身份认证因素

指“你拥有什么”，如智能卡、ATM 卡、令牌设备和内存卡等。

Type 3 authentication factor：类型 3 身份认证因素

指“你是什么”，如指纹、语音记录、视网膜样本、虹膜样本、脸部形状、掌纹和手型等。

U

unauthenticated scan：未经验证的扫描

一种漏洞扫描形式，可测试目标系统，而不必具有授予扫描程序特殊权限的密码或其他特殊信息。这允许扫描从攻击者的角度运行，但也限制了扫描程序完全评估可能漏洞的能力。

unclassified：未分类

最低级别的政府/军方分类。用于既不敏感也不用保密的数据。未分类数据的泄露既不会危及机密性，也不会造成任何明显的损坏。

underflow：下溢出

当驱动器的写缓冲区在写入过程中空闲时会发生此错误，这会导致介质上的错误，从而使其无用。

unicast：单播

向单一标识的接收者进行的通信传输。

Unified Threat Management：统一威胁管理(UTM)

一种安全装置，包括传统的功能，如数据包过滤和状态检测。它能够执行数据包检测技术，使其能够识别和阻止恶意流量。它可以过滤使用定义文件和/或白名单和黑名单的恶意软件。它还包括入侵检测和/或入侵防御能力，也称为下一代防火墙。

Uniform Computer Information Transactions Act：统一计算机信息处理法案(UCITA)

被所有 50 个州采纳的美国联邦法律，它提供了计算机相关业务处理行为的共同架构。

Uninterruptible Power Supply：不间断电源(UPS)

一种自充电的电池类型，可以为敏感的设备提供连续和平稳的电力。UPS 基本的工作方式是：从壁装电源插座上取得电力并存储在电池中，将电力从电池中输出，然后把这些电力供给与它相连的任何设备。通过使用电池中的电流，UPS 能够维持连续和平稳的电力供应。

unit testing：单元测试

一种测试软件的方法。每个单元的代码被独立测试，以便发现错误和疏漏，保证功能完善。单元测试应该由开发人员实施。

Unshielded Twisted-Pair：非屏蔽双绞线(UTP)

一种双绞线类型，不包括额外的 EMI 保护。大多数双绞线都是 UTP。

USA Patriot Act of 2001：2001 年的美国爱国者法案

9 • 11 恐怖袭击后在美国实施的一项法案。美国爱国者法案大大扩大了执法机构和情报机构跨多个领域的力量，包括对电子通信的监视。

user：用户

任何具有安全系统访问权限的人。用户的访问权限与他们的工作任务联系在一起，并且受到限制，所以他们只具有工作职务所要求的能保证完成任务所需的有限权限(也就是最小特权原则)，也被称为终端用户和员工。

User Datagram Protocol：用户数据报协议(UDP)

OSI 模型第 4 层上一种无连接的协议。

user mode：用户模式

在执行用户应用时由 CPU 使用的基本模式。

V

VENONA

美国谍报工作的一个主要成功之处是：由于密码分析人员破解了依赖使用一次性填充的绝密的 Soviet 密码系统，例如 VENONA。

Vernam 密码

这种设备实现以 26 为模的 26 字母替代密码。它的功能与一次性填充相同。

view：视图

用于与数据库交互的客户界面。视图限制了能够看到数据库的客户及其能够执行的功能。

Vigenere 密码

一种多字母替代密码。

violation analysis：违规分析

使用阈值级别的审计形式。

virtual machine：虚拟机

虚拟机是计算机的软件模拟环境，进程可以在这个环境内执行。每个虚拟机都具有自己的内存地址空间，并且虚拟机之间的通信受到安全控制。

virtual memory：虚拟存储器

一种特殊类型的辅助存储器，它由操作系统负责管理，就像是实际存储器一样。

Virtual Private Network：虚拟专用网(VPN)

