

前言

本书可为你参加 CISSP(注册信息系统安全师)认证考试打下坚实基础。买下这本书，就表明你想学习并通过这一认证提高自己的专业技能。这里将对本书和CISSP 考试做基本介绍。

本书为想以努力学习方式通过 CISSP 认证考试的读者和学生而设计。如果你的目标是成为一名持证安全专业人员，则 CISSP 认证和本学习指南是你的最佳选择。本书的目的就是帮助你为参加 CISSP 考试做好准备。

在深入阅读本书前，你首先要完成几项任务。你需要对 IT 和安全有一个大致了解。你应该在 CISSP 考试涵盖的 8 个知识域中的两个或多个拥有 5 年全职全薪工作经验(如果你有本科学历，则有 4 年工作经验即可)。如果根据(ISC)² 规定的条件你具备了参加 CISSP 考试的资格，则意味着你做好了充分准备可借助本书备考 CISSP。有关(ISC)² 的详细信息，稍后介绍。

如果你拥有(ISC)² 先决条件路径认可的其他认证，(ISC)² 也允许把 5 年工作经验的要求减掉一年。这些认证包括 CAP、CISM、CISA、CCNA Security、Security+、MCSA、MCSE 等，以及多种 GIAC 认证。有关资格认证的完整列表，可访问 <https://www.isc2.org/certifications/CISSP/Prerequisite-pathway> 查询。需要指出的是，你只能用一种方法减少工作经验年限，要么是本科学历，要么是认证证书，不能两者都用。

(ISC)²

CISSP 考试由国际信息系统安全认证联盟(International Information Systems Security Certification Consortium)管理，该联盟的英文简称是(ISC)²。(ISC)² 是一个全球性非营利组织，致力于实现 4 大任务目标：

- 为信息系统安全领域维护通用知识体系(CBK)。
- 为信息系统安全专业人员和从业者提供认证。
- 开展认证培训并管理认证考试。
- 通过继续教育，监察合格认证申请人的持续评审工作。

(ISC)² 由董事会管理，董事从持证从业人员中按级别选出。

(ISC)² 支持和提供多项专业认证，其中包括 CISSP、SSCP、CAP、CSSLP、CCFP、HCISPP 和 CCSP。这些认证旨在验证所有行业 IT 安全专业人员的知识和技术水平。有关(ISC)² 及其证书认证的详情，可访问(ISC)² 网站 www.isc2.org 查询。

CISSP 证书专为在组织内负责设计和维护安全基础设施的安全专业人员而设。

知识域

CISSP 认证涵盖 8 个知识域的内容，分别是：

- 安全与风险管理
- 资产安全
- 安全架构和工程
- 通信与网络安全
- 身份和访问管理
- 安全评估与测试
- 安全运营
- 软件开发安全

这 8 个知识域以独立于厂商的视角展现了一个通用安全框架。这个框架是支持在全球所有类型的组织中讨论安全实践的基础。

最新修订的主题域在 2018 年 4 月 15 日开始的考试中体现出来。若需要根据 8 个知识域的划分全面了解 CISSP 考试涵盖的主题范围，请访问^{(ISC)²}网站 www.isc2.org，索取“申请人信息公告”(Candidate Information Bulletin)。这份文件包含完整的考试大纲以及有关认证的其他相关信息。

资格预审

^{(ISC)²}

规定了成为一名 CISSP 必须满足的资格要求。首先，你必须是一名有 5 年以上全职全薪工作经验或者有 4 年工作经验并具有 IT 或 IS 本科学历的安全专业从业人员。专业工作经验的定义是：在 8 个 CBK 域的两个或多个域内有工资或佣金收入的安全工作。

其次，你必须同意遵守道德规范。CISSP 道德规范是^{(ISC)²}希望所有 CISSP 申请人都严格遵守的一套行为准则，目的是在信息系统安全领域保持专业素养。你可在^{(ISC)²}网站 www.isc2.org 的信息栏下查询有关内容。

^{(ISC)²}

还提供一个名为“(ISC)²准会员”的入门方案。这个方案允许没有任何从业经验或经验不足的申请人参加 CISSP 考试，通过考试后再获得工作经验。准会员资格有 6 年有效期，申请人需要在这 6 年时间里获得 5 年安全工作经验。只有在提交 5 年工作经验证明(通常是有正式签名的文件和一份简历)之后，准会员才能得到 CISSP 证书。

CISSP 考试简介

CISSP 考试堪称从万米高空俯瞰安全，涉及更多的是理论和概念，而非执行方案和规程。它的涵盖面很广，但并不很深。若想通过这个考试，你需要熟知所有的域，但不必对每个域都那么精通。

2017 年 12 月 18 日后，CISSP 英语考试将以自适应形式呈现。^{(ISC)²}给新版考试定名为

CISSP-CAT(计算机化自适应考试)。有关这一新版考试呈现形式的详细信息，可访问<https://www.isc2.org/certifications/CISSP/CISSP-CAT>查询。

CISSP-CAT 考试将最少含 100 道考题，最多含 150 道考题。呈现给你的所有考项不会全部计入你的分数或考试通过状态。^{(ISC)²}把这些不计分考项定名为考前题(pretest question)，而计分考项叫作操作项(operational item)。这些考题在考试中均不标明计入考分还是不计入考分。认证申请人会在考试中遇到 25 个不计分考项——无论他们只做 100 道考题就达到了通过等级还是看全了所有 150 道题。

CISSP-CAT 考试时间最长不超过 3 小时。如果你没等达到某个通过等级就用完了时间，将被自动判定失败。

CISSP-CAT 不允许返回前面的考题修改答案。你离开一道考题后，你选择的答案将是最终结果。

CISSP-CAT 没有公布或设置需要达到的分数。相反，你必须在最后的 75 个操作项(即考题)之内展示自己具有超过^{(ISC)²}通过线(也叫通过标准)的答题能力。

如果计算机判断你达到通过标准的概率低于 5%，而且你已答过 75 个操作项，你的考试将自动以失败告终。一旦计算机评分系统根据必要数量考题以 95% 的信心得出结论，判断你有能力达到或无法达到通过标准，将不保证有更多考题展示给你。

如果你第一次未能顺利通过 CISSP 考试，你可在以下条件下再次参加 CISSP 考试：

- 每 12 个月内你最多可以参加 3 次 CISSP 考试。
 - 从第一次考试到第二次考试之间，你必须等待 30 天。
 - 从第二次考试到第三次考试之间，你必须再等待 90 天。
 - 从第三次考试到下次考试之间，你必须再等待 180 天，或者第一次考试之日起满 12 个月。
- 每次考试都需要支付全额考试费。

从前的纸质或 CBT(基于计算机的考试)平面 250 题版考试已不可能重现。CISSP 现在只使用 CBT CISSP-CAT 格式。

更新后的 CISSP 考试将以英文、法文、德文、巴西葡萄牙文、西班牙文、日文、简体中文和韩文等版本提供。

自 2017 年 12 月 18 日起，CISSP(注册信息系统安全师)考试(仅英语考试)将通过^{(ISC)²}授权的 Pearson VUE 考试中心在所授权地区以 CAT 形式进行。英文以外其他语言 CISSP 考试以及^{(ISC)²}所有其他认证考试将继续以固定的线性考试(linear examination)方式进行。

CISSP 考试的考题类型

CISSP 考试的大多数考题都有 4 个选项，这种题目只有一个正确答案。有些考题很简单，比如要求你选一个定义。有些考题则复杂一些，要求你选出合适的概念或最佳实践规范。有些考题会向你呈现一个场景或一种情况，让你选出最佳答案。下面举一个例子：

1. 以下哪一项是安全解决方案的最重要目标并具有最高优先级？
 - A. 防止泄露
 - B. 保持完整性
 - C. 保持人身安全

D. 保持可用性

你必须选出一个正确或最佳答案并把它标记出来。有时，正确答案一目了然。而在其他时候，几个答案似乎全都正确。遇到这种情况时，你必须为所问的问题选出最佳答案，你应该留意一般性、特定、通用、超集和子集答案选项。还有些时候，几个答案看起来全都不对。遇到这种情况时，你需要把最不正确的那个答案选出来。



注意：

顺便提一句，这道题的答案是 C. 保持人身安全永远是重中之重。

除了标准多选题格式以外，(ISC)²还增加了一种高级考题格式，叫作高级创新题(advanced innovative question)。其中包括拖放题和热点题。这些类型考题要求你按操作顺序、优先级偏好或与所需解决方案的适当位置的关联来排列主题或概念。具体来说，拖放题要求参试者移动标签或图标，以在图像上把考项标记出来。热点题要求考生用十字记号笔在图像上标出一个位置。这些考题涉及的概念很容易处理和理解，但你要注意放置或标记操作的准确性。

有关考试的建议

CISSP 考试由两个关键元素组成。首先，你需要熟知 8 个知识域涉及的内容。其次，你必须掌握高超的考试技巧。你最多只有 3 小时时间，期间可能要回答多达 150 道题。如此算来，每道题的答题时间平均只有 1 分多钟。因此，快速答题至关重要，但也不必太过匆忙，只要不浪费时间就好。

(ISC)²对 CISSP-CAT 格式的描述并未讲明猜答案是不是适合每种情况的好办法，但是这似乎确实是比跳题答问更好的策略。我们建议你在猜一道题的答案之前尽量减少选项的数量；如果实在无法排除任何答案选项，可考虑跳过这道题，而不进行随机猜测。对减少了数量的选项作出有根据的猜测，可以提高答对考题的概率。

我们还要请大家注意，(ISC)²并没有说明，面对由多个部分组成的考题时，如果你只答对了部分内容，是否会得到部分考分。因此，你需要注意带复选框(而不是带单选按钮)的考题，并且确保按需要的数量选择考项，以适当解决问题。

你将被发给一块白板和一支记号笔，用来记下你的思路和想法。但是写在白板上的任何东西都不能改变你的考分。离开考场之前，你必须把这块白板还给考试管理员。

为帮助你在考试中取得最好成绩，这里提出几条一般性指南：

- 先读一遍考题，再把答案选项读一遍，之后再读一遍考题。
- 先排除错误答案，再选择正确答案。
- 注意双重否定。
- 确保自己明白考题在问什么。

掌控好自己的时间。尽管可在考试过程中歇一会儿，但这毕竟会把部分考试时间消耗掉。你可以考虑带些饮品和零食，但食物和饮料不可带进考场，而且休息所用的时间是要计入考试时间的。确保自己只随身携带药物或其他必需的物品，所有电子产品都要留在家里或汽车

里。你应该避免在手腕上戴任何东西，其中包括手表、健身跟踪器和首饰。你不可使用任何形式的防噪耳机或耳塞式耳机，不过你可使用泡沫耳塞。我们还建议你穿着舒适的衣服，并带上一件薄外套（一些考场有点儿凉）。

如果英语不是你的第一语言，你可注册其他语言版本的考试。或者，如果你选择使用英文版考试，你将被允许使用翻译词典（务必事先联系你的考场，以便提前做好安排）。你必须能够证明你确实需要这样一部词典，这通常需要你出示自己的出生证或护照。



注意：

考试或考试目标偶尔会发生一些小变化。每逢这种情况，Sybex 都会在自己网站上贴出更新的内容。参加考试前应访问 www.wiley.com/go/cissp8e，确保自己掌握最新信息。

学习和备考技巧

我们建议你为 CISSP 考试制定一个月左右的晚间强化学习计划。这里提几点建议，可以最大限度增加你的学习时间；你可根据自己的学习习惯做必要修改：

- 用一两个晚上细读本书的每一章并把它的复习材料做一遍。
- 回答所有复习题，并把本书和考试引擎中的练习考试做一遍。完成每章的书面实验，并利用每章的复习题来找到一些主题，投入更多时间对它们进行深入学习，掌握其中的关键概念和战略，或许能令你受益。
- 复习(ISC)² 的考试大纲：www.isc2.org。
- 利用学习工具附带的速记卡来强化自己对概念的理解。



提示：

我们建议你把一半的学习时间用来阅读和复习概念，把另一半时间用来做练习题。有学生报告说，花在练习题上的时间越多，考试主题记得越清楚。除了本学习指南的练习考试外，Sybex 还出版了《(ISC)：CISSP 官方习题集》。这本书为每个域都设置了 100 多道练习题，还含 4 个完整的练习考试。与本学习指南一样，它还有在线版考题。

完成认证流程

你被通知成功通过 CISSP 认证考试后，你离真正获得 CISSP 证书还差最后一步。最后一步是背书(endorsement)。这基本上是让一个本身是 CISSP 或(ISC)² 其他证书持有者、有很高声望并熟悉你的职业履历的人为你提交一份举荐表。通知你通过考试的电子邮件会附带把这个举荐表发给你。举荐人必须审查你的履历，确保你在 8 个 CISSP 知识域有足够的工作经验。

然后以数字形式或通过传真或邮寄方式把举荐表提交给(ISC)²。你必须在收到通知考试成绩的电子邮件后的 90 天内，向(ISC)² 递交举荐文件。(ISC)² 将在收到举荐表后结束整个认证流程，并将通过美国邮政(USPS)给你寄送欢迎包。

CISSP 考试后的专项加强认证

(ISC)² 为 CISSP 证书持有者设置了 3 个专项加强认证。(ISC)² 围绕 CISSP 考试介绍的概念设置专项加强认证，主要针对架构、管理和工程这 3 个具体方面。这 3 个专项加强认证如下。

信息系统安全架构师(ISSAP) 面向从事信息安全架构工作的人员。涉及的关键域包括：访问控制系统和方法，密码学，物理安全集成，需求分析和安全标准，指南及准则，业务连续性计划和灾难恢复计划中与技术相关的方面，以及电信和网络安全。这是专为设计安全系统或基础设施的人员，或审计和分析这些结构的人员设置的一种证书。

信息系统安全管理师(ISSMP) 面向从事信息安全策略、实践规范、原则和规程管理的人员，涉及的关键域包括：企业安全管理实践规范，企业系统开发安全，法律、调查、犯罪取证和职业操守，运营安全合规监督，以及了解业务连续性计划，灾难恢复计划和运行连续性计划。这是专为负责安全基础设施(特别是必须强制合规的安全基础设施)的人员设置的一种证书。

信息系统安全工程师(ISSEP) 面向设计安全软硬件信息系统、组件或应用程序的人员，涉及的关键域包括：认证和认可、系统安全工程、技术管理和美国政府信息保障法规。大多数 ISSEP 为美国政府部门或管理政府安全审查的政府承包商工作。

有关这些专项加强认证的详细信息，可访问(ISC)² 网站 www.isc2.org 查阅。

本书的组织结构

本书涵盖 CISSP 通用知识体系的 8 个域，其深度足以让你清晰掌握相关资料。本书的主体由 21 章构成。域和各章的关系说明如下。

第 1~4 章：安全与风险管理。

第 5 章：资产安全。

第 6~10 章：安全架构和工程。

第 11 章和第 12 章：通信与网络安全。

第 13 章和第 14 章：身份和访问管理(IAM)。

第 15 章：安全评估与测试。

第 16~19 章：安全运营。

第 20 章和第 21 章：软件开发安全。

每章包含的元素可帮助你归纳学习重点和检验你掌握的知识。有关每章所涵盖域主题的详情，请见本书目录和各章介绍。

本学习指南的元素

你在阅读本学习指南的过程中会见到许多反复出现的元素。下面将介绍其中的部分元素：

考试要点 考试要点突出了可能以某种形式出现在考试中的主题。虽然我们显然无从确切知道某次考试将包括哪些内容，但这个元素将强化对于掌握 CBK 特定方面知识及 CISSP 考试规范至关重要的概念。

复习题 每章都设有复习题，旨在衡量你对该章所述关键理念的掌握程度。你应该在读完每章内容后把这些题做一遍：如果你答错了一些题，说明你需要耗费更长时间来钻研相关主题。本书附录 B 给出复习题的答案。

书面实验 每章都设有书面实验，用以综述该章出现的各种概念和主题。书面实验提出的问题旨在帮助你把散布于该章各处的重要内容归纳到一起形成一个整体，使你能够提出或描述潜在安全战略或解决方案。

真实场景 在学习各章内容的过程中，你会发现对典型且真实可信的工作场景的描述，在这些情景下，你从该章学到的安全战略和方法可在解决问题或化解潜在困难的过程中发挥作用。这让你有机会了解如何把具体安全策略、指南或实践规范应用到实际工作中。

本章小结 这是对该章的简要回顾，归纳了该章涵盖的内容。

附加的学习工具

本书的读者可以得到一些附加的学习工具。我们努力提供一些必要工具，帮助你完成认证考试。请在准备考试时把下列所有工具都载入你的工作站。



注意：

访问 www.wiley.com/go/cissptestprep 可得到下面介绍的工具。

Sybex 备考软件

Sybex 专家开发的备考软件可帮助你为 CISSP 考试作好充分准备。你会在这个测验引擎中找到本书包含的所有复习题和评估题。你可进行评估测验，逐章检验自己的复习进展，也可选用练习考试或选用涵盖了所有方面问题的随机生成的考试。

电子速记卡

Sybex 开发的电子速记卡包含数百道考题，旨在进一步挑战你参加 CISSP 考试的能力。从复习题、练习考试和速记卡中，你总能找到足够的练习来应对考试！

PDF 格式词汇表

Sybex 提供了一个 PDF 格式的强大词汇表。这个可搜索的全面词汇表包含了你应该掌握的所有关键词语。

附加练习考试

Sybex 包含附加练习考试，每个考试的考题设置旨在了解你对 CISSP CBK 的关键元素掌握了多少。本书有 6 个附加练习考试，每个考试含 150 道考题，以与真实考试最长的时间长度匹配。访问 <http://www.wiley.com/go/sybextestprep> 便可得到这些考试。

如何使用本书的学习工具

本书设计的许多特性旨在辅导你准备 CISSP 认证考试。本书在每一章的开头列出该章涵盖的 CISSP 通用知识体系域主题，同时确保该章对每个主题进行充分论述，以此对你提供帮助。每章末尾的复习题和练习考试是为了检验你对学过的内容记住了多少，确保你清楚自己还需要在哪些方面多加努力。以下是使用本书和学习工具的几点建议(详见 www.wiley.com/go/cissptestprep)：

- 开始阅读本书之前先进行一次评估测验。这会让你了解哪些方面需要自己投入更多学习时间，以及哪些方面只需要简单复习一下即可。
- 读完每一章后回答复习题：每当你的答案有误时，都应回到该章重读相关主题，若还需要更多信息，则可从其他资源找出相关内容深入学习。
- 把速记卡下载到你的移动设备上，白天有空闲时间时就看几分钟。
- 抓住每个机会测试自己。除了评估测验和复习题以外，附带的学习工具还有附加练习考试。在不参考相关章节的情况下进行这些考试，看看自己做到什么程度，然后回头复习与丢分相关的主题，直到你完全掌握所有内容并能灵活应用这些概念为止。

最后，如果可能，找一个伙伴。有个人陪伴你一起复习备考，当你遇到有困难的主题时伸手帮你一把，这会使整个过程变得轻松愉快。你還可在伙伴的薄弱环节帮助他，以此来巩固自己学过的知识。

评估测验

1. 以下哪类访问控制寻求发现不良、未经授权、非法行为的证据？
 - 预防
 - 威慑
 - 检测
 - 纠正

2. 定义和详述口令挑选过程中可把良好口令选择与最终属于糟糕的口令选择区分开来的方面。

- A. 难猜或无法预料
- B. 符合最低长度要求
- C. 符合特定复杂性要求
- D. 以上所有

3. 以下哪一项最有可能检测出 DoS 攻击？

- A. 基于主机的 IDS
- B. 基于网络的 IDS
- C. 漏洞扫描器
- D. 渗透测试

4. 以下哪一项属于 DoS 攻击？

- A. 在电话上假扮一名技术经理，要求接听者更改他们的口令
- B. 上网向一台 Web 服务器发送一条畸形 URL，造成系统占用百分之百 CPU
- C. 复制从某一特定子网流过的数据包，以此窃听通信流
- D. 出于骚扰目的向没有提出请求的接收者发送消息包

5. 路由器在 OSI 模型的哪一层运行？

- A. 网络层
- B. 第 1 层
- C. 传输层
- D. 第 5 层

6. 哪种防火墙可以根据当前会话的通信流内容自动调整过滤规则？

- A. 静态数据包过滤
- B. 应用级网关
- C. 电路级网关
- D. 动态数据包过滤

7. VPN 可在以下哪种连接上建立？

- A. 无线 LAN 连接
- B. 远程访问拨号连接
- C. WAN 链接
- D. 以上所有

8. 哪种恶意软件利用社会工程伎俩诱骗受害者安装？

- A. 病毒
- B. 蠕虫
- C. 木马
- D. 逻辑炸弹

9. 构成 CIA 三部曲的是哪些元素？

- A. 邻接、互操作、安全有序
- B. 身份验证、授权和问责制

- C. 胜任、可用、一体化
 - D. 可用性、保密性、完整性
10. 以下哪一项不是支持问责制所有要求的成分?
- A. 审计
 - B. 隐私
 - C. 身份验证
 - D. 授权
11. 以下哪一项不属于防范串通的措施?
- A. 职责分离
 - B. 受限岗位责任
 - C. 组用户账户
 - D. 岗位轮换
12. 数据托管员在 _____ 为资源分配安全标签后负责确保资源安全。
- A. 高管
 - B. 数据所有者
 - C. 审计员
 - D. 安全人员
13. 软件能力成熟度模型(SW-CMM)在哪个阶段用量化测量获得对软件开发过程的详细了解?
- A. 可重复级
 - B. 定义级
 - C. 管理级
 - D. 优化级
14. 环保护方案通常不在以下哪一层实际执行?
- A. 第 0 层
 - B. 第 1 层
 - C. 第 3 层
 - D. 第 4 层
15. TCP/IP 三次握手序列的最后阶段是什么?
- A. SYN 包
 - B. ACK 包
 - C. NAK 包
 - D. SYN/ACK 包
16. 参数检查是解决以下哪种漏洞的最佳方式?
- A. 对使用时间的时间检查
 - B. 缓冲区溢出
 - C. SYN 洪水
 - D. 分布式拒绝服务

17. 以下哪一项是下面所示逻辑运算的值?

X:	0 1 1 0 1 0
Y:	0 0 1 1 0 1

X \vee Y: ?

- A. 011111
- B. 011010
- C. 001000
- D. 001101

18. 在哪类密码中, 明文消息的字母被重新排列而形成密文?

- A. 替换密码
- B. 块密码
- C. 移位密码
- D. 单次密本

19. 以下哪一项是 MD5 算法生成的消息摘要的长度?

- A. 64 位
- B. 128 位
- C. 256 位
- D. 384 位

20. 如果 Renee 收到 Mike 发来的一条有数字签名的消息, 她用哪个密钥来验证消息确实发自 Mike?

- A. Renee 的公钥
- B. Renee 的私钥
- C. Mike 的公钥
- D. Mike 的私钥

21. 以下哪一项不涉及安全模型的构成原理?

- A. 级联
- B. 反馈
- C. 迭代
- D. 连接

22. TCB 中共同执行引用监测功能的组件集是什么?

- A. 安全边界
- B. 安全内核
- C. 访问矩阵
- D. 受限界面

23. 以下哪个陈述是正确的?

- A. 系统越不复杂, 漏洞越多
- B. 系统越复杂, 提供的保障越少
- C. 系统越简单, 可信度越低
- D. 系统越复杂, 所形成的受攻击面越小

24. 从被称为保护环的设计架构安全机制的角度看, 0 环还指以下四项中除哪一项外的其他三项?
- A. 特权模式
 - B. 监管模式
 - C. 系统模式
 - D. 用户模式
25. 审计踪迹、日志、闭路电视监控系统(CCTV)、入侵检测系统、杀毒软件、渗透测试、口令破解器、性能监控和循环冗余校验(CRC)是以下哪一项的例子?
- A. 指示控制
 - B. 预防控制
 - C. 检测控制
 - D. 纠正控制
26. 系统架构、系统完整性、隐蔽通道分析、可信设施管理和可信恢复是什么安全准则的元素?
- A. 质量保障
 - B. 运行保障
 - C. 生命周期保障
 - D. 数量保障
27. 以下哪一项是专为测试并或许绕过系统安全控制而设计的一种规程?
- A. 日志使用数据
 - B. 战争拨号
 - C. 渗透测试
 - D. 部署受保护台式机工作站
28. 审计是用来保持和执行什么的因素?
- A. 问责制
 - B. 保密性
 - C. 可访问性
 - D. 冗余
29. 以下哪一项是用来计算 ALE 的公式?
- A. $ALE = AV * EF * ARO$
 - B. $ALE = ARO * EF$
 - C. $ALE = AV * ARO$
 - D. $ALE = EF * ARO$
30. 以下哪一项是业务影响评估流程的第一步?
- A. 确定优先级
 - B. 可能性评估
 - C. 风险识别
 - D. 资源优先级排序

31. 以下哪一项代表了可能会对组织构成威胁或风险的自然事件?
- A. 地震
 - B. 洪水
 - C. 龙卷风
 - D. 以上所有
32. 哪种恢复设施可使组织在主设施发生事故后尽快恢复运行?
- A. 热站点
 - B. 温站点
 - C. 冷站点
 - D. 以上所有
33. 以下哪种形式的知识产权可用来保护文字、口号和徽标?
- A. 专利
 - B. 版权
 - C. 商标
 - D. 商业机密
34. 以下哪类证据是指可拿到法庭上证明某个事实的书面文件?
- A. 最佳证据
 - B. 工资表证据
 - C. 文档证据
 - D. 言辞证据
35. 军事和情报攻击为什么被列在最严重计算机罪行之中?
- A. 落入敌人之手的信息一旦被利用,有可能对国家利益产生深远的不利战略影响。
 - B. 军事信息保存在安全的机器里,一旦被成功攻击,会令人颜面尽失。
 - C. 机密信息被人长期用于政治目的,会影响一个国家的领导地位。
 - D. 军事和情报机构已确保保护他们的信息的法律是最严厉的法律。
36. 哪类被检测出来的事件可为调查提供最长时间?
- A. 破坏
 - B. 拒绝服务
 - C. 恶意代码
 - D. 扫描
37. 如果你想限制一个设施的进出,你会选用以下哪一项?
- A. 大门
 - B. 旋转门
 - C. 围栏
 - D. 捕人陷阱
38. 二级验证系统的意义是什么?
- A. 验证用户的身份
 - B. 验证用户的活动
 - C. 验证系统的完整性
 - D. 验证系统的正确性

39. 当有大量不请自来的消息被发送给受害者时，就发生了垃圾邮件攻击。由于发送给受害者的数据多得足以阻止正常活动，这种攻击又叫什么？
- A. 嗅探
 - B. 拒绝服务
 - C. 蛮力攻击
 - D. 缓冲区溢出攻击
40. 哪类入侵检测系统(IDS)可视为一种专家系统？
- A. 基于主机的 IDS
 - B. 基于网络的 IDS
 - C. 基于知识的 IDS
 - D. 基于行为的 IDS

评估测验答案

1. C. 检测访问控制用于发现(并记录)不良或未经授权活动。
2. D. 强口令选择难猜、不可预料和且符合规定的最低长度要求，以确保口令条目不可能被自动确定。口令可随机生成，使用所有字母、数字和标点符号字符；它们绝不应被写下来或与人共享；它们不应保存在可公开访问或通常可读的位置；它们还不应被明文传送。
3. B. 基于网络的 IDS 通常能检测攻击的发起或实施攻击的持续尝试(包括拒绝服务，即 DoS)。但它们不能提供信息说明攻击是否得逞或哪些具体系统、用户账号、文件或应用程序受到影响。基于主机的 IDS 在检测和跟踪 DoS 攻击方面有些困难。漏洞扫描器不检测 DoS 攻击。它们测试可能存在的漏洞。渗透测试可能会造成 DoS 攻击或用于测试 DoS 漏洞，但它不属于检测工具。
4. B. 并非 DoS 攻击的所有情况都是恶意动机的结果。在编写操作系统、服务和应用程序时出现的错误也曾导致出现 DoS 情况。这方面的例子包括一个进程未能释放对 CPU 的控制，或一项服务对系统资源的消耗与该服务正在处理的服务请求不成比例。社会工程和嗅探通常不属于 DoS 攻击。
5. A. 网络硬件设备(包括路由器)在第 3 层(即网络层)运行。
6. D. 动态包过滤服务器可根据通信流内容，实时修改过滤规则。
7. D. VPN 链接可在任何其他网络通信连接上建立。它们可能是典型的 LAN 电缆连接、无线 LAN 连接、远程访问拨号连接、WAN 连接，甚至可能是客户端为访问办公室 LAN 而使用的互联网连接。
8. C. 木马是恶意软件的一种形式，借助社会工程伎俩诱使受害者安装——所用伎俩是使受害者相信，他们下载或得到的只是一个主机文件，而实际上，却是一个隐藏的恶意载荷。
9. D. CIA 三部曲的成分是保密性、可用性和完整性。
10. B. 隐私不必支持问责制。
11. C. 组用户账户允许多人以一个用户账户登录。由于它阻碍问责，因此使串通得以实现。

12. B. 数据所有者在数据托管员对资源实施适当保护之前，必须先给资源分配一个安全标签。

13. C. SW-CMM 的“管理级”阶段涉及使用量化开发测量指标。SEI 把这一层涉及关键流程的方面定义为量化流程管理和软件质量管理。

14. B. 第 1 层和第 2 层含设备驱动，但通常不实际执行。第 0 层始终含安全内核。第 3 层含用户应用程序。第 4 层不存在。

15. B. SYN 包首先从发起主机发送给目的主机。目的主机随后用一个 SYN/ACK 包回应。发起主机这时发送一个 ACK 包，连接由此建立。

16. B. 参数检查用于预防出现缓冲区溢出攻击的可能性。

17. A. ~OR 符号表示 OR 函数，当一个或两个输入位为真时为真。

18. C. 移位密码通过一种加密算法重新排列明文消息的字母，形成密文消息。

19. B. MD5 算法可为任何输入生成 128 位消息摘要。

20. C. 任何接收者都能用 Mike 的公钥验证数字签名的真实性。

21. C. 迭代不属涉及安全模型的构成原理。级联、反馈和连接是三大构成原理。

22. B. TCB 中共同执行参考监测功能的组件集叫安全内核。

23. B. 系统越复杂，提供的保障越低。更复杂意味着更多方面存在漏洞，更多方面必须在保护下抵御威胁。更多的漏洞和威胁意味着系统随之提供的安全保护可靠性较低。

24. D. 0 环可直接访问大多数资源；因此，用户模式并不是合适的标签，因为用户模式要求通过限制条件来制约对资源的访问。

25. C. 检测控制的例子包括审计踪迹、日志、CCTV、入侵检测系统、杀毒软件、渗透测试、口令破解器、性能监控和循环冗余校验(CRC)。

26. B. 保障是指你在满足计算机、网络、解决方案等的安全需要时所能给予的可信程度。运行保障侧重于可帮助支持安全性的系统基本性能和架构。

27. C. 渗透测试尝试绕过安全控制以检测系统的总体安全性。

28. A. 审计是用来保持和执行问责制的因素。

29. A. 年度损失期望(ALE)是资产价值(AV)乘以暴露因子(EF)后再乘以年度发生率(ARO)的积。这是公式 $ALE = SLE * ARO$ 的加长形式。这里显示的其他公式不能准确反映这一计算。

30. A. 确定优先级是业务影响评估流程的第一步。

31. D. 会对组织构成威胁的自然事件包括地震、洪水、飓风、龙卷风、火灾以及其他自然灾害。因此，选项 A、B、C 都正确，因为它们是自然发生而非人为的。

32. A. 热站点提供的备份设施始终保持一种工作状态，完全可接管业务运行。温站点为业务运行预先配置好了硬件和软件，但这些硬件和软件不含关键业务信息。冷站点是配备了电力和环境支持系统的简单设施，但不含经过配置的硬件、软件或服务。灾难恢复服务可代表一家公司推进并运行这些站点。

33. C. 商标可用来保护代表一家公司及其产品或服务的文字、口号和徽标。

34. C. 拿到法庭上证明某一案件的事实性的书面文件叫作文档证据。

35. A. 军事和情报攻击的目的是获取机密信息。这些信息落入敌人之手一旦被利用，会造成近乎无限的不利影响。这类攻击由极其老练的攻击者发起，往往很难查明哪些文件被成功攫取。所以当这种破坏事件发生时，你经常无法搞清损失到底有多大。

36. D。扫描事件往往是侦察性攻击，而对系统真正造成损害的是后续攻击，因此，如果你早期检测出扫描攻击，你可能会有一些时间来作出反应。

37. B。旋转门是一种大门，可防止多人同时进入，并且往往把行进限制在一个方向上。它用于让人只进不出，或只出不进。

38. D。建立二级验证机制是为了形成验证检测系统和传感器正确性的手段。这往往意味着把多种类型传感器或系统(CCTV、热和运动传感器等)组合到一起，共同勾勒被测出事件的更完整图像。

39. B。垃圾邮件攻击(发送大量不请自来的电子邮件)可当作一种拒绝服务攻击手段使用。它不借助窃听方法，因此不属于嗅探。蛮力攻击旨在破解口令。缓冲区溢出攻击向系统发送数据串，旨在造成系统瘫痪。

40. D。基于行为的 IDS 可贴上专家系统或伪人工智能系统的标签，因为它能够学习并对事件作出假设。换句话说，这种 IDS 可像人类专家那样对照已知事件评估当前事件。基于知识的 IDS 通过“已知攻击方法”数据库来检测攻击。基于主机和基于网络的 IDS 可基于知识或行为，也可同时基于知识和行为。

目 录

第1章 实现安全治理的原则和策略	1
1.1 理解和应用保密性、完整性及可用性的概念	1
1.1.1 保密性	2
1.1.2 完整性	3
1.1.3 可用性	4
1.1.4 其他安全概念	6
1.1.5 保护机制	8
1.1.6 分层	9
1.1.7 抽象	9
1.1.8 数据隐藏	9
1.1.9 加密	10
1.2 评估和应用安全治理原则	10
1.2.1 与业务战略、目标、使命和宗旨相一致的安全功能	10
1.2.2 组织的流程	12
1.2.3 组织的角色与责任	16
1.2.4 安全控制框架	17
1.2.5 应尽关心和尽职审查	18
1.3 开发、记录和实施安全策略、标准、程序和指南	18
1.3.1 安全策略	18
1.3.2 标准、基线和指南	19
1.3.3 程序	20
1.4 理解与应用威胁建模的概念和方法	21
1.4.1 识别威胁	22
1.4.2 确定和绘制潜在的攻击	25
1.4.3 执行简化分析	26
1.4.4 优先级排序和响应	26
1.5 将基于风险的管理理念应用到供应链	27
1.6 本章小结	28
1.7 考试要点	29
1.8 书面实验	31
1.9 复习题	31
第2章 人员安全和风险管理的概念	35
2.1 人员安全策略和程序	36
2.1.1 候选人筛选及招聘	38
2.1.2 雇佣协议及策略	38
2.1.3 入职和离职程序	39
2.1.4 供应商、顾问和承包商的协议和控制	41
2.1.5 合规策略要求	42
2.1.6 隐私策略要求	42
2.2 安全治理	43
2.3 理解并应用风险管理理念	44
2.3.1 风险术语	45
2.3.2 识别威胁和脆弱性	46
2.3.3 风险评估/分析	47
2.3.4 风险响应	53
2.3.5 选择与实施控制措施	54
2.3.6 适用的控制类型	56
2.3.7 安全控制评估	57
2.3.8 监视和测量	57
2.3.9 资产估值与报告	57
2.3.10 持续改进	58
2.3.11 风险框架	59
2.4 建立和维护安全意识、教育和培训计划	60
2.5 管理安全功能	61
2.6 本章小结	62
2.7 考试要点	62
2.8 书面实验	64
2.9 复习题	64
第3章 业务连续性计划	68
3.1 业务连续性计划简介	68

3.2 项目范围和计划	69	4.8 复习题	107
3.2.1 业务组织分析	69		
3.2.2 选择 BCP 团队	70		
3.2.3 资源需求	71		
3.2.4 法律和法规要求	72		
3.3 业务影响评估	73		
3.3.1 确定优先级	74		
3.3.2 风险识别	74		
3.3.3 可能性评估	75		
3.3.4 影响评估	76		
3.3.5 资源优先级排序	77		
3.4 连续性计划	77		
3.4.1 策略开发	77		
3.4.2 预备和处理	78		
3.5 计划批准和实施	79		
3.5.1 计划批准	79		
3.5.2 计划实施	79		
3.5.3 培训和教育	80		
3.5.4 BCP 文档化	80		
3.6 本章小结	83		
3.7 考试要点	83		
3.8 书面实验	84		
3.9 复习题	84		
第 4 章 法律、法规和合规	88		
4.1 法律的分类	88		
4.1.1 刑法	89		
4.1.2 民法	90		
4.1.3 行政法	90		
4.2 法律	90		
4.2.1 计算机犯罪	91		
4.2.2 知识产权	94		
4.2.3 许可	97		
4.2.4 进口/出口控制	98		
4.2.5 隐私	98		
4.3 合规	104		
4.4 合同和采购	105		
4.5 本章小结	105		
4.6 考试要点	106		
4.7 书面实验	106		
第 5 章 保护资产安全	110		
5.1 资产识别和分类	110		
5.1.1 定义敏感数据	111		
5.1.2 定义数据分类	112		
5.1.3 定义资产分类	114		
5.1.4 确定数据的安全控制	114		
5.1.5 理解数据状态	115		
5.1.6 管理信息和资产	116		
5.1.7 数据保护方法	121		
5.2 定义数据所有权	123		
5.2.1 数据所有者	123		
5.2.2 资产所有者	124		
5.2.3 业务/任务所有者	124		
5.2.4 数据使用者	125		
5.2.5 管理员	127		
5.2.6 托管员	127		
5.2.7 用户	128		
5.2.8 保护隐私	128		
5.3 使用安全基线	128		
5.3.1 范围界定和接受定制	129		
5.3.2 选择标准	129		
5.4 本章小结	130		
5.5 考试要点	130		
5.6 书面实验	131		
5.7 复习题	131		
第 6 章 密码学和对称密钥算法	135		
6.1 密码学的历史里程碑	135		
6.1.1 凯撒密码	136		
6.1.2 美国南北战争	136		
6.1.3 Ultra 与 Enigma	137		
6.2 密码学基本知识	137		
6.2.1 密码学的目标	137		
6.2.2 密码学的概念	139		
6.2.3 密码数学	140		
6.2.4 密码	144		
6.3 现代密码学	149		
6.3.1 密码密钥	149		
6.3.2 对称密钥算法	150		

6.3.3 非对称密钥算法	151	7.6.5 联网	185
6.3.4 散列算法	153	7.7 密码攻击	187
6.4 对称密码	154	7.8 本章小结	189
6.4.1 数据加密标准	154	7.9 考试要点	190
6.4.2 三重 DES	155	7.10 书面实验	191
6.4.3 国际数据加密算法	156	7.11 复习题	191
6.4.4 Blowfish	157		
6.4.5 Skipjack	157		
6.4.6 高级加密标准	157		
6.4.7 对称密钥管理	158		
6.5 密码生命周期	160	第 8 章 安全模型、设计和能力的原则	195
6.6 本章小结	160	8.1 使用安全设计原则实施和 管理工程过程	195
6.7 考试要点	161	8.1.1 客体和主体	196
6.8 书面实验	162	8.1.2 封闭系统和开放系统	196
6.9 复习题	162	8.1.3 用于确保保密性、完整性和 可用性的技术	197
第 7 章 PKI 和密码应用	166	8.1.4 控制	198
7.1 非对称密码	166	8.1.5 信任与保证	198
7.1.1 公钥和私钥	167	8.2 理解安全模型的基本概念	199
7.1.2 RSA	167	8.2.1 可信计算基	200
7.1.3 El Gamal	169	8.2.2 状态机模型	201
7.1.4 椭圆曲线	169	8.2.3 信息流模型	201
7.2 散列函数	170	8.2.4 非干扰模型	202
7.2.1 SHA	171	8.2.5 Take-Grant 模型	202
7.2.2 MD2	171	8.2.6 访问控制矩阵	203
7.2.3 MD4	171	8.2.7 Bell-LaPadula 模型	204
7.2.4 MD5	172	8.2.8 Biba 模型	206
7.3 数字签名	172	8.2.9 Clark-Wilson 模型	207
7.3.1 HMAC	173	8.2.10 Brewer and Nash 模型	208
7.3.2 数字签名标准	174	8.2.11 Goguen-Meseguer 模型	208
7.4 公钥基础设施	174	8.2.12 Sutherland 模型	209
7.4.1 证书	174	8.2.13 Graham-Denning 模型	209
7.4.2 发证机构	175	8.3 基于系统安全需求选择控制 措施	209
7.4.3 证书的生成和销毁	176	8.3.1 彩虹系列	210
7.5 非对称密钥管理	177	8.3.2 TCSEC 分类和所需功能	211
7.6 应用密码学	178	8.3.3 通用准则	214
7.6.1 便携设备	178	8.3.4 行业和国际安全实施指南	217
7.6.2 电子邮件	179	8.3.5 认证和鉴定	217
7.6.3 Web 应用程序	180	8.4 理解信息系统的安全功能	219
7.6.4 数字版权管理	182	8.4.1 内存保护	219
		8.4.2 虚拟化	220

8.4.3 可信平台模块	220	9.11 基本安全保护机制	270
8.4.4 接口	220	9.11.1 技术机制	270
8.4.5 容错	221	9.11.2 安全策略和计算机架构	272
8.5 本章小结	221	9.11.3 策略机制	273
8.6 考试要点	221	9.12 常见的架构缺陷和安全问题	273
8.7 书面实验	222	9.12.1 隐蔽通道	274
8.8 复习题	222	9.12.2 基于设计或编码缺陷的攻击和 安全问题	274
第 9 章 安全漏洞、威胁和对策	226	9.12.3 编程	276
9.1 评估和缓解安全漏洞	227	9.12.4 计时、状态改变和通信中断	277
9.1.1 硬件	227	9.12.5 技术和过程集成	277
9.1.2 固件	241	9.12.6 电磁辐射	277
9.2 基于客户端的系统	242	9.13 本章小结	278
9.2.1 applet	242	9.14 考试要点	278
9.2.2 本地缓存	244	9.15 书面实验	280
9.3 基于服务端的系统	245	9.16 复习题	281
9.4 数据库系统安全	246	第 10 章 物理安全要求	284
9.4.1 聚合	246	10.1 站点与设施设计的安全原则	285
9.4.2 推理	246	10.1.1 安全设施计划	285
9.4.3 数据挖掘和数据仓库	247	10.1.2 站点选择	285
9.4.4 数据分析	247	10.1.3 可见度	286
9.4.5 大规模并行数据系统	248	10.1.4 自然灾害	286
9.5 分布式系统和端点安全	248	10.1.5 设施设计	286
9.5.1 基于云的系统和云计算	250	10.2 实现站点与设施安全控制	287
9.5.2 网格计算	253	10.2.1 设备故障	288
9.5.3 对等网络	253	10.2.2 配线间	288
9.6 物联网	254	10.2.3 服务器间与数据中心	290
9.7 工业控制系统	255	10.2.4 介质存储设施	293
9.8 评估和缓解基于 Web 系统的 漏洞	255	10.2.5 证据存储	293
9.9 评估和缓解移动系统的漏洞	259	10.2.6 受限区与工作区安全	294
9.9.1 设备安全	260	10.2.7 基础设施与 HVAC	295
9.9.2 应用安全	263	10.2.8 灾灾预防、探测与消防	297
9.9.3 BYOD 关注点	264	10.3 物理安全的实现与管理	300
9.10 评估和缓解嵌入式设备和 信息物理系统的漏洞	267	10.3.1 边界安全控制	300
9.10.1 嵌入式系统和静态系统的 示例	267	10.3.2 内部安全控制	303
9.10.2 保护嵌入式和静态系统的 方法	268	10.4 本章小结	306
		10.5 考试要点	307
		10.6 书面实验	309
		10.7 复习题	309

第 11 章 安全网络架构和保护网络组件	312	12.2 语音通信的安全	375
11.1 OSI 模型	312	12.2.1 VoIP	375
11.1.1 OSI 模型的历史	313	12.2.2 社会工程	376
11.1.2 OSI 功能	313	12.2.3 欺骗与滥用	377
11.1.3 封装/解封	314	12.3 多媒体合作	378
11.1.4 OSI 模型层次	315	12.3.1 远程会议	379
11.2 TCP/IP 模型	321	12.3.2 即时通信	379
11.3 融合协议	334	12.4 管理邮件安全	379
11.4 无线网络	336	12.4.1 邮件安全目标	380
11.4.1 保护无线接入点	336	12.4.2 理解邮件安全问题	381
11.4.2 保护 SSID	338	12.4.3 邮件安全解决方案	381
11.4.3 进行现场调查	338	12.5 远程访问安全管理	383
11.4.4 使用安全加密协议	339	12.5.1 远程访问安全计划	385
11.4.5 天线放置	341	12.5.2 拨号上网协议	386
11.4.6 天线类型	342	12.5.3 中心化远程身份验证服务	386
11.4.7 调整功率电平控制	342	12.6 虚拟专用网	387
11.4.8 WPS	342	12.6.1 隧道技术	387
11.4.9 使用强制门户	343	12.6.2 VPN 的工作机理	388
11.4.10 一般 Wi-Fi 安全程序	343	12.6.3 常用的 VPN 协议	388
11.4.11 无线攻击	344	12.6.4 虚拟局域网	390
11.5 安全网络组件	346	12.7 虚拟化	391
11.5.1 网络访问控制	347	12.7.1 虚拟软件	391
11.5.2 防火墙	347	12.7.2 虚拟化网络	392
11.5.3 端点安全	350	12.8 网络地址转换	392
11.5.4 硬件的安全操作	351	12.8.1 私有 IP 地址	393
11.6 布线、无线、拓扑、通信和 传输介质技术	353	12.8.2 有状态 NAT	394
11.6.1 传输介质	354	12.8.3 静态与动态 NAT	395
11.6.2 网络拓扑	357	12.8.4 自动私有 IP 分配	395
11.6.3 无线通信与安全	359	12.9 交换技术	396
11.6.4 局域网技术	363	12.9.1 电路交换	396
11.7 本章小结	366	12.9.2 分组交换	397
11.8 考试要点	367	12.9.3 虚电路	397
11.9 书面实验	369	12.10 WAN 技术	398
11.10 复习题	369	12.10.1 WAN 连接技术	399
第 12 章 安全通信与网络攻击	373	12.10.2 拨号封装协议	401
12.1 网络与协议安全机制	373	12.11 多种安全控制特征	401
12.1.1 安全通信协议	374	12.11.1 透明性	402
12.1.2 身份验证协议	374	12.11.2 验证完整性	402
		12.11.3 传输机制	402
		12.12 安全边界	403

12.13 防止或减轻网络攻击.....	403	13.6 考试要点.....	440
12.13.1 DoS 与 DDoS.....	404	13.7 书面实验.....	441
12.13.2 窃听.....	404	13.8 复习题.....	441
12.13.3 假冒/伪装.....	405	第 14 章 控制和监控访问.....	445
12.13.4 重放攻击.....	405	14.1 比较访问控制模型.....	445
12.13.5 修改攻击.....	406	14.1.1 比较权限、权利和特权.....	445
12.13.6 地址解析协议欺骗.....	406	14.1.2 理解授权机制.....	446
12.13.7 DNS 毒化、劫持及劫持.....	406	14.1.3 使用安全策略定义需求.....	447
12.13.8 超链接欺骗.....	407	14.1.4 实施纵深防御.....	447
12.14 本章小结.....	407	14.1.5 总结访问控制模型.....	448
12.15 考试要点.....	409	14.1.6 自主访问控制.....	449
12.16 书面实验.....	410	14.1.7 非自主访问控制.....	449
12.17 复习题.....	410	14.2 了解访问控制攻击.....	454
第 13 章 管理身份和身份验证.....	414	14.2.1 风险要素.....	454
13.1 控制对资产的访问.....	414	14.2.2 识别资产.....	455
13.1.1 比较主体和客体.....	415	14.2.3 识别威胁.....	456
13.1.2 CIA 三性和访问控制.....	416	14.2.4 识别漏洞.....	457
13.1.3 访问控制的类型.....	416	14.2.5 常见的访问控制攻击.....	457
13.2 比较身份识别和身份验证.....	418	14.2.6 保护方法综述.....	465
13.2.1 身份注册和证明.....	418	14.3 本章小结.....	467
13.2.2 授权和问责.....	419	14.4 考试要点.....	467
13.2.3 身份验证因素.....	420	14.5 书面实验.....	468
13.2.4 密码.....	421	14.6 复习题.....	468
13.2.5 智能卡和令牌.....	423	第 15 章 安全评估与测试.....	472
13.2.6 生物识别技术.....	425	15.1 构建安全评估和测试方案.....	473
13.2.7 多因素身份验证.....	428	15.1.1 安全测试.....	473
13.2.8 设备验证.....	429	15.1.2 安全评估.....	474
13.2.9 服务身份验证.....	429	15.1.3 安全审计.....	474
13.3 实施身份管理.....	430	15.2 开展漏洞评估.....	476
13.3.1 单点登录.....	430	15.2.1 漏洞描述.....	477
13.3.2 凭据管理系统.....	434	15.2.2 漏洞扫描.....	477
13.3.3 集成身份服务.....	434	15.2.3 渗透测试.....	484
13.3.4 管理会话.....	435	15.3 测试软件.....	486
13.3.5 AAA 协议.....	435	15.3.1 代码审查与测试.....	486
13.4 管理身份和访问配置生命周期.....	437	15.3.2 接口测试.....	489
13.4.1 访问配置.....	437	15.3.3 错用例测试.....	489
13.4.2 账户审核.....	438	15.3.4 测试覆盖率分析.....	490
13.4.3 账户撤销.....	439	15.3.5 网站监测.....	490
13.5 本章小结.....	439		

15.4 实施安全管理流程	491	16.8 书面实验	522
15.4.1 日志审查	491	16.9 复习题	523
15.4.2 账户管理	491	第 17 章 事件的预防和响应	526
15.4.3 备份验证	492	17.1 事件响应管理	527
15.4.4 关键绩效和风险指标	492	17.1.1 事件的定义	527
15.5 本章小结	492	17.1.2 事件响应步骤	527
15.6 考试要点	493	17.2 落实检测和预防措施	532
15.7 书面实验	494	17.2.1 基本预防措施	532
15.8 复习题	494	17.2.2 了解攻击	533
第 16 章 安全运营管理	498	17.2.3 入侵检测和预防系统	540
16.1 应用安全运营概念	498	17.2.4 具体预防措施	545
16.1.1 知其所需和最小特权	499	17.3 日志记录、监测和审计	553
16.1.2 职责分离	500	17.3.1 日志记录和监测	553
16.1.3 岗位轮换	502	17.3.2 出口监测	559
16.1.4 强制休假	503	17.3.3 效果评价审计	561
16.1.5 特权账户管理	503	17.3.4 安全审计和审查	564
16.1.6 管理信息生命周期	504	17.3.5 报告审计结果	564
16.1.7 服务水平协议	505	17.4 本章小结	566
16.1.8 关注人员安全	506	17.5 考试要点	567
16.2 安全配置资源	507	17.6 书面实验	569
16.2.1 管理硬件和软件资产	507	17.7 复习题	570
16.2.2 保护物理资产	508	第 18 章 灾难恢复计划	573
16.2.3 管理虚拟资产	509	18.1 灾难的本质	574
16.2.4 管理云资产	509	18.1.1 自然灾难	574
16.2.5 介质管理	510	18.1.2 人为灾难	577
16.3 配置管理	513	18.2 理解系统恢复和容错能力	580
16.3.1 基线	513	18.2.1 保护硬盘驱动器	581
16.3.2 使用镜像技术创建基线	513	18.2.2 保护服务器	582
16.4 变更管理	514	18.2.3 保护电源	583
16.4.1 安全影响分析	516	18.2.4 受信恢复	583
16.4.2 版本控制	516	18.2.5 服务质量	584
16.4.3 配置文档	517	18.3 恢复策略	585
16.5 补丁管理和漏洞减少	517	18.3.1 确定业务单元的优先顺序	585
16.5.1 系统管理	517	18.3.2 危机管理	586
16.5.2 补丁管理	518	18.3.3 应急通信	586
16.5.3 漏洞管理	519	18.3.4 工作组恢复	586
16.5.4 常见的漏洞和风险	520	18.3.5 可替代的工作站点	587
16.6 本章小结	521	18.3.6 相互援助协议	590
16.7 考试要点	521	18.3.7 数据库恢复	590

18.4 恢复计划开发	592	19.6 书面实验	619	
18.4.1 紧急事件响应	592	19.7 复习题	619	
18.4.2 人员通知	593	第 20 章	软件开发安全	623
18.4.3 评估	593	20.1 系统开发控制概述	623	
18.4.4 备份和离站存储	593	20.1.1 软件开发	624	
18.4.5 软件托管协议	596	20.1.2 系统开发生命周期	628	
18.4.6 外部通信	597	20.1.3 生命周期模型	630	
18.4.7 公用设施	597	20.1.4 甘特图与 PERT	635	
18.4.8 物流和供应	597	20.1.5 变更和配置管理	635	
18.4.9 恢复与还原的比较	597	20.1.6 DevOps 方法	636	
18.5 培训、意识与文档记录	598	20.1.7 应用编程接口	637	
18.6 测试与维护	599	20.1.8 软件测试	638	
18.6.1 通过测试	599	20.1.9 代码仓库	639	
18.6.2 结构化演练	599	20.1.10 服务水平协议	639	
18.6.3 模拟测试	599	20.1.11 软件采购	640	
18.6.4 并行测试	599	20.2 创建数据库和数据仓储	640	
18.6.5 完全中断测试	599	20.2.1 数据库管理系统的体系结构	641	
18.6.6 维护	600	20.2.2 数据库事务	643	
18.7 本章小结	600	20.2.3 多级数据库的安全性	644	
18.8 考试要点	600	20.2.4 ODBC	646	
18.9 书面实验	601	20.2.5 NoSQL	646	
18.10 复习题	601	20.3 存储数据和信息	647	
第 19 章 调查和道德	605	20.3.1 存储器的类型	647	
19.1 调查	605	20.3.2 存储器威胁	647	
19.1.1 调查的类型	606	20.4 理解基于知识的系统	648	
19.1.2 证据	607	20.4.1 专家系统	648	
19.1.3 调查过程	610	20.4.2 机器学习	649	
19.2 计算机犯罪的主要类别	613	20.4.3 神经网络	649	
19.2.1 军事和情报攻击	613	20.4.4 安全性应用	649	
19.2.2 商业攻击	614	20.5 本章小结	650	
19.2.3 财务攻击	614	20.6 考试要点	650	
19.2.4 恐怖攻击	614	20.7 书面实验	651	
19.2.5 恶意攻击	615	20.8 复习题	651	
19.2.6 共同攻击	616	第 21 章 恶意代码和应用攻击	654	
19.3 道德规范	616	21.1 恶意代码	654	
19.3.1 (ISC) ² 的道德规范	616	21.1.1 恶意代码的来源	654	
19.3.2 道德规范和互联网	617	21.1.2 病毒	655	
19.4 本章小结	618	21.1.3 逻辑炸弹	659	
19.5 考试要点	618	21.1.4 特洛伊木马	660	

21.1.5 蠕虫	661	21.4.3 SQL注入攻击	669
21.1.6 间谍软件与广告软件	662	21.5 侦察攻击	671
21.1.7 零日(Zero-Day)攻击	663	21.5.1 IP探测	672
21.2 密码攻击	663	21.5.2 端口扫描	672
21.2.1 密码猜测攻击	663	21.5.3 漏洞扫描	672
21.2.2 字典攻击	664	21.6 伪装攻击	673
21.2.3 社会工程学	665	21.6.1 IP欺骗	673
21.2.4 对策	666	21.6.2 会话劫持	673
21.3 应用程序攻击	666	21.7 本章小结	673
21.3.1 缓冲区溢出	666	21.8 考试要点	674
21.3.2 检验时间到使用时间	667	21.9 书面实验	674
21.3.3 后门	667	21.10 复习题	675
21.3.4 权限提升和 rootkit	667		
21.4 Web 应用的安全性	668	附录 A 书面实验答案	678
21.4.1 跨站脚本	668	附录 B 复习题答案	687
21.4.2 跨站请求伪造	669		

实现安全治理的原则和策略

本章涵盖的 CISSP 认证考试主题包括：

✓ 域 1：安全与风险管理

- 1.1 理解和应用保密性、完整性及可用性的概念
- 1.2 评估和应用安全治理原则

 1.2.1 与业务战略、目标、使命和宗旨相一致的安全功能

 1.2.2 组织的流程

 1.2.3 组织的角色与责任

 1.2.4 安全控制框架

 1.2.5 应尽关心和尽职审查

- 1.6 开发、记录和实施安全策略、标准、程序和指南

- 1.10 理解与应用威胁建模的概念和方法

 1.10.1 威胁建模的方法

 1.10.2 威胁建模的概念

- 1.11 将基于风险的管理理念应用到供应链

 1.11.1 与硬件、软件和服务相关的风险

 1.11.2 第三方评估与监测

 1.11.3 最低安全需求

 1.11.4 服务水平要求

CISSP 认证考试通用知识体系(CBK)的“安全与风险管理”域涉及安全解决方案中的许多基础性概念，包括设计、实现和管理安全机制需要了解的原理。“安全与风险管理”域的内容在第 1~4 章以及第 19 章中讨论，请务必阅读所有这些章节以全面认识“安全与风险管理”域的考试主题。

1.1 理解和应用保密性、完整性及可用性的概念

安全管理的概念与原则是实施安全策略和安全解决方案的核心内容。安全管理的概念与原则定义了安全环境中必需的基本参数，也定义了安全策略设计人员和系统实施人员为创建安全解决方案必须实现的目标。对于现实世界中的安全专业人员及 CISSP 考生来说，透彻理解这些内容是非常重要的。本章包含一系列对全球性大企业和小公司安全都适用的安全治理主题。

安全必须要有起点。通常这个起点是最重要的安全原则列表。在这个列表中，保密性、完整性和可用性(Confidentiality, Integrity and Availability, CIA)始终存在，因为它们经常被视为安全基础架构中主要的安全目标和宗旨。它们作为安全基础要素频频出现，以至于被简称为 CIA 三元组(见图 1.1)。



图 1.1 CIA 三元组

安全控制评估通常用来评价这三个核心信息安全原则的符合情况。总的来说，一个完整的安全解决方案应该充分满足这些原则。对脆弱性和风险的评估也基于它们对一个或多个 CIA 三元组原则的威胁。因此，有必要熟悉这些原则并将其作为判断所有安全相关事项的准则。

这三个信息安全原则被视为安全领域最重要的原则。每个原则对特定组织有多重要取决于该组织的安全目标和需求以及组织安全受到威胁的程度。

1.1.1 保密性

CIA 三元组的第一个原则是“保密性”。保密性指为保障数据、客体或资源保密状态而采取的措施。保密性保护的目标是阻止或最小化未经授权的数据访问。保密性关注的安全措施重点在于确保除预期收件人外的任何人都不会接收到或读取到信息。保密性保护为授权用户提供访问资源以及与资源交互的方法，同时主动阻止未经授权的用户对资源的访问。许多安全控制措施可提供保密性保护，包括但不限于加密、访问控制和隐身术。

如果安全机制提供保密性，那它就对阻止未经授权的主体访问数据、客体或资源提供了高度保障。如果保密性受到威胁，就会出现未经授权的信息泄露。客体(object)是安全关系中的被动元素，如文件、计算机、网络连接和应用程序。主体(subject)是安全关系中的主动元素，如用户、程序和计算机。主体作用于客体或对抗客体。主体与客体之间的关系管理称为访问控制。

总的来说，要维护网络中的保密性，必须保护数据避免在存储、处理和传输过程中遭受未经授权的访问、使用或泄露。对于数据、资源和对象的每种状态，都需要独特的安全控制来保持保密性。

许多攻击都聚焦在违反保密性上。这些攻击包括抓包网络流量与窃取密码文件，以及社会工程、端口扫描、肩窥、窃听、嗅探、特权升级等。

违反保密性的行为不仅包括直接的故意攻击，也包括许多由人为错误、疏忽或不称职造成的未经授权的敏感或机密信息泄露。致使违反保密性的事件包括：未正确实现的加密传输，在传输数据前未对远程系统充分进行身份验证，开放的非安全访问点，访问恶意代码打开的后门，错误路由传真，文件遗留在打印机上，甚至在访问终端仍显示数据时走开。

违反保密性可能是因为最终用户或系统管理员的不当行为，也可能是因为安全策略中的疏漏或配置有误的安全控制。

许多控制措施有利于保障保密性以抵御潜在的威胁。这些控制措施包括加密、填充网络流量、严格的访问控制、严格的身份验证程序、数据分类和充分的人员培训。

保密性和完整性相互依赖。没有客体完整性(换句话说，没能力保证客体不受未经授权的修改)，就无法维持客体保密性。保密性的其他相关概念、条件和特征包括：

敏感性 敏感性指信息的特性，这种特性的数据一旦泄露会导致伤害或损失。维持敏感信息的保密性有助于预防伤害或损失。

判断力 判断力是一种操作者可影响或控制信息泄露，以将伤害或损失程度降至最低的决策行为。

关键性 信息的关键程度是其关键性的衡量标准。关键级别越高，越需要保持信息的保密性。高级别的关键性对一个组织的运营和功能必不可少。

隐藏 隐藏(Concealment)指藏匿或防止泄露的行为。通常，隐藏被看成一种掩盖、混淆和干扰注意力的手段。与隐藏相关的一个概念是通过晦涩获得安全，即试图通过隐藏、沉默或保密获得保护。虽然通过晦涩保持安全的有效性未得到公认，但有些情况下它仍然有价值。

保密 保密是指对某事保密或防止信息泄露的行为。

隐私 隐私指对个人身份或可能对他人造成伤害、令他人感到尴尬的信息保密。

隔绝 隔绝(Seclusion)就是把东西放在不可到达的地方。这个位置还可提供严格的访问控制。隔绝有助于实施保密性保护。

隔离 隔离(Isolation)是保持把某些事物与其他事物分离的行为。隔离可用于防止信息混合或信息泄露。

每个组织都需要评估他们想要实施的具体保密性措施。用于实现某种形式保密性的工具和技术可能不支持或不允许其他形式的保密性。

1.1.2 完整性

CIA三元组的第二个原则是完整性。完整性是保护数据可靠性和正确性的概念。完整性保护措施防止了未经授权的数据更改。它确保数据保持准确、未被替换。恰当实施的完整性保护措施允许合法修改数据，同时可预防故意和恶意的未经授权的活动(如病毒和入侵)以及授权用户的误操作(如错误或疏忽)。

为保持完整性，客体必须保持其准确性，并仅由授权的主体按预期方式修改。如果安全机制提供了完整性，它就高度保证数据、客体和资源不会由最初的受保护状态转变到非保护状态。客体在存储、传输或过程中都不应遭受未经授权的更改。因此，保持完整性意味着客体本身不被未经授权地更改，且管理和操作客体的操作系统和程序实体不被破坏。

可从以下三个方面检验完整性：

- 防止未经授权的主体进行修改。
- 防止授权主体进行未经授权的修改，如引入错误。
- 保持客体内外一致以使客体的数据能够真实反映现实世界，而且与任何子客体、对等客体或父客体的关系都是有效的、一致的和可验证的。

为在系统中维持完整性，必须对数据、客体和资源的访问设置严格的控制措施。此外，应

该使用活动记录日志来确保只有经过授权的用户才能访问各自的资源。在存储、传输和处理中维护和验证客体的完整性需要多种控制和监督措施。

许多攻击聚焦在破坏完整性上。这些攻击包括病毒、逻辑炸弹、未经授权的访问、编码和应用程序中的错误、恶意修改、故意替换及系统后门。

与保密性一样，能破坏完整性的不仅有蓄意攻击。人为错误、疏忽或不称职造成了很多未经授权修改敏感信息的案例。导致完整性破坏的事件包括：修改或删除文件，输入无效的数据，修改配置时在命令、代码和脚本中引入错误，引入的病毒，执行恶意代码(如特洛伊木马)。导致完整性破坏的原因可能是任何用户(包括管理员)的操作，也可能是安全策略中的疏漏或配置有误的安全控制。

许多控制措施可预防对完整性的威胁。这些控制措施包括严格的访问控制、严格的身份验证流程、入侵检测系统、客体/数据加密、散列值验证(见第 6 章)、接口限制、输入/功能检查和充分的人员培训。

完整性依赖于保密性。完整性相关的其他概念、条件和特征如下。

- **准确性：**正确且精确无误。
- **真实性：**真实地反映现实。
- **可信性：**可信的或非伪造的。
- **有效性：**实际上(或逻辑上)是正确的。
- **不可否认性：**不能否认执行过某个动作或活动，或能证明通过了某个通信或事件的初始验证。
- **问责制：**对行为和结果负有责任或义务。
- **职责：**负责或控制某人或某事。
- **完整性：**拥有全部需要和必要的组件或部件。
- **全面性：**完整的范围，充分包含所有需要的元素。

不可否认性

不可否认性(Nonrepudiation)确保事件的主体或引发事件的人不能否认事件的发生。不可否认性可预防主体否认发送过消息、执行过动作或导致某个事件的发生。通过标识、身份验证、授权、问责制和审计使不可否认性成为可能。可使用数字证书、会话标识符、事务日志以及其他许多事务性机制和访问控制机制来实施不可否认性。在构建的系统中，如果没有正确实现不可否认性，就不能证明某个特定实体执行了某个操作。不可否认性是问责制的重要组成部分。如果嫌疑人能够证明起诉不成立，他就不会被追究责任。

1.1.3 可用性

CIA 三元组的第三个原则是可用性，这意味着授权主体被授予实时的、不间断的客体访问权限。通常，可用性保护控制措施提供组织所需的充足带宽和实时的处理能力。如果安全机制提供了可用性，它就提供了对数据、客体和资源可被授权主体访问的高度保障。

可用性包括对客体的有效持续访问及抵御拒绝服务(DoS)攻击。可用性还意味着支撑性基础设施(包括网络服务、通信和访问控制机制)是可用的，并允许授权用户获得授权的访问。

要在系统上维护可用性，必须有适当的控制措施以确保授权的访问和可接受的性能水平，能快速处理终端，能提供冗余，能维护可靠的备份，能防止数据丢失或受损。

有很多针对可用性的威胁。这些威胁包括设备故障、软件错误和环境问题(过热、静电、洪水、断电等)。还有一些聚焦于破坏可用性的攻击形式，包括DoS攻击、客体破坏和通信中断。

与保密性和完整性一样，对可用性的侵犯不仅限于蓄意攻击。许多未经授权修改敏感信息的实例都是由人为错误、疏忽或不称职造成的。导致可用性破坏的一些事件包括意外删除文件、滥用硬件或软件组件、资源分配不足、错误标记或错误的客体分类。

破坏可用性的原因可能是任意用户(包括管理员)的操作。安全策略中的疏漏或配置有误的安全控制也会破坏可用性。

大量控制措施可防御潜在的可用性威胁。这包括正确设计中转传递系统、有效使用访问控制、监控性能和网络流量、使用防火墙和路由器防止DoS攻击。对关键系统实施冗余机制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(BCP)关注不同级别的访问/存储/安全(即磁盘、服务器或站点)上的容错特性。目标是消除单点故障，保障关键系统的可用性。

可用性依赖于完整性和保密性。没有完整性和相互信任，就无法维持可用性。与可用性相关的其他一些相关概念、条件和特征如下。

- 可用性：能够容易被主体使用或学习的状态，或能被主体理解和控制。
- 可访问性：保证全部授权主体可与资源交互而不考虑主体的能力或限制。
- 及时性：及时、准时，在合理的时间内响应，或提供低时延的响应。



真实场景

CIA优先级排序

每个组织都有独特的安全需求。在CISSP考试中，大多数安全概念都用通用术语来说明，但在真实世界中，只有通用概念和最佳实践还不够。管理团队和安全团队必须协力确定组织安全需求的优先级别。这包括制定预算和支出计划，分配专业人员和工作时间，关注信息技术(IT)和安全人员的工作成果。这项工作中的一个关键任务是对组织的安全需求进行优先级排序。清楚在创建安全的环境及最后部署安全解决方案时哪个原则或资产更重要。通常，进行优先级排序是一个难题。解决这个难题的一个可行做法是首先确定保密性、完整性和可用性这三个主要安全原则的优先级。定义这些原则中的哪个对组织制定充分的安全解决方案是最重要的。这就建立了一个从概念到设计、架构、部署，最后到维护的可复用模式。

你知道CIA三元组中每个原则对组织的优先级别吗？如果不知道，那就去寻找答案。CIA三元组的优先级别中一个普遍存在的情况是军方和政府机构很多时候倾向于优先考虑保密性而不是完整性和可用性，而私营企业倾向于优先考虑可用性而不是保密性和完整性。尽管这些优先级别侧重于CIA三元组的某个原则，但这并不意味着会忽略或不恰当处理排在第二或第三优先级别的原则。OT(操作技术)系统的例子有PLC(可编程逻辑控制器)、SCADA(监控和数据采集)以及制造车间使用的MES(制造执行系统)设备和系统。将标准IT系统与OT系统进行比较时，发现了另一种观点。IT系统(甚至在私营企业)倾向于满足CIA三元组；而OT系统虽然倾向于满足CIA三元组，但其中可用性的优先级别最高，完整性又优先于保密性。再次强调，这只是一个概述，但它可能有助于你在CISSP考试中回答问题。每个独立组织都会决定自身的安全优先级别。

1.1.4 其他安全概念

除了 CIA 三元组外，在设计安全策略和部署安全解决方案时，还需要考虑其他许多与安全相关的概念和原则。

你也许听说过 AAA 服务的概念。这 3 个字母 A 分别代表身份验证(Authentication)、授权(Authorization)和记账(Accounting)；最后一个 A 有时也指审计(Auditing)。尽管缩写中只有三个字母，但实际上代表了五项内容：标识(Identification)、身份验证、授权、审计和记账，如图 1.2 所示。

这五项内容代表以下安全程序。

- 标识：当试图访问受保护的区域或系统时声明自己的身份。
- 身份验证：证实身份。
- 授权：对一个具体身份定义其对资源和客体的访问许可(如：允许/授予和/或拒绝)。
- 审计：记录与系统和主体相关的事件与活动日志。
- 记账(又名问责制)：通过审查日志文件来核查合规和违规情况，以便让主体对自身行为负责。

虽然经常讲 AAA 与身份验证系统关联在一起，但实际上，AAA 是一个安全基础概念。缺少这五个要素之一，安全机制就是不完整的。下面将分别讨论这五个要素。



图 1.2 AAA 服务的五个要素

1. 标识

标识是主体声明身份和责任的过程。主体必须为系统提供身份标识来启动身份验证、授权和记账过程。提供身份标识可能需要：输入用户名，刷卡，摇动一台近场通信设备，说出一个短语，或将你的脸、手掌或手指放入摄像机或扫描设备。提供流程 ID 号也是一种标识过程。如果没有身份标识，系统就无法将身份验证因素与主体相关联。

一旦主体被标识(即，一旦主体的身份被标识和验证)，该主体要对其接下来的所有行为负责。IT 系统通过身份标识来跟踪活动，而不是通过主体本身。计算机并不知道一个人与另一个人的区别，但它知道你的用户账户与其他所有用户账户是不同的。主体的身份通常被标记为或被认为是公开信息。然而，简单地声明身份并不意味着访问或授权。在允许访问受控资源(验证授权)之前，必须证明身份(验证)或验证身份(确保不可否认性)。这个过程就是身份验证。

2. 身份验证

验证或测试声明的身份是否有效的过程称为身份验证。身份验证要求主体提供与所要求的身份对应的附加信息。最常见的身份验证形式是使用密码(这包括个人身份识别码和密码短语)。

身份验证通过将一个或多个因子与有效的身份数据库(即用户账户)进行比较来验证主体的身份。用于身份验证的身份验证因子通常被标记为或被认为是私有信息。主体和系统对身份验证因子的保密能力直接反映了系统的安全性水平。如果非法获取和使用目标用户身份验证因子的过程比较容易，那身份验证系统就不安全。如果这个过程比较困难，那么身份验证系统是相当安全的。

通常在一个流程中完成标识和身份验证两个步骤。提供身份标识是第一步，提供身份验证因子是第二步。如果不能同时提供，主体就不能访问系统——就安全性而言，单独使用任一身份验证因子都不是有效的。在某些系统中，看起来好像只提供了一个身份验证因子，但也获得了访问权限，例如在输入 ID 代码或 PIN 时。其实在此类情况下，标识是通过另一种方式处理的，比如物理位置，或者以物理形式访问系统的能力。标识和身份验证都会进行，但你可能不会像手动输入用户名和密码时那样意识到它们的存在。

一个主体可提供多种类型的身份验证因子——例如，你知道的东西(如密码、PIN)、你拥有的东西(如密钥、令牌、智能卡)、你具备的东西(即生物特征识别，如指纹、虹膜或语音识别)等。每种身份验证技术或身份验证因子都有优缺点。因此，重要的是根据环境来评估每种身份验证机制的部署可行性。

3. 授权

一旦主体通过身份验证，就必须进行访问授权。授权过程确保对已通过验证的身份所请求的活动或对客体的访问是可以被赋予的权利和特权。大多数情况下，系统评估一个访问控制矩阵来对比主体、客体与预期的活动。如果特定行为是允许的，则对主体进行授权。如果特定行为不被允许，就不对主体进行授权。

请记住，仅因为主体已通过标识和身份验证过程，并不意味着主体已被授权执行任意功能或访问受控环境中的所有资源。主体或许可登录到网络(即经过标识和身份验证)，但会被禁止访问文件或将其打印(即未授权执行该活动)。大多数网络用户仅被授权对特定资源集执行有限的活动。

标识和身份验证体现了访问控制的全有或全无特性。对于环境中的每个主体，授权在全部允许或全部拒绝之间有广泛的变化。用户可读取文件但不能删除，可打印文档但不更改打印队列，或者可登录到系统但不访问任何资源。通常使用访问控制模型来定义授权，例如自主访问控制(Discretionary Access Control, DAC)、强制访问控制(Mandatory Access Control, MAC)或基于角色的访问控制(Role Based Access Control, RBAC 或角色 BAC)；详见第 14 章。

4. 审计

审计或监控是追踪和记录主体的操作，以便在验证过的系统中让主体为其行为负责的程序化过程。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。审计不仅记录主体及其客体的活动，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到日志中而创建的审计踪迹可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用于发现系统出现故障的原因。日志文件为重构事件、入侵或系统故障的历史记录提供了审计踪迹。

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置功能。因此，配置系统功能来记录特定类型事件的审计信息非常简单。

监控是审计的组成部分，而审计日志是监控系统的组成部分，但监控和审计这两个术语具有不同含义。监控是一种观测或监督，而审计是把信息记录到档案或文件。可在没有审计的情况下进行监控。不过如果没有某种形式的监控，则无法进行审计。虽然有此差异，但在不太严谨的讨论中，这两个术语常被互换使用。

5. 记账(或问责制)

组织的安全策略只有在有问责制的情况下才能得到适当实施。换句话说，只有在主体对他们的行为负责时，才能保持安全性。有效的问责制依赖于检验主体身份及追踪其活动的能力。通过安全服务和审计、身份验证、授权和身份标识等机制，将人员与在线身份的活动联系起来，进而建立问责制。因此，人员的问责制最终取决于身份验证过程的强度。如果没有强大的身份验证过程，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问责制，你可能需要能够在法庭上支持你的安全决策及实施。如果不能在法律上支持安全方面的努力，就不太可能让某人对与用户账户有关的行为负责。只使用密码进行身份验证，这显然值得怀疑。密码是最不安全的身份验证形式，有数十种不同类型的攻击可破坏这种身份验证形式。不过，使用多因素身份验证，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验证过程来假冒代表特定用户账户的人员。

法律上可防卫的安全

安全的要点是在防止坏事发生的同时支持好事的出现。坏事发生时，组织常希望借助法律实施和法律系统的援助来获得补偿。为获得法律赔偿，就必须证明存在犯罪行为或嫌疑人实施了犯罪，以及组织已尽力阻止罪行的发生，这意味着组织的安全需要是合法防御的。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，就无法获得赔偿。最终，这需要一个完整的安全解决方案，其中应当使用强大的多因素身份验证技术、可靠的授权机制和无可挑剔的审计系统。此外，还必须证明组织机构遵守了所有适用的法律和规则；发布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。这是一个相当有挑战性的标准。因此，一个组织应该对其安全基础设施进行评估，并再次考虑如何设计和实现合法防御的安全。

1.1.5 保护机制

理解和应用保密性、完整性和可用性概念的另一个方面是保护机制或保护控制。保护机制是安全控制的共同特征。并不是所有安全控制都必须具有这些机制，但许多保护控制通过使用这些机制提供了保密性、完整性和可用性。这些机制的常见示例包括使用多层或分层访问、利用抽象、隐藏数据和使用加密技术。

1.1.6 分层

分层(layering)也被称为纵深防御，指简单使用一系列控制中的多个控制。没有哪个控制能防范所有可能的威胁。使用多层防护解决方案允许使用许多不同的控制措施来抵御随时出现的威胁。在设计分层防护安全解决方案时，一个控制失效不会导致系统或数据暴露。

使用串行层而不是并行层是很重要的。在串行层中执行安全控制意味着以线性方式连续执行一个又一个控制。只有通过串行层的配置，安全控制才能扫描、评估或减轻每个攻击。在串行层的配置中，单个安全控制的失败并不会导致整个解决方案失效。如果安全控制是并行实现的，威胁就可通过一个没有处理其特定恶意活动的检查点而导致整个解决方案失效。

串行配置的范围很窄，但层级很深；而并行配置的范围很宽，但层级很浅。并行系统在分布式计算应用程序中很有用，但在安全领域中，平行机制往往不是一个有用的概念。

想想通向建筑物的物理入口。购物中心采用并行配置。商场周边的多个地方都有出入口。串行配置最可能用于银行或机场。这些地方只提供单一入口，这个入口实际上是为了进入建筑物活动区而必须按顺序通过的多个关口或检查点。

分层还包括网络由许多独立实体组成的概念，每个实体都有自己独特的安全控制和脆弱性。在有效的安全解决方案中，所有联网系统之间存在协同作用，从而构建了统一的安全防线。使用独立的安全系统可创建分层的安全解决方案。

1.1.7 抽象

抽象(abstraction)是为了提高效率。相似的元素被放入组、类或角色中作为一个集合被指派安全控制、限制或许可。因此，可将抽象的概念应用到对客体进行分类或向主体分配角色。抽象概念还包括对客体和主体类型的定义或客体自身的定义(即，用于定义实体类的模板的数据结构)。抽象用于定义客体可包含哪些类型的数据、可在该客体上或由该客体执行哪些类型的功能以及该客体具有哪些功能。抽象使你可将安全控制分配给按类型或功能归类的客体集，由此简化安全。

1.1.8 数据隐藏

顾名思义，数据隐藏是将数据存放在主体无法访问或读取的逻辑存储空间以防止数据被泄露或访问。数据隐藏的形式包括防止未经授权的访问者访问数据库，以及限制安全级别较低的主体访问安全级别较高的数据。阻止应用程序直接访问存储硬件也是一种数据隐藏形式。数据隐藏通常是安全控制和编程中的关键元素。

通过隐匿(obscurity)保持安全与数据隐藏是类似的，不过通过隐匿保持安全是另一种概念。数据隐藏是指故意将数据存放在未授权的主体无法查看或访问的位置，而通过隐匿保持安全是指不告知主体有客体存在，从而希望主体不发现该客体。通过隐匿保持安全实际上并没有提供任何形式的保护。它只是寄希望通过保持重要事物的保密性进而不让其泄露。通过隐匿保持安全的一个实例是：虽然程序员知道软件代码存在缺陷，但他们还是发布了产品，并希望没人会发现和利用代码中存在的缺陷。

1.1.9 加密

加密(encryption)是关于对非预期的接收者隐藏通信的真实含义和意图的艺术与科学，它能将信息传递的意义或意图隐藏起来。加密有多种形式并适用于各种类型的电子通信，包括文本、音频和视频文件及应用程序。加密是安全控制中的重要内容，特别在系统间传输数据时。有多种强度的加密技术，每种加密都被设计为适用于特定用途。较弱或较差的加密可被认为类似于隐匿或通过忽略保持安全。加密将在第 6 章和第 7 章中详细讨论。

1.2 评估和应用安全治理原则

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。安全治理原则通常与公司和 IT 治理密切相关，并常常交织在一起。这三类治理的工作目标一般是相同的或相互关联的。例如，组织治理的共同目标是确保组织能持续存在并随着时间不断成长或扩张。因此，治理的共同目标是维护业务流程，同时努力实现增长和弹性。

组织迫于法律和法规的要求必须实施治理，也被要求遵守行业指南或许可证要求。所有形式的治理(包括安全治理)都必须不时进行评估和验证。由于政府法规或行业最佳实践，可能存在各种审计和验证要求。通常不同的行业与国家面临的治理合规性问题也有所不同。随着多个组织的扩展和走向全球市场，治理问题变得更复杂。当不同国家的法律不一致或实际上存在冲突时，这个难题更难解决。组织作为一个整体应该具备方向、指导和工具以提供有效的监督和管理能力，解决威胁和风险；重点是缩短停机时间，并将潜在的损失或损害降至最低。

正如你看到的，安全治理通常是较严格和高层次的内容。最终，安全治理指实施安全解决方案以及与之紧密关联的管理方法。安全治理直接监督并涉及所有级别的安全。安全不完全是 IT 事务，也不应该仅被视为 IT 事务。相反，安全会影响组织的方方面面，不是仅靠 IT 人员自身能力就能处理好的事情。安全是业务运营事务，是组织流程，而不仅是 IT 极客在后台实施的事情。使用术语“安全治理”指出安全需要在整个组织中进行管理和治理，而不仅是在 IT 部门，就是为了强调这一点。

安全治理通常由治理委员会或至少由董事会管理。这是一群有影响力专家，他们的主要任务是监督和指导组织安全与运营行动。安全是一项复杂任务。组织通常是庞大的，并很难从单一角度去理解。为实现可靠的安全治理，让一组专家协同工作是一项可靠战略。

有许多安全框架和治理指南，包括 NIST 800-53 或 NIST 800-100。虽然 NIST 主要应用在政府和军事行业，但也能调整它，供其他类型的组织采用。许多组织采用安全框架，以标准化和有序方式组织那些复杂且混乱的活动，即努力实现可接受的安全治理。

1.2.1 与业务战略、目标、使命和宗旨相一致的安全功能

安全管理计划确保正确地创建、执行和实施安全策略。安全管理计划使安全功能与业务战略、目标、使命和宗旨相一致。这包括基于业务场景、预算限制或资源稀缺来设计和实现安全。业务场景通常是文档化的参数或声明的立场，用来定义作出决策或采取某类行为的需求。创建

新的业务场景是指：对于特定业务需求，要修改现有流程或选择完成业务任务的方法。业务场景常用来证明新项目的启动是合理的，特别是与安全相关的项目。考虑可分配给基于业务需求的安全项目的预算也很重要。安全可能很昂贵，但通常比没有安全的代价更低。因此，安全是可靠和长期经营的基本要素。在大多数组织中，资金和资源(如人员、技术和空间)都是有限的。由于这些资源的限制，任何努力都需要获得最大利益。

最能有效处理安全管理计划的一个方法是自上而下。上层、高级或管理部门负责启动和定义组织的策略。安全策略为组织架构内的各个级别提供指导。中层管理人员负责将安全策略落实到标准、基线、指导方针和程序。然后，操作管理人员或安全专业人员必须实现安全管理文档中规定的配置。最后，最终用户必须遵守组织的所有安全策略。

注意：



与自上而下方法相反的是自下而上方法。在采用自下而上方法的环境中，IT人员直接做出安全决策，而不需要高级管理人员的参与。组织中很少使用自下而上方法。

在IT行业中，该方法被认为是有问题的。

安全管理是上层管理人员的责任，而不是IT人员的责任，它也被认为是业务操作问题，而不是IT管理问题。在组织中负责安全的团队或部门应该是独立的。信息安全(InfoSec)团队应由指定的首席信息官(CISO)领导。CISO必须直接向高级管理层汇报。将CISO和CISO团队赋予组织典型架构之外的自主权可改进整个组织的安全管理。这还有助于避免跨部门和内部问题。首席安全官(CSO)有时等同于CISO，不过在很多组织中，CSO是CISO的下属职位，主要关注物理安全。另一个可能替代CISO的术语是信息安全官(ISO)，但ISO也可以是CISO下属职位。

安全管理计划的内容包括：定义安全角色，规定如何管理安全、由谁负责安全以及如何检验安全的有效性，制定安全策略，执行风险分析，要求对员工进行安全教育。这些工作都通过制定管理计划来完成。

如果没有高级管理人员批准这个关键过程，即使最好的安全计划也毫无用处。没有高级管理层的批准和承诺，安全策略就不会取得成功。策略开发团队的责任是充分培训高级管理人员，使其了解即使在部署了策略中规定的安全措施后仍然存在的风险和责任。制定和执行安全策略体现了高级管理人员的应尽关心(due care)与尽职审查(due diligence)。如果一家公司的管理层在安全方面没有给予应尽关心或没有实施尽职审查，管理者就要对疏忽负责，并应对资产和财务损失负责。

安全管理计划团队应该开发三种类型的计划，如图1.3所示。

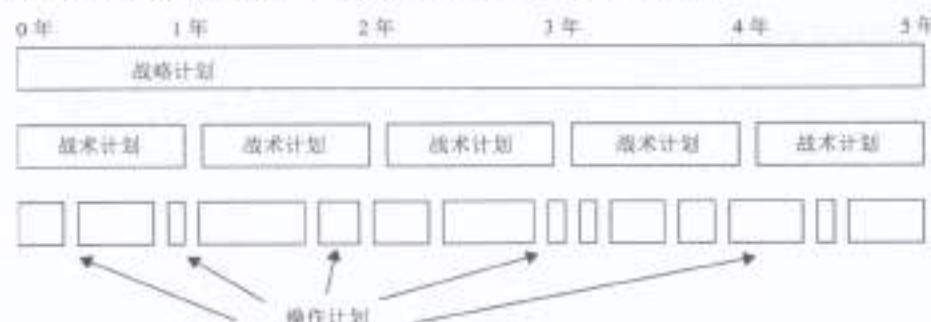


图1.3 战略计划、战术计划和操作计划的时间跨度比较

战略计划 战略计划(strategic plan)是一个相对稳定的长期计划。它定义了组织的安全目的，还有助于理解安全功能，并使其与组织的目标、使命和宗旨相一致。如果每年进行维护和更新，战略计划的有效期大约是5年。战略计划也可作为计划范围。战略计划中讨论了未来的长期目标和远景。战略计划还应包括风险评估。

战术计划 战术计划(tactical plan)是为实现战略计划中设定的目标提供更多细节而制定的中期计划，或可根据不可预测的事件临时制定。战术计划通常在一年左右的时间内有用，通常规定和安排实现组织目标所需的任务。战术计划的一些示例包括项目计划、收购计划、招聘计划、预算计划、维护计划、支持计划和系统开发计划。

操作计划 操作计划(operational plan)是在战略计划和战术计划的基础上，制定的短期、高度详细的计划。操作计划只在短时间内有效或有用。操作计划必须经常更新(如每月或每季)，以保持符合战术计划。操作计划阐明了如何实现组织的各种目标，包括资源分配、预算需求、人员分配、进度安排与细化或执行程序。操作计划包括如何符合组织安全策略的实施细节。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。

安全是一个持续的过程。因此，安全管理计划的活动可能有一个确定的起点，但它的任务和工作从来没有完成或实现过。有效的安全计划重点集中在具体和可实现的目标、预测变化和潜在问题上，并作为整个组织决策的基础。安全文档应该是具体的、定义完善的和明确说明的，为使安全计划有效，必须开发、维护和实际使用安全计划。

1.2.2 组织的流程

安全治理需要关注组织的方方面面，包括收购、剥离和治理委员会的流程。收购与兼并会增加组织的风险等级。这些风险包括不恰当的信息泄露、数据丢失、停机或未能获得足够的投资回报率(Return On Investment, ROI)。除了所有兼并与收购中的典型业务和财务方面外，对于降低在转型期间发生损失的可能性，良好的安全监督和加强的审查通常也是极其重要的。

同样，资产剥离或任何形式的资产减少或员工裁减都会增加风险，进而增加对集中安全治理的需求。需要对资产进行消磁以防止数据泄露。应该删除和销毁存储介质，因为介质净化处理技术不能保证残留数据不被恢复。需要对不再负责相关事宜的员工询问工作完成情况，该过程通常被称为离职面谈。这一过程通常包括审查所有保密协议及其他任何在雇佣关系终止后仍继续生效的约束合同或协议。

加强安全治理的另外两个组织流程示例是变更控制/变更管理和数据分类。

1. 变更控制/变更管理

变更控制或变更管理是安全管理的另一重要内容。安全环境的变更可能引入漏洞、重叠、客体丢失和疏忽进而导致出现新脆弱性。面对变更，维护安全的唯一途径就是系统性的变更管理。这通常涉及与安全控制和安全机制相关的活动，包括广泛的计划、测试、日志记录、审计和监控。然后对环境变化进行记录来识别变更发起者，无论变更发起者是客体、主体、程序、通信路径还是网络本身。

变更管理的目标是确保变更不会消减或损坏安全。变更管理还负责让变更能回滚到变更前的安全状态。变更管理可在任意系统上实现而不考虑安全级别。最终，变更管理通过保护已实现的安全，使安全不受无意的、间接的或负面的影响。从而提升环境的安全性。尽管变更管理

的重要目标是防止非预期的安全降低。但它的首要目标是使所有变更被详细记录和审计，从而使变更能被管理层检查和审核。

变更管理应该用于监督系统的所有变更，包括硬件配置和操作系统(OS)以及应用软件。应该在设计、开发、测试、评估、实现、分发、演进、发展、持续操作和修改中都进行变更管理。变更管理需要每个组件和配置的详细清单。它还需要收集和维护每个系统组件(包括硬件、软件)的全部文档，从配置到安全特性。

配置管理或变更管理的变更控制过程有以下几个目标或要求：

- 在受监控的环境中有序实施更改。
- 包含正式的测试过程，验证变更能实现预期效果。
- 所有变更都能够撤消(也称为回退或回滚计划/程序)。
- 在变更实施前通知用户，以防止影响生产效率。
- 对变更影响进行系统性分析，以确定变更是否会对安全或业务流程产生负面影响。
- 最小化变更对能力、功能和性能方面的负面影响。
- 变更顾问委员会(Change Advisory Board, CAB)需要评审和批准变更。

变更管理过程的一个示例是并行运行，在这种新的系统部署测试中，新系统和旧系统并行运行。在新旧系统中同时执行所有主要的或重要的用户流程，以确保新系统能支持旧系统提供的所有业务功能。

2. 数据分类

数据分类(data classification，也称数据分级)是基于数据的保密性、敏感性或秘密性需求而对其进行保护的主要手段。在设计和实现安全系统时，以相同方式处理所有数据是低效的，因为有些数据项比其他数据项需要更多安全性。用低级别安全保护所有内容意味着敏感数据很容易被访问。用高级别安全保护所有内容又过于昂贵，并且限制了对未分类的、非关键数据的访问。数据分类用于确定为保护数据和控制对数据的访问而分配多少精力、金钱和资源。数据分类或分级是将条目、主体、客体等组织成具有相似性的组、类别或集合的过程。这些相似性可能是价值、成本、敏感性、风险、脆弱性、权利、特权、可能的损失程度或“知其所需”。

数据分类方案的主要目标是基于指定的重要性与敏感性标签，对数据进行正式化和分层化的安全防护过程。数据分类为数据存储、处理和传输提供安全机制，还确定了该如何从系统中删除和销毁数据。

以下是使用数据分类方案的好处：

- 数据分类证实了组织对有价值的资源和资产的保护承诺。
- 数据分类帮助组织确定最重要的或最有价值的资产。
- 数据分类给保护机制的选择提供了凭据。
- 数据分类通常是法规或法律限制的要求。
- 数据分类有助于定义访问级别、使用的授权类型，以及定义不再具有价值的资源的销毁和/或降级的参数。
- 数据分类有助于在数据的生命周期管理中确定数据存储时间(保留时间)，并确定数据使用和数据销毁方式。

数据分类标准因实施数据分类的组织而异。不过，可从通用的或标准化的分类系统总结出很多通用特征：

- 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
- 数据的生命周期(或何时过期)
- 与人员的关联
- 数据泄露损失评估(即数据泄露将如何影响组织)
- 数据修改损失评估(即数据修改将如何影响组织)
- 数据对国家安全的影响
- 对数据的已授权访问(即谁有权访问数据)
- 对数据的访问限制(即谁对数据的访问受到限制)
- 维护和监测数据(即谁应该维护和监控数据)
- 数据存储

使用任何适合组织的数据分类标准，都要对数据进行评估，并为其分配适当的数据分类标签。某些情况下，数据分类标签会被添加到数据对象中。在其他情况下，在数据存储或对数据实施安全保护机制后，会自动进行数据分类标记。

要实现数据分类方案，必须执行七个主要的步骤或阶段：

- (1) 确定管理人员，并定义其职责。
- (2) 指定信息如何分类和标记的评估标准。
- (3) 对每个资源进行数据分类和增加标签(数据所有者会执行此步骤，监督者应予以审核)。
- (4) 记录数据分类策略中发现的任何异常，并集成到评估标准中。
- (5) 选择将应用于每个分类级别的安全控制措施，以提供必要的保护级别。
- (6) 指定解除资源分类的流程，以及将资源保管权转移给外部实体的流程。
- (7) 建立组织范围的培训程序来指导所有人员使用分类系统。

解除分类常在设计分类系统和编写使用程序时被忽略。一旦资产不再被授权保护其当前指定的分类或敏感级别，就需要解除分类。换句话说，如果新增资产，它将被分配一个比当前指定的敏感级别更低的标签。如果资产未按照需要解除分类，安全资源会被浪费。

两种常用的数据分类方案是政府/军事分类(图 1.4)和商业/私营部门分类。政府/军事分类方案分为五个分类级别。



图 1.4 政府/军事分类方案

绝密(Top Secret) 绝密是最高级别的分类。未经授权泄露绝密数据，将对国家安全造成严重影响和严重损害。最高机密数据是基于“知其所需”划分的，这样用户就可以拥有最高机

密权限，并在“知其所需”前不访问任何数据。

秘密(Secret) 秘密用于描述具备限制性质的数据。未经授权泄露被列为秘密的数据，将对国家安全造成重大影响和重大损害。

机密(Confidential) 机密用于敏感的、专有的或高度有价值的数据。未经授权泄露机密信息，将对国家安全造成明显的影响和严重损害。这个级别适用于“秘密”和“敏感但非分类”之间的所有数据。

敏感但未分类 敏感但未分类(Sensitive But Unclassified, SBU)用于内部使用或仅用于办公室使用(For Office Use Only, FOUO)的数据。SBU 常用来保护可能侵犯个人隐私权的信息。这不是严格意义上的分类标签，而是表示使用或管理的标记或标签。

未分类 未分类(Unclassified)描述既不敏感也不需要分级的数据。泄露未分类数据不会损害保密性或造成任何明显的损害。这不是严格意义上的分类标签，而是表示使用或管理的标记或标签。



提示：

采用首字母记忆法按从最低安全到最高安全的顺序可轻易记住政府/军事分类方案中的 5 个名称：美国可停止恐怖主义(U.S. Can Stop Terrorism)。请注意，五个大写字母分别代表五个分类级别，从左边的最低安全级别到右边的最高安全级别(或按图 1.4 中自下向上的顺序)。

带有秘密、机密和绝密的标签统称为分类的级别。通常，向未经授权的个人透露数据的分类级别是一种侵犯行为。因此，术语“分类”通常指分类的级别在非分类级别之上的全部数据。所有分类的数据都不受《信息自由法案》以及许多其他法律法规的约束。美国军事分类方案最关心数据的敏感性，重点是保密性(即防止泄露)。可根据危害保密性事件发生时造成损害的严重程度粗略定义每个分类级别或分类标签。绝密数据将对国家安全造成严重损害，未分类数据不会对国家或地方安全造成任何严重损害。

商业公司和私营机构的分类系统差别很大，因为一般来说他们不需要遵守相同的标准或规定。CISSP 考试侧重于四个常见的或可能的商业分类级别，如图 1.5 所示。



图 1.5 商业/私营部门分类方案

机密(Confidential) 机密是最高级别的分类。用于极度敏感的和只在内部使用的数据。如果机密数据被泄露，将对公司产生重大的负面影响。有时会用专有(proprietary)代替机密标签。有时专有数据被认为是一种特定形式的机密信息。如果泄露了专有数据，会给组织的竞争优势

带来极大的负面影响。

私有(Private) 私有指私有的或个人特有的及仅供内部使用的数据。如果公司或个人的私有数据被泄露，将产生重大的负面影响。



注意:

商业/私营部门分类方案中，对机密数据和私有数据的安全保护大致上都是相同的级别。这两个标签的真正区别在于，机密数据是公司数据，而私有数据是与个人相关的数据，如医疗数据。

敏感(Sensitive) 敏感用于比公开数据分类级别更高的数据。如果敏感数据被泄露，会给公司带来负面影响。

公开(Public) 公开是分类级别的最低层级。用于所有不适合较高分类级别的数据。泄露公开数据不会给组织带来严重的负面影响。

与数据分类或分级相关的另一相关因素是所有权。所有权将职责正式分配到个人或团体。文件或其他类型的客体可被指定所有者，这清晰而明确地体现了操作系统中的所有权。通常，所有者对其拥有的客体具有全部功能和权限。一般将所有权授予操作系统中最强大的账户，如 Windows 中的管理员账户、UNIX 中的 root 账户或 Linux 中的 root 账户。大多数情况下，创建新客体的主体默认为该客体的所有者。在某些环境中，安全策略要求在创建新客体时，必须将所有权从最终用户正式更改为管理员或管理用户。这种情况下，管理员账户可简单地获得新客体的所有权。

在正规的 IT 架构之外，客体的所有权通常不那么明显。在公司文档中可为设施、业务任务、流程、资产等定义所有者。不过，这样的文档在现实世界中并不总能“实现”所有权。文件客体的所有权由操作系统和文件系统强制执行，而物理客体、无形资产或组织概念(如研究部门或开发项目)的所有权仅在文档中定义，所以很容易遭到破坏。必须对现实世界中的所有权实施其他安全治理。

1.2.3 组织的角色与责任

安全角色是个人在组织内安全实施和管理总体方案中扮演的角色。安全角色不是固定或静止的，所以并不需要预先在工作内容中说明。熟悉安全角色对在组织内建立通信和支持结构是很有帮助的。这种结构能够支持安全策略的部署和执行。根据在安全环境中出现的逻辑顺序介绍如下六个角色。

高级管理者 组织所有者(高级管理者)角色被分配给最终对组织安全的维护负责及最关心资产保护的人员。高级管理者必须在所有策略问题上签字。事实上，执行所有活动前都必须经过高级管理者的认可和批准。如果缺少高级管理者的授权和支持，就没有有效的安全策略。高级管理者对安全策略的认可表明组织内已实现的、安全的可接受所有权。高级管理者将对安全解决方案的总体成功或失败负责，并负责在为组织建立安全方面给予应尽关心和实施尽职审查。

尽管高级管理者最终负责安全，但他们很少直接实施安全解决方案。大多数情况下，这种责任被分配给组织内的安全专业人员。

安全专业人员 安全专业人员角色或计算机事件响应小组(Incident Response Team, IRT)角色被分配给受过培训和经验丰富的网络、系统和安全工程师们，他们负责落实高级管理者下达

的指示。安全专业人员的职责是保证安全性，包括编写和执行安全策略。安全专业人员可被称为 IS/IT 功能角色。安全专业人员角色通常由一支团队完成，该团队负责根据已批准的安全策略设计和实现安全解决方案。安全专业人员不是决策者，而是实施者。所有决策都必须由高级管理者决定。

数据所有者 数据所有者(data owner)角色将被分配给在安全解决方案中负责布置和保护信息分类的人员。数据所有者通常是高级管理人员，他们最终对数据保护负责。然而，数据所有者通常将实际数据管理任务的责任委托给数据托管员。

数据托管员 数据托管员(data custodian)角色被分配给负责执行安全策略与高级管理者规定的保护任务的人员。数据托管员执行所有必要的活动，为实现数据的 CIA 三元组(保密性、完整性和可用性)提供充分的数据支持，并履行上级管理部门委派的要求和职责。这些活动包括执行和测试备份、验证数据完整性、部署安全解决方案以及基于分类管理数据存储。

用户 用户(最终用户或操作者)角色被分配给任何能访问安全系统的人员。用户的访问权限与他们的工作任务相关并受限，因此他们只有足够的访问权限来执行工作岗位所需的任务(最小特权原则)。用户有责任通过遵守规定的操作程序和在规定的安全参数内进行操作来理解和维护组织的安全策略。

审计人员 审计人员(auditor)负责审查和验证安全策略是否正确执行，以及相关的安全解决方案是否完备。审计人员角色可分配给安全专业人员或受过培训的用户。审计人员出具由高级管理者审核的审计报告。高级管理者将在这些报告中发现的问题作为新的工作内容分配给安全专业人员或数据托管员。不过，因为审计人员需要对活动发起者(即在环境中工作的用户或操作人员)进行审计或监控，所以审计人员被列为最后一个角色。

所有这些角色都在安全环境中发挥着重要作用。这些角色有助于确定义务和责任以及确定分级管理和授权方案。

1.2.4 安全控制框架

为组织制定安全声明通常涉及很多事项，并非只是写下几条远大理想。多数情况下，需要很多规划才能制定出可靠的安全策略。许多读者可能认为召开会议为未来的会议制定计划是一种荒谬的做法。但实际上，安全规划必须首先制定计划，然后规划标准和合规，最后实际开发和设计计划。跳过这些“规划-计划”步骤中的任何一个，都可能在组织的安全解决方案实施之前就破坏它。

安全规划步骤中的第一步最重要，就是考虑组织所希望的安全解决方案的总体安全控制框架或结构。可从几个相关的安全控制框架中进行选择，不过被应用广泛的安全控制框架之一是信息和相关技术控制目标(COBIT)。COBIT 是由信息系统审计和控制协会(ISACA)编制的一套记录最佳 IT 安全实践的文档。它规定了安全控制的目标和需求，并鼓励将 IT 安全思路映射到业务目标。COBIT 5 的基础是企业 IT 治理和管理的如下五个关键原则。

- 原则 1：满足利益相关方的需求
- 原则 2：从端到端覆盖整个企业
- 原则 3：使用单一的集成框架
- 原则 4：采用整体分析法
- 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，还可作为审计人员的工作指南。COBIT 是一个得到广泛认可与重视的安全控制框架。

幸运的是，在考试中只引用了 COBIT 的大体内容，不需要了解进一步的细节。不过如果你对这个概念感兴趣，请访问 ISACA 网站(www.isaca.org)；或者如果需要总体概述，请阅读 Wikipedia 上的 COBIT 条目。

IT 安全还有其他许多标准和指南，包括：

- **开源安全测试方法手册(Open Source Security Testing Methodology Manual, OSSTMM)** 安全基础设施测试和分析的同行评议指南，参见 www.isecom.org/research/。
- **ISO/IEC 27002(取代了 ISO 17799)** 一个国际标准，可作为实施组织信息安全及相关管理实践的基础，参见 www.iso.org/standard/54533.html。
- **信息技术基础设施库(Information Technology Infrastructure Library, ITIL)** ITIL 最初由英国政府精心设计，它是一套推荐的核心 IT 安全和操作流程的最佳实践，经常用作定制 IT 安全解决方案的起点。

1.2.5 应尽关心和尽职审查

为什么计划安全如此重要？原因之一是需要应尽关心(due care)和尽职审查(due diligence)。“应尽关心”指使用合理的关注来保护组织的利益，“尽职审查”指的是具体的实践活动。对于考试，应尽关心是指制定一种正式的安全框架，包含安全策略、标准、基线、指南和程序。尽职审查是指将这种安全框架持续应用到组织的 IT 基础设施上，操作性安全指组织内的所有责任相关方持续给予应尽关心和实施尽职审查。

在当今的商业环境中，谨慎是必需的。在安全事故发生时，拿出应尽关心和尽职审查的证据是证明没有疏忽的唯一方法。高级管理人员必须在安全事故发生时出示应尽关心和尽职审查的记录以减少对他们的处罚和承担的罪责。

1.3 开发、记录和实施安全策略、标准、程序和指南

对大多数组织来说，维护安全是业务发展的重要内容。如果安全受到严重破坏，许多组织都将无法正常运转。为降低安全故障出现的可能性，实施安全的流程在某种程度上就是按照组织架构确定的文档。每个级别都聚焦于信息和问题的一个特定类别。开发和实现文档化的安全策略、标准、程序和指南可以生成可靠的、可依赖的安全基础设施。这种规范化过程极大地减少了 IT 基础设施设计和实现的安全解决方案中的混乱和复杂性。

1.3.1 安全策略

规范化的最高层级文件是安全策略。安全策略定义了组织所需的安全范围，讨论需要保护的资产以及安全解决方案需要提供的必要保护程度。安全策略是对组织安全需求的概述或归纳，它定义了主要的安全目标，并概述了组织的安全框架。安全策略还确定了数据处理的主要功能

领域，并澄清和定义了所有相关术语。安全策略应该清楚地定义为什么安全性是重要的，以及哪些资产是有价值的。安全策略是安全实施的战略计划。安全策略应概述为保护组织利益而应采取的安全目标和做法。安全策略讨论了安全对日常业务运营的各个方面的重要性，以及高级管理者支持安全实施的重要性。安全策略用于分配职责、定义角色、指定审计需求、概述实施过程、确定合规性需求和定义可接受的风险级别。安全策略常用来证明高级管理者在保护组织免受入侵、攻击和灾难时已经给予了应尽关心。安全策略是强制性的。

很多组织使用多种类型的安全策略来定义或概述其总体安全策略。组织安全策略重点关注与整个组织相关的问题。特定问题的安全策略集中在特定的网络工作服务、部门、功能或有别于组织整体的其他不同方面。特定系统的安全策略关注于单个系统或系统类型，并规定了经过批准的硬件和软件。概述了锁定系统的方法，甚至强制要求采用防火墙或其他特定的安全控制。

除了这些针对特定类型的安全策略外，还有三大类综合的安全策略：监管性策略、建议性策略和信息性策略。当组织有需要遵守的行业或法律标准时，就需要监管性策略。该策略讨论了必须遵守的法规，并概述了用于促进满足监管要求的程序。建议性策略讨论可接受的行为和活动，并定义违规的后果。它说明了高级管理者对组织内安全性和合规性的期望，大多数策略都是建议性的。信息性策略旨在提供关于特定主体的信息或知识，如公司目标、任务声明或组织如何与合作伙伴和客户交流。信息性策略提供与整体策略特定要素相关的支持、研究或背景信息。

从安全策略可引出完整安全解决方案所需的其他很多文档或子元素。策略是宽泛的概述，而标准、基线、指南和程序包括关于实际安全解决方案的更具体、更详细的信息。标准是安全策略的下一级别。

安全策略与人员

作为一条经验法则，安全策略（以及标准、程序和指南）不应该针对特定的个人。安全策略应该为特定角色定义任务和职责，而不是为某个人定义任务和职责。这种角色可具备行政控制或人事管理职能。因此，安全策略不是定义谁要做什么，而是定义在安全基础结构内的各个角色必须做什么。然后将这些定义好的安全角色作为工作描述或工作任务分配给个人。

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，它是整个安全文档基础结构的一个组成部分。可接受的使用策略专门用来分配组织内的安全角色，并确保职责与这些角色相关联。该策略定义了可接受的性能级别及期望的行为和活动。不遵守该策略可能导致工作行为警告、处罚或解聘。

1.3.2 标准、基线和指南

一旦完成主要的安全策略，就可在这些策略的指导下编制其他安全文档。标准对硬件、软件、技术和安全控制方法的一致性定义了强制性要求。标准提供了在整个组织中统一实施技术和程序的操作过程。标准是战术计划文档，规定了达到安全策略定义的目标和总体方向的步骤或方法。

下一层级是基线。基线定义了整个组织中每个系统必须满足的最低安全级别。所有不符合

基线要求的系统在满足基线要求之前都不能上线生产。基线建立了通用的基础安全状态，在此之上可实施所有额外的、更严格的安全措施。基线通常是系统特定的，一般参考行业或政府标准，如 TCSEC(可信计算机系统评估标准)或 ITSEC(信息技术安全评估和标准)或 NIST(美国国家标准与技术研究院)标准。

指南是规范化安全策略结构中基线的下一个元素。指南提供了关于如何实现标准和基线的建议，并作为安全专业人员和用户的操作指南。指南具有灵活性，所以可针对每个特定的系统或条件分别制定指南，并可在新程序的创建中使用指南。指南说明应该部署哪些安全机制，而不是规定特定的产品或控制措施，并详细说明配置。指南概述了方法(包括建议的行动)，但并非强制性的。

1.3.3 程序

程序是规范化安全策略结构的最后一个元素。标准操作程序(Standard Operating Procedure, SOP)是详细的分步实施文档，描述了实现特定安全机制、控制或解决方案所需的具体操作。程序可讨论整个系统部署操作，或关注单个产品或方面，如部署防火墙或更新病毒定义。大多数情况下，程序是针对特定系统和软件的。程序必须随着系统硬件与软件的发展而不断更新。程序的目的是确保业务流程的完整性。如果一切都是通过遵循详细的程序来完成的，那么所有活动都应该遵守策略、标准和指南。程序有助于在所有系统之间确保安全的标准化。

通常，安全策略、标准、基线、指南和程序的制定只是在顾问或审计人员的敦促下才会加以考虑。如果这些文档没有被使用和更新，安全环境的管理将无法把它们当成指南使用。如果没有这些文件提供的规划、设计、结构和监督，就无法维护环境的安全，也无法表示已经尽责地给予了应尽关心。

制定一个包含上述所有元素内容的文档也是常见的做法。不过应该避免这种做法。这些结构中的每个都必须作为独立实体存在，因为每个结构都实现了不同的特殊功能。在规范化安全策略文档结构中，顶层的文档较少，因为它们一般是对观点和目标的广泛讨论。在规范化安全策略文档结构的下层有很多文档(即指南和程序)，因为它们包含了数量有限的系统、网络、部门和区域的特定详细信息。

将这些文档作为独立实体保存有几个好处：

- 并非所有用户都需要知道所有安全分类级别的安全标准、基线、指南和程序。
- 当发生更改时，可以较方便地只更新和重新分发受影响的策略，而不是更新全部策略并在整个组织中重新分发。

制定整个安全策略和所有支持文档是一项艰巨任务。许多组织只是致力于定义基本的安全参数，对日常活动每个方面的详细描述较少。然而在理论上，详细和完整的安全策略能以针对性的、高效的和特定的方式支持现实世界的安全。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、响应问题以及预测未来的发展趋势。安全策略不应该是一种事后的想法，而应是组织建立中的关键部分。

对于包含完整安全策略的文档的理解还有其他一些看法。图 1.6 显示了这些组件的依赖性：策略、标准、指南和程序。安全策略定义组织安全文档的总体结构。然后，标准是基于策略及法规和合同的约束。从中推演得到指南。最后，程序基于其他三个组件。使用金字塔可以传达每种文档的大小。完整安全策略中的程序通常远远超过任何单个元素的程序。相比之下，指南

比程序少，标准也比程序少，整体或组织范围内的安全策略通常更比程序少。



1.4 理解与应用威胁建模的概念和方法

威胁建模是识别、分类和分析潜在威胁的安全过程。威胁建模可当作设计和开发期间的一种主动措施被执行，也可作为产品部署后的一种被动措施被执行。这两种情况下，威胁建模过程都识别了潜在危害、发生的可能性、关注的优先级以及消除或减少威胁的手段。本节将介绍威胁建模概念的多个应用实例以及几种威胁建模方法。

威胁建模不是一个独立事件。组织通常在进行系统设计过程早期就开始进行威胁建模，并持续贯穿于系统整个生命周期中。例如，微软使用安全开发生命周期(SDL)过程在产品开发的每个阶段考虑和实现安全。这种做法支持“设计安全，默认安全，部署和通信安全”(也称为SD3+C)的座右铭。这一过程有两个目标：

- 降低与安全相关设计和编码的缺陷数量。
- 降低剩余缺陷的严重程度。

换句话说，尽力减少脆弱性与降低任何现存脆弱性的影响。总体结果也就降低了风险。

主动式威胁建模发生在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法。这种方法基于在编码和制作过程中预测威胁和设计特定防御，而不是依赖于部署后更新和打补丁。大多数情况下，集成的安全解决方案成本效益更高，比后期追加的解决方案更有效。遗憾的是，并非所有威胁都能在设计阶段被预测到，所以仍然需要被动式威胁建模来解决不可预见的问题。

被动式威胁建模发生在产品创建与部署后。这种部署可在测试或实验室环境中进行，或在通用市场中进行。此类威胁建模也称为对抗性方法。这种威胁建模技术是道德黑客、渗透测试、源代码审查和模糊测试背后的核心概念。尽管这些过程在发现需要解决的缺陷和威胁方面通常很有用，但遗憾的是，它们导致需要在编码中添加新对策的工作。从长远看，回到设计阶段可能生产出更好的产品，但从头开始会耗费大量时间，并导致产品发布时间的延迟。因此，最简单的方法是在部署后向产品中增加更新或补丁。但这样做的结果是在可能降低功能和用户友好的前提下，并没有带来更有效的安全改进(过度主动的威胁建模)。

**注意:**

模糊(Fuzz)测试是一种专用的动态测试技术，它向软件提供许多不同类型的输入，以强调其局限性并发现以前未发现的缺陷。模糊测试软件向软件提供无效的输入。这些输入可以是随机生成的，也可以是专门为触发已知的软件漏洞而设计的。然后，模糊测试人员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期望的和/或不可预测的结果。有关模糊测试的更多信息，请参阅第 15 章。

1.4.1 识别威胁

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

关注资产 该方法以资产为中心，利用资产评估结果，试图识别对有价值资产的威胁。例如，可对特定资产进行评估，以确定它是否容易受到攻击。如果资产中承载数据，则可通过评估访问控制来识别能绕过身份验证或授权机制的威胁。

关注攻击者 有些组织能识别潜在攻击者，并能根据攻击者的目标识别代表的威胁。例如，政府通常能识别潜在的攻击者以及攻击者想要达到的目标。然后，可利用这些数据来识别和保护相关资产。这种方法面临的一个挑战是，可能会出现之前未视为威胁的新攻击者。

关注软件 如果组织开发了软件，就需要考虑针对软件的潜在威胁。虽然前几年组织一般不自己开发软件，但现今这样做已经非常普遍。具体来说，大多数组织都存在 Web 应用，许多组织都创建自己的 Web 页面。精美的网页会带来更多流量，但也需要更复杂的编程，并会带来更多威胁。

如果威胁被确定为攻击者(而不是自然威胁)，威胁建模将尝试识别攻击者可能想要达到的目标。有些攻击者可能想要禁用系统，而其他攻击者可能想要窃取数据。一旦这些威胁被识别出来，就可根据目标或动机进行分类。此外，通常将威胁与脆弱性结合起来，以识别能够利用脆弱性并对组织带来重大风险的威胁。威胁建模的最终目标是对危害组织有价值资产的潜在威胁进行优先级排序。

当尝试对威胁进行盘点和分类时，使用指南或参考通常很有帮助。微软开发了一种被称为 STRIDE 的威胁分类方案。STRIDE 通常用于评估对应用程序或操作系统的威胁。但是，它也可以在其他情况下应用。STRIDE 是以下单词的首字母缩写。

- **欺骗(Spoofing):** 通过使用伪造的身份获得对目标系统访问权限的攻击行为。欺骗可用于 IP 地址、MAC 地址、用户名、系统名、无线网络服务集标识符(SSID)、电子邮件地址和其他许多类型的逻辑标识。当攻击者将他们的身份伪造成合法的或授权的实体时，他们通常能够绕过针对未经授权的过滤器和封锁。一旦攻击者利用欺骗攻击成功获得对目标系统的访问权，就可以在随后发起攻击，包括滥用、数据窃取或权限升级。
- **篡改(Tampering):** 对传输或存储中的数据进行任何未经授权的更改或操纵。篡改被用来伪造通信或改变静态信息。这种攻击破坏了完整性和可用性。

- **否认(Repudiation):** 用户或攻击者否认执行动作或活动的能力。通常，攻击者会否认攻击以保持合理的辩解，从而不对自己的行为负责。否认攻击还可能导致无辜的第三方因安全违规而受到指责。
- **信息泄露(Information Disclosure):** 将私有、机密或受控信息泄露或发送给外部或未经授权的实体。这些信息可能包括客户身份信息、财务信息或专有业务操作细节。信息泄露可利用系统设计和实现上的错误，如未删除的调试代码，遗留的示例应用程序和账户，未删除客户端可见内容的编程注释(如 HTML 文档中的注释)或将过于详细的错误信息展示给用户。
- **拒绝服务(DoS):** 该攻击试图阻止对资源的授权使用。这类攻击可通过利用缺陷、过载连接或爆发流量来进行。DoS 攻击不一定导致资源完全无法访问，而是会减低吞吐量或提高延迟，阻碍对资源的有效使用。虽然大多数 DoS 攻击带来的危害是临时性的，只有在攻击者实施攻击时存在，但也有一些 DoS 攻击带来的危害是长久性的。长久性 DoS 攻击可能包括对数据集的破坏，用恶意软件替换原有软件，或劫持可能被中断的固件闪存操作或安装有问题的固件。这些 DoS 攻击中的任何一种都会导致系统永久受损，无法通过简单的重启或通过等待攻击者结束攻击而恢复到正常操作。要从永久性 DoS 攻击中恢复，需要完整的系统修复和备份恢复。
- **特权提升(Elevation of Privilege):** 该攻击是将权限有限的用户账户转换为具有更大特权、权利和访问权限的账户。这类攻击可能通过窃取或利用高级账户的凭据来实现，例如管理员(administrator)或根用户(root)。特权提升攻击也包括攻击系统或应用程序，使权限有限的其他账户临时或永久地获得额外权限。

虽然 STRIDE 通常针对应用程序威胁，但也适用于其他情况，比如网络威胁和主机威胁。其他攻击可能比网络攻击和主机攻击更特别，例如嗅探和劫持网络、恶意软件以及主机的任意代码执行，不过 STRIDE 的六个威胁概念有相当广泛的应用。

攻击模拟和威胁分析(Process for Attack Simulation and Threat Analysis, PASTA)过程是一种由七个阶段构成(见图 1.7)的威胁建模方法。PASTA 方法是以风险为核心，旨在选择或开发与要保护的资产价值相关的防护措施。PASTA 的七个阶段如下。

- 阶段 1：为风险分析定义目标
- 阶段 2：定义技术范围(Definition of the Technical Scope, DTS)
- 阶段 3：分解和分析应用程序(Application Decomposition and Analysis, ADA)
- 阶段 4：威胁分析(Threat Analysis, TA)
- 阶段 5：弱点和脆弱性分析(Weakness and Vulnerability Analysis, WVA)
- 阶段 6：攻击建模与仿真(Attack Modeling & Simulation, AMS)
- 阶段 7：风险分析和管理(Risk Analysis & Management, RAM)

PASTA 的每个阶段都有该阶段需要完成的目标和交付物的特别目标清单。有关 PASTA 的更多信息，请参阅 Tony UcedaVelez 和 Marco M. Moruna 撰写的书籍《以风险为中心的威胁建模：攻击模拟和威胁分析的过程》。你可在线阅读该书附录，可在 <http://www.isaca.org/chapters5/Ireland/Documents/2013%20Presentations/PASTA%20Methodology%20Appendix%20-%20November%202013.pdf> 上找到对 PASTA 的介绍。

Trike 是另一种基于风险的威胁建模方法，侧重于基于风险，而不是依赖于 STRIDE 和 DREAD(Disaster, Reproducibility, Exploitability, Affected Users and Discoverability，潜在破坏、可

再现性、可利用性、受影响用户和可发现性)中使用的聚合威胁模型。有关 DREAD 的讨论, 见后面的“优先级排序和响应”一节)。Trike 提供了一种可靠的、可重复的安全审核方法。它还为安全工作人员之间的通信和协作提供了一致的框架。Trike 对每种资产的可接受风险水平进行评估, 然后确定适当的风险响应行动。

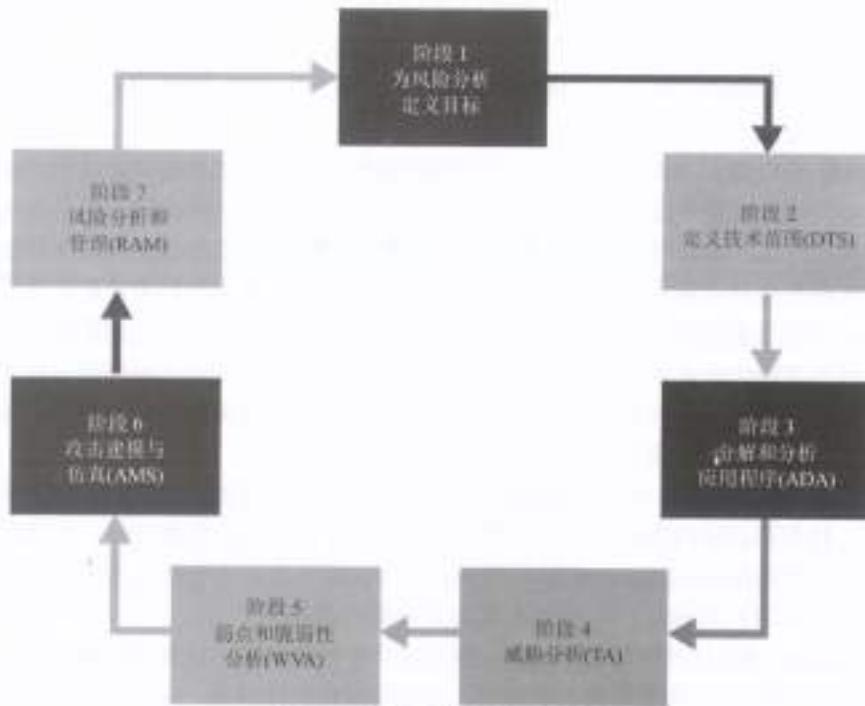


图 1.7 揭露威胁问题的图表示例

VAST(Visual, Agile, and Simple Threat, 视觉、敏捷和简单威胁)是一种基于敏捷项目管理和编程原则的威胁建模概念。VAST 的目标是在可伸缩的基础上将威胁和风险管理集成到敏捷编程环境中。

上述这些只是由社区团体、商业组织、政府机构和国际协会提供的多种威胁建模概念和方法中的一小部分。

通常 STRIDE 和其他威胁建模方法的目的是考虑危害问题的范围, 并关注攻击的目标或最终结果。尝试识别出每一种特定的攻击方法和技术是不可能完成的任务——因为新攻击不断出现。虽然仅能对攻击的目标或目的进行粗略分类和分组, 但分类和分组保持相对稳定。

警惕个人威胁

竞争通常是企业成长的一个关键因素, 但过度竞争会增加来自个人的威胁程度。除了恶意黑客和心怀不满的雇员, 对手、承包商、员工甚至是值得信赖的合作伙伴都可能因为关系恶化而成为组织的威胁。

- 永远不要认为顾问或承包商对公司的忠诚度与长期员工一样高。承包商和顾问实际上就是雇佣兵, 他们只为出价最高的人工作。也不要把员工的忠诚看成理所应当。如果对工作环境不满或觉得受到不公正待遇, 员工可能试图进行报复。经济困难的雇员可能为自身利益考虑进行不道德和非法的活动, 从而对企业造成威胁。

- 可信的合作伙伴仅仅是值得信赖的合作伙伴，只要你们彼此友好合作。如果最后的合作关系恶化或成为竞争对手，那么之前的合作伙伴可能会采取对组织业务构成威胁的行动。

组织的潜在威胁是多种多样的。公司面临着源于自然环境、技术和人员的威胁。大多数企业在防御威胁上关注了自然灾害和IT攻击，但考虑来自个人的潜在威胁同样重要。始终考虑组织的活动、决策和交互行为可能带来的最佳结果与最糟结果。识别威胁是设计防御以帮助减少或消除停机、危害和损失的第一步。

1.4.2 确定和绘制潜在的攻击

一旦对开发项目或部署的基础设施面临的威胁有所了解，威胁建模的下一步就是确定可能发生的潜在攻击。这通常通过创建事务中的元素图表及数据流和权限边界来完成(见图1.8)。这是一个数据流的示意图，显示了系统的每个主要组件。安全区域之间的边界以及信息和数据的潜在流动或传输。通过为每个环境或系统制作这样的图表，可以更仔细地检查可能发生危害的每个关键点。

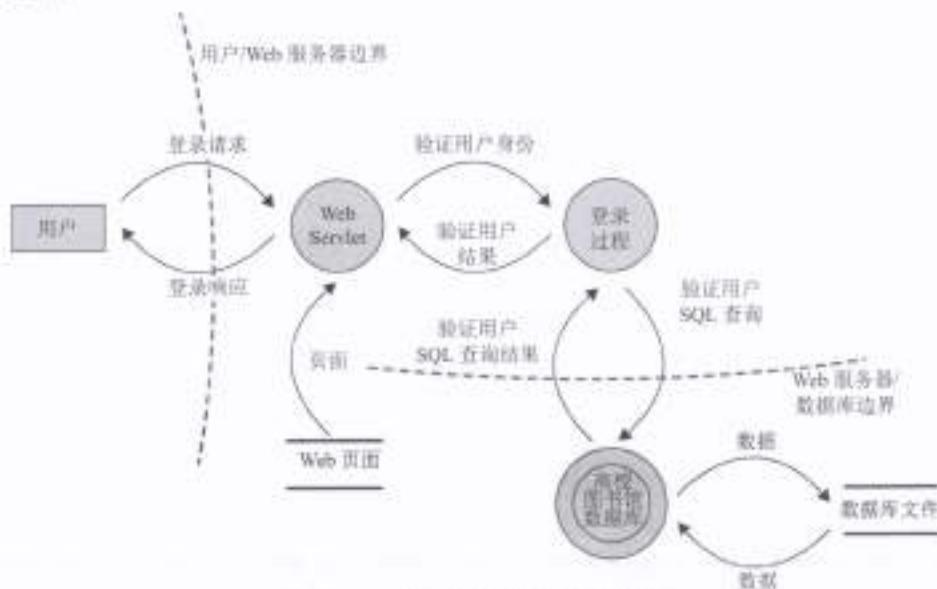


图1.8 一个用图表来揭示威胁的例子

这种数据流图通过可视化表示，有助于更好地理解资源和数据流动之间的关系。绘制图表的过程也称为绘制架构图。创建图表有助于详细描述业务任务、开发过程或工作活动中的每个元素的功能和目的。重要的是要包括用户、处理器、应用程序、数据存储以及执行特定任务或操作需要的其他所有基本元素。这是高层次的概述而不是对编码逻辑的详细评估。但对于较复杂的系统，可能需要创建多个图表，关注不同的焦点并把细节进行不同层级的放大。

一旦绘制出图表，就要确定涉及的所有技术，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。

接下来，要确定针对图表中每个元素的攻击，请记住，要考虑到各种攻击类型，包括逻辑/

技术、物理和社会。例如，确保包括欺骗、篡改和社会工程。这个过程将引导你进入威胁建模的下一阶段：执行简化分析。

1.4.3 执行简化分析

威胁建模的下一步是执行简化分析。简化分析也称为分解应用程序、系统或环境。这项任务的目的是更好地理解产品的逻辑及其与外部元素的交互。无论应用程序、系统或整个环境，都需要划分为更小的容器或单元。如果关注的是软件、计算机或操作系统，那么这些可能是子程序、模块或客体；如果关注的是系统或网络，这些可能是协议。如果关注的是整个业务基础结构，这些可能是部门、任务和网络。为理解输入、处理、信息安全、数据管理、存储和输出，应该对每个已识别的子元素进行评估。

在分解过程中，必须确定五个关键概念：

信任边界 信任级别或安全级别发生变化的位置。

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拥有更大特权的任何活动，通常需要修改系统或更改安全性。

安全声明和方法的细节 关于安全策略、安全基础和安全假设的声明。

将系统分解成各个组成部分能够更容易地识别每个元素的关键组件，并注意到脆弱性和攻击点。对程序、系统或环境的操作的了解越清楚，就越容易识别出针对它们的威胁。

1.4.4 优先级排序和响应

因为通过威胁建模过程识别出威胁，所以需要规定额外的活动来完成整个过程。下一步是全面记录这些威胁。在这个文档中，应该说明威胁的手段、目标和后果。要考虑完成开发所需的技术以及列出可能的控制措施和防护措施。

编辑文档后，要对威胁进行排序或定级。可使用多种技术来完成这个过程，如“概率×潜在损失”排序、高/中/低评级或 DREAD 系统。

“概率×潜在损失”排序技术会生成一个代表风险严重性的编号。编号范围为 1~100，100 代表可能发生的最严重风险；初始值范围为 1~10，1 最低，10 最高。这些排名从某些程度上看有些武断和主观，但如果由同一个人或团队为组织指定数字，仍会产生相对准确的评估结果。

高/中/低评级过程更简单。从这三个优先级标签中为每个威胁指定一个优先级标签。被指定高优先级标签的威胁需要立即解决。被指定中优先级标签的威胁最终也要得到解决，但不需要立即采取行动。被指定低优先级的威胁可能会被解决，但若解决这类威胁对整个项目来说需要付出太多努力或费用，那么是否解决它们是可以选择的。

DREAD 评级系统旨在提供一种灵活的评级解决方案，它基于对每个威胁的五个主要问题的回答。

- 潜在破坏：如果威胁成真，可能造成的伤害有多严重？
- 可再现性：攻击者复现攻击有多复杂？
- 可利用性：实施攻击的难度有多大？

- 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：攻击者发现弱点有多难？

通过询问上述问题及潜在的附加定制化问题，并为答案指定 H/M/L 或 3/2/1 值，就可以建立详细的威胁优先级表。

一旦确定了威胁优先级，就需要确定对这些威胁的响应。

要考虑解决威胁的技术和过程，并对成本与收益进行权衡。响应选项应该包括对软件体系结构进行调整、更改操作和流程以及实现防御性与探测性组件。

1.5 将基于风险的管理理念应用到供应链

将基于风险的管理理念应用到供应链是一种确保安全策略更加可靠与成功的手段，适合在所有规模的组织中运用。供应链的概念并非指单个实体，而是包括大多数计算机、设备、网络和系统。事实上，我们所知道的大多数电脑和设备制造公司——如 Dell、Cisco、Extreme Networks、Juniper、Asus、Acer 和 Apple——一般都是按每台电脑的组装形式生产，而不是生产所有单个部件。通常 CPU、内存、驱动控制器、硬盘驱动器、SSD 卡和显卡都由其他第三方供应商生产。即便是这些大型销售商，也不太可能自行开采金属、加工石油制成塑料或生产蚀刻芯片的硅。因此，任何已完成的系统都有一段漫长而复杂的历史，这也使得供应链得以存在。

安全供应链指的是供应链中的所有供应商或链接都是可靠的、值得信赖的、信誉良好的组织，他们向业务伙伴(尽管不一定向公众)披露他们的实践和安全需求。供应链中的每个环节都是可靠的，并对下一个环节负责。从原材料到精炼产品，从电子部件到计算机部件，再到成品的每一次交接都经过适当的组织、记录、管理和审核。安全供应链的目标是确保成品质量，满足性能和操作目标，并提供规定的安全机制。在这个过程中，没有任何伪造或遭受未经授权或恶意操纵或破坏的节点。有关供应链风险的其他观点，请参阅 NIST 的一个案例研究，位于 https://www.nist.gov/sites/default/files/documents/itl/csd/NIST_USRP-Boeing-Exostar-Case-Study.pdf。

如果在未考虑安全性的情况下进行收购和兼并，那么所收购产品的固有风险将在整个部署生命周期中一直存在。将收购元素的固有威胁最小化能减少安全管理成本，并可能减少安全违规。

评估与硬件、软件和服务相关的风险很重要。具有弹性集成安全性的产品和解决方案通常比那些没有安全基础的产品和解决方案更昂贵。然而，与满足不良设计产品安全需求的费用相比，这种额外的初始费用通常更具有成本效益。因此在考虑兼并/收购成本时，重要的是考虑产品部署的整个生命周期内的总成本，而不只是考虑初始购买和实施费用。

收购不仅涉及硬件和软件，也包括外包、与供应商签订合同、聘请顾问等内容。与外部实体协同工作时，集成的安全性评估与确保在产品设计时考虑了安全性同等重要。

许多情况下，可能需要持续的安全监控、管理和评估。这可能是行业最佳实践或监管要求。这种评估和共同监督可能在组织内部进行，也可由外部审计人员完成。当使用第三方评估和监控服务时，请记住，外部实体需要在其业务操作中体现出安全意识。如果外部组织无法在安全的基础上管理自身的内部操作，他们又将如何为你提供可靠的安全管理功能呢？

在为安全集成而评估第三方时，请考虑以下过程：

现场评估 到组织现场进行访谈，并观察工作人员的操作习惯。

文件交换和审查 调查数据和文件记录交换的方式，以及执行评估和审查的正式过程。

过程/策略审查 要求提供安全策略、过程/程序，以及事件和响应文件的副本以供审查。

第三方审计 根据美国注册会计师协会(AICPA)的定义，拥有独立的第三方审计机构可根据 SOC 报告，对实体的安全基础设施进行公正的审查。认证业务标准声明(SSAE)是一项规定，定义了服务组织如何使用各种 SOC 报告来报告合规性。自 2011 年 6 月 15 日起生效的 SSAE 16 版本在 2017 年 5 月 1 日被 SSAE 18 取代。为进行安全性评估，需要考虑 SOC 1 和 SOC 2 审计框架。SOC 1 审计侧重于根据安全机制的描述来评估其适用性。SOC 2 审计侧重于实现与可用性、安全性、完整性、隐私性和保密性相关的安全控制。有关 SOC 审计的更多信息，请参见 <https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socguidesandpublications.html>。

为所有收购设立最低限度的安全要求。这些要求应以现有安全策略为模板。新的硬件、软件或服务的安全需求应该始终满足或超过现有基础设施的安全性。在使用外部服务时，一定要检查服务水平协议(SLA)，确保服务合同中有关于安全的规定。这可能包括针对特定需求制定服务级别的细则。

以下是一些与并购整合的安全相关的优秀资源：

- “通过收购提高网络安全和弹性”。源于美国国防部和总务管理局的最终报告，发表于 2013 年 11 月(www.gsa.gov/portal/getMediaData?mediaId=185371)。
- NIST 的特别出版物 800-64 版本 2：“系统开发生命周期中的安全考虑”(<http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf>)。

1.6 本章小结

安全治理、安全管理和安全原则是安全策略和解决方案部署中的核心内容。它们定义了安全环境所需的基本参数及安全策略设计人员和系统实施人员为创建安全的解决方案必须实现的目标和宗旨。

安全的宗旨包含在 CIA 三元组中：保密性、完整性和可用性。这三项原则被认为是安全领域最重要的原则。它们对组织的重要性取决于组织的安全目标和需求以及环境中安全受到的威胁程度。

CIA 三元组的第一个原则是保密性，即不向未经授权的主体泄露客体信息。安全机制提供了保密性，即对防御未经授权的主体访问数据、客体或资源提供了高度保障。如果存在对保密性的威胁，就可能发生未经授权的泄露。

CIA 三元组的第二个原则是完整性，即客体保持真实性且只被授权的主体进行有目的的修改。如果安全机制提供了完整性，那么它就高度保证数据、客体和资源不会由最初的受保护状态转变到非保护状态。客体在存储、传输或过程中都不应遭受未经授权的更改。因此，保持完整性意味着客体本身不被未经授权地更改，且管理和操作客体的操作系统和程序实体不受破坏。

CIA 三元组的第三个原则是可用性，这意味着授权主体被授予了实时与不间断地访问客体的权限。安全机制提供了可用性，即提供了对数据、客体和资源可被授权主体访问的高度保障。可用性包括对客体的有效持续访问及抵御拒绝服务(DoS)攻击。可用性还意味着支撑性基础设施是可用的，并允许授权用户获得授权的访问。

在设计安全策略和部署安全解决方案时应该考虑和处理的其他与安全相关的概念和原则是

隐私、标识、身份验证、授权、问责制、不可否认性和审计。

安全解决方案概念和原则的另一块内容是保护机制：分层、抽象、数据隐藏和加密。保护机制是安全控制的共同特征，并不是所有的安全控制都必须具有这些机制，但是许多保护控制通过使用这些机制提供了保密性、完整性和可用性。

安全角色决定谁对组织资产的安全负责。担任高级管理者角色的人员对任何资产损失负有最终的职责和义务，并定义安全策略。安全专业人员负责实现安全策略，用户负责遵守安全策略。担任数据所有者角色的人员负责对信息进行分类，数据托管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恰当地保护资产。

规范化的安全策略结构由策略、标准/基线、指南和程序组成。这些独立文档是任何环境中安全设计和实现安全的基本元素。

变更控制或变更管理是安全管理的另一项重要内容。安全环境的变更可能引入漏洞、重叠、客体丢失和疏忽，进而导致出现新的脆弱性。不过，可通过系统的变更管理来维护安全。这通常涉及与安全控制和安全机制相关的活动，包括广泛的计划、测试、日志记录、审计和监控。然后对环境变化进行记录来识别变更发起者，无论变更发起者是客体、主体、程序、通信路径还是网络本身。

数据分类是基于数据的保密性、敏感性或秘密性需求而对其进行保护的主要手段。在设计和实现安全系统时，以相同的方式处理所有数据是低效的，因为有些数据项比其他数据项需要更高的安全性。用低级别安全保护所有内容意味着敏感数据很容易被访问，用高级别安全保护所有内容又过于昂贵，并且限制了对未分类的、非关键数据的访问。数据分类用于确定为保护数据和控制对数据的访问而分配多少精力、金钱和资源。

安全管理计划的一个重要方面是正确实施安全策略。为保证效果，安全管理必须采用自上而下方法，上层或高级管理者负责启动和定义组织的策略。安全策略为组织架构内的较低级别提供指导。中层管理人员负责将安全策略落实到标准、基线、指南和程序。操作管理人员或安全专业人员实现安全管理文档中规定的配置。最后，最终用户遵守组织的所有安全策略。

安全管理计划包括定义安全角色、制定安全策略、执行风险分析以及要求员工接受安全教育。这些职责以制定的管理计划为指导。安全管理团队应制定战略计划、战术计划和操作计划。

威胁建模是识别、分类和分析潜在威胁的安全过程。威胁建模可当作设计和开发期间的一种主动措施被执行，也可作为产品部署后的一种被动措施被执行。这两种情况下，威胁建模过程都识别了潜在危害、发生的可能性、关注的优先级以及消除(或减少)威胁的手段。

将基于风险的管理理念应用到供应链是一种确保安全策略更加可靠与成功的手段，适合在所有规模的组织中运用。如果在没有考虑安全性的情况下进行收购和兼并，那么所收购产品的固有风险将在整个部署生命周期中一直存在。

1.7 考试要点

理解由保密性、完整性和可用性组成的 CIA 三元组。保密性原则是指客体不会被泄露给未经授权的主体。完整性原则是指客体保持真实性且只被经过授权的主体进行有目的的修改。可用性原则指被授权的主体能实时和不间断地访问客体。了解这些原则为什么很重要，并了解支持它们的机制，以及针对每种原则的攻击和有效的控制措施。

能够解释身份标识是如何工作的。身份标识是下属部门承认身份和责任的过程。主体必须为系统提供标识，以便启动身份验证、授权和问责制的过程。

理解身份验证过程。身份验证是验证或测试声称的身份是否有效的过程。身份验证需要来自主体的信息，这些信息必须与指示的身份完全一致。

了解授权如何用于安全计划。一旦对主体进行了身份验证，就必须对其访问进行授权。授权过程确保所请求的活动或对象访问是可能的，前提是赋予已验证身份的权利和特权。

理解安全治理。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。

能够解释审计过程。审计(或监控追踪和记录)主体的操作，以便在验证过的系统中让主体为其行为负责。审计也对系统中未经授权的或异常的活动进行检测。需要实施审计来检测主体的恶意行为、尝试的入侵和系统故障，以及重构事件、提供起诉证据、生成问题报告和分析结果。

理解问责制的重要性。组织安全策略只有在有问责制的情况下才能得到适当实施。换句话说，只有在主体对他们的行为负责时，才能保持安全性。有效的问责制依赖于检验主体身份及追踪其活动的能力。

能够解释不可否认性。不可否认性确保活动或事件的主体不能否认事件的发生。它防止主体声称没有发送过消息、没有执行过动作或没有导致事件的发生。

理解安全管理计划。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。战略计划是相对稳定的长期计划，它定义了组织的目的、任务和目标。战术计划是中期计划，为实现战略计划中设定的目标提供更多细节。操作计划是基于战略和战术计划的短期和高度详细的计划。

了解规范化安全策略结构的组成要素。要创建一个全面的安全计划，需要具备以下内容：安全策略、标准/基线、指南和程序。这些文件清楚地说明安全要求，并促使责任各方实施尽职审查。

了解关键的安全角色。主要的安全角色有高级管理者、组织所有者、上层管理人员、安全专业人员、用户、数据所有者、数据托管员和审计人员。通过创建安全角色的层次结构，可以全面限制风险。

了解如何实施安全意识培训。在进行实际培训前，必须使用户树立安全意识，此后就可以开始培训或教育员工去执行工作任务并遵守安全策略。所有新员工都需要一定程度的培训，以便他们遵守安全策略中规定的标准、指南和程序。教育是一项更细致的工作，学生/用户学习的内容远远超过他们完成实际工作所需要了解的内容。教育最常与身份验证考试或寻求工作晋升的用户关联。

了解分层防御如何简化安全。分层防御使用一系列控制中的多个控制。使用多层次防御解决方案允许使用许多不同的控制措施来抵御威胁。

能够解释抽象的概念。抽象用于将相似的元素放入组、类或角色中，作为集合被指派安全控制、限制或许可。抽象增加了安全计划的实施效率。

理解数据隐藏。顾名思义，数据隐藏指将数据存放在主体无法访问或读取的逻辑存储空间以防数据被泄露或访问。数据隐藏通常是安全控制和编程中的关键元素。

理解加密的必要性。加密是对非预期的接收者隐藏通信的真实含义和意图的艺术与科学。加密有多种形式，适用于各种类型的电子通信，包括文本、音频和视频文件及应用程序。加密是安全控制中的重要内容，特别是在系统间传输数据时。

能够解释变更控制和变更管理的概念。安全环境的变更可能引入漏洞、重叠、客体丢失和疏忽，进而导致出现新的脆弱性。面对变更，维护安全的唯一途径就是系统性的变更管理。

了解为什么以及如何对数据进行分类。对数据进行分类是为将安全控制分配过程简化成分配给一组客体而不是单个客体。两个常见的分类方案是政府/军事分类和商业/私营部门分类。了解政府/军事分类方案的五个级别和商业/私营部门分类方案的四个分类级别。

理解解除分类的重要性。一旦资产不再被授权保护其当前指定的分类或敏感级别，就需要解除分类。

了解 COBIT 的基础知识。COBIT 是一种安全控制基础架构，用于为企业制定复合的安全解决方案。

了解威胁建模的基础知识。威胁建模是识别、分类和分析潜在威胁的安全过程。威胁建模可当成设计和开发期间的一种主动措施执行，也可作为产品部署后的一种被动措施执行。关键概念包括资产/攻击者/软件、STRIDE、PASTA、Trike、VAST、图表、简化/分解和 DREAD。

理解将基于风险的管理理念应用于供应链的必要性。将基于风险的管理理念应用到供应链中，可确保所有规模的组织都具有更加可靠和成功的安全策略。若收购时未考虑安全因素，这些产品的固有风险在整个部署生命周期中都存在。

1.8 书面实验

1. 讨论和描述 CIA 三元组。
2. 要求某人对其用户账户的行为负责的要求是什么？
3. 描述变更控制管理的好处。
4. 实施分类计划的七个主要步骤或阶段是什么？
5. 请说出(ISC)²为 CISSP 定义的六个主要安全角色名称。
6. 完整的组织安全策略由哪四个组成部分？其基本目的是什么？

1.9 复习题

1. 下列哪一项是安全的主要目标？
 - A. 网络的边界范围
 - B. CIA 三元组
 - C. 独立系统
 - D. 互联网
2. 对脆弱性和风险的评估基于以下哪种威胁？
 - A. CIA 三元组的一个或多个原则
 - B. 数据有效性
 - C. 应尽关心
 - D. 尽责程度

3. 下列哪一项是 CIA 三元组中的原则，代表授权主体被授予及时和不间断地访问客体的权限？
- A. 标识
 - B. 可用性
 - C. 加密
 - D. 分层防御
4. 下列哪一项不被视为违反保密性？
- A. 窃取密码
 - B. 窃听
 - C. 破坏硬件
 - D. 社会工程
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的故意攻击。
 - D. 当传输没有正确加密时可能发生违反保密性的情况。
6. STRIDE 常用于评估对应用程序或操作系统的威胁。下列哪一项不是 STRIDE 的元素？
- A. 欺骗
 - B. 特权提升
 - C. 否认
 - D. 泄露
7. 如果安全机制提供了可用性，它就提供了高度保障，授权的主体可以 _____ 数据、客体和资源。
- A. 控制
 - B. 审计
 - C. 访问
 - D. 否认
8. _____ 指对个人身份信息或可能对他人造成伤害、令他人感到尴尬的信息加以保密。
- A. 隔绝
 - B. 隐藏
 - C. 隐私
 - D. 关键性
9. 对于所有受影响的个人，除了下列哪一项之外，个人都有知情权？
- A. 限制个人电子邮件
 - B. 录音电话交谈
 - C. 收集有关上网习惯的信息
 - D. 用于保存电子邮件的备份机制

10. 数据分类管理的什么元素可覆盖所有其他形式的访问控制?

- A. 分类
- B. 物理访问
- C. 管理员职责
- D. 获得所有权

11. 以下哪一项确保活动或事件的主体不能否认事件的发生?

- A. CIA三元组
- B. 抽象
- C. 不可否认性
- D. 散列值

12. 以下哪个概念相对于分层安全是最重要和最特别的?

- A. 多层
- B. 串行
- C. 并行
- D. 过滤

13. 下列哪一项不是数据隐藏的例子?

- A. 防止授权的客体阅读者删除客体
- B. 防止未经授权的访问者访问数据库
- C. 限制较低分类级别的主体访问较高分类级别的数据
- 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. 使用户得到变更通知
- C. 允许失败的变更进行回滚
- D. 防止安全危害

15. 数据分类方案的主要目标是什么?

- A. 控制授权主体对客体的访问。
- B. 根据指定的重要性和敏感性标签，对数据进行程序化和分层的保护过程。
- C. 为问责制建立事务跟踪。
- D. 为操作访问控制提供最有效的方法来授予或限制功能。

16. 对数据进行分类时，通常不考虑下列哪一项特征?

- A. 价值
- B. 客体的大小
- C. 可用的生命周期
- D. 对国家安全的影响

17. 两种常见的数据分类方案是什么?