在已有的专有或公共网络上，两个系统间建立的网络连接。VPN 通过加密为网络通信提供机密

性和完整性服务。

VPN protocol：虚拟专用网协议

用于创建 VPN 的协议，如 PPTP、L2TP 和 IPSec。

virtualization：虚拟化

虚拟化技术是用来在单一的主机内存中运行一个或多个操作系统。这种机制允许在任意硬件上虚拟运行任何操作系统，也允许多个操作系统同时工作在相同的硬件上。

virus：病毒

病毒是折磨电脑空间的恶意代码客体的最古老形式。一旦它们进入了系统，就会将自己附加到合法的操作系统、用户文件以及应用程序上，并且正常地执行一些类型的不良操作，从在显示屏上显示一些无伤大雅的讨厌信息直至恶意破坏整个本地文件系统。

virus decryption routine：病毒解密程序

加密病毒使用一个很短的、被称为病毒解密程序的代码段，这个代码段包含必要的密码学信息，用于对存储在磁盘上其他地方的主病毒代码进行加载和解密。

vishing：语音钓鱼

使用 IP 语音(VoIP)欺骗用户的网络钓鱼形式。它会经常通过欺骗呼叫者 ID 来欺骗系统主叫的实际电话号码。

VLAN

在交换机和网桥上实现逻辑网络分段，用于管理流量。多个 VLAN 可以放在同一交换机上，但是它们被隔离，就像它们在单独的物理网络上一样。只有通过由提供路由功能的多层交换机，才能进行跨 VLAN 通信。VLAN 的作用类似于物理网段。

VLAN 跳跃

通过滥用 IEEE 802.1Q VLAN 标签(被称为双重封装)使网络流量在 VLAN 之间跳跃的能力。

VoIP

通过在 IP 网络上像网络数据包一样传递语音，从而提供语音通信服务的网络服务。

voice pattern：语音模式

生物测定学因素的一个例子，它是主体独有的行为或生理上的特征。语音、语调、声调和个人声音的音调都被用来建立身份标识或提供身份认证。

volatile storage：易失性存储设备

一种在资源断电时会丢失其上存储内容的存储介质，如 RAM。

voluntary surrender：自愿交出证据

愿意交出证据的举动。

vulnerability：脆弱性

防护措施或应对措施的缺乏或薄弱被称为脆弱性。换句话说，脆弱性就 IT 基础设施或组织其他方面的缺陷、漏洞、疏忽、错误、局限性、过失或容易受到攻击。

vulnerability analysis：脆弱性分析

用于识别漏洞或弱点的过程，可以包括技术手段，例如漏洞扫描，以及非技术手段，例如评估或检查现有威胁和漏洞的数据。

vulnerability management：漏洞管理

一个程序，能够帮助组织检测漏洞。漏洞管理程序的两个常见要素是漏洞扫描和脆弱性评估。漏洞扫描是定期执行的技术扫描，以及漏洞评估通常与风险评估相结合。

vulnerability scan：漏洞扫描

在系统上执行测试，以发现安全基础设施中的弱点。漏洞扫描会自动地探测系统、应用程序和网络，寻找可能被攻击者利用的漏洞。这些测试中使用的扫描工具提供了快速的指向和点击测试，执行其他烦琐的任务，而不需要手动干预。

vulnerability scanner：脆弱性扫描仪

一种用于测试系统中已知的安全脆弱性和缺陷的工具。脆弱性扫描仪可以生成报告，报告中指出系统中需要加以管理以提高安全性的区域或方面。

W

wait state：等待状态

进程准备执行但是必须等待某种操作(如键盘输入、打印或文件写入)结束的状态。

war dialing：战争拨号

这种行为使用调制解调器搜索允许入站连接尝试的系统。

war driving：战争驾驶

使用无线电信号检测器或无线网络检测器来定位无线网络的行为。

warm site：基本完备场所

介于完备场所和基础场所之间的灾难恢复专家可以选择的中间场所。这种场所总是包含快速建立运营体系所需的设备和数据线路，但是通常不包含用户数据的备份。

warning banners：警告标题

用于通知可能存在入侵者或者企图违反安全策略的人，这些人的故意行为要受到限制，并且任何进一步的活动也都要受到审计和监控。警告标题基本上是禁止非法入侵标志的电子同义词。

watermarking：水印

数字水印的过程将只有文件创建者知道的信息隐藏到文件中。如果有人之后创建了内容的未授权副本，可以使用水印来检测副本，并且(如果向每个原始接收者提供唯一加水印的文件)这将追溯违规副本的源头。