- A. 政府/军事分类方案和商业/私营部门分类方案
- B. 个人和政府
- C. 私营部门和非限制性部门
- D. 已分类和未分类

18. 对于已分类的数据，下列哪一项是最低的军事数据分类级别？
- A. 敏感
 - B. 机密
 - C. 专有
 - D. 私有
19. 商业/私营部门的哪个数据分类级别用于控制组织内的个人信息？
- A. 机密
 - B. 私有
 - C. 敏感
 - D. 专有
20. 数据分类可用在除哪一项之外的所有安全控制中？
- A. 存储
 - B. 处理
 - C. 分层
 - D. 传输

人员安全和风险管理的概念

本章涵盖的 CISSP 认证考试主题包括：

✓ 域 1：安全与风险管理

- 1.8 促进和执行人员安全策略和程序

- 1.8.1 候选人筛选与招聘

- 1.8.2 雇佣协议及策略

- 1.8.3 入职和离职程序

- 1.8.4 供应商、顾问和承包商的协议和控制

- 1.8.5 合规策略要求

- 1.8.6 隐私策略要求

- 1.9 理解并应用风险管理理念

- 1.9.1 识别威胁和脆弱性

- 1.9.2 风险评估/分析

- 1.9.3 风险响应

- 1.9.4 选择与实施控制措施

- 1.9.5 适用的控制类型(如预防、检测、纠正)

- 1.9.6 安全控制评估(SCA)

- 1.9.7 监视和测量

- 1.9.8 资产估值

- 1.9.9 报告

- 1.9.10 持续改进

- 1.9.11 风险框架

- 1.12 建立和维护安全意识、教育和培训计划

- 1.12.1 展示意识和培训的方法和技巧

- 1.12.2 定期内容评审

- 1.12.3 计划有效性评估

✓ 域 6：安全评估与测试

- 6.3.5 培训和意识

CISSP 认证考试 CBK 中的“安全与风险管理”域涉及很多安全解决方案的基础元素。这些也是设计、实施和管理安全机制所需的基本元素。

“安全与风险管理”域内的其他内容在第 1 章、第 3 章和第 4 章中讨论。请务必阅读所有

章节，以对这个知识域的全部内容有一个完整的认知。

由于硬件和软件控制的复杂性和重要性，在总体安全规划中经常忽略对人员的安全管理。本章探讨人员安全管理方面的内容，从建立安全的招聘过程、职责描述到开发员工基础架构。此外，还考虑在创建安全环境时如何把员工培训、管理和离职实践作为组成部分。最后研究如何评估和管理安全风险。

2.1 人员安全策略和程序

在所有安全解决方案中，人员都是最脆弱的元素。无论部署了什么物理或逻辑控制措施，人总是可以找到方法来规避、绕过控制措施，或使控制措施失效。因此，为环境设计和部署安全解决方案时，考虑人性是非常重要的。为理解和应用安全治理，必须应对安全链中最薄弱的环节，即人员。

与人员相关的事件、问题和损害可能发生在制定安全解决方案的所有阶段。这是因为任何解决方案的开发、部署和持续管理都涉及人员。因此，必须评估用户、设计人员、程序员、开发人员、管理人员和实施人员对过程的影响。

招聘新员工通常包括几个不同步骤：创建职责描述或岗位描述、设置工作级别、筛选应聘者、招聘和培训最适合该职位的人。如果没有职责描述，就不能对招聘哪类人员达成共识。因此，制定职责描述是定义与人员相关安全需求并招聘到新员工的第一步。有些组织认识到角色描述和职责描述之间的区别。角色通常与等级特权一致，而职责描述与特定分配的职责和任务相对应。

人员被组织招聘进来是因为需要该员工特定的工作技能和工作经验。组织内对于任何职位的职责描述都应该考虑相关安全问题。必须考虑职位是否需要处理敏感材料或访问机密信息等事项。实际上，职责描述定义了需要分配给员工执行工作任务的角色。职责描述还应定义该职位在安全网络环境中需要访问的类型和范围。一旦确定了这些问题，为职责描述分配的安全分类就相当标准了。



提示：职责描述的重要性

职责描述对于安全解决方案的设计和支持非常重要。然而，许多组织要么忽视这一点，要么内容陈旧，与现实不符。试着找出自己的职责描述。有这样的职责描述吗？如果有，最近一次更新是什么时候？它能准确反映工作职责吗？它是否描述了执行规定的工作职责所需的安全访问类型？一些组织必须编制职责描述以符合 SOC 2，而另一些遵循 ISO 27001 的组织则要求对职责描述进行年度审查。

在拟定符合组织过程的职责描述时，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(separation of duties)是一种安全概念，指将关键的、敏感的工作任务分给几个不同的管理员或高级操作员(见图 2.1)。这样做可防止任何个人具备破坏或颠覆关键安全机制的能力。可将职责分离看作最小特权原则在管理员之间的应用。职责分离也是防止串通的防护措施。串通(collusion)指两人或多人为了欺诈、盗窃或间谍活动而进行的破坏活动。通过限制个人权利，职责分离要求员工与他人合作才能实施较大的违规行为。寻找他人合伙执行违规

操作的行为很可能留下证据并被发现，这直接减少了串通的发生(通过他们可能被抓的机会进行威慑)。因此，串通是困难的，并增大了发起人在实施该行为前被发现的风险。

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
资源的管理员	管理员 1	管理员 2	管理员 3 和 4	管理员 5	管理员 6 和 7

图 2.1 一个关于 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(job responsibilities)指员工常规执行的具体工作任务。根据员工的职责，他们需要访问各种对象、资源和服务。在安全的网络环境中，必须向用户授予与工作任务相关元素的访问权限。为保持最大的安全性，访问应按最小特权原则进行分配。

最小特权原则规定在安全的环境中，用户应获得完成所需工作任务或职责必备的最小访问权限。要真正应用这一原则，需要对所有资源和功能进行细粒度的访问控制。

岗位轮换 岗位轮换(job rotation)或在多个工作岗位之间轮换员工，是组织提高整体安全性的一种简单手段(见图 2.2)。岗位轮换有两个功能。首先，它提供一种知识备份。当多名员工都能完成多个职位所要求的工作任务时，如果因为患病或其他事故使一名或多名员工长时间内无法工作，组织也不太可能出现严重的停摆或生产力下降。其次，岗位轮换可降低欺诈、数据更改、盗窃、破坏和信息滥用的风险。员工在特定职位上工作时间越长，就越可能被分配到其他工作任务，从而扩展了员工的特权和访问权限。当个人越来越熟悉工作任务时，就可能出于个人利益或恶意而滥用特权。如果某个员工有误用或滥用职权的行为，那么其他了解工作岗位和工作职责的员工就很容易察觉到。因此，岗位轮换也提供了一种同级审计形式，并可防止串通。

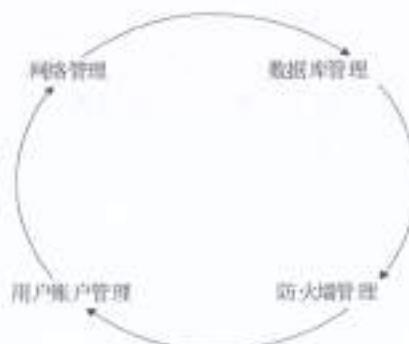


图 2.2 管理岗位轮换的一个例子

岗位轮换要求对安全特权和访问控制进行审核以维护最小特权原则。对岗位轮换、交叉培训和长期任职的员工有顾虑的问题之一是他们会持续获得特权和访问权限，其中许多特权和访

间权限并不是他们需要的。应该定期审核特权、许可、权利、访问权限等的分配，以检查是否存在特权蔓延或特权与工作职责不一致的情况。当员工随着工作职责变化而不断获得特权时，就会发生特权蔓延。最终结果是员工拥有的特权超过基于最小特权原则所规定的工作特权。

交叉培训

交叉培训常被当作岗位轮换的替代方案。这两种情况下，员工都能了解到多个岗位的职责和任务。然而，在交叉培训时，员工只是做好了完成其他工作的准备；而不是定期轮岗。交叉培训作为一类应急响应程序使现有的其他人员在恰当的员工不能工作时能填补职位空缺。

几个人共同完成一起犯罪叫作串通。采用职责分离、限制工作职责和岗位轮换方式，降低了员工愿意合伙进行非法活动或滥用职权的可能性，因为被检测到的风险非常高。通过严格监视指定的特权，例如管理员、备份操作员、用户管理员，可减少串通和其他特权的滥用。

职责描述并非专用于招聘过程中，在整个组织生命周期中都应对其进行维护。只有通过详细的职责描述才能对员工应该负责什么和他们实际负责什么进行比较。确保职责描述尽可能少地重复，确保一名员工的职责与另一名员工的职责不重叠或冲突是一项管理任务。同样，管理人员应该审核特权分配，以确保员工不会获得他们完成工作任务时不需要的访问权限。

2.1.1 候选人筛选及招聘

对岗位候选人的筛选基于职责描述定义的敏感性和分类。特定职位的敏感性和分类取决于担任该职位的人员有意或无意地违反安全规定造成的危害程度。因此，候选人筛选过程应反映招聘职位的安全性。

为保证岗位的安全性，候选人筛选、背景调查、推荐信调查、学历验证和安全调查验证都是证实有能力的、有资质的和值得信任的候选人的必备要素。背景调查包括：获得候选人的工作和教育背景，检查推荐信，验证学历，访谈同事、邻居和朋友，检查被捕或从事非法活动的管理记录，通过指纹、驾照和出生证明验证身份，进行个人面试。这个过程也可包括测谎仪测试、药物测试和性格测试/评估。

对很多公司来说，对申请人进行在线背景调查和社交网络账户审查已成为标准做法。如果潜在雇员在他们的分享网站、社交网络博客或公共即时通信服务上发布了不适当的材料，那么他们就不如那些没有发布的申请人有吸引力。当我们的行为被记录在文本、照片或视频中，并发布到网上，这些行为在公众视野中就会永久存在。通过查看个人的在线信息，可快速收集到个人的态度、智慧、忠诚、常识、勤奋、诚实、尊重、一致性和遵守社会规范和/或企业文化的总体情况。

2.1.2 雇佣协议及策略

聘用新员工时，应该签署雇佣协议。该文件概述了组织的规则、限制、安全策略、可接受的行为和活动策略、职责描述的细节、违规行为和后果，以及员工担任该职位的时间长度。这些内容也可能被分列到多个文档中。这种情况下，雇佣协议用于确认候选人已经阅读并理解其预期工作职位的相关文件。

除了雇佣协议，可能还需要确认与安全相关的其他文件。常见的文件之一是保密协议(Non-disclosure Agreement, NDA)。NDA 用于防止已离职的员工泄露组织的机密信息。当个人签署保密协议时，他同意不向组织以外的任何人透露任何被定义为机密的信息。违反保密协议的行为通常会受到严厉惩罚。



真实场景

NCA：与 NDA 同类

非竞争协议(Noncompete Agreement, NCA)与 NDA 同类。非竞争协议试图阻止了解组织秘密的员工加入另一个与该组织存在竞争关系的组织，使第二个组织不能利用该员工了解的秘密谋利。NCA 还用于防止员工仅为加薪或其他激励措施而跳槽到有竞争关系的另一家公司。NCA 通常有时间限制，如 6 个月、1 年甚至 3 年。NCA 的目标是保持人力资源持续为公司的利益工作，而不是与公司作对。从而保持原有公司的竞争优势。

许多公司要求新员工签署 NCA。然而，在法庭上彻底实施 NCA 通常是一场艰难的辩论。法院赞同员工利用他们拥有的技能和知识来获得收入并养家糊口。如果 NCA 阻止个人获得合理收入，法院通常会宣布 NCA 无效或拒绝实施惩罚后果。

虽然 NCA 未必强制执行，但这并不意味着它对原来的公司没有好处，例如：

- 违反 NCA 会带来诉讼威胁，这通常足以阻止员工在新公司求职时违反保密条款。
- 如果员工确实违反了 NCA 条款，那么即使由于法院限制无法实施具体的违规后果，法庭审理的漫长时间，以及个人耗费的精力和经济成本也足以令人望而生畏了。

在被雇用时，你签了 NCA 吗？如果签了，你了解所有条款和违反 NCA 的潜在后果吗？

在员工的整个雇佣期内，经理应该定期审计每位员工的职责描述、工作任务、特权和责任。随着时间的流逝，通常工作任务和特权会漂移，这可能导致一些任务被忽略，而另一些任务被多次执行。漂移或特权蔓延也可能导致安全违规。定期审查每个职责描述的范围与实际发生的情况有助于将安全违规行为保持到最低程度。

该审查过程中的关键部分是强制休假。在许多安全的环境中，一到两周的强制休假被用于审计和验证员工的工作任务和特权。强制休假使员工离开工作环境，并安排其他员工接替工作，这样会更容易发现原来员工的滥用、欺诈或疏忽行为。

2.1.3 入职和离职程序

入职是在组织的 IAM(Identity and Access Management, 身份和访问管理)系统中添加新员工的过程。当员工的角色或职位发生变化，或该员工获得其他特权或访问权限时，都可以使用入职流程。

离职则正好相反，指在员工离开公司后，将其身份从 IAM 系统删除。这包括取消和/或删除用户账户、撤消证书、取消访问代码的特权以及终止其他特定特权。还可能包括通知保安人员和其他物理访问管理人员，后续不再允许该员工进入办公大楼。

需要明确记录入职和离职流程，来确保一致性以及符合规章或合同义务。

入职也指组织特性的社会化。在这个过程中新员工接受培训，以便为履行工作职责做好充

分准备。入职可包括培训，获得工作技能，调整做事方式，努力使员工有效融入现有的组织过程和程序。精心设计的入职培训可提高工作满意度和生产效率，使员工更快地融入环境，提高员工对组织的忠诚度，减轻压力，减少离职率。在职责分离的背景下，精心设计的入职培训的另一个好处是，实现了前面讨论过的最小特权原则。

当一名员工必须被解雇或离职时，需要处理许多问题。在解雇过程中，安全部门和人力资源(HR)部门之间建立牢固的关系对维持控制和最小化风险是非常重要的。为维护一个安全环境，当组织必须解雇某个心怀不满的员工时，解雇过程或解雇策略是必需的。被解雇员工的反应可能是平静、理解和接受，也可能是反应强烈、极其愤怒等。必须设计和实施合理的解雇程序以减少意外事故的发生。

应该以私下的和尊重的态度来处理员工解雇过程。然而，这并不意味着不应该采取预防措施。终止合同时应至少有一名证人在场，证人最好是一名高级经理和/或安保人员。一旦员工被通知解雇完成，他们应该立刻被护送出工作场所，并且不允许出于任何原因在无人陪同情况下返回工作区域。在解雇完成前，应该收集组织特有的所有身份标识、访问权限或安全标志以及门卡、密钥和访问令牌(见图 2.3)。一般来说，解雇员工的最佳时间是在他们轮岗的工作周结束后。可提前通知，让前雇员有时间申请失业和/或在周末前开始寻找新工作。此外，在轮岗时解雇员工可让员工更轻松自然地与其他员工告别。

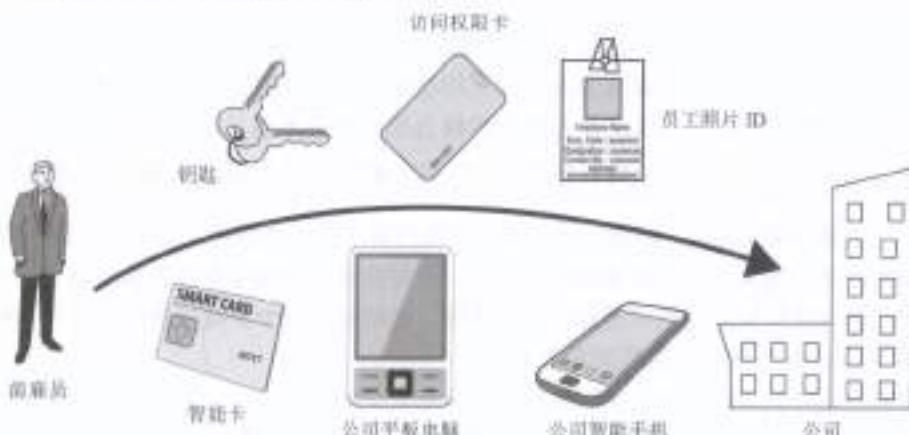


图 2.3 前雇员必须归还所有公司财产

如有可能，应该进行离职面谈。不过这通常取决于员工被解雇后的精神状态以及其他许多因素。如果无法在解雇时立即进行离职面谈，也要尽快进行。离职面谈的主要目的是根据雇佣协议、保密协议和任何其他与安全有关的文件，对前雇员的责任和限制进行审查。

以下是其他一些需要尽快处理的事宜：

- 确保员工已归还交通工具和家中的所有公司设备或用品。
- 删除或禁用员工的网络用户账户。
- 通知人力资源部发放最后的薪资，支付所有未使用假期的折算费用，并终止所有福利待遇。
- 安排一名安全部门人员陪同被解雇员工在工作区域收拾个人物品。
- 通知所有安保人员、巡查人员或监控出入口的人员，以确保前雇员在没有护送的情况下无法再次进入办公大楼。

大多数情况下，应在通知员工被解雇的同时禁用或删除其系统的访问权限。如果该员工能访问机密数据，或具有更改或损坏数据或服务的专业知识或访问权限，就更应该这样做。如果不能限制已解雇员工的活动，将使组织面临各种脆弱性，包括对物理财产和逻辑数据的盗窃和破坏。



真实场景

解雇：不再只是解雇通知书

解雇员工是一个复杂过程。仅向员工邮箱中发送解雇通知就算完成解雇的日子已经一去不复返了。在大多数以 IT 为中心的组织中，终止雇佣关系可能带来的一种情况是员工带来危害，使组织处于风险之中。这也是为什么需要一个精心设计的离职面谈过程的原因。

然而，仅有离职面谈过程是不够的。还需要能在解雇过程中正确地实施。遗憾的是，这样的情况并非总是发生。你可能听说过一些因为仓促的离职面谈而产生的惨痛结果。常见例子包括在正式通知员工终止雇佣关系前执行下列任何一项操作(员工由此预感到自己将被解雇)：

- IT 部门要求归还笔记本电脑。
- 禁用网络账户。
- 停用办公场所入口的个人身份识别码(PIN)或智能卡。
- 撤消停车证。
- 分发公司的重组图表。
- 把新员工安排在小隔间里。
- 允许将解雇信息泄露给媒体。

毫无疑问，为使离职面谈和安全解雇程序能够正常运作，必须在恰当的时间(即在离职面谈开始时)按照恰当的顺序实施这些过程，例如以下实例：

- 告知员工其被解雇。
- 要求返回所有访问标识、密钥和公司设备。
- 禁止该员工对组织的所有方面进行电子访问。
- 提醒该员工关于 NDA 的义务。
- 护送该员工离开办公场所。

2.1.4 供应商、顾问和承包商的协议和控制

供应商、顾问和承包商的控制用来确定组织主要外部实体、人员或组织的绩效水平、期望、薪酬和影响。通常，这些控制条款是 SLA 文档或策略中规定的。

使用 SLA 确保组织向其内部或外部客户提供的各种服务保持在服务方和客户都满意的恰当服务水平，这种方式日趋普遍。将 SLA 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至关重要的关键组件都是明智的。在使用任何类型的第三方服务提供商(包括云服务供应商)时，SLA 都很重要。在 SLA 中通常会提到以下问题：

- 系统运行时间(占总运行时间的百分比)
- 最长连续停机时间(以秒/分钟等计算)

- 最大负载
- 平均负载
- 诊断职责
- 故障切换时间(如果采取了冗余措施)

SLA 通常还包括在无法维持协议规定的情况下约定的赔偿措施。例如，如果一个关键电路的故障时间超过 15 分钟，服务提供商可能同意扣减该电路一周的所有费用。

SLA 以及供应商、顾问和承包商的控制是降低风险和规避风险的重要部分。通过明确规定对外部各方的期望和惩罚，每个相关人员都知道对他们的期望是什么，以及如果不能满足这些期望会有什么后果。从外部提供商获取许多业务功能或服务，费用可能非常便宜，但潜在的攻击面和漏洞范围的扩大确实提高了可能面临的风险。SLA 除了确保以合理价格提供高质量和及时的服务外，还应注重保护和改进安全。有些 SLA 是已设置好而无法调整的，而其他一些 SLA 则允许对其内容进行重大调整。应该确保 SLA 是支持安全策略和基础架构的原则，而不是与之冲突，否则会引入弱点、脆弱性或异常。

2.1.5 合规策略要求

合规是符合或遵守规则、策略、法规、标准或要求的行为。对安全治理来说，合规是一项重要内容。在人员层面，合规关系到员工个人是否遵守公司的策略，是否按照规定的程序完成工作任务。许多组织依靠员工的合规性以保持高质量、一致性、效率和节约成本。如果员工不遵守规则，就会在利润、市场份额、认可和声誉方面给组织带来损害。员工需要接受培训，以便知道他们需要做什么(即符合公司安全策略规定的标准，遵守任何合约义务，如遵守 PCI DSS 来维持信用卡处理能力)。只有这样，他们才能对违反规定或不遵守规定的行为负责。

2.1.6 隐私策略要求

隐私是一个很难定义的概念。在很多情况下频繁使用这个词时没有进行太多的量化或限定。以下是对隐私的一些定义：

- 主动防止未经授权访问个人可识别的信息(即直接连接到个人或组织的数据点)。
- 防止未经授权访问私有或机密信息。
- 防止在未同意或知情的情况下被观察、监视或检查。



注意：

在讨论隐私时经常出现的一个概念是 PII (Personally Identifiable Information，个人信息)。PII 是可以很容易和/或明显地追溯到原始作者或相关人员的任何数据项。电话号码、电子邮件地址、邮寄地址、社会保险号和姓名都是 PII。MAC 地址、IP 地址、操作系统类型、喜欢的度假地点、吉祥物的名字等通常不被认为是 PII。然而，这并不是通用的正确观点。在德国和其他欧盟成员国，IP 地址和 MAC 地址在某些情况下被认为是 PII(参见 <https://www.whitecase.com/publications/alert/court-confirms-ip-addresses-are-personal-data-some-cases>)。

在IT领域内处理隐私时，通常需要在个人权利和组织的权利或活动之间取得平衡。有人认为，个人有权控制可否收集与他们相关的信息，以及如何使用这些信息。其他人则认为，在公共场合执行的任何活动，如在互联网上执行的大多数活动或在公司设备上执行的活动，可在不告知或未许可的情况下对个人进行监控，而且从这些监控中收集的信息可用于组织认为适当的或可取的任何目的。

通常有必要保护个人免受不必要的监控，避免商家直销，防止隐秘的、私有的或机密的信息被披露。然而，一些组织声称通过人口统计学研究、信息收集和聚焦市场改进了商业模式，减少了广告浪费，并节省了人力成本。

在隐私方面有许多法律与法规的合规性问题。许多美国法案都有关于隐私的要求，如健康保险流通与责任法案(Health Insurance Portability and Accountability Act, HIPAA)、2002年的萨班斯-奥克斯利法案(Sarbanes-Oxley Act, SOX)、家庭教育权利和隐私法案(Family Educational Rights and Privacy Act, FERPA)和金融服务现代化法案。欧盟指令95/46/EC(又名数据保护指令)、通用数据保护条例和支付卡行业数据安全标准(Payment Card Industry Data Security Standard, PCI DSS)也有隐私要求。重要的是理解组织必须遵守的所有政府规定，并确保合规性，特别是隐私保护方面。

无论个人或组织的立场如何，都必须在组织安全策略中包括在线隐私问题。不仅是对外部访客、客户、员工、供应商和承包商访问组织在线信息时都需要考虑隐私问题。如果要收集与个人或公司相关的任何类型信息，必须解决隐私问题。

大多数情况下，特别是当隐私受到侵犯或限制时，必须通知个人和公司，否则可能面临法律纠纷。在允许或限制个人使用电子邮件、保留电子邮件、记录电话通话、收集上网或消费习惯等信息时，也必须解决隐私问题。

2.2 安全治理

安全治理是与支持、定义和指导组织的安全工作相关的实践的集合。安全治理通常与公司治理和IT治理密切相关并有交集。这三项治理工作的目标常常是相互关联或相同的。例如，组织治理的一个共同目标是确保组织将长期存在并随时间成长。因此，三种治理形式的共同目标都是维护业务流程，同时努力实现增长和弹性。

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强制规定的监督制度。实际的治理方法可能有所不同，但通常包括外部调查员或审计人员。这些审计人员可能由监管机构指定，也可能是目标组织雇用的顾问。

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。许多组织选择把业务运营的各个方面外包出去。外包业务可包括保安、维护、技术支持和会计服务。第三方需要遵守主要组织的安全立场。否则，就会给主要组织带来额外风险和脆弱性。

第三方治理的重点是验证安全目标、需求、法规和合同义务的合规性。现场评估为某个位置使用的安全机制提供最真实的信息。在现场进行评估或审计的人员需要遵守审计协议(如COBIT)，并需要有符合特定要求的检查清单。

在审计和评估过程中，目标单位和监管机构都应进行全面和开放的文件交换和审查。组织需要详细了解必须遵守的要求。组织应向监管机构提交安全策略和自我评估报告。这种开放的

文件交换确保各方就所有关注的问题达成共识，减少未知需求或不切合实际的期望。文件交换后，会启动文件审查过程。

文件审查是阅读交换材料并根据标准和期望进行验证的过程。文件审查通常在现场审查前进行。如果交换的文档足够多，且符合预期，那么现场审查就能聚焦于文档的符合性方面。若文档不完整、不准确或不充分，则需要更新和修改文档，现场审查将推迟。这一步很重要，因为如果文档不符合要求，现场也不符合要求。

许多情况下，特别是与政府或军事机构或承包商有关时，如果未能提供足够的文件以满足第三方监管的要求，可能导致授权操作(ATO)损失或失效。完整和充分的文档通常可维护现有的 ATO 或提供临时 ATO(TATO)。在 ATO 丢失或撤消后，若要重新建立 ATO，通常需要再次进行完整的文件审查和现场审查。

文件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。文件审查确保声明的和实现的业务任务、系统和方法是实用的、高效的和节约成本的，最重要的是(至少在安全治理方面)通过减少脆弱性和规避、减轻风险来支持安全目标。风险管理、风险评估和风险处置都是执行过程/策略审查所涉及的方法与技术。

2.3 理解并应用风险管理理念

安全的目的是在防止数据丢失或泄露的同时保持已授权的访问。发生损害、破坏或泄露数据或其他资源的可能性称为风险。理解风险管理的概念，不仅对 CISSP 考试很重要，对建立充分的安全环境、适当的安全治理以及应尽关心和尽职审查的法律证明也很重要。

因此，管理风险是维持安全环境的一个因素。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露的因素，根据数据价值和控制措施的成本评估这些因素，并实施具有成本效益的解决方案来减轻风险。风险管理的整体过程用于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。

风险管理的主要目标是将风险降至可接受的水平。这个水平实际上取决于组织、资产价值、预算以及其他许多因素。某个组织认为可接受的风险对另一个组织来说可能是无法接受的高风险。设计和实施一个完全没有风险的环境是不可能的，但通过较少努力就显著降低风险却是可能的。

IT 基础设施面临的风险不只源于计算机方面。事实上，许多风险来自非计算机方面。对组织进行风险评估时，考虑所有可能的风险是很重要的。如果不能正确评估和响应所有形式的风险，公司就容易受到攻击。请记住，IT 安全(通常称为逻辑或技术安全性)只针对逻辑或技术攻击提供保护。为防止 IT 安全受到物理攻击，就必须建立物理保护措施。

实现风险管理目标的过程称为风险分析。风险分析包括：检查环境中的风险，评估每个威胁事件发生的可能性和实际发生后造成的损失，评估各种风险控制措施的成本，完成风险防护措施的成本/收益报告并向高级管理层汇报。除了这些以风险为中心的活动外，风险管理还需要对组织中的所有资产进行估算、评估和估值。如果没有正确的资产估值，就不能划分资产的优先级，也不能比较风险可能造成的损失。

2.3.1 风险术语

风险管理引入大量术语，必须清楚地理解这些术语。特别是在 CISSP 考试中。本节定义并讨论与风险相关的所有重要术语：

资产(Asset) 资产可以是环境中需要保护的任何事物，包括业务流程或任务中用到的所有资源。可以是计算机文件、网络服务、系统资源、流程、程序、产品、IT 基础设施、数据库、硬件设备、家具、产品配方、知识产权、人员、软件、设施等。如果组织认为其控制的某种资源有价值并需要保护，那么这种资源即可称为资产。以便进行风险管理或风险分析。资产出现损失或泄露会危及组织整体的安全，导致生产效率降低、利润减少、额外开支增加、组织停工以及许多无形的不良后果。

资产估值 资产估值是根据实际成本和非货币性支出给资产指定的货币价值。其中包括开发、维护、管理、宣传、支持、维修和替换资产的成本，还包括许多难以估算的价值，比如公众信心、行业支持、生产效率的提升、知识产权和所有权利益。稍后将详细讨论资产估值。

威胁(Threat) 任何可能发生的、对组织或特定资产造成不良或非预期结果的潜在事件都是威胁。威胁指任何可能导致资产受损、毁坏、变更、丢失或泄露的行为或不作为，或可能阻碍访问或维护资产的行为。威胁可大可小，会造成或大或小的后果。威胁可能是故意的或意外的，可来自于人员、组织、硬件、网络、结构或自然界。威胁主体有目的地利用脆弱性。威胁主体通常是人员，但也可能是程序、硬件或系统。威胁事件是对脆弱性的意外和有意利用。威胁事件可以是自发的或人为的，包括火灾、地震、洪水、系统故障、人为错误(由于缺乏训练或无知)和断电。

脆弱性(Vulnerability) 脆弱性是资产中的弱点。是防护措施或控制措施的弱点，或缺乏防护措施/控制措施。

换句话说，脆弱性是 IT 基础设施或组织其他方面的缺陷、漏洞、疏忽、错误、局限性、过失或薄弱环节。如果脆弱性被利用，就可能造成资产的破坏或损失。

暴露(Exposure) 暴露指脆弱性会被威胁主体或威胁事件加以利用的可能性是存在的。暴露并不意味着导致损失的事件正在发生。暴露仅表示如果存在脆弱性和能利用脆弱性的威胁，就可能发生威胁事件或出现潜在的暴露。“最坏的情况是什么？”的答案是另一种描述暴露的方式，不是说伤害已发生或实际将发生，只是说发生伤害的潜在可能，以及伤害可能有多大或多严重。可从这个概念推导出在定量风险分析中使用的暴露因子(EF)值。

风险(Risk) 风险是威胁利用脆弱性对资产造成损害的概率。它是对概率、可能性或机会的评估。威胁事件发生的可能性越大，风险越大。每个暴露实例都是一种风险。如果用公式表达，那么风险可定义为：风险=威胁*脆弱性。

因此，减少威胁主体或脆弱性都可直接降低风险。当风险发生时，威胁主体、威胁执行者或威胁事件已利用脆弱性对一个或多个资产造成损害或泄露。安全的整体目的是通过消除脆弱性和防止威胁主体和威胁事件危害资产，来避免风险成为现实。作为一种风险管理工具，实施防护措施能实现安全。

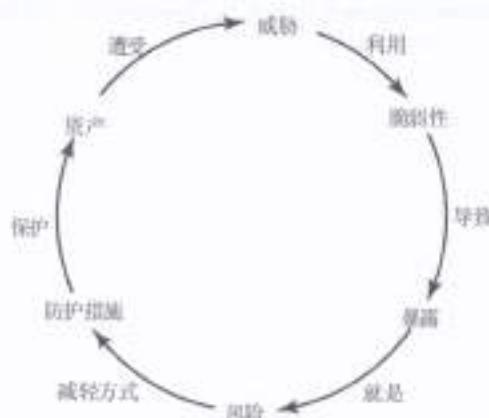
防护措施(Safeguard) 防护措施(或控制措施)指任何能消除或减少脆弱性，或能抵御一个或多个特定威胁的事物。防护措施可以是安装软件补丁、更改配置、雇用保安、改变基础设施、修改流程、改善安全策略、更有效地培训人员、给周边围栏通电、安装照明灯等。防护措施是

能消除或减少组织内任何位置的威胁或脆弱性以降低风险的任何行动或产品，是减轻或消除风险的唯一手段。有一点非常重要：防护措施、安全控制或控制措施未必是购买新产品，重新配置现有元素甚至从基础设施中删除某些元素也是有效的防护措施。

攻击(Attack) 攻击是威胁主体对脆弱性的利用。换句话说，攻击就是任何故意利用组织安全基础设施的脆弱性并造成资产受损或泄露的行为。攻击也可被看成违反或未遵守组织的安全策略。

破坏(Breach) 破坏指安全机制被威胁主体绕过或阻止。当破坏与攻击相结合时，就可能导致渗透或入侵。渗透指威胁主体通过规避安全控制获得对组织基础设施的访问，并能直接危及资产。

资产、威胁、脆弱性、暴露、风险和防护措施相互关联，如图 2.4 所示。资产遭受威胁，威胁利用脆弱性，脆弱性导致暴露，暴露就是风险，而防护措施可减轻风险，以保护资产的安全。



2.3.2 识别威胁和脆弱性

风险管理的一个基础部分是识别与检查威胁。这涉及为组织已识别的资产创建一个尽可能详尽的威胁列表。该列表应该包括威胁主体以及威胁事件。重要的是要记住威胁可能来自任何地方。对 IT 的威胁不仅限于 IT 方面。在编制威胁列表时，需要考虑以下因素：

- 病毒
- 级联错误(一系列不断升级的错误)和依赖性错误(由于依赖于不存在的事件或内容而引起)
- 已授权用户的犯罪活动(间谍活动、IP 盗用、贪污等)
- 运动(振动、炸裂声等)
- 故意攻击
- 重组
- 已授权用户所患的疾病或流行病
- 恶意黑客
- 心怀不满的员工
- 用户错误

- 自然灾害(地震、洪水、火灾、火山爆发、飓风、龙卷风、海啸等)
- 物理损坏(碎裂、抛射、电缆被切断等)
- 滥用数据、资源或服务
- 更改或破坏数据分类或安全策略
- 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
- 极端温度
- 能量异常(静态、EM 脉冲、无线电频率[RF]、电源损耗、电涌等)
- 数据丢失
- 信息战
- 商业活动的破产或更改/中断
- 编码/编程错误
- 入侵者(物理和逻辑)
- 环境因素(存在的天然气、液体、生物等)
- 设备故障
- 物理盗窃
- 社会工程学

大多数情况下，执行风险评估和分析的应该是一个团队而不是单独的个人。而且，团队成员应该来自组织内的各个部门。通常情况下，并不要求所有团队成员都是安全专业人员或网络/系统管理员。以组织人员为基础，确定多样化的团队成员将有助于彻底识别和解决所有可能存在的威胁和风险。

风险管理顾问

风险评估是一个高度棘手、琐碎、复杂和冗长的过程。由于风险的大小、范围或责任，现有员工通常无法恰当地实施风险分析，因此，许多组织都外聘风险管理顾问来完成这项工作。这提供高水平的专业知识，不会让员工觉得难以完成工作，而且可以更可靠地衡量真实世界的风险。风险管理顾问不只进行书面上的风险评估和分析，他们通常使用复杂而昂贵的风险评估软件。此类软件简化了整个任务，提供了更可靠的结果，并生成可被保险公司、董事会等接受的标准化报告。

2.3.3 风险评估/分析

风险评估/分析主要是高层管理人员的工作。他们负责通过定义工作的范围和目标来启动和支持风险分析和评估。风险分析的实际执行过程通常分配给安全专业人员或评估团队。然而，所有风险评估、结果、决策和结果都必须得到高层管理人员的理解和批准，这是“应尽关心”的一部分。

所有 IT 系统都存在风险。无法消除全部风险。但高层管理人员必须决定哪些风险是可接受的，哪些风险是不可接受的。决定可接受哪些风险时，需要进行详细而复杂的资产和风险评估。

一旦制定了威胁列表，就必须单独评估每个威胁及其相关风险。有两种风险评估方法：定

量风险分析和定性风险分析。定量风险分析用实际的货币价值来计算资产损失。定性风险分析用主观的和无形的价值来表示资产损失。对于完整的风险分析来说，这两种方法都是必要的，大多数环境都混合使用这两种风险评估方法。

1. 定量风险分析

定量风险分析可计算出具体概率。这意味着定量风险分析的最终结果是一份包含风险级别、潜在损失、应对措施成本和防护措施价值等货币数据的报告。这份报告通常容易理解，特别是对于任何了解电子表格和预算报告的人来说。可将定量风险分析看作用数字衡量风险的行为，换句话说，就是用货币形式表示每项资产和威胁。然而，完全靠定量分析是不可行的，并不是所有分析元素和内容都可量化，因为有些元素和内容是定性的、主观的或无形的。

定量风险分析的过程从资产估值和威胁识别开始。接下来评估每个风险的可能性和发生频率。然后用这些信息计算用于评估防护措施的各种成本函数。

定量风险分析的六个主要步骤或阶段如图 2.5 所示。



图 2.5 定量风险分析的六大要素

(1) 编制资产清单，并为每个资产分配资产价值(Asset Valuation, AV)。

(2) 研究每一项资产，列出每一项资产可能面临的所有威胁。对于每个列出的威胁，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，计算每个威胁在一年之内实际发生的可能性，也就是年度发生率(Annualized Rate of Occurrence, ARO)。

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

(5) 研究每种威胁的应对措施，然后基于已采用的控制措施，计算 ARO 和 ALE 的变化。

(6) 针对每项资产的每个威胁的每个防护措施进行成本/效益分析。为每个威胁选择最合适的防护措施。

与定量风险分析相关的成本函数包括暴露因子、单一损失期望、年度发生率和年度损失期望：

暴露因子(EF) 暴露因子(EF)表示如果已发生的风险对组织的某个特定资产造成破坏，组织将因此遭受的损失百分比。EF 也可称为潜在损失。大多数情况下，已发生的风险不会导致资产的完全损失。EF 仅表示当单个风险发生时对整体资产价值造成的损失预计值。对于容易替换的资产(如硬件)，EF 通常很小。但对于不可替代的或专有的资产(如产品设计或客户数据库)，它可能非常大。EF 用百分比表示。

单一损失期望(SLE) 需要 EF 来计算 SLE。单一损失期望(SLE)是特定资产发生单一风险的相关成本。SLE 代表的是如果某个资产被特定威胁损害，组织将遭受的确切损失。

SLE 的计算公式如下：

$$\text{SLE} = \text{资产价值(AV)} * \text{暴露因子(EF)}$$

或更简单：

$$\text{SLE} = \text{AV} * \text{EF}$$

SLE 以货币为单位。例如，如果资产价值是 200 000 美元，对于特定威胁的 EF 为 45%，那么对于该资产这项威胁的 SLE 就是 90 000 美元。

年度发生率 年度发生率(ARO)是在一年内特定威胁或风险发生的预期频率。ARO 的值可以是 0(零)，表示威胁或风险永远不会发生，也可以是非常大的数字，表示威胁或风险经常发生。计算 ARO 是很复杂的，可从历史记录、统计分析或推算得出结果。ARO 计算也称为概率测定。某些威胁或风险的 ARO 是通过将单个威胁发生的可能性乘以引起威胁的用户数量来计算的。例如，塔尔萨发生地震的 ARO 可能是 0.000 01，而旧金山发生地震的 ARO 可能是 0.03(就 6.7+ 震级而言)；或者可对比在塔尔萨发生地震的 ARO(0.000 01)与在塔尔萨办公室中发生电子邮件病毒的 ARO(10 000 000)。

年度损失期望 年度损失期望(ALE)是针对特定资产的所有可发生的特定威胁，在年度内可能造成的损失成本。

ALE 计算公式如下：

$$\text{ALE} = \text{单一损失期望(SLE)} * \text{年度发生率(ARO)}$$

或更简单：

$$\text{ALE} = \text{SLE} * \text{ARO}$$

例如，如果资产的 SLE 是 90 000 美元，而针对特定威胁的 ARO(如全部断电)是 0.5，那么 ALE 是 45 000 美元。另一方面，如果针对特定威胁的 ARO 为 15(如用户账户受到攻击)，则 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 是一项艰巨的任务。幸运的是，定量风险评估软件工具可简化和自动处理这一过程。这些工具生成资产估值的详细清单，然后使用预定义的 ARO 以及一些定制选项(即，行业、位置、IT 组件等)生成风险分析报告。下面是经常涉及的计算：

计算使用防护措施后的年度损失期望 除了确定防护措施的年度成本外，还必须计算实施防护措施后的资产的 ALE。这需要重新计算防护措施实施后的 EF 和 ARO。大多数情况下，即使采用防护措施后，资产的 EF 仍保持不变(EF 是风险发生时造成的损失大小)。换句话说，如果防护措施失效，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，但子弹却穿

过防弹衣打中你的心脏，那你仍会遭受与没有防弹衣时相同的伤害。因此，如果防护措施失效，资产上的损失通常与没有防护措施时相同。然而，有些安全措施在即使不能完全阻止攻击的情况下，也仍可降低攻击造成的伤害。例如，虽然火灾仍可能发生，火灾和洒水器中的水可能会破坏基础设施，但这些总的损失可能远小于整个建筑物被烧毁的损失。

即使 EF 不变，防护措施也会改变 ARO。实际上，安全措施的目的是降低 ARO。换句话说，安全措施应该减少攻击真正对资产造成损害的次数。在所有可能的安全措施中，最好的办法是将 ARO 降至零。虽然有些防护措施是完美的，但大多数都不是。因此，许多安全措施都有应用后的 ARO，比防护措施应用前的 ARO 小一些，但通常不会为零。有了更新的 ARO 和可能更新的 EF，防护措施实施后的新 ALE 就可以计算出来了。

计算实施防护措施前的 ALE 和实施防护措施后的 ALE 后，为进行成本效益分析，还需要再计算一个数值。这个额外数值是防护措施的年度成本。

计算防护措施成本。针对每个特定风险，必须在成本/收益的基础上评估一个或多个防护措施或控制措施。要执行此评估，必须首先编制一份针对每种威胁的防护措施清单。然后为每个安全措施分配部署价值。实际上，必须度量部署费用或防护措施的成本与受保护资产价值之间的关系。因此，受保护资产的价值决定了保护机制的最大支出。安全应该具有成本效益，因此保护某个资产的成本(包括现金或资源)超过其对组织的价值是不明智的。如果控制措施的成本高于资产的价值(即风险的成本)，那么应该接受风险。

在计算控制措施的价值时，涉及许多因素：

- 购买、开发和许可的成本
- 实施和定制的成本
- 年度运营、维护、管理等费用
- 年度修理和升级的成本
- 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，就可以评估将防护措施应用到基础设施的收益。如前所述，防护措施的年度成本不应超过资产的年度损失期望值。

计算防护措施的成本效益 这个过程中的最后计算成本/效益，以确定防护措施能否通过较低成本真正提高安全性。为确定防护措施的支出是否合理，可用下列公式进行计算：

$$\text{防护措施实施前的 ALE} - \text{防护措施实施后的 ALE} = \text{防护措施的年度成本(ACS)}$$

- 防护措施对公司的价值

如果上面计算的结果是负数，防护措施就不具有经济价值，不可接受。如果结果是正数，那么这个值就是组织通过部署防护措施可能获得的年度收益，因为发生的概率并不代表实际会发生。

评估防护措施时，每年节省或消耗的费用不应该是唯一考虑的因素，还应该考虑法律责任和应尽关心原则。某些情况下，因为配置防护措施而损失一些金钱比在资产暴露或损失时承担法律责任更有意义。

回顾一下，要对防护措施进行成本/效益分析，必须计算出以下三个元素：

- 资产与威胁组合在控制措施实施前的 ALE

- 资产与威胁组合在控制措施实施后的 ALE
- ACS(Annual Cost of the Safeguard, 防护措施的年度成本)

有了这些元素，最终可得到针对特定资产的特定风险所采用的特定防护措施的成本/收益计算公式：

$$(控制措施实施前的 ALE - 控制措施实施后的 ALE) - ACS$$

或者更简单：

$$(ALE_1 - ALE_2) - ACS$$

在成本/收益计算中结果值最大的控制措施，就是针对特定资产和威胁组合进行部署的最经济控制措施。表 2.1 给出与定量风险分析相关的各种公式。

表 2.1 定量风险分析公式

概念	公式
暴露因子(EF)	%
单一损失期望(SLE)	$SLE = AV * EF$
年度发生率(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	$(ALE_1 - ALE_2) - ACS$

天啊，这么多数学公式！

是的，定量风险分析包括大量数学运算。考试中的数学题很可能是简单的乘法题。在 CISSP 考试中，最可能遇到的是综合了定义、应用和概念的考题。这意味着需要了解等式/公式和值的含义，它们为什么重要以及如何用来帮助组织。至少需要知道 AV、EF、SLE、ARO、ALE 的概念以及成本/效益计算公式。

认识到可使用定量风险评估过程中计算得到的最终值进行优先级排序和选择是非常重要的。显然，因为在风险评估过程中需要进行猜测、统计分析和概率预测，这些值本身并不能真实反映现实世界中由于安全破坏而造成实际损失或成本。

一旦为影响资产的每种风险计算了每个防护措施的成本/收益，接下来必须对这些值进行排序。大多数情况下，成本/收益最大的就是针对特定资产的特定风险实施的最佳防护措施。但与现实世界中的所有事情一样，这只是决策过程的一部分。虽然成本/收益非常重要，而且通常是主要的指导因素，但并非唯一的元素。其他因素包括实际成本、安全预算、与现有系统的兼容性、IT 人员的技能/知识库、产品的可用性、政治问题、合作伙伴关系、市场趋势、流行时尚、市场营销、合同和倾向。高级管理人员和 IT 人员应通过获取或使用所有可用的数据和信息，为组织做出最佳的安全决策。

大多数组织的预算都是有限的。因此，安全管理中的一个重要部分就是以有限的成本获取最佳的安全。为有效地管理安全功能，必须评估预算、收益和性能指标，以及每个安全控制所需的资源。只有经过彻底评估，才能确定哪些控制是必要的且有收益的。

2. 定性风险分析

定性风险分析更多的是基于场景而不是基于计算，这种方式不用货币价值表示可能的损失，而对威胁进行分级，以评估其风险、成本和影响。由于无法进行纯粹的定量风险评估，因此需要对定量分析的结果进行平衡。将定量分析和定性分析混合使用到组织最终的风险评估过程的方式称为混合评估或混合分析。进行定性风险分析的过程包括判断、直觉和经验。可用多种技术来执行定性风险分析：

- 头脑风暴
- Delphi 技术
- 故事板
- 焦点小组
- 调查
- 问卷
- 检查清单
- 一对一的会议
- 面谈

决定采用哪种机制取决于组织的文化以及涉及的风险和资产的类型。通常会综合使用几种方法，并在提交给高层管理人员的最终风险分析报告中对比各种方法的结果。

场景

所有这些机制的基本过程都需要创建场景。场景是对单个主要威胁的书面描述。重点描述威胁如何产生，以及可能对组织、IT 基础结构和特定资产带来哪些影响。通常，这些场景被限制在一页纸内。对于每个场景，有一种或多种防护措施可完全或部分应对场景中描述的主要威胁。然后，参与分析的人员分配场景的威胁级别、可能的损失和每种安全措施的优点。分配威胁级别时，既可简单使用高、中、低或 1~10 的数字，也可使用详明的文字。然后将所有参与者的反馈汇总成一份报告，交给管理层。有关参考评级的例子，请参阅美国国家标准与技术研究院(NIST)的特殊出版物(SP) 800-30 中的表 3.6 和表 3.7：

<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

定性风险分析的有用性和有效性随着评估参与者的数量和多样性的增加而提高。无论何时，尽可能包括组织层次结构内每个层次中的一个或多个人员，范围从高级管理人员到最终用户。把每个主要部门、办公室或分支机构的交叉人员包括进来也很重要。

Delphi 技术

Delphi 技术可能是上一列表中唯一不能被立即识别和理解的机制。Delphi 技术只是一个匿名的反馈和响应过程，用于在一个小组中匿名达成共识。它的主要目的是从所有参与者中得到诚实而不受影响的反馈。参与者通常聚在一个会议室里，对于每个反馈请求，每个参与者都匿名在纸上写下反馈。反馈结果被汇编并提交给风险分析小组进行评估。这个过程不断重复，直至达成共识。

定量和定性风险分析机制都能提供有用的结果。然而，每种技术都包括评估相同财产和风险的独特方法。精明的应尽关心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 定量风险分析与定性风险分析的比较

特征	定性风险分析	定量风险分析
使用复杂计算	否	是
使用成本/收益分析	否	是
得到具体数值	否	是
需要估算	是	否
支持自动化	否	是
涉及大量信息	否	是
是客观的	否	是
使用主观意见	是	否
需要耗费大量时间和精力	否	是
提供有用和有意义的结果	是	是

2.3.4 风险响应

风险分析的结果如下：

- 所有资产完整的、详细的估值。
- 包括所有威胁和风险、发生概率及造成损失程度的详细清单。
- 针对特定威胁的有效防护措施和控制措施列表。
- 每个防护措施的成本/效益分析。

这些信息至关重要，使管理层能做出实施安全防护措施和变更安全策略的明智决策。

一旦完成风险分析，管理人员必须处理每个特定风险。对风险有以下几种可能的反应：

- 降低或缓解
- 转让或转移
- 接受
- 威慑
- 规避
- 拒绝或忽略

你需要了解关于可能的风险响应的以下信息：

风险缓解(Risk Mitigation) 风险缓解(或风险降低)指通过实施防护措施和控制措施以消除脆弱性或阻止威胁，选择最具成本效益或最有利的控制措施是风险管理的一部分，但不是风险评估的内容。实际上，选择控制措施是风险评估或风险分析后的一项活动。风险缓解的一个可能变体是风险规避，即通过消除风险发生的原因来规避风险。一个简单例子是从服务器删除 FTP 协议以避免攻击；更大的例子是转移到内陆地区来规避飓风带来的风险。

风险转移(Risk Assignment) 风险转移或风险转让指将风险带来的损失转嫁给另一个实体或组织。转让或转移风险的常见形式是购买保险和外包。

风险接受(Risk Acceptance) 风险接受(或风险容忍)指成本/收益分析表明控制措施的成本超过风险的潜在损失。这也意味着管理层已同意接受风险造成的后果和损失。大多数情况下，

接受风险需要进行明确的书面陈述，通常以书面签名形式说明为什么未实施防护措施、谁对决定负责以及如果风险发生谁对损失负责。组织决定是否接受风险取决于组织的风险容忍度。风险容忍度也称为风险偏好。

风险威慑(Risk Deterrence) 风险威慑是对可能违反安全和策略的违规者实施威慑的过程。例如，实施审计、安全摄像头、保安、指导性标识、警告横幅、运动探测器、强制身份证件等措施，并让公众知道该组织愿意与司法部门合作，起诉实施网络犯罪的人。

风险规避(Risk Avoidance) 风险规避是选择替代的选项或活动的过程，替代选项或活动的风险低于默认的、通用的、权宜的或廉价的选项。例如，选择飞往目的地而不是驾车前往是一种规避风险的方式。另一个例子是为了避免飓风的风险，在亚利桑那州而不是佛罗里达州建立企业。

风险拒绝(Risk Rejection) 最后一个对风险的可能响应是拒绝或忽视。否认风险的存在并希望永远不会发生，并不是合法的、正确的风险响应方式。

一旦采取了控制措施，余下的风险就称为残余风险。残余风险是针对特定资产的威胁，高级管理人员选择不实施防护措施。换句话说，残余风险是管理层选择接受而不去减轻的风险。大多数情况下，残余风险的存在表明：成本/效益分析显示现有的防护措施并不具有成本效益。

总风险指在没有实施防护措施的情况下组织面临的全部风险。总风险的计算公式如下：

$$\text{威胁} * \text{脆弱性} * \text{资产价值} = \text{总风险}$$

注意这里的*并不表示乘法，只起联合作用，这不是一个真正的数学公式。总风险和残余风险的差额称为控制间隙。控制间隙指通过实施保障措施而减少的风险。残余风险的计算公式如下：

$$\text{总风险} - \text{控制间隙} = \text{残余风险}$$

风险处理与风险管理一样，都不是一次性过程。相反，安全必须持续维护和重复确定。事实上，重复进行风险评估和分析过程是评估安全计划的完整性和有效性的一种机制，也有助于定位缺陷和发生变化的区域。因为随着时间的推移，安全会发生变化，所以定期重新评估对于维护恰当的安全至关重要。

2.3.5 选择与实施控制措施

在风险管理领域中选择控制措施或安全控制在很大程度上依赖于成本/收益分析结果。然而，在评估安全控制的价值或相关性时，还需要考虑以下因素：

- 控制措施的成本应该低于资产的价值。
- 控制措施的成本应该低于控制措施的收益。
- 应用控制措施的结果应使攻击者的攻击成本高于攻击带来的收益。
- 控制措施应该为真实的和明确的问题提供解决方案(不要仅因为它们是可用的、被宣传的或听起来很酷就实施控制措施)。
- 控制措施的好处不应依赖于对其保密。这意味着“通过隐匿实现安全”不可行，任何可行的控制措施都能经得起公开披露和审查。
- 控制措施的收益应当是可检验和可验证的。

- 控制措施应在所有用户、系统、协议之间提供一致的保护。
- 控制措施应该几乎(或完全)没有依赖项，以减少级联故障。
- 完成初始部署和配置后，控制措施只需要最低限度的人为干预。
- 应该防止篡改控制措施。
- 只有拥有特权的操作员才能全面访问控制措施。
- 应当为控制措施提供故障安全和/或故障保护选项。

记住，安全应该被设计成支持和保障业务的任务和功能。因此，需要在业务任务的上下文中评估控制措施和防护措施。

安全控制、控制措施和防护措施可以是管理性、逻辑性/技术性或物理性的。这三种安全机制应以纵深防御方式实现，以提供最大收益(见图 2.6)。

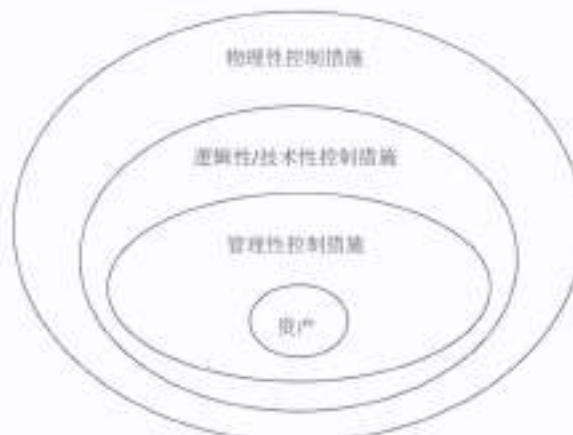


图 2.6 纵深防御中实施的安全控制分类

1. 技术性控制措施

技术性或逻辑性控制措施包括硬件或软件机制，可用于管理访问权限以及为系统和资源提供安全保护。顾名思义，就是使用技术。逻辑性或技术性控制措施的例子包括身份验证方法(如用户名、密码、智能卡和生物识别技术)、加密、限制接口、访问控制列表、协议、防火墙、路由器、入侵检测系统(IDS)和阈值级别。

2. 管理性控制措施

管理性控制措施是依组织的安全策略和其他法规或要求而规定的策略和程序。它们有时称为管理控制。这些控制集中于人员和业务实践。管理性控制措施的例子包括策略、程序、招聘实践、背景调查、数据分类、数据标签、安全意识培训、休假记录、报告和审查、工作监督、人员控制和测试。

3. 物理性控制措施

物理性控制措施是可实际接触到的措施，包括阻止、监测或检测对基础设施内系统或区域的直接接触的物理性控制措施。物理性控制措施的例子包括保安、栅栏、动作探测器、上锁的门、密封的窗户、灯、电缆保护、笔记本电脑锁、徽章、刷卡、看门狗、摄像机、陷阱和报警器。

2.3.6 适用的控制类型

术语“安全控制”指执行广泛控制，确保只有授权用户可登录和防止未授权用户访问资源等。安全控制可降低各种信息安全风险。

无论何时，都希望阻止发生任何类型的安全问题或事件。但防不胜防，总会发生意外事件。一旦有事件发生，就希望能尽快检测到事件。一旦可检测到事件，就想要纠正它们。

当阅读控制措施描述时，会发现列出的有些安全控制示例不止出现在一种安全控制类型中。例如，建筑物周围设置的围栏可以是预防控制(物理上阻止某人进入建筑物)和/或威慑控制(阻止某人尝试进入)。

1. 威慑控制

部署威慑控制以阻止违反安全策略。威慑控制和预防控制是类似的，但威慑控制往往取决于个人决定不采取不必要的行动。相比之下，预防控制实际上阻碍了行动。威慑控制的例子包括策略、安全意识培训、锁、栅栏、安全标识、保安、陷阱和安全摄像头。

2. 预防控制

部署预防控制以阻挠或阻止非预期的或未经授权的活动的发生。预防控制的例子包括栅栏、锁、生物识别技术、陷阱、灯光、报警系统、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、智能卡、回滚程序、安全策略、安全意识培训、杀毒软件、防火墙和入侵预防系统(IPS)。

3. 检测控制

部署检测控制以发现或检测非预期的或未经授权的活动。检测控制并非实时进行，而是在活动发生后才运行。检测控制的例子包括保安、移动探测器、记录和审查安全摄像头或闭路电视捕捉到的事件、岗位轮换、强制休假、审计踪迹、蜜罐或蜜网、入侵检测系统(IDS)、违规报告、对用户的监督和审查以及事件调查。

4. 补偿控制

补偿控制用于为其他现有的控制提供各种选项，从而帮助增强和支持安全策略。补偿控制可以是一些其他的控制或现有控制的另一个替换。例如，组织策略可能要求所有数据都必须加密。审查发现，预防控制在数据库中加密所有数据，但通过网络传输的是明文。可添加补偿控制来保护传输中的数据。

5. 纠正控制

纠正控制会修改环境，把系统从发生的非预期的或未经授权的活动中恢复到正常状态。纠正控制试图纠正安全事故引发的任何问题。纠正控制可以是简单的，例如终止恶意活动或重新启动系统。也可包括删除或隔离病毒的杀毒解决方案、用于确保数据丢失后可以恢复的备份和恢复计划，以及能修改环境以阻止正在进行的攻击的活动。安全策略被破坏后，可部署纠正控制以修复或恢复资源、功能和能力。

6. 恢复控制

恢复控制是纠正控制的扩展，但具有更高级、更复杂的能力。恢复控制的例子包括备份和恢复、容错驱动系统、系统镜像、服务器集群、杀毒软件、数据库或虚拟机镜像。对于业务连续性和灾难恢复，恢复控制可包括热站点、温站点、冷站点、备用处理设施、服务机构、互惠协议、云服务供应商、流动移动操作中心和多站点解决方案。

7. 指示控制

指示控制用于指导、限制或控制主体的行为，以强制或鼓励遵守安全策略。指示控制的例子包括安全策略要求或标准、发布的通知、逃生路线出口标志、监控、监督和程序。

2.3.7 安全控制评估

安全控制评估(Security Control Assessment, SCA)是根据基线或可靠性期望对安全基础设施的各个机制进行的正式评估，可作为渗透测试或漏洞评估的补充内容，或作为完整的安全评估被执行。

SCA 的目标是确保安全机制的有效性，评估组织风险管理过程的质量和彻底性，并生成已部署的安全基础设施相对优缺点的报告。

通常，SCA 是 NIST 特别出版物 800-53A(“联邦信息系统中的安全控制评价指南”的过程。然而，虽然被定义为政府过程，但对每个致力于维持成功的安全成果的组织来说，评估安全控制的可靠性和有效性的概念都应该被采纳。

2.3.8 监视和测量

安全控制提供的收益应该是可被监视和测量的。如果安全控制提供的收益无法被量化、评估或比较，那么这种控制实际上没有提供任何安全。安全控制可能提供本地或内部监视，或者可能需要外部监视。在选择初步控制措施时，应该考虑到这一点。

许多控制措施提供了一定程度的改善而不是具体的关于防止破坏或阻止攻击的数量。通常为了测量控制措施的成败，在安全措施执行前后进行监视和记录是十分必要的。只有知道了起点(即正常点或初始风险水平)，才能准确地衡量收益。

成本/收益分析公式中有一部分也考虑到控制措施的监视和测量。安全控制在一定程度上增强安全性，但未必意味着所获得的收益是合算的。应识别出安全方面的重大改进来清楚地证明部署新控制措施的花费是合理的。

2.3.9 资产估值与报告

风险分析的一个重要步骤是估算组织资产的价值。资产如果没有价值，就没必要为其提供保护。风险分析的主要目标是确保只部署具有成本效益的防护措施。花 10 万美元保护价值仅 1000 美元的资产是没有意义的。资产的价值直接影响和引导为保护资产而部署的防护措施和安全水平。一般来说，防护措施的年度成本不应超过资产的年度损失期望。

评估资产成本时，需要考虑许多方面。评估资产的目标是为资产分配具体的货币价值，既包括有形的成本，也包括无形的成本。确定资产的精确价值通常是很困难或不可能的，尽管如此，具体的价值必须被确定(可参见前面关于定性风险分析和定量风险分析的讨论)。不适当当地给资产赋值可能导致不能适当地保护资产或实施财务上不合算的防护措施。下列出一些有助于估算有形资产和无形资产的事项：

- 采购成本
- 开发成本
- 行政或管理成本
- 维护或保养费用
- 获得资产的成本
- 保护或维持资产的成本
- 对所有者和用户的价值
- 对竞争对手的价值
- 知识产权或股票价值
- 市场估值(可持续的价格)
- 重置成本
- 生产率的提高或下降
- 资产存在和损失的运营成本
- 资产损失责任
- 有用性

为组织分配或确定资产的价值可以满足许多要求。资产估值是通过部署防护措施实现资产保护的成本/收益分析的基础，是选择或评估防护措施和控制措施的一种手段。能根据资产估值来购买保险，并为组织确定总体的净资产或净值，有助于高级管理人员准确了解组织中存在的风险。了解资产的价值还有助于防止未给予应尽关心，并促进遵守法律要求、行业法规和内部安全策略。

风险报告是风险分析的最后一项关键任务。风险报告包括编制风险报告，并将该报告呈现给利益相关方。对于许多组织来说，风险报告只作为内部参考，而其他的一些组织可能规定必须向第三方或公众报告他们的风险结果。

风险报告应能准确、及时、全面地反映整个组织的情况，能清晰和准确地支持决策的制定，并定期更新。

2.3.10 持续改进

风险分析旨在向高级管理层提供必要的详细信息，以决定哪些风险应该被缓解，哪些应该被转移，哪些应该拒绝，哪些应该被规避，哪些应该被接受。其结果就是对资产的预期损失成本和部署应对威胁及脆弱性的安全措施成本进行成本/收益分析比较。风险分析可识别风险，量化威胁的影响，并帮助编制安全预算，还有助于将安全策略的需求和目标与组织的业务目标和宗旨相结合。风险分析/风险评估是一种“时间点”度量。威胁和脆弱性不断变化，风险评估需要定期进行以支持持续改进。

安全在不断变化。因此，随着时间的推移，任何已实施的安全解决方案都需要进行更新。如果已使用的控制措施不能持续改进，则应该将其替换，从而为安全提供可扩展的改进控制措施。

2.3.11 风险框架

风险框架是关于如何评估、解决和监控风险的指南或方法。考试提到的有关风险框架的主要案例是由特别刊物 800-37 给出的定义(<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf>)。鼓励大家完整阅读这篇文章，以下是该出版物中相关内容的摘录：

该特别出版物为在联邦信息系统中实施风险管理框架(Risk Management Framework, RMF)提供了指导方针。RMF 包括 6 个步骤：安全分类、选择安全控制、实施安全控制、评估安全控制、授权信息系统和监视安全控制。风险管理框架通过实施强劲且持续的监视过程，促进实时风险管理与持续的信息系统授权概念的实施；向高层管理人员提供必要的信息，以便对组织信息系统做出基于风险且成本有效的决策来支持其核心任务和业务功能，并将信息安全集成到企业体系结构和系统开发生命周期(System Development Lifecycle, SDLC)中。强调安全控制的选择、实施、评估和监测以及信息系统的授权。在企业内实施风险管理框架可通过风险管理职能部门，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关联起来，为部署在组织信息系统中并被这些系统使用的安全控制(如通用控制)建立责任和问责一体化制度。

RMF 步骤如图 2.7 所示。

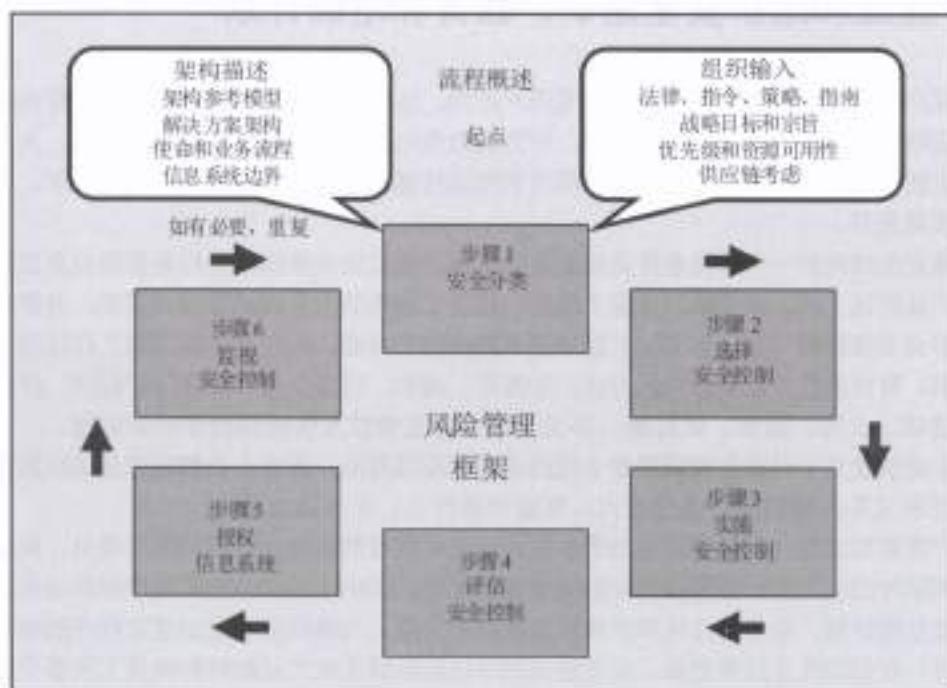


图 2.7 风险管理框架的六个步骤

- 对信息系统和根据影响分析将被该系统处理、存储和传输的数据进行分类。

- 基于安全分类为信息系统选择初始化安全控制基线，基于组织对风险和现场情况的评估，根据需要调整和补充安全控制基线。
- 实施安全控制并描述如何在信息系统及其操作环境中使用安全控制。
- 使用适当的评估程序对安全控制进行评估，来确定安全控制在多大程度上得到了正确实施、完成了预期操作并产生符合系统安全要求的期望结果。
- 基于对组织运营和信息系统操作涉及的资产、个人、其他组织和国家的风险决策，对信息系统操作进行授权，并确定风险是可以接受的。
- 持续监视信息系统中的安全控制，包括评估控制的有效性，记录系统或其运行环境的变化，对相关变化进行安全影响分析，并向指定的组织管理人员报告系统的安全状态。在特别出版物中有更多关于的细节，请查阅该文档以便全面了解整个风险框架。

尽管考试的主要重点是 NIST 风险管理框架，但你可能需要了解现实世界中使用的其他风险管理框架。请考虑可操作的关键威胁、资产和脆弱性评估(Operational Critical Threat, Asset, and Vulnerability Evaluation, OCTAVE)、信息风险因素分析(Factor Analysis of Information Risk, FAIR)和威胁代理风险评估(Threat Agent Risk Assessment, TARA)。若要进一步研究，可参考这篇有价值的文章：www.csoonline.com/article/2125140/metrics-budgets/it-riskassessment-frameworks-real-world-experience.html。理解当前存在许多被公共认可的框架并选择一个符合组织需求和风格的框架是非常重要的。

2.4 建立和维护安全意识、教育和培训计划

为成功实施安全解决方案，必须改变用户行为。这些改变主要包括改变常规工作活动以符合安全策略中规定的标准、指南和程序。行为的改变包括用户完成一定层次的学习。为开发和管理安全教育、培训和意识，所有相关项目知识传递都必须明确标识，并制定展示、公开、协同和实施程序。

实施安全培训的一个前提条件是建立安全意识。建立安全意识的目标是要将安全放到首位并让用户认可这一点。安全意识在整个组织中建立了通用的安全理解基线或基础，并聚焦于所有员工都必须理解的与安全相关的关键或基本的内容和问题。可在课堂练习和工作环境中建立安全意识。有许多建立安全意识的方法，如海报、通知、时事文章、屏幕保护程序、经理在集会上的讲话、公告、演讲、鼠标垫、办公用品、备忘录以及传统的教学培训课程。

安全意识建立了对安全理解的最小化的通用标准或基础。所有人员都应充分认识到自身的安全责任和义务。他们应该接受培训，知道该做什么，不该做什么。

用户需要知道的问题包括避免浪费、欺诈和未经授权的活动。组织的所有成员，从高级管理人员到临时的实习生，都需要同样的安全意识水平。组织中的安全意识程序应该与其安全策略、事故处理计划、业务连续性和灾难恢复程序相关联。为确保安全意识建立程序的有效性，必须及时、有创造性且经常更新。安全意识程序还应理解企业文化如何影响员工及整个组织的安全。如果员工没有看到安全策略和标准的实施，特别是没有意识到这个问题，那么他们可能就不觉得有义务遵守这些策略和标准。

培训是教导员工执行他们的工作任务和遵守安全策略。培训通常由组织主办，面向具有类似工作职能的员工群体。所有新员工都需要某种程度的培训以便他们能够遵守安全策略中规定

的所有标准、指南和程序。新用户需要知道如何使用基础设施、数据存储在哪里以及为什么要对资源进行分类。许多组织选择在授权新员工访问网络前对他们进行培训，而其他一些组织则会在新用户完成特定工作岗位的培训前只给他们有限的访问权限。培训是一项需要持续进行的活动，每个员工在工作期间都必须持续接受培训。培训是一种管理性安全控制。

随着时间的推移，开展安全意识和培训的方法和技术都应得到修订和改进以便最大限度地提高收益。这需要对培训指标进行收集与评估，可能包括学习后的测试，也包括监控工作一致性的改进，以及停机时间、安全事件或错误的降低。这可以看作一种程序有效性评估。

安全意识和培训通常是内部提供的，这意味着这些教学工具都在组织内创建和部署。然而，下一个知识传播层次通常是从外部第三方获得的。

教育是一项更详细的工作，学生/用户学习的内容比完成他们的工作任务实际需要知道的内容多得多。教育最常与用户参加认证或寻求工作晋升关联。教育是个人成为安全专家的典型要求。安全专业人员需要掌握大量的安全知识并对整个组织的本地环境有广泛的了解，而不仅是了解他们的具体工作任务。

应采用周期性内容评审的方式，定期对组织内所需的意识、培训和教育恰当程度进行评估。培训工作需要随着组织的发展进行更新和调整。

此外，应该采用新颖的思维方式，保持内容的新鲜感和相关性。如果不能定期检查内容的相关性，内容就会过时而不适用，员工可能倾向于自己制定的指南和程序。安全治理团队的责任是建立安全策略，并为进一步实施这些策略提供培训和教育。

2.5 管理安全功能

要管理安全功能，组织必须实现适当和充分的安全治理。执行风险评估以驱动安全策略的行为是安全功能管理最显著和最直接的示例。

安全必须是成本有效的。组织的预算有限，因此必须合理地分配资金。此外，组织预算需要包括用于安全方面的费用比例，这与大多数其他业务任务和流程需要的资金类似，不只包括员工酬劳、保险费、退休金等。安全应该足以抵御组织的典型或标准的威胁，但如果保护措施的成本高于资产本身的价值，那通常就不是有效的解决方案。

安全必须是可测量的。可测量的安全意味着安全机制的各方面功能提供了明确收益，并有一个或多个可记录和分析的指标。与性能指标类似，安全指标是与安全特性相关的功能、操作、行动等指标。当实施了控制措施或防护措施时，安全指标应该表示为意外事件的减少或检测到攻击次数的增加。否则，安全机制就没有实现预期的收益。测量和评估安全指标的行为是评估安全程序的完整性和有效性的实践，这应该包括评测通用安全指南和追踪控制的成功案例。追踪和评估安全指标是确保安全治理有效的一部分工作。然而，值得注意的是，如果选择的安全指标不正确，则可能导致严重问题，例如选择监视或测量安全人员无法控制的事物或基于外部驱动的事物。

安全机制本身与安全治理过程都会消耗资源。显然，安全机制应消耗尽可能少的资源，尽量降低对生产效率或系统吞吐量的影响。然而，所有硬件和软件的控制措施以及用户必须遵循的各项策略和程序都会消耗资源。在选择、部署和调优控制措施前后都要意识到并评估资源消耗，这也是安全治理和管理安全功能的重要组成部分。

安全管理功能包括信息安全策略的开发和实现。考试的大部分内容涉及信息安全策略开发与实施的方方面面。

2.6 本章小结

在规划安全解决方案时，重要的是要考虑到这样一个事实，即人通常是组织安全中最薄弱的环节。无论部署了什么物理的或逻辑的控制措施，人都可以找到方法来规避、绕过或消除它们，或使控制措施失效。因此，在环境设计和部署安全解决方案时，必须将用户的因素考虑进去。安全的招聘实践、角色、策略、标准、指南、程序、风险管理、意识培训和管理计划都有助于保护资产。使用这些安全结构能在一定程度上防止人为威胁。

安全的招聘实践需要详细的职责描述。职责描述可作为选择候选人和评估他们是否符合职位的指南。可通过在职责描述中使用职责分离、工作责任和岗位轮换来维护安全。

为保护组织和现有的员工，需要有解雇策略。

解雇程序应包括有证人在场、归还公司财产、禁止网络访问、离职面谈和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、合同义务或许可要求强制规定的监督制度。实际的治理方法可能有所不同，但通常包括外部调查员或审计人员。这些审计人员可能由监管机构指定，也可能是目标组织雇用的顾问。

识别、评估和阻止或减轻风险的过程称为风险管理。风险管理的主要目标是将风险降低到可接受的水平。可接受水平的确定取决于组织、资产价值和预算规模。设计和实施一个完全没有风险的环境是不可能的，但通过较少努力就显著降低风险却是可能的。风险分析是实现风险管理目标的过程，包括分析环境中存在的风险，评估每个风险发生的可能性和造成的损失，评估应对每个风险的各种控制措施的成本，创建防护措施成本收益报告并提交给高层管理人员。

为成功实施安全解决方案，必须改变用户行为。这些改变包括改变常规工作活动乃至遵守安全策略中规定的标准、指南和程序。行为的改变包括用户完成一定层次的学习。常见有三种公认的学习层次：安全意识、培训和教育。

2.7 考试要点

理解雇用新员工对安全的影响。为实施恰当的安全计划，必须为职责描述、职位分类、工作任务、工作职责、防止串通、候选人筛选、背景调查、安全许可、雇佣协议和保密协议等设立标准。通过采用这些机制，可确保新员工了解所需的安全标准，从而保护组织的资产。

能够解释职责分离。职责分离的概念是将关键的、敏感的工作任务划分给多个人员。通过以这种方式划分职责，可确保没有能够危害系统安全的个人。

理解最小特权原则。最小特权原则要求在安全的环境中，用户应获得完成工作任务或工作职责所需的最小访问权限。通过将用户的访问限制在他们完成工作任务所需的资源上，就可以限制敏感信息的脆弱性。

了解岗位轮换和强制休假的必要性。岗位轮换有两个功能。它提供了一种知识备份，岗位

轮换还可以降低欺诈。数据修改、盗窃、破坏和信息滥用的风险。

为了审计和核实员工的工作任务和特权，可使用一到两周的强制休假。强制休假能够轻易发现特权滥用、欺诈或疏忽。

理解供应商、顾问和承包商的控制。供应商、顾问和承包商的控制用来确定组织主要的外部实体、人员或组织的绩效水平、期望、薪酬和影响。通常，这些控制条款在 SLA 文档或策略中规定。

能够解释恰当的解雇策略。解雇策略规定解雇员工的程序，应该包括有现场证人、禁用员工的网络访问权限和执行离职面谈等内容。解雇策略还应包括护送被解雇员工离开公司，并要求归还安全令牌、徽章和公司财产。

了解隐私如何适合于安全领域。了解隐私的多重含义/定义，为什么保护隐私很重要，以及工作环境中与隐私相关的问题。

能够讨论第三方安全治理。第三方安全治理是由法律、法规、行业标准、合同义务或许可要求强制规定的监督制度。

能够定义整体的风险管理。风险管理过程包括识别可能造成数据损坏或泄露的因素，根据数据价值和控制措施的成本评估这些因素，并实施具有成本效益的解决方案来减轻风险。通过执行风险管理，为全面降低风险奠定基础。

理解风险分析和相关要素。风险分析是向高层管理人员提供详细信息以决定哪些风险应该缓解，哪些应该转移，哪些应该接受的过程。要全面评估风险并采取适当的预防措施，必须分析以下内容：资产、资产价值、威胁、脆弱性、暴露、风险、已实现风险、防护措施、控制措施、攻击和侵入。

知道如何评估威胁。威胁有许多来源，包括人类和自然。以团队形式评估威胁以便提供最广泛的视角。通过从各个角度全面评估风险可降低系统的脆弱性。

理解定量风险分析。定量风险分析聚焦于货币价值和百分比。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。定量风险分析包括资产估值和威胁识别，然后确定威胁的潜在发生频率和造成的损害，结果是防护措施的成本/效益分析。

能够解释暴露因子(EF)概念。暴露因子是定量风险分析的一个元素，表示如果已发生的风险对组织的某个特定资产造成破坏，组织将因此遭受的损失百分比。通过计算风险暴露因子，就能实施良好的风险管理策略。

了解单一损失期望(SLE)的含义和计算方式。SLE 是定量风险分析的一个元素，代表已发生的单个风险给特定资产带来的损失。计算公式为： $SLE = \text{资产价值}(AV) * \text{暴露因子}(EF)$ 。

理解年度发生率(ARO)。ARO 是量化风险分析的一个元素，代表特定威胁或风险在一年内发生(或实现)的预期频率。进一步了解可帮助计算风险并采取适当的预防措施。

了解年度损失期望(ALE)的含义和计算方式。ALE 是定量风险分析的一个元素，指的是针对特定资产的所有可发生的特定威胁，在年度内可能造成的损失成本。计算公式为： $ALE = \text{单一损失期望}(SLE) * \text{年度发生率}(ARO)$ 。

了解评估防护措施的公式。除了确定防护措施的年度成本外，还需要为资产计算防护措施实施后的 ALE。可使用这个计算公式：防护措施实施前的 ALE - 防护措施实施后的 ALE - 防护措施的年度成本 = 防护措施对公司的价值，或 $(ALE_1 - ALE_2) - ACS$ 。

理解定性风险分析。定性风险分析更多的是基于场景而不是基于计算。这种方式不用货币价值表示可能的损失，而对威胁进行分级，以评估其风险、成本和影响。这种分析方式可帮助

那些负责制定适当的风险管理策略的人员。

理解 Delphi 技术。Delphi 技术是一个简单的匿名反馈和响应过程，用来达成共识。这样的共识让各责任方有机会正确评估风险并实施解决方案。

了解处理风险的方法。风险降低(即风险缓解)就是实施防护措施和控制措施。风险转让或风险转移是将风险造成的损失成本转嫁给另一个实体或组织；购买保险是风险转移的一种形式。风险接受意味着管理层已经对可能的防护措施进行了成本/效益分析，并确定了防护措施的成本远大于风险可能造成的损失成本。这也意味着管理层同意承担风险发生后的结果和损失。

能够解释总风险、残余风险和控制间隙。总风险是指如果不实施防护措施，组织将面临的风险。可用这个公式计算总风险：威胁*脆弱性*资产价值=总风险。残余风险是管理层选择接受而不再进行减轻的风险。总风险和残余风险之间的差额是控制间隙，即通过实施防护措施而减少的风险。残余风险的计算公式为：总风险-控制间隙=残余风险。

理解控制类型。术语“控制”指广泛控制，执行诸如确保只有授权用户可以登录和防止未授权用户访问资源等任务。控制类型包括预防、检测、纠正、威慑、恢复、指示和补偿控制。控制也可分为管理性、逻辑性或物理性控制。

了解如何实施安全意识培训。在接受真正的培训前，必须让用户树立已认可的安全意识。一旦树立了安全意识，就可以开始培训或教导员工执行他们的工作任务并遵守安全策略。所有新员工都需要一定程度的培训以便他们遵守安全策略中规定的标准、指南和程序。教育是一项更详细的工作，学生/用户学习的内容比他们完成工作任务实际需要知道的要多得多。教育通常与用户参加认证或寻求工作晋升关联。

理解如何管理安全功能。为管理安全功能，组织必须实现适当和充分的安全治理。通过风险评估来驱动安全策略的实施是最明显、最直接的管理安全功能的实例。这也与预算、测量、资源、信息安全策略以及评估安全计划的完整性和有效性相关。

了解风险管理框架的六个步骤。风险管理框架的六个步骤是：安全分类、选择安全控制、实施安全控制、评估安全控制、授权信息系统和监视安全控制。

2.8 书面实验

1. 列出 6 种用于保证人员安全的不同管理性控制措施。
2. 定量风险评估用到的基本计算公式有哪些？
3. 描述在定性风险评估中用于达成匿名共识的过程或技术。
4. 讨论进行“平衡的风险评估”的需求。可使用哪些技术？为什么需要这样做？

2.9 复习题

1. 下列哪一项是所有安全解决方案中最薄弱的环节？

- A. 软件产品
- B. 互联网连接
- C. 安全策略

- D. 人员
2. 招聘新员工的第一步是什么?
- A. 创建职责描述
 - B. 设置职位分类
 - C. 筛选候选人
 - D. 申请简历
3. 下列哪一项是离职面谈的主要目的?
- A. 退还离职员工的个人财物。
 - B. 审查保密协议。
 - C. 评估离职员工的工作表现。
 - D. 取消离职员工的网络访问账户。
4. 当一名雇员要被解雇时,下列哪一项是应该做的?
- A. 在正式解雇前几小时通知该员工。
 - B. 一旦通知员工被解雇,就禁用员工的网络访问权限。
 - C. 群发电子邮件,通知所有人员该员工将被解雇。
 - D. 等到仅有你和那名员工在办公室的时候,再宣布解雇。
5. 如果一个组织与外部实体签订合同来获得关键的业务功能或服务,例如账户或技术支持,那么可使用什么过程来确保这些外部实体支持充分的安全性?
- A. 资产识别
 - B. 第三方治理
 - C. 离职面谈
 - D. 定性分析
6. _____的一部分是对业务流程和组织策略的逻辑和实际调查。这个过程/策略审查确保声明与实现的业务任务、系统和方法是实用的、高效的和具有成本效益的,但最重要的是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. 选择控制措施
 - D. 文件审查
7. 下列哪一项不正确?
- A. IT 安全性只能提供针对逻辑或技术性攻击的保护
 - B. 实现风险管理目标的过程称为风险分析
 - C. 基础设施的风险都是基于计算机的
 - D. 资产是业务流程或任务中使用的任何事物
8. 下列哪一项不是风险分析过程的要素?
- A. 分析环境中存在的风险
 - B. 创建防护措施的成本/收益报告并提交给高层管理人员
 - C. 选择适当的防护措施并加以实施
 - D. 评估每一个威胁事件发生的可能性和造成的损失

9. 在风险分析中，下列哪一项通常不被认为是资产？
 - A. 开发过程
 - B. 基础架构
 - C. 专有系统资源
 - D. 用户个人文件
10. 下列哪一项代表意外或故意地利用脆弱性？
 - A. 威胁事件
 - B. 风险
 - C. 威胁主体
 - D. 破坏
11. 当防护措施或控制措施缺失或存在不足时，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. 对概率、可能性或机会的评估。
 - B. 任何消除脆弱性或免受一个或多个特定威胁的东西。
 - C. 风险=威胁*脆弱性。
 - D. 每一个暴露实例。
13. 在评估防护措施时，大多数情况下应遵守的规则是什么？
 - A. 资产年度损失期望不应超过防护措施的年度成本。
 - B. 防护措施的年度成本应与资产价值相等。
 - C. 防护措施的年度成本不应超过资产年度损失期望。
 - D. 防护措施的年度成本不应超过安全预算的 10%。
14. 如何计算单一损失期望(SLE)？
 - A. 威胁+脆弱性
 - B. 资产价值(S)*暴露因子
 - C. 年度发生率*脆弱性
 - D. 年度发生率*资产价值*暴露因子
15. 如何计算公司防护措施的价值？
 - A. 防护措施实施前的 ALE-防护措施实施后的 ALE-防护措施年度成本
 - B. 防护措施实施前的 ALE*防护措施的 ARO
 - C. 防护措施实施后的 ALE+防护措施的年度成本-控制间隙
 - D. 总风险-控制间隙
16. 什么样的安全控制措施直接关注于防止串通？
 - A. 最小特权原则
 - B. 职责描述
 - C. 职责分离
 - D. 定性风险分析

17. 什么样的过程或事件通常由组织主持并针对具有类似工作职能的员工群体?

- A. 教育
- B. 意识
- C. 培训
- D. 解雇

18. 下列哪一项与管理组织的安全功能没有具体或直接的关系?

- A. 员工工作满意度
- B. 指标
- C. 信息安全战略
- D. 预算

19. 在进行风险分析时, 因为缺少灭火器, 你认为具有发生火灾的威胁和脆弱性。根据这些信息, 下列哪一项是可能出现的风险?

- A. 病毒感染
- B. 设备损坏
- C. 系统故障
- D. 未经授权访问机密信息

20. 你已经对特定的威胁/脆弱性/风险关系进行了基本的定量风险分析, 并选择了一种可行的控制措施。当再次进行计算时, 下列哪个因素会发生变化?

- A. 暴露因子
- B. 单一损失期望(SLE)
- C. 资产价值
- D. 年度发生率

业务连续性计划

本章涵盖的 CISSP 认证考试主题包括：

- ✓ 域 1：安全与风险管理
 - 1.7 业务连续性(BC)需求的识别、分析与优先级排序
 - 1.7.1 制定并记录范围和计划
 - 1.7.2 业务影响评估(BIA)
- ✓ 域 7：安全运营
 - 7.14 参与业务连续性计划和演练

不管我们的愿望有多么美好，总会有这样或那样的灾难降临到每个组织。无论是飓风或地震等自然灾害还是建筑物着火或水管爆裂等人为灾难，每个组织都可能遇到威胁其运营甚至生存的事件。

有弹性的组织会制定计划和程序以帮助减轻灾难对持续运营的影响，并加速恢复到正常运营状态。^{(ISC)²}认识到业务连续性(Business Continuity, BC)计划和灾难恢复(Disaster Recovery, DR)计划的重要性，将这两个过程包含到 CISSP 认证考试的 CBK 中。理解这些基础性主题有助于备考 CISSP 认证考试，也有助于组织应对意外事件。

本章将探讨业务连续性计划(BCP)背后的概念。第 18 章将继续讨论和探究组织在遭受灾难袭击后，可采取的尽快恢复到正常运营的技术控制细节。

3.1 业务连续性计划简介

业务连续性计划(Business Continuity Plan, BCP)涉及评估组织流程的风险，并创建策略、计划和程序，以最大限度地降低这些风险发生时对组织产生的不良影响。BCP 用于在紧急情况下维持业务的连续运营。BCP 计划者的目标是通过综合实施策略、程序和流程，将潜在的破坏性事件对业务的影响降至最低。

BCP 专注于在降低的或受限的基础设施能力或资源上维持业务运营。只要能继续维持组织执行关键工作任务的能力，就可以利用 BCP 管理和恢复生产环境。

业务连续性计划与灾难恢复计划

CISSP 考生常对业务连续性计划(BCP)和灾难恢复计划(Disaster Recovery Planning, DRP)之间的差异感到困惑，可能尝试对二者排序，或尝试划清界限。真实情况是，这些界限在现实中是模糊的，不适合把它们分为完全不同的类别。

二者之间的区别在于视角。这两项活动旨在帮助组织应对灾难，目标是在可能的情况下，保持业务持续运行，并在中断后尽快恢复运营。视角差异在于：业务连续性计划通常战略性地关注上层，以业务流程和运营为中心；灾难恢复计划本质上更具战术性，描述恢复站点、备份和容错等技术活动。

无论如何，不要纠结于二者之间的差异。我们还没有看到哪个考试题目迫使人们严格区别这两项活动。理解这两个相关领域所涉及的流程和技术更重要。

你将在第 18 章中了解关于灾难恢复计划的更多内容。

BCP 的总体目标是在紧急情况下提供快速、冷静和有效的响应，提高公司从破坏性事件中快速恢复的能力。BCP 流程有四个主要阶段：

- 项目范围和计划
- 业务影响评估
- 连续性计划
- 计划批准和实施

接下来将详细介绍这些阶段。最后一节将介绍在编制组织的业务连续性计划文档时应考虑的一些要素。



提示：

人员安全一直是 BCP 和 DRP 最先考虑的。先让人们远离伤害，然后才能完成 IT 恢复和问题修复。

3.2 项目范围和计划

与任何正式业务流程一样，制定强大的业务连续性计划需要使用成熟的方法。要求如下：

- 从危机规划的角度对业务组织进行结构化分析。
- 在高级管理层的批准下创建 BCP 团队。
- 评估可用于业务连续性活动的资源。
- 分析在处理灾难性事件方面，组织需要遵守的法律以及所处的监管环境。

具体流程取决于组织及其业务的规模和性质。业务连续性计划没有“放之四海而皆准”的指南。你应咨询组织内的项目规划专业人员，并根据组织文化确定最有效的方法。

3.2.1 业务组织分析

负责业务连续性计划的人员的首要职责之一是对业务组织进行分析，以识别与 BCP 流程具有利害关系的所有部门和个人。需要考虑的范围如下：

- 负责向客户提供核心服务业务的运营部门。
- 关键支持服务部门(如 IT 部门)、设施和维护人员以及负责维护支持运营系统的其他团队。
- 负责物理安全的公司安全团队，他们在多数情况下是安全事故的第一响应者，也负责主要基础设施和备用处理设施的物理保护。
- 高级管理人员和对组织持续运营来说至关重要的其他人员。

出于以下两个原因，这个识别过程非常重要。首先，它完成了确定 BCP 团队潜在成员所需的基础工作(见下一节)。其次，为在 BCP 过程中开展其他工作打下了基础。

通常，业务组织分析由负责 BCP 工作的人员执行。这是做法是被认可的，因为他们通常使用分析结果来协助选择 BCP 团队的其他成员。不过，整个 BCP 团队成立后要完成的第一项任务是对分析结果进行一次全面审查。这一步非常关键，因为执行原始分析的人员可能忽略了某些关键业务功能，而 BCP 团队中其他成员却对这些内容非常了解。如果 BCP 团队未能修正存在错误的分析结果，整个 BCP 流程将受到负面影响，导致制定的业务连续性计划无法完全满足整个组织的应急响应需求。



提示：

制定业务连续性计划时，务必考虑总部和所有分支机构。该计划应考虑到组织开展业务的任何地点可能发生的灾难。

3.2.2 选择 BCP 团队

在许多组织中，IT 和/或安全部门负责 BCP 的所有工作，不从其他运营和支持部门获得输入信息。事实上，这些部门在灾难发生或危机爆发前甚至不知道 BCP 的存在。这是一个非常致命的错误！孤立的开发业务连续性计划可能从两个方面导致灾难。首先，计划本身可能没有考虑负责日常运营的业务人员需要的知识。其次，关于计划详情的操作要素在计划实施前一直不能确定下来。这降低了操作要素与计划条款保持一致并有效实施的可能性，还否认了组织针对该计划进行结构化培训和测试所取得的效果。

为防止这些情况对 BCP 程序造成不利影响，负责这项工作的人员在选择 BCP 团队时应特别慎重。BCP 团队应至少包括下列人员：

- 负责执行业务核心服务的每个组织部门的代表。
- 根据组织分析确定的来自不同职能区域的业务单元团队成员。
- BCP 所涉及领域内拥有技术专长的 IT 专家。
- 掌握 BCP 流程知识的网络安全团队成员。
- 负责工厂实体物理安全和设施管理的团队。
- 熟悉公司法規、监管和合同责任的律师。
- 可解决人员配置问题以及对员工个人产生影响的人力资源团队成员。
- 需要制定在发生中断时如何与利益相关方和公众进行沟通的公共关系团队成员。
- 高级管理层代表，这些代表能设定愿景、确定优先级别和分配资源。

组建一支高效 BCP 团队的技巧

慎重选择团队成员！目标应是创建一支尽可能多样化且能和谐共处的团队。你需要在选择持有不同观点的团队成员和创建一支个性迥异的团队之间取得平衡。目标是创建一支尽可能多样化的团队，并保持和谐运行。

花时间考虑一下 BCP 团队成员资格和哪些人适合组织的技术、财务和环境。你会选择谁？

前面列出的每个人对 BCP 过程都有独特看法，存在个人倾向。例如，每个运营部门的代表通常都认为他们的部门对组织的持续运营最重要。尽管这些倾向初看起来可能引起分歧，但 BCP 团队的领导者应坦然接受，并以富有成效的方式加以利用。每个代表都提出其部门的需求，如果有效利用，这些倾向将有助于在最终计划中实现健康的平衡。另一方面，如果缺乏恰当的领导力，这些倾向可能转变为破坏性的地盘争斗，从而破坏 BCP 成果，并损害整个组织。

高级管理层与 BCP

高级管理层在 BCP 流程中的作用因组织而异，具体取决于公司文化、关注点以及业务运营的法律和监管环境。高级管理层的重要职责通常包括确定优先事项，提供人力和财务资源，以及仲裁有关服务关键性(即相对重要性)的争议。

本书的一位作者最近完成了一家大型非营利机构的 BCP 咨询工作。在工作启动时，他有机会与组织的一位高级管理人员讨论他们共同工作的目标和任务。在那次会议上，那位高级管理人员问他：“为完成这项工作，有什么需要我做的吗？”

这位高级管理人员肯定期待得到敷衍的回答，因为当开始回答时，他的眼睛瞪得很大，“好吧，实际上……”，然后他了解到他积极参与 BCP 过程对成功至关重要。

BCP 团队负责人在制定业务连续性计划时，必须尽可能争取高级管理层的积极支持。高级管理层的积极支持会将 BCP 流程的重要性传达到整个组织，并促进员工积极参与 BCP 活动。否则他们可能认为编制 BCP 是浪费时间，还不如去做其他运营活动。此外，法律法规可能要求这些高级领导人积极参与规划过程。如果你在一家上市公司工作，你可能要提醒高管们，如果一场灾难使公司陷入瘫痪，并发现他们在应急计划中没有实施尽职审查，那么高管和董事要承担个人责任。

可能还必须说服管理层勿将 BCP 和 DRP 花费视为可有可无的支出。管理层对股东的信托责任要求他们至少确保采取适度的 BCP 措施。

在上述 BCP 工作中，这位高级管理人员认识到支持与积极参与的重要性。他给全体员工发了一封电子邮件，介绍 BCP 工作，并表示自己会全力支持。他还参加了几次高层计划会议，并在全公司的股东会议上提到这项工作。

3.2.3 资源需求

BCP 团队确认业务组织分析结果后，就开始评估 BCP 工作的资源需求。这涉及三个不同 BCP 阶段所需的资源。

开发 BCP 团队需要一些资源来执行 BCP 流程的四个阶段(项目范围和计划、业务影响评估、连续性计划以及计划批准和实施)。这个阶段主要耗费人力资源，即 BCP 团队成员和召集过来协助制定计划的支持人员。

测试、培训和维护 在 BCP 的测试、培训和维护阶段，将需要一些硬件和软件资源；同样，这个阶段的主要资源是参与这些活动的员工付出的人力。

实施 当灾难发生且 BCP 团队认为有必要全面实施业务连续性计划时，将需要大量资源。这些资源包括大量实施工作（BCP 可能成为组织关注的重点）和对实际资源的消耗。出于这个原因，对 BCP 团队来说，果断、明智地使用 BCP 的能力是非常重要的。

有效的业务连续性计划需要耗费大量资源，从购买和部署冗余计算设施到团队成员编制计划草稿所用的笔纸。但如前所述，BCP 过程中消耗的最重要资源之一是人力。许多安全专业人员未计算所耗费人力资源的重要性。不过你可放心，高级管理层不会忘掉耗费的人力资源。企业领导能敏锐意识到耗时的 BCP 活动对组织运营生产的影响以及对员工工资、福利与失去市场机会实际成本的影响。当你申请高级管理人员花时间参与 BCP 时，这些问题会变得特别重要。

你应该意识到，管理资源的领导者会严格审核你提交的 BCP 方案，你需要用有条理的、逻辑严密的 BCP 业务案例观点来证明该计划的必要性。



真实场景

宣传 BCP 的收益

在最近一次会议上，本书一位作者与来自一个美国中等城市的卫生系统的一位 CISO（首席信息安全官）讨论了业务连续性计划。该 CISO 的态度令人震惊。他所在的组织尚未实施正式的 BCP 过程；他坚信，灾难事件发生的概率非常小，即便真正发生，他采用“随机应变”方法就能处理好问题。

这种“随机应变”是反对向 BCP 提供资源的最常见理由。许多组织的思路是，企业需要存活下来，在遇到危机时，主要领导再给出“随机应变”的解决方案。如果听到这种反对意见，你可向管理层指明业务每停顿一天所产生的成本（包括直接成本和失去市场机会而导致的间接成本）。然后请他们斟酌，与有序、有计划的业务连续性恢复操作相比，“随机应变”恢复需要多长时间。

3.2.4 法律和法规要求

受到联邦、州和地方法律或法规约束的许多行业可能发现，这些法律或法规要求他们实施不同程度的 BCP。本章已讨论过一个例子，即上市公司的高管和董事在执行业务连续性职责时负有受托责任，需要实施尽职审查。其他情况下，要求可能更严格，失职的后果更严重。

应急服务机构（如警察局、消防队和救护队）负责在灾难发生时维持社会的持续运行。实际上，在公共安全受到威胁的紧急情况下，应急服务机构提供的服务变得更重要。如果他们不能成功实施可靠的 BCP，可能导致生命和/或财产的损失，并削弱民众对政府的信心。

在许多国家，金融机构（如银行、证券公司和处理数据的公司）都受到严格的政府法规以及国际银行和证券法规的约束。这些规定十分严格，旨在确保机构作为经济的关键部分能继续运作。当制药企业必须在灾难发生后的非理想情况下生产药品时，将需要向政府监管机构证明药品纯度。无数个实例说明，有多个法律法规对紧急情况下的持续运营提出了要求。

即使不受这些法律法规要求的约束，你也可能要对客户承担合同义务，这要求你实施合理的 BCP 实践。如果合同中包含对客户的 SLA 承诺，那么当灾难导致服务中断时，你会发现自

已违反了这些合同条款。许多客户可能为你感到遗憾，并希望继续使用你的产品/服务，但业务需求可能迫使他们终止合同，并寻找新的供应商。

另一方面，开发完善的、文档化的业务连续性计划可帮助组织赢得新客户和现有客户的其他业务。如果能向客户展示出当灾难发生后，公司具有恰当的响应程序能持续向客户提供服务，他们将对公司更有信心，且非常可能将公司视为他们的首选供应商。这会让公司处于十分有利的位置！

所有这些问题都可归结为一个结论，即让组织的法律顾问参与 BCP 过程非常重要。法律顾问非常熟悉适用于组织的法律、法规和合同义务，可帮助团队实现计划来满足这些要求，同时保证组织的持续运营，使所有员工、股东、供应商和客户都从中受益。



警告：

与计算系统、业务实践和灾难管理相关的法律法规经常变化，在不同的司法管辖区中也存在差异。确保公司的法律顾问全程参与整个 BCP 过程(包括测试和维护阶段)。如果公司的法律顾问仅参与计划实施前的审核，那么可能不会了解到法律法规的变化对公司职责的影响。

3.3 业务影响评估

一旦 BCP 团队完成准备创建业务连续性计划的四个阶段，就进入工作的核心部分：业务影响评估(Business Impact Assessment, BIA)。BIA 确定组织持续运营所需的资源和这些资源面临的威胁，还评估每个威胁实际发生的可能性以及威胁事件对业务的影响。BIA 结果提供了度量措施，可对用于解决组织面临的各种本地、区域及全球风险而投入的业务连续性资源进行优先级排序。

业务计划者在进行决策时，必须意识到需要使用以下两种不同类型的分析方法。

定量决策 定量决策涉及使用数字和公式得出结论。这类数据结果通常用货币价值表示与业务相关的选项。

定性决策 定性决策考虑非数字因素，如声誉、投资者/客户信心、员工稳定性和其他相关事项。这类数据结果通常用优先级别(如高、中、低) 表示。



注意：

在 BCP 过程中，定量分析和定性分析都扮演着重要角色。然后，很多人倾向于只使用其中一种分析方法。在选择 BCP 团队成员时，应努力在倾向不同分析策略的人员之间取得平衡，以制定出完善的 BCP，让组织长期受益。

本章分别从定量和定性 BIA 的角度阐述 BIA 过程。不过，对于 BCP 团队来说，使用数字进行定量评估是很有吸引力的方式，而定性评估则较困难。BCP 团队对影响 BCP 过程的因素进行定性分析非常重要。例如，如果业务高度依赖于少数几个重要客户，那么管理团队可能愿意承担较大的短期财务损失以长期留住这些客户。BCP 团队(最好有高级管理层的参与)必须一起仔细进行定性分析，以找出满足所有利益相关方的综合解决方法。

3.3.1 确定优先级

BCP 团队要完成的第一个 BIA 任务是确定业务优先级。根据业务范围，当灾难发生时，有些活动对维持日常运营极为关键。确认优先级或关键性涉及创建业务流程的综合列表，并按重要性进行排序。这项任务看起来有些令人生畏，但实际上并非如此。

可在团队成员之间划分工作任务，让每个参与者负责制定一个涵盖其部门业务功能的优先级列表。当整个 BCP 团队开会讨论时，团队成员可基于这些优先级列表为整个组织创建优先级主列表。采用这种方法的一个注意事项是：如果团队不能真正全面代表组织，就可能错过关键的优先事项。要确保收集到组织中各个组成部分的意见。

这个过程有助于定性地确定业务优先级。前面提过同时开展定性和定量 BIA 的尝试。要开始定量评估，BCP 团队需要一起制定组织资产清单，并为每项资产分配货币形式的资产价值(AV)。这些数字将在后续 BIA 步骤中使用，从而实施基于财务的 BIA。

BCP 团队必须开发的第二个量化指标是 MTD(Maximum Tolerable Downtime，最大允许中断时间)，有时也称为最大容忍中断时间(Maximum Tolerable Outage，MTO)。MTD 是业务功能出现故障但不会对业务产生无法弥补的损害所允许的最长时间。在执行 BCP 和 DRP 计划时，MTD 提供了重要信息。

对于每个业务功能，还需要另一个度量指标，即恢复时间目标(Recovery Time Objective，RTO)。RTO 是指当中断发生后实际恢复业务功能所需的时间。一旦定义了恢复目标，就可以设计和规划所需的步骤去完成恢复任务。

BCP 过程的目标是确保 RTO 小于 MTD，这使一个业务功能不可用的时间永远不会超过最大允许中断时间。

3.3.2 风险识别

接下来的 BIA 阶段是识别组织面临的风险。在这个组织特有的风险列表中，有些风险很容易被想到，但要识别其他一些较模糊的风险，可能需要 BCP 团队付出一番努力。

风险有两种形式：自然风险和人为风险。下面列出一些引发自然风险的事件：

- 暴风雨/飓风/龙卷风/暴风雪
- 雷击
- 地震
- 泥石流/雪崩
- 火山喷发

人为风险包括以下事件：

- 恐怖活动/战争/内乱
- 盗窃/破坏
- 火灾/爆炸
- 长时间断电
- 建筑物倒塌
- 运输故障

- 互联网中断
- 服务提供商停运

记住，上面并未列出所有风险，只是确定了许多组织面临的一些共同风险。可将这些风险作为起点；但要罗列出组织面临的所有风险，还需要 BCP 团队成员的共同努力。

BIA 过程的风险识别部分本质上是纯粹的定性分析。在这个过程中，BCP 团队不应关注每种风险实际发生的可能性，或风险发生后会对业务持续运营造成的损害程度。这种分析结果有助于对剩余 BIA 任务进行定性和定量分析。

业务影响评估和云计算

在进行业务影响评估时，不要忘记考虑组织依赖的任何云供应商。根据云服务的性质，供应商自身的业务连续性计划可能对组织的业务运营产生重大影响。

例如，有一个将电子邮件和日常安排外包给第三方 SaaS(软件即服务)提供商的公司。与该提供商签订的合同是否包含有关提供商 SLA 的详细信息以及在灾难发生时恢复运营的承诺？

还要记住，在选择云提供商时，合同通常不足以证实已经实施了尽职审查。应该去验证他们是否有适当的控制措施来履行合同承诺。虽然你可能无法亲自考察供应商设施来验证其控制的实施情况，但可选择让其他人代为考察！

现在，在挑选考察代表和预订出差航班前，要意识到供应商的许多客户都可能问同样的问题。出于这个原因，供应商可能已聘请了一家独立的审计公司对其控制情况进行评估。审计公司可按 SOC(Service Organization Control，服务组织控制)报告的形式向你提供评估结果。

SOC 报告有三种不同版本。最简单的一种是 SOC-1 报告，仅涵盖财务报告的内部控制。如果要验证安全性、隐私和可用性方面的控制，则需要查看 SOC-2 或 SOC-3 报告。美国注册会计师协会(American Institute of Certified Public Accountants, AICPA)制定并维护有关这些报告的标准，以保持不同会计师事务所审计师之间的一致性。

有关此主题的更多信息，请参阅 AICPA 的文档并比较文档中不同类型的 SOC 报告。网址为 <https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/comparison-soc-1-3.pdf>。

3.3.3 可能性评估

在前面的步骤中，BCP 团队完整列出可能对组织构成威胁的事件。你可能认识到某些事件比其他事件更容易发生。例如，对于南加州的企业而言，遭受地震的风险比遭受热带风暴的风险更大；而对于佛罗里达州的企业来说，情况正好相反。

为解释这些差异，业务影响评估的下一阶段就是确定每种风险发生的可能性。为保持计算的一致性，可能性的评估结果通常用年度发生率(ARO)表示，年度发生率反映企业每年预期遭受特定灾难的次数。

BCP 团队应该一起为之前识别出的每种风险确定 ARO。这些数字应基于公司历史、团队成员的专业经验以及专家(如气象学家、地震学家、防火专业人员和其他顾问)的建议。

**提示：**

除了本章提到的政府资源外，还有保险公司为其精算过程开发的大型风险信息库。你可从他们那里获取这些信息来协助你开展 BCP 工作。毕竟，在预防业务破坏方面，你们有着共同的利益！

许多情况下，你可能不需要成本就能获得由专家提供的某些风险的可能性评估结果。例如，美国地质勘探局(USGS)提供的地震灾害图说明了美国各地区的地震 ARO。同样，美国联邦应急管理署(FEMA)负责绘制美国各个地区的详细洪水地图。这些资源都可在线获取，可为组织进行业务影响评估提供大量信息。

3.3.4 影响评估

顾名思义，影响评估是业务影响评估中最关键的部分之一。在此阶段，将分析在风险识别和可能性评估期间收集的数据，并尝试确定每个已识别风险对业务的影响。

从定量的角度看，将涉及三个具体指标：暴露因子、单一损失期望和年度损失期望。这些指标中的每一个都针对在先前阶段中评估的每个特定风险/资产组合计算值。

暴露因子(EF)是风险对资产造成的损害程度，以资产价值的百分比表示。例如，如果 BCP 团队咨询消防专家并确定建筑物发生火灾后将导致 70% 的建筑物被摧毁，那么建筑物火灾的暴露因子就是 70%。

单一损失期望(SLE)是每次风险发生后预期造成的货币损失。可用以下公式计算 SLE：

$$SLE = AV \times EF$$

继续前面的例子，如果建筑价值 500 000 美元，那么单一损失期望将是 500 000 美元的 70%，即 350 000 美元。可解释为：建筑物发生一次火灾预计造成 350 000 美元的损失。

年度损失期望(ALE)是一年内由于风险危害资产给公司预期带来的货币损失。你已经拥有执行此计算所需的全部数据。SLE 是每次风险发生后预期造成的货币损失，ARO(来自可能性分析)是风险每年预期发生的次数，可将这两个数字简单相乘来计算 ALE：

$$ALE = SLE \times ARO$$

再回到前面提到的建筑物示例。如果火灾专家预测建筑每 30 年会发生一次火灾，那 ARO 就是 1/30 或约为 3%。ALE 是 350 000 美元 SLE 的 3%，即 10 500 美元。你可将这个数字解释为，由于建筑物失火，公司每年预期将损失 10 500 美元。

显然，每年不一定都会发生火灾，这个数字代表了 30 年间发生火灾的平均成本。在考虑预算时，这个数字没有特别用途，但在给特定风险划分 BCP 资源优先级时，它就能体现原本无法衡量的价值。这些概念在第 2 章中介绍过。

**提示：**

确保熟悉本章中包含的定量计算公式以及资产价值、暴露因子、年度发生率、单一损失期望和年度损失期望等概念。了解公式并能应用在场景中。

从定性角度看，你必须考虑中断可能对业务产生的、不能以货币价值衡量的影响。例如，可能需要考虑以下事项：

- 在客户群中丧失的信誉
- 长时间停工后造成员工流失
- 公众的社会/道德责任
- 负面宣传

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造成的影响，但它们同样重要。毕竟，如果损失客户基础，即使准备好重新开始运营，也无法返回到先前的状态！

3.3.5 资源优先级排序

BIA 的最后一步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，这些风险已在前面的 BIA 任务中进行了识别和评估。

从定量的角度看，这个过程相对简单。只需要创建一个在 BIA 过程中分析过的所有风险的列表，并根据影响评估阶段计算的 ALE 按降序对其进行排序，这提供了需要处理的风险的优先级列表。从列表顶部选择想要同时处理的尽可能多的风险，并逐一解决。最终，你将达到这个状况：处理完列表中的全部风险(不太可能！)或耗尽所有可用资源(更有可能！)。

前面已强调过用定性方式分析关键问题的重要性。在 BIA 的前几个阶段，虽然有些分析有所重复，我们仍将定量和定性分析视为独立的重要功能来看待。现在是时候合并两个优先级列表：这更像是一门艺术，而不是一门科学。你必须与 BCP 团队和高级管理团队的代表一起将两个列表合并为一个优先级列表。

定性分析可证实对风险优先级的提高或降低是否正确，这些风险在定量分析结果列表中存在并按 ALE 排序。例如，如果你经营一家消防公司，尽管地震可能造成更多物理损害，但排在第一优先级的可能是防止主要营业场所发生火灾。如果消防公司遭到火灾的破坏，这将在商界造成无法挽回的声誉损失，并最终导致公司倒闭，因此要调高优先级。

3.4 连续性计划

BCP 流程的前两个阶段(项目范围和计划以及业务影响评估)重点确定 BCP 流程将如何工作，并对必须保护以防止中断的业务资产进行优先级排序。BCP 开发的下一个阶段是编制连续性计划，重点是开发和实现连续性战略，尽量减少已发生的风险对被保护资产的影响。

在本节中，你将学习连续性计划中涉及的下列子任务：

- 策略开发
- 预备和处理
- 计划批准
- 计划实施
- 培训和教育

3.4.1 策略开发

策略开发阶段在业务影响评估与 BCP 开发的连续性计划阶段之间架起桥梁。BCP 团队现

在必须采用由定量和定性资源优先排序工作提出的优先级问题清单，确定业务连续性计划将处理哪些风险。要完全解决所有意外事件，需要实施在面临所有可能风险的情况下保持零故障时间的预备和处理。出于显而易见的原因，根本不可能实施这样一个综合策略。

BCP 团队应回顾在 BIA 早期阶段创建的 MTD 估值，并确定哪些风险是可接受的，哪些风险必须通过 BCP 连续性措施予以缓解。有些决定很容易，如暴风雪袭击埃及运营设施的风险可视为能够接受的风险，可忽略不计；而新德里雨季的风险非常大，必须通过 BCP 措施予以减轻。

一旦 BCP 团队确定哪些风险需要缓解以及将为每个缓解任务提供的资源水平，他们就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计划的关键部分。在这个任务中，BCP 团队设计具体的过程和机制来减轻在策略开发阶段被认为不可接受的风险。

有三类资产必须通过 BCP 预备和处理进行保护：人员、建筑物/设施和基础设施。接下来将探讨一些可用于保护这些资产类型的技术。

1. 人员

首先，你必须确保组织内的人员在紧急情况发生前、发生期间和发生后都是安全的。实现这一目标后，需要制定条款授权员工在尽可能正常的情况下执行他们的 BCP 和操作任务。



警告：

不要忽视这个事实：人是最宝贵的资产。人员的安全必须优先于组织的商业目标。

确保 BCP 为员工、客户、供应商以及可能受影响的其他人的安全提供充分保障！

应该为人们提供完成所分配任务必需的全部资源。同时，如果需要人们加班，还必须安排好住所和食物。任何要求这些预备品的连续性计划都应包括 BCP 团队在面对灾难事件时的详细指导。组织应保持充足的储备库存以便在可访问的地点长时间为业务和支持小组提供支持。计划应规定这些库存物品需要定期更换以防变质。

2. 建筑物和设施

许多业务需要专业设施来执行其关键操作。这些设施可能包括标准办公设备、生产工厂、运营中心、仓库、配送/物流中心以及维修/维修站等。在执行 BIA 时，你将确定在组织持续运营中发挥关键作用的设施。连续性计划应针对每个关键设施的以下两方面进行说明。

加固预备措施 BCP 应概述可实施的机制和程序来保护现有设施免受策略开发阶段中定义的风险的影响。这可能包括一些像修补漏水屋顶这样简单的步骤，或像安装强化的飓风避难所和防火墙这样复杂的步骤。

替代站点 如果无法通过加固设施来抵御风险，BCP 应识别出可用于立即恢复业务活动（或至少可在少于最大容忍中断时间内提供所有关键业务功能）的备用站点。第 18 章将描述此阶段

可能用到的一些设施类型。

3. 基础设施

每个业务的关键处理都依赖于某种基础设施。对许多业务而言，基础设施的关键部分是通信的 IT 主干，以及处理订单、管理供应链、处理客户交互和执行其他业务功能的计算机系统。通信的 IT 主干包括许多服务器、工作站和不同站点之间的关键通信链路。BCP 必须确定如何保护这些系统免受策略开发阶段识别出的风险的影响。与建筑物和设施一样，可采用两种主要方法对基础设施进行保护。

物理性加固系统 可引入计算机安全灭火系统和不间断电源等保护措施来保护系统。

备用系统 还可引入冗余(冗余组件或依赖于不同设施的完全冗余系统/通信链路)来保护业务功能。

这些原则同样适用于为关键业务流程提供服务的任何基础设施组件，包括运输系统、电网、银行系统、财务系统和供水系统等。

3.5 计划批准和实施

一旦 BCP 团队完成 BCP 文档的设计阶段，就应当向最高管理层申请批准该计划。如果很幸运，整个计划的开发阶段都有高级管理人员参与，那么获得批准就是相当简单的过程。相反，如果这是你第一次向高级管理层提交 BCP 文件，那么你应该准备好对该计划的目的和具体规定进行详细解释。



提示：

高级管理层的批准和参与对整个 BCP 工作的成功极为重要。

3.5.1 计划批准

如有可能，应该尝试让企业高层，如首席执行官、主席、总裁或类似的业务领导批准该计划。这可证明计划对整个组织的重要性，并展示业务领导对业务连续性的承诺。高层领导在计划中的签名，也使计划在其他高级管理人员眼中具有更高的重要性和可信度，否则他们可能将其视为一项必要但微不足道的 IT 计划。

3.5.2 计划实施

一旦获得高级管理层的批准，即可开始实施计划。BCP 团队应该共同开发实施计划，该计划使用分配的资源，根据给定的修改范围和组织环境，尽快实现所描述的过程和预备目标。

完全部署所有资源后，BCP 团队应监督相应 BCP 维护程序的执行情况，以确保计划能响应业务需求的不断变化。

3.5.3 培训和教育

培训和教育是 BCP 实施的基本要素。所有直接或间接参与计划的人员都应接受关于总体计划及个人责任的培训。

组织中的每个人都应该至少收到一份计划简报，使他们相信业务领导已考虑到业务持续运营可能面临的风险，并制定了计划来减轻风险对组织的影响。

直接负责 BCP 工作的人员应接受培训，并对特定 BCP 任务进行评估以确保他们能在灾难发生时有效完成这些任务。此外，应为每个 BCP 任务至少培训一名备用人员，确保在紧急情况下人员受伤或无法到达工作场所时有备用人员。

3.5.4 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 方法记录到纸上可提供了几个重要好处。

- 确保在紧急情况下，即使没有高级 BCP 团队成员来指导工作，BCP 人员也有一份书面的连续性计划可以参考。
- 提供 BCP 过程的历史记录，这有助于将来的人员理解各种过程背后的原因并对计划进行必要修改。
- 促使团队成员将想法写下来，这个过程通常有助于识别计划中的缺陷。在纸上制定计划还可将文件草稿分发给不在 BCP 团队中的人员进行“合理性检查”。

接下来探讨书面业务连续性计划的一些重要组成部分。

1. 连续性计划的目标

首先描述 BCP 团队和高级管理层提出的连续性计划的目标。这些目标应在第一次 BCP 团队会议中或之前决定，很可能在 BCP 的整个生命周期内保持不变。

最常见的 BCP 目标很简单：确保在紧急情况下业务的持续运营。为满足组织需求，该文档也可能列出其他目标。例如，可将目标设置为：客户呼叫中心的连续停机时间不超过 15 分钟，或备份服务器可在启用后 1 小时内处理 75% 的负载。

2. 重要性声明

重要性声明反映了 BCP 对组织持续运行的重要性。这份文件通常以信函形式提供给员工，说明为什么组织将大量资源用于 BCP 开发过程，并要求所有人员在 BCP 实施阶段进行配合。

这就是高级管理人员参与 BCP 的重要性。如果信函中有首席执行官(CEO)或类似级别领导的签名，当你尝试在整个组织中进行改变时，这个计划将产生极大影响。如果是较低级别经理的签名，那么在尝试与组织中不由其直接领导的其他部门互动时，可能遇到阻力。

3. 优先级声明

优先级声明是业务影响评估的优先级确认阶段的直接产物。它只按优先顺序列出对业务连续运营至关重要的功能。在列出这些优先级时，还应该包含一个声明，表明这是 BCP 过程的一

部分，并说明紧急情况下这些功能对业务连续运营的重要性。否则，这个优先级列表可能用于非预期目标，并导致竞争组织之间的争斗，从而损害业务连续性计划。

4. 组织职责声明

组织职责声明也来自高级管理人员，可与重要性声明合并在同一文档中。它基本上反映了“业务连续性是每个人的职业”这个观点。组织职责声明重申组织对业务连续性计划的承诺，并告知员工、供应商和附属企业，要求他们尽力协助实施 BCP 过程。

5. 紧急程度和时限声明

紧急程度和时限声明表达了实施 BCP 的重要性，概述由 BCP 团队决定的并由高层管理人员批准的实施时间表。该声明的措辞将取决于组织领导层给 BCP 过程指定的实际紧急程度。如果该声明本身与优先级声明和组织职责声明在同一文件中，那么应将时间表放在单个文件中。否则，可将时间表和此声明放在同一文件中。

6. 风险评估

BCP 文档的风险评估部分基本上重述在业务影响评估期间的决策过程。它应该包括对 BIA 过程中所有风险的讨论，以及为评估这些风险进行的定量分析和定性分析。对于定量分析，应该包括实际的 AV、EF、ARO、SLE 和 ALE 值。对于定性分析，应该向阅读者提供风险分析背后的思考过程。需要注意，风险评估内容必须定期更新，因为它反映的是某个时间点的评估结果。

7. 风险接受/风险缓解

BCP 文件中的风险接受/风险缓解部分包含 BCP 过程的策略开发部分的结果。它应涵盖风险分析部分确定的所有风险，并对下面两个思考过程中的一个进行说明。

- 对于被认为可接受的风险，应概述接受原因以及未来可能需要重新考虑此决定的可能事件。
- 对于被认为不可接受的风险，应概述要采取的缓解风险的预备措施和过程，以降低风险对组织持续运营的影响。



警告：

在遇到风险缓解挑战时，往往听到“我们接受这种风险”的说法。BCP 人员应该抵制上述陈述，并要求业务领导提供一份记录他们决定接受风险的正式文件。如果审计员稍后审查业务连续性计划，他们肯定会在 BCP 过程中查找所有风险接受决策的正式文件。

8. 重要记录计划

BCP 文件还应概述组织的重要记录计划。该文档说明了存储关键业务记录的位置以及建立和存储这些记录的备份副本的过程。

实施重要记录计划面临的最大挑战之一通常是首先识别重要记录！当许多组织从基于纸质的工作流转变为数字工作流时，常失去创建和维护正式文件结构的严谨性。重要记录现在可能

分布在各种 IT 系统和云服务中。有些可能存储在团队可访问的中央服务器上，而其他可能位于分配给单个员工的数字仓库中。

如果遇到这种混乱状况，你可能首先需要识别对业务真正关键的重要记录。与职能部门的领导一起探讨，并询问他们：“如果我们今天需要在一个完全陌生的地方重建组织，并且无法访问任何电脑或文件，你们需要哪些记录？”以这种方式提出问题迫使团队认真思考重建操作的实际过程，当他们在脑海中遍历这些步骤时，将生成组织重要记录的清单。这份清单会随着人们不断记起其他重要信息源而发生变化，因此你应该考虑通过召开多次会议来完成它。

一旦确定了组织认为至关重要的记录，下一个任务就艰难了：找到它们！你应该能够识别出重要记录清单中确定的每条记录的存储位置。完成此任务后，使用这个重要记录清单来报告余下的业务连续性计划工作。

9. 应急响应指南

应急响应指南概述组织和个人立即响应紧急事件的职责。该文档为第一个发现紧急情况的员工提供了启动“BCP 预案”的步骤，BCP 预案不会自动激活。这些指南应包括以下内容：

- 立即响应程序(安全和安全程序、灭火程序，以及通知适当的应急响应机构等)。
- 事故通知人员名单(高管、BCP 团队成员等)。
- 第一响应人员在等待 BCP 团队集结时应采取的二级响应程序。

应急响应指南应该很容易被组织的所有人员理解，每个人都可能是紧急事件的第一响应人员。当中断发生时，时间非常宝贵。延缓激活业务连续性过程可能导致业务运营出现非预期的中断。

10. 维护

BCP 文件和计划本身必须即时更新。每个组织都在不断变化，这种动态性使得业务连续性要求随之变化。BCP 团队不应在计划开发完成后就立即解散，而是应定期召开会议讨论计划并审核计划测试的结果，以确保一直能满足组织需求。

显然，对计划进行微小改动不需要从头开发完整的 BCP，只需要在 BCP 团队的非正式会议上一致通过即可。但请记住，如果组织的任务或资源发生巨大改变，则可能需要从头开发 BCP。

每次更改 BCP 时，都必须进行良好的版本控制。所有 BCP 旧版本都应该被物理销毁并替换为最新版本，这样便于弄清哪个是正确的 BCP 实施版本。

在职位描述中包含 BCP 组件是确保 BCP 保持更新并正确实施的良好实践。在员工的职位描述中包括 BCP 职责也可保证绩效考核过程中的公平竞争。

11. 测试和演练

BCP 文档中还应包括一个正式的演练程序，以确保该计划仍然有效，并确保所有相关人员都经过充分培训，能在发生灾难时履行职责。BCP 的测试过程与用于灾难恢复计划的测试过程非常相似，详见第 18 章的讨论。

3.6 本章小结

每个依靠技术资源维持生存的组织都应制定全面的业务连续性计划，以确保在意外紧急情况下组织的持续运营。有许多重要概念构成了可靠的业务连续性计划实践的基础，包括项目范围和计划、业务影响评估、连续性计划以及计划批准和实施。

每个组织都必须制定计划和程序，以减轻灾难对持续运营的影响，并加快恢复正常运营。要确定业务面临的风险以及需要缓解的风险，必须与其他职能团队合作，从定性和定量两个角度进行业务影响评估。必须采取适当步骤为组织开发连续性战略，并知道如何应对未来的灾难。

最后，必须创建所需的文档，以确保计划有效传达给现在和未来的 BCP 团队成员。此类文档应该包括连续性计划指南。业务连续性计划还必须包含对重要性、优先级、组织职责、紧急程度和时限的声明。此外，该文档还应包括风险评估、风险接受和缓解计划，包括重要记录程序、应急响应指南以及维护与测试计划。

第 18 章将讨论如何制定下一步计划：开发和实施灾难恢复计划；其中包括使业务在灾难发生后保持运营所需的技术性控制措施。

3.7 考试要点

了解 BCP 过程的四个步骤。BCP 包括四个不同阶段：项目范围和计划、业务影响评估、连续性计划、计划批准和实施。每项任务都有助于确保实现在紧急情况下业务保持持续运营的总体目标。

描述如何执行业务组织分析。在业务组织分析中，负责领导 BCP 过程的人员确定哪些部门和个人参与业务连续性计划。该分析是选择 BCP 团队的基础，经 BCP 团队确认后，用于指导 BCP 开发的后续阶段。

列出 BCP 团队的必要成员。BCP 团队至少应包括：来自每个运营和支持部门的代表，IT 部门的技术专家，具备 BCP 技能的物理和 IT 安全人员，熟悉公司法律、监管和合同责任的法律代表，以及高级管理层的代表。其他团队成员取决于组织的结构和性质。

了解 BCP 人员面临的法律和监管要求。企业领导必须实施尽职审查，以确保在灾难发生时保护股东的利益。某些行业还受制于联邦、州和地方法规对 BCP 程序的特定要求。许多企业在灾难发生前后都有履行客户合约的义务。

解释业务影响评估过程的步骤。业务影响评估过程的五个步骤是：确定优先级、风险识别、可能性评估、影响评估和资源优先级排序。

描述连续性策略的开发过程。在策略开发阶段，BCP 团队确定要减轻哪些风险。在预备和处理阶段，设计可降低风险的机制和程序。然后，该计划必须得到高级管理层的批准并予以实施。人员还必须接受与他们在 BCP 过程中角色相关的培训。

解释对组织业务连续性计划进行全面文档化的重要性。将计划记录下来，可在灾难发生时给组织提供一个可遵守的书面程序。这可确保在紧急情况下有序实施计划。

3.8 书面实验

1. 为什么在业务连续性计划团队中包含法律代表很重要？
2. “随机应变”的业务连续性计划有什么问题？
3. 定量风险评估和定性风险评估有什么区别？
4. 业务连续性培训计划应包含哪些关键部分？
5. 业务连续性计划过程的四个主要步骤是什么？

3.9 复习题

1. 负责制定业务连续性计划的人员应该执行的第一项任务是什么？
 - A. 选择 BCP 团队
 - B. 业务组织分析
 - C. 资源需求分析
 - D. 法律和监管评估
2. 一旦选择 BCP 团队，团队议程中的第一个任务应该是什么？
 - A. 业务影响评估
 - B. 业务组织分析
 - C. 资源需求分析
 - D. 法律和监管评估
3. 哪个术语描述了公司高管和董事应采取适当措施以最大限度地减少灾难对组织持续运营影响的职责？
 - A. 企业责任
 - B. 灾难需求
 - C. 尽职审查
 - D. 持续经营责任
4. 在 BCP 过程中，BCP 阶段消耗的主要资源是什么？
 - A. 硬件
 - B. 软件
 - C. 处理时间
 - D. 人员
5. 在业务影响评估的确定优先级阶段，应使用什么计量单位为资产分配定量值？
 - A. 货币
 - B. 效用
 - C. 重要性
 - D. 时间

6. 以下哪个 BIA 条款表示针对给定风险企业预期每年可能损失的金额?

- A. ARO
- B. SLE
- C. ALE
- D. EF

7. 可使用哪个 BIA 指标来表示业务功能无法使用但不会给组织造成无法弥补的损失的最长中断时间?

- A. SLE
- B. EF
- C. MTD
- D. ARO

8. 你担心雪崩会给价值 300 万美元的运输设施带来风险。根据专家意见, 你确定每年发生雪崩的概率为 5%。专家提醒你雪崩会完全摧毁你的建筑, 并需要你在同一块土地上重建。这个运输设施价值 300 万美元, 其中 90% 的价值是建筑大楼, 10% 的价值是土地。运输设施在雪崩中的单一损失期望是多少?

- A. \$3 000 000
- B. \$2 700 000
- C. \$270 000
- D. \$135 000

9. 参考第 8 题的情景, 年度损失期望是多少?

- A. \$3 000 000
- B. \$2 700 000
- C. \$270 000
- D. \$135 000

10. 你担心飓风会给位于南佛罗里达的公司总部带来风险。这栋建筑本身估价 1500 万美元。在咨询了美国国家气象局后, 你确定飓风在一年内袭击的可能性为 10%。你雇用了一支由建筑师和工程师组成的团队, 他们均认为飓风大约会摧毁 50% 的建筑。那么年度损失期望(ALE)是多少?

- A. \$750 000
- B. \$1 500 000
- C. \$7 500 000
- D. \$15 000 000

11. BCP 的哪个任务弥补了业务影响评估和连续性计划阶段之间的差距?

- A. 资源优先级排序
- B. 可能性评估
- C. 策略开发
- D. 预备和处理

12. 在设计连续性计划的预备和处理阶段时，应首先保护哪种资源？
- A. 物理设备
 - B. 基础设施
 - C. 财务资源
 - D. 人员
13. 在业务影响评估期间，下列哪一项问题不适合进行定量测量？
- A. 厂房的损失
 - B. 车辆的损坏
 - C. 负面宣传
 - D. 停电
14. Lighter Than 航空公司预计，如果龙卷风袭击其飞机运营设施，将损失 1000 万美元。预计每 100 年该设施会被龙卷风袭击一次。这个场景下的单一损失期望是多少？
- A. 0.01
 - B. \$10 000 000
 - C. \$100 000
 - D. 0.10
15. 参考第 14 题中的情景，年度损失期望是多少？
- A. 0.01
 - B. \$10 000 000
 - C. \$100 000
 - D. 0.10
16. 在业务连续性计划的哪个任务中，你会实际地设计程序和机制来降低 BCP 团队认为不可接受的风险？
- A. 策略开发
 - B. 业务影响评估
 - C. 预备和处理
 - D. 资源优先级排序
17. 安装冗余通信链路时，使用何种类型的缓解措施？
- A. 加固系统
 - B. 定义系统
 - C. 减少系统
 - D. 备用系统
18. 什么类型的计划涉及与备用处理设施、备份和容错相关的技术控制？
- A. 业务连续性计划
 - B. 业务影响评估
 - C. 灾难恢复计划
 - D. 漏洞评估

19. 在风险评估情景中用于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. 在下列人员中，谁将为业务连续性计划的重要性声明提供最好的支持？

- A. 业务运营副总裁
- B. 首席信息官
- C. 首席执行官
- D. 业务连续性管理人员

法律、法规和合规

本章涵盖的 CISSP 认证考试主题包括：

✓ 域 1：安全与风险管理

- 1.3 确定合规要求

- 1.3.1 合同、法律、行业标准和监管要求

- 1.3.2 隐私要求

- 1.4 了解全球范围内与信息安全相关的法律和监管问题

- 1.4.1 网络犯罪和数据泄露

- 1.4.2 许可和知识产权要求

- 1.4.3 进口/出口控制

- 1.4.4 跨境数据流

- 1.4.5 隐私

对于 IT 和网络安全专业人士来说，合规是关于法律与监管的重要问题。国家、州和地方政府都颁发了交叉的法律，以拼凑方式管理网络安全的不同组成部分。局面十分混乱，给必须协调多个司法管辖权法律的安全专业人员带来了困难。对于必须遵守不同国际法的跨国公司来说，事情变得更复杂。

近年来，执法机构积极应对网络犯罪问题。世界各国政府的立法部门都试图解决网络犯罪问题。许多执法机构都配备了受过良好训练的专职计算机犯罪调查人员，这些人员接受过高级安全培训。

本章将介绍处理计算机安全问题的各种法律，将研究与计算机犯罪、隐私、知识产权等主题相关的法律问题，还将介绍基本的调查技术，包括请求执法部门协助的利弊。

4.1 法律的分类

在法律系统中，有三种主要法律类型。每种法律都用来应对各种不同情况，在不同类别的法律下对违法行为的处罚差别也很大。下面将分析刑法、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

刑法是维护和平、保障社会安全的法律体系的基石。许多引人注目的法庭案件涉及刑法问题，刑法也是警察和其他执法机构关注的法律。刑法包含针对某些行为的禁令，如谋杀、袭击、抢劫和纵火等行为。对违反刑法的处罚是有范围的，包括强制时长的社区服务、货币形式的罚款以及以监禁形式剥夺公民自由。



真实场景

警察很聪明！

本书一位作者的好友是当地警察局的技术犯罪调查员。他经常接手威胁邮件和网站帖子这样的计算机滥用案件。

最近，他分享了一起通过电子邮件向当地中心发送炸弹威胁的案件。罪犯给校长发了一封威胁邮件，宣称炸弹将在下午1点爆炸，并警告他撤离学校。作者的好友在上午11时收到报警，此次他只有两个小时的时间来调查犯罪行为以及向校长提出最佳应对建议。

他立刻向互联网服务提供商发出紧急传票，并追踪到威胁邮件来自学校图书馆的一台计算机。中午12:15，他向嫌疑人出示了监控录像和审计记录，监控记录中显示嫌疑人正在操作图书馆计算机，审计日志证实了嫌疑人发送过该邮件。这名学生很快承认发这种威胁邮件只是想让学校提前几个小时放学。他的解释是：“我不认为有人能发现真相。”

事实表明，这名学生的想法是错误的。

许多刑法通过打击计算机犯罪来保护社会安全。随后几节将提到一些法律，如《计算机欺诈和滥用法案》《电子通信隐私法案》《身份盗用与侵占防治法》等，以及如何对严重的计算机犯罪案件进行刑事处罚。经验丰富的检察官与相关执法机构联手，对“地下黑客”行为进行严厉打击，他们利用法院系统，对那些曾被视为无害的恶作剧判处漫长的刑期。

在美国，各级政府立法机构通过选举产生的代表制定刑法。在联邦政府层面，包括众议院和参议院通常必须获得多数赞同票，才可使刑法法案变成法律。一旦投票通过，这些法案就会成为联邦法律，并适用于联邦政府有权管辖的所有案件(主要包括州间贸易案件、跨越州界的案件或违反联邦政府法律的案件)。如果联邦司法权不适用，州执政当局会以相似方式使用由州议员通过的法律来处理案件。

所有联邦和州的法律都必须遵守美国的最高法律《美国宪法》，它规定了美国政府如何进行执政工作。所有法律都要受到地方法院的司法审查，这些地方法院有权上诉到美国最高法院。如果地方法院发现某个法律违反了宪法，就有权将其推翻并认定其无效。

记住，刑法非常严肃。如果发现自己作为证人、被告或受害者卷入刑事案件，特别是计算机犯罪案件，强烈建议向熟悉刑法系统的律师寻求帮助。在这种复杂的法律系统中，仅凭借个人能力“单打独斗”是不明智的。

4.1.2 民法

民法是法律体系的主体，用于维护社会秩序，管理不属于犯罪行为但需要由公正的仲裁者解决的个人和组织间的问题。由民法判决的事项类型包括合同纠纷、房地产交易、雇佣问题和财产/遗嘱公证程序。民法也用于创建政府架构，行政部门使用这个架构来履行自己的职责。这些法律为政府活动提供预算，并授予行政部门制定行政法的权力。

民法的制定方式与刑法相同，在成为法律前，必须通过立法程序，并同样受到宪法条款和司法审查程序的约束。在联邦层面，刑法和民法都收录在《美国法典》(USC)中。

民法和刑法的主要区别在于执行方式。通常，执法当局除了采取必要的行动恢复秩序外，不会介入民法事务。在刑事诉讼中，政府通过执法调查人员和检察官对被指控犯罪的人员提起诉讼。在民事问题中，认为自己冤枉的人有责任聘请法律顾问，并向他们认为应对自己的冤屈负责的人提起民事诉讼。政府(除非是原告或被告)在争端中不偏袒任何一方，也不主张任何一方的立场。政府在民事案件中的唯一作用是提供审理民事案件的法官、陪审团和法院设施，并在管理司法系统与法律一致方面发挥行政作用。

与刑法一样，如果你认为需要提起民事诉讼，或有人对你提起民事诉讼，那么最好去寻求法律援助。虽然民法没有监禁处罚，但败诉的一方可能面临严重的经济处罚。从每天播放的晚间新闻中可看到包括对烟草公司、大公司和富人处罚数百万美元的案件。这样的事情几乎天天都在发生。

4.1.3 行政法

政府行政部门要求许多机构对保证政府的有效运作承担广泛责任。这些机构的责任就是遵守和执行立法部门制定的刑法和民法。然而，很容易就能想到，刑法和民法不可能制定出在任何情况下都应该遵守的规则和程序。因此，行政机构在制定管理机构日常运作的政策、程序和规章方面有一定余地。行政法涉及的既可是琐碎的事情，如联邦机构购买办公电话的程序，也可是重大问题，如用于执行由国会通过的法律移民政策。行政法被包括在《美国联邦法规》中，《美国联邦法规》通常简称为 CFR(Code of Federal Regulations)。

虽然行政法不需要通过立法部门的行动来获得法律效力，但它必须遵守所有现有的民法和刑法。政府机构不得执行与现行法律直接抵触的法规。此外，行政法规(以及政府机构的行动)也必须符合美国宪法的规定并接受司法审查。

要了解合规要求和程序，必须充分了解法律的复杂性。从行政法到民法再到刑法(在一些国家甚至有宗教法)，顺应监管环境是一项艰巨任务。CISSP 考试重点在于对法律、法规、调查和合规性的概括，因为它们会影响组织的安全工作。不过，你有责任向专业人员(如律师)寻求帮助，他们将指导你维护法律及法律所支持的安全工作。

4.2 法律

下面将研究一些与信息技术相关的法律。根据需要，讨论都以美国为中心，也是 CISSP 考

试会涉及的法律内容。还简要介绍几个广受关注的非美国法律，例如欧盟的通用数据保护条例(GDPR)。然而，如果运营环境涉及外国的司法管辖权，则应聘请当地的法律顾问来指导你了解他们的法律系统。



警告：

每个信息安全专业人员都应对与信息技术相关的法律有基本了解。不过，最重要的教训是知道什么时候应该请律师。如果你认为自己正处于法律的“灰色地带”，最好寻求专业建议。

4.2.1 计算机犯罪

立法者判定的第一批计算机安全案件是那些涉及计算机犯罪的事件。根据传统刑法，早期的许多计算机犯罪起诉案件都被驳回，因为法官认为将传统法律应用到这种现代类型的犯罪太过牵强。为此，立法者通过了专门法规，在其中定义了计算机犯罪，并对各种犯罪制定了具体的惩罚措施。接下来将介绍其中一些法规。



提示：

本章讨论的美国法律都是联邦法律。但要记住，美国几乎每个州都针对计算机安全问题制定了某些形式的法律。由于互联网覆盖全球，大多数计算机犯罪都跨越了州的边界，因此属于联邦司法管辖范围内并在联邦法院系统中进行诉讼。然而，某些情况下，州法律可能比联邦法律更严格，处罚也更严厉。

1.《计算机欺诈和滥用法案》

《计算机欺诈和滥用法案》(CFAA)是美国针对网络犯罪的第一项重要立法。作为《全面控制犯罪法》(CCCA)的一部分，美国国会早在1984年就颁布了这个计算机犯罪相关法律。CFAA措辞谨慎，专门针对跨越州界的计算机犯罪，以免侵犯各州的权利和触犯宪法。在最初CCCA的主要条款中，将以下行为判定为犯罪：

- 未经授权或超出授权权限访问联邦系统中的机密信息或财务信息。
- 未经授权进入联邦政府专用的计算机。
- 使用联邦计算机进行欺诈(除非欺诈的唯一目的是使用计算机)。
- 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，从而妨碍或可能妨碍个人的检查、诊断、治疗或医疗护理。
- 非法交易计算机秘密，如果非法交易影响了州际贸易或涉及联邦计算机系统。

当国会通过CFAA时，将损失阈值从1000美元提高到5000美元，也显著改变了监管范围。该方案不再只针对处理敏感信息的联邦计算机，而改为针对涉及“联邦利益”的所有计算机。这把法案的适用范围扩大到包括以下方面：

- 美国政府专用的计算机。
- 金融机构专用的计算机。
- 如果被破坏，会妨碍政府或金融机构使用系统的任何专用计算机。
- 被组合起来实施犯罪的不在同一个州的所有计算机。

**提示：**

在准备 CISSP 考试时，请确保你能简要描述本章讨论的每个法律的用途。

2. 修正案

在 1994 年美国国会认识到，从 1986 年对 CFAA 进行最后一次修订起，计算机安全领域发生了巨大变化。于是对该法案进行了多次大范围修改。这些修改统称为《1994 年计算机滥用修正案》，其中包括以下条款：

- 宣布创建任何可能对计算机系统造成损害的恶意代码行为是不合法的。
- 修改 CFAA，使其适用于州际贸易中使用的所有计算机，而不仅适用于有“联邦利益”的计算机系统。
- 允许关押违法者，不管他们是否造成实际损坏。
- 为计算机犯罪的受害者提供了提起民事诉讼的法律授权，使他们可通过民事诉讼获得法令救济和损害赔偿。

在 1994 年第一次修正 CFAA 后，美国国会又分别在 1996 年、2001 年、2002 年和 2008 年通过了附加修正案，作为其他网络犯罪法律的一部分。本章将讨论这些修正案。

虽然 CFAA 可能用来起诉各种计算机犯罪，但也被安全和隐私界的许多人评判为过于宽泛。在某些解释中，CFAA 将违反网站服务条款的行为定为刑事犯罪。这项法律曾用来裁判麻省理工学院的学生 Aaron Schwartz，因为他从麻省理工学院网络上的数据库下载了大量的学术研究论文。Aaron 在 2013 年自杀，这个事件触发起草了 CFAA 修正案，该修正案从 CFAA 中删除了违反网站服务条款的行为。该法案被称为“Aaron 法案”，不过没有到国会进行表决。

3. 联邦量刑指南

1991 年颁布的联邦量刑指南对联邦法官判决计算机犯罪提供了处罚指南。指南中三个主要条款对信息安全界产生了持久影响。

- 指南正式提出谨慎人规则，该规则要求高级管理人员为“应尽关心”而承担个人责任。这条规则从财务职责领域发展而来，也适用于信息安全方面。
- 指南允许组织和高级管理人员通过证明他们在履行信息安全职责时实施了尽职审查，将对违规行为的惩罚降至最低。
- 指南概述了对于疏忽的三种举证责任。首先，被指控疏忽的人必须负有法律上不可推脱的责任。其次，被指控人员必须没有遵守公认的标准。最后，疏忽行为与后续的损害之间必然存在因果关系。

4. 1996 年的美国《国家信息基础设施保护法案》

1996 年，美国国会还通过了对《计算机欺诈和滥用法案》的另一项修正案，旨在进一步扩大保护范围。《国家信息基础设施保护法案》包括下列这些主要的新领域：

- 扩大 CFAA 范围，使其涵盖国际贸易中使用的计算机系统以及州际贸易中使用的系统。
- 将类似的保护扩展到计算系统以外的其他国家基础设施，如铁路、天然气管道、电网和电信线路。
- 将任何对国家基础设施关键部分造成损害的故意或鲁莽行为视为重罪。

5.《联邦信息安全管理法案》

2002年通过的《联邦信息安全管理法案》(FISMA)要求联邦机构实施涵盖机构运营的信息安全程序。FISMA还要求政府机构将合同商的活动纳入安全管理程序。FISMA废除并取代了之前的两个法案：1987年的《计算机安全法案》和2000年的《政府信息安全改革法案》。

美国国家标准与技术研究院(NIST)负责制定FISMA实施指南，下面概述有效的信息安全程序的组成要素：

- 定期评估风险，包括未经授权访问、使用、泄露、中断、修改或破坏信息和信息系统(用于支持组织运营)，以及组织资产可能受到的损害程度。
- 基于风险评估的策略和程序，以合理费用将信息安全风险降至可接受的水平，并确保将信息安全贯穿到组织信息系统的生命周期中。
- 为网络、设施、信息系统或信息系统群组提供适当的信息安全细分计划。
- 开展安全意识培训，告知员工(包括合同商和其他支持组织运营的信息系统用户)与他们的工作相关的信息安全风险，并告知他们有责任遵守组织为降低这些风险而设计的策略和程序。
- 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，但不少于每年一次。
- 规划、实施、评估和记录补救措施的过程，以解决组织信息安全策略、程序和实践中的任何缺陷。
- 检测、报告和响应安全事件的程序。
- 制定计划和程序，确保支持组织业务和资产的信息系统的业务连续性。

FISMA对联邦机构和政府承包商造成很大负担，要求他们必须编写和维护关于FISMA合规活动的大量文档。

6. 2014年的联邦网络安全法案

2014年，美国总统奥巴马签署了一系列法案，使联邦政府处理网络安全问题的方法与时俱进。

第一个是令人费解的《联邦信息系统现代化法案》(也被缩写为FISMA)。2014年的FISMA修改了2002年发布的FISMA的规则，将联邦网络安全责任集中到美国国土安全部。不过有两个例外情况：国防相关网络安全问题仍由美国国防部负责，而美国国家情报机构负责与情报相关的问题。

其次，美国国会通过了《网络安全增强法案》，该法案要求NIST负责协调全国范围内的自愿网络安全标准工作。NIST为联邦政府编制了与计算机安全相关的800系列特别出版物。这些出版物对所有安全从业人员都很有用，可在<http://csrc.nist.gov/publications/PubsSPs.html>上免费获得。

以下是NIST的常用标准。

- NIST SP 800-53：联邦信息系统和组织的安全和隐私控制。该标准适用于联邦计算系统，也常作为行业网络安全基准使用。
- NIST SP 800-171：保护非联邦信息系统和组织中受控的非分类信息。遵守该标准的安全控制(与NIST 800-53的安全控制非常相似)经常列入政府机构的合同要求。联邦承包商通常必须遵守NIST SP 800-171。

- NIST 网络安全框架(CSF)。是一套标准，旨在作为自发的基于风险的框架，用于保护信息和系统。

与这一波新要求相关的第三部法律是《国家网络安全保护法》。这部法律要求美国国土安全部建立集中的国家网络安全和通信中心。该中心充当联邦机构和民间组织之间的接口，共享网络安全风险、事件、分析和警告。

4.2.2 知识产权

在全球经济中，美国的角色正在从商品制造商向服务提供商转变。这种趋势也在世界上许多工业化国家体现出来。随着向服务提供商的转变，知识产权对很多公司来说越来越重要。实际上，许多大型跨国公司中最有价值的资产，只是我们都已认可的品牌名称。戴尔(Dell)、宝洁(Procter & Gamble)和默克(Merck)等公司的名称就是产品信誉的保证。出版公司、电影制片人和艺术家依靠他们的创作谋生。许多产品都依赖于秘方或生产工艺，如可口可乐或肯德基的草药与香料秘密配方。

这些无形资产统称为知识产权，并有一整套保护知识产权所有者权益的法律。毕竟，如果一家音乐商店只买艺术家的一份 CD，然后复制多份 CD 向所有顾客出售，将是不公平的，因为侵占了艺术家的劳动成果。接下来将探讨四种主要的知识产权类型，即版权、商标、专利和商业秘密，还将讨论信息安全专业人员应该如何关注这些概念。许多国家以不同方式保护(或不予保护)这些权利，但基本概念在全世界都是被认同的。

1. 版权和数字千年版权法

版权法保护“原创作品”的创作者，防止创作者的作品遭受未经授权的复制。有资格受到版权保护的作品有八大类：

- 文学作品
- 音乐作品
- 戏剧作品
- 喜剧和舞蹈作品
- 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

计算机软件版权是有先例的，它属于文学作品范畴。然而，重要的是要注意到版权法只保护计算机软件固有的表现形式，即实际的源代码，不保护软件背后的思想或过程。版权法是否扩展到保护软件包 UI 的“外观和感觉”还有一些争论。对这类问题，两种判定结果法院都给出过。如果卷入这类问题，应该向知识产权方面的资深律师进行请教，以确定当前的立法情况和法律案件。

获得版权有正式程序，包括向美国版权局发送受保护作品的副本和适当的注册费。有关这一过程的更多信息，请访问官方网站 www.copyright.gov。然而要注意，正式注册版权并不是实施版权的先决条件。事实上，法律规定作品的创作者从作品创作的那一刻起就自动拥有版权。如果能在法庭上证明你是作品的创作者，你就受到版权法的保护。正式的注册仅是让政府确认

在特定日期收到了你的作品。

版权总是默认归作品的创作者所有。对这个规定的特例是：因受雇而创作的作品。

员工在日常工作中创造出来的作品被认为是因受雇而创作的作品。例如，在公司公共关系部门的员工写了一篇新闻稿，这份新闻稿就被认为是受雇而创作的作品。当在书面合同中说明了因受雇而创作作品时，那也是因受雇而创作的作品。

现在的版权法提供了一个相当长的保护期。一个或多个作者的作品，被保护的时间是最晚一位去世作者离世后的 70 年。因受雇而创作的作品和署名作品被保护的时间是：第一次发表日期后的 95 年，或从创建之日起的 120 年，这两个时间中较短的一个。

1998 年，美国国会认识到快速变化的数字领域正在延伸到现有版权法的范围。为应对这一挑战，国会颁布了备受争议的《数字千年版权法》(DMCA)。DMCA 也让美国的版权法符合世界知识产权组织(WIPO)条约中的两个条款。

DMCA 的第一个主要条款是阻止那些试图规避版权所有者对受保护作品采用的保护机制的企图。这一条款的目的是防止复制数字介质，如 CD 和 DVD。DMCA 规定，对侵犯处以最高 100 万美元的罚款和 10 年监禁。图书馆和学校等非营利机构不受这一条款的约束。

DMCA 还限制了当罪犯利用 ISP 线路从事违反版权法的活动时 ISP 应该承担的责任。DMCA 认识到互联网服务提供商的法律地位与电话公司“公共运营商”的地位类似，不要求他们对用户的“临时性活动”承担责任。为符合豁免条款的资格，服务提供商的活动必须符合以下要求(直接引用 1998 年 12 月美国版权办公室摘要，DMCA 1988)：

- 传输必须由提供商以外的人发起。
- 传输、路由、连接的提供或复制必须由自动化技术过程执行，而不需要服务提供商进行选择。
- 服务提供商不能确定数据的接收者。
- 任何中间副本通常不能被预期收件人以外的任何人访问，而且保留期限不得超过合理需要的时间。
- 数据必须在不改变内容的情况下传输。

DMCA 还免除了服务提供商与系统缓存、搜索引擎和个人用户在网络上存储信息相关的活动。但这些情况下，服务提供商必须在收到侵权通知后立即采取行动，删除受版权保护的内容。

美国国会还在 DMCA 中规定，允许备份计算机软件和任何维护、测试或复制软件的日常使用活动。这个规定仅适用于被许可在特定计算机上使用的软件，其使用符合许可协议，且当这些备份不再被许可的活动需要时应当立刻被删除。

最后，DMCA 说明了版权法条款在互联网上音频和/or 视频数据流中的应用。DMCA 声明，这些使用被视为“合格的非预期传输”。

2. 商标

版权法用于保护创造性作品，对于用来辨识公司及其产品或服务的文字、口号和标志的商标也有保护机制。例如，一家企业可能获得其销售手册的版权，以确保竞争对手不能复制其销售材料。该企业还可能寻求商标保护，从而保护公司名称以及提供给客户的特定产品与服务的名称。

保护商标的宗旨是在保护个人与组织的知识产权的同时避免市场混乱。与版权保护一样，商标不需要正式注册就能获得法律保护。如果在公共活动中用到某个商标，你会自动获得

相关商标法律的保护，可使用™符号来表明想要保护作为商标的文字或标语。如果想要官方认可你的商标，可向美国专利商标局(USPTO)注册。这一过程通常需要律师对已存在的商标进行一次全面的尽职审查，排除注册障碍。整个注册过程从开始到结束可能需要一年多的时间。一旦收到来自 USPTO 的注册证书，即可使用®符号来表示这是已注册的商标。

商标注册的一个主要好处是可注册一个打算使用(但未必现在使用)的商标。这种申请类型称为意向使用申请，从提供文档的申请之日起保护商标，前提是在特定期限内真正在商业活动中使用该商标。如果选择不向 USPTO 注册商标，那么对商标的保护只有在第一次使用时才开始。

在美国接受商标申请需要满足两个重点要求：

- 该商标不能与其他商标类似，以免造成混淆。这需要律师在尽职审查期间予以确定。在该商标开放接受反对意见期间，其他公司可对申请的商标提出质疑。
- 该商标不能是所提供的产品与服务的说明。例如，“Mike's Software Company”就不是一个好的商标候选名称，因为它描述了公司生产的产品。如果 USPTO 认为商标具有描述性，可能拒绝批准申请。

在美国，商标批准后的初始有效期为 10 年，到期后可按每次 10 年的有效期延续无数次。

3. 专利

“专利”保护发明者的知识产权。专利提供 20 年的保护期限，在此期间发明者具有独家使用该发明的权利(直接使用或通过许可协议使用)。在专利专有期结束后，该发明在公共领域允许任何人使用。

专利有三个重点要求：

- 发明必须具有新颖性。只有创意新颖的发明才能获得专利。
- 发明必须具有实用性。发明必须能实际使用并完成某种任务。
- 发明必须具有创造性，不能平淡无奇。例如，你不能把用喝水的杯子收集雨水这个想法申请专利，因为这是一个平淡无奇的解决方案。不过，你可能使用这个方案申请到专利：一种特殊设计的水杯，能在收集尽可能多雨水的同时最大限度减少蒸发。

在技术领域，专利一直用来保护硬件设备和制造过程。在那些领域，有非常多的发明者受到专利保护的先例。最近还发布了涉及软件程序和类似机制的专利，但科技界对这些专利存在争议，认为其中许多专利过于宽泛。这些宽泛的专利的发行，导致了仅靠持有专利生存的公司的业务演变。这些公司对他们认为侵犯了自己公司专利的公司提起法律诉讼来获取赔偿。这些公司在科技界被称为“专利流氓”。

4. 商业秘密

许多公司拥有对其业务来说极其重要的知识产权，如果这些知识产权被泄露给竞争对手或公众，将造成重大损失。这些知识产权就是商业秘密。之前提到流行文化中这类信息的两个例子，可口可乐的秘密配方和肯德基的“草药和香料的混合秘密”。其他例子还有很多，制造公司可能想要对只有少数关键员工完全了解的某个制造过程保密，或统计分析公司可能想对为内部使用而开发的先进模型进行保密。

可用前面讨论的版权和专利这两种知识产权来保护商业秘密信息，但存在如下两个主要缺点。

- 申请版权或专利需要公开透露作品或发明细节。这将自动消除所有物的“秘密”性质，由于消除了所有物的神秘性或允许不择手段的竞争者通过违反国际知识产权法复制该所有物而对本公司造成伤害。
- 版权和专利提供的保护都有时间期限。一旦合法保护到期，其他公司可随意使用你的工作成果，而且他们拥有在你申请过程中公开的所有细节！

实际上商业秘密有一个官方程序。根据商业秘密的特性，你不必向任何人登记而是自己持有它们。为保守商业秘密，必须在组织中实施充分控制，确保只有经过授权的、需要知道秘密的人员才能访问它们。还必须确保任何拥有访问权限的人都遵守保密协议(NDA)的规定，不会与他人共享信息，并对违反协议的行为给予惩罚。请咨询律师确保保密协议在法律允许的最长期限内有效。此外，必须采取措施证明你重视并保护了知识产权，否则可能导致商业秘密保护的失效。

保护商业秘密是保护计算机软件的最佳方法之一。如前所述，专利法没有对计算机软件产品提供足够保护。版权法只保护源代码的实际文本，并不禁止其他人以不同形式重写代码并实现同一目标。如果将源代码视为商业机密，那么首先需要不让竞争对手拿到源代码。这是微软等大型软件开发公司用来保护核心技术知识产权的基础。

1996年《经济间谍法案》

商业秘密通常是大公司“至宝”，当美国国会于1996年颁布《经济间谍法案》时，美国政府认识到保护这类知识产权的重要性。该法案中有两个主要规定：

- 任何窃取美国商业机密并意图从外国政府或代理人获取相关利益的个人，可能被罚款50万元美金和最高15年的监禁。
- 其他情况下窃取商业秘密的人员可能被处以最高25万美元的罚款和最高10年的监禁。

《经济间谍法案》条款真正保护商业秘密所有者的知识产权。执行这项法律要求公司采取充分的措施，确保他们的商业秘密得到很好保护，而不是被意外地放入公共领域。

4.2.3 许可

安全专业人员还应熟悉与软件许可协议相关的法律问题。目前有四种常见的许可协议类型。

- 合同许可协议使用书面合同，列出软件供应商和客户之间的责任。这些协议适用于高价和/或特别专业化的软件包。
- 开封生效许可协议被写在软件包装的外部。它们通常包括一个条款，指出只要打开包装上的收缩包装封条就被视为认可合同。
- 单击生效许可协议正变得比开封生效协议更常见。在这类协议中，合同条款要么写在软件包装盒上，要么包含在软件文档中。在安装过程中，要求用户单击一个按钮来表明已阅读并同意遵守这些协议条款。这增加了对协议流程的积极认可，确保个人在安装前知道许可协议的存在。
- 云服务许可协议将单击生效许可协议发挥到极致。大多数云服务不需要任何形式的书面协议，只在屏幕上快速显示法律条款以供检阅。某些情况下，可能简单地提供法律条款的链接以及用户确认已阅读并同意这些条款的确认框。大多数用户在急于访问一个

新服务时，只是单击“确认”按钮而没有真正阅读协议条款，就可能无意中让整个组织承受繁杂的法律责任条款与条件。



注意：

行业组织提供有关软件许可的指导和实施活动。可从他们的网站上获得更多信息。一个主要的软件联盟组织是 www.bsa.org。

4.2.4 进口/出口控制

美国联邦政府认识到，驱动互联网和电子商务发展的计算机与加密技术，还可在军事领域成为极强大工具。因此，在冷战期间，美国政府制定了一套复杂的规章制度以管制向其他国家出口敏感的硬件和软件产品，管理跨国界流动的新技术、知识产权和个人身份信息。

直到最近，除了少数几个盟国外，从美国对外出口高性能计算机是很困难的事情。对加密软件的出口控制更严格，实质上几乎不可能从美国向国外出口任何加密技术。最近联邦政策有些变化，放松了这些限制，提供了更开放的商业环境。

1. 计算机出口控制

目前，美国企业可向几乎所有国家出口高性能计算系统，而不必事先得到政府的批准。

2. 加密技术出口控制

美国商务部工业和安全局向美国境外出口加密产品做了相关规定。根据之前的規定，即使从美国出口较低级别的加密技术也是不可能的。这使得美国软件制造商在与没有这些限制的外国公司竞争时处于不利地位。经过软件企业的长期游说后，美国总统指示商务部修改了相关规定以促进美国安全软件业的发展。

目前的监管规定指定了零售和大众市场安全软件的类别。现在这些规定允许公司提交这些产品供商务部审查，审查时间不超过 30 天。审查成功后，公司可自由地出口这些产品。

4.2.5 隐私

多年来隐私权在美国一直是备受争议的话题。争论的主要原因是宪法的权利法案没有明确规定隐私权。然而，这一权利已得到许多法院的支持，美国公民自由联盟(ACLU)等组织也在积极追求这项权利。

欧洲也一直关注个人隐私。事实上，瑞士等国以其保守金融秘密的能力闻名世界。稍后将研究欧盟数据隐私方案如何影响公司和互联网用户。

1. 美国隐私法

虽然没有宪法保障隐私，但很多联邦法律(许多是近年来颁布的)可用于保护政府维护的隐私信息，这些隐私信息与公民以及金融、教育和医疗机构等私营部门的关键部分有关。接下来将研究一些联邦法律。

第四修正案 隐私权的基础是美国宪法的第四修正案。全文如下：

公民的人身、住宅、文件和财产不受无理搜查和扣押的权利，不得受到侵犯。除依照合理根据，以宣誓或代替宣誓保证，并具体说明搜查地点和扣押的人或物，不得发出搜查和扣押状。

该修正案的直接解释防止政府机构在没有搜查令和合理理由的情况下搜查私人财产。法院扩大了第四修正案的适用范围，包括针对窃听和其他侵犯隐私行为的保护。

1974年《隐私法案》 1974年颁布的《隐私法案》是对美国联邦政府处理公民个人隐私信息的方式进行限制的一部最重要的隐私法。它严格限制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其他人或其他机构透露隐私信息的能力。它还规定了人口普查、执法、国家档案、健康和安全以及法院命令等方面例外情况。

《隐私法案》规定政府机构只保留业务运作所需的记录，并在政府的合法职能不再需要这些记录时销毁它们。这个法案为个人提供了正式程序，可让个人查阅政府留存的与己相关的记录，并要求修改错误记录。

注意：



1974年颁布的《隐私法案》只适用于政府机构。许多人误解了这项法律，认为它适用于公司和其他组织处理敏感的个人信息，但事实上并非如此。

1986年颁布的《电子通信隐私法案》《电子通信隐私法案》(ECPA)将侵犯个人电子隐私的行为定义为犯罪。该法案扩大了以前只针对通过物理线路进行通信的《联邦政府监听法案》的范围，适用于任何非法拦截电子通信或未经授权访问电子存储数据的行为。它禁止拦截或泄露电子通信，并定义公开电子通信的合法情况。该法案可防止对电子邮件和语音邮件通信的监控，并防止这些服务的提供者对其内容进行未经授权的披露。

ECPA最著名的规定是将对手机通话的监听定义为非法。事实上，这种监控可被处以最高500美元的罚款和最高5年的监禁。

1994年颁布的《通信执法协助法案》 1994年颁布的《通信执法协助法案》(CALEA)在1986年被重命名为《电子通信隐私法案》。CALEA要求所有通信运营商，无论使用何种技术，都要允许持有适当法院判决的执法人员进行窃听。

1996年《经济间谍法案》 1996年颁布的《经济间谍法案》将财产的定义扩大到包括专有经济信息，从而可将窃取这类信息视为针对行业或企业的间谍行为。这改变了偷窃的法律定义，使其不再受物理约束的限制。

1996年颁布的《健康保险流通与责任法案》(HIPAA) 1996年，国会通过了对医疗保险和健康维护组织(HMO)的法律进行的大量修改。

HIPAA的规定包括隐私和安全法规，要求医院、医生、保险公司和其他处理或存储私人医疗信息的组织采取严格的安全措施。

HIPAA还明确规定了作为医疗记录主体的个人的权利，并要求维护这些记录的组织以书面形式表明这些权利。

提示：



HIPAA隐私和安全法规相当复杂。你应该熟悉这里提到的该法案的广泛用途。如果你在医疗行业工作，应当考虑花些时间深入研究这部法律条款。

2009年颁布的《健康信息技术促进经济和临床健康法案》 2009年，美国国会通过《健康

信息技术促进经济和临床健康法案》(HITECH)来修订 HIPAA。该法案更新了 HIPAA 的许多隐私和安全要求，并在 2013 年通过 HIPAA Omnibus Rule 实施。

新法规要求的一个变化是法律对待商业伙伴的方式，商业伙伴指处理受保护的健康信息(PHI)的组织，代表 HIPAA 约束的实体。受约束实体与商业伙伴之间的任何关系都必须受商业伙伴协议(BAA)的书面合同约束。根据新规定，商业伙伴与受约束实体一样，直接受到 HIPAA 和 HIPAA 执法活动的约束。

HITECH 新增了数据泄露通知要求。根据 HITECH 违约通知规则，受 HIPAA 约束的实体如果发生数据泄露，必须将信息泄露情况通知到受影响的个人，当信息泄露影响到超过 500 人时，必须通知卫生与社会服务部门和媒体。

《数据泄露通知法案》

HITECH 的数据泄露通知法案之所以如此特别，是因为它是一项由联邦法律授权对受影响的个人进行通知的规定。除了医疗记录要求外，在美国各州之间对数据泄露通知的要求差别很大。

2002 年，加州通过了 SB 1386 法案，成为第一个需要立即向个人告知已知或疑似个人信息被泄露的州。个人信息包括个人姓名和下列任意信息的未加密内容：

- 社会安全号码。
- 驾驶执照号码。
- 国家身份证识别卡号码。
- 信用卡或借记卡号码。
- 与安全代码、访问代码或口令相结合的银行账户号码，允许对账户进行访问。
- 医疗记录。
- 健康保险信息。

在 SB 1386 颁布后的几年中，其余大部分州仿照加州的数据泄露通知法案制定了类似的规定。截至 2017 年底，只有 Alabama 和 South Dakota 还没有与此相关的州级法律。