web application firewall：web 应用防火墙

专门配置的应用层防火墙，用于防止基于 Web 的攻击和利用。

web bot：web 机器人

一种代理，持续抓取各种用户检索网站和处理数据的行为。

Webcasting：网播

其递送方式有时与广播之类的传统通信业务非常相似。也可以包括视频广播、音频广播、播客、网络广播、互联网电视和 IP 电视。

well-known ports：知名端口

TCP 和 UDP 的前 1024 个端口，它们常被分配给经常使用的服务和应用。

wet pipe system：湿管道系统

总是充满了水的防火系统。当灭火装置被烟或火触发的时候，立刻放水，也被称为封闭头系统。

whaling：捕鲸

捕鲸是钓鱼的一种形式，它的目标是高层或高管人员，比如公司的 CEO 和总裁。

white box testing：白盒测试

一种程序测试形式，用于检测程序的内部逻辑结构。

white box：白盒

用于控制电话系统。白盒是一种双音多频(DTMF)生成器(就是键盘)。

Wide Area Network：广域网(WAN)

地理分隔的一种网络或一种 LAN。通常租用线路被用于在两个远程的组件之间建立连接。

Wi-Fi Protected Access：Wi-Fi 安全访问(WPA)

WEP 的早期替代方案，基于秘密的密码短语，使用 LEAP 和 TKIP 密码系统。通过密码短语猜

想能够对其进行攻击。

WiMax 802.16

定义全球性无线接入技术的一种无线标准。这个标准目前仍然被广泛部署。

Wired Equivalent Privacy：有线等价隐私(WEP)

利用 RC4 的一种加密身份认证。WEP 只支持从客户端到 WAP 的单向身份认证。因为其设计和实现存在若干缺陷，所以 WEP 被视为不够安全。

wired extension mode：有线扩展模式

无线接入点连接无线客户端到一个有线网络的一种无线网络配置。

Wireless Application Protocol：无线应用协议(WAP)

一个有效的行业驱动的协议堆栈，借助于具备 WAP 能力的设备(如移动电话)，通过运营商的网络与互联网进行通信。

wireless networking(802.11)：无线网络连接(802.11)

根据 802.11 标准将无线电波用作连接介质的网络连接形式，常常被称为 WiFi。

wiring closet：配线间

是整个建筑或一个楼层中连接到其他重要设备的网络电缆所在的地方，如配线架、交换机、路由器、局域网扩展、骨干渠道。配线间的一个更专业的技术名称是房屋线缆分布室。

work function 或 work factor：工作函数或工作因数

通过从成本和/或时间方面来度量付出的努力，来度量密码学系统的强度。通常，针对加密系统执行完全穷举攻击所需的时间和努力就是工作函数所表示的内容。密码系统提供的安全性和保护与工作函数/因数的值成正比。

Worm：蠕虫

蠕虫是恶意代码的一种形式，它会自己进行复制，但是并没有对主机系统进行直接的威胁。蠕虫主要的目的是将自己复制到其他的系统，并且收集信息。蠕虫通常会大量繁殖，并且由于自身复制的企图耗尽了系统的资源和网络带宽，常常会导致拒绝服务。

X

X.25

一种广域网协议，使用电信交换机在共享的网络介质上提供端到端的连接。

XOR

当只有一个输入值为真时，函数值为真。如果两个输入值都为假或都为真，XOR 函数的结果为假。

Z

zero day exploit：零日利用

利用他人未知的系统漏洞对系统发起攻击。通常，它表示供应商不知道一个或多个攻击者已知的漏洞。在某些情况下，供应商可能了解该漏洞，但尚未编写或发布该漏洞的补丁。

zero knowledge proof：零知识证明

交换特定类型信息但是不交换实际数据的一个通信概念。这个思想的重要示例为数字签名和数字证书。

zero-knowledge teams：零知识水平团队

在安全评估或渗透测试期间，这支团队只了解组织的基本信息。

zzuf

一种软件工具，通过根据用户规范操纵输入来将变异模糊测试的过程自动化。