对于州级数据泄露通知法案的完整列表，请参阅 www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx。

1998 年颁布的《儿童在线隐私保护法》 2000 年 4 月，《儿童在线隐私保护法》(COPPA) 成为美国法律。

COPPA 对关注儿童或有意收集儿童信息的网站提出一系列要求。

- 网站必须有隐私声明，明确说明所收集信息的类型和用途，包括是否有任何信息泄露给第三方。隐私通知还必须包括网站运营商的联系信息。
- 必须向父母提供机会，复查从孩子那里收集的任何信息，并可从网站记录中永久删除这些信息。
- 如果儿童的年龄小于 13 岁，在收集任何信息前，必须征得父母的同意。法律中有例外情况，允许网站为获得父母的同意而收集最少量的信息。

《Gramm-Leach-Bliley 法案》(1999 年) 直到《Gramm-Leach-Bliley 法案》(GLBA)于 1999 年成为法律，对金融机构才有了严格的监管规定。银行、保险公司和信贷提供商在提供服务和分享信息方面受到严重限制。GLBA 在一定程度上放宽了对每个组织提供服务的规定。当美国

国会通过这项法律时，意识到这一范围的扩大可能对隐私产生深远影响。基于这个顾虑，该法案包括对同一公司的子公司之间交换的多类信息的限制，并要求从2001年7月1日起，金融机构向所有客户提供书面的隐私政策。

2001年颁布的《美国爱国者法案》 作为对2001年9月11日在纽约和华盛顿发生的恐怖袭击的直接回应，美国国会在2001年通过了《美国爱国者法案》，该法案提供了拦截和阻止恐怖主义所需的适当法律工具。《美国爱国者法案》大大扩展了执法机构和情报机构在多个领域的权力，包括监控电子通信。

《美国爱国者法案》带来的一个重大变化是政府机构获得监听授权的方式。此前，警方在证实通信线路由监控对象使用后每次只能获得对一条线路的监听授权。《美国爱国者法案》中有条款允许官方机构获得针对个人的一系列监听授权，然后可根据这一项授权监听某个人的所有通信线路。

《美国爱国者法案》带来另一个主要变化是政府处理ISP信息的方式。根据《美国爱国者法案》的条款，网络服务提供商可自愿向政府提供大量信息。《美国爱国者法案》还允许政府通过传票获取用户活动的详细信息(而非监听)。

最后，《美国爱国者法案》修正了《计算机欺诈和滥用法案》(另一修正案)，对犯罪行为施加更严厉的惩罚。《美国爱国者法案》规定了最长20年的监禁，再次扩大了CFAA的适用范围。

《美国爱国者法案》具有复杂的立法历史。《美国爱国者法案》中的许多关键条款在2015年到期，当时美国国会未能通过更新的法案。不过美国国会在2015年6月通过了《美国自由法案》，其中保留了《美国爱国者法案》中的关键条款，《美国自由法案》将在2019年12月过期，除非美国国会再次通过这些条款。

《家庭教育权利和隐私法案》 《家庭教育权利和隐私法案》(FERPA)是另一种特殊的隐私法案，影响着所有接受联邦政府资助的教育机构(绝大多数学校)。该法案对18岁以上的学生和未成年学生的父母赋予了明确的隐私权。FERPA的具体保护措施包括：

- 父母/学生有权检查学校对学生的任何教育记录。
- 父母/学生有权要求更正他们认为错误的记录，并有权在记录中包括对任何未更正记录的声明陈述。
- 除特殊情况外，学校不得在未经书面同意的情况下公布学生记录中的个人信息。

《身份盗用与侵占防治法》 在1998年，美国总统签署了《身份盗用与侵占防治法》，使其成为法律。此前，身份盗用的唯一合法受害者是被欺诈的债权人。该法案将身份盗用定义为针对被盗用身份个人的犯罪行为，并规定了对所有违法人员处以严厉处罚(最高可判处15年监禁和/或25万美元罚款)。



真实场景

工作场所的隐私

本书一位作者最近与一位亲戚在家庭圣诞聚会进行了一次有趣的谈话。这位亲戚谈到他在网上看到的关于本地公司的几位员工因滥用互联网权限被解雇的事。这位亲戚备感震惊，认为公司侵犯了员工的隐私权。

正如你在本章看到的，美国法院系统长期坚持“传统的隐私权是宪法基本权利的延伸”。然而法院认为这项权利的一个要素是，只有在“隐私预期”合理时，才能保证隐私。例如，如果

你向某人寄一封被密封的信件，你就有理由期望它在邮寄途中不被拆开阅读，这个隐私预期是合理的。另一方面，如果你通过明信片传递信息，你要意识到在明信片到达接收方之前可能有一人或多人看过你的信息，因为这种情况下没有合理的隐私预期。

最近的法庭裁决已表明，员工在工作场所使用雇主的所有通信设备时，对隐私没有合理的预期。如果你使用雇主的计算机、网络、电话或其他通信设备发送信息，雇主可将其作为常规的商务程序进行监控。

如果打算监控员工的通信，应采取合理的预防措施，以确保没有隐含的隐私预期。下面是一些可供参考的常见措施：

- 雇佣合同的条款规定雇员在使用公司设备时没有隐私期望。
- 在公司可接受的使用和隐私政策中作出类似的书面声明。
- 在登录框中警示所有通信都受到监控。
- 在计算机和电话上贴上警告标签来警告监视。

与本章讨论的许多问题一样，在进行任何通信监视前咨询法律顾问是一个好做法。

2. 欧盟隐私法

1995 年 10 月 24 日，欧盟议会通过了一项全面性法令，概述了为保护信息系统中处理的个人数据必须采取的隐私措施。该法令在 3 年后(即 1998 年 10 月)起生效。该法令要求对所有个人数据的处理都符合以下标准之一：

- 同意
- 合同
- 法律义务
- 数据主体的重大利益
- 平衡数据所有者和数据主体之间的利益

该法令还概述了数据被持有和/或处理的个人关键权利：

- 访问数据的权利
- 有权知道数据的来源
- 纠正不准确数据的权利
- 某些情况下不同意处理数据的权利
- 这些权利被侵犯时可采取法律行动的权利

即使是欧洲以外的组织，根据跨境数据流的规定，也必须考虑这些规定的适用情况。当欧盟公民的个人信息离开欧盟时，那些发送数据的人必须确保数据仍受到保护。在欧洲开展业务的美国公司可根据欧盟和美国之间的隐私盾(Privacy Shield)协议进行数据保护，隐私盾协议允许美国商务部和联邦贸易委员会(FTC)对遵守规定的企业进行认证，并为他们提供“安全港”免遭诉讼。

注意：



你可能听说过在 2015 年 10 月，欧洲法院宣布废除美国和欧盟之间的安全港协议。这是事实，使用安全港协议的公司在接下来的 9 个月依然是合法的。隐私盾协议于 2016 年 7 月被欧盟委员会批准，取代了被废除的安全港协议。

为获得受隐私盾协议保护的资格，在欧洲开展业务的美国公司在处理个人信息时必须满足以下七项要求：

告知个人数据处理情况 公司必须在其隐私政策中包含对隐私盾原则的承诺，并使其可通过美国法律强制执行。公司还必须告知个人在隐私盾框架下的个人权利。

提供免费和易用的纠纷解决方案 实施隐私盾协议的公司必须在 45 天内回应消费者的任何投诉，并接受包括有约束力的仲裁的起诉程序。

与美国商务部合作 遵守隐私盾协议的公司必须提供信息，及时回应由美国商务部发出的与隐私盾实施相关的请求。

维护数据完整性和目的限制 实施隐私盾协议的公司必须只收集和保留与其声明的收集信息目的相关的个人信息。

确保数据被转移给第三方的责任 隐私盾协议的实践者在向第三方传输信息前必须遵守严格的要求。这些要求旨在确保数据转移是为了受限和特定的目的，而且接收者将充分保护信息的隐私。

执法行动的透明度 如果隐私盾实践者因未能遵守程序而收到执法行动或法院命令，则必须公开提交给 FTC 的任何合规或评估报告。

确保承诺在持有数据期间都有效 只要保留了根据协议收集的信息，离开隐私盾协议的组织必须继续每年对其合规性进行认证。



提示：

有关美国公司可用的隐私盾保护框架的更多信息，请访问 FTC 的隐私盾网站：
<https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework>。

3. 欧盟《通用数据保护条例》

2016 年，欧盟通过了一项涵盖个人信息保护的综合性新法律。《通用数据保护条例》(GDPR) 于 2018 年 5 月 25 日生效，取代了之前的数据保护法令。这项法律旨在针对整个欧盟的数据提供独立的、统一的法律。

GDPR 与数据保护法令的一个主要区别在于扩大了监管范围。新法律适用于所有收集欧盟居民数据或代表某人处理这些信息的组织。重要的是，这项法律甚至适用于收集欧盟居民信息的非欧盟组织。根据法院对这一条款的解释，因为其广泛的覆盖范围，GDPR 具有国际性。欧盟能否在全球范围内执行这项法律目前还是一个待确定的问题。

GDPR 的一些主要规定如下：

- 数据泄露通知要求公司在 24 小时内将严重的数据泄露情况通知官方机构。
- 在每个欧盟成员国建立集中化数据保护机构。
- 规定个人可访问自己拥有的数据。
- 数据可移植性规定将根据个人要求促进服务提供商之间的个人信息传输。
- “遗忘权”允许人们要求公司删除不再需要的个人信息。

4.3 合规

近十年来，信息安全监管环境日趋复杂。组织可能发现自己受制于各种法律(其中许多法律在本章前面提到过)和由监管机构或合同义务强制实施的规定。



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(PCI DSS)是合规要求的一个好例子，它不是由法律而是由合同义务规定的。PCI DSS 管理信用卡信息的安全性，通过接受信用卡的企业与处理业务交易的银行之间的商业协议条款来强制执行。

PCI DSS 有 12 个主要要求。

- 安装和维护防火墙配置以保护持卡人数据。
- 不要使用由供应商提供的默认系统密码和其他默认安全参数。
- 保护存储的持卡人数据。
- 在开放的公共网络加密传输持卡人数据。
- 保护所有系统免受恶意软件攻击并定期更新杀毒软件。
- 开发、维护安全系统和应用程序。
- 基于业务的知其所需原则，限制对持卡人数据的访问。
- 识别和验证对系统组件的访问。
- 限制对持卡人数据的物理访问。
- 跟踪和监控对网络资源和持卡人数据的所有访问。
- 定期测试安全系统和流程。
- 维护针对所有人员的信息安全的策略。

所有这些要求在完整的 PCI DSS 标准中详细说明，可在 www.pcisecuritystandards.org/ 上找到。

组织在处理许多相互重叠的(甚至相互矛盾的)合规需求时，需要认真规划。许多组织聘用全职 IT 合规人员，负责跟踪监管环境、监视控制，以确保持续合规，促进合规审计，并履行组织的合规报告责任。



警告：

代表商业组织存储、处理或传输信用卡信息的非商业组织也必须遵守 PCI DSS。例如，这个要求也适用于共享主机提供商。

组织可能要接受合规审计，审计者可能是标准的内部审计人员和外部审计师，也可能是监管机构或其代理机构。例如，组织的财务审计员可进行 IT 控制审计，确保组织财务系统的信息安全控制遵守《萨班斯-奥克斯利法案》(SOX)。一些法规(如 PCI DSS)可能要求组织雇用得到认可的独立审计师，来验证控制并直接向监管机构提供报告。

除了正式审计外，组织通常还必须向一些内部和外部股东报告法律合规情况。例如，组织的董事会(或董事会审计委员会)可能需要定期报告合规义务和状况。同样，PCI DSS 非强制性地要求组织进行正式的第三方审计，并提交一份关于合规状况的自我评估报告。

4.4 合同和采购

越来越多的用户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。这导致组织开始关注可在合同和采购过程中实施的安全审查和控制。安全专业人员应当审查供应商实施的安全控制，包括最初的供应商选择和评估流程，以及持续管理审查。

以下是这些供应商管理审查期间要包括的一些问题：

- 供应商存储、处理或传输哪些类型的敏感信息？
- 采取哪些控制措施来保护组织的信息？
- 如何区分组织的信息与其他客户的信息？
- 如果加密是一种值得信赖的安全机制，要使用什么加密算法和密钥长度？如何进行密钥管理？
- 供应商执行了什么类型的安全审计，客户对这些审计有什么访问权限？
- 供应商是否依赖其他第三方来存储、处理或传输数据？合同中有关安全的条款如何适用于第三方？
- 数据存储、处理和传输发生在哪些地方？如果客户和/或供应商在国外，会产生什么影响？
- 供应商的事件响应流程是什么？何时通知客户可能的安全破坏？
- 有哪些规定来持续确保客户数据的完整性和可用性？

上面只是需要关注问题的一个简短清单。应根据组织的具体关注事项、供应商提供的服务类型以及与他们共享的信息，调整安全审查范围。

4.5 本章小结

计算机安全必然需要法律团体的高度参与。在本章中，你了解了管理安全问题的法律，如计算机犯罪、知识产权、数据隐私和软件许可。

影响信息安全专业人士的法律主要有三类。刑法概述了严重侵犯公共信任的规则和制裁。民法为我们提供了进行商业处理的框架。政府机构利用行政法来颁布解释现行法律的日常法规。

管理信息安全活动的法律多种多样，覆盖了三种法律类别。有些是刑法，如《电子通信隐私法案》和《数字千年版权法》，违法行为可能导致刑事罚款和/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，许多政府机构颁布了影响特定行业和数据类型的行政法，如 HIPAA 安全规则。

信息安全专业人员应该了解其行业和业务活动的合规要求。跟踪这些要求是一项复杂任务，应分配给一个或多个合规专家，他们会监控法律的变化、业务环境的变化以及这两个领域的交叉点。

仅担心自己的安全性和合规性是不够的。随着越来越多地采用云计算，许多组织现在与云供应商共享敏感信息和个人数据。安全专业人员必须采取步骤，确保供应商与组织自身一样慎重处理数据，并满足任何适用的合规性要求。

4.6 考试要点

了解刑法、民法和行政法的区别。刑法保护社会免受违反我们所信仰的基本原则的行为的侵害。违反刑法的行为将由美国联邦和州政府进行起诉。民法为人与组织之间的商业交易提供了框架。违反民法的行为将通过法庭，由受影响的当事人进行辩论。行政法是政府机构有效地执行日常事务的法律。

能够解释旨在保护社会免受计算犯罪影响的主要法律的基本条款。《计算机欺诈和滥用法案》(修正案)保护政府或州际贸易中使用的计算机不被滥用。《电子通信隐私法案》(ECPA)规定侵犯个人的电子隐私是犯罪行为。

了解版权、商标、专利和商业秘密之间的区别。版权保护创作者的原创作品，如书籍、文章、诗歌和歌曲。商标是标识公司、产品或服务的名称、标语和标志。专利为新发明的创造者提供保护。商业秘密法保护企业的经营秘密。

能够解释 1998 年颁布的《数字千年版权法》的基本条款。《数字千年版权法》禁止绕过数字媒体中的版权保护机制，并限制互联网服务提供商对用户活动的责任。

了解《经济间谍法案》的基本条款。《经济间谍法案》对窃取商业机密的个人进行惩罚。当窃取者知道外国政府将从这些信息中获益而故意为之时，会受到更严厉的惩罚。

了解不同类型的软件许可协议。合同许可协议是软件供应商和用户之间的书面协议。开封生效协议写在软件包装上，当用户打开包装时生效。单击生效许可协议包含在软件包中，但要求用户在软件安装过程中接受这些条款。

理解对遭受数据破坏的组织的通告要求。加州颁发的 SB 1386 是第一个在全州范围内要求通知当事人其信息被泄露的法律。美国目前大多数州通过了类似法律。目前，联邦法律只要求受 HIPAA 约束的实体，当其保护的个人健康信息被破坏时，通知到个人。

理解美国和欧盟对管理个人信息隐私的主要法律。美国有许多隐私法律会影响政府对信息的使用以及特定行业信息的使用，例如处理敏感信息的金融服务公司和医疗健康组织。欧盟有非常全面的《通用数据保护条例》来管理对个人信息的使用和交换。

解释全面合规程序的重要性。大多数组织都受制于与信息安全相关的各种法律和法规要求。构建合规性程序可确保你能实现并始终遵守这些经常重叠的合规需求。

了解如何将安全纳入采购和供应商管理流程。许多组织广泛使用云服务，需要在供应商选择过程中以及在持续供应商管理过程中对信息安全控制进行审查。

4.7 书面实验

1. 美国和欧盟之间的隐私盾框架协议的主要条款是什么？
2. 在考虑外包信息存储、处理或传输时，组织应该考虑哪些常见问题？
3. 雇主采取哪些常见步骤来通知雇员会进行系统监控？

4.8 复习题

1. 哪个是第一部对病毒、蠕虫和其他对计算机系统造成危害的恶意代码的创造者进行惩罚的美国刑法？
 - A. 《计算机安全法案》
 - B. 《国家信息基础设施保护法案》
 - C. 《计算机欺诈和滥用法案》
 - D. 《电子通信隐私法案》
2. 哪部法律管理联邦机构的信息安全操作？
 - A. FISMA
 - B. FERPA
 - C. CFAA
 - D. ECPA
3. 哪类法律不要求美国国会在联邦层面实施，而由行政部门以法规、政策和程序的形式制定？
 - A. 刑法
 - B. 普通法
 - C. 民法
 - D. 行政法
4. 哪个联邦政府机构有责任确保不用于处理敏感和/或机密信息的政府计算机系统的安全？
 - A. 美国国家安全局
 - B. 美国联邦调查局
 - C. 美国国家标准与技术研究院
 - D. 美国特工处
5. 经修订的《计算机欺诈和滥用法案》可保护的最广泛计算机系统类别是什么？
 - A. 政府拥有的系统
 - B. 与联邦利益相关的系统
 - C. 州际贸易中使用的系统
 - D. 美国境内的系统
6. 哪部法律通过限制政府机构搜查私人住宅和设施的权力来保护公民的隐私权？
 - 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 最近创作了一个解决数学问题的新算法，他想与全世界分享。然而，在将软件代码发表在技术期刊前，他希望获得某种形式的知识产权保护。哪种类型的保护最能满足需要？
 - A. 版权
 - B. 商标
 - C. 专利
 - D. 商业秘密

8. Mary 是制造公司 Acme Widgets 的联合创始人。她与合作伙伴 Joe 一起开发了一种特殊的油，这种油将大大改善小部件的制造工艺。为保守配方的秘密，Mary 和 Joe 计划在其他工人离开后自行在工厂里大量制造这种油。她们希望尽可能长时间地保护这个配方。哪种类型的知识产权保护最能满足需要？

- A. 版权
- B. 商标
- C. 专利
- D. 商业秘密

9. Richard 最近打算为即将使用的新产品起一个好名字。他与律师进行了交谈，并提出了适当的申请，以保护产品名称，但还没有收到政府对申请的回复。他想立即开始使用这个名字。他应该在名字旁边用什么符号来表示它的受保护状态？

- A. ©
- B. ®
- C. ™
- D. †

10. 什么法律阻止政府机构披露个人在受保护的情况下向政府提供的个人信息？

- A. 《隐私法案》
- B. 《电子通信隐私法案》
- C. 《健康保险流通和责任法案》
- D. 《Gramm-Leach-Bliley 法案》

11. 什么框架允许美国公司证明其遵守欧盟隐私法？

- A. COBIT
- B. 隐私盾
- C. 隐私锁
- D. EuroLock

12. 《儿童在线隐私保护法》(COPPA)旨在保护使用互联网的儿童的隐私。在未经父母同意的情况下，公司可从孩子身上收集个人身份信息的最低年龄是？

- A. 13
- B. 14
- C. 15
- D. 16

13. 为获得《数字千年版权法》“临时性活动”条款的保护，以下哪一项不是互联网服务供应商必须满足的要求？

- A. 服务提供者和消息的发起者必须位于不同位置。
- B. 传输、路由、连接的提供或复制必须由自动化技术过程执行，而不需要服务提供商进行选择。
- C. 任何中间副本通常不得被预期接收者以外的任何人访问，而且保留期限不得超过必要的合理时间。
- D. 传输必须由提供商以外的人发起。

14. 下列哪一项法律并非旨在保护消费者和互联网用户的隐私权？
A. 《健康保险流通与责任法案》
B. 《身份盗用与侵占防治法》
C. 《美国爱国者法案》
D. 《Gramm-Leach-Bliley 法案》
15. 以下哪一种许可协议类型不要求用户在执行协议前承认他们已经阅读过协议？
A. 合同许可协议
B. 开封生效许可协议
C. 单击生效许可协议
D. 口头协议
16. 哪个行业最直接受到《Gramm-Leach-Bliley 法案》条款的影响？
A. 医疗保健
B. 银行
C. 执法机构
D. 国防承包商
17. 在美国，专利保护的标准期限是多少？
A. 自申请之日起 14 年
B. 自专利被授予之日起 14 年
C. 自申请日起 20 年
D. 自专利被授予之日起 20 年
18. 以下哪一项是欧盟于 2016 年通过并于 2018 年生效的关于数据隐私的综合法律？
A. DPD
B. GLBA
C. GDPR
D. SOX
19. 哪个合规责任与信用卡信息的处理有关？
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)的隐私和安全要求？
A. HITECH
B. CALEA
C. CFAA
D. CCCA

保护资产安全

本章涵盖的 CISSP 认证考试主题包括：

- ✓ 域 2：资产安全
 - 2.1 信息和资产的识别和分类
 - 2.1.1 数据分类
 - 2.1.2 资产分类
 - 2.2 界定及维护信息和资产所有权
 - 2.3 隐私保护
 - 2.3.1 数据所有者
 - 2.3.2 数据使用者
 - 2.3.3 数据残留
 - 2.3.4 收集限制
 - 2.4 确保适当的资产保留期
 - 2.5 确定数据安全控制
 - 2.5.1 理解数据状态
 - 2.5.2 范围界定和按需定制
 - 2.5.3 选择标准
 - 2.5.4 数据保护方法
 - 2.6 建立信息和资产处理要求

“资产安全”域的重点是在整个生命周期中收集、处理和保护信息。这个领域的一个主要工作是根据信息对组织的价值进行分类。所有后续操作都取决于分类。例如，高度机密的数据需要严格的安全控制。相比之下，非机密数据使用较少的安全控制。

5.1 资产识别和分类

资产安全的第一步是识别和分类信息和资产。组织常在安全策略中包含分类定义。然后，人员根据安全策略要求适当地标记资产。这里所述的资产包括敏感数据、用于处理它们的硬件和用于保存它们的介质。

5.1.1 定义敏感数据

敏感数据是任何非公开或非机密的信息，包括机密的、专有的、受保护的或因其对组织的价值或按照现有的法律和法规而需要组织保护的任何其他类型的数据。

1. 个人信息

个人信息(Personally Identifiable Information, PII)是任何可以识别个人的信息。美国国家标准与技术研究所(NIST)特别出版物(SP)800-122 提供了如下更正式的定义。

PII 是由机构保存的关于个人的任何信息，包括：

(A) 任何可用于识别或追踪个人身份的信息，如姓名、社会保险账号、出生日期、出生地点、母亲的娘家姓或生物识别记录。

(B) 与个人有联系或可联系的其他信息，如医疗、教育、金融和就业信息。

最重要的是，组织有责任保护 PII，包括与员工和客户相关的 PII。许多法律要求，在数据泄露导致 PII 丢失时，组织要通知个人。



提示：

对个人信息(PII)的保护推动了全世界(特别是北美和欧盟)对规则、法规和立法的隐私和保密要求。NIST SP 800-122 “个人信息信息保密指南”提供了关于如何保护 PII 的更多信息。可从 NIST 的特别出版物(800 系列)下载页面获得：<http://csrc.nist.gov/publications/PubsSPs.html>。

2. 受保护的健康信息

受保护的健康信息(Protected Health Information, PHI)是与特定个人有关的任何健康信息。在美国，《健康保险流通与责任法案》(HIPAA)要求保护 PHI。HIPAA 提供了 PHI 的更正式定义。

健康信息指以口头、媒介或任何形式记录的任何信息。

(A) 这些信息由如下结构设立或接收：卫生保健提供者、健康计划部门、卫生行政部门、雇主、人寿保险公司、学校或卫生保健信息交换所。

(B) 涉及任何个人的如下信息：过去、现在或将来在身体方面、精神方面的健康状况，向个人提供的健康保健条款；过去、现在或将来为个人提供医疗保健而支付的费用。

有些人认为只有像医生和医院这样的医疗保健机构才需要保护 PHI。然而，HIPAA 对 PHI 的定义更宽泛。任何提供或补充医疗保健政策的雇主都会收集并处理 PHI。组织提供或补充医疗保健政策是很常见的，所以 HIPAA 适用于美国的大部分组织。

3. 专有数据

专有数据指任何有助于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。如果竞争对手能访问专有数据，将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，但这是不够的。许多罪犯不注意版权、专利和商业秘密法律。同样，外国组织机构也窃取了大量机密数据。

5.1.2 定义数据分类

组织通常在其安全策略或单独的数据策略中包含数据分类。数据分类可识别数据对组织的价值，对于保护数据的保密性和完整性至关重要。这个策略识别出组织内使用的分类标签，还确定了数据所有者如何确定适当分类，以及人员如何根据分类保护数据。

例如，政府数据分类包括绝密(Top Secret)、秘密(Secret)、机密(Confidential)和未分类(Unclassified)。任何超过未分类级别的数据都是敏感数据，但很明显，它们具有不同价值。美国政府为这些分类提供了明确定义。注意每个定义除了几个关键字外措辞都很接近。绝密使用短语“异常严重的损害”，秘密使用短语“严重损害”，机密使用短语“损害”。

绝密标签是“未经授权的信息披露可能对国家安全造成异常严重的损害，而这正是最初的保密机构能够识别或描述的。”

秘密标签是“未经授权的信息披露会对国家安全造成严重损害，最初的保密机构能识别或描述这些信息。”

机密标签是“未经授权的披露会对国家安全造成损害，最初的分类机构能识别或描述”。

未分类数据指不符合绝密、秘密或机密数据描述的任何数据。在美国，任何人都可获得未分类数据，尽管通常要求个人使用《信息自由法》(FOIA)中确定的程序请求信息。

还有一些额外的子分类，如“官方使用”(For Official Use Only, FOUO)和“敏感但未分类”(Sensitive But Unclassified, SBU)。具有这些名称的文件要有严格控制，限制其分发。例如，美国国税局(IRS)对个人税务记录使用 SBU，限制对这些记录的访问。

分类机构是将原始分类应用于敏感数据的实体。严格的规则确定谁可以这样做。例如，美国总统、副总统和机构负责人可对美国的数据进行分类。此外，这些职位中的任何一个都可以授权其他人对数据进行分类。

虽然分类的重点通常是数据，但这些分类也适用于硬件资产。这包括处理或保存这些数据的任何计算系统或介质。

非政府组织很少需要根据对国家安全的潜在损害对数据进行分类。管理层关心的是对组织的潜在损害。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，组织不仅要考虑数据的敏感性，还要考虑数据的临界性。可使用美国政府在描述绝密、秘密和机密数据时使用的相同短语“异常严重的损害”“严重损害”和“损害”。

一些非政府组织使用 Class 3、Class 2、Class 1 和 Class 0 等标签。其他组织使用更有意义的标签，如机密/专有(Confidential/Proprietary)、私有(Private)、敏感(Sensitive)和公开(Public)。图 5.1 显示了左边的政府分类和右边的非政府分类之间的关系。正如政府可根据数据泄露可能带来的负面影响来定义数据一样，组织也可使用类似的描述。

政府和业界的分类都依据数据对组织的相对价值，在图 5.1 中，绝密代表政府的最高分类，机密代表组织的最高分类。然而，重要的是要记住，非政府组织可使用他们想要的任何标签。当使用图 5.1 中的标签时，敏感信息是指不属于未分类(使用政府标签时)或未公开(使用非政府组织分类信息时)的任何信息。下面将介绍一些常见的非政府分类的含义。请记住，尽管这些标准是常用的，但没有一个标准是所有非政府组织强制使用的。

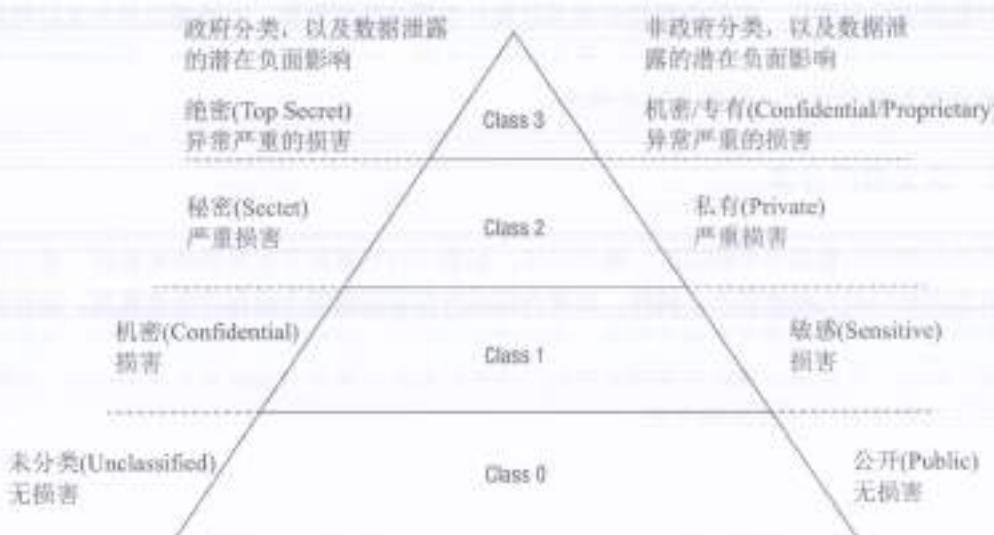


图 5.1 数据分类

机密/专有 机密/专有标签通常指最高级别的机密数据。在这方面，数据泄露将对本组织的任务造成异常严重的损害。例如，攻击者多次攻击索尼公司，窃取超过 100TB 的数据，包括未发行电影的完整版本。这些很快就出现在文件共享网站上，安全专家估计，人们下载这些电影的次数高达 100 万次。有了盗版电影，当索尼最终发行时，很多人选择不再观看。这直接触及索尼的底线。这些电影是专有的，该组织可能认为这是非常严重的损害。回顾过去，他们可能选择将电影贴上机密/专有标签，并使用最强大的访问控制来保护它们。

私有 私有标签指在组织中应该保持私有但不符合机密/专有数据定义的数据。在这方面，数据泄露将对本组织的任务造成严重损害。许多组织将 PII 和 PHI 数据标记为私有。将内部员工数据和一些财务数据标记为私有也很常见。例如，公司的工资单部门可访问工资单数据，但这些数据不对普通员工开放访问。

敏感 敏感数据与机密数据类似。这种情况下，数据泄露将对本组织的任务造成损害。例如，组织中的 IT 人员可能拥有关于内部网络的大量数据，包括布局、设备、操作系统、软件、IP 地址等。如果攻击者可方便地访问这些数据，那么他们发动攻击就会容易得多。管理层可能会决定，不想让公众知道这些信息，所以给这些信息贴上“敏感”标签。

公开 公开数据类似于非机密数据，包括发布在网站、手册或其他任何公共资源的信息。虽然组织不保护公开数据的保密性，但确实采取措施保护其完整性。例如，任何人都可查看发布在网站上的公开数据。但是，组织不希望攻击者修改数据，因此需要采取措施保护数据。



提示：

尽管有些来源将“敏感”信息称为非公开的数据，但许多组织将“敏感”信息用作标签。换句话说，“敏感”这个词在一个组织中可能意味着一件事，而在另一个组织中可能意味着另一件事。对于 CISSP 考试，请记住“敏感”信息常指任何非公开的信息。

民间组织不需要使用任何特定的分类标签。然而，重要的是要以某种方式对数据进行分类，并确保人员理解分类。不管组织使用什么标签，都有义务保护敏感信息。

对数据进行分类后，组织会根据分类采取额外步骤来管理数据。对敏感信息的未经授权的访问可能给组织造成重大损失。然而，基本的安全实践，如正确标记、处理、存储和销毁基于分类的数据和硬件资产，有助于防止损失。

5.1.3 定义资产分类

资产分类应与数据分类相匹配。换句话说，如果一台计算机正在处理绝密数据，那么这台计算机也应被归类为绝密资产。同样，如果内部或外部驱动器等介质保存绝密数据，该介质也应被归类为绝密资产。通常在硬件资产上使用清晰的标记，以便提醒人员可在资产上处理或存储数据。例如，如果用计算机处理绝密数据，计算机和显示器会有清晰而显著的标签，提醒用户可在计算机中处理的数据的分类。

5.1.4 确定数据的安全控制

定义了数据和资产分类后，重要的是要定义安全需求并识别安全控制以满足这些安全需求。假设组织已决定使用前述的机密/专有、私有、敏感和公开数据标签。然后，管理层决定制定一个数据安全策略，规定使用特定安全控制来保护这些类别中的数据。该策略可能处理存储在文件、数据库、服务器(包括电子邮件服务器)，用户系统中的数据，以及通过电子邮件发送和存储云中的数据。

在本例中，我们将数据类型限制为电子邮件。组织已定义了如何在每个数据类别中保护电子邮件。他们决定，任何公开类别的电子邮件都不需要加密。但在发送期间(传输中的数据)以及存储在电子邮件服务器(静止的数据)时，其他所有类别(机密/专有、私有、敏感)的电子邮件都必须加密。

加密将明文数据转换为密文，使其更难阅读。使用强加密方法，如带有 256 位加密密钥的高级加密标准(AES 256)，使得未经授权的人员几乎不可能读取文本。

表 5.1 显示了管理层在其数据安全策略中定义的其他电子邮件安全需求。请注意，级别最高的分类类别(机密/专有)中的数据具有安全策略中定义的最安全需求。

表 5.1 保护电子邮件数据

分类	电子邮件的安全要求
机密/专有 (任何数据的最高级别保护)	电子邮件和附件必须用 AES 256 加密 电子邮件和附件保持加密，除非查看 电子邮件只能发送到组织内的收件人 电子邮件只能被收件人打开和查看(转发的电子邮件不能被打开) 可以打开和查看附件，但不能保存 电子邮件内容不能复制、粘贴到其他文档中 电子邮件不能被打印出来
私有 (例如 PII 和 PHI)	电子邮件和附件必须用 AES 256 加密 除非在查看时，电子邮件和附件仍然加密 只能发送到组织内的收件人

(续表)

分类	电子邮件的安全要求
敏感 (机密资料的最低保障级别)	电子邮件和附件必须用 AES 256 加密
公开	电子邮件和附件可用明文发送

**注意：**

表 5.1 中列出的需求仅作为示例提供。任何组织都可使用这些需求或定义其他需求。

安全管理员使用安全策略中定义的需求来识别安全控制。对于表 5.1，主要的安全控制是使用 AES 256 进行强加密。管理员将确定使员工更容易满足安全需求的方法。

尽管可满足表 5.1 中的所有需求，但它们需要实现其他解决方案。例如，软件公司 Boldon James 销售一些产品，组织可使用这些产品来自动执行此类任务。在发送电子邮件前，用户要对其贴上相关标签(如机密、私有、敏感和公开)。这些电子邮件通过 DLP(数据丢失预防)服务器检测标签并应用所需的保护。

**注意：**

当然，Boldon James 并非唯一创建和销售 DLP 软件的组织。其他提供类似 DLP 解决方案的公司包括 TITUS 和 Spirion。

表 5.1 显示组织可能希望应用于电子邮件的需求。然而，组织不会就此止步。组织想要保护的任何类型的数据都需要类似的安全定义。例如，组织将定义存储在资产(如服务器)上的数据、存储在站点内外的数据备份以及专有数据的需求。

此外，身份和访问管理(IAM)安全控制有助于确保只有经过授权的人才能访问资源。第 13 章和第 14 章将深入地介绍 IAM 安全控制。

WannaCry 勒索病毒

人们可能还记得从 2017 年 5 月 12 日开始的 WannaCry 恶意勒索事件。它迅速蔓延到 150 多个国家，感染了 30 多万台计算机，瘫痪了多家医院、公共设施和大型组织，还有许多普通用户。和大多数勒索软件一样，它加密数据，并要求受害者支付 300~600 美元的赎金。

尽管病毒传播速度很快，感染了很多计算机，但犯罪分子的阴谋并未明显得逞。报告显示，与受感染系统的数量相比，支付的赎金数量较少。好消息是，大多数组织都了解数据的价值。即使受到勒索软件的攻击，由于有可靠的数据备份，因此能快速恢复它们。

5.1.5 理解数据状态

保护所有状态(包括静止、运动和使用)的数据是很重要的。

静态数据 静态数据是存储在系统硬盘、外部 USB 驱动器、SAN(存储区域网络)和备份磁盘等介质上的任何数据。

动态数据 传输中的数据(有时称为动态数据)是通过网络传输的任何数据。这包括使用有

线或无线方式通过内部网络传输的数据，以及通过公共网络(如 Internet)传输的数据。

使用中的数据 使用中的数据指应用程序使用内存或临时存储缓冲区中的数据。因为应用程序不能处理加密数据，所以必须在内存中对数据进行解密。

保护数据保密性的最佳方法是使用强加密协议，稍后将对此进行讨论。此外，强身份验证和授权控制有助于防止未经授权的访问。

例如，考虑一个 Web 应用程序，该 Web 应用程序检索信用卡数据，以便在用户允许的情况下快速执行电子商务交易。信用卡数据存储在单台数据库服务器上，并在静态、动态和使用中受到保护。

数据库管理员采取步骤加密存储在数据库服务器上的敏感数据(静止数据)。例如，将加密存储敏感数据(如信用卡数据)的列。此外，将实现强身份验证和授权控制，以防止未经授权的实体访问数据库。

当 Web 应用程序从 Web 服务器发送数据请求时，数据库服务器将验证 Web 应用程序是否有权检索数据，如果有权，数据库服务器将发送数据。然而，这需要几个步骤。例如，数据库管理系统首先检索和解密数据，并以 Web 应用程序可读取的方式对其进行格式化。然后，数据库服务器使用传输加密算法在传输数据前对其进行加密，以确保传输中的数据是安全的。

Web 服务器以加密格式接收数据，解密数据并发送给 Web 应用程序。Web 应用程序在给予交易授权时将数据存储在临时内存缓冲区中。当 Web 应用程序不再需要数据时，会采取步骤清除内存缓冲区，确保所有剩余的敏感数据完全从内存中删除。



注意：

身份盗窃资源中心(ITRC)定期跟踪数据泄露，该中心通过网站(www.idtheftcenter.org/)发布免费报告。在 2017 年，该中心追踪了 1300 多起数据泄露事件，曝光了超过 1.74 亿条已知记录。遗憾的是，这些泄密事件中被曝光的记录数量并不为公众所知。在此之前，每年都有越来越多的数据被入侵，而这些数据被入侵大多是由外部攻击者造成的。

5.1.6 管理信息和资产

管理敏感数据的一个关键目标就是阻止数据泄露。数据泄露指未获授权的实体查阅和访问敏感数据。如果你留意这方面新闻，会知道这经常发生。大的数据泄露如 2017 年的 Equifax 攻击主流新闻网站。攻击者窃取了约 14 300 000 个美国人的信息，包括身份证号、姓名、地址和出生日期。

或许你从未听说过较小的数据泄露，但实际上它们是定期发生的，在 2017 年平均每周发生超过 25 次数据泄露。下面是组织内人员为限制数据泄露所遵循的基本步骤。

1. 标记敏感数据和资产

标记敏感信息(即添加标签)确保用户可方便地识别任何数据的分类级别。标记(或标签)提供的最重要信息是数据类别。例如，一个绝密标签向任何看到该标签的人表明该信息被分类为绝密。当用户知道数据的价值时，他们更可能根据分类，采取适当步骤来控制和保护它。标签包括物理和电子标签。

物理标签表示存储在介质或在系统的数据的安全类别。例如，如果备份磁带携带秘密数据，则物理标签会附着在磁带上，向用户表明它携带秘密数据。与此类似，如果计算机处理敏感信息，则计算机将有一个表示它所处理信息的最高分类的标签。常用于处理机密、秘密和绝密数据的计算机应该用标签标记。物理标签在整个生命周期内会一直存留在系统或介质上。



提示：

许多组织使用颜色编码硬件来帮助标记。例如，一些组织大量购买红色USB闪存驱动器，目的是让人员只能将保密数据复制到这些闪存驱动器上。技术安全控制使用一个通用唯一标识符(UUID)来标识这些闪存驱动器，并可执行安全策略。DLP系统可阻止用户将数据复制到其他USB设备，并确保当用户将数据复制到这些设备时对数据进行加密。

标签还包括使用数字标记或标签。一种简单方法是将分类标签放在文档的页眉或页脚，或将其嵌入水印。这些方法的优点是它们会出现在打印出的资料上。即使用户的打印输出上包括页眉和页脚，大多数组织都要求用户将打印出来的敏感文献放在一个含标签的文件夹中或在封面上清晰地标明分类。头信息并不仅限于文件。备份磁带通常包括头信息，分类信息可包含在该头信息中。

页眉、页脚和水印的另一个好处是，DLP系统可识别包括敏感信息的文档，并应用适当的安全控制。一些DLP系统在检测到文档被分类时也会向文档添加元数据标签。这些标签有助于理解文档内容，并帮助DLP系统适当地处理文档。

类似地，一些组织在其计算机上指定特定的桌面背景。例如，用于处理专有数据的系统可能有黑色桌面背景，“专有”一词为白色和橙色粗边框，背景还可包括诸如“此计算机处理专有数据”之类的语句和提醒用户保护数据的语句。

在许多安全的环境中，也会对未分类的介质和设备使用标签。这可以防止未标记敏感信息的遗漏错误。例如，如果未标记保存敏感数据的备份磁带，用户可能认为它保存着未分类的数据。然而，如果组织也标记了未分类的数据，则未标记的介质将很容易被察觉，用户将更慎重地查看未加标记的磁带。

组织通常通过特定程序来降级介质。例如，如果备份磁带包含机密信息，管理员可能希望将磁带降级为未分类的。组织将用一个可信程序清除磁带上所有可用数据。管理员清除磁带数据后，可以降级，并替换标签。

然而，许多组织完全禁止介质降级。例如，数据策略可能禁止降级包含绝密数据的备份磁带。相反，该策略可能要求在该磁带生命周期结束时销毁该磁带。同样，降级一个系统是罕见的。换言之，如果一个系统一直在处理绝密数据，那么很少会把它降级或将重新标记为未分类系统。任何情况下，都需要建立已经批准的程序以确保正确地降级。



注意：

如果需要将介质或计算系统降级为不那么敏感的类别，则必须使用本章“销毁敏感数据”一节中描述的适当过程对其进行净化。然而，通过购买新的介质或设备比执行净化步骤以使重新使用通常更安全和容易。许多组织采用禁止任何介质或系统降级的策略。

2. 处理敏感信息和资产

处理(handling)指的是介质在有效期内的安全传输。人员根据数据的价值和分类以不同方式处理数据：正如你所期望的，高度保密的信息需要更多保护。虽然这是常识，人们仍会犯错。很多时候，人们处理敏感信息时变得麻木，不那么热心去保护它。

例如，在 2011 年，英国国防部为响应信息自由的要求，错误地公布了关于核潜艇的保密信息以及其他敏感信息。他们利用图像编辑软件将保密数据涂黑。然而，任何试图复制数据的人都可以复制所有文本，包括被涂黑的数据。

另一种常见情况是备份磁带失控。备份磁带应该与备份数据具有相同级别的保护。换句话说，如果机密信息在备份磁带上，则备份磁带应作为机密信息受到保护。然而，很多情况下，事情并非如此。例如，TD 银行在 2012 丢失了两个备份磁带，其中包含超过 260 000 条客户数据记录。随着许多数据违规的出现，细节逐渐显露出来。TD 银行在磁带丢失后约六个月向客户报告了数据泄露。约两年后，在 2014 年 10 月，TD 银行最终同意支付 850 000 美元进行改革。

最近，对存储在 Amazon 网络服务器(AWS)简单存储服务(Simple Storage Service，简写为 S3)中的数据的不正确权限暴露了数十 TB 的数据。AWS S3 是基于云的服务，美国政府的“前哨”计划公开收集了来自社交媒体和其他互联网页面的数据。收集网络数据和监控社交媒体并不是什么新鲜事。然而，这些数据被存储在一个名为 CENTCOM 的可公开访问的存档中。存档没有被加密或受到权限保护。

我们需要制定政策和程序以确保人们了解如何处理敏感数据。这是通过确保系统和介质被适当地标记开始的。第 17 章讨论记录、监测和审计的重要性。这些控制验证敏感信息在发生显著损失前得到了适当处理。如果确实发生了损失，调查人员使用审计踪迹来帮助发现错误。任何由于人员没有适当处理数据而发生的事件都应该迅速进行调查，并采取措施防止再次发生。

3. 存储敏感数据

敏感数据应以防止它受到任何损失类型的影响的方式存储。AES 256 提供强加密。许多应用都使用 AES 256 加密数据。此外，许多操作系统包括内置功能，可在文件级别和磁盘级别对数据进行加密。

如果敏感数据存储在诸如便携式磁盘驱动器或备份磁带的物理介质上，那么人员应该遵循基本的物理安全实践来防止由于盗窃造成的损失。这包括将这些设备存储在加锁的保险箱或保险库中，或存储在包括若干附加物理安全控制的安全房间内。例如，服务器房间包括物理安全措施以防止未经授权的访问，因此将便携式介质存储在服务器房间的加锁箱内将提供强有力的保护。

此外，环境控制应该用来保护介质。这包括温度和湿度控制，如供暖、通风和空调(Heating, Ventilation and Air Conditioning, HVAC)系统。

终端用户常忘记一点：任何敏感数据的价值都远大于保存敏感数据的介质的价值。换句话说，购买高质量的介质是具有成本效益的，特别是如果数据将存储很长时间，例如存储在备份磁带上。类似地，购买内置加密的高质量 USB 闪存驱动器是值得的。一些 USB 闪存驱动器包括使用诸如指纹的生物特征身份验证机制，以提供附加保护。

**注意：**

敏感数据的加密提供额外的保护层。如果数据被加密，即使它被窃取，攻击者访问它也会变得更困难。

4. 销毁敏感数据

组织不再需要敏感数据时，应该销毁它。适当地销毁确保它不会落入坏人之手，导致未经授权的泄露。高度机密数据需要比低级别的数据使用更多步骤来销毁。组织的安全策略或数据策略应该基于数据的分类来确定可接受的销毁方法。例如，组织可能要求完全销毁保存高度机密数据的介质，但允许使用软件工具覆盖较低级别的数据文件。

NIST SP 800-88 r1 “介质净化指南”提供了不同净化方法的全面细节。处理方法(如清理、清除和销毁)确保数据不能以任何方式回收。当计算机被处理时，净化(Sanitization)包括确保所有非易失性存储器被移除或销毁；系统在任何驱动器中都没有光盘(CD)或数字多功能盘(DVD)；以及内部驱动器(硬盘驱动器和固态驱动器)被净化、去除或销毁。净化指直接销毁介质或使用可信方法从介质中清除机密数据而不销毁它。

5. 消除数据残留

数据残留(Data Remanence)是擦除后仍遗留在介质上的数据。通常将硬盘驱动器上的数据称为剩磁。使用系统工具删除数据通常会将许多数据保留在介质上，并且很多工具会很容易地取消删除操作。即使你使用复杂工具来覆盖介质，原始数据的痕迹也可能保留为不易察觉的磁场。这与ghost图像类似，如果长时间显示相同的数据，ghost图像可保留在某些电视和计算机显示屏上。法院专家和攻击者可使用工具来检索数据。

消除数据残留的一种方法是用消磁器。消磁器产生一个重磁场，它在磁性介质(如传统硬盘驱动器、磁带和软盘驱动器)中重新调整磁场。使用一定功率的消磁器可靠地重写这些磁场并去除数据剩磁。然而，它们仅在磁性介质上有效。

相反，SSD 使用集成电路代替旋转磁盘上的磁通。因此，消磁 SSD 不会删除数据。然而，即使使用其他方法从 SSD 中删除数据，数据残留也经常保留。在一篇题为“可靠擦除基于闪存的固态驱动器的数据”的论文(www.usenix.org/legacy/event/fast11/tech/full_papers/Wei.pdf)中，作者发现对个人文件进行净化的传统方法没有一个是有效的。

一些 SSD 包含内置擦除命令来净化整个磁盘，但是，这些对不同制造商的一些 SSD 无效。由于这些风险，净化 SSD 的最佳方法是销毁。美国国家安全局(NSA)要求使用已批准的粉碎机销毁 SSD。批准的粉碎机将 SSD 切碎为 2mm 或更小的尺寸。许多组织出售由国家安全局批准的多个信息销毁和净化解决方案。

保护 SSD 的另一种方法是确保存储的所有数据都被加密。如果净化方法无法去除所有数据残留物，这种方法会使剩余数据不可读。

**警告：**

执行任何类型的清理、清除或净化过程时要小心。人类操作员或活动中涉及的工具可能无法正确地从介质中完全删除数据。软件可能存在缺陷，磁体可能出错，也可能被误用。在执行任何净化处理后，总需要验证所需的结果。

下面列出与销毁数据相关的一些常见术语：

擦除(Erasing) 擦除介质只对文件执行删除操作，选择一个文件或整个介质。大多数情况下，删除或移除过程只删除数据的目录或目录链接。实际数据保留在驱动器上。当新文件写入介质时，系统最终覆盖被擦除的数据，但取决于驱动器的大小、有多少空闲空间以及若干其他因素，数据可能几个月内不会被覆盖。任何人都可使用取消删除工具检索数据。

清理(Clearing) 清理或覆盖操作，以便重新使用介质，并确保攻击者不能使用传统恢复工具来恢复已经清理的数据。当介质被清理时，介质上的所有可寻址位置上写入未分类的数据。一种方法是在整个介质上写入单个字符或指定位模式。更彻底的方法是在整个介质上写入单个字符，写入该字符的补码。写入随机位，在三个不同通道中重复这一点，如图 5.2 所示。虽然这听起来像是原始数据永远丢失了，但有时使用复杂的实验室或取证技术来检索一些原始数据是可能的。此外，某些类型的数据存储对清理技术没有很好的响应。例如，硬盘上的备用扇区，标记为“坏”的扇区和许多现代 SSD 上的区域不一定被清除，仍可能保留数据。

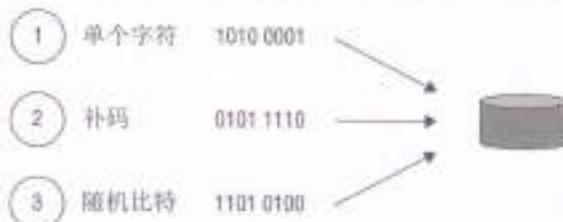


图 5.2 清理磁盘

清除(Purging) 清除是一种更强烈的清理形式，为在不太安全的环境中重用介质做准备。它提供了使用任何已知方法都无法恢复原始数据的级别。清除过程将多次重复清除，并可与另一种方法(如消磁)组合以完全去除数据。尽管清除是为了清除所有数据残留物，但它并不总是可信的。例如，美国政府不考虑清除机密数据的任何清除方法。介质标记为绝密将永远是绝密，直到它被销毁。

消磁(Degaussing) 消磁器产生一个强磁场，在消磁过程中擦除某些介质上的数据。技术人员通常使用消磁方法从磁带去除数据，目的是使磁带恢复到原来的状态。也可对硬盘进行消磁，但我们不推荐这种做法。对硬盘进行消磁通常会销毁用于访问数据的电子设备。但你无法保证磁盘上的所有数据都被销毁。其他人可在净室中打开驱动器，并在不同驱动器上安装盘片来读取数据。消磁不影响光学 CD、DVD 或 SSD。

销毁(Destruction) 销毁是介质生命周期中的一个阶段，是最安全的介质净化方法。当销毁介质时，确保介质不能被重用或修复以及不能从被销毁的介质中提取数据是很重要的。销毁方法包括焚烧、粉碎、分解和使用腐蚀性或酸性化学品溶解。一些组织在高度保密的磁盘驱动器中卸下盘片并分别销毁它们。



注意：

当组织捐赠或出售二手计算机设备时，通常卸下并销毁保存敏感数据的存储设备，而非试图清除它们，以免因为清洗过程不完整而导致保密性的丧失。

解除分类(Declassification) 指任何在不保密环境中为重复使用介质或系统而清除数据的过程。可用净化方法为解除介质分类做准备，但通常安全解除介质分类所需的努力远大于在较不

安全环境中使用新介质的成本。此外，即使清除的数据不能使用任何已知方法恢复，但可能存在未知的方法。许多组织为了不承担风险，选择不对任何介质解除分类，而是在不需要的时候销毁它。

6. 确保适当的资产保留期

保留要求适用于数据或记录、保存敏感数据的介质、处理敏感数据的系统和访问敏感数据的人员。记录保留和介质保留是资产保留最重要的因素。记录保留指需要时就保留和维护重要信息，不需要时就销毁它。组织的安全策略或数据策略通常标识保留时间帧。一些法律法规指定了组织保存数据的时间长度，如三年、七年甚至不确定期限。组织有责任认识法律法规，并应用和遵守它们。然而，即使在没有外部需求的情况下，组织仍然应该确定保留数据的时间。

例如，许多组织需要将所有审计日志保留特定的时间长度。该时间长度取决于法律、法规、其他合作组织的要求或内部管理决定。这些审计日志允许组织重构过去的安全事件细节。当组织没有保留策略时，管理员可能更早删除有价值的数据，或试图无限期地保留数据。数据被保留的时间越长，在介质、存储位置和保护人员方面的花费越多。

大多数硬件都有更换周期，每三年更换一次。硬件保留主要是在硬件被正确净化之前一直保存它。

人员保留指对人员在组织雇用时所获得的知识进行保护。在雇用新员工时，组织通常要求员工签署保密协议(NDA)，这些协议防止员工离岗，并与他人共享专有数据。



真实场景

保留策略可减少经济损失

保存数据的时间比必要的时间更长也会带来不必要的法律问题。例如，飞机制造商波音一度是集体诉讼的目标。索赔人的律师了解到波音公司有一个仓库保存着 14 000 个电子邮件备份磁带。不是所有磁带都与诉讼有关，但波音公司必须首先修复 14 000 盘磁带，并检查其内容，然后才能将其移交。波音公司最终以 9250 万美元的价格解决了诉讼，分析人士猜测，如果不存在 14 000 盘录音带，结果可能会有所不同。

波音公司的例子是一个极端例子，但不是唯一例子。这些事件促使许多公司积极实施电子邮件保留策略。电子邮件策略常要求删除超过六个月的所有电子邮件。这些策略通常使用自动工具实现，这些工具会搜索旧电子邮件并在没有任何用户或管理员干预的情况下删除它们。

在受到起诉后，公司删除潜在证据是不合法的。然而，如果保留策略规定在设定时间后删除数据，则是合法的。这种做法不仅防止了浪费资源来存储不必要的数据，而且通过查看旧的、不相关的信息，为防止浪费资源提供了额外的法律保护层。

5.1.7 数据保护方法

保护数据的保密性的主要方法之一是加密。第 6 章和第 7 章将深入讨论密码算法。然而需要指出，用于静止数据(data at rest)和传输数据(data in transit)的算法之间存在差异。在后文中，也根据上下文将“传输数据”称为“传输中的数据”“传输中数据”或“运动中的数据”。

例如，加密将明文数据转换为加密密文。当数据是明文格式时，任何人都可读取数据。然而，当使用强加密算法时，几乎不可能读取加密的密文。

1. 用对称加密保护数据

对称加密使用相同的密钥对数据进行加密和解密。换句话说，如果算法用密钥 123 加密数据，将用相同密钥 123 对其解密。对称算法对不同数据不使用相同密钥。例如，可用密钥 123 加密一组数据，用密钥 456 加密下一组数据。这里重要的一点是，使用密钥 123 加密的文件只能用相同密钥 123 解密。在实践中，密钥大小要大得多。例如，AES 使用 128 位或 192 位大小的密钥，AES 256 使用 256 位大小的密钥。

下面列出一些常用的对称加密算法。虽然这些算法中的许多用于对静态数据进行加密，但其中一些也用于下一节讨论的传输加密算法。另外，这并非加密算法的完整列表，第 6 章涵盖更多加密算法。

高级加密标准：高级加密标准(Advanced Encryption Standard, AES)是目前最流行的对称加密算法之一。NIST 在 2001 选择它作为旧数据加密标准(DES)的替换。从那时起，开发人员稳步地将 AES 应用到其他许多算法和协议中。例如，微软的 BitLocker(与可信平台模块一起使用的全磁盘加密应用)使用 AES。微软加密文件系统(EFS)使用 AES 进行文件和文件夹加密。AES 支持 128 位、192 位和 256 位的密钥大小，美国政府已批准用它来保护机密乃至绝密数据。较大的密钥长度提供了额外的安全性，使得未授权人员对数据解密变得更困难。

3DES：开发人员创建了三重 DES(或 3DES)作为 DES 的可能替代品。第一次实现使用 56 位密钥，但较新的实现使用 112 位或 168 位密钥。较大的密钥提供更高级别的安全性。三重 DES 用于万事达卡、VISA(EMV)和 Europay 标准的智能支付卡实现。这些智能卡包括一个芯片，并要求用户在购买时输入个人身份识别码(PIN)。PIN 和 3DES(或其他安全算法)的组合提供了没有 PIN 就不可用的附加身份验证层。

BlowFish：安全专家 Bruce Schneier 开发了 BlowFish 作为 DES 的一种可能替代方案。它可使用 32 位到 448 位的密钥长度，而且是强加密协议。Linux 系统使用 Bcrypt 对密码进行加密，而 Bcrypt 是基于 Blowfish 的。Bcrypt 增加了 128 位。

2. 用传输加密保护数据

传输加密方法在传输数据前对数据进行加密，保护传输中的数据。在网络上发送未加密数据的主要风险是嗅探攻击。攻击者可使用嗅探器或协议分析器捕获通过网络发送的流量。嗅探器允许攻击者读取发送的所有明文数据。然而，攻击者无法读取用强加密协议加密的数据。

举一个例子，Web 浏览器使用 HTTPS 来加密电子商务交易。这会阻止攻击者捕获数据并使用信用卡信息来收取费用。相比之下，HTTP 传输明文数据。

几乎所有 HTTPS 传输都使用传输层安全(TLS 1.1)作为底层加密协议。SSL 是 TLS 的前身。Netscape 在 1995 创建并发布了 SSL。后来，IETF 发布了 TLS 作为替代。在 2014 年，谷歌发现 SSL 对 POODLE 攻击很敏感。因此，许多组织在其应用程序中禁用了 SSL。

组织通常允许远程访问解决方案，如虚拟专用网络(VPN)。VPN 允许员工在家中或旅行时访问组织的内部网络。VPN 业务涉及公共网络，如互联网，所以加密很重要。VPN 使用加密协议，如 TLS 和 IPsec。

IPsec 常与第二层隧道协议(L2TP)结合用于 VPN。L2TP 以明文形式传输数据，但 L2TP/IPsec 对数据进行加密，并使用隧道模式通过互联网发送，以便在传输过程中保护数据。IPsec 包括 AH 和 ESP：AH 提供身份验证和完整性，ESP 提供保密性。

在内部网络传输敏感数据前加密也是合适的。IPsec 和 SSH 常用于保护内部网络中的数据。SSH 是一种强加密协议，包括其他协议，如 SCP 和 SFTP。SCP 和 SFTP 都是用于在网络上传输加密文件的安全协议。诸如 FTP 的协议以明文形式传输数据，因此不适合通过网络传输敏感数据。

许多管理员在管理远程服务器时使用 SSH。明显的优点是 SSH 加密所有事务，包括管理员的证书。历史上，许多管理员使用 telnet 管理远程服务器。然而，telnet 通过明文发送网络上的通信数据，这就是为什么管理员认为它不应该再使用的原因。有人建议在加密 VPN 隧道内使用 telnet，但事实并非如此。通信数据从客户端到 VPN 服务器是加密的，但它以明文形式从 VPN 服务器发送到 telnet 服务器。



注意：

安全壳(Secure Shell, SSH)是管理员用来连接到远程服务器的主要协议。虽然可在加密的 VPN 连接上使用 telnet，但不推荐使用。使用 SSH 更简单。

5.2 定义数据所有权

组织内的许多人管理、处理和使用数据，不同角色有不同的需求。不同文档资料对这些角色的定义稍有不同。你可能看到一些术语与 NIST 文档中使用的专业术语相匹配，而其他术语与欧盟(EU)通用数据保护条例(General Data Protection Regulation, GDPR)中使用的一些专业术语相匹配。在适当的时候，我们列出来源，以便你深入挖掘这些术语。

这里最重要的概念之一是确保员工知道谁拥有信息和资产。所有者对保护数据和资产负有主要责任。

5.2.1 数据所有者

数据所有者(Data Owner)是对数据负有最终组织责任的人。所有者通常是首席运营官(CEO)、总裁或部门主管(DH)。

数据所有者识别数据的分类，并确保正确地标记它。他们还确保根据分类和组织的安全策略要求有足够的安全控制。所有者如未能在制定和执行安全策略以保护和维持敏感资料方面付出适当努力，可能对疏忽负责。

NIST SP 800-18 概述了信息所有者的以下职责，可将其解释为与数据所有者相同的职责。

- 建立适当使用和保护主体数据/信息的规则(行为规则)。
- 向信息系统所有者提供有关信息所在系统的安全要求和安全控制的输入。
- 决定谁有权访问信息系统，以及使用何种特权或访问权限。
- 协助识别和评估信息的公共安全控制状况。

注意：

NIST SP 800-18 常使用短语“行为规则”，这实际上与可接受的使用策略(Acceptable Use Policy, AUP)相同。两者都概述了个人的责任和预期行为，并说明了不遵守规则或 AUP 的后果。此外，个人需要定期承认他们已阅读、理解并同意遵守规则或 AUP。许多组织在网站上发布这些信息，并允许用户承认他们理解并同意使用在线电子数字签名来遵守这些信息。

5.2.2 资产所有者

资产所有者(或系统所有者)是拥有处理敏感数据的资产或系统的人员。NIST SP 800-18 概述了系统所有者的以下职责：

- 与信息所有者、系统管理员和功能终端用户协作开发系统安全计划。
- 维护系统安全计划，确保系统按照约定的安全要求部署和运行。
- 确保系统用户和支持人员接受适当的安全培训，如行为规则指导(或 AUP)。
- 在发生重大更改时更新系统安全计划。
- 协助识别、执行和评估通用安全控制。

系统所有者和数据所有者通常是同一个人，但有时不是同一个人。例如不同的部门主管(DH)，有的只拥有系统，有的只拥有数据。以用于电子商务的 Web 服务器与后端数据库服务器为例：软件开发部门可执行数据库开发和数据库管理操作，IT 部门负责维护 Web 服务器。这种情况下，软件开发部门是数据库服务器的系统所有者，IT 部门是 Web 服务器的系统所有者。但是，一个人(如单个部门主管)控制两个服务器的现象更常见，而这个人将是这两个系统的系统所有者。

系统所有者要确保系统中处理的数据的安全性，这包括识别出系统处理的最高安全级别的数据。然后，系统所有者要确保系统被准确地标记，并提供相应的安全控制措施以保护数据。系统所有者与数据所有者进行交互，以确保当数据保存在系统中时、当数据在系统间传输时以及当数据被系统上的应用程序使用时是受到保护的。

5.2.3 业务/任务所有者

在不同的定义中，业务/任务所有者所扮演的角色是不同的。NIST SP 800-18 将业务/任务所有者称为项目经理或信息系统所有者。因此，业务/任务所有者的职责可与系统所有者的职责重叠，或者二者可交替使用。

业务所有者也可使用被其他实体管理的系统。例如，销售部门是业务所有者，IT 部门和软件开发部门是销售流程中使用的系统的所有者。想象一下，销售部门主要通过电子商务网站访问后端数据库服务器进行在线销售。与上例一样，IT 部门管理 Web 服务器，软件开发部门管理数据库服务器，即使销售部门不是这些系统所有者，也可使用这些系统来完成一个完整的销售流程。

在企业中，业务所有者的责任是确保各个系统能为企业提供价值，这听起来理所当然。但是，IT 部门有时不考虑其对业务或其自身的任务的影响而实施安全控制。

在许多业务中，成本和利润存在潜在冲突。IT 部门不会产生收入，相反，它是一个产生成本的成本中心。相比之下，业务部门将作为利润中心。IT 部门产生的成本会消耗业务部门产生的利润。此外，IT 部门实施的许多安全控制措施都会降低系统的可用性。如果综合考虑以上情况，你可以看到业务部门有时将 IT 部门视为一个只会花钱，只会减少利润，并使业务部门更难以产生利润的一个部门。

公司通常实施一些对 IT 部门的治理方法，例如信息和相关技术控制目标(COBIT)，来帮助企业所有者和任务所有者平衡安全控制要求与业务需求之间的关系。

5.2.4 数据使用者

通常，任何处理数据的系统都可以叫做数据使用者。GDPR 对于数据使用者有更具体的定义。GDPR 将数据使用者定义为“自然人、法人、公共权力机构、代理机构或其他机构，并且仅代表数据控制者处理个人数据。”在 GDPR 中，数据控制者是一个控制数据处理流程的人或实体。

例如，一个收集员工个人信息来制作工资单的公司是一个数据控制者。如果公司将员工信息交付给第三方公司让其完成处理工资单的任务，则第三方公司就是数据使用者。在此示例中，第三方公司(数据使用者)不得将员工工资单数据用于除原公司要求以外的任何其他用途。

GDPR 限制欧盟组织向欧盟以外的国家传输数据。欧盟组织必须遵守 GDPR 中的所有规定。违反 GDPR 隐私规定的公司会面临其全球收入的 4% 的巨额罚款。但由于 GDPR 包含太多法律规定，因此很多方面都限制了组织的发展。例如，GDPR 第 107 条包括以下声明：“禁止将个人数据转让给第三国或国际组织，除非本条例中有关转让的规定符合适当的保障措施，包括具有约束力的公司规则，以及对特定情况的免除条款”。

欧盟委员会和美国政府制定了欧盟-美国隐私盾计划以取代之前的隐私保护计划(安全港)。同样，瑞士和美国官方共同创建了瑞士-美国隐私保护框架。这两个项目均由美国商务部国际贸易管理局(ITA)管理。

组织可通过美国商务部进行自我认证，也就是说要遵守隐私保护原则。自我认证过程就是回答一个极长的问卷，并且该组织需要提供自身的详细信息，尤其是组织的隐私策略。认证时，商务部会查看组织是否承诺在其隐私策略中增加 7 项主要隐私保护原则和 16 项隐私保护补充原则。

隐私保护原则的内容非常有深度，不容易理解，特将其总结如下：

- **通知：**组织必须告知个人收集和使用信息的目的。
- **选择：**组织赋予个人选择退出的权利。
- **向前传输：**组织只能将数据传输给符合以上的“通知”和“选择”原则的组织。
- **安全：**组织必须采取合理的预防措施来保护个人数据。
- **数据完整性和仅收集与自己相关的数据：**组织仅可收集为达到“通知”原则中的目的所需的数据，而不允许收集其他数据。组织还负责采取合理措施确保个人数据准确、完整和最新。
- **可访问：**个人必须能访问组织持有的个人信息。当个人信息不准确时，个人还必须能纠正、修改或删除信息。

- 方法、强化和责任：组织必须建立一套机制以确保其所有操作都遵守隐私保护原则，并建立投诉机制以处理来自个人的投诉。

1. 假名

一个组织可实施的两个技术安全控制措施是加密和假名(pseudonymization)。如前所述，传输中的所有敏感数据和静止的敏感数据都应加密。当有效运用假名时，它就有助于达到安全控制所需的要求，否则，若我们想达到相同的安全控制要求，就必须遵守通用数据保护条例(GDPR)。

假名就是别名。例如《哈利·波特》作者 J. K. 罗琳以 Robert Galbraith 的笔名出版了一本名为 *The Cuckoo's Calling* 的书籍。如果你知道她的假名，你就会知道 Robert Galbraith 撰写的任何书都实际上是由 J. K. 罗琳撰写的。

假名是一个使用假名来表示数据的过程。这样做可防止直接通过数据识别实体，比如识别一个人。例如，医生的医疗记录中不包含患者的姓名、地址和电话号码等个人信息，而在记录中将患者称为患者 23456。但医生仍然需要这些个人信息。我们将这些个人信息保存在一个与患者假名关联的另一个数据库中，当医生需要查询患者个人信息时，可通过患者假名在另一个数据库中进行查询。

值得注意的是，在上例中，假名(患者 23456)可代表关于该人的若干信息。但假名也可用于单个信息。例如，你可用一个假名代表某人的名字，用另一个假名代表其姓氏。综上，正确使用假名的关键是要有一个资源(例如一个数据库)允许你使用假名在其中读取原始数据信息。

GDPR 将假名定义为用人为标识符替换数据，这些人为标识符就叫做假名。

2. 匿名

正如上例的医疗记录，如果你不需要个人数据，另一种方法是使用匿名化(Anonymization)。匿名化是删除所有相关数据的过程，从而达到无法识别原始主体或人的目的。如果有效地完成匿名化，匿名数据就不必再遵守 GDPR。但是，将数据真正匿名化是很困难的，即使个人相关数据被删除，也能被数据推断技术识别出来。

例如，有一个数据库，其中包括过去 75 年中在电影中担任主角或联袂担任主演的所有演员的列表，以及他们为每部电影赚取的钱。该数据库有三个表，Actor 表包括演员姓名，Movie 表包括电影名称，Payment 表包括每个演员为每部电影赚取的收益金额。这三个表是关联的，因此你可通过查询数据库得到任何演员为任何电影赚取的收入。

如果你从 Actor 表中删除了演员姓名，则此表不再包含个人数据，但这并不是真正的匿名。例如，艾伦·阿金(Alan Arkin)已经出演了 50 多部电影，而且每部电影中都没有其他主演，只有他一个主演。如果你已经识别出这 50 多部电影，你现在可查询数据库并准确了解他为每部电影赚取的收入。尽管他的名字已从数据库中删除，并且名字是数据库中唯一一个明显的个人数据，但数据推断技术仍可识别出与他对应的记录。

数据屏蔽是一种匿名化数据的有效方法。数据屏蔽是指交换单个数据列中的数据，以便每一条记录不再代表真实的数据。但是，数据仍然保持一个可用于其他目的的聚合值，比如科学目的。例如，表 5.2 显示了具有原始值的数据库中的四个记录。四个人的平均年龄就是一个聚合数据，即 29 岁。

表 5.2 在数据库中未被修改过的数据

名	姓	年龄
Joe	Smith	25
Sally	Jones	28
Bob	Johnson	37
Maria	Doe	26

表 5.3 显示了数据交换后的记录，有效地屏蔽了原始数据。请注意，交换后的数据变为一个随机的名字集，一个随机的姓氏集和一个随机的年龄集。它们看起来像真实数据，但实际上列与列之间相互没有关联。但我们仍可从表中检索出聚合数据，即平均年龄仍为 29 岁。

表 5.3 隐藏后的数据

名	姓	年龄
Sally	Doe	37
Maria	Johnson	25
Bob	Smith	28
Joe	Jones	26

如果一个表只有四行三列，那么熟悉此表的人可能还原出一些数据。而如果一个表有十几列和数千条记录，就不可能还原出数据，因此，这种情况下，数据屏蔽是一种有效的匿名数据方法。与假名化和标记化不同，屏蔽化是不可逆转的，在随机屏蔽数据后，数据是不能返回到原始状态的。

5.2.5 管理员

数据管理员负责授予人员适当的访问权限，管理员未必具有全部管理员权限和特权，但具备分配权限的能力。管理员根据“最小特权”原则和“知其所需”原则分配权限，仅授予用户工作所需的权限。

管理员通常使用基于角色的访问控制模型分配权限。换句话说，他们将用户添加到组，然后向这些组授予权限。当用户不再需要访问数据时，管理员会从该组中移除该用户。第 13 章更深入地介绍基于角色的访问控制模型。

5.2.6 托管员

数据所有者常将日常任务委托给托管员(Custodian)。托管员通过正确存储和正确保护数据来帮助保护数据的完整性和安全性。例如，托管员要确保数据备份是根据备份策略备份的；再者，如果管理员已对数据进行审核，则托管员也会将这些情况记录在日志中。

实际上，通常 IT 部门员工或系统安全管理员是托管员，他们也可能充当为数据分配权限的管理员。

5.2.7 用户

用户是通过计算系统访问数据以完成工作任务的人。用户只能访问执行工作任务所需的数据。我们还可将员工或终端用户视为用户。

5.2.8 保护隐私

组织有义务保护他们收集和维护的数据，对于 PII 和 PHI 数据尤其如此。许多法律法规要求保护隐私数据。组织有义务了解它们需要遵守哪些法律法规，此外，组织需要确保其操作符合这些法律和法规。

许多法律要求组织“公开”所收集的数据、收集的原因以及组织准备如何使用这些信息。此外，这些法律禁止组织在其打算使用数据的范围以外使用这些信息。例如，如果组织声明它正在收集电子邮件地址以与客户就购买进行通信，则组织不应将电子邮件地址出售给第三方。

对一个组织来说，在其网站上遵循在线隐私政策是很常见且必需的。一些要求严格遵守隐私法的国家或地区包括：美国(HIPAA 隐私规则、2003 年加州在线隐私保护法案)、加拿大(个人信息保护和电子文件法)和欧盟(GDPR)。

其中许多法律规定组织在其管辖范围内运作时需要符合规定。例如，加州在线隐私保护法案(CalOPPA)要求任何一个收集加州居民个人信息的商业网站或在线服务提供明确的隐私政策。实际上，这可能适用于世界上任何收集个人信息的网站，因为如果一个网站可在互联网上被访问，那么任何加州居民都可访问它。许多人认为 CalOPPA 是美国最严格的法律之一，符合加州法律要求的美国组织通常符合其他地区的要求。但是，组织仍有义务确定适用于自己的法律并遵循这些法律。

在保护隐私时，组织通常使用几种不同的安全控制。选择适当的安全控制方法是一项艰巨任务，对于新组织而言尤其如此。但使用安全基线和确定相关标准可更容易地选择出适当的安全控制方法。

许多法律文件包含收集限制原则。虽然不同法律的措辞各不相同，但核心要求是一致的，重点要求是数据收集应仅限于所需的数据。例如，如果组织需要用户的电子邮件地址来完成用户注册，则组织不应收集与此无关的数据，比如用户的出生日期或电话号码。

此外，数据应通过合法和公平的方法获得。在适当情况下，必须在个人知情和/或同意的情况下收集数据。

5.3 使用安全基线

一旦组织对其资产进行识别并分类，这就代表着组织希望保护资产，而安全基线就是用于保护资产的。安全基线提供了一个基点并确保了最低安全标准。组织经常使用的安全基线是映像。第 16 章涵盖了如何配置管理环境中的映像。这里简单介绍一下，管理员使用所需设置配置单个系统，将其捕获为映像，然后将映像部署到其他系统。这可确保所有系统都配置为相同的安全状态，有助于保护数据的隐私。

将系统部署为安全状态后，审计进程会定期检查系统以确保它们一直处于安全状态。例如，

Microsoft 组策略可定期检查系统并重新应用设置以匹配基线安全状态。

NIST SP 800-53(第五次修订版)将安全控制基线视为安全控制列表。它强调仅一组安全控制方法并不适用于所有情况，但任何组织都可先选择一组基线安全控制方法，然后按需将其制作成适合自己的安全控制方法。SP 800-53 的附录 D 包括一个完整的安全控制方法清单，并将其按优先级分为低影响、中等影响和高影响的安全控制方法。这些优先级按照系统遭到破坏、数据发生泄露对一个组织所造成的最坏影响的级别排序。

设想某个系统受到破坏，这种破坏对系统的保密性、完整性或可用性有何影响？对该系统中的数据又有何影响？

- 如果影响较小，你可将标识为低影响的安全控制方法添加到安全基线中。
- 如果影响是中等的，那么除了低影响控制安全控制方法外，你可添加中等影响的安全控制方法。
- 如果影响很大，除了低影响和中等影响的安全控制方法外，你可添加高影响的安全控制方法。

值得注意的是，标记为低影响的许多安全控制方法都是基本安全措施。例如，访问控制策略和过程(AC 系列)确保用户具有唯一标识(如用户名)，并通过安全身份验证过程证明其身份。管理员根据已证实的身份授予用户访问资源的权限(授权流程)。

同样，实施基本安全原则(如最小特权原则)对于参加 CISSP 考试的人来说并不陌生。当然，不能仅因为这些是基本措施，就认定组织会实现它们。不幸的是，许多组织未采取这些基本安全措施，也尚未意识到自己需要采取这些措施。

5.3.1 范围界定和按需定制

范围界定(Scoping)指审查基线安全控制列表，并仅选择适用于你要保护的 IT 系统的安全控制方法。例如，如果系统不允许两个人同时登录，则不需要应用并发会话控制安全方法。

按需定制(Tailoring)指修改基线内的安全控制列表，以使它们与组织要求的任务保持一致。例如，组织可能发现，一组基线安全控制措施非常适用于其主要位置的主机，但其中某些安全控制措施对于位于远程位置的主机是不适合的或不可行的。这种情况下，组织可选择补偿安全控制措施为远程位置主机按需定制一组基线安全控制措施。

5.3.2 选择标准

在基线内或其他情况下选择安全控制措施时，组织需要确保安全控制措施符合某些外部安全标准。外部要素通常为组织定义强制性要求。例如，PCI DSS 定义了企业处理信用卡时必须遵循的要求。同样，与欧盟国家之间传输数据的组织必须遵守 GDPR 的要求。

显然，并非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，不向欧盟国家/地区传输数据的组织也不需要遵守 GDPR 要求。因此，组织需要确定适用于自己的标准，并确保他们选择的安全控制措施符合此标准。

即使法律上没有要求你的组织遵循特定标准，但遵守优秀标准对你的组织是非常有帮助的。例如，美国的政府组织必须遵循 NIST SP 800 文件的许多标准。在私有企业领域，许多组织同样使用这些标准来帮助他们制定和实施安全标准。

5.4 本章小结

资产安全侧重于收集、处理信息和在信息的整个生命周期内对信息进行保护。它包括在计算系统上存储或处理的或通过网络传输的敏感信息的安全，以及在这些过程中使用的资产的安全。敏感信息就是组织需要保密的任何信息，它分为几种处于不同等级的类别。

资产安全化过程中的关键步骤是在安全策略或数据策略中定义分类标签。政府使用诸如绝密、秘密、机密和未分类等标签，非政府组织可以使用他们选择的任何标签，关键是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)提供数据的定义。

组织采取具体步骤来标记、处理、存储和销毁敏感信息和硬件资产，这些步骤有助于防止因未经授权的泄露而导致的保密性丢失。此外，组织通常会制定特定的规则保留数据以确保在需要时可使用这些数据。此外，数据保留策略还可减少因长时间保存数据而带来的开销。

加密是保护数据保密性的主要方法。对称加密协议(如 AES)可加密静态数据(存储在介质上)。传输加密协议通过在传输数据之前对其进行加密来保护传输中的数据。应用程序通过确保其正在使用的数据仅保存在临时存储缓冲区中来保证这些数据的安全性，并当应用程序不再使用这些数据时清除临时缓冲区。

处理数据时，各个部分扮演不同角色。数据所有者最终负责对数据进行分类、标记和保护。系统所有者负责管理处理数据的系统。业务/任务所有者控制数据处理流程并确保系统能为组织创造价值。数据使用者通常是为组织处理数据的第三方实体。管理员根据数据所有者提供的准则授予对数据的访问权限。托管员负责日常数据的正确存储并保护数据。用户(常称为最终用户)访问系统中的数据。

欧盟通用数据保护条例(GDPR)要求保护隐私数据并限制数据传入或传出欧盟。数据控制者可雇用“第三方”来处理数据，在这种情况下“第三方”被称为数据使用者，数据使用者有责任保护数据的隐私，不得将数据用于除数据控制者指示外的其他任何目的。GDPR 中提到的两个主要安全控制措施是加密和假名。假名指用假的名称代替原始数据的名称。

安全基线提供一组安全控制措施，组织可将其作为安全基点。一些出版物(如 NIST SP 800-53)确定了安全控制基线。但这些基线并非适用于所有组织。取而代之的是，组织使用范围界定和按需定制技术来确定其安全基线应该包含哪些安全控制措施。

5.5 考试要点

了解数据和资产分类的重要性。数据所有者负责维护数据和资产分类，并确保数据和系统被正确标记。此外，数据所有者还提出了在不同的分类信息中保护数据的新要求。比如在静止和传输中加密敏感数据。数据分类通常在安全策略或数据策略中定义。

了解 PII 和 PHI。个人身份信息(PII)是能够识别个人的任何信息。受保护的健康信息(PHI)是特定的人的任何与健康相关的信息。许多法律法规规定了 PII 和 PHI 的保护。你需要知道如何管理敏感信息。敏感信息是任何类型的机密信息，适当的管理有助于防止未经授权的泄露导致机密损失。正确的管理包括对敏感信息的标识、处理、存储和销毁。组织经常遗漏的两个方面是充分保护保存敏感信息的备份介质，并在其生命周期结束时对介质或设备进行净化。

理解记录保存。记录保留策略确保数据在需要时保持可用状态，在不再需要时销毁它。许多法律法规要求在特定时段内保存数据，但在没有正式规定的情况下，组织根据策略确定保留期。审计踪迹数据需要保持足够长的时间以重构过去的事件，但组织必须确定他们要调查多久之前的事。许多组织目前的趋势是通过实现电子邮件短保留策略来减少法律责任。

了解不同角色之间的差异。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/任务拥有者负责过程并确保系统为组织提供价值。数据使用者通常是处理数据的第三方实体。管理员根据数据所有者提供的指南授予数据的访问权限。用户在执行任务时访问数据。托管员有责任保护和存储数据。

了解GDPR安全控制。GDPR规定了隐私数据的保护方法。GDPR中提到的两个关键安全控制是加密和假名。假名是用化名替换某些数据元素的过程。这使得识别个人身份更加困难。

了解安全控制基线。安全控制基线提供了组织可作为基线应用的控件列表。并非所有基线都适用于所有组织。然而，组织可应用范围界定和按需定制技术使基线适应自己的需求。

5.6 书面实验

1. 描述 PII 和 PHI。
2. 描述净化固态硬盘的最好方法。
3. 描述假名。
4. 描述范围界定和按需定制。

5.7 复习题

1. 下列哪一项确定了信息分类过程的主要目的？
 - A. 定义保护敏感数据的需求
 - B. 定义备份数据的需求
 - C. 定义存储数据的需求
 - D. 确定传输数据的要求
2. 在确定数据的分类时，下列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. 下列哪个答案不会被列为敏感数据？
 - 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. 标记介质最重要的方面是什么?
 - A. 日期标签
 - B. 内容描述
 - C. 电子标签
 - D. 分类
5. 管理员在较不安全的环境下重用机密介质前会做什么处理?
 - A. 擦除
 - B. 清理
 - C. 清除
 - D. 覆盖
6. 下列哪一项陈述正确指出了净化方法的问题?
 - A. 无法使用方法删除数据，以确保未经授权的人员无法检索数据。
 - B. 即使是完全焚化的介质也可以提供可提取的数据。
 - C. 人员执行净化的步骤不当。
 - D. 存储的数据被物理蚀刻到介质中。
7. 以下哪一种选择是销毁固态硬盘数据最可靠的方法?
 - A. 擦除
 - B. 消磁
 - C. 删除
 - D. 清除
8. 以下哪种方法删除 DVD 上的数据最安全?
 - A. 格式化
 - B. 删除
 - C. 物理销毁
 - D. 消磁
9. 下列哪一项不会擦除数据?
 - A. 清理
 - B. 清除
 - C. 覆盖
 - D. 刷磁
10. 下面哪一个基于 Blowfish 算法，并有助于防止彩虹表攻击?
 - A. 3DES
 - B. AES
 - C. Bcrypt
 - D. SCP
11. 管理员可使用以下哪种方式安全地连接到远程服务器以进行管理?
 - A. Telnet
 - B. SFTP
 - C. SCP
 - D. Secure Shell (SSH)

12. 下列哪一项是数据托管员最可能执行的工作？
- 访问数据
 - 数据分类
 - 为数据分配权限
 - 备份数据
13. 以下哪个数据角色最可能分配权限，使用户能访问数据？
- 管理员
 - 托管员
 - 所有者
 - 用户
14. 下列哪一项是数据所有者建立“行为规则”的最好定义？
- 确保只允许用户访问他们需要的内容
 - 确定谁可以访问系统
 - 确定数据的适当使用和保护
 - 对系统应用安全控制
15. 在欧盟的 GDPR 中，数据使用者是指？
- 代表数据控制者处理个人数据的实体
 - 控制数据处理的实体
 - 处理数据的计算系统
 - 处理数据的网络
16. 你的组织有一个大的客户数据库。为遵守欧盟 GDPR，管理者计划使用假名。以下哪一项对假名化的描述最恰当？
- 用另一个标识符替换某些数据的过程
 - 删除所有个人资料的过程
 - 加密数据的过程
 - 存储数据的过程
17. 组织正在实现预先选定的安全控制基线，但发现有些控制与自己的需求无关。他们应该怎么做？
- 无论如何都要实现所有控制
 - 确定另一个基线
 - 重新创建基线
 - 根据需要调整基线

在回答问题 18~20 时参考以下场景。

一个组织有一个处理高度敏感信息的数据中心，每天 24 小时工作。数据中心包括电子邮件服务器，管理员清除超过六个月的电子邮件以遵守组织的安全策略。对数据中心的访问受到控制，所有处理敏感信息的系统都被标记。管理员通常会备份在数据中心中处理的数据。

他们在现场保留备份的副本，并将未标记的副本发送到公司的一个仓库。仓库工人按日期组织介质，他们有过去 20 年的备份。员工白天在仓库工作，晚上和周末离开时锁好仓库。最近仓库里发生一起盗窃案导致了所有现场外备份磁带的丢失。后来，他们的数据副本(包括多年

前的敏感电子邮件)开始出现在互联网上，暴露了该组织的内部敏感数据。

18. 在下列选择中，哪一项能在不牺牲安全性的情况下避免这种损失？
 - A. 标记场外保持的介质
 - B. 不要在场外存储数据
 - C. 销毁在场外存储的备份
 - D. 使用安全的异地存储设备
19. 管理员下列哪个操作可能阻止此事件？
 - A. 在把磁带送到仓库之前，把它们标上记号。
 - B. 在备份数据之前先清除磁带。
 - C. 在备份数据之前先消磁。
 - D. 将磁带添加到资产管理数据库。
20. 关于备份介质，没有遵循以下哪种策略？
 - A. 介质销毁
 - B. 记录保留
 - C. 配置管理
 - D. 版本控制

密码学和对称密钥算法

本章涵盖的 CISSP 认证考试主题包括：

- ✓ 域 2：资产安全
 - 2.5 确定数据安全控制
 - 2.5.1 了解数据状态
- ✓ 域 3：安全架构和工程
 - 3.5 评价和抑制安全架构、设计和解决方案元素的漏洞
 - 3.5.4 密码系统
 - 3.9 应用密码学
 - 3.9.1 密码生命周期(如密钥管理、算法挑选)
 - 3.9.2 加密方法(如对称、非对称、椭圆曲线)
 - 3.9.6 不可否认性
 - 3.9.7 完整性(如散列)

密码可为已存储(静止中)、通过网络传送(传输中)和存在于内存中(使用中)的敏感信息提供保密性、完整性、身份验证和不可否认性保护。密码是一项极其重要的安全技术，嵌在许多控制器里用于保护信息免遭未经授权查看和使用。

许多年来，为了提高数据保护水平，数学家和计算机科学家开发出一系列密码算法，逐级提升算法的复杂性。在密码学家耗费大量时间开发强加密算法的同时，黑客和政府同样投入大量资源来了解这些算法。这导致密码学领域形成一场“军备竞赛”，推动极其尖端的算法在当今的应用中得到不断发展。

本章将介绍密码学的历史、密码通信的基础知识以及私钥密码算法的基本原则。下一章还将继续讨论密码学，但重点介绍公钥密码系统以及攻击者用来打败密码的各种技术手段。

6.1 密码学的历史里程碑

从文明最初出现开始，人类一直在设计各种书面交流系统，其中从古人写在洞穴岩壁上的象形文字，到可容纳成套现代英语百科全书内容的闪存装置，应有尽有。一直以来，人们在交流的过程中，往往会采用秘密手段来隐藏交流的真实含义，以躲过旁人偷窥的眼睛。古代社会在战争期间会采用一种复杂的秘密符号系统来表示可以藏身的安全地点。现代文明则用各种代码和密码来便于个人和群体之间的私下交流。在接下来的小节里，你将看到现代密码学的演变过程以及历史上有名的几次秘密拦截并破译加密通信的尝试。

6.1.1 凯撒密码

古罗马时代征战欧洲的朱利叶斯·凯撒用来与身在罗马的西塞罗传递消息的密码，是最早成名的密码系统之一。凯撒对送信途中会有多少风险心知肚明——没准哪个送信人就是敌人的奸细，也没准哪个送信人会在路上遭遇敌人埋伏。出于这方面的考虑，凯撒开发了一个密码系统，被后人称作“凯撒密码”。这个系统非常简单。加密一条消息时，你只需要将字母表上的每个字母向右移三位就可以了。例如，A 变成 D，B 变成 E。如果你在这个过程中到了字母表的末尾，则你只需要返回来从头开始使用字母表便可以了，即 X 变成 A，Y 变成 B，Z 变成 C。出于这一原因，凯撒密码还被叫作 ROT3(或 Rotate 3，轮转 3)密码。凯撒密码是一种采用单字母替换法的替换密码。



注意：

尽管凯撒密码采用的是 3 字母移位，但常规移位密码可依照使用者的要求，用相同的算法移位任意数量字母。例如 ROT12 将 A 变成 M，B 变成 N，以此类推。

这里举一个凯撒密码的实际使用例子。下面第一行是原始语句，第二行则是用凯撒密码加密后看上去像句子的东西。

```
THE DIE HAS BEEN CAST.  
WKR GLH KDV EHHQ FDWW,
```

你只需要将每个字母向左移 3 位，便可解密这条消息。



警告：

凯撒密码虽然便于使用，但破解起来也轻而易举。面对一种叫作“频率分析”的攻击类型时，它会表现得非常脆弱。英语语言中使用最频繁的字母是 E、T、A、O、N、R、I、S 和 H。攻击者破解用凯撒类密码编码的英语消息时，只需要在被加密的文本中找出最常用的字母，然后尝试替换这些常用字母，便可确定文本模式。

6.1.2 美国南北战争

从凯撒时代到美国建国初期，历经许多代科学家和数学家的努力，使古文明使用的早期密码有了长足进步。到了美国南北战争期间，北方联邦和南方联盟的军队都用相对高级的密码系统在前线秘密通信，因为每一方都在对方的电报线路上搭线监听，以求窃取对方情报。这些系统采用复杂的文字替换和移位组合(详情请见 6.2.4 “密码”一节)，力争让敌方的破译陷入徒劳。南北战争期间被广泛使用的另一系统是军医 Albert J. Myer 开发的一套旗语。



注意：

本章讨论的许多内容配有图片，可访问 www.nsa.gov/about/cryptologic_heritage/museum 查看。

6.1.3 Ultra 与 Enigma

并非只有美国人投入大量资源研发代码生成机器。第二次世界大战之前，德国军工企业为政府改造了一台商用代码机，取名 Enigma。这台机器用一系列 3 到 6 位轮转执行一种极其复杂的替换密码。在当时的技术条件下，解密消息的唯一可行办法是使用一台类似的机器，配以传输设备采用的相同轮转设定(rotor setting)。德国人极其重视对这些设备的保护，设置重重防卫，使盟国几乎无法弄到一台。

为攻击 Enigma 代码，盟军军队开始了一次绝密行动，代号 Ultra。直到波兰军队成功重建一台 Enigma 样机并把他们的发现通报英美密码专家时，盟军的努力终见成效。盟军在阿兰·图灵的领导下于 1940 年成功破解 Enigma 代码，历史学家确信，这一成就对于盟军最终击败轴心国发挥了至关重要的作用。盟军破解 Enigma 的故事已被多部著名电影广泛歌颂，其中包括《猎杀 U-571》和《模仿游戏》。

日本人在二战中使用了一台类似的机器，叫作日本紫密机。美国人对这一密码系统的猛烈攻击造成日本代码在战争结束前被破解。日本的发报机采用非常正式的消息格式，使多条信息中存在大量相似文本，给密码分析带来了方便——这无疑帮助了美国人。

6.2 密码学基本知识

对任何一门学科的学习都必须从讨论构建该学科的一些基本原则入手。以下各节将通过介绍密码学的目标、概述密码技术的基本概念和讲解密码系统所用主要数学原理来打下这个基础。

6.2.1 密码学的目标

安全从业者可借助密码系统达到 4 个基本目标：保密性、完整性、身份验证和不可否认性。其中每个目标的实现都需要满足诸多设计要求，而且并非所有密码系统都是为达到所有 4 个目标而设计的。下面将详细讲解这 4 个目标并简要描述实现目标需要满足的技术条件。

1. 保密性

保密性(Confidentiality)确保数据在静止、传输和使用等三种不同状态下始终保持私密。

保密性是指为存储的信息或个人和群体之间的通信保守秘密——保密性称得上是被最广泛提及的一个密码系统目标。有两大类密码系统专用于实现保密性。

- 对称密码系统，使用一个共享秘密密钥，提供给密码系统的所有用户。
- 非对称密码系统，使用为系统每个用户单独组合的公钥和私钥。6.3 节“现代密码学”将探讨对称和非对称概念。



提示：

保护静止数据和传输中数据的概念往往是 CISSP 考试的必考内容。你应该知道，传输中的数据也叫线路上的数据，这个线路是指进行数据通信的网络电缆。

如果你开发用于提供保密性的密码系统，你必须考虑 3 种不同类型的数据。

- 静止数据，或被存储数据，是指驻留在一个永久位置上等待访问的数据。保存在硬盘、备份磁带、云存储服务、USB 装置和其他存储介质中的数据都属于静止数据。
- 运动中的数据，或线路上的数据，是指正在两个系统之间通过网络传送的数据。运动中的数据可能通过公司网络、无线网络或公共互联网传送。
- 使用中的数据，是指保存在计算机系统的活跃内存中，可供在系统上运行的流程访问的数据。

以上每种情况会带来不同类型保密性风险，但这些风险可通过密码抵御。例如，运动中的数据对于窃听十分脆弱，而静止数据则对物理设备盗窃更脆弱。如果操作系统没有适当隔离不同流程，使用中的数据有可能被未经授权流程访问。

2. 完整性

完整性(Integrity)确保数据没有被人未经授权更改。如果有完整性机制正常运行，消息的接收者可确定，他收到的消息与发出的消息相同。同样，完整性检查可确保，被存储数据自创建起到被访问时，不曾有过更改。完整性控制抵御所有形式的更改，其中包括第三方为试图插入假信息而做的有意篡改、有意删除部分数据和因传输过程的故障而发生的无意更改。

消息完整性通过使用加密的消息摘要实现：这个摘要叫“数字签名”，是在消息传输时创建的。消息接收者只需要验证消息的数字签名有效，就能确保消息在传输过程中未被改动。完整性保障由公钥和私钥密码系统提供。这一概念将在第 7 章中讨论。用密码散列函数保护文件的完整性，则将在第 21 章中讨论。

3. 身份验证

身份验证(Authentication)用于验证系统用户所声称的身份，是密码系统的一项主要功能。举例来说，假设 Bob 要与 Alice 建立一个通信会话，而他俩都是一个共享秘密通信系统的参与者。Alice 可能用一种挑战-应答身份验证技术来确保 Bob 就是他说的那个人。

图 6.1 显示这个挑战-应答协议是如何工作的。在这个例子里，Alice 和 Bob 使用的共享秘密代码相当简单——只是把一个单词的字母颠倒了而已。Bob 首先联系 Alice 并表明自己的身份。Alice 随后向 Bob 发送一条挑战消息，请 Bob 用只有 Alice 和 Bob 知道的秘密代码加密一条短消息。Bob 回复加密后的消息。Alice 验证被加密消息正确后，确信连接的另一端确实是 Bob 本人。

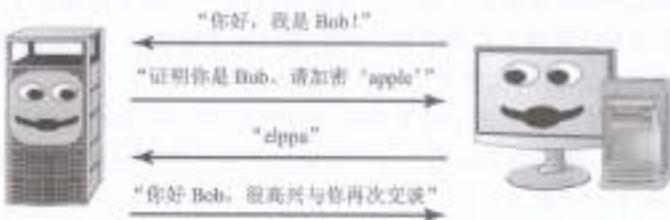


图 6.1 挑战-应答身份验证协议

4. 不可否认性

不可否认性(Nonrepudiation)向接收者保证：消息发自发送者，而且没有人冒充发送者。不

可否认性还防止发送者声称自己绝对没有发送过消息(也叫否认消息)。秘密密钥或对称密钥密码系统(例如简单的替换密码)不提供不可否认性保障。如果 Jim 和 Bob 同是一个秘密密钥通信系统的参与者, 他们都能用自己的共享秘密密钥生成相同的加密消息。不可否认性由公钥或非对称密钥密码系统提供, 这一主题将在第 7 章详细讨论。

6.2.2 密码学的概念

与任何学科一样, 在开始学习密码学之前, 你首先必须熟悉某些术语。让我们先来看几个用来描述代码和密码的关键术语。一条消息进入编码形式之前, 叫作明文消息, 描述加密功能时用字母 P 表示。一条消息的发送者用一种密码算法给明文消息加密, 生成一条密文消息, 用字母 C 表示。这条消息以某种物理或电子方式传送给接收者。接收者随后用一种预定算法来解密密文消息并恢复明文版本(有关这一流程的演示, 请见后面的图 6.3)。

所有密码算法都靠密钥维持安全。多数情况下, 密钥无非是一个数。它通常是一个极大的二进制数, 但尽管如此, 它也仅是一个数而已。每种算法都有一个特定密钥空间。密钥空间是一个特定的数值范围, 而某一特定算法的密钥在这个范围内才有效。密钥空间由位大小决定。位的大小其实也就是密钥内二进制位(0 和 1)的数量。密钥空间是从全 0 密钥到全 1 密钥的范围。换句话说, 密钥空间是从 0 到 2^n 的数范围, 其中 n 是密钥的位大小。因此, 一个 128 位密钥可以拥有一个从 0 到 2^{128} 的值——大致是 $3.40282367 \times 10^{38}$, 一个无比庞大的数! 密钥空间对于保护秘密密钥的安全至关重要。事实上, 你从密码得到的安全保护, 完全取决于你为所用密钥保守秘密的能力。

科克霍夫原则

所有密码都依赖算法。所谓算法, 其实就是一套规则, 通常是数学规则, 规定了加密和解密过程应该怎样进行。大多数密码学家都遵从科克霍夫原则; 正是这个概念使算法完全公开, 允许任何人研究和测试。具体而言, 科克霍夫原则(也叫科克霍夫假设)是说, 即便有关密码系统的一切尽人皆知, 只要密钥不被别人掌握, 密码系统也应该是安全的。一言以蔽之, 这个原则就是在讲: “随敌人去了解我们的系统。”

尽管大多数密码学家都信奉这一原则, 但也并非全都赞同科克霍夫的观点。事实上, 一些密码学家相信, 同时为算法和密钥保密, 可以保持更高的总体安全性。科克霍夫的追随者反驳说, 这种反其道而行之的方法包含了“通过隐蔽获得安全”的可疑理念。他们认为, 算法公布于众可以带来更多活力, 更容易暴露出更多弱点, 最终导致放弃不够强力的算法, 更快采用合适的算法。

你会在本章和下一章的学习过程中发现, 不同类型的算法会要求使用不同类型的密钥。在私钥(或秘密密钥)密码系统下, 所有参与者都使用一个共享密钥。在公钥密码系统中, 每个参与者都各有一个密钥对。密码密钥有时是指密码变量(cryptovariable)。

创建和执行秘密代码和密码的技艺叫密码术(也叫加密法)。而与这套实践规范并行的还有一项技艺叫密码分析, 研究的是打败代码和密码的方法。密码术和密码分析合在一起, 就是我们通常说的密码学。一种代码或密码在硬件和软件中的具体执行叫密码系统。联邦信息处理标准(FIPS)140-2“密码模块的安全要求”定义了可供联邦政府使用的密码模块的硬件和软件要求。

**提示：**

在继续本章和下一章的学习之前，首先要确保自己掌握了本节涉及的术语的含义。它们是了解后面所述密码算法的技术细节的关键。

6.2.3 密码数学

密码学与大多数计算机科学学科一样，能从数学科学中找到它的根基。要想全面了解密码学，你首先必须了解二进制数学的基本原理以及用来操控二进制值的逻辑运算。下面将简要描述你应该掌握的一些最基本概念。

1. 布尔数学

布尔数学定义了用于构成任何计算机神经系统的位和字节的规则。你可能对十进制系统再熟悉不过了。这是一个逢十进位的系统，其中的每个位上都有一个从 0 到 9 的整数，每个位值都是 10 的倍数。我们对十进制系统的依赖极可能起源于生物学方面的原因——人类用来数数的恰恰是十根手指头。

**提示：**

初学布尔数学时常常会有些迷惑，但是投入时间来了解逻辑函数的工作方式还是非常值得的。只有掌握这些概念后，才能真正搞清密码算法的内部工作原理。

同样，计算机对布尔系统的依赖起源于电学方面的原因。一个电路只会有两种可能的状态——“开”（代表有电流存在）和“关”（代表不存在电流）。电气设备的所有计算都必须用这两个词来表达，从而带来了布尔计算在现代电子学中的使用。一般来说，计算机科学家把“开”状态叫作真值，把“关”状态叫作假值。

2. 逻辑运算

密码学涉及的布尔数学利用各种逻辑函数来操控数据。下面将简单介绍其中的几种运算。

AND(与)

“AND”运算（用符号“ \wedge ”表示）检查两个值是否都真。下面的真值表显示了“AND”函数的全部 4 个可能输出。请记住，AND 函数只取两个变量作为输入。在布尔数学中，这些变量的每一个都只有两个可能的值，从而导致 AND 函数会有 4 个可能的输入。正是这种有限数量的可能性使计算机能极其容易地在硬件中执行逻辑函数。请注意下面这个真值表，其中只有一种输入组合（即两个输入全为真）产生一个输出真值：

X	Y	$X \wedge Y$
0	0	0
0	1	0
1	0	0
1	1	1

逻辑运算往往在整个布尔词而非单个值上进行。请看下面这个例子：

X:	0 1 1 0 1 1 0 0
Y:	1 0 1 0 0 1 1 1
<hr/>	
X AND Y:	0 0 1 0 0 1 0 0

请注意，AND 函数是通过比较每列中的 X 和 Y 值算出的。只有在 X 和 Y 都为真的列中，输出值为真。

OR(或)

“OR” 运算(用符号 “ \vee ” 表示)检查输入值中是否至少一个为真。下面这个真值表可以看到“OR” 函数的所有可能值。请注意，只有当两个值都为假时，OR 函数才返回一个假值：

X	Y	X \vee Y
0	0	0
0	1	1
1	0	1
1	1	1

我们还用前面小节的那个例子来显示，如果把 X 和 Y 输入 OR 函数而不是 AND 函数中，会得到什么输出：

X:	0 1 1 0 1 1 0 0
Y:	1 0 1 0 0 1 1 1
<hr/>	
X \vee Y:	1 1 1 0 1 1 1 1

NOT(非)

“NOT” 运算(用符号 “ \sim ” 或 “ $!$ ” 表示)只是颠倒一个输入变量的值。这个函数一次只在一个变量上运算。下面是 NOT 函数的真值表：

X	\sim X
0	1
1	0

在这个例子中，你可以从前面的例子中取 X 值，然后对它运行 NOT 函数：

X:	0 1 1 0 1 1 0 0
<hr/>	
\sim X:	1 0 0 1 0 0 1 1

Exclusive OR(异或)

你在本章学习的最后一个逻辑函数在密码学应用中或许是最重要和最常用的——Exclusive OR(异或)函数。数学文献把它写成 XOR 函数，通常用符号 “ \oplus ” 表示。只有当一个输入值为

真的时候，XOR 函数才返回一个真值。如果两个值都为假或两个值都为真，则 XOR 函数的输出为假。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

以下运算显示了 X 和 Y 用作 XOR 函数的输入时的情况：

$$\begin{array}{l} X: 0\ 1\ 1\ 0\ 1\ 1\ 0\ 0 \\ Y: 1\ 0\ 1\ 0\ 0\ 1\ 1\ 1 \end{array}$$

$$X \oplus Y: 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1$$

3. 模函数

模函数在密码学领域极其重要。请不妨回顾一下你小时候初学除法的情景。那时你还没学过小数，每次做除法题时都要把除不尽的余数写出来补上去。计算机其实也不懂除法，而这些余数会在计算机运算许多数学函数的过程中发挥关键作用。模函数非常简单，它是一次除法运算之后留下的余数。



提示：

模函数对于密码学的重要性不亚于逻辑运算。确保自己掌握模函数的功能，可以做一些简单的模数学运算。

模函数在等式中通常用它的缩写“mod”表示，不过有时也用运算符“%”表示。下面列举几个模函数的输入和输出：

$$\begin{array}{l} 8 \bmod 4 = 0 \\ 6 \bmod 8 = 6 \\ 10 \bmod 3 = 1 \\ 10 \bmod 2 = 0 \\ 32 \bmod 8 = 0 \end{array}$$

我们将在第 7 章探讨 RSA 公钥加密算法(以发明者 Rivest、Shamir 和 Adleman 的名字命名)时再次论及这个函数。

4. 单向函数

单向函数(One-Way Function)是便于为输入的每种可能组合生成输出值的一种数学运算，但这一运算会导致无法恢复输入值。公钥加密系统全都建立在某种单向函数的基础之上。但是实践又从来没有证明，任何具体的已知函数确实是单向的。密码学家依靠被他们确信是单向的函数，但是这些函数被未来的密码分析者破解的可能性始终存在。

下面举一个例子。假设你有一个由三个数相乘得出的函数。如果你把输入限制为个位数，

逆向还原这个函数并通过查看数字输出确定可能的输入值会显得轻而易举。例如用输入值 1、3 和 5 创建输出值 15。但是，假设你把输入限制为 5 位素数。虽然用一台计算机或性能好些的计算器依然可以相当容易地得到输出值，但是逆向还原就没有刚才那样简单了。对于输出值 10 718 488 075 259，你能算出组成它的三个素数吗？没那么容易了，对不对？原来，这个数是三个素数 17 093、22 441 和 27 943 的乘积。由于 5 位素数总共才有 8363 个，所以对这道题用一台计算机或一种蛮力算法或许就能成功破解，但是想靠心算算出来，纯粹是天方夜谭。

5. Nonce

密码常通过给加密过程添加随机性来获得强度。做到这一点的方法之一就是使用 Nonce。Nonce 是一个随机数，可在数学函数中充当占位符变量。每当函数执行时，Nonce 都会被一个在开始处理的那一刻生成的一次性随机数替换。Nonce 每次使用时都必须是一个唯一的数。比较有名的 Nonce 例子之一是初始化向量(IV)，这是一个随机位串，长度与块大小相同，针对消息执行 XOR 操作。当同一条消息每次用同一个密钥加密时，IV 用于创建唯一的密文。

6. 零知识证明

你向某个第三方证明，你确实知道一个事实，但同时不把这个事实本身披露给该第三方——这样的机制借助密码学形成，通常通过口令和其他秘密鉴别符实现。

零知识证明的经典例子涉及 Peggy 和 Victor 这两个人物。如图 6.2 所示，Peggy 知道一个环形岩洞里一道密门的口令。Victor 想从 Peggy 手中买这个口令，但是他在付钱之前要求 Peggy 证明自己确实知道这个口令。而 Peggy 不愿提前把口令告诉 Victor，担心他知道口令后赖账。零知识证明可以帮他们走出这个困境。



图 6.2 密门

Victor 站在入口处看着 Peggy 沿通道 1 出发。Peggy 到达密门后用口令打开密门，然后穿过密门沿通道 2 返回。Victor 目睹 Peggy 沿通道 1 出发又从通道 2 返回的全过程，这证明 Peggy 必定知道打开密门的正确口令。

7. 分割知识

当执行某项操作所要求的信息或权限被分散到多名用户手中时，任何一个人都不会具有足够的权限来破坏环境的安全。这种把职责分离和双人控制融于一个解决方案的做法叫“分割知识”。“密钥托管”概念是体现分割知识的最佳例子。采用密钥托管后，秘密密钥、数字签名乃至数字证书都可以保存或备份到一个叫作密钥托管数据库的专用数据库中。如果一个用户的密钥丢失或损坏了，可从备份中提取密钥。然而，如果只存在一个密钥托管恢复操办人，就会出现欺诈和滥用这一权限的机会。 N 分之 M 控制要求操办人总数(N)中至少要有 M 个操办人同时在场才能执行高安全级任务。因此，八分之三控制要求，在被指派可执行密钥托管恢复任务的 8 个操办人中，要有 3 个同时在场才能从密钥托管数据库中提取一个密钥(其中 M 永远要小于或等于 N)。

8. 代价函数

你可用代价函数或代价因子从耗费成本和/或时间的角度衡量破解一个密码系统需要付出的努力，以此来衡量密码系统的强度。对一个加密系统实施一次完整蛮力攻击所需付出的时间和精力，通常是代价函数所代表的内容。密码系统提供的安全和保护与代价函数/因子的值呈正比例关系。代价函数的大小应该与受保护资产的价值匹配。代价函数只需要略大于该资产的时间值即可。换言之，包括密码保护在内的所有安全措施都应该是有成本效益和成本效率的。为保护一个资产所付出的努力不应超出它的需要，同时又要保证所提供的保护是充分的。因此，如果信息随时间的推移而逐渐贬值，代价函数也只需要大得足以提供安全保障即可，直到数据完全丧失价值。

挑选密码系统的安全专业人员除了了解数据具有价值的时间长度外，还必须了解新涌现的技术可能对破解密码的努力产生什么影响。例如，可能会有研究者在第二年发现一种密码算法的一个缺陷，使该算法保护的信息变得不再安全。同样，基于云的平行计算和量子计算技术在经过一段时间的发展之后，可能会令蛮力攻击的可行性大增。

6.2.4 密码

密码系统已被力求保护通信保密性的个人和政府使用了很长时间。下面将介绍密码的定义，同时探索构成现代密码基础的几种常用密码类型。请务必记住，这些概念看起来属于基本概念，但是把它们组合在一起，会给密码分析者带来可怕对手，迫使他们长时间陷于挫败之中。

1. 代码与密码

人们通常交替使用“代码”和“密码”这两个词，但从技术角度看，这两个词不能混为一谈。二者在概念上有重要区别。代码是由代表单词和短语的符号构成的密码系统；代码尽管有时是保密的，但它们并不一定提供保密性保护。执法机关采用的“10 号通信系统”是代码的一个常见例子。在这套系统下，“I received your communication and understand the contents”这句话用代码短语“10-4”表示。这个代码虽然尽人皆知，但是它确实给通信带来了方便。有些代码是保密的。它们通过一个秘密代码簿传递机密信息；这个代码簿上的代码只有发送者和接收者才知道它们的含义。例如，一个间谍用“老鹰已着陆”这句话来报告敌军派来一架飞机。

另一方面，密码始终要隐藏消息的真实含义。密码通过各种技术手段更改和/或重新排列消息的字符或位，以达到实现保密性的目的。密码以位(即一个个位二进制代码)、字符(即 ASCII 消息的一个单个字符)或块(即消息的一个固定片段，通常以位数表示)为单位将消息从明文转变成密文。下面将介绍当今使用的几种常见密码。



提示：

有一个窍门可帮助你搞清代码与密码的区别：你只需要记住，代码作用于单词和短语，而密码作用于字符和位。

2. 移位密码

移位密码通过一种加密算法重新安排明文消息的字母，形成密文消息。解密算法只需要逆向执行加密转换便可恢复原始消息。

图 6.1 所示的那个挑战-应答协议例子用一个简单的移位密码颠倒了消息的字母顺序，使“apple”变成“elppa”。移位密码的实际应用比这复杂得多。例如，你可以用一个关键词进行列移位。在下面这个例子中，我们尝试用秘密密钥“attacker”给消息“The fighter will strike the enemy bases at noon”加密。我们首先提取关键词字母，然后按字母表顺序给它们标注数字。第一个出现的字母 A 接受的值为 1，字母表上第二靠前的字母赋值 2。按字母表顺序下一个出现的字母 C 标注为 3，以此类推。下面是由这个顺序得出的结果：

A	T	T	A	C	K	E	R
1	7	8	2	3	5	4	6

接下来，我们把消息的字母在关键词的字母下面按顺序逐个写出。

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	N	E	T	H	E
E	N	E	M	Y	B	A	S
E	S	A	T	N	O	O	N

最后，发送者以每列逐字母往下读的方式给消息加密；各列读出的顺序与第一步分配的数字对应，产生密文如下：

T H E E F W K M T I T E Y N H L H A O G L T B O T S E S N H R N S E S I E A

在另一端，接收者用密文和相同的密钥重建 8 列矩阵，逐行读出明文消息。

3. 替换密码

“替换密码”(substitution cipher)通过加密算法用一个不同的字符替换明文消息的每个字符或位。本章开头时讨论的凯撒密码就是替换密码的一个好例子。既然你已经掌握了一点密码数学知识，我们不妨回过头来再看看凯撒密码。你一定还记得，我们把消息中每个字母向右简单 3 位生成密文。然而，当我们来到字母表末尾时，会遇到掉出字母表的问题。我们绕回到字

母表的开头，使明文字符 Z 变成密文字符 C，解决了这个问题。

```
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
```

你可将每个字母逐个转换成它的十进制等同物(其中 A 为 0, Z 为 25)，从而以数学方式表述 ROT3 密码。这时，你可通过给每个明文字母加 3 来形成密文。你可以用“密码数学”小节讨论的模函数来说明这个环绕。凯撒密码的最终加密函数会是这个样子：

$$c = (p + 3) \bmod 26$$

与之对应的解密函数会是这样：

$$p = (c - 3) \bmod 26$$

与移位密码一样，也存在许多比本章所举例子更复杂的替换密码。多表替换密码在同一条消息中使用多个字母表，以此给破解制造障碍。多表替换密码系统的最著名例子之一是 Vigenere 密码系统。Vigenere 密码使用了一个上文所示加密/解密图。

请注意，这张图在报头下重复写出 26 个字母(共 26 遍)，每遍移动一个字母。使用这个系统需要有一个密钥。譬如，这个密钥是 secret。接下来，可执行以下加密流程：

- (1) 写出明文。
- (2) 在明文下面写出加密密钥，按需要重复这个密钥直到形成一行与明文长度相同的文本。

- (3) 把每个字母位置从明文变成密文。
- 定位以第一个明文字符开头的列(a)。
 - 定位以第一个密钥字符开头的行(s)。
 - 定位这两项的交叉处，在这里写下所出现的那个字母(s)。这就是该字母位置的密文。
- (4) 在明文中为每个字母重复步骤(1)至(3)。

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 q d s x f r a g

多表替换虽然可以抵御直接频率分析，但是遇到叫作周期分析的二阶式频率分析时就显得无能为力了——周期分析根据密钥的重复使用情况进行频率分析。

4. 单次密本

“单次密本”(one-time pad)是极其强力的一种替换密码。单次密本为明文消息中的每个字母使用一个不同的替换字母表，它们可用以下加密函数表示，其中 K 是用于将明文字母 P 加密成密文字母 C 的加密密钥：

$$C = (P + K) \bmod 26$$

单次密本通常被写成一个很长的数字系列插入函数。



注意：

单次密本也叫 Vernam 密码，以它们的发明者 AT&T 贝尔实验室的 Gilbert Sandford Vernam 命名。

单次密本的优势在于，如果使用得当，它能够不可破解。字母表替换中不存在任何重复模式，这使密码分析的努力只能归于徒劳。但必须满足有几点要求才能保证算法的完整性：

- 单次密本必须随机生成。若是使用从一本书中摘取的短语或段落，将使密码分析者有机会破解代码。
- 单次密本必须处于物理保护之下，以防泄露。敌人如果拿到密本拷贝，将能轻松解密经过加密的消息。



注意：

到了这里你可能发现，凯撒密码、Vigenere 密码和单次密本彼此很像。你想得没错！它们之间的唯一区别是密钥长度。凯撒移位密码所用密钥的长度为 1，Vigenere 密码使用的密钥要长一些(通常是一个词或一句话)，而单次密本使用的密钥与消息本身一样长。

- 每个单次密本必须只使用一次。如果密本重复使用，密码分析者将能在用同一密本加密的多条消息之间比较相同点，进而有可能确定所使用的密钥值。
- 密钥必须至少与将被加密的消息一样长。这是因为，密钥的每个字符只用于给消息中的一个字符编码。

**提示：**

单次密本的这些安全要求是任何网络安全专业人员都必须掌握的基本知识。人们往往一方面尝试着执行单次密本密码系统，另一方面又不去满足其中的一项或多项基本要求。下面这个例子值得深思，它讲述了欧洲某国的整个代码系统因为这样的疏忽而被击破的情况。

这些要求中若有任何一项未被满足，单次密本原本让人无法破解的特质会立刻失灵。事实上，正是密码分析员破解了一个依赖单次密本的欧洲某国绝密密码系统，造就了美国情报机构的一次重大成功。这个代号 VENONA 的计划发现，该国为他们的密本生成密钥值时惯用一种模式。这个模式的存在违背了单次密本密码系统的第一项要求：密钥必须随机生成，不可使用任何重复模式。整个 VENONA 计划已于最近解密，所有内容在国家安全局网站 https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/publications/coldwar/assets/files/venona_story.pdf 上对公众开放。

单次密本有着悠久的历史，被用来保护极其敏感的通信。单次密本始终未被推广使用，究其原因，主要是因为生成、分发和保护所要求的冗长密钥实在太难。由于密钥长度的关系，单次密本在现实中只能用于较短的消息。

5. 运动密钥密码

密码密钥长度有限，自然会存在许多密码漏洞。如前所述，单次密本使用的密钥至少与消息一样长，从而规避了这些漏洞。然而，单次密本执行起来却非常棘手，因为它们需要物理交换密本。

化解这个困境的一种常见方法是使用一种运动密钥密码(running key cipher)，也可将这种密码称为书密码。在这套密码中，加密密钥与消息本身一样长，而且往往选自一本普通书籍。例如，发送者和接收者提前达成一致，把《白鲸》的一章文本从第 3 段开始用作密钥。他们两人只需要按必要的数量用连续的字符来执行加密和解密操作。

举一个例子。假设你要用前面刚讲的密钥加密这样一条消息：“Richard will deliver the secret package to Matthew at the bus station tomorrow”。这条消息长 66 个字符，因此你要用运动密钥的头 66 个字符：“With much interest I sat watching him. Savage though he was, and hideously marr”。接下来，你可以用任何算法来通过这个密钥给明文消息加密。再举一个模 26 加法的例子——模 26 加法将每个字母分别转换成一个十进制对等体，把明文加到密钥上，然后进行模 26 运算，得出密文。如果你给字母 A 赋值 0，给字母 Z 赋值 25，你可对明文的头两个词进行以下加密运算：

明文:	R	I	C	#	A	R	D	W	I	L	L
密钥:	W	I	T	H	M	U	C	E	I	N	T
数值明文:	17	8	2	7	0	17	3	22	8	11	11
数字密钥:	22	8	19	7	12	20	2	7	8	13	19
数字密文:	13	16	21	14	12	11	5	3	16	24	4
密文:	N	Q	V	D	M	L	F	D	Q	Y	E

接收者收到密文后使用同样的密钥，然后从密文中减去密钥，进行模26运算，最终将得出的明文转回字母字符。

6. 块密码

块密码(block cipher)在消息“块”上运算，在同一时间对整个消息执行加密算法。移位密码(transposition cipher)是块密码的例子。挑战-应答算法使用的简单算法提取整个词，然后反向排列词的字母。比较复杂的列移位密码在整条消息(或消息的某个片段)上运算，用移位算法给消息和一个秘密密钥加密。大多数现代加密算法都执行某类块密码。

7. 流密码

流密码(stream cipher)一次在消息(或消息流)的一个字符或一个位上运行。凯撒密码是流密码的一个例子。单次密本也是一种流密码，因为算法在明文消息的每个字母上单独运行。流密码也可以发挥某种类型块密码的作用。这种运算会把实时数据填满一个缓冲区，然后把数据加密成块传送给接收者。

8. 混淆和扩散

密码算法依靠两种基本运算来隐藏明文消息——混淆(confusion)和扩散(diffusion)。明文和密钥之间有着极复杂的关系，迫使攻击者放弃只靠改动明文和分析结果密文来确定密钥——这就是混淆。明文中发生的一点变化，会导致多个变化在整个密文中传播——这就是扩散。请设想这样一个例子：一种密码算法首先进行一次复杂的替换，然后通过移位重新安排被替换密文的字符位置。在这个例子中，替换带来的就是混淆，移位带来的就是扩散。

6.3 现代密码学

现代密码系统通过计算机化复杂算法和长密码密钥来实现密码学的保密性、完整性、身份验证和不可否认性目标。下面首先讨论密码密钥在数据安全世界中扮演的角色，然后介绍当今常用的三类算法：对称加密算法、非对称加密算法和散列算法。

6.3.1 密码密钥

早期密码学有一条“通过隐蔽获得安全”的主导原则。当时的一些密码学家认为，确保一种加密算法安全的最佳方法是把算法的细节藏匿起来不让外人知道。老密码系统要求通信双方保守秘密，不让第三方知道用于加密和解密消息的算法。算法的任何泄露，都有可能导致整个系统被敌人破解。

现代密码系统不依靠算法的保密性。事实上，大多数密码系统的算法都在相关文献和互联网上广泛公开，可供公众查看。把算法面向大众开放，其实对算法不断提高自身安全性起着敦促作用。计算机安全界对算法的广泛分析，使从业者得以发现和纠正算法的潜在安全漏洞，确保他们使用的算法可以最妥善地保护通信安全。

现代密码系统不再依靠秘密算法，所依靠的是为一个或多个密码密钥保密，而这些密钥将用于为特定用户或用户群体个性化定制算法。我们回顾一下前文讨论的移位密码：这种密码用一个关键词通过列移位来引导加密和解密。用于执行列移位的算法尽人皆知——你从本书就读到了它的细节！然而，列移位还可用于保护双方之间的通信——只要选用的关键词不会被外人猜出即可。只要这个关键词是安全的，第三方知不知道算法细节将无所谓。

注意：



虽然算法的公开性不会破坏列移位的安全，但是这种方法天生存在多个弱点，使其面对密码分析时脆弱不堪。因此，这项技术并不适合现代安全通信。

你从前文有关单次密本的讨论中学过，单次密本算法之所以强度高，主要是因为它使用了一个极长的密钥。事实上，这种算法的密钥至少与消息本身一样长。大多数现代密码系统都不会使用这么长的密钥，但是对于决定密码系统的强度以及确定加密是否有可能被密码分析技术破解来说，密钥的长度依然是极其重要的因素。

计算能力的快速提高允许你在加密工作中使用越来越长的密钥。然而，试图击败你的算法的密码分析者也会掌握同样强大的计算能力。因此，你若想超越放手，就必须使用长度足以挫败当前密码分析能力的密钥。此外，若想增加机会，使自己的数据将能够抵御密码分析的纠缠，始终安全无恙直到未来的某个时候，你还一定要在数据必须保持安全的整个时期内设法使用会超过密码分析能力预期发展步伐的密钥。例如，正如本章前面讨论过的那样，量子计算的出现，可能给密码学带来翻天覆地的变化，使当前使用的密码系统变得不再安全。

几十年前，当 DES(数据加密标准)出台的时候，56 位密钥被认为足以确保任何数据的安全。然而，如今业界取得广泛共识：由于密码分析技术的进步和超级计算能力的涌现，56 位 DES 算法已不再安全。现代密码系统用至少 128 位的密钥来保护数据不被人偷窥。请记住，密钥的长度与密码系统的代价函数直接相关：密钥越长，破解密码系统越难。

6.3.2 对称密钥算法

对称密钥算法依靠一个分发给所有通信参与方的“共享秘密”加密密钥。这个密钥被所有各方用来加密解密消息，因此，发送者和接收者都拥有一个共享密钥拷贝。发送者用这个共享秘密密钥加密，接收者用它来解密。当使用的密钥极大时，对称加密会非常难于破解。这样的密钥主要用于进行海量加密，只提供保密性安全服务。对称密钥加密法也叫秘密密钥加密法和私钥加密法。图 6.3 显示了对称密钥加密和解密的过程。

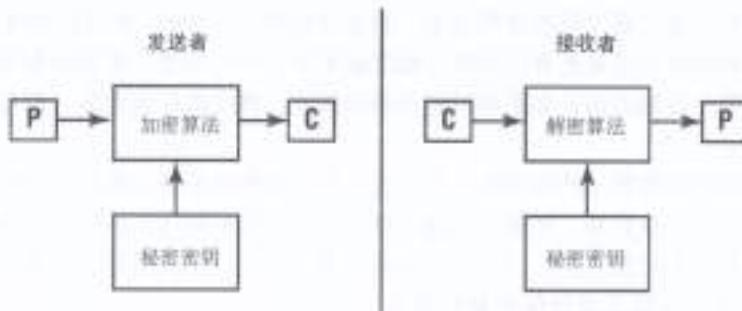


图 6.3 对称密钥加密法

**注意：**

私钥这个术语有些不太好解释，因为它是三个不同术语的成分，具两个不同的含义。私钥这个词本身永远都指公钥加密法(亦称非对称加密法)密钥对中的私钥。然而，无论是私钥加密法还是共享私钥，都属于对称加密法。“私”这个字的含义被延伸为涉及两个人，他们共享一个共同保守的秘密。而“私”这个字的真实含义其实只涉及一个人，由他来保守一个秘密。确保不要在学习中弄混了这几个词。

对称密钥加密法有几个弱点。

密钥分发是主要问题。双方在通过一个对称密钥协议建立通信之前，首先必须找到一种安全的方法来交换秘密密钥。如果这时没有现成的安全电子信道可供使用，则往往需要采用一种安全的线下密钥分发方法(即带外交换)。

对称密钥加密法不提供不可否认性。由于任何通信方都能用共享的秘密密钥加密解密消息，因此无法证明一条消息到底是从何处发出的。

算法缺乏可伸缩性。如果通信群体规模较大，将很难使用对称密钥加密法。只有在每个可能的用户组合都共享一个私钥情况下，才能在群体内的个人之间实现安全私密通信。

密钥必须经常重新生成。每当有参与者离开通信群体时，该参与者知道的所有密钥都必须弃用。

对称密钥加密法的主要优势在于它的运算速度。对称密钥加密非常快，往往比非对称算法快 1000 到 10 000 倍。从数学的属性看，对称密钥加密法本身自然更适合硬件执行，从而为更高速的运算创造了机会。

稍后的“对称密码”一节将详细讨论主要秘密密钥算法在当今的使用情况。

6.3.3 非对称密钥算法

非对称密钥算法也叫公钥算法，可提供解决方案消弭对称密钥加密的弱点。在这些系统中，每个用户都有两个密钥：一个是所有用户共享的公钥，另一个是只有用户自己知道并保守秘密的私钥。但这里也有扭曲的地方：相反和相关的两个密钥必须一先一后用于加密和解密。换言之，如果公钥加密了一条消息，则只有对应的私钥可解密这条消息，反之亦然。

图 6.4 显示了公钥密码系统中用于加密和解密消息的算法。我们举个例子。如果 Alice 想用公钥加密法给 Bob 发一条消息，她首先创建这条消息，然后用 Bob 的公钥给消息加密。解密这个密文的唯一可能手段是 Bob 的私钥，而且唯一有权访问这个密钥的只有 Bob 本人。因此，Alice 给消息加密后，连她本人也无法将其解密。如果 Bob 想回复 Alice，他只需要用 Alice 的公钥给消息加密，而 Alice 用自己的私钥解密消息后便可以浏览了。

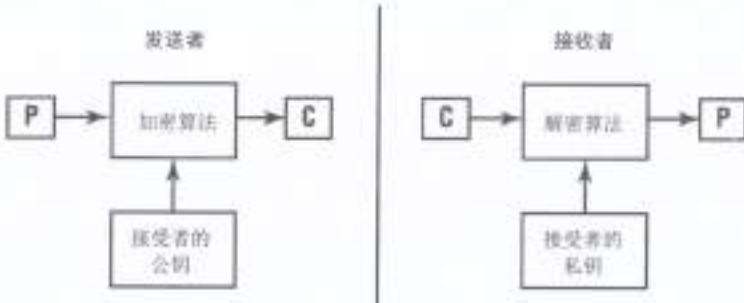


图 6.4 非对称密钥加密法



其实场景

密钥要求

本书的一位作者最近在课堂上讲到，学生一定要看清与对称加密算法相关的可伸缩问题的演示过程。对称加密系统要求每对潜在通信者都必须拥有一个共享私钥，这种情况使算法丧失可伸缩性。通过对称加密法完全连接 n 个参与方所要求的密钥总数可从下式得出：

$$\text{密钥数} = \frac{n(n-1)}{2}$$

这么来看，事情好像没那么糟(而且这不是针对小系统的)，但考虑到下面这组数字，你可能就不这么想了。显然，人数越多，对称密码系统适合满足需要的可能性越低。

参与者人数	所要求的对称密钥数	所要求的非对称密钥数
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

非对称密钥算法还支持数字签名技术。我们基本上还是用前面那个例子：如果 Bob 要向其他用户保证，有他署名的一条消息确实是 he 发送的，他首先要用一种散列算法(下一节会介绍各种散列算法)创建一个消息摘要。Bob 随后用自己的私钥给这个摘要加密。任何想验证签名的用户只需要用 Bob 的公钥解密消息摘要并验证被解密消息摘要准确就可以了。第 7 章将详细说明这个过程。

下面讲述非对称密钥加密法的主要长处：

添加新用户时只需要生成一个公钥-私钥对。这个密钥对可用来与非对称密码系统的所有用户通信。算法因此而具有极高的可扩展性。

便于从非对称系统移除用户。非对称密码系统提供一个密钥注销机制，从而使取消一个密钥，进而从系统有效移除一个用户得以实现。

只需要在用户私钥失信的情况下重新生成密钥。一个用户离开社区时，系统管理员只需要宣布该用户的密钥失效。只要其他密钥没有失信，就没必要为任何其他用户重新生成密钥。

非对称密钥加密可提供完整性、身份验证和不可否认性。一个用户只要没有把自己的私钥泄露给别人，由该用户签名的消息就可显示为准确无误、来自特定来源，而且事后不可否认。

密钥分发简便易行。用户若想加入系统，只需要把自己的公钥提供给任何通信对象即可。任何人都不可能从公钥推导出私钥。

不需要预先建立通信关联，两个人从开始通信的那一刻起始终保持通信安全。非对称加密法不要求以预先建立关系的方式来提供数据交换安全机制。

公钥加密法的主要弱点是运算速度缓慢。由于这一原因，许多需要安全传输大量数据的应用先用公钥加密法建立连接，以此交换一个对称秘密密钥，然后安排剩余的会话使用对称加密法。表 6.1 比较对称和非对称的密码系统。仔细研究这张表可发现，一个系统的一个弱点，恰恰可以被另一系统的长处弥补。

表 6.1 对称和非对称密码系统比较

对称	非对称
单个共享密钥	密钥对集
带外交换	带内交换
不可扩展	可扩展
速度快	速度慢
大批量加密	小块数据、数字签名、数字封装、数字证书
保密性	保密性、完整性、身份验证、不可否认性



注意：

第 7 章将介绍现代公钥加密算法的技术细节以及它们的一些应用。

6.3.4 散列算法

前一节的学习让你了解到，公钥密码系统与消息摘要配套使用可提供数字签名能力。消息摘要是由散列算法生成的消息内容归纳(与文件校验和没什么不同)。想从理想散列函数推导消息本身，即便不是完全不可能，也极其困难，而且两条消息产生相同的散列值也几乎是不可能的事情。一个散列函数为两种不同方法产生相同值的情况叫作冲突(碰撞)，而冲突的存在通常会导致散列算法贬值。

第 7 章将详细介绍当前的散列算法，说明可以怎样用它们来提供数字签名能力，而数字签名将有助于实现密码的完整性和不可否认性目标。

6.4 对称密码

你已学习了对称密钥加密法、非对称密钥加密法和散列函数的基本概念。下面将深入探讨几种常用对称密码系统：数据加密标准(Data Encryption Standard, DES)、三重 DES(Triple DES, 3DES)、国际数据加密算法(International Data Encryption Algorithm, IDEA)、Blowfish、Skipjack 和高级加密标准(Advanced Encryption Standard, AES)。

6.4.1 数据加密标准

美国政府于 1977 年发布数据加密标准，提议将其用作所有政府通信的标准密码系统。由于算法存在缺陷，密码学家和联邦政府现已不再认为 DES 是安全的。业界广泛认为，情报机构可以随意解密用 DES 加密的信息。DES 后于 2001 年 12 月被高级加密标准取代。但是即便如此，了解 DES 也非常 important，因为它是将在下一节讨论的一种强加密算法三重 DES(3DES)的基础构件。

DES 是一种 64 位块密码，共有 5 种运算模式：电子密码本(Electronic Code Book, ECB)模式、密码块链接(Cipher Block Chaining, CBC)模式、密码反馈(Cipher Feedback, CFB)模式、输出反馈(Output Feedback, OFB)模式和计数器(Counter, CTR)模式。下面将逐一说明这些模式。DES 的所有模式都是一次在 64 位明文上进行运算，生成 64 位密文块。DES 使用的密钥长 56 位。

DES 通过长长的一系列异或(XOR)运算生成密文。这个过程会为每个加密/解密操作重复 16 遍。每一次重复通常叫作一轮加密——这解释了 DES 需要执行 16 轮加密的说法。



注意：

如前所述，DES 用 56 位密钥推动加密和解密进程。不过，你可能从一些文献上读过，DES 使用 64 位密钥。这两种说法其实并不矛盾，完全可从逻辑上解释清楚。DES 规范要求使用 64 位密钥。但在这 64 位中，只有 56 位含密钥信息，余下的 8 位应该包含奇偶校验信息，以确保其他 56 位准确无误。但是实践中很少使用这些奇偶校验位。你只需要记住 56 位这个数字就可以了。

1. 电子密码本模式

电子密码本(ECB)模式是最容易理解的简单模式，也最不安全。算法每次处理一个 64 位块，它只用选好的秘密密钥给块加密。这意味着，算法如果多次遇到同一个块，会生成相同的加密块。如果敌人在窃听通信，他们很容易根据所有可能的加密值构建一个“密码本”。收集到足够数量的块后，便可用密码分析手段来解密其中的一些块并破解加密方案。

这一漏洞使 ECB 模式变得无法使用——只有最短的传输除外。在日常工作中，ECB 模式只用来交换少量数据，例如用于启动其他 DES 模式的密钥和参数以及数据库的计算单元。

2. 密码块链接模式

在密码块链接(CBC)模式中，每块未加密文本在通过 DES 算法加密前，先要借助前面刚生成的密文块接受异或(XOR)运算。解密流程只需要解密密文并进行反向异或运算即可。CBC 执

行一个初始化向量(IV)并用第一个消息块进行异或运算，每次运算生成一个唯一的输出。IV 必须发送给接收者，或许是将 IV 以明文形式附着在完成的密文前面，也或许是用加密消息的同一个密钥对 IV 实施 ECB 模式加密保护。使用 CBC 模式时，错误传播是需要考虑的一个重要问题——如果一个块在传输过程中损坏，这个块以及其后的块将无法解密。

3. 密码反馈模式

密码反馈(CFB)模式是 CBC 模式的流密码版。换句话说，CFB 针对实时生成的数据进行运算。但是，CFB 模式不把消息分解成块，而是使用与块大小相同的存储缓冲区。系统在缓冲区填满时给数据加密，然后把密文发送给接收者。接下来，系统等待缓冲区下次被新生成的数据填满，然后将它们加密并传输。除将使用原先就有的数据变成使用实时数据这一点外，CFB 采用的方式与 CBC 相同。它使用了一个 IV，此外使用了链接。

4. 输出反馈模式

在输出反馈(OFB)模式下，DES 以与 CFB 模式几乎完全相同的方式运行。所不同的是，DES 不是对前一个密文块的加密版进行异或运算，而用一个种子值对明文进行异或运算。对于第一个被加密的块，DES 用一个初始化向量来创建种子值。而后面的种子值则通过 DES 算法在前一个种子值上的运算得出。OFB 模式的主要优势在于，不存在链接函数，传输错误不会传播，影响后面块的解密。

5. 计数器模式

以计数器(CTR)模式运行的 DES 使用了与 CFB 和 OFB 模式类似的流密码。但是，CTR 模式不是根据以前的种子值结果为每次加密/解密运算创建种子值，而是利用一个简单的计数器为每次运算增量。与 OFB 模式一样，CTR 模式不会传播错误。



提示：

CTR 模式允许你将一次加密或解密运算分解成多个独立的步骤，这使 CTR 模式非常适合于平行计算。

6.4.2 三重 DES

如前面所述，数据加密标准(DES)的 56 位密钥不再被认为足以应对现代密码分析技术和超级计算能力。但是，改进版 DES——三重 DES(3DES)——却能通过相同的算法产生更安全的加密。

3DES 共有 4 个版本。第一个版本主要用 3 个不同的密钥(K_1 、 K_2 和 K_3)给明文加密三遍。这叫 DES-EEE3 模式(其中 E 表示有三次加密运算，而 3 表示使用了 3 个不同的密钥)，DES-EEE3 可用下面这个符号表达，其中 $E(K,P)$ 表示用密钥 K 给明文 P 加密：

$$E(K_1, E(K_2, E(K_3, P)))$$

DES-EEE3 的有效密钥长度为 168 位。

第二个变体(DES-EDE3)也使用 3 个密钥，但是用一次解密运算替换了第二次加密运算：

$E(K_1, D(K_2, E(K_1, P)))$ 3DES 的第三个版本(DES-EEE2)只使用两个密钥 K_1 和 K_2 : $E(K_1, E(K_2, E(K_1, P)))$

3DES 的第四个变体(DES-EDE2)也使用两个密钥，但中间使用了一个解密运算:

 $E(K_1, D(K_2, E(K_2, P)))$

第三和第四个变体的有效密钥长度都为 112 位。

**注意：**

从技术角度看，3DES 还有第 5 个变体：DES-EDE1。这个变体只使用一个密码密钥，却能导致出现与标准 DES 相同的算法；这种算法对于大多数应用来说显得过弱，到了无法接受的地步，因此只用于向后兼容目的。

3DES 这四个变体的开发历经数年，原因是有关密码破译家提出理论争议，指出其中的某个变体比其他变体更安全。然而当今的业界人士普遍认为，所有四个模式在安全性上水平相当。

**提示：**

你应该拿出一些时间来了解 3DES 的这些变体；应该静下心来做足功课，确保自己搞清了每个变体是怎样用两个或三个密钥实现更强加密的。

**注意：**

本节的讨论引出一个明显的问题——双重 DES(2DES)究竟发生了什么？你将在第 7 章发现，双重 DES 被拿来尝试过，但当它在攻击下被证明还不如标准 DES 更安全时，很快就被放弃了。

6.4.3 国际数据加密算法

国际数据加密算法(IDEA)块密码是在业界普遍抱怨 DES 算法缺乏充分密钥长度的情况下开发出来的。与 DES 一样，IDEA 在 64 位明文/密文块上运行。不过，IDEA 是用一个 128 位密钥开始运算的。这个密钥被分解成 52 个 16 位子密钥进行一系列运算。子密钥随后通过异或与模运算的一次结合作用到输入文本上，产生输入消息的加密/解密版。IDEA 能在 DES 使用的 5 种模式(ECB、CBC、CFB、OFB 和 CTR)下运行。

**警告：**

有关密钥长度块大小和加密轮数的材料读起来好像枯燥无比，然而这些材料却至关重要，因此准备考试时应该认真复习。

IDEA 算法由它的瑞士开发者取得专利。但专利于 2012 年到期，如今已能无限制使用。在 Phil Zimmerman 颇受欢迎的 PGP(Pretty Good Privacy，良好隐私)安全邮件软件包中，可以看到

IDEA 的一种盛行执行方案。第 7 章将详细讨论 PGP。

6.4.4 Blowfish

Bruce Schneier 的 Blowfish 块密码是 DES 和 IDEA 的另一个替代方案。Blowfish 与它的前身一样，在 64 位文本块上运行。不过，Blowfish 允许密钥长度可变，其中最短为相对不太安全的 32 位，最长为极强的 448 位，从而进一步拓展了 IDEA 的密钥强度。显而易见，密钥的加长会导致加密/解密时间相应增加。但时间试验证明，Blowfish 这种算法比 IDEA 和 DES 的速度要快得多。况且 Schneier 先生对公众开放 Blowfish，使用它不需要任何许可证。Blowfish 加密算法已被许多商用软件产品和操作系统采用。有大量 Blowfish 资料可供软件开发人员参考。

6.4.5 Skipjack

Skipjack 算法被美国政府在联邦信息处理标准(FIPS)185 EES 中批准使用。与许多块密码一样，Skipjack 在 64 位文本块上运行。它使用 80 位密钥，支持 DES 支持的 4 种运行模式。Skipjack 很快被美国政府接受，提供支持 Clipper 和 Capstone 加密芯片的密码例程。

然而，Skipjack 多了一点扭曲——这是因为它支持加密密钥托管。两家政府机构，一家是国家标准与技术研究院(NIST)，另一家是财政部，各持有重建 Skipjack 密钥所需信息的一部分。执法部门得到合法授权执法时，可与这两家机构联系以获取密钥片段，然后便能解密所涉两方之间的通信。

Skipjack 和 Clipper 芯片并不受密码界欢迎，这在很大程度上是因为美国政府的现行托管规程并不值得信任。

Rivest Cipher 5(RC5)

Rivest Cipher 5(RC5)是 Rivest-Shamir-Adleman (RSA) Data Security 公司获取专利的一种对称算法：正是这 3 人共同开发了 RSA 非对称算法。RC5 是一种块大小可变(32、64 或 128 位)的块密码，所用密钥大小在 0 到 2040 位之间。RC5 是不再被认为安全的旧算法 RC2 的改进版。RSA 还开发了一种新算法 RC6，它构建在 RC5 的基础上，但迄今还没有被广泛采用。

RC5 接受了蛮力破解试验。测试者借助大量业界计算资源开展了一次大规模行动，试图破解一条用 RC5 64 位密钥加密的消息，但这次行动花了四年多时间才把这条消息破解。

6.4.6 高级加密标准

2000 年 10 月，NIST 宣布，Rijndael(读作“rhine-doll”)块密码已被选择用来代替 DES。2001 年 11 月，NIST 发布 FIPS 197，强制规定美国政府用 AES/Rijndael 加密所有敏感但未分类的数据。

高级加密标准(AES)密码允许使用 3 种密钥强度：128 位、192 位和 256 位。AES 只允许处理 128 位块，但 Rijndael 超出了这个规定，允许密码学家使用与密钥长度相等的块大小。加密的轮数取决于所选的密钥长度：

- 128 位密钥要求 10 轮加密。
- 192 位密钥要求 12 轮加密。
- 256 位密钥要求 14 轮加密。

Twofish

Bruce Schneier(也是 Blowfish 的创造者)开发的 Twofish 算法是 AES 的另一个终极品。与 Rijndael 一样, Twofish 是一种块密码。它在 128 位数据块上运行, 能够使用最长达 256 位的密钥。

Twofish 使用的两项技术是在其他算法中找不到的:

预白化处理(prewhitening) 指第 1 轮加密前用一个单独的子密钥对明文进行异或运算;

白化后处理(postwhitening) 指第 16 轮加密后执行同样的运算。

AES 只是你需要掌握的多种对称加密算法中的一种。表 6.2 列出了几种常用和知名的对称加密算法, 同时标出了它们的块大小和密钥大小。

**提示：**

表 6.2 所含内容是 CISSP 考题的重要内容, 请务必熟记于心。

表 6.2 对称密码熟记表

名称	块大小	密钥大小
高级加密标准(AES)	128	128、192、256
Rijndael	可变	128、192、256
Blowfish(常用于 SSH)	64	32~448
数据加密标准(DES)	64	56
IDEA(用于 PGP)	64	128
Rivest Cipher 2 (RC2)	64	128
Rivest Cipher 5 (RC5)	32、64、128	0~2040
Skipjack	64	80
三重 DES(3DES)	64	112 或 168
Twofish	128	1~256

6.4.7 对称密钥管理

由于密码密钥所含信息对于密码系统的安全至关重要, 密码系统的用户和管理员采取超常措施保护密钥材料的安全义不容辞。这些安全措施统称为密钥管理实践规范, 其中包括涉及秘密密钥创建、分发、存储、销毁、恢复和托管的防护手段。

1. 创建和分发对称密钥

如前所述, 涉及对称加密算法的主要问题之一是运行算法所需秘密密钥的安全分发。用于安全交换秘密密钥的方法主要有三种: 线下分发、公钥加密和 Diffie-Hellman 密钥交换算法。

线下分发。这种在技术上最简单的方法涉及物理交换密钥材料。一方向另一方提供写了秘密密钥的一张纸或装有秘密密钥的一块存储介质。在许多硬件加密设备中, 这一密钥材料以电子设备的形式交付, 由这个电子设备将实际密钥组装在一起, 插入加密设备使用。然而, 每种

线下密钥分发方法都有自己固有的缺陷。如果密钥材料通过邮件发送，可能会被人拦截。电话可能被人窃听，写有密钥的纸张可能被人无意中扔进垃圾桶或丢失。

公钥加密。许多通信者希望享受秘密密钥加密的速度好处而免去分发密钥的麻烦。出于这一理由，许多人首先利用公钥加密建立一个初步通信连接。这个连接成功建立且各方相互验证身份后，他们便通过这个安全的公钥连接交换秘密密钥。随后，他们将通信从公钥算法转换到秘密密钥算法，享受着不断提高的处理速度。一般来说，秘密密钥加密在速度上要比公钥加密快数千倍。

Diffie-Hellman。有时，无论是公钥加密还是线下分发都不够用。双方可能需要相互直接沟通，但他们之间又没有物理手段可用来交换密钥材料，而且也没有现成的公钥基础设施便于交换秘密密钥。这种情况下，诸如 Diffie-Hellman 的密钥交换算法会被证明是最实用的机制。



提示：

安全 RPC(S-RPC)就是用 Diffie-Hellman 来进行密钥交换的。

关于 Diffie-Hellman 算法

Diffie-Hellman 算法在 1976 年发布时，代表了密码科学状态的一大进步。这种算法一直沿用至今。它的工作原理是这样的：

(1) 通信双方(假设是 Richard 和 Sue)就两个大数达成一致： p (一个素数)和 g (一个整数)，因此， $1 < g < p$ 。

(2) Richard 选择了一个随机大整数 r ，然后进行以下计算：

$$R = g^r \bmod p$$

(3) Sue 选择了一个随机大整数 s ，然后进行以下计算：

$$S = g^s \bmod p$$

(4) Richard 把 R 发送给 Sue，Sue 把 S 发送给 Richard。

(5) Richard 随后进行以下计算：

$$K = S^r \bmod p$$

(6) Sue 随后进行以下计算：

$$K = R^s \bmod p$$

这时，Richard 和 Sue 都有了一个相同的值 K ，从而可以把这个值用于双方之间的秘密密钥通信。

2. 存储和销毁对称密钥

使用对称密钥加密法的另一重大挑战是，密码系统使用的所有密钥都必须确保安全。这其中包括遵循最佳实践规范存储加密密钥：

- 绝不将加密密钥与被加密数据保存在同一个系统里。否则会让攻击者大行其便！
- 对于敏感密钥，考虑安排两个人各持一半片段。这两人以后必须同时到场才能重建整个密钥。这就是所谓分割知识原则(前文曾经讨论过)。

当一名知道秘密密钥的用户从本机构离职或不再被允许访问被该密钥保护的材料时，密钥必须更换，而且所有加密材料必须用新密钥重新加密。销毁一个密钥以将一名用户从一个对称

密码系统剔除是很难实现的事情，这也是机构转而选用非对称算法的主要原因之一——关于非对称算法，我们将在第 7 章中讨论。

3. 密钥托管和恢复

密码是一种强有力的工具。与大多数工具一样，它不仅可以用于诸多有益目的，同时也可用来达到恶意企图。面对密码工具的爆炸性增长，各国政府提出了使用密钥托管系统的主张。这些系统允许政府在有限的情况下(如按照法院的命令)从一个中央存储设施获取用于某一特定通信的密码密钥。

过去 10 年来，被提出用于密钥托管的方法主要有两种。

公平密码系统。在这种托管方法中，用于通信的秘密密钥被分解成两个或多个片段。每个片段都交付一个独立第三方保管。每个密钥片段都不能单独发挥功效，但各个片段重新组合到一起可以形成秘密密钥。政府部门得到可以访问特定密钥的合法授权后，要向每个第三方出示法庭命令的证据，然后才能重新组合秘密密钥。

受托加密标准。这种托管方法向政府提供了解密密文的技术手段。该标准是前文所述的 Skipjack 算法的基础。

政府监管部门几乎不可能越过为广泛执行密钥托管而设置的法律和隐私障碍。技术可能是现成的，但普通公众可能绝不接受由此带来潜在政府侵权。

6.5 密码生命周期

除了单次密本以外，所有密码系统的使用寿命都是有限的。摩尔定律对计算能力发展趋势的预测已被普遍接受；它指出，最先进微处理器的处理能力大约每两年会提高一倍。这意味着，处理器迟早会达到随意猜出通信所用加密密钥的强度等级。

安全专业人员在挑选加密算法时，必须重视密码生命周期问题，必须通过适当的管治控制确保，无论需要多长时间保证受保护信息不泄密，所选中的算法、协议和密钥长度都足以保持密码系统的完整性。以下是可供安全专业人员使用的算法和协议管治控制：

- 规定机构可接受的密码算法，例如 AES、3DES 和 RSA；
- 根据被传输信息的敏感性识别可与每种算法配套使用的可接受密钥长度；
- 枚举可用的安全交易协议，例如 SSL 和 TLS。

举例来说，如果你在设计一个密码系统，用以保护预计将在下周启动的业务计划的安全，你完全没有必要担心，或许会有一台处理器经过开发在 10 年后能把这些计划破解出来。另一方面，如果你要保护的是可能用来建造一颗原子弹的信息，那你几乎肯定会要求这一信息在未来 10 年里始终保密。

6.6 本章小结

密码学家与密码分析者处于一场永不休止的竞赛之中，一方要开发更安全的密码系统，另一方则要设计出更先进的密码分析技术击败这些系统。

密码学最早可以追溯到古罗马凯撒时代，几千年来，密码学始终都是一个不断发展的研究课题。在本章，你学习了密码学领域的一些基本概念，基本掌握了密码学家常用的术语，同时了解了密码学早期使用的一些历史代码和密码。

本章还阐述了对称密钥加密法(通信参与方使用同一个密钥)和非对称密钥加密法(每个通信方都拥有一对公钥和私钥)之间的异同。

接下来分析了当前可供使用的一些对称算法以及它们的长处和短处。最后讨论了密码生命周期问题以及算法/协议管治在企业安全中扮演的角色。

下一章将延伸本章的论述，涵盖当代公钥密码算法。此外，下一章还将探讨用来击败两类密码系统的一些常用密码分析技术。

6.7 考试要点

了解保密性、完整性和不可否认性在密码系统中扮演的角色。保密性是密码学追求的主要目标之一。它保护静止和传输中的数据的秘密。完整性向消息接收者保证，数据从创建之时起到访问之时止，不曾有过改动(不管是有意的还是无意的)。不可否认性则提供不可辩驳的证据证明，消息发送者确实授权了消息。这可防止发送者日后否认自己发送过原始消息。

理解密码系统实现身份验证目标的方式。身份验证可提供用户身份保障。挑战-应答协议是执行身份验证的一种方案，要求远程用户用一个只有通信参与方知道的密钥给一条消息加密。对称和非对称密码系统都能执行身份验证。

熟知密码学基本术语。一个发送者若要将一条私密消息发送给一个接收者，他首先要提取明文(未经加密的)消息，然后用一种算法和一个密钥给其加密。这将生成一条密文消息传送给接收者。接收者随后将用同一种算法和密钥解密密文，重建原始明文消息以便查看。

了解代码和密码的差异，讲出密码的基本类型。代码是作用在单词或短语上的符号密码系统，有时是保密的，但不会始终提供保密性安全服务。而密码则始终会隐藏消息的真实含义。搞清以下几类密码的工作原理：移位密码、替换密码(包括单次密本)、流密码和块密码。

了解成功使用单次密本的要求。单次密本若想成功，密钥必须随机生成且不带任何可为人知的模式。密钥必须至少与被加密消息一样长。密本必须严防物理泄露，每个密本必须使用一次后废弃。

掌握零知识证明概念。零知识证明是一个通信概念。其间交换一种特定类型信息，但是不传递真实数据，情况与数字签名和数字证书类似。

了解分割知识。分割知识指将执行某个操作所要求的信息或权限拆分给多个用户。这样做可以确保任何一个人都没有足够的权限破坏环境安全。“N分之M”控制是分割知识的一个例子。

了解代价函数(代价因子)。代价函数或代价因子从耗费成本和/或时间的角度测量解密一条消息需要付出的努力，以此来衡量密码系统的强度。针对一个加密系统完整实施一次蛮力攻击所需花费的时间和精力，通常就是代价函数评定所表达的内容。一个密码系统提供的保护与它的代价函数/因子值呈正比例关系。

了解密钥安全的重要性。密码密钥为密码系统提供必要的保密元素。现代密码系统用至少128位长的密钥提供适当的安全保护。业界一致认为，数据加密标准(DES)的56位密钥在长度

上已不足以提供安全保障。

了解对称和非对称密码系统的差异。对称密钥密码系统(或秘密密钥密码系统)依靠使用一个共享秘密密钥。对称密钥密码系统的运算速度比非对称密码系统快很多，但是它们不太支持可扩展性、密钥的简便分发和不可否认性。非对称密码系统为通信双方之间的通信使用公钥-私钥对，但运行速度比对称算法慢得多。

理解数据加密标准(DES)和三重 DES(3DES)的基本运行模式。数据加密标准有 5 种运行模式：电子密码本(ECB)模式、密码块链接(CBC)模式、密码反馈(CFB)模式、输出反馈(OFB)模式和计数器(CTR)模式。ECB 模式被认为最不安全，只用于传送简短消息。3DES 用两个或三个不同的密钥对 DES 进行三次迭代，把有效密钥强度分别提升至 112 或 168 位。

了解高级加密标准(AES)。高级加密标准(AES)使用了 Rijndael 算法，是安全交换敏感但未分类数据的美国政府标准。AES 用 128、192 和 256 位密钥长度和 128 位固定块大小来实现比旧版 DES 算法高得多的安全保护水平。

6.8 书面实验

- 阻止单次密本密码系统被广泛用来保证数据保密性的主要障碍是什么？
- 用关键词 SECURE 通过列移位加密消息 “I will pass the CISSP exam and become certified next month”。
- 用凯撒 ROT3 替换密码解密消息 “FR QJUDWXODWLRQVBRXJRWLW”。

6.9 复习题

1. 4 位密钥空间会有多少个可能的密钥？

- A. 4 个
- B. 8 个
- C. 16 个
- D. 128 个

2. John 最近收到 Bill 的一封电子邮件。需要实现哪个密码学目标才能让 John 相信 Bill 确实是发送邮件的那个人？

- A. 不可否认性
- B. 保密性
- C. 可用性
- D. 完整性

3. 数据加密标准(DES)密码系统使用的密码密钥有多长？

- A. 56 位
- B. 128 位
- C. 192 位
- D. 256 位

4. 哪种类型密码依靠改变字符在消息中的位置来实现保密性?
 - A. 流密码
 - B. 移位密码
 - C. 块密码
 - D. 替换密码
5. 以下哪一项不是高级加密标准 Rijndael 密码的可能密钥长度?
 - A. 56 位
 - B. 128 位
 - C. 192 位
 - D. 256 位
6. 以下哪一项是秘密密钥密码系统不能实现的?
 - A. 不可否认性
 - B. 保密性
 - C. 身份验证
 - D. 密钥分发
7. 只有哪种密码系统在正确执行的情况下被视为是不可破解的?
 - A. 移位密码
 - B. 替换密码
 - C. 高级加密标准
 - D. 单次密本
8. 数学函数 $16 \bmod 3$ 的输出值是什么?
 - A. 0
 - B. 1
 - C. 3
 - D. 5
9. 3DES 加密算法使用多大的块大小?
 - A. 32 位
 - B. 64 位
 - C. 128 位
 - D. 256 位
10. 以下哪类密码在大块消息而非消息的单个字符或位上运行?
 - A. 流密码
 - B. 凯撒密码
 - C. 块密码
 - D. ROT3 密码
11. 要在对称密钥加密法中确保双向通信安全，最少需要使用多少个密码密钥?
 - A. 1 个
 - B. 2 个
 - C. 3 个
 - D. 4 个

12. Dave 正在开发一个密钥托管系统，要求多人协作才能恢复一个密钥，但又不要求所有参与者全部到场。Dave 使用的是哪类技术？
- A. 分割知识
 - B. “N 分之 M” 控制
 - C. 代价函数
 - D. 零知识证明
13. 以下数据加密标准(DES)运行模式中，哪一种用于大消息时可保证加密/解密过程中早期发生的错误不会毁掉整个通信的结果？
- A. 密码块链接(CBC)
 - B. 电子密码本(ECB)
 - C. 密码反馈(CFB)
 - D. 输出反馈(OFB)
14. 许多密码算法建立在大素数乘积难以被因式分解的基础上。就这道题具体而言，它们依靠的是哪个特点？
- A. 它包含扩散
 - B. 它包含混淆
 - C. 它是一个单向函数
 - D. 它符合科克霍夫原则
15. 在有 10 人参与的情况下，若想完全执行一种对称算法，需要多少个密钥？
- A. 10 个
 - B. 20 个
 - C. 45 个
 - D. 100 个
16. 高级加密标准使用多大的块大小？
- A. 32 位
 - B. 64 位
 - C. 128 位
 - D. 可变
17. 哪种攻击导致凯撒密码最终失效？
- A. 中间人攻击
 - B. 托管攻击
 - C. 频率分析攻击
 - D. 移位攻击
18. 哪类密码系统常从名著中摘取段落充当加密密钥？
- A. Vernam 密码
 - B. 运动密钥密码
 - C. Skipjack 密码
 - D. Twofish 密码

19. AES 的哪个最终品使用了预白化和白化后处理技术？
- A. Rijndael
 - B. Twofish
 - C. Blowfish
 - D. Skipjack
20. 在有 10 人参与的情况下，若想完全执行一种非对称算法，需要多少个加密密钥？
- A. 10 个
 - B. 20 个
 - C. 45 个
 - D. 100 个

PKI 和密码应用

本章涵盖的 CISSP 认证考试主题包括：

✓ 域 3：安全架构和工程

- 3.9 应用密码学

- 3.9.1 密码生命周期(例如，密钥管理、算法挑选)
- 3.9.2 加密方法
- 3.9.3 公钥基础设施(PKI)
- 3.9.4 密钥管理实践规范
- 3.9.5 数字签名
- 3.9.6 不可否认性
- 3.9.7 完整性
- 3.9.8 了解密码分析攻击的方法
- 3.9.9 数字版权管理(DRM)

第 6 章介绍了密码学的基本概念，探讨了各种私钥密码系统。这些对称密码系统一方面可以提供快速、安全的通信，但另一方面也对以前并无关系的各方之间交换密钥提出了严峻挑战。

本章将探讨非对称(或公钥)密码世界和公钥基础设施(Public Key Infrastructure, PKI)；在后者支持下，原先并不一定相识的各方可以在世界范围内实现安全通信。非对称算法不仅提供方便的密钥交换机制，而且伸缩性良好，可容纳巨量用户，而这两点，都是对称密码系统无法做到的。

本章还将介绍非对称密码的几种实际应用：保护电子邮件、Web 通信、电子商务、数字版权管理和联网的安全。本章最后还将探讨可能会被居心不良者用来破坏弱密码系统的各种攻击手段。

7.1 非对称密码

第 6 章的“现代密码学”一节介绍了私钥(对称)和公钥(非对称)密码的基本原则。你曾学过，对称密钥密码系统要求通信双方使用同一个共享秘密密钥，从而形成安全分发密钥的问题。你还曾学过，非对称密码系统跨过了这道坎，用公钥和私钥对给安全通信带来方便，免去了复杂密钥分发系统的负担。逆向推导单向函数的难度，决定了这些系统的安全性。

下面各节将详细说明公钥密码的概念，还将介绍当今用得比较多的三种公钥密码系统：

Rivest-Shamir-Adleman (RSA)、El Gamal 和椭圆曲线密码(Elliptic Curve Cryptography, ECC)。

7.1.1 公钥和私钥

你一定还记得，前文第6章讲过，公钥密码系统依靠分配给每个密码系统用户的密钥对。每个用户都同时持有一个公钥和一个私钥。顾名思义，公钥密码系统用户可以随意把自己的公钥交给他们要与之通信的任何人。第三方只拥有公钥不会对密码系统有任何削弱。另一方面，私钥留给密钥对拥有者单独使用。私钥绝不与任何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简明直接，图7.1演示了这个过程。

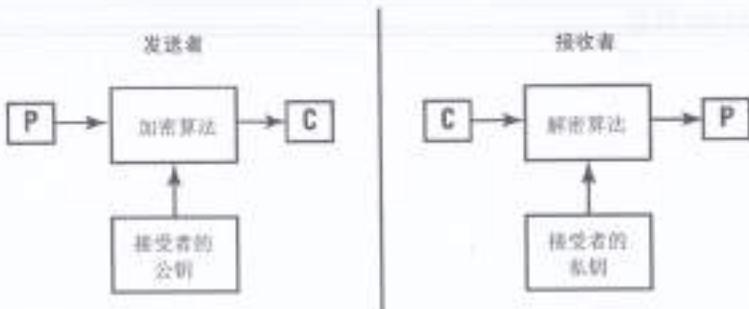


图7.1 非对称密钥加密法

请注意，这个过程不要求共享私钥。发送者用接收者的公钥加密明文消息(P)，创建密文消息(C)。接收者打开密文消息后，用自己的私钥将其解密，重建原始明文消息。

发送者用接收者的公钥给消息加密后，包括他本人在内的任何用户由于不知道接收者的私钥(用于生成消息的公钥-私钥对的第二部分)，都将不能解密这条消息。这就是公钥密码的美妙之处——公钥可以通过不受保护的通信自由共享，然后用于在以前互不相识的用户之间建立安全通信信道。

前一章还讲过，公钥密码需要提高计算复杂性。公钥系统使用的密钥必须比私钥系统所用密钥更长，才能产生同等强度的密码系统。

7.1.2 RSA

这个最著名的公钥密码系统以它的创建者命名。1977年，Ronald Rivest、Adi Shamir 和 Leonard Adleman 提出 RSA 公钥算法，直到今天，这个算法始终都是被全世界接受的一个标准。Rivest、Shamir 和 Adleman 取得算法专利权，组建了一个名为 RSA Security 的公司，为他们的安全技术开发主流执行方案。如今，RSA 算法已进入公共领域，被广泛用于安全通信。

RSA 算法所依靠的是因式分解大素数的天然计算难度。密码系统的每个用户都用以下步骤涉及的算法生成一对公钥和私钥：

- (1) 选择两个大素数(每个都约为200位)，用 p 和 q 表示。
- (2) 计算这两个数的乘积： $n = p \cdot q$ 。
- (3) 挑选一个满足以下两项要求的数 e：
 - a. e 小于 n。
 - b. e 和 $(p - 1)(q - 1)$ 是互素的——即，这两个数没有除了 1 以外的公因数。

(4) 找到一个数 d , 使 $(ed - 1) \bmod (p - 1)(q - 1) = 1$ 。

(5) 把 e 和 n 作为公钥分发给密码系统的所有用户。 d 作为私钥保密。

如果 Alice 要发送一条经过加密的消息给 Bob, 她用下式(其中 e 是 Bob 的公钥, n 是密钥生成过程中产生的 p 和 q 的乘积)从明文(P)生成密文(C):

$$C = P^e \bmod n$$

Bob 收到消息时, 将执行以下计算来检索明文消息:

$$P = C^d \bmod n$$

Merkle-Hellman 背包

Merkle-Hellman 背包算法是早期的另一种非对称算法, 于 RSA 发布的第二年被开发出来。与 RSA 一样, 这种算法也基于进行因式分解运算的艰难性, 但是它所依靠的是集合理论的一个组成部分(即超递增集)而非大素数。Merkle-Hellman 于 1984 年被破解, 被证明无效。

密钥长度的重要性

密码密钥的长度或许称得上是可由安全管理员自主设定的最重要的一个安全参数。你必须搞清你的加密算法的能力, 必须选择一个可以提供适当保护水平的密钥长度。作出这种判断的依据来自根据数据的重要性对击败某一特定密钥长度的难度的计量(即测量击败密码系统所需花费的处理时间量)。

一般来说, 你的数据越关键, 用来保护它的密钥应该越强。数据的时效性也是需要考虑的一个重要因素。你还必须考虑计算能力快速提高的问题——摩尔定律指出, 计算能力大约会每两年翻一番。如果说当前的计算机需要用一年的处理时间来破解你的密码, 那么到了四年后, 用那时的技术再来做这件事, 大概只需 3 个月就够了。如果你预计你的数据到了四年后还属敏感范畴, 那你就应该选择一个很长的密码密钥, 使它即便在将来也始终能保持安全。

此外, 由于攻击者如今已经能够利用云计算资源, 他们能以更高效率攻击被加密数据自然不在话下。云允许攻击者租用可扩展计算能力, 其中包括按小时租用强大的图形处理单元(GPU)和在非高峰时间使用过剩能力时享受大幅打折优惠。这使强大计算能力到了许多攻击者的经济承受范围之内。

各种密钥的强度还会因为你使用的密码系统而表现出巨大差异。下表所示 3 个非对称密码系统的密钥长度都将提供同等级别的保护:

密码系统	密钥长度
RSA	1 024 位
DSA	1 024 位
椭圆曲线	160 位

7.1.3 El Gamal

你在第6章学过，Diffie-Hellman 算法借助大整数和模运算，给经由不安全通信信道安全交换秘密密钥带来了方便。1985年，T. El Gamal 博士发表一篇论文，说明 Diffie-Hellman 密钥交換算法所基于的数学原则经过扩展，可支持用来加密解密消息的整个公钥密码系统。

论文面世时，El Gamal 优于 RSA 算法的主要优势之一，就在于他的论文是在公共领域公开发布的。El Gamal 博士没有为他扩展 Diffie-Hellman 算法的研究成果申请专利权，可免费供人使用，这与当时已取得专利的 RSA 技术不同，RSA 到 2000 年才把算法在公共领域公开。

不过，El Gamal 也有劣势——把由它加密的任何消息都加长了一倍。这在加密长消息或将通过窄带宽通信线路传输的数据时，会造成很大的困难。

7.1.4 椭圆曲线

同在 1985 年，另外两位数学家，华盛顿大学的 Neal Koblitz 和 IBM 的 Victor Miller 独立提出将椭圆曲线密码学(ECC)理论用于开发安全密码系统。

注意：

椭圆曲线所基于的数学概念相当复杂，大大超出了本书的论述范围。不过你在准备 CISSP 考试的时候，还是应该大致了解椭圆曲线算法和它的潜在应用。如果你有兴趣深入学习椭圆曲线密码系统的数学原理，从下面这个网址可以找到很好的辅导材料：<https://www.certicom.com/content/certicom/en/ecc-tutorial.html>。

任何椭圆曲线都可由下式定义：

$$y^2 = x^3 + ax + b$$

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相应的椭圆曲线群，由椭圆曲线上的点和位于无限远的点 O 组成。同一个椭圆曲线群内的两个点(P 和 Q)可以用一种椭圆曲线加法算法相加。这个运算表达起来非常简单：

$$P + Q$$

如果设 Q 是 P 的倍数，则这道题可以扩展，引入乘法，如下式：

$$Q = xP$$

计算机科学家和数学家相信，即使 P 和 Q 是已知的，也极难算出 x。正是这道难题——叫作椭圆曲线离散对数题——构成了椭圆曲线密码的基础。业界广泛认为，与 RSA 密码算法所基于的素数因式分解题，以及 Diffie-Hellman 和 El Gamal 使用的标准离散对数题相比，解这道题更难。前文图文框“密钥长度的重要性”中表格所示数据就说明了这一点：在这个表中，1024 位 RSA 密钥在密码强度上等同于 160 位椭圆曲线密码系统密钥。

7.2 散列函数

接下来，你将在本章学习密码系统如何通过执行数字签名来证明一条消息源发自密码系统的某一特定用户，同时确保消息在双方之间传递的过程中未曾改动过。在你能完全掌握这个概念之前，我们将先讲解一下散列函数的概念。我们将探讨散列函数的基本原理，介绍几个经常用在现代数字签名算法中的散列函数。

散列函数的目的非常简单——提取一条可能会比较长的长消息，然后从消息内容中衍生出一个唯一输出值，这个值就是我们常说的消息摘要。消息摘要可由消息的发送者生成，出于两个原因与整条消息一起发送给接收者。

第一个原因，接收者可用同一个散列函数根据整条消息重算消息摘要。接收者随后可将算出的消息摘要与传来的消息摘要进行比较，确保原发者发送的消息与接收者收到的消息相同。如果两个消息摘要不匹配，意味着消息在传输过程中有某种程度改动。值得注意的是，消息必须摘要完全相同才可能匹配。即便消息只在空格、标点符号或内容上有微小差异，消息摘要值也会完全不同。仅靠比较摘要并不能区分两条消息的差异有多大。但即便是微小差异也会产生完全不同的摘要值。

第二个原因，消息摘要可用来执行数字签名算法。这个概念将在本章“数字签名”一节讨论。



注意：

消息摘要被人们用各种说法交替表示，其中包括散列、散列值、散列总和、CRC、指纹、校验和和数字 ID。

多数情况下，消息摘要 128 位或更长。然而，一个个位值便可用来执行奇偶校验功能，一个低级或个位校验和值可用来提供一个检验单点。多数时候，消息摘要越长，它的完整性检验越可靠。

RSA Security 公司指出，密码散列函数有 5 个基本要求：

- 输入可以是任何长度。
- 输出有一个固定长度。
- 为任何输入计算散列函数都相对容易。
- 散列函数是单向的(意味着很难根据输出确定输入)。第 6 章描述过单向函数及其在密码学中的用途。
- 散列函数无冲突(意味着几乎不可能找到可以产生相同散列值的两条消息)。

下面将介绍 4 种常用散列算法：安全散列算法(SHA)、消息摘要 2(MD2)、消息摘要 4(MD4)和消息摘要 5(MD5)，稍后将讨论散列消息鉴别码(HMAC)。



提示：

有许多散列算法并不在 CISSP 考试的涵盖范围之内。但是除了 SHA、MD2、MD4、MD5 和 HMAC 以外，你还应该知道 HAVAL。可变长度散列(HAVAL)是 MD5 的修订版。HAVAL 使用 1024 位块，产生 128、160、192、224 和 256 位散列值。

7.2.1 SHA

安全散列算法(Secure Hash Algorithm, SHA)及其后继者 SHA-1、SHA-2 和 SHA-3 是美国国家标准与技术研究院(NIST)力推的政府标准散列函数，已被一份正式政府出版物作出规定——联邦信息处理标准(FIPS)180 “安全散列标准”(SHS)。

SHA-1 实际上可以提取任何长度的输入(该算法的实际上限约为 2 097 152 太字节)，由此生成一个 160 位消息摘要。SHA-1 算法可处理 512 位块中的消息。因此，如果消息长度不是 512 的倍数，SHA 算法将用附加数据来填充消息，直到它的长度达到 512 的下一个最高倍数。

密码分析攻击揭示了 SHA-1 算法存在的弱点，这导致 SHA-2 面世；SHA-2 有 4 个变体：

- SHA-256，用 512 位块大小生成 256 位消息摘要。
- SHA-224，借用了 SHA-256 散列的缩减版，用 512 位块大小生成 224 位消息摘要。
- SHA-512，用 1024 位块大小生成 512 位消息摘要。
- SHA-384，借用了 SHA-512 散列的缩减版，用 1024 位块大小生成 384 位消息摘要。



提示：

这里讲述的内容看起来并不起眼，但你还是应该拿出时间把本章描述的每种散列算法生成的消息摘要的大小牢记于心。

密码学界普遍认为，SHA-2 算法是安全的，然而从理论上说，它们存在着与 SHA-1 算法相同的弱点。2015 年，联邦政府宣布将 Keccak 算法定为 SHA-3 标准。SHA-3 系列的开发是为了插进来取代 SHA-2 散列函数，通过一种更安全的算法提供与 SHA-2 相同的变体和散列长度。

7.2.2 MD2

消息摘要 2(MD2)被 Ronald Rivest(就是大名鼎鼎的 Rivest、Shamir 和 Adleman 中的那个 Rivest)于 1989 年开发出来，可为 8 位处理器提供安全散列函数。MD2 填充消息，使其长度达到 16 字节的倍数。MD2 随后算出一个 16 字节校验和，把它附在消息末尾。然后，根据整条原始消息外加所附校验和，生成一个 128 位消息摘要。

针对 MD2 算法的密码分析攻击始终存在。具体来说，Nathalie Rogier 和 Pascal Chauvaud 发现，如果在计算摘要之前没有把校验和附在消息末尾，很容易发生冲突。Frederic Mueller 后来证明，MD2 并不是单向函数。因此，它应该不再使用。

7.2.3 MD4

1990 年，Rivest 强化了他的消息摘要算法，以支持 32 位处理器并提高安全性。这一经过强化的算法就是 MD4。它首先填充消息，确保消息的长度比 512 位的倍数小 64 位。例如，一个 16 位消息要填充 432 位数据，使其达到 448 位，而这比 512 位消息小 64 位。

MD4 算法随后通过 3 轮计算处理 512 位消息块。最终的输出是 128 位消息摘要。



提示：

MD2、MD4 和 MD5 算法不再被业界认为是合适的散列算法。尽管如此，直到今天也还有人在使用它们，因此，这些算法的细节可能出现在 CISSP 考题中。

多名数学家发表论文指出完整版 MD4 存在的缺陷以及未被适当执行的 MD4 版本。尤其是 Hans Dobbertin 于 1996 年发表一篇论文，描述如何用一台现代个人计算机在不到一分钟的时间里找到 MD4 消息摘要中的冲突。正是因为这篇论文，MD4 不再是安全的散列算法，只要可能，就应该避免使用。

7.2.4 MD5

1991 年，Rivest 发表他的下一版消息摘要算法，他称之为 MD5。MD5 还是处理 512 位消息块，但它通过 4 轮不同的计算生成一个长度与 MD2 和 MD4 算法相同的摘要(128 位)。MD5 的填充要求与 MD4 相同——消息长度必须比 512 位的倍数小 64 位。

MD5 执行新增的安全性能，大幅降低了消息摘要的生成速度。然而不幸的是，最近的密码分析攻击显示，MD5 协议也非常容易出现冲突，阻碍它成为保证消息完整性的手段。尤其是 Arjen Lenstra 等人于 2005 年证明，根据拥有相同 MD5 散列的不同公钥，完全可以创建两个数字证书。

表 7.1 列出了著名散列算法以及执行算法得出的以位为单位的散列值长度。请在这一页做上标记，牢牢记住其中的内容。

表 7.1 散列算法记忆表

名称	散列值长度
可变长度散列(HAVAL)——MD5 的一个变体	128、160、192、224 和 256 位
散列消息鉴别码(HMAC)	可变
消息摘要 2(MD2)	128
消息摘要 4(MD4)	128
消息摘要 5(MD5)	128
安全散列算法(SHA-1)	160
SHA2-224/SHA3-224	224
SHA2-256/SHA3-256	256
SHA2-384/SHA3-384	384
SHA2-512/SHA3-512	512

7.3 数字签名

你选好密码学意义上合适的散列算法后，便可用它来执行数字签名系统了。数字签名基础设施旨在达到两个不同目的：

- 有数字签名的消息可以向接收者保证，消息确实来自声称的发送者。这样的消息还可提供不可否认性保障(即，它们可使发送者日后不能声称消息是伪造的)。
- 有数字签名的消息可以向接收者保证，消息在发送者与接收者之间的传送过程中不曾有过改动。这样可以抵御恶意篡改(第三方篡改消息的含义)和无意改动(由于通信过程中发生的故障，例如电子干扰等)。

数字签名算法依靠本章前文讨论过的两大概念发挥组合作用——公钥加密法和散列函数。

如果 Alice 要给发送给 Bob 的一条消息加上数字签名，她会执行以下步骤：

(1) Alice 用密码学意义上合适的一种散列算法(例如 SHA3-512)为原始明文消息生成一个消息摘要。

(2) Alice 随后用自己的私钥只给消息摘要加密。这个被加密的消息摘要就是数字签名。

(3) Alice 把签名的消息摘要附在明文消息末尾。

(4) Alice 把有附件的消息发送给 Bob。

Bob 收到有数字签名的消息后，逆向执行如下操作。

(1) Bob 用 Alice 的公钥解密数字签名。

(2) Bob 用同一个散列函数为收到的整条明文消息创建一个消息摘要。

(3) Bob 随后将收到并解密了的消息摘要与自己算出的消息摘要进行比较。如果两个摘要匹配，他可以确定，自己收到的消息发自 Alice。如果二者不匹配，则要么消息不是 Alice 发送的，要么消息在传送过程中曾被改动。

注意：



数字签名不仅用于消息。软件厂家常用数字签名技术来鉴别从互联网下载的代码，例如 applet 和软件补丁。

请注意，数字签名流程并不对自己所含内容以及签名本身提供任何隐私保护。它只确保实现密码的完整性、鉴别和不可否认性目标。不过，如果 Alice 想确保自己发送给 Bob 的消息所含隐私不外泄，她应该给消息创建流程加一个步骤。在将经过签名的消息摘要附在明文消息末尾之后，Alice 可以用 Bob 的公钥给整条消息加密。Bob 收到消息时，可在执行前文所述步骤之前，先用自己的私钥给消息解密。

7.3.1 HMAC

经过散列处理的消息鉴别码(Hashed Message Authentication Code, HMAC)算法执行部分数字签名——可保证消息在传输过程中的完整性，但不提供不可否认性服务。

我该用哪个密钥？

如果你是初学公钥加密法的新手，在为各种应用挑选正确密钥时可能会感到困惑。加密、解密、消息签名和签名验证全都使用同一种算法，只是密钥输入不同。这里介绍几条简单规则，帮助你在准备 CISSP 考试时记住这些概念：

- 如果你要加密消息，使用接收者的公钥。
- 如果你要解密发送给你的消息，使用自己的私钥。
- 如果你要给将发送给别人的消息加上数字签名，使用自己的私钥。
- 如果你要验证别人发来的消息上的签名，使用发送者的公钥。

这四条规则是公钥加密法和数字签名的核心原则。如果你掌握了每条规则，你无疑有了一个良好开端！

HMAC 可通过一个共享秘密密钥与任何标准消息摘要生成算法(例如 SHA-3)配套使用。因此, 只有知道密钥的通信参与方可以生成或验证数字签名。如果接收者解密了消息摘要后却不能使其与根据明文消息生成的消息摘要成功匹配, 这说明消息在传送过程中发生了变动。

由于 HMAC 依靠一个共享秘密密钥, 它不提供任何不可否认性功能(如前文所述)。然而, 它的运行方式比下一节将要描述的数字签名标准更有效, 并且可能适用于使用对称密钥加密法的应用程序。简而言之, HMAC 是介于不经加密使用一种消息摘要算法, 与基于公钥加密法、计算成本昂贵的数字签名算法之间的一个中点。

7.3.2 数字签名标准

NIST 在 FIPS 186-4 DSS 中为联邦政府的使用规定了可接受数字签名算法。这份文件规定, 联邦批准的所有数字签名算法都必须使用 SHA-3 散列函数。

DSS 还规定了可用来支持数字签名基础设施的加密算法。当前得到批准的标准加密算法有三种:

- FIPS 186-4 规定的数字签名算法(DSA);
- ANSI X9.31 规定的 Rivest-Shamir-Adleman(RSA)算法;
- ANSI X9.62 规定的椭圆曲线 DSA(ECDSA)。



提示:

另外还有两种数字签名算法。你至少应该知道它们的名称: Schnorr 签名算法和 Nyberg-Rueppel 签名算法。

7.4 公钥基础设施

公钥加密的主要优势在于它能为以前不相识的双方之间的通信提供方便。这是通过公钥基础设施(PKI)信任关系层级体系实现的。这些信任关系使我们得以把非对称加密法与对称加密法, 再加上散列函数和数字证书结合到一起使用, 从而形成混合加密法。

在以下几个小节中, 你将学习公钥基础设施的基本成分以及使全球安全通信得以实现的密码学概念。你还将学习数字证书的构成、发证机构扮演的角色以及生成和销毁证书的流程。

7.4.1 证书

数字证书向通信双方保证, 与他们通信的确实是他们声称的人。数字证书其实就是一个公钥的签注副本。当用户验证一份证书由一个可信发证机构(CA)签署时, 他们知道, 公钥是合法的。

数字证书内含具体识别信息, 它们的构成受国际标准 X.509 约制。符合 X.509 的证书包含以下数据:

- 证书遵守的 X.509 版本:

- 序号(证书创建者编制);
- 签名算法标识符(规定了发证机构给证书内容数字签名时采用的技术);
- 发证者名称(标识签发证书的发证机构);
- 有效期(规定了证书保持有效的日期和时间——起始日期和时间以及终止日期和时间);
- 主体名称(含拥有证书所含公钥的实体的可识别名, DN);
- 主体的公钥(证书的主要内容——证书拥有者用来建立安全通信的实际公钥)。

X.509 的当前版本(第3版)支持证书扩展——自定义变量, 内含由发证机构插入证书的数据, 用于支持对证书或各种应用程序的跟踪。



注意:

无论你有兴趣自己构建 X.509 证书, 还是仅仅想研究公钥基础设施的内部工作原理, 你都可以从国际电信联盟(ITU)购买完整的正式版 X.509 标准。X.509 是“开放系统互连”(OSI)系列通信标准的组成部分。可从 ITU 网站 www.itu.int 网购。

7.4.2 发证机构

发证机构(CA)是将公钥基础设施结合到一起的粘合剂。这些中性机构提供数字证书公证服务。你若想从一家信誉良好的 CA 获得数字证书, 你首先必须证明自己的身份达到了这家 CA 的要求。下面列出几大 CA, 它们提供的数字证书被广泛接受:

- Symantec
- IdenTrust
- Amazon Web Services
- GlobalSign
- Comodo
- Certum
- GoDaddy
- DigiCert
- Secom
- Entrust
- Actalis
- Trustwave

目前没有规定禁止什么机构不可以开店经营 CA。但是, CA 签发的证书起码要对得起人们对证书的信任。这是收到第三方数字证书时需要考虑的一个重要问题。如果你不承认和不信任签发证书的 CA, 你就应该信任来自这家 CA 的证书。PKI 依靠的正是信任关系的层级体系。如果你把自己的浏览器设置成信任一家 CA, 浏览器将自动信任这家 CA 签发的所有数字证书。浏览器开发商预先把浏览器设置成信任几家知名 CA, 以免这个负担落到用户身上。

注册机构(RA)分担了 CA 签发数字证书前验证用户身份的负担。RA 虽然本身并不直接签发证书, 但是它们在认证流程中扮演了重要角色, 允许 CA 远程验证用户的身份。



其实场景

证书路径验证

你在学习发证机构的过程中可能知道了证书路径验证(CPV)的说法。CPV 是为了证明每个证书在从原始起点(或信任根)到所涉服务端或客户端的证书路径上始终有效、合法。如果你需要验证“可信”端点之间的每条链路都是最新、有效和可信的，CPV 会非常重要。

当中间系统的证书到期或更换时，这样的问题就会出现：这会打破信任链或验证路径。你需要通过重新验证所有层级的信任关系来重建所有信任链路，证明假定的信任始终都是有保障的。

7.4.3 证书的生成和销毁

公钥基础设施背后的技术概念比较简单。下面将讨论发证机构用于创建、验证和注销客户端证书的流程。

1. 注册

你要想得到一份数字证书，你首先必须以某种方式向 CA 证明自己的身份；这个过程就是注册。如前文所述，注册有时需要拿着自己的相关身份文件与发证机构办事员会面。有些发证机构会提供其他验证渠道，其中包括使用信用报告数据和值得信赖的单位领导人出具的身份证明。

向发证机构证明了自己的身份后，你还要向他们提供自己的公钥。CA 接下来会创建一个 X.509 数字证书，内含你的身份识别信息和一个公钥拷贝。CA 随后会在证书上用 CA 的私钥写上数字签名，并把签了名的数字证书拷贝一个副本交给你。以后，你便可以把这份证书出示给你要与之安全通信的任何人了。

2. 验证

你收到某个你要与之通信的人的数字证书时，你要用 CA 的公钥检查 CA 在证书上的数字签名，以此来验证这份证书。接下来，你必须对照证书注销列表(Certificate Revocation List, CRL)或在线证书状态协议(Online Certificate Status Protocol, OCSP)对证书进行检查，确保这份证书未被注销。这时，只要证书满足以下要求，你便可以认定证书所列公钥是真实的了：

- CA 的数字签名真实；
- 你信任这家 CA；
- 证书没有列在 CRL 上；
- 证书确实包含你信任的数据。

最后一点微妙而又极其重要。你在相信某人的身份信息前，首先要确定这些信息确实包含在证书内。如果证书只含电子邮件地址(billjones@foo.com)而不含个人姓名，则你可以确定，证书所含公钥只与该电子邮件地址关联。CA 没有对 billjones@foo.com 电子邮件账号所涉实际身份下任何结论。然而，如果证书包含 Bill Jones 这个姓名外带一个地址和电话号码，则 CA 还证明了这一信息。

许多流行的 Web 浏览器和电子邮件客户端都嵌入了数字证书验证算法，因此你通常不需要介

入验证流程的细节。然而，始终掌握后台发生的技术细节，对于为机构作出恰当安全判断来说，还是非常重要的。这也是为什么在购买数字证书时，要挑选一家在业界赢得广泛信任的 CA 的原因。如果一家 CA 未被一个主流浏览器收入可信 CA 名单，或者后来被从名单中删除，这势必会大大限制你对证书的使用。

2017 年，数字证书业发生了一起重大安全事故。Symantec 通过一系列关联公司签发了多个不符合行业安全标准的数字证书。Google 作出回应，宣布 Chrome 浏览器不再信任 Symantec 的证书。Symantec 最终只得将自己的正式签发证书的业务出售给 DigiCert，后者允诺签发证书前对证书进行适当验证。这起事故充分证明，适当验证证书请求有多么重要。规程上一连串看上去不起眼的小过失足以毁掉一家 CA 的大部分业务。

3. 注销

发证机构偶尔需要注销证书。这种情况的出现可能由以下原因造成：

- 证书失信(例如，证书拥有者意外泄露了私钥)。
- 证书误发(例如，CA 未经适当验证就错误签发了证书)。
- 证书细节更改(例如，主体名称发生变化)。
- 安全关联变更(例如，主体不再被申请证书的机构雇用)。



提示：

注销请求宽限期是 CA 执行任何“被请求注销”的最长响应时间。该宽限期由“证书实践规范陈述”(CPS)定义。CPS 规定了 CA 在签发或管理证书时所应遵循的实践规范。

以下两种技术手段可以帮助你验证证书的真实性和识别被注销的证书：

证书注销列表。证书注销列表(CRL)由各家发证机构建立和维护，内含 CA 签发和注销的证书序号，外带注销的生效日期和时间。证书注销列表的问题在于，用户必须定期下载 CRL 并交叉查对，这在证书注销的时间与最终用户得到注销通知的时间之间产生了一个滞后期。尽管如此，CRL 依然是当今检查证书状态的最常用方法。

在线证书状态协议(OCSP)。这一协议提供了实时验证证书的渠道，消除了证书注销列表固有的时间滞后。客户端收到一份证书后可向 CA 的 OCSP 服务器发送一个 OCSP 请求。服务器随后将把该证书的有效、无效或未知状态回复给客户端。

7.5 非对称密钥管理

你若是在公钥基础设施内工作，你必须遵守多项最佳实践规范要求，以确保自身通信安全。

首先，挑选加密系统时要理智审慎。前面第 6 章讲过，“通过隧道获得安全”算不上是好办法。你要挑选这样的加密系统：它配备的算法已在公共领域公开，经历了业界专家的百般挑剔。对于那些采用某种“暗箱”方法，始终认为算法保密是确保密码系统完整性之关键的系统，你最好敬而远之。

你还必须以合适的方式挑选密钥。所用密钥的长度要能在安全要求和性能考虑之间取得平衡。此外，你还要确保密钥确实是随机生成的。密钥内存在的任何成形模式都会提高攻击者破解加密信息和降低密码系统安全性的可能性。

你若使用公钥加密，你必须为私钥严格保密！任何情况下都不允许其他任何人接触你的私钥。请务必记住，无论是谁，只要你允许他访问你的私钥，哪怕仅仅一次，都有可能造成你(过去、现在或将来)用这个私钥加密的所有通信永久性失信，使第三方有机会成功假冒你的身份。

密钥完成使命后要退役。许多机构为避免出现未被察觉的密钥失信情况，提出了强制性密钥轮换要求。如果所在机构没有正式制定必须遵守的相关策略，你必须根据自己的密钥使用频率为密钥挑选一个轮换时限。如果可行，你可能需要每隔几个月更换一次密钥对。

你还必须备份自己的密钥！当你因为数据损毁、灾害或其他情况而丢失保存私钥的文件时，你肯定需要有一个备份马上拿来使用。你可能需要自己创建密钥备份，或者使用密钥托管服务，请第三方为你保存备份。无论属于哪种情况，你都要确保备份有安全保障。密钥备份毕竟与主密钥文件同等重要！

硬件安全模块(HSM)也提供管理加密密钥的有效方法。这些硬件设备以某种安全的方式存储和管理加密密钥，使人员不必直接接触密钥。不同的 HSM 在适用范围和复杂性上差异很大，其中既有最简单的设备，例如把密钥加密后拷进 USB 装置供人使用的 YubiKey，也有安放在数据中心的更复杂企业产品。云供应商，例如 Amazon、Microsoft，也配备了基于云的 HSM，由这些 HSM 提供安全密钥管理 IaaS 服务。

7.6 应用密码学

到目前为止，你已学习了有关密码学基础知识、各种密码算法的内部工作机理以及利用公钥基础设施通过数字证书分发身份凭据的大量内容。现在，你应该已经熟悉密码学的基本原理，做好准备进入下一阶段学习：利用这一技术解决日常通信问题。

下面将探讨如何用密码技术来保护静止中的数据(例如存储在便携设备里的数据)，以及借助安全电子邮件、加密的 Web 通信、联网等技术传输的数据。

7.6.1 便携设备

眼下，笔记本电脑、上网本、智能手机和平板电脑无处不在，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，一旦丢失或失窃，会对所涉机构、机构的客户、员工和下属单位造成严重伤害。出于这一原因，许多机构转向用加密技术来保护这些设备上的数据，以防它们被到处乱放。

流行操作系统的当前版本如今都有硬盘加密能力，便于用户在便携设备上使用和管理加密。例如，Microsoft Windows 配备了 BitLocker 和 Encrypting File System(EFS)技术，Mac OS X 配备了 FileVault 加密，而 VeraCrypt 开放源程序包可用来在 Linux、Windows 和 Mac 系统上给硬盘加密。

可信平台模块

现代计算机往往配有一个叫作可信平台模块(Trusted Platform Module, TPM)的专用密码组件。TPM 是安放在设备主板上的一块芯片，可发挥诸多作用，其中包括保存和管理用于全硬盘加密(FDE)解决方案的密钥。TPM 向操作系统提供密钥访问权，防止有人从设备上移除硬盘驱动器并将其插进另一设备以访问驱动器上的数据。

市场上有许多现成的商用工具可以提供额外的性能和管理能力。这些工具的主要差别在于，它们怎样保护保存在内存中的密钥，它们所提供的是否是全硬盘加密还是卷加密，以及它们是否能与基于硬件的 TPM 集成到一起提供额外的安全保护。挑选加密软件的任何工作都应包含对备选产品在这些特点上的优劣进行分析。



提示：

制定便携设备加密策略时千万不要漏掉智能手机。主要智能手机和平板电脑平台都具有支持给手机保存的数据加密的企业级功能。

7.6.2 电子邮件

我们讲过多次，安全是讲究成本效益的。当安全涉及电子邮件时，简便易行是成本效益最高的选择方案。但是有时，你会不得不使用加密功能提供的特定安全服务。鉴于在确保安全的同时也要追求成本效益，下面介绍几条有关电子邮件加密的简单规则：

- 如果你发送的电子邮件需要保密性，你应该给邮件加密。
- 如果你的邮件必须保持完整性，你必须对邮件进行一次散列运算。
- 如果你的邮件需要鉴别、完整性和/或不可否认性，你应该给邮件加上数字签名。
- 如果你的邮件要求保密性、完整性、鉴别和不可否认性，你应该给邮件加密后再加上数字签名。

采用恰当机制确保邮件或传输的安全(即保持保密性、完整性、真实性和不可否认性)，永远是该由发送者承担的责任。

密码学的最大应用需求之一是给电子邮件消息加密和签名。直到最近，经过加密的电子邮件依然要求使用复杂、难用的软件，而这反过来要求人工介入，执行复杂的密钥交换规程。近年来，人们对安全的重视程度不断提高，导致要求对主流电子邮件软件包执行强加密技术。接下来将介绍当今广泛使用的几个安全电子邮件标准。

1. 良好隐私

1991 年，Phil Zimmerman 的良好隐私(Pretty Good Privacy, PGP)安全电子邮件系统在计算机安全领域初露头角。它把本章前文描述过的 CA 层级体系与“信任网”概念结合到了一起——也就是说，你必须得到一名或多名为 PGP 用户的信任才能开始使用系统。接下来，你要接受其他用户对新增用户有效性的判断，以此类推，你还要信任一个从你最初获得信任判断的级别逐级往下延续的多层次用户“网”。

PGP 的推广使用在最初遇到许多障碍。其中最难逾越的是美国政府的出口规定，这些规定将加密技术列为军用品，禁止强加密技术对外出口。幸运的是，这一限制后来被取消，PGP 如今已经可以自由出售给大多数国家。

PGP 有两个可用版本。商业版用 RSA 进行密钥交换，用 IDEA 进行加密/解密，用 MD5 生成消息摘要。免费版(基于极其相似的 OpenPGP 标准)用 Diffie-Hellman 进行密钥交换，用 Carlisle Adams/Stafford Tavares(CAST)128 位加密/解密算法进行加密/解密，用 SHA-1 散列函数生成消息摘要。

许多商业供应商还以基于 Web 的云电子邮件服务、移动设备应用程序或 Webmail 插件的形式提供基于 PGP 的电子邮件服务。这些服务深受管理员和最终用户欢迎，因为它们取消了配置和维护加密证书的复杂操作，为用户提供了受严格管理的安全电子邮件服务。StartMail、Mailvelope、SafeGmail 和 Hushmail 就属于这类产品。

2. S/MIME

安全/多用途互联网邮件扩展(Secure/Multipurpose Internet Mail Extensions, S/MIME)协议已经成为加密电子邮件的事实标准。S/MIME 使用 RSA 加密算法，得到业界大佬的支持，其中包括 RSA Security。S/MIME 目前已被大量商业产品采用，其中包括：

- Microsoft Outlook 和 Office 365；
- Mozilla Thunderbird；
- Mac OS X Mail；
- GSuite 企业版。

S/MIME 通过 X.509 证书交换密码密钥。这些证书包含的公钥用于数字签名和交换对称密钥，而这些对称密钥将用于较长的通信会话。RSA 是 S/MIME 唯一支持的公钥密码协议。这一协议支持 AES 和 3DES 对称加密算法。

尽管 S/MIME 标准得到业界强力支持，但是它的技术局限阻碍了它被广泛采用。虽然主要品牌桌面邮件应用程序都支持 S/MIME 电子邮件，但是基于 Web 的主流邮件系统并不支持它(需要使用浏览器扩展)。

7.6.3 Web 应用程序

加密被广泛用于保护网上交易。这主要源自于电子商务的强劲发展，以及电子商务供应商和消费者在网络上安全交换财务信息(例如信用卡信息)的需求。接下来将探讨在 Web 浏览器中负责小锁锁定图标(small lock icon)的两项技术——安全套接字层(SSL)和传输层安全(TLS)。

SSL 由 Netscape 开发，可向客户端/服务端提供 Web 流量加密。超文本传输协议安全(HTTPS)通过端口 443 来协商 Web 服务器与浏览器客户端之间的加密通信会话。SSL 最初作为 Netscape 浏览器的一项标准推出，但是 Microsoft 也把它用作自己的流行浏览器 Internet Explorer 的安全标准。这两大浏览器产品的采用，使 SSL 成为事实上的互联网标准。

SSL 依靠交换服务器数字证书在浏览器与 Web 服务器之间协商加密/解密参数。SSL 的目的是创建面向整个 Web 浏览会话开放的安全通信信道。它依赖于对称和非对称加密法的相互结合。以下是其中涉及的步骤：

- (1) 当一名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钥。
- (2) 浏览器随后创建一个随机对称密钥，用服务器的公钥对密钥加密，然后将加密后的对称密钥发送给服务器。
- (3) 服务器随后用自己的私钥解密对称密钥，两个系统这时通过对称加密密钥交换所有未来消息。

这种方法允许 SSL 借用非对称加密法的高级功能，同时用速度更快的对称算法加密和解密数据的绝大部分内容。

1999 年，安全工程师提出了可替换 SSL 标准的 TLS，后者当时已是第 3 版。与 SSL 一样，TLS 使用 TCP 端口 443。TLS 在 SSL 技术的基础上采用了许多安全强化方案，最终取代 SSL 被大多数应用程序采用。早期版本的 TLS 遇到通信双方都不支持 TLS 的情况时，支持降级至 SSL v3.0 进行通信会话。不过到了 2011 年，TLS v1.2 取消了这项向后兼容。

2014 年，一次名为“Padding Oracle On Downgraded Legacy Encryption”(POODLE)的攻击揭示 TLS 的 SSL 3.0 回退机制存在一个严重缺陷。在修复这一漏洞的过程中，许多机构完全取消对 SSL 的支持，如今只依靠 TLS 的安全保护了。



提示：

即使 TLS 已经存在十多年，现在依然还有许多人误称其为 SSL。由于这一原因，TLS 得到了一个 SSL 3.1 的外号。

隐写术和水印

隐写术(Steganography)是通过加密技术把秘密消息嵌入另一条消息的技艺。隐写算法的工作原理是从构成图像文件的大量位中选出最不重要的部分作出改动。这种技术使通信参与方得以把消息藏匿在光天化日之下——例如，通信参与方可以把一条秘密消息镶嵌到一个原本毫无关系的网页里。

使用隐写术的人一般会把秘密消息嵌入图像文件或 WAV 文件，因为这两种文件通常体积庞大，即便是眼光最敏锐的检查者也难免漏过隐藏在其中的秘密消息。隐写术往往是非法或可疑勾当的惯用手段，例如间谍活动和色情活动。

当然，隐写术也可以用于合法目的。给文件加上数字水印(watermark)以保护知识产权，就是通过隐写术实现的。隐藏在水印中的信息只有文件的创建者知情。若是日后有人未经授权拷贝文件内容，水印可用来检测拷贝，如果加上独有水印的文件被提供给每个原始接收者的话，还可以用来从侵权拷贝回追溯到来源。

隐写术简便易用，网上就能找到免费工具。图 7.2 演示了一款此类工具 iSteg 的完整界面。这个工具只要你规定一个内含你的秘密消息的文本文件和一个你想用来隐藏消息的图像文件，图 7.3 则显示一张嵌入了秘密消息的图片；一个人只凭肉眼根本无法查出图片中的消息。

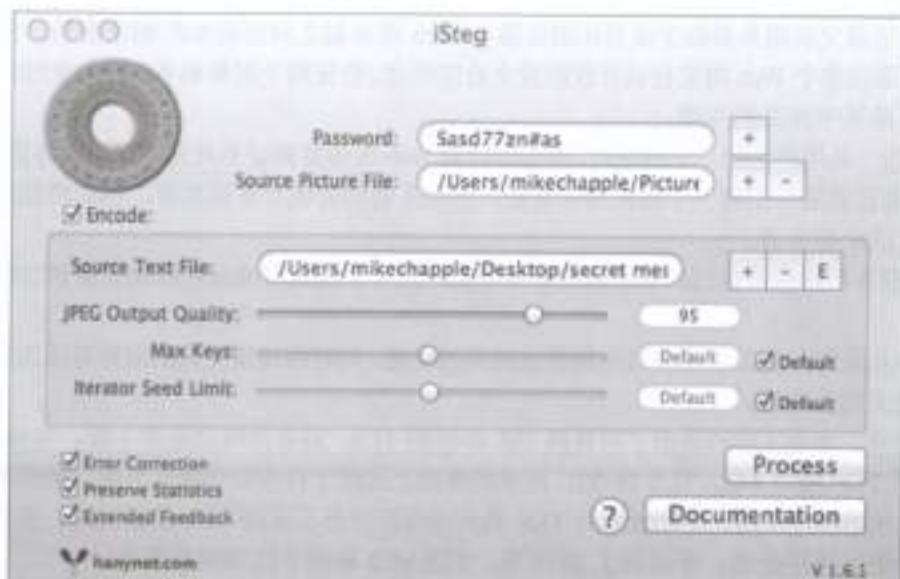


图 7.2 隐写工具



图 7.3 嵌入了消息的图像

7.6.4 数字版权管理

数字版权管理(Digital Right Management, DRM)软件通过加密在数字媒体上执行版权限制。过去 10 年来，出版界一直在尝试给各类媒体配上 DRM 方案，其中包括音乐、电影和图书。许多情况下，尤其在音乐方面，反对者激烈抵制部署 DRM 的尝试，他们指出，DRM 的使用践踏了他们自由享用得到合法许可的媒体文件并制作拷贝的权利。

**注意：**

正如你在本节中看到的，广泛配备 DRM 的许多商业尝试在用户视此项技术为侵权和/或阻碍的反对声浪中失败了。

1. 音乐 DRM

多年来，音乐行业一直在与盗版进行斗争，这场战斗可以追溯到自行复制卡式磁带以及转换光盘和数字格式的时代。音乐发行公司尝试使用各种 DRM 方案，但大多在消费者的压力下放弃了这一技术。

面对消费者的反对，苹果公司取消了对通过 iTunes Store 出售的音乐采用 FairPlay DRM 的做法，从而导致 DRM 推广使用的步伐大大减慢。2007 年，苹果公司联合创始人史蒂夫·乔布斯向音乐行业发出一封公开信，呼吁业界允许苹果公司出售无 DRM 的音乐——这预示了 DRM 的这一发展趋势。这封信公开信的部分内容如下：

第三种选择是完全废除 DRM。我们不妨想象，如果每家电商都可以出售以开放授权格式编码的无 DRM 音乐，那会是怎样一个世界。在这样的世界里，任何乐迷都可以播放从任何商店购买的音乐，任何店家都可以出售所有音乐爱好者都可以享受的音乐。这显然是对消费者最有利的选择方案，而苹果公司愿意张开双臂拥抱它。如果四大唱片公司能够不以要求处于 DRM 保护之下为条件为苹果公司提供音乐授权，我们会转而在 iTunes Store 里只出售无 DRM 音乐。以后出品的每一台 iPod 都将只播放这种无 DRM 音乐。

苹果公司网站已经不再刊载这封公开信的全文，但是你可以在 <http://bit.ly/1TyBm5e> 找到它的存档拷贝。

目前，DRM 技术在音乐领域主要用于基于订阅的服务，如 Napster 和 Kazaa，这些服务在用户订阅期结束时利用 DRM 技术撤消用户对已下载音乐的访问权。

**注意：**

本节对 DRM 技术的描述是不是有些含混不清？这是有原因的：制造商通常不会透露他们所用 DRM 功能的细节，因为他们担心盗版会利用这些信息来击败 DRM 方案。

2. 电影 DRM

多年以来，电影业一直在用各种 DRM 方案来对付全世界泛滥的电影盗版问题。以下是用来保护大众传播媒体的两项主要技术：

高带宽数字内容保护(HDCP)，可为通过数字连接(包括 HDMI、DisplayPort 和 DVI 接口)传送的内容提供 DRM 保护。尽管当前在许多执行方案中还能看到这一技术的影子，但是自黑客于 2010 年披露一个 HDCP 主密钥起，它提供的服务已完全归于无效。

高级访问内容系统(AACS)，可保护存储在 Blu-Ray 和 HD DVD 介质中的内容。黑客们展示，他们的攻击恢复了 AACS 的加密密钥并把这些密钥在互联网上张贴出来。

业界出版人和黑客如今还在继续这场猫捉老鼠游戏：媒体公司试图保护他们的内容，而黑客则寻求获得对未加密拷贝的持续访问权。

3. 电子书 DRM

部署 DRM 技术的最成功案例，恐怕非图书和文档出版领域莫属。当今市场上的大多数电子图书都使用了某种形式的 DRM，这些技术还能为配备了 DRM 能力的公司保护所生成的敏感文档。



提示：

今天使用中的所有 DRM 方案都有一个致命弱点：用来访问内容的设备必须有权访问解密密钥。如果解密密钥保存在最终用户拥有一台设备中，用户总有机会操控设备访问密钥。

Adobe Systems 通过 Adobe Digital Experience Protection Technology (ADEPT) 为出售的各种格式电子书提供 DRM 技术。ADEPT 结合使用了加密介质内容的 AES 技术和保护 AES 密钥的 RSA 加密技术。许多电子书阅读器借助这一技术保护自己的内容——Amazon Kindle 是值得注意的例外：Amazon 的 Kindle 电子书阅读器以各种格式销售图书，每种格式都包含自己的加密技术。

4. 电子游戏 DRM

许多电子游戏都执行了 DRM 技术，依靠游戏机通过一个活跃的互联网连接来验证一项基于云的服务签发的游戏许可证。这些技术，比如 Ubisoft 公司的 Uplay，曾经要求游戏必须持续联网游戏才能往下进行。玩家如果中途断网，游戏便会停下来。

2010 年 3 月，Uplay 系统遭遇拒绝服务攻击，世界各地的 Uplay 游戏玩家无法像以往那样玩正常运行的游戏，因为他们的游戏机无法访问 Uplay 服务器。这导致公众提出强烈抗议，Ubisoft 随后取消了永远在线要求，转向采用一种 DRM 方法——只需要最初在游戏机上激活游戏，游戏便可以不受限制地往下进行。

5. 文档 DRM

虽然保护娱乐内容是 DRM 技术的最常见用途，但机构还可以用 DRM 来保护以 PDF 文件、办公文档和其他格式保存的敏感信息的安全。商用 DRM 产品(如 Vitrium 和 FileOpen)，通过加密保护源内容，使机构得以严格控制文档访问权限。

下面列几个文档 DRM 解决方案限制的常见许可权：

- 读文件；
- 修改文件内容；
- 移除文件水印；
- 下载/保存文件；
- 打印文件；
- 文件内容截图。

DRM 解决方案可以在需要时授予权限，在不再需要时注销权限，乃至在既定期限届满后自动宣布权限到期，以这样的方式帮助机构控制这些权限。

7.6.5 联网

本章探讨的密码学的最后一项应用是用密码算法保护联网服务的安全。下面将简要介绍用于确保通信线路安全的两种方法。我们还将讨论 IPsec 和互联网安全关联和密钥管理协议 (Internet Security Association and Key Management Protocol, ISAKMP)，并讨论与无线联网相关的一些安全问题。

1. 线路加密

安全管理员可用两种加密技术保护在网络上传送的数据：

- **链路加密** 通过在两点之间创建一条安全隧道来保护整个通信线路；创建隧道的具体做法是使用硬件解决方案或软件解决方案；使用软件解决方案时，方案在隧道的一端加密进入的所有通信流，然后在另一端解密流出的所有通信流。例如一家有两个办公地点的公司用一条数据线路连接两个办公室，这家公司可能会用链路加密来防止有攻击者在两个办公室之间的某个点上监视通信线路。
- **端到端加密** 独立于链路加密执行，保护通信双方(例如一个客户端和一台服务器)之间的通信。用 TLS 来保护一个用户与一台 Web 服务器之间的通信是端到端加密的例子。这种做法可防止入侵者在已加密链路的安全端监视通信流，也可防止入侵者监视通过未加密链路传递的通信流。

链路加密和端到端加密之间的关键差别在于，在链路加密中，所有数据(包括消息报头、消息尾部、地址和路由数据)都是被加密的。因此，每个数据包在每个中继段只有解密后重新加密，才能正常进入下一个中继段继续发送，这减慢了路由的速度。端到端加密不给报头、尾部、地址和路由数据加密，因此从一个点到另一个点的传送速度更快，但面对嗅探器和窃听者也显得更脆弱。

加密在 OSI 模型的较高层级进行时，通常采用端到端加密；如果加密在 OSI 模型的较低层级进行，通常使用链路加密。

SSH(安全壳)是端到端加密技术的一个好例子。这套程序为常用互联网应用程序提供了加密备选方案，如文件传输协议(FTP)、Telnet、rlogin 等。SSH 其实有两个版本。SSH1(如今已被业界认为不安全)支持数据加密标准(DES)、三重 DES(3DES)、国际数据加密算法(IDEA)和 Blowfish 算法。SSH2 取消了对 DES 和 IDEA 的支持，又增加了对其他几种算法的支持。

2. IPsec

当今有各种安全架构可供使用，每个架构都是为解决不同环境中的安全问题而设计的。互联网协议安全(IPsec)标准就是其中支持安全通信的一个架构。IPsec 是由互联网工程任务组(IETF)提出的一个标准架构，用于在交换信息的两个实体之间建立安全信道。

通过 IPsec 进行通信的实体可以是两个系统、两台路由器、两个网关或任何实体组合。IPsec 虽然一般用于连接两个网络，但也可以用于连接单个计算机，例如一台服务器和一个工作站，或一对工作站(或许是发送者和接收者)。IPsec 没有规定任何执行细节，但它是一个开放的模块化框架，使许多制造商和软件开发商得以自行开发可与其他厂家的产品良好兼容的 IPsec 解决方案。

IPsec 通过公钥加密法提供加密、访问控制、不可否认性和消息鉴别，全部使用基于 IP 的协议。IPsec 主要用于虚拟专用网(VPN)，因此 IPsec 可在传输或隧道模式下运行。IPsec 通常与第二层隧道协议(L2TP)配对，形成 L2TP/IPsec。

IPsec 协议为受保护的网络通信提供了一个完整的基础设施。IPsec 如今赢得广泛认可，已成为许多商用操作系统产品包的必含之物。IPsec 所依靠的是安全关联，其中包含两个主要成分：

- **身份验证头(AH)** 提供消息完整性和不可否认性保障。AH 还提供鉴别和访问控制，可抵御重放攻击。
- **封装安全载荷(ESP)** 提供数据包内容的保密性和完整性保障。ESP 还提供加密和有限的鉴别，也可抵御重放攻击。



注意：

ESP 还可以提供一些有限的鉴别服务，但达不到 AH 的程度。虽然 ESP 有时也脱离 AH 单独使用，但是这种情况毕竟非常少见。

IPsec 可在两种离散模式下运行。IPsec 在传输模式下使用时，只加密数据包载荷。这种模式是为对等通信设计的。IPsec 在隧道模式下使用时，将加密包括报头在内的整个数据包。这一模式是为网关到网关的通信设计的。



提示：

IPsec 是现代计算机安全的一个极其重要的概念。务必确保自己熟知 IPsec 的成分协议和运行模式。

在运行过程中，你要通过创建一个安全关联(SA)来建立 IPsec 会话。SA 代表通信会话，记录了有关连接的所有配置和状态信息。SA 还代表一次单纯连接。你若是想建立一条双向信道，你将需要建立两个 SA，两个方向各用一个。此外，你若是想建立一条支持同时使用了 AH 和 ESP 的双向信道，你将需要建立 4 个 SA。

在 IPsec 的最大长处中，有一些来自于它能基于每个 SA 对通信进行过滤或管理，这样一来，存在安全关联的客户端或网关，无论它们使用哪些协议或服务，只要能够使用 IPsec 连接，就能受到严格管理。此外，在没有明确定义有效安全关联的情况下，成对的用户或网关之间将不能建立 IPsec 链路。

有关 IPsec 算法的详细内容，请见本书第 11 章。

3. ISAKMP

ISAKMP(互联网安全关联和密钥管理协议)通过协商、建立、修改和删除安全关联为 IPsec 提供后台安全支持服务。你在前一节刚学过，IPsec 依靠的是安全关联系统(SA)。这些 SA 通过 ISAKMP 接受管理。互联网 RFC 2408 对 ISAKMP 提出了四点基本要求：

- 鉴别通信伙伴；
- 创建和管理安全关联；
- 提供密钥生成机制；
- 抵御威胁(例如重放和拒绝服务攻击)。

4. 无线联网

无线网络的快速推广带来了巨大安全风险。许多传统网络并不对本地网络上主机之间的日常通信加密，它们坚信这样的假设：攻击者很难物理接触安全地点内的网络线路，因此不可能搭线监听网络。然而，无线网络是在空中传输数据的。面对拦截自然极其脆弱。用于保护无线网络安全的方案主要有两类：

有线等效保密。有线等效保密(Wired Equivalent Privacy, WEP)为保护无线局域网内的通信提供 64 和 128 位加密选项。IEEE 802.11 将 WEP 描述为无线联网标准的一个可选成分。



警告：

密码分析已确凿证明 WEP 算法存在重大缺陷，这些缺陷使几秒内完全破坏受 WEP 保护的网络成为可能。你绝不可用 WEP 加密来保护无线网络。事实上，2007 年被媒体大肆渲染的 TJX 安全漏洞，其罪魁祸首就是商店网络使用了 WEP 加密。再次强调，你绝不可在无线网络上使用 WEP 加密。

WiFi 受保护访问。WiFi 受保护访问(WPA)以执行临时密钥完整性协议(TKIP)的方式消除破坏 WEP 的密码缺陷，从而提高了 WEP 加密的安全水平。这一技术的进一步改进版叫 WPA2，增加了 AES 密码。WPA2 提供的安全算法适于在现代无线网络上使用。



警告：

请记住，WPA 并不提供端到端安全解决方案。它只给一部移动计算机与最近的无线访问点之间的通信流加密。通信流到达有线网后将变回明文。

另一项常用安全标准是 IEEE 802.1x，可为有线和无线网络内的鉴别和密钥管理提供一个灵活框架。客户端使用 802.1x 时首先要运行一款叫作 Supplicant 的软件。Supplicant 与鉴别服务器建立通信。客户端通过鉴别后，网络交换机或无线访问点将允许客户端访问网络。WPA 就是为与 802.1x 鉴别服务器交互而设计的。

7.7 密码攻击

与任何安全机制遇到的情况一样，心怀歹意的人找出了许多攻击手段来击败密码系统。你若想将自己的系统面临的风险降到最低，就必须对各种密码攻击的威胁了如指掌——这一点至关重要。

分析攻击。这是试图降低算法复杂性的一种代数操作。分析攻击的焦点是算法本身的逻辑。

执行攻击。这是探寻密码系统在执行过程中暴露的弱点的一种攻击。它着重于挖掘软件代码，其中不仅包括错误和缺陷，还涉及用来给加密系统编程的方法。

统计攻击。统计攻击探寻密码系统的统计学弱点，例如浮点错误和无力生成真随机数。统计攻击试图在承载密码应用的硬件或操作系统中找到漏洞。

蛮力攻击。蛮力攻击是直截了当的攻击。这种攻击尝试找出密钥或口令的每种可能的有效组合。攻击的实施涉及用大量处理能力来系统化猜测用于加密通信的密钥。

就无缺陷协议(nonflawed protocol)而言，通过蛮力攻击发现密钥所需要的平均时间与密钥长度成正比。只要时间充分，蛮力攻击早晚会成功。密钥长度每增加一位，执行蛮力攻击的时间

会增加一倍，因为潜在密钥的数量也翻了一番。

蛮力攻击如今做了两点改进，蛮力攻击的效果由此得到提升：

- 彩虹表为密码散列提供预先算出的值。彩虹表通常用于破解以散列形式保存在系统中的口令。
- 专为蛮力攻击设计的专用可扩展计算硬件，可以大幅提高这一攻击手段的效率。

加盐保护口令

盐或许会危害你的健康，但它却能保护你的口令。为了帮助打击蛮力攻击，其中包括借助词典和彩虹表的蛮力攻击，密码学家利用了一种叫作密码盐的技术。

密码盐是一个随机值，在操作系统对口令进行散列运算之前添加到口令的末尾。盐随后与散列一起保存在口令文件中。操作系统要将用户提交的口令与口令文件比较时，首先检索盐并将其附在口令之后。操作系统向散列函数输入连续值，然后将得出的散列与保存在口令文件里的散列进行对比。

PBKDF2、Bcrypt、Scrypt 等专用口令散列函数允许利用盐创建散列，同时采用一种叫作密钥拉伸(key stretching)的技术，增加了猜测口令的难度。

加盐技术的使用，特别是与密钥拉伸技术结合在一起的时候，会令蛮力攻击的难度大幅度上升。任何人若想创建彩虹表，都必须为密码盐的每个可能值单独建表。

频率分析和唯密文攻击。许多时候，可供攻击者摆弄的只有经过加密的密文消息——这种情景就是唯密文攻击。在这样的情况下，频率分析——即计数每个字母在密文中出现的次数——被证明是可以帮助破解简单密码的一种技术手段。众所周知，E、T、A、O、I、N 是英语中最常用字母：攻击者就是借助这个知识来测试以下两个假设的：

- 如果这些字母也在密文中使用得最频繁，则密码可能是一种移位密码，即重新排列了明文字符而未加任何改动。
- 如果密文中使用得最频繁的是其他字母，则密码可能是某种替换密码，即更换了明文字符。

这是频率分析的简单形式，而这一技术的许多复杂变体可用来破解多表密码和其他复杂密码系统。

已知明文。在已知明文攻击中，攻击者掌握了加密消息的拷贝以及用于生成密文(拷贝)的明文消息。掌握这些信息可为攻击者破解弱代码提供很大帮助。例如，我们不妨想象一下，如果你掌握了同一条消息的明文拷贝和密文拷贝，破解第 6 章所述凯撒密码将是一件多么轻而易举的事情。

选择密文。在选择密文攻击中，攻击者能够解密密文消息中被选中的部分，然后用解密后的那部分消息来发现密钥。

选择明文。在选择明文攻击中，攻击者能给他们选中的明文消息加密，然后根据加密算法分析密文输出。

中间相遇。攻击者可能通过中间相遇攻击手段来击败采用两轮加密的加密算法。恰恰因为这种攻击的出现，造成作为 DES 加密可行强化版的双重 DES(2DES)很快被弃用，被三重 DES(3DES)取代。

攻击者在中间相遇攻击中使用一条已知的明文消息，这条明文消息随后用每个可能的密钥

(k1)加密，得出的密文再用所有可能的密钥(k2)解密。找到匹配时，对应的一对(k1、k2)将代表双重加密的两个部分。这种攻击的耗时通常只是破解提供最低附加保护的单轮加密所需时间的两倍(或 2^n ，而不是预计的 2^{n+2^n})。

中间人。在中间人攻击中，一个心怀歹意之人在位于两个通信方之间的一个地方拦截所有通信(其中包括密码会话的设定)。攻击者回应原发者的初始化请求并与原发者建立一个安全会话。攻击者随后用一个不同的密钥冒充原发者与预期接收者建立第二个安全会话。攻击者这时便“位于通信中间”了，可以读取两个通信参与方之间的所有流经通信内容。



提示：

切记不要把中间相遇攻击与中间人攻击弄混。它们看似名称相近，却是完全不同的两种攻击。

生日。生日攻击也叫碰撞攻击或反向散列匹配(请见第14章中有关蛮力攻击和词典攻击的讨论)。这种攻击寻求从散列函数的一对一性质中找出破绽。实施生日攻击时，心怀歹意者尝试在有数字签名的通信中换用一条可生成相同消息摘要的不同消息，从而保持原始数字签名的有效性。



注意：

切记，社会工程技术手段也能用于密码分析。你若是只需要找发送者问问就能搞到解密密钥，岂不比破解密码系统容易太多？

重放。重放攻击用于针对没有采用临时保护措施的密码算法。在这种攻击中，心怀歹意之人在通信双方之间拦截经过加密的消息(常常是鉴别请求)，然后通过“重放”捕捉来的消息建立一个新会话。采用时间戳并给每条消息设定过期时间，可以挫败重放攻击。

7.8 本章小结

非对称密钥加密法(或公钥加密)提供了一种极其灵活的基础设施，可为发起通信之前并不一定彼此相识的各方之间进行简单、安全通信带来极大方便。它还提供了消息数字签名框架，可确保消息的不可否认性和完整性。

本章探讨了公钥加密，这种方法为大量用户提供了一种可伸缩的密码架构。我们还描述了一些流行的密码算法，例如链路加密和端到端加密。最后介绍公钥基础设施，它通过发证机构(CA)生成数字证书，内含系统用户的公钥以及数字签名，而数字证书所依靠的是公钥加密法与散列函数的结合使用。

我们还介绍了密码技术在解决日常问题方面的一些常见应用情况。你学习了密码可以怎样用来保护电子邮件(通过PGP和S/MIME)、Web通信(通过SSL和TLS)、对等和网关到网关联网(通过IPsec和ISAKMP)以及无线通信(通过WPA和WPA2)。

最后，我们讨论了心怀歹意之人用来干扰或拦截两方之间加密通信的几种比较常见的攻击手段，其中包括密码分析攻击、重放攻击、蛮力攻击、已知明文攻击、选择明文攻击、选择密文攻击、中间相遇攻击、中间人攻击和生日攻击。你若想挫败这些攻击，提供适当安全保护，你就要对它们了如指掌。

7.9 考试要点

了解非对称加密法所用密钥类型。公钥可在通信参与方之间自由共享，而私钥必须保密。给消息加密时使用接收者的公钥。给消息解密时使用自己的私钥。给消息签名时使用自己的私钥。验证签名时使用发送者的公钥。

熟知三种主要公钥密码系统。RSA 是最著名的公钥密码系统，由 Rivest、Shamir 和 Adleman 于 1977 年开发。该密码系统所依赖的素数乘积很难被因式分解。El Gamal 是 Diffie-Hellman 密钥交换算法的一种扩展，所依赖的是模运算。椭圆曲线算法依靠椭圆曲线离散对数题，如果所用的密钥与其他算法使用的密钥相同，它会比其他算法安全性更高。

了解散列函数的基本要求。优质散列函数有五点要求。它们必须接受任何长度输入、提供固定长度输出、方便地为任何输入计算散列函数、提供单向功能以及不存在冲突。

熟知主要散列算法。安全散列算法(SHA)的后继者 SHA-1 和 SHA-2 构成了政府标准消息摘要功能。SHA-1 生成 160 位消息摘要，SHA-2 支持可变长度，最高到 512 位。SHA-3 提高了 SHA-2 的安全性，支持相同散列长度。

了解密码盐提高口令散列安全性的原理。如果对口令直接进行散列运算后保存到口令文件中，攻击者可用预先算好数值的彩虹表来识别常用口令。但在进行散列运算前给口令加上盐，则可以降低彩虹表攻击的效果。一些常用口令散列算法还用密钥拉伸技术进一步增加了攻击难度。PBKDF2、Bcrypt 和 Scrypt 是其中的三种。

了解数字签名的生成和验证过程。你若给消息写数字签名，首先用散列函数生成一个消息摘要，然后用自己的私钥给摘要加密。你若验证消息的数字签名，首先用发送者的公钥解密摘要，然后将消息摘要与自己生成的摘要进行比较。如果二者匹配，则消息真实可信。

了解数字签名标准(DSS)的成分。数字签名标准使用了 SHA-1、SHA-2 和 SHA-3 消息摘要函数外加以下三种加密算法中的一种：数字签名算法(DSA)、RSA(Rivest、Shamir、Adleman)算法或椭圆曲线 DSA(ECDSA)算法。

了解公钥基础设施(PKI)。在公钥基础设施中，发证机构(CA)生成内含系统用户公钥的数字证书。用户随后将这些证书分发给他们要与之通信的人。证书接收者用 CA 的公钥验证证书。

了解密码用于保护电子邮件的常见做法。S/MIME 协议是新涌现的邮件消息加密标准。另一个流行的电子邮件安全工具是 Phil Zimmerman 的 PGP。电子邮件加密的大多数用户都给自己的电子邮件客户端或基于 Web 的电子邮件服务配备了这一技术。

了解密码用于保护 Web 活动的常见做法。保护 Web 通信流的事实标准是在 TLS 或较老的 SSL 的基础上使用 HTTP。大多数 Web 浏览器都支持这两个标准，但是许多网站出于安全方面的考虑，如今已取消对 SSL 的支持。

了解密码用于保护网络连接的常见做法。IPsec 协议标准为加密网络通信流提供了一个通用框架，被配备到许多流行操作系统中。在 IPsec 传输模式下，数据包内容会被为对等通信加密。在隧道模式下，整个数据包(包括报头信息)，会为网关到网关通信加密。

要能描述 IPsec。IPsec 是支持 IP 安全通信的一种安全架构框架。IPsec 会在传输模式或隧道模式下建立一条安全信道。IPsec 可用来在计算机之间建立直接通信或在网络之间建立一个虚拟专用网(VPN)。IPsec 使用了两个协议：身份验证头(AH)和封装安全载荷(ESP)。

能说明常见密码攻击。蛮力攻击尝试随机发现正确的密码密钥。已知明文、选择密文和选

择明文攻击要求攻击者除了拿到密文以外，还必须掌握一些附加信息。中间相遇攻击利用进行两轮加密的协议。中间人攻击欺骗通信双方，使他们都与攻击者通信，而不是相互直接通信。生日攻击试图找到散列函数的冲突点。重放攻击试图重新使用鉴别请求。

了解使用数字版权管理(DRM)的使用情况。数字版权管理(DRM)解决方案允许内容拥有者限制他人对内容的使用。DRM 解决方案通常用于保护娱乐内容，如音乐、电影、电子书等，不过偶尔也会有企业用它们来保护存储在文档中的敏感信息。

7.10 书面实验

1. 如果 Bob 要通过非对称密码将一条保密消息发送给 Alice，请说明 Bob 应采用的流程。
2. 请说明 Alice 用来解密上题所述 Bob 消息的流程。
3. 请说明 Bob 用来给发送给 Alice 的消息加上数字签名的流程。
4. 请说明 Alice 用来验证问题 3 所述 Bob 消息上数字签名的流程。

7.11 复习题

1. 在 RSA 公钥加密系统中，以下哪个数会永远是最大数？
 - e
 - n
 - p
 - q
2. 哪种密码算法是 El Gamal 密码系统的基础？
 - RSA
 - Diffie-Hellman
 - 3DES
 - IDEA
3. 如果 Richard 要借助一个公钥密码系统给 Sue 发送一条加密信息，他会用哪个密钥给消息加密？
 - Richard 的公钥
 - Richard 的私钥
 - Sue 的公钥
 - Sue 的私钥
4. 如果一条 2048 位明文消息通过 El Gamal 公钥密码系统加密，所得的密文消息有多长？
 - 1024 位
 - 2048 位
 - 4096 位
 - 8192 位

5. Acme Widgets 公司目前全面采用 1024 位 RSA 加密标准。该公司计划从 RSA 转向使用椭圆曲线密码系统。如果该公司希望保持同等密码强度，它应该使用哪种 ECC 密钥长度？
- A. 160 位
 - B. 512 位
 - C. 1024 位
 - D. 2048 位
6. John 打算为要发送给 Mary 的一条 2048 字节消息生成一个消息摘要。如果他使用 SHA-1 散列算法，那么这条特定消息的消息摘要有多大？
- A. 160 位
 - B. 512 位
 - C. 1024 位
 - D. 2048 位
7. 以下四项技术中，哪一项被认为存在缺陷因而不应再使用？
- A. SHA-3
 - B. PGP
 - C. WEP
 - D. TLS
8. WPA 采用哪项加密技术保护无线通信？
- A. TKIP
 - B. DES
 - C. 3DES
 - D. AES
9. Richard 收到 Sue 发给他的一条加密消息。他应该用哪个密钥来解密消息？
- A. Richard 的公钥
 - B. Richard 的私钥
 - C. Sue 的公钥
 - D. Sue 的私钥
10. Richard 要为准备发送给 Sue 的一条消息加上数字签名，以便 Sue 能够确定消息发自 Richard 并在传输过程中未发生改动。Richard 应该用哪个密钥给消息摘要加密？
- A. Richard 的公钥
 - B. Richard 的私钥
 - C. Sue 的公钥
 - D. Sue 的私钥
11. 以下算法中，哪一种是数字签名标准不支持的？
- A. 数字签名算法
 - B. RSA
 - C. El Gamal DSA
 - D. 椭圆曲线 DSA

12. 安全电子通信数字证书的创建和认可应该遵循国际电信联盟(ITU)的哪项标准?
- A. X.500
 - B. X.509
 - C. X.900
 - D. X.905
13. 哪种密码系统为商用版 Phil Zimmerman “良好隐私” 安全电子邮件系统提供加密/解密技术?
- A. ROT13
 - B. IDEA
 - C. ECC
 - D. El Gamal
14. 传输层安全通信流使用哪个 TCP/IP 通信端口?
- A. 80
 - B. 220
 - C. 443
 - D. 559
15. 哪种密码攻击证明双重 DES(2DES)不比标准 DES 加密效果更好?
- A. 生日攻击
 - B. 选择密文攻击
 - C. 中间相遇攻击
 - D. 中间人攻击
16. 以下哪种工具可用来提高暴力口令破解攻击的效果?
- A. 彩虹表
 - B. 分层筛选
 - C. TKIP
 - D. 随机强化
17. 以下哪种链路受 WPA 加密保护?
- A. 防火墙到防火墙
 - B. 路由器到防火墙
 - C. 客户端到无线访问点
 - D. 无线访问点到路由器
18. 使用证书注销列表的主要劣势是什么?
- A. 密钥管理
 - B. 延迟
 - C. 记录即时更新
 - D. 面对暴力攻击脆弱
19. 以下哪种加密算法如今被认为不安全了?
- A. El Gamal
 - B. RSA

- C. 椭圆曲线密码
 - D. Merkle-Hellman 背包
20. IPsec 的定义是什么？
- A. 特定配置的所有可能安全分类
 - B. 一种用于建立安全通信信道的框架
 - C. Biba 模型的有效过渡状态
 - D. TCSEC 安全类别

安全模型、设计和能力的原则

本章涵盖的 CISSP 认证考试主题包括：

- ✓ 域 3：安全架构和工程
 - 3.1 使用安全设计原则实施和管理工程过程
 - 3.2 理解安全模型的基本概念
 - 3.3 根据系统安全需求选择控制措施
 - 3.4 理解关于信息系统的安全能力

针对特定的安全需求选择最好的控制措施时，理解安全解决方案背后的原理，有助于你缩小搜索范围。本章将讨论安全模型，包括状态机、Bell-LaPadula、Biba、Clark-Wilson、Take-Grant 以及 Brewer and Nash 模型。本章也将介绍通用准则(Common Criteria)和其他方法，尤其会重点介绍美国国防部和国际安全评估标准，政府和公司使用这些准则评估信息系统的安全性。最后讨论常见的设计缺陷和其他问题，它们可能导致系统容易受到攻击。

确定一个系统的安全程度的过程既困难又耗费时间。本章讲解如何评估一个计算机系统的安全级别。首先介绍和解释用来描述信息系统安全性的基本概念和术语，并讨论安全计算、安全边界、安全和访问监控器以及内核代码。接下来讨论安全模型，解释如何实现访问和安全控制措施。我们也将简要解释系统安全如何分类，例如分为开放的和封闭的；描述一组用于保证数据保密性、完整性和可用性的标准安全技术；讨论安全控制；介绍一套标准的网络安全保护协议族。

本域的其他内容在第 6 章、第 7 章、第 9 章以及第 10 章中讨论。需要学习所有这些章节，以确保全面掌握本域的主题。

8.1 使用安全设计原则实施和管理工程过程

在系统开发的每个阶段都应考虑安全。程序员应该努力为他们开发的每个应用构建安全性，为关键应用以及处理敏感信息的应用提供更高级别的安全性。在开发项目的早期就考虑安全的影响非常重要，因为在系统开发时加入安全性比在已有系统上添加安全性更容易。下面讨论一些基本的安全设计原则。在硬件或软件项目工程过程的早期就应该实现和管理这些原则。

8.1.1 客体和主体

对安全系统中任何资源的访问控制都涉及两个实体。主体(subject)是发出访问资源请求的用户或进程。访问意味着可读取一个资源或在其中写入数据。客体(object)是用户或进程想要访问的资源。记住，主体和客体由某些特定的访问请求决定；因此在不同的访问请求中，相同的资源即可能是主体也可能是客体。

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 是第一个请求的客体并且是第二个请求的主体：

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 且 B 信任 C，那么 A 通过传递属性继承 C 的信任。这与代数式类似：如果 $a = b$ ，并且 $b = c$ ，那么 $a = c$ 。在上例中，当 A 向 B 请求数据时，B 向 C 请求数据，A 收到的数据本质上是从 C 来的，信任传递是一个严重的安全问题，因为它可能绕过 A 和 C 之间的约束或限制，尤其是当 A 和 C 都支持与 B 交互的时候。例如，组织为提高员工的工作效率，禁止访问 Facebook 或 YouTube。因此，员工(A)无法访问某些互联网站点(C)。但是，如果员工能访问 Web 代理、虚拟专用网络(VPN)或匿名服务，就可以通过这些手段绕过本地网络限制。也就是说，如果员工(A)正在访问 VPN 服务(B)，并且 VPN 服务(B)可访问被屏蔽的互联网服务(C)，A 就能利用信任传递漏洞通过 B 来访问 C。

8.1.2 封闭系统和开放系统

可以根据两种不同的理念设计和构建系统：封闭系统的设计使其只能与很少的系统协作，通常都是来自同一制造商。封闭系统的标准一般是专有的，通常不会公开。另一方面，开放系统使用公认的行业标准设计。开放系统很容易与来自支持相同标准的不同厂商的系统进行集成。

封闭系统很难与相异的系统集成，但是它们更安全。封闭系统通常由不符合行业标准的专用硬件和软件组成。缺少易集成性意味着很多针对通用系统组件的攻击，要么不起作用，要么必须定制才能攻击成功。很多时候，攻击封闭系统比攻击开放系统更难。很多具有已知漏洞的软件和硬件组件在封闭系统中可能根本不存在。除了封闭系统中不存在有漏洞的组件之外，通常只有深入了解特定目标系统，才能对其发动一次成功的攻击。

开放系统通常更容易与其他开放系统集成。例如，使用 Microsoft Windows Server 计算机、Linux 计算机和 Macintosh 计算机创建局域网(LAN)很容易。虽然这三台计算机使用不同的操作系统而且可代表多达三种不同的硬件架构，但每种架构都支持行业标准，所以可轻松实现联网或其他通信。但这种便利是有代价的。因为这三个开放系统都包含标准的通信组件，所以有更多可预见的入口点和发动攻击的方法。一般来说，开放系统的开放性使它们更容易受到攻击，并且它们的广泛存在使攻击者能找到(甚至实践)大量潜在目标。此外，开放系统比封闭系统更受欢迎，并引起更多关注。掌握基本攻击技能的攻击者会在开放系统上找到比封闭系统上更多的目标。潜在目标的“市场”更大，通常意味着更强调瞄准开放系统。与封闭系统相比，在如何攻击开放系统方面，攻击者无疑拥有更多的共享经验和知识。

开源与闭源

记住开源(Open Source)和闭源(Closed Source)系统之间的区别也很有用。开源解决方案是源代码和其他内部逻辑都向公众公开的解决方案。闭源解决方案是源代码和其他内部逻辑对公众隐藏的解决方案。开源解决方案通常依赖于公众检查和审查，随着时间的推移改进产品。闭源解决方案更依赖供应商/程序员随着时间推移改进产品。开源和闭源解决方案都可供出售或免费提供，但商用一词通常意味着闭源。但是，闭源系统的源代码一般是通过供应商妥协或反编译得到。前者通常违反道德甚至法律，而后者则是道德的逆向工程或系统分析的标准要素。

也存在这样的情况。闭源程序可以是开放系统或封闭系统，开源程序也可以是开放系统或封闭系统。

8.1.3 用于确保保密性、完整性和可用性的技术

为保证数据的保密性、完整性和可用性，必须确保所有能访问数据的组件都是安全的且行为端正。软件设计者使用不同的技术来确保程序只能执行所需的操作。假设一个程序写入和读取另一个程序正在使用的内存区域。第一个程序可能会违反所有三个安全原则：保密性、完整性和可用性。如果受影响的程序正在处理敏感或机密数据，则该数据的保密性将无法得到保证。如果以不可预测的方式覆盖或更改该数据(当多个读取器和写入器无意中访问相同的共享数据时常见的问题)，则无法保证其完整性。而且，如果数据修改导致损坏或彻底丢失，则可能数据将来也无法使用。虽然下面讨论的概念都与软件程序有关，但它们也常用于所有安全领域。例如，物理限制可确保对硬件的所有物理访问都会受到控制。

1. 限制(Confinement)

软件设计者使用“进程限制”来约束程序的行为。简而言之，进程限制使进程只能对某些内存位置和资源进行读取和写入，这也被称为沙箱。操作系统或某些其他安全组件不允许非法的读/写请求。如果进程尝试执行超出其授权的操作，该操作将被拒绝。此外，还会采取类似记录违规尝试的后续措施。那些必须遵守更高安全评级的系统通常会记录所有违规行为并以某种明确方式做出响应。通常会终止违规进程的运行。限制可在操作系统本身实现(例如通过进程隔离和内存保护)，通过使用限制应用程序或服务(如 www.sandboxie.com 上的 Sandboxie)实现，或通过虚拟化或虚拟机方案(如 VMware 或 Oracle 的 VirtualBox)实现。

2. 界限(Bound)

在系统上运行的每个进程都有授权级别。授权级别告知操作系统进程可执行什么操作。在简单系统中，可能只有两种授权级别：用户和内核。授权级别告知操作系统如何设置进程的界限。进程的界限由对其可以访问的内存地址和资源所设置的限制组成。界限规定了限制和包含进程的区域。在大多数系统中，这些界限划分出每个进程使用的内存逻辑区域。操作系统负责强制执行这些逻辑界限并禁止其他进程访问。更安全的系统可能需要物理上限制进程。物理界限要求每个受限进程的运行内存与其他受限进程的运行内存物理上(而不仅是逻辑上)隔离。物理上限定内存可能非常昂贵，但它比逻辑边界更安全。

3. 隔离(Isolation)

当通过执行访问界限来限制进程时，该进程将以隔离状态运行。进程隔离可确保隔离状态进程的任何行为仅影响与其关联的内存和资源。隔离用来保护操作环境、操作系统(OS)的内核以及其他独立应用程序。隔离是一个稳定的操作系统的重要组成部分。隔离能阻止一个应用访问另一个应用的内存或资源，不论是善意还是恶意的访问。操作系统可以提供中间服务，例如剪切和粘贴以及资源共享(像键盘、网络接口和存储设备访问)。

限制、界限和隔离这三个概念使得设计安全程序和操作系统变得更困难，但它们也使实现更安全的系统成为可能。

8.1.4 控制

为确保系统的安全性，主体只能访问经过授权的客体。控制使用访问规则(Control)来限制主体对客体的访问。访问规则声明了每个主体可以合法访问的客体。此外，一个客体可能对某一类别访问合法的，但对另一类别访问却是非法的。文件访问控制是一种常见控制。为防止文件被修改，可设置大多数用户的权限为只读，而只对已授权修改文件的少数用户设置读写权限。

有两种访问控制，分别称为强制访问控制(Mandatory Access Control, MAC)和自主访问控制(Discretionary Access Control, DAC)；有关访问控制的深入讨论，请参见第 14 章。在强制访问控制中，是否许可一个访问由主体和客体的静态属性来决定。每个主体都拥有属性，用来定义其访问资源的许可或授权。每个客体拥有属性，用来定义其分类。不同类型的安全方法用不同的方式对资源进行分类。例如，如果安全系统可以找到一条规则，允许一个具有 A 的许可级别的主体访问一个具有 B 的分类的客体，则主体 A 被授予对客体 B 的访问权。

自主访问控制与强制访问控制的不同之处在于，主体具有一些定义要访问的客体的能力。在一定范围内，自主访问控制允许主体根据需要定义要访问的客体列表。这些访问控制列表是主体可修改的动态访问规则集。对于修改的约束通常与主体的身份相关。基于主体身份，可以允许主体添加或修改对客体的访问规则。

强制访问控制和自主访问控制都限制主体对客体的访问。访问控制的主要目标是，通过阻止已授权或未授权的主体的未授权访问，确保数据的保密性和完整性。

8.1.5 信任与保证

为了生产出可靠的安全产品，在设计和架构阶段之前以及进行期间，必须集成适当的安全原则、控制和机制。安全问题不应该在事后才加以考虑，这会导致疏忽、成本增加以及可靠性降低。一旦将安全性集成到设计中，就必须对其进行设计、实现、测试、审核、评估、认证并最终获得认可。

“可信系统”(trusted system)指所有保护机制协同工作的系统，为许多类型的用户处理敏感数据，同时维护稳定和安全的计算环境。“保证”(Assurance)简单地定义为满足安全需求的可信程度。保证需要持续地维护、更新以及重新验证。当可信系统经历了已知的变化或者时间已经过了很久，更应该如此。在任何一种情况下，变化都已经在某种级别上发生。变化往往是安全的对立面，它经常会降低安全性。因此，无论何时发生变化，都需要重新评估系统，以验证其

先前提供的安全级别是否仍然完好无缺，保证因系统而异，必须针对单独的系统建立。但是，有些保证的等级或级别可以适用于很多相同类型的系统，支持相同服务的系统或者部署在同一地理位置的系统。因此，信任可通过实现特定的安全功能构建到系统中，而保证是在真实情况下对这些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，模型提供了一种形式化安全策略的方法。这些模型可以是抽象的或直观的（有些是明确的数学模型），但所有模型都旨在提供一组明确规则，计算机可遵循这些规则来实现构成安全策略的基本安全概念、过程和程序。这些模型提供了一种方式，可加深你对如何设计和开发支持特定安全策略的计算机操作系统的理解。

安全模型为设计人员提供一种将抽象陈述映射到安全策略的方法，该策略规定了构建硬件和软件所需的算法和数据结构。因此，安全模型为软件设计人员提供了一些衡量其设计和实现的标准。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，开发人员可确保他们的安全实现能支持安全策略。

令牌、能力和标签

有几种不同的方法来描述客体必要的安全属性。安全令牌(Token)是与资源关联的独立客体，它描述资源的安全属性。在请求访问实际客体之前，令牌可传达关于客体的安全信息。在其他实现中，使用各种列表存储关于多个客体的安全信息。能力(Capability)列表为每个受控客体维护一行安全属性信息。尽管不像令牌方式那样灵活，但是能力列表能在主体请求访问客体时提供更快的查找。安全标签(Label)是第三种常见的属性存储类型，通常是其所附加客体的永久部分。安全标签设置后，通常无法更改。这种持久性提供了另一种防止篡改的保护措施，无论是令牌还是能力列表都没有提供。

你将在以下部分中学习几种安全模型；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上安全性：

- 可信计算基
- 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 模型
- Biba 模型
- Clark-Wilson 模型
- Brewer and Nash 模型
- Goguen-Meseguer 模型
- Sutherland 模型
- Graham-Denning 模型

尽管没有一个系统可以做到绝对安全，但可以设计和构建适度安全的系统。实际上，如果一个安全系统符合一组特定的安全标准，则可以说它具有一定的信任级别。因此，可将信任构建到系统中，然后进行评估、认证和认可。但在讨论各种安全模型前，我们必须建立一个构建大多数安全模型的基础。这个基础就是可信计算基(Trusted Computing Base, TCB)。

8.2.1 可信计算基

TCSEC(Trusted Computer System Evaluation Criteria, 可信计算机系统评估标准)是美国国防部的一个较早的标准，俗称橘皮书(美国国防部标准 5200.28，稍后的“彩虹系列”一节将详细介绍)，该标准将可信计算基(Trusted Computing Base, TCB)描述为硬件、软件和控件的组合，它们协同工作构成执行安全策略的可信根基。TCB 是完整信息系统的子集。它应尽可能小，以对其详细分析，从而合理地确保系统符合设计规范和要求。TCB 是系统中唯一可信任的部分，其遵守并执行安全策略。系统中的每个组件未必都是可信的。但从安全角度考虑系统时，应该对构成系统 TCB 的所有可信组件进行评估。

通常，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 组件通常会限制 TCB 外部组件的活动。TCB 组件的职责是确保系统在所有情况下都能正常运行，在所有情况下都遵守安全策略。

1. 安全边界

系统的安全边界(Security Perimeter)是一个假想的边界，将 TCB 与系统的其余部分分开(图 8.1)。该边界确保 TCB 与计算机系统的其余元件之间不会发生不安全的通信或交互。TCB 要想与系统的其余部分进行通信，必须创建安全通道，也称为可信路径。可信路径是使用严格标准建立的通道，在不将 TCB 暴露于安全漏洞的情况下允许进行必要的通信。可信路径还可以保护系统用户(有时称为主体)免受因 TCB 交换而导致的影响。当你在本章后面了解有关正式安全准则和评估标准的更多信息后，还将了解到，在寻求为其用户提供高级别安全性的系统中需要可信路径。根据 TCSEC 指南，高信任级别系统(如 TCSEC B2 级或更高级别的系统)需要可信路径。

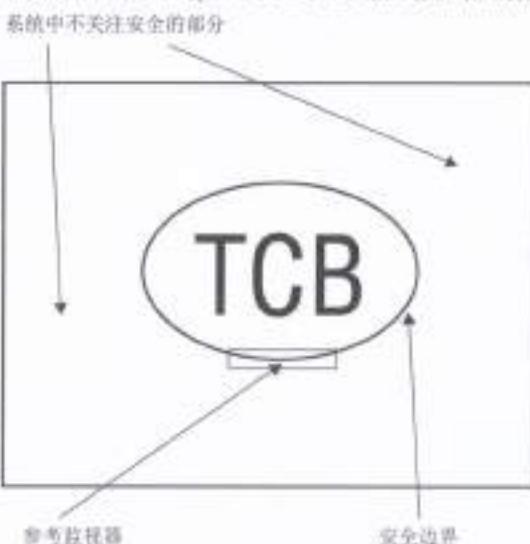


图 8.1 TCB、安全边界和参考监视器

2. 参考监视器和内核

当实现安全系统时，必须开发 TCB 的某些部分以对系统资产和资源(有时称为客体)实施访问控制。TCB 中负责在授权访问请求之前验证资源的部分称为参考监视器(图 8.1)。参考监视器位于每个主体和客体之间，在允许任何请求继续之前，验证请求主体的凭据是否满足客体的访问要求。如果不满足此类访问要求，则拒绝访问请求。实际上，参考监视器是 TCB 的访问控制执行者。因此，已授权、安全的行动和活动才允许发生，而未授权、不安全的活动和行动会被拒绝且被阻止发生。参考监视器根据所设计的安全模型执行访问控制或授权，无论是自主的、强制的、基于角色的还是某种其他形式的访问控制。参考监视器可以是 TCB 中的概念性部分；它不必是一个实际的、单独的或独立工作的系统组件。

TCB 中用于实现参考监视器功能的组件集合称为安全内核。参考监视器是通过在软件和硬件中实现安全内核而付诸实践的概念或理论。安全内核的目标是启动适当的组件以执行参考监视器功能并抵御所有已知攻击。安全内核使用可信路径与主体进行通信。它还决定所有对资源的访问请求，仅允许那些与系统中使用的适当访问规则相匹配的请求。

参考监视器需要有关其保护的每个资源的描述性信息。此类信息通常包括其分类和名称。当主体请求访问客体时，参考监视器会查询客体的描述性信息，以确定应该允许还是拒绝访问(有关其工作原理的更多信息，请参阅边栏“令牌、能力和标签”).

8.2.2 状态机模型

状态机模型描述了一个系统，它无论处于什么状态总是安全的。它基于有限状态机(Finite State Machine, FSM)的计算机科学定义。FSM 将外部输入与内部机器状态相结合，为各种复杂系统建模，包括解析器、解码器和解释器。给定一个输入和一个状态，FSM 会转换到另一个状态并可能产生一个输出。从数学角度看，下一个状态是当前状态和输入的函数；即，下一个状态= $F(\text{输入}, \text{当前状态})$ 。同样，输出也是输入和当前状态的函数；即，输出= $F(\text{输入}, \text{当前状态})$ 。

许多安全模型都基于安全状态概念。根据状态机模型，状态是特定时刻系统的快照。如果一个状态的所有方面都符合安全策略的要求，那么该状态就是安全的。接受输入或产生输出时都会发生转换。一个转换总会产生新状态(也称为状态转换)。必须评估所有状态转换。如果每个可能的状态转换都转换到另一个安全状态，则该系统可称为安全状态机。安全状态机模型系统始终引导进入安全状态，在所有转换中保持安全状态，并允许主体仅以符合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

信息流模型侧重于信息流。信息流模型基于状态机模型。Bell-LaPadula 和 Biba 模型(本章后面将详细讨论)，它们都是信息流模型。Bell-LaPadula 模型关注的是防止信息从高安全级别流向较低安全级别。Biba 模型关注的是防止信息从较低安全级别流向高安全级别。信息流模型不一定只处理信息流的方向，还可处理流动的类型。

信息流模型旨在防止未经授权、不安全或受限制的信息流，通常在不同的安全级别之间(这

些通常被称为多级模型)。信息可在相同分类级别的主体和客体之间传递，也可在不同分类级别的主体和客体之间传递。信息流模型允许所有已授权信息流，无论是在相同的分类级别内还是在分类级别之间。信息流模型防止所有未经授权的信息流，无论是在同一分类级别还是在分类级别之间。

关于信息流模型的另一个有趣的方面是：信息流模型可以用于建立同一对象不同时间点的两个版本或状态之间的关系。因此，信息流指示对象从一个时间点的一个状态到另一个时间点的另一个状态的转换。信息流模型还可以通过明确排除所有非定义流动路径来解决隐蔽通道问题。

8.2.4 非干扰模型

非干扰模型大致基于信息流模型。然而，非干扰模型并非关注信息流，而是关注较高安全级别的主体的动作如何影响系统状态或较低安全级别的主体的动作。基本上，主体 A(高级别)的行为不应影响主体 B(低级别)的行为，甚至不应引起主体 B 的注意。非干扰模型真正关注的是防止处在高安全分类水平的主体的行为影响处于较低安全分类水平的系统状态。如果发生这种情况，主体 B 可能处于不安全状态，或者可能会推断出有关更高级别分类的信息。这是一种信息泄露，并且暗中创建了隐蔽通道。因此，使用非干扰模型可以提供一种保护形式，防止诸如特洛伊木马的恶意程序造成的损害。



真实场景

组合理论

属于信息流类别的其他一些模型建立在多个系统之间的输入和输出如何相互关联的概念之上，其依据是信息如何在系统之间而不是在单个系统内流动。这些被称为组合理论，因为它们解释了一个系统的输出如何与另一个系统的输入相关。有三种公认的组合理论类型：

- 级联(Cascading)：一个系统的输入来自另一个系统的输出。
- 反馈(Feedback)：一个系统向另一个系统提供输入，该系统通过颠倒这些角色进行互动(即系统 A 首先为系统 B 提供输入，然后系统 B 向系统 A 提供输入)。
- 连接(Hookup)：一个系统将输入发送到另一个系统，但也将输入发送到外部实体。

8.2.5 Take-Grant 模型

Take-Grant 模型使用有向图(图 8.2)来规定如何将权限从一个主体传递到另一个主体或从主体传递到客体。简单地说，具有“授予”权限的主体可将他们拥有的任何其他权限授予另一个主体或另一个客体。同样，具有“获取”权限的主体可从另一个主体获取权限。除了这两个主要规则外，Take-Grant 模型可采用创建规则和删除规则来生成或删除权限。此模型的关键是使用这些规则可以让你了解系统中的权限何时可能更改以及可能发生泄露(即无意的权限分配)的位置。

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
删除规则	允许主体删除其拥有的权限

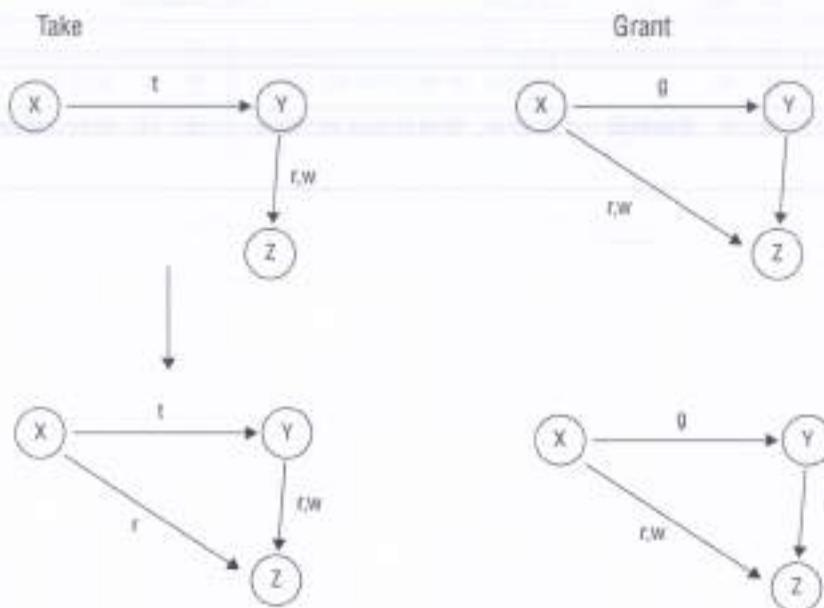


图 8.2 Take-Grant 模型的有向图

8.2.6 访问控制矩阵

访问控制矩阵是主体和客体的表，其指示每个主体可对每个客体执行的动作或功能。矩阵的每列是访问控制列表(ACL)。矩阵的每一行都是一个能力列表。ACL 与客体绑定，它列出了每个主体可执行的有效操作。能力列表与主体相关联，它列出可对每个客体执行的有效操作。从管理角度看，仅使用能力列表进行访问控制是一项管理噩梦。访问控制的能力列表方法可通过在每个主体上存储主体对每个客体具有的权限列表来完成。这有效地为每个用户提供了关键的访问环和安全域中对象的权限。要删除对特定客体的访问权限，必须单独操作每个有权访问它的用户(主体)。因此，管理每个用户账户的访问权限比管理每个客体的访问权限要困难得多。

实现访问控制矩阵模型通常涉及以下内容：

- 构建可以创建和管理主体和客体列表的环境。
- 编写一个函数，它的输入可以是任何类型的对象，函数可以返回与此对象相关的类型(这很重要，因为客体的类型决定了可对它应用哪种操作)。

表 8.1 所示的访问控制矩阵用于自主访问控制系统。可简单地通过使用分类或角色替换主体名称来构建强制型或基于规则的矩阵。系统使用访问控制矩阵来快速确定主体对客体所请求的动作是否被授权。

表 8.1 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

美国国防部(DoD)在 20 世纪 70 年代开发了 Bell-LaPadula 模型，以解决保护机密信息的问题。国防部管理多级分类资源，Bell-LaPadula 多级模型源自国防部的多级安全策略。国防部使用的分类很多，但是，CISSP CBK 内的分类讨论通常仅限于：未分类、敏感但未分类、机密(confidential)、秘密(secret)和绝密(top secret)。多级安全策略规定，具有任何级别许可的主体可以访问其许可级别或以下级别的资源。但在较高许可级别内，仅在“知其所需”(need-to-know)的基础上授予访问权限。换句话说，仅当特定工作任务需要这种访问时，才授予对特定客体的分类级别的访问权限。例如，任何具有秘密安全许可的人都可访问秘密、机密、敏感但未分类和未分类的文档，但不能访问绝密文档。此外，为访问秘密级别的文档，试图访问的人还必须对文档具有“知其所需”权限。

设计上，Bell-LaPadula 模型可防止机密信息泄露或转移到较低的安全许可级别。这是通过阻止较低分类的主体访问较高级别的客体来实现的。利用这些限制，Bell-LaPadula 模型专注于维护客体的保密性。因此，在 Bell-LaPadula 模型中解决了确保文档保密性所涉及的复杂问题。但是，Bell-LaPadula 没有解决客体的完整性或可用性方面的问题。Bell-LaPadula 也是多级安全策略中的第一个数学模型。



真实场景

基于格子的访问控制

第 13 章将介绍这种非自主访问控制的通用类别。这里是一个关于此主题的更详细信息的快速预览(它是大多数访问控制安全模型的基础)：基于格子(lattice)的访问控制中的主体被分配了一个在格子中的位置。这些位置介于已定义的安全标签或分类级别之间。根据主体在格子中的位置定义的标签或分类，主体只能访问落在最低上限(高于其格子位置的最近安全标签或分类)与标签的最高下限(低于其格子位置的最近安全标签或分类)之间的客体。因此，某商业方案中分类级别由低至高分别为公开(public)、敏感、私有(private)、专有(proprietary)和机密，位于私有和敏感标签之间的主体只能访问公开和敏感数据，而不能访问私有、专有或机密数据。基于格子的访问控制也是信息流模型的通用类别，主要解决保密性问题(这是与 Bell-LaPadula 关联的原因)。

Bell-LaPadula 模型建立在状态机概念和信息流模型之上，还采用了强制访问控制和格子概念。格子层级是组织安全策略使用的分类级别。状态机支持多个状态，可明确在任何两个状态之间转换；使用这个概念是因为可在数学上证明机器的正确性和文件保密性的保证。这个状态机有三个基本属性：

- 简单安全属性(Simple Security Property)规定主体不能读取较高敏感度级别的信息(不准向上读)。
- *安全属性(* Security Property)规定主体不能将信息写入位于较低敏感度级别的客体(不准向下写)，这也称为限制属性(Confinement Property)。
- 自由安全属性(Discretionary Security Property)规定系统使用访问矩阵执行自主访问控制。

前两个属性定义了系统可以转换到的状态，不允许其他状态转换。所有可通过这两个规则访问到的状态都是安全状态。因此，基于 Bell-LaPadula 模型的系统可提供状态机模型的安全性(见图 8.3)。

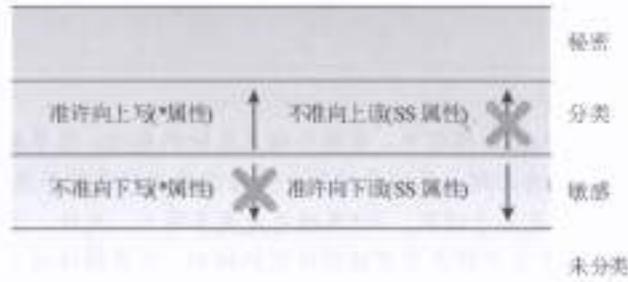


图 8.3 Bell-LaPadula 模型

Bell-LaPadula 属性适用于保护数据保密性。主体不能读取分类级别高于其级别的客体。由于一个级别客体的数据比低级别客体中的数据更敏感或保密，因此主体(非受信任主体)不能将数据从一个级别写入较低级别的客体中。该操作类似于将绝密备忘录粘贴到未分类的文档文件中。第三个属性实现了主体具有“知其所需”权限才能访问客体的规则。

注意：



Bell-LaPadula 模型中的一个例外是“受信任的主体”不受*安全属性的约束。受信任主体的定义是“主体保证即使可能，也不会违反安全规则传输信息”。这意味着允许受信任的主体违反*安全属性执行向下写操作，当对有效的客体执行降级或重新分级时，需要此机制。

Bell-LaPadula 模型仅解决数据的保密性问题，但没有涉及数据的完整性和可用性。因为它是在 20 世纪 70 年代设计的，所以它不支持目前常见的许多操作，例如文件共享和网络连接。它还假设安全层之间的转换是安全的，并且没有解决隐蔽通道问题(第 9 章中介绍)。Bell-LaPadula 模型确实很好地处理了保密性问题，因此它经常与提供处理完整性和可用性机制的其他模型结合使用。

8.2.8 Biba 模型

对于一些非军事组织而言，完整性比保密性更重要。出于这种需求，开发了几种以完整性为重点的安全模型，例如由 Biba 和 Clark-Wilson 开发的模型。Biba 模型是在 Bell-LaPadula 模型之后设计的。Bell-LaPadula 模型解决的是保密性问题，Biba 模型解决的是完整性问题。Biba 模型也建立在状态机概念上，基于信息流，是一个多级别模型。实际上，Biba 模型看起来与 Bell-LaPadula 模型非常相似，除了方向相反之外。两者都使用状态和转换，都有基本属性。两个模型最大的不同在于主要的关注点：Biba 模型主要保护数据完整性。以下是 Biba 模型状态机的基本属性或公理：

- 简单完整性属性(Simple Integrity Property)规定主体不能读取较低完整性级别的客体(不准向下读)。
- *完整性属性(* Integrity Property)规定主体不能修改更高完整性级别的对象(不准向上写)。



注意：

在 Biba 和 Bell-LaPadula 模型中，有两个相互反转的属性：简单属性和*属性。但是，它们也可能被标记为公理、原则或规则。你应该关注的是简单属性和*属性的标识。注意，简单属性总是关于读取，而*属性总是关于写入。此外，这两种情况下，简单属性和*属性都是定义不能或不应该做什么的规则。大多数情况下，未被阻止或禁止的操作就是受支持或允许的。

图 8.4 说明了这些 Biba 模型公理。

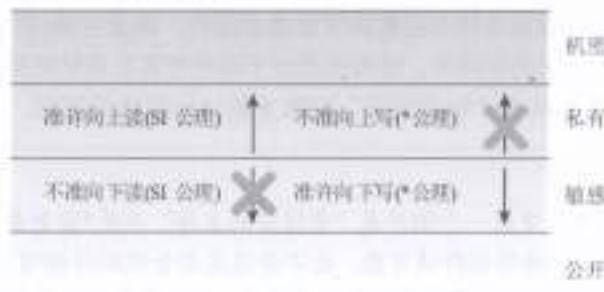


图 8.4 Biba 模型

比较 Biba 模型与 Bell-LaPadula 模型时，会发现它们看起来像是对立的。那是因为他们专注于不同的安全领域。Bell-LaPadula 模型确保数据的保密性，而 Biba 模型则确保数据完整性。

Biba 模型旨在解决三个完整性问题：

- 防止未授权的主体修改客体。
- 防止授权主体对客体进行未经授权的修改。
- 保护内部和外部客体的一致性。

与 Bell-LaPadula 模型一样，Biba 模型要求所有主体和客体都有分类标签，因此，数据完整性保护依赖于数据分类。

看一下 Biba 模型的属性。Biba 模型的第二个属性非常简单。主体不能对处于更高的完整性级别的客体进行写操作。这很有意义。第一个属性怎么样？为什么主体不能读取处于较低完整性级别的对象？回答这个问题需要一点思考。将完整性级别视为空气的纯度级别。你不希望将吸烟区的空气引入环境清新的房间。这同样适用于数据。当完整性很重要时。你不希望将未经验证的数据读入已验证的文档中。数据污染的可能性太大，因此不允许此类访问。

有一些对 Biba 模型的批评，揭示出以下缺点：

- 它仅解决了完整性问题，没解决保密性或可用性问题。
- 重点是保护客体免受外部威胁；它假定内部威胁以程序化方式处理。
- 它没有涉及访问控制管理，也没有提供方法来分配或更改客体或主体的分类级别。
- 它不能阻止隐蔽通道。

由于 Biba 模型侧重于数据完整性，因此与 Bell-LaPadula 模型相比，Biba 模型更多应用于商业安全模型。一些商业组织更关注其数据的完整性而不是保密性。更注重完整性而非保密性的商业组织可能会选择实施 Biba 模型，但大多数组织需要在保密性和完整性之间取得平衡，导致他们实施的解决方案比任何单一模型都复杂。

8.2.9 Clark-Wilson 模型

尽管 Biba 模型在商业应用中发挥了作用，但在 1987 年专门针对商业环境设计出另一种模型。Clark-Wilson 模型采用多方面的措施来实施数据完整性。Clark-Wilson 模型没有定义正式的状态机，而是定义每个数据项目且仅允许通过某一小组程序进行修改。

Clark-Wilson 模型不需要使用格子结构；相反，它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/事务/客体)的三部分关系。主体无法直接访问客体。客体只能通过程序访问。通过使用两个原则：标准格式的事务和职责分离，Clark-Wilson 模型提供了保护完整性的有效手段。

标准格式的事务采用程序的形式。主体只能通过使用程序、接口或访问门户来访问客体(图 8.5)。每个程序对客体(例如数据库或其他资源)可以做什么和不能做什么都有特定限制。这有效地限制了主体的能力，称为约束接口。如果程序设计合理，则这种三元组关系就能提供保护客体完整性的方法。



图 8.5 Clark-Wilson 模型

Clark-Wilson 模型定义了以下数据项和程序：

- 受约束数据项(Constrained Data Item, CDI)是完整性受到安全模型保护的任何数据项。
- 无约束数据项(Unconstrained Data Item, UDI)是不受安全模型控制的任何数据项。任何输入但未验证的数据或任何输出，将被视为无约束数据项。

- 完整性验证过程(Integrity Verification Procedure, IVP)是扫描数据项并确认其完整性的过程。
- 转换过程(Transformation Procedures, TP)是唯一允许修改 CDI 的过程。通过 TP 限制对 CDI 的访问构成了 Clark-Wilson 完整性模型的支柱。

Clark-Wilson 模型使用安全标签来授予客体的访问权限。但仅限于通过转换过程和受限制的接口模型。受限制的接口模型使用基于分类的限制来仅仅提供特定主体的授权信息和功能。处于一个分类级别的一个主体将只能看到一组数据并可访问一组功能，而处于另一个不同分类级别的主体将看到不同数据并可访问另一组功能。为向不同级别或分类的用户提供不同的功能，可向所有用户显示所有功能但是禁用未授权给特定用户的那些功能，或者仅显示授予特定用户的那些功能。通过这些机制，Clark-Wilson 模型可确保数据不会被任何用户未经授权而更改。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商业应用的通用模型。

8.2.10 Brewer and Nash 模型

创建 Brewer and Nash 模型是为了允许访问控制可以基于用户先前的活动而动态改变(这使其成为一种状态机模型)。该模型适用于单个集成的数据库，它试图创建对利益冲突概念敏感的安全域(例如，如果 A 和 B 这两个公司互相竞争，那么在 C 公司工作且有权访问 A 公司专有数据的人不应该被允许访问 B 公司的类似数据)。该模型创建了一类数据，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。打个比方，这会在任何有冲突类别中的信息周围建立一道墙。因此，对于每个冲突类，该模型还使用数据隔离原则，这样用户可远离潜在的利益冲突情况(例如，公司数据集的管理)。由于公司关系一直在变化，因此动态更新冲突类的成员和定义非常重要。

研究或考虑 Brewer 和 Nash 模型的另一种方式是：管理员根据其所分配的工作职责和工作任务，对系统中的大量数据拥有完全的访问控制。但在对任何数据项执行操作时，管理员对任何冲突数据项的访问将暂时被阻止。在操作期间，只能访问与初始数据项相关的数据项。任务完成后，管理员的权限将恢复为完全控制。

8.2.11 Goguen-Meseguer 模型

Goguen-Meseguer 模型是一个完整性模型，但不像 Biba 和其模型那样有名。事实上，这个模型被认为是非干涉概念理论的基础。通常当某人提到非干涉模型时，他们实际上是指 Goguen-Meseguer 模型。

Goguen-Meseguer 模型基于预先确定集合或域(主体可访问的客体列表)。该模型基于自动化理论和域隔离。这意味着仅允许主体对预定客体执行预定动作。当相似的用户被分组到他们自己的域(即集合)时，一个主体域的成员不能干扰另一个主体域的成员。因此，主体不能干扰彼此的活动。

8.2.12 Sutherland 模型

Sutherland 模型是一个完整性模型。它侧重于防止干扰以支持完整性。它正式地基于状态机模型和信息流模型。但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、初始状态以及状态转换的思想。通过仅使用这些预定的安全状态来保持完整性并且阻止干扰。

使用 Sutherland 模型的一个常见例子是：防止隐蔽通道被用来影响过程或活动的结果。有关隐蔽通道的讨论，请参阅第 9 章。

8.2.13 Graham-Denning 模型

Graham-Denning 模型专注于主体和客体的安全创建与删除。Graham-Denning 是八个主要保护规则或操作的集合，用于定义某些安全操作的边界：

- 安全地创建客体。
- 安全地创建主体。
- 安全地删除客体。
- 安全地删除主体。
- 安全地提供读取访问权限。
- 安全地提供授权访问权限。
- 安全地提供删除访问权限。
- 安全地提供传输访问权限。

通常，主体的针对一组客体的特定能力或权限定义在访问矩阵(也称为访问控制矩阵)中。

8.3 基于系统安全需求选择控制措施

为了某些类型的业务应用而购买信息系统的用户(如国家安全机构)的敏感信息可能非常有价值(或在坏人手中非常危险)；中央银行或证券交易商的某些数据可能价值数十亿美元。这些买家希望了解信息系统的安全优势和弱点，通常只愿意考虑那些事先经过正式评估并已获得某种安全评级的系统。买家想要知道他们购买的系统安全性怎么样，一般需要采取哪些措施来保证这些系统尽可能安全。

在进行正式评估时，系统通常需要经过两个步骤：

- (1) 对系统进行测试和技术评估，以确保系统的安全功能符合其预期使用的标准。
- (2) 系统应对其设计和安全标准及其实际能力和性能进行正式比较，负责此类系统安全性和准确性的人员必须决定是接受它们还是拒绝它们，还是对标准进行一些修改，然后再试一次。
- (3) 通常会聘请可信的第三方来执行此类评估。这种测试最重要的结果是他们的“批准印章”(即系统符合所有基本标准)。

注意：

你应该知道 TCSEC 已经被废除并被通用标准(以及许多其他国防部指令)取代。这里仍然包含它，是把它作为历史参考和静态评估标准的示例。与动态(尽管主观)评估标准对比以发现动态评估标准的优点。记住，CISSP 考试侧重于“为什么安全”而不是“怎么做到安全”，换句话说，它关注概念和理论而不是技术和实现。因此，一些这样的历史信息可能出现在考题中。

无论评估是在组织内部进行的还是在组织外部进行的，采购系统的组织都必须决定接受还是拒绝所建议的系统。是否接受系统和何时接受系统，是组织的管理层必须承担的正式责任，并要承担与采购系统的部署和使用相关的任何风险。

这里将探讨的三个主要评估模型或分类标准模型是：TCSEC、ITSEC 和通用准则(CC)。

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面临着采用和使用信息系统所面临的风险。这导致出现了一系列历史性的信息安全标准，这些标准试图为各种使用类别规定最低可接受的安全标准。这些类别很重要，因为购买者希望获得和部署能够保护和保存其内容的系统，或者满足各种强制性安全要求的系统(例如，承包商与政府开展业务时必须满足一些例行要求)。因为美国国防部(DoD)致力于为其购买和使用的系统开发和实施安全标准，第一套这样的标准导致在 20 世纪 80 年代创建了可信计算机系统评估标准(TCSEC)。紧接着，到 20 世纪 90 年代中期，完成了整个系列标准的出版。由于这些出版物通常通过其封面的颜色来识别，因此它们统称为彩虹系列。

紧随美国国防部的脚步，其他政府或标准机构也制定了计算机安全标准，这些标准建立在彩虹系列元素基础之上并对其进行了改进。这些标准中的一个重要的欧洲模型称为信息技术安全评估标准(ITSEC)，该标准于 1990 年开发并一直使用到 1998 年。最终，TCSEC 和 ITSEC 被所谓的通用准则(Common Criteria, CC)所取代，1998 年美国、加拿大、法国、德国和英国采用了该标准，它被更正式地称为“IT 安全领域通用准则认证认可协议”。ITSEC 和通用准则将在后续章节中讨论。

当政府或其他有安全意识的机构评估信息系统时，他们会使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，因为其封面颜色，通常称之为橘皮书。TCSEC 建立了从安全角度评估独立的计算机时使用的指导原则。这些指导原则涉及基本的安全功能，使评估人员可对系统功能和可信度进行度量和评级。实际上，在 TCSEC 中功能和安全保证是组合在一起的，而不像以后开发的安全标准那样将二者分开。TCSEC 指导原则旨在用于评估供应商产品，也被供应商用来确保它们为新产品构建了所有必要的功能和安全保障。在继续阅读本节的其余部分时，请记住，在 2005 年，TCSEC 已被通用准则(CC)所取代，稍后将对此进行讨论。

接下来将介绍橘皮书本身的一些细节，然后讨论彩虹系列中的其他一些重要元素。

8.3.2 TCSEC 分类和所需功能

TCSEC 融合了功能性和保证，将系统提供的保密性保护等级分为四大类。然后将这些类别进一步细分为用数字标识的其他子类别，例如 C1 和 C2。此外，通过对目标系统评估来指定其 TCSEC 的类别。TCSEC 适用的系统是不联网的独立系统。TCSEC 定义了下列主要类别：

类别 A 已验证保护。最高级别的安全性。

类别 B 强制保护。

类别 C 自主保护。

类别 D 最小保护。用于已被评估但达不到其他类别的要求的系统。

下面的列表包括对类别 A 到 C 的简要讨论，以及表示任何适用的子类别的数字后缀(图 8.6)。

级别标签	要求
D	最小保护
C1	自主保护
C2	受控访问保护
B1	标签化安全
B2	结构化保护
B3	安全域
A1	已验证保护

图 8.6 TCSEC 的级别

自主保护(类别 C1、C2) 自主保护系统提供了基本的访问控制。此类别中的系统确实提供了一些安全控制，但缺乏更复杂和严格的控制，不能满足安全系统的特定需求。C1 和 C2 类别的系统提供了基本的控制，并为系统安装和配置提供了完整的文档。

- 自主保护(C1)** 自主性安全保护系统通过用户 ID 和/或组实现控制访问。尽管存在一些限制对客体访问的控制，但此类别中的系统只能提供较弱的保护。
- 受控访问保护(C2)** 受控访问保护系统比 C1 系统更安全。用户只有经过单独识别后才能访问客体。C2 系统还必须强制执行介质清理。通过执行介质清理，任何介质必须在其他用户重复使用前彻底清理，防止残余数据被查看或使用。此外，必须强制执行严格的登录过程，以限制无效或未授权用户的访问。

强制保护(类别 B1、B2、B3) 强制保护系统比 C 类或 D 类系统提供了更多的安全控制。由于具备更细粒度的控制，因此安全管理员可使用特定的控制，只允许非常有限的主体/客体访问集合。此类系统基于 Bell-LaPadula 模型。强制访问控制基于安全标签。

- 标签化安全(B1)** 标签化安全系统中，每个主体和客体都有一个安全标签。B1 系统通过匹配主体和客体的标签并比较其权限兼容性来授予访问权限。B1 系统为保存已分类数据提供了足够的安全性。
- 结构化保护(B2)** 除了对安全标签的要求(就像在 B1 系统中一样)，B2 系统必须确保不存在隐蔽通道。操作员和管理员职责分离，并且进程也要保持隔离。与 B1 系统相比，B2 系统为已分类数据提供更多安全功能。

- **安全域(B3)** 安全域系统通过进一步增加不相关进程的分离和隔离来提供更安全的功能。它明确地定义管理功能，并与其他用户使用的功能分开。B3 系统的重点转向简单性，以减少未使用或额外代码中的漏洞暴露的风险。在初始引导过程中就必须保证 B3 系统处于安全状态。很难攻破 B3 系统，它为非常敏感或秘密的数据提供了充分的安全控制。

已验证保护(类 A1) 已验证保护系统与 B3 系统中采用的结构和控制类似。不同之处在于开发周期。开发周期的每个阶段都使用正式方法进行控制。在进行下一步之前，每个阶段的设计都需要记录、评估和验证。在开发和部署的所有步骤中都非常关注安全，并且是正式地保证系统强安全性的唯一方法。

已验证设计系统从设计文档开始，该文档说明了最终系统如何满足安全策略。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。功能性至关重要，但保证比在低安全性类别中更重要。A1 系统代表最高级别的安全性，旨在处理绝密数据。从设计到交付和安装，每个步骤都经过记录和验证。

彩虹系列中的其他颜色

总之，美国国防部文档集合中有近 30 个书目，这些书要么是对橘皮书的补充，要么就是对其进一步阐述。尽管颜色并没有什么意义，但它们用于识别本系列中发布的各种标准。



注意：

重要的是要理解：彩虹系列中的大多数书籍现已过时，已被更新的标准、指南和指令所取代。此处提及它们仅供你参考，以帮助你解答考试题目。

本文档集中的其他重要元素包括以下内容：

红皮书 由于橘皮书仅适用于未连接到网络的独立计算机，而即使在 20 世纪 80 年代，网络上使用的系统也很多，因此开发了红皮书以在网络环境中解释阐明 TCSEC。事实上，红皮书的官方标题是“TCSEC 的可信网络解读”，可以认为是对橘皮书应用于网络环境中的一种解释。很快，对于系统购买者和构建者来说，红皮书比橘皮书更有价值、更重要。下面列出红皮书的其他一些功能：

- 保密性和完整性的等级。
- 解决通信完整性问题。
- 解决拒绝服务保护问题。
- 解决危害(即入侵)预防和保护。
- 仅限于标记为“使用单一鉴别的集中式网络”的有限类别的网络。
- 仅使用四个评级：无(None)、C1(最小，Minimum)、C2(一般，Fair)和 B2(好，Good)。

绿皮书 绿皮书或“美国国防部密码管理指南”提供密码创建和管理的指南；对于那些配置和管理可信系统的人来说，绿皮书很重要。

表 8.2 列出了彩虹系列中更完整的书籍清单。有关更多信息以及下载书籍，请参阅彩虹系列网页：

<https://csrc.nist.gov/publications/detail/white-paper/1985/12/26/dod-rainbow-series/final>
<https://fas.org/irp/nsa/rainbow.htm>

表 8.2 彩虹系统的一些元素

出版号	标题	书籍名称
5200.28-STD	DoD 可信计算机系统评估标准	橘皮书
CSC-STD-002-85	DoD 密码管理指南	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 安全注意事项	浅蓝皮书
NCSC-TG-003	理解可信系统中自主访问控制的指南	氤氲皮书
NCSC-TG-004	计算机安全术语表	浅绿皮书
NCSC-TG-005	可信网络解释	红皮书
NCSC-TG-006	理解可信系统中配置管理的指南	琥珀皮书
NCSC-TG-007	理解可信系统中设计文档的指南	紫红皮书
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

考虑到制定 TCSEC 需要的所有时间和精力，很难理解为什么评估标准要不断更新并推出更多高级标准。撇开时间和技术不谈，这主要是因为对 TCSEC 的重要批评，它们有助于解释为什么全球范围内正使用更新的标准：

- 尽管 TCSEC 非常重视控制用户对信息的访问，却不控制授权用户如何处理信息。这在军事和商业应用中都是一个问题。
- 鉴于评估标准起源于美国国防部，TCSEC 完全关注保密性是可理解的，TCSEC 假设控制用户访问数据的方式至关重要，而不关注数据准确性或完整性。这在商业环境中不起作用，在此类环境中，数据准确性和完整性可能比保密性更重要。
- 除评估标准自身强调访问控制外，TCSEC 没有认真解决为完全实施安全策略必须采取的人员、物理和程序的政策问题，也未提供保障措施。另外 TCSEC 并未处理影响系统安全的问题。
- 橘皮书本身并不涉及网络问题(虽然红皮书涉及网络问题，但是在 1987 年后期开发的)。

在某种程度上，这些批评反映出了开发 TCSEC 的美国军方独特的安全关注点。并且，当时广泛使用的流行计算工具和技术(网络在 1985 年刚刚出现)也产生了一定影响。当然，组织内部越来越复杂和全面的安全观也有助于解释 TCSEC 在过程性和政策方面的不足和原因。但 ITSEC 已经在很大程度上被通用准则所取代，下一节将说明 ITSEC 是迈向通用准则过程中所经历的一步。

ITSEC 类别与所需保证和功能

ITSEC 代表了欧洲在制定安全评估标准的初步尝试。它是作为 TCSEC 指南的替代方案而开发的。ITSEC 指南评估系统的功能和保证，每个类别使用不同的评级。这种情况下，系统的功能是对用户的系统效用值的度量。系统的功能评级表明系统执行所有必要的功能与其设计和预期目标的符合程度。保证等级表示系统以一致的方式正常工作的可信程度。

ITSEC 将评估中的系统称为评估目标(Target Of Evaluation, TOE)。所有评级均以两类 TOE

评级表示。ITSEC 使用两个尺度来评估功能和保证。

系统的功能等级从 F-D 到 F-B3 进行评级(没有 F-A1)。系统的保证等级从 E0 到 E6 进行评级。大多数 ITSEC 等级通常与 TCSEC 等级相对应(例如，TCSEC C1 系统对应于 ITSEC F-C1、E1 系统)。有关 TCSEC、ITSEC 和通用准则(CC)等级的比较，请参见表 8.4。



注意：

某些情况下，ITSEC 的 F 等级是用 F1 到 F5 定义的，而不是重用 TCSEC 中的标签。这些替代标记的对应关系是：F1 = F-C1，F2 = F-C2，F3 = F-B1，F4 = F-B2 和 F5 = F-B3。F 等级中 F-D 一般没有编号，但少数情况下使用 F0。这是一个相当荒谬的标签，因为如果没有需要评级的功能，就不需要评级标签。

TCSEC 和 ITSEC 之间的差异很多且各不相同。以下是两个标准之间最重要的一些差异：

- TCSEC 几乎只专注于保密性，而 ITSEC 除了保密性外，还解决了缺少完整性和可用性的问题，从而涵盖了维护完整的信息安全性的三个重要因素。
- ITSEC 不依赖于 TCB 的概念，也不要求在 TCB 中隔离系统的安全组件。
- TCSEC 要求任何已更改的系统都要重新评估——无论是操作系统升级、打补丁还是修复，以及应用程序升级或变更等；与 TCSEC 不同，ITSEC 在发生此类变更后不需要进行新的正式评估，而将其包含在评估目标维护的范畴里。

有关 ITSEC 的更多信息(现在已基本被通用准则取代，通用准则将在下一节介绍)，请参阅以下网站：

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/TISicherheitskriterien/itsec-en_pdf.pdf?blob=publicationFile

<https://www.sogis.org/documents/itsec/itsec-en.pdf>

或者可在此处查看原始的 ITSEC 规范：

<http://www.ssi.gouv.fr/uploads/2015/01/ITSEC-uk.pdf>

8.3.3 通用准则

通用准则(CC)代表了或多或少的全球性努力，涉及 TCSEC 和 ITSEC 参与者以及其他全球参与者。最终，它导致了人们能够购买经过 CC 评估的产品。通用准则定义了测试和确认系统安全功能的各种级别。级别的数字表示执行了哪种类型的测试和确认。然而，很容易看出来，即使最高的 CC 评级也不等同于保证这些系统绝对安全，或者说它们完全没有可利用的漏洞或脆弱点。CC 被设计为一个产品评估模型。

1. 通用准则的认可

除了警告和免责声明之外，1998 年加拿大、法国、德国、英国和美国政府组织的代表签署了“IT 安全领域通用准则认证的认可协议”文件，使 CC 成为一个国际标准。该文件由 ISO 转换为官方标准：ISO 15408，信息技术安全评估标准。CC 指南的目标如下：

- 增加购买者对已评估和已评级的 IT 产品安全性的信心。

- 为消除重复评估(此外，这意味着如果一个国家、机构或验证组织在评定特定系统和配置时遵循 CC，那么其他地方就不必重复此工作)。
- 使安全评估和认证过程更具有效益和效率。
- 确保 IT 产品的评估符合高标准和一致的标准。
- 促进评估，并提高已评估和已评级的 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(也就是系统被信任的程度)。

CC 文档可在 www.niap-cc-evals.org/cc-scheme/ 上找到。访问这个站点可获取有关 CC 指南最新版本的信息，以及有关使用 CC 的指南和其他许多有用的相关信息。

通用准则过程基于两个要素：保护范畴和安全目标。保护范畴(Protection Profile, PP)为要评估的产品(TOE)指定安全要求和保护，这些要求和保护被认为是客户的安全要求或“客户想要的安全”。安全目标(Security Targets, ST)指定了供应商在 TOE 内构建的安全声明。ST 被认为是已实施的安全措施或是供应商的“我将提供的安全”声明。除了提供安全目标外，供应商还可提供其他安全功能包。包是“安全需求”组件的中间分组，既可添加到 TOE 中，也可从 TOE 中删除(就像购买新车时的选项包)。

将 PP 与来自所选供应商的 TOE 中的各种 ST 进行比较。最接近或最匹配的就是客户购买的产品。对于当前可用的系统，客户最初根据已公布或上市的评估保证级别(Evaluation Assurance Level, EAL)选择供应商(有关 EAL 的更多详细信息，请参阅下一节)。使用通用准则选择供应商，允许客户准确地请求他们需要的安全性，而不必使用静态的固定安全级别。通用准则还允许供应商在设计和创建产品时更加灵活。一套明确定义的通用准则支持主观性和多用性，它可以自动适应不断变化的技术和威胁环境。此外，EAL 提供了一种更标准的比较供应商系统的方法(就像旧的 TCSEC 一样)。

2. 通用准则的结构

CC 指南分为如下三个部分：

部分 1 “简介”和“通用模型”描述了用于评估 IT 安全性的一般概念和基础模型，以及指定评估目标涉及的内容。它包含有用的介绍性和解释性材料，适用于那些不熟悉安全评估过程工作或需要帮助以阅读和解释评估结果的人员。

部分 2 “安全功能要求”描述安全审计、通信安全、安全性密码学支持、用户数据保护、身份标识、身份验证、安全管理、TOE 安全功能(TSF)、资源利用、系统访问和可信路径等方面的功能要求。涵盖了 CC 评估过程中预想到的全部安全功能。另加附录(称为附件)以解释每个功能区域。

部分 3 “安全保障”涵盖 TOE 在配置管理、交付和运营、开发、指导文档和生命周期支持以及保证测试和漏洞评估等方面的保证要求。涵盖了 CC 评估过程中预想的全部安全保证检查和保护范畴，以及描述系统设计、检查和测试方式的评估保证级别的信息。

最重要的是，这些不同的 CC 文件中出现的信息(至少值得浏览一遍)通常称为评估保证级别(EAL)。表 8.3 总结了 EAL 1 到 7 有关 EAL 的完整说明，请参阅 <https://www.niap-cc-evals.org/> 上的 CC 文档，并查看部分 3 的最新版本。

表 8.3 CC 评估保证级别

级别	保证级别	说明
EAL1	功能测试	适用于对正确操作有一定可信度要求，但安全威胁不严重的情况。当采取适当谨慎的态度保护个人信息，需要独立的保证时，这个级别最合适。
EAL2	结构测试	适用于交付设计信息和测试结果符合良好商业惯例的情况。当开发人员或用户需要低至中等水平的独立保证安全性时，这个级别很合适。在评估遗留系统时，IT 与此级别密切关联。
EAL3	系统测试并检查	适用于安全工程从设计阶段开始并且在后续过程中没有实质性更改的情况。当开发人员或用户需要中等程度独立地保证安全性时，包括彻底调查 TOE 及其开复，这个级别很合适。
EAL4	系统级设计、测试和评审	适用于使用了严格、积极的安全工程和良好的商业开发实践的情况。这个级别不需要大量的专业知识、技能或资源。它涉及所有 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（包括专业安全工程技术），来进行半正式测试。这适用于开发人员或用户，在计划开发方法以及随后严格开发的过程中，都需要高级别的独立保证安全的情况。
EAL6	半正式验证、设计和测试	在设计、开发和测试的所有阶段使用直接、严格的安全工程技术，来生产优质的 TOE。这适用于需要针对高风险情况的 TOE，其中受保护资产的价值会证明额外成本是合理的。广泛的测试降低了渗透的风险、隐蔽通道的可能性以及易受攻击的脆弱性。
EAL7	正式验证、设计和测试	仅用于最高风险情况或涉及高价值资产的情况。仅限于此类 TOE：密切关注的安全功能需要进行广泛的正式分析和测试。

虽然CC指南非常灵活，足以满足大多数安全需求和要求，但绝非完美。与其他评估标准一样，CC指南并不确保用户对数据的操作方式也是安全的。CC指南也没有解决特定安全范围之外的管理问题。与其他评估标准一样，CC指南不包括现场安全评估——也就是说，它们不涉及与人员、组织实践和过程或物理安全相关的控制。同样，CC指南没有解决对电磁辐射的控制，也没有明确规定对加密算法强度进行评级的标准。尽管如此，CC指南仍然代表了可对系统进行安全评级的一些最佳技术。为结束对安全评估标准的讨论，表8.4总结了如何比较TCSEC、ITSEC和CC的各种评级；从中可以看出，每个标准的评级具有相似但不相同的评估标准。

表 8.4 安全评估标准比较

TCSEC	ITSEC	CC	描述
D	F-D+E0	EAL0, EAL1	最小无保护
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

8.3.4 行业和国际安全实施指南

除了整体的安全访问模型，例如 CC，还有其他许多更具体或更集中的安全标准，用于存储、通信、交易等各个方面。其中有两个标准你应该熟悉，它们就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 是一组提高电子支付交易安全性的要求。这些标准由 PCI 安全标准委员会成员制定。这些成员主要是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、软件设计和其他关键保护措施的要求。有关 PCI DSS 的更多信息，请访问网站 www.pcisecuritystandards.org。

ISO 是由各个国家标准组织的代表组成的全球标准制定组织。ISO 定义了工业和商业设备、软件、协议和管理以及其他标准。它发布了六个主要产品：国际标准、技术报告、技术规范、公开可用规范、技术勘误和指南。ISO 标准在许多行业中被广泛接受，甚至被各国政府采纳为要求或法律。有关 ISO 的更多信息，请访问网站 www.iso.org。

8.3.5 认证和鉴定

需要系统安全的组织需要一种或多种方法来评估系统满足其安全要求的程度。正式的评估过程分为两个阶段，称为认证和鉴定。每个阶段所需的实际步骤取决于组织选择的评估标准。CISSP 考生必须了解每个阶段的需求以及通常用于评估系统的标准。接下来的两节将讨论两个评估阶段，然后介绍评估系统安全性时必须考虑的各种评估标准和注意事项。认证和鉴定流程用于评估应用程序安全性以及操作系统和硬件安全性的有效性。

评估过程提供了一种方法，用来衡量系统与所期望的安全级别的符合程度。由于每个系统的安全级别取决于很多因素，因此在评估期间必须考虑所有这些因素。即使系统一开始被认为安全的，但安装过程、物理环境和一般配置细节也都会对系统真正达到整体安全有所影响。由于配置或安装差异，可能导致两个相同的系统在不同的安全级别进行评估。



提示：

接下来使用的术语“认证”“鉴定”和“维护”是美国国防机构使用的官方术语，你应该熟悉它们。

认证和鉴定是软件和 IT 系统开发过程中的额外步骤，通常美国国防部承包商和其他军事环境中的工作要求这些步骤。美国政府使用的这些术语的官方定义来自于美国国防部指令 5200.40 的附件 2。

1. 认证(Certification)

整个评估过程的第一阶段是认证。认证是对 IT 系统以及为支持鉴定过程而制定的其他保护措施的技术和非技术安全功能的综合评估，从而确定特定设计和实施满足一组特定安全要求的程度。

系统认证是对计算机系统各个部分的技术评估，以评估其与安全标准的一致性。首先，你必须选择评估标准(稍后将介绍标准备选方案)。选择要使用的标准后，你将分析每个系统组件

以确定它是否满足所期望的安全目标。认证分析包括测试系统的硬件、软件和配置。在此阶段评估所有控件，包括管理性的、技术和物理性控制。

评估整个系统后，可对结果进行评估，以确定系统在其当前环境中支持的安全级别。系统环境是认证分析的关键部分，因此其周围环境可能或多或少地影响系统的安全。将安全系统连接到网络的方式可能会改变其安全性。同样，系统周围的物理安全性会影响整体的安全评级。对一个系统进行认证时，你必须考虑所有因素。

评估完所有因素并确定系统的安全级别后，即可完成认证阶段。记住，认证仅对特定环境和配置中的系统有效。任何更改都可能导致认证失效。一旦你为某个特定的配置认证了安全评级，就可以准备系统验收了。管理层通过鉴定流程接受系统的已认证安全配置。

2. 鉴定(Accreditation)

在认证阶段，你测试并记录了特定配置中系统的安全功能。有了这些信息，组织的管理层就会将系统的安全功能与组织的需求进行比较。安全策略必须明确说明安全系统的要求。管理层审核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满足他们的需求，系统就被鉴定了。鉴定是指定审批机构(DAA)正式声明：IT 系统被批准在特定安全模式下使用规定的一套保障措施在可接受的风险水平下运行。一旦鉴定完毕，管理层就可以正式认可评估系统的整体安全性能。



注意：

认证和鉴定似乎是相似，因此理解它们往往是一个挑战。你可能参考的一个观点是：认证通常是对安全性的内部验证，并且只有你的组织信任该验证结果。鉴定通常由第三方测试服务机构执行，并且结果对于信任所涉及的特定测试组织的每个人都是可信的。

认证和鉴定的过程通常是迭代的。在鉴定阶段，经常要求更改配置或增加控件来解决安全问题。请记住，无论何时更改配置，都必须重新验证新配置。同样，你需要在经过特定时间段或进行了任何配置更改后重新认证系统。你的安全策略应指出在什么情况下需要重新认证。合理策略会列出认证的有效时间，并列出哪些更改需要重新启动认证和鉴定流程。

3. 认证和鉴定系统

目前有两种政府标准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，参考 <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/855101p.pdf>)，该标准最近取代了美国国防部信息保障认证和鉴定流程(DIACAP)，而 DIACAP 取代的是美国国防信息技术安全认证和鉴定流程(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)。可参见(<https://www.cnss.gov/CNSS/issuances/Policies.cfm>；向下滚动到 CNSSP 22 链接)。CNSSP 取代了美国国家信息保障认证和鉴定过程(NIACAP)。但是，CISSP 可能涉及现行或者以前的标准。这些过程分为四个阶段：

阶段 1：定义 涉及指派适当的项目人员、任务需求的文档，以及注册、协商和创建系统安全授权协议(SSAA)，用于指导整个认证和鉴定过程。

阶段 2：验证 包括 SSAA 的细化、系统开发活动和认证分析。

阶段 3：确认 包括进一步细化 SSAA，对集成系统进行认证评估、向 DAA 提出建议以及 DAA 的鉴定决定。

阶段 4：鉴定后 包括 SSAA 的维护、系统操作、变更管理和合规性验证。

由美国国家安全局信息系统安全组织管理的 NIACAP 流程概述了可能授予的三种类型的鉴定。这些鉴定类型的定义(来自美国国家安全电信和信息系统安全指令 1000)如下所示：

- 对于系统的鉴定，将评估主要的应用程序或一般支撑系统。
- 对于场所的鉴定，将评估特定的独立位置的应用程序和系统。
- 对于类型的鉴定，将评估分布到多个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(TPM)、接口和容错。仔细评估基础架构的各个方面以确保其充分支撑安全性是非常重要的。如果不了解信息系统的安全功能，就无法对其进行评估，也无法正确地实施它们。

8.4.1 内存保护

内存保护是核心安全组件，在操作系统中必须设计和实现。无论系统中执行哪些程序，都必须执行内存保护，否则可能导致不稳定、侵害完整性、拒绝服务和泄露等结果。内存保护用于防止活动的进程与不是专门指派或分配给它的内存区域进行交互。

将在第 9 章讨论内存保护，相关的主题包括隔离、虚拟内存、分段、内存管理和保护环等。

Meltdown 和 Spectre

在 2017 年底，发现了两个重要的内存错误。这两个漏洞被命名为 Meltdown(熔毁)和 Spectre(幽灵)。这些漏洞源于现代 CPU 用于预测未来指令以优化性能的方法。这使得处理器似乎能够在实际请求之前对要检索或处理的代码做出可靠预测。然而，当预测执行错误时，该过程并未彻底回退(也就是说，并没有把每个不正确的预测步骤都撤销)。这可能导致一些内存中的残余数据处于未受保护的状态。

利用 Meltdown 漏洞，可以允许非特权进程读取私有的系统内核内存中的数据。利用 Spectre 漏洞，可从其他正在运行的应用程序中批量窃取内存中的数据。受两个漏洞或其中之一影响的处理器范围非常广泛。虽然是两个不同漏洞，但它们几乎同时被发现并同时被公开。到本书出版时，可能已发布了补丁，可用于解决现有硬件中的这些问题，未来的处理器自身应具有防止此类攻击的机制。

有关这些问题的详尽讨论，请收听 Security Now 播客，或观看剧集 #645(The Speculation Meltdown)、#646(Inspectre)和#648(Post Spectre?)，网址为 <https://www.grc.com/securitynow.htm>。

8.4.2 虚拟化

虚拟化技术用于在单一主机的内存中运行一个或多个操作系统。这种机制几乎允许任何操作系统在任何硬件上虚拟运行。它还允许多个操作系统在同一硬件上同时工作。常见例子包括 VMware Workstation Pro、VMware vSphere、vSphere Hypervisor、适用于 Mac 的 VMware Fusion、Microsoft Hyper-V、Oracle VirtualBox、XenServer 和适用于 Mac 的 Parallels Desktop。

虚拟化有很多好处，例如能根据需要启动服务器或服务的单个实例、实时可扩展、能运行特定应用程序所需的确切操作系统版本。从用户的角度看，虚拟化服务器和服务与传统的服务器和服务没什么区别。此外，恢复损坏、崩溃或毁坏的虚拟系统通常很快，只需要将虚拟系统的主硬盘驱动器文件替换为干净的备份版本，然后重新启动即可（虚拟化及其相关风险的附加内容将在第 9 章中与云计算一起讨论）。

8.4.3 可信平台模块

可信平台模块(Trusted Platform Module, TPM)既是主板上的加密处理器芯片的规范，也是实现此规范的通用名称。TPM 芯片用于存储和处理加密密钥，用于满足基于硬件支持/实现的硬盘加密系统。通常认为用硬件实现硬盘加密比用纯软件实现更安全。

当使用基于 TPM 的全盘加密技术时，用户/操作员必须向计算机提供密码或物理 USB 令牌设备以进行认证，然后才允许 TPM 芯片将硬盘加密密钥加载到内存。虽然这看起来类似于软件实现，但关键区别在于：如果把硬盘从原始系统中拿走，则无法对其进行解密。只有使用原来的 TPM 芯片才能对密文进行解密和访问。如果使用纯软件加密硬盘，则可将硬盘驱动器安装到其他计算机上，而不会有任何的访问或使用限制。

硬件安全模块(HSM)是一种加密处理器，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以及改进身份验证。HSM 通常是附加的适配器或外围设备，或是 TCP/IP 网络设备。HSM 包括篡改保护以防止滥用，即使攻击者可对其进行物理访问也无计可施。TPM 只是 HSM 的一个例子。

HSM 为大型(2048 位以上)非对称加密计算提供加速解决方案而且提供密钥安全存储库。许多证书颁发机构系统使用 HSM 来存储证书；ATM 和 POS 银行终端通常使用专有的 HSM；硬件 SSL 加速器可包括 HSM 支持；兼容域名系统安全扩展(DNSSEC)的域名系统(DNS)服务器使用 HSM 进行密钥和区域文件存储。

8.4.4 接口

通过在应用程序中实现受约束或受限制的接口，以限制用户根据其权限执行操作或查看内容。拥有完全权限的用户可以访问应用程序的所有功能。权限受限的用户访问则受到限制。

应用程序使用不同的方法约束接口。一种常见方法是在用户无权使用该功能时隐藏该功能。管理员可以通过菜单或右键单击一项来使用命令，但如果普通用户没有权限，则不会显示该命令。有时候，虽然显示命令，但是被变暗或禁用。普通用户可以看到它，却无法使用它。

受约束接口的目的是限制或约束已授权和未授权用户的操作。这种接口的使用是

Clark-Wilson 安全模型的一种实际的实现。

8.4.5 容错

容错是指系统遭受故障后仍然能继续运行的能力。容错通过添加冗余组件实现，如在廉价磁盘冗余阵列(RAID)中添加额外磁盘，或故障转移集群配置中添加额外的服务器。容错是安全设计的基本要素。它也被认为是避免单点故障和实现冗余的部分措施。有关容错、冗余服务器、RAID 和故障转移解决方案的详细信息，请参见第 18 章。

8.5 本章小结

安全系统不是组装起来即可奏效，它们需要通过设计才能支持安全性。必须确保安全的系统根据其支持和实施安全策略的能力来判断是否安全。认证是对计算机系统的有效性进行评估的过程。认证过程是对系统实现其设计目标的能力的技术评估。一旦系统满意地通过了技术评估，组织的管理层就开始正式地接受系统。正式的接受过程就是鉴定。

整个认证和鉴定过程取决于标准评估准则，其中有几个标准是用来评估计算机安全系统的。最早的 TCSEC 是由美国国防部开发的。TCSEC 也称为橘皮书，提供了评估系统安全组件的功能和保证的准则。ITSEC 是 TCSEC 指南的替代品，主要在欧洲国家使用。2005 年，TCSEC 被通用准则(CC)取代。无论你使用哪个标准，评估过程都要包括检查每个安全控制是否符合安全策略。系统强制执行“主体以良好行为访问客体”的策略越好，安全级别就越高。

在设计安全系统时，创建安全模型通常会很有帮助，安全模型表明了系统用来实施安全策略的方法。本章讨论了几种安全模型。Bell-LaPadula 模型仅支持数据保密性。它专为军方设计，满足军事需求。Biba 模型和 Clark-Wilson 模型解决了数据的完整性问题，并以各种不同的方式实现。在为商业应用程序设计安全基础架构时，这些模型通常作为基础的一部分。

对所有这一切的理解最终必须形成一个由预防、检测和纠正控制构成的有效的系统安全实现。这就是为什么必须还要知道访问控制模型及其功能的原因。这些模型包括状态机模型、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。了解访问控制模型及其功能。状态机模型确保访问客体的所有主体实例都是安全的。信息流模型旨在防止未经授权、不安全或受限制的信息流。非干扰模型防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 模型规定了权限如何从一个主体传递到另一个主体或从主体传递到客体。访问控制矩阵是主体和客体组成的表，规定了每个主体可以对每个客体执行的动作或功能。Bell-LaPadula 模型的主体具有一个许可级别，仅能访问具有相应分类级别的客体，这实现了保密性。Biba 模型能够防止安全级别较低的主体对安全级别较高的客体执行写入操作。Clark-Wilson 模型是一种依赖于审计的完整性模型，能

够确保未经授权的主体无法访问客体且已授权用户可以正确地访问客体。Biba 模型和 Clark-Wilson 模型实现了完整性。Goguen-Meseguer 模型和 Sutherland 模型专注于完整性。Graham-Denning 模型专注于安全地创建和删除主体和客体。

了解认证和鉴定的定义。认证是对计算机系统各部分的技术评估，以评估其与安全标准的一致性。鉴定是指定机构正式接受认证配置的过程。

能够描述开放和封闭的系统。开放系统采用行业标准设计，通常易于与其他开放系统集成。封闭系统通常是专有硬件和/或软件。它们的规范通常不会公开，并且通常难以与其他系统集成。

知道什么是限制、界限和隔离。对进程读取或写入某些内存地址进行限制。界限是进程在读取或写入时不能超过的内存地址限制范围。隔离是通过使用内存界限将一个进程进行限制的一种运行模式。

能够从访问控制的角度定义客体和主体。主体是发出访问资源请求的用户或进程。客体是用户或进程想要访问的资源。

了解安全控制的工作原理及功能。安全控件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(CC)的类别。TCSEC 的类别包括已验证保护、强制保护、自主保护和最小保护。表 8.4 涵盖并比较了 TCSEC、ITSEC 和 CC 的等效和适用的评级(记住，ITSEC 中从 F7 到 F10 的功能评级在 TCSEC 中没有相应的评级)。

定义可信计算基(TCB)。TCB 是硬件、软件和控件的组合，它们构成了一个执行安全策略的可信基础。

能够解释安全边界。安全边界是将 TCB 与系统其余部分分开的假想边界。TCB 组件使用可信路径与非 TCB 组件通信。

了解参考监视器和安全内核。参考监视器是 TCB 的逻辑部分，用于在授予访问权限之前确认主体是否有权使用资源。安全内核是实现参考监视器功能的 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

- (1) 说出至少 7 个安全模型。
- (2) 描述 TCB 的主要组件。
- (3) Bell-LaPadula 模型的两个主要的规则或原则是什么？Biba 模型的两条规则是什么？
- (4) 开放系统和封闭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. 正式接受所声明的系统配置。
 - B. 对计算机系统的每个部分进行技术评估，以评估其是否符合安全标准。
 - C. 对制造商每个硬件和软件组件的目标进行功能评估，以满足集成标准。
 - D. 制造商的证书，说明所有组件都已正确安装和配置。

2. 系统鉴定是什么?
 - A. 正式接受所声明的系统配置。
 - B. 对制造商每个硬件和软件组件的目标进行功能评估，以满足集成标准。
 - C. 接受证明计算机系统实施安全策略的测试结果。
 - D. 指定机器之间安全通信的过程。
3. 封闭系统是什么?
 - A. 围绕着不可更改的或封闭标准设计的系统。
 - B. 包括行业标准的系统。
 - C. 使用未公开协议的专有系统。
 - D. 任何没有运行 Windows 的机器。
4. 以下哪项更好地描述了受限制或受约束的进程?
 - A. 仅可以运行有限时间的进程。
 - B. 仅可以在一天中某些时间运行的进程。
 - C. 仅可以访问某些内存位置的进程。
 - D. 控制对客体进行访问的进程。
5. 访问客体是什么?
 - A. 用户或进程想要访问的资源。
 - B. 想要访问资源的用户或进程。
 - C. 有效访问规则的列表。
 - D. 有效访问类型的序列。
6. 安全控制是什么?
 - A. 用于存储描述对象的属性的安全组件。
 - B. 列出所有数据分级类型的文档。
 - C. 有效访问规则的列表。
 - D. 限制访问客体的机制。
7. 对于特定的、独立位置的应用和系统进行的评估，是哪类信息系统安全鉴定?
 - A. 系统鉴定
 - B. 现场鉴定
 - C. 应用鉴定
 - D. 类型鉴定
8. TCSEC 标准定义了几种主要类别?
 - A. 2
 - B. 3
 - C. 4
 - D. 5
9. 可信计算基(TCB)是什么?
 - A. 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、软件和控制组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？(选择所有正确答案)
- A. 系统周围物理安全区域的边界。
 - B. 将 TCB 与系统其余部分隔离的假想边界。
 - C. 防火墙所在的网络。
 - D. 与计算机系统的任何连接。
11. 在授予所请求的访问权限之前，TCB 概念的哪个部分验证了对每个资源的访问？
- A. TCB 分区
 - B. 可信库
 - C. 参考监视器
 - D. 安全内核
12. 安全模型的最佳定义是什么？
- A. 安全模型声明组织必须遵循的策略。
 - B. 安全模型提供实现安全策略的框架。
 - C. 安全模型是对计算机系统的每个部分的技术评估，以评估其与安全标准的一致性。
 - D. 安全模型是正式接受已认证配置的过程。
13. 下列哪个安全模型建立在状态机模型之上？
- A. Bell-LaPadula 模型和 Take-Grant 模型。
 - B. Biba 模型和 Clark-Wilson 模型。
 - C. Clark-Wilson 模型和 Bell-LaPadula 模型。
 - D. Bell-LaPadula 模型和 Biba 模型。
14. 下列哪个安全模型解决数据保密性问题？
- A. Bell-LaPadula 模型
 - B. Biba 模型
 - C. Clark-Wilson 模型
 - D. Brewer and Nash 模型
15. Bell-LaPadula 模型中什么属性阻止较低级别的主体访问较高安全级别的客体？
- A. (*)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 Bell-LaPadula 模型的*(星)安全属性，以对低级别客体执行写操作时，可能发生哪些有效的操作？
- A. 扰动
 - B. 多实例

C. 聚合

D. 降级

18. 什么安全方法、机制或模型显示主体对多个客体的能力列表？

A. 职责分离

B. 访问控制矩阵

C. Biba 模型

D. Clark-Wilson 模型

19. 什么安全模型理论上有一个名称或标签的功能，但在解决方案中实现时，会采用安全内核的名称或标签？

A. Graham-Denning 模型

B. Deployment 模式

C. 可信计算基

D. Brewer and Nash

20. 以下哪项不是 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

安全漏洞、威胁和对策

本章涵盖的 CISSP 认证考试主题包括：

✓ 域 3：安全架构和工程

- 3.5 评估和缓解安全架构、设计和解决方案要素的漏洞
 - 3.5.1 基于客户端的系统
 - 3.5.2 基于服务端的系统
 - 3.5.3 数据库系统
 - 3.5.5 工业控制系统(ICS)
 - 3.5.6 基于云的系统
 - 3.5.7 分布式系统
 - 3.5.8 物联网(IoT)
- 3.6 评估和缓解基于 Web 系统的漏洞
- 3.7 评估和缓解移动系统的漏洞
- 3.8 评估和缓解嵌入式系统的漏洞

前几章介绍了基本的安全原则以及为防止违反这些原则而采取的保护机制，还研究了一些寻求绕过这些保护机制的恶意个人使用的特定类型的攻击。至此，在讨论预防措施时，我们关注的是策略措施和系统上运行的软件。但安全专业人员还必须特别关注系统本身，并确保其更高级别的保护控制不是建立在不可靠的基础上。毕竟，如果运行的计算机具有基本的安全漏洞，允许恶意个人轻易地绕过防火墙，那么世界上最安全的防火墙配置也将无济于事。

本章将简要描述“计算机体系结构”领域计算机各种组件的物理设计，分析潜在的安全问题。将从安全角度检查计算系统的每个主要物理组件——硬件和固件。显然，由于资源和时间的限制，很难对系统硬件组件进行详细分析。但所有安全专业人员在遇到深层次的系统设计级别的安全事件时，应至少对这些概念有基本的了解。

安全工程领域处理了广泛的关注点和问题，包括安全设计元素、安全架构、漏洞、威胁和相关的对策。该领域的其他元素在第 6~8 章和第 10 章中讨论。请务必学习所有这些章节，以全面了解该领域的主题。

9.1 评估和缓解安全漏洞

计算机体系结构是一门工程学科，在逻辑层面关注计算系统的设计和构造。许多学院级别的计算机工程和计算机科学课程，很难在一个学期课程内涵盖计算机体系结构的所有基本原理，因此对于本科生，这些课程通常需要两个学期学完。计算机体系结构课程在“比特”(bit)级别深入研究中央处理单元(CPU)组件、内存设备、设备通信以及类似主题的设计，为只做简单的“0或1”运算的各个逻辑设备定义处理路径。大多数安全专业人员不需要如此深的知识水平，这远超出本书和 CISSP 考试范围。但如果你将参与此级别计算系统的安全性方面的设计工作，建议你对该领域进行更深入的研究。

对计算机体系结构的初步讨论，乍看似乎与 CISSP 无关，但大多数安全体系结构和设计元素都基于对计算机硬件扎实的理解和实践。



提示：

系统越复杂，它提供的保证就越少。更多的复杂性意味着存在更多有漏洞的区域以及需要保护更多区域免受威胁。更多漏洞和威胁意味着系统后续提供的安全性不太可靠。

9.1.1 硬件

任何计算专业人员都熟悉硬件的概念。与建筑行业一样，硬件是构成计算机的物理“原料”。术语“硬件”包含计算机中可以实际触摸到的任何有形部分，从键盘和显示器到其 CPU、存储介质和内存芯片。请注意，虽然存储设备(如硬盘或闪存)的物理部分可能被视为硬件，但这些设备中的内容——由“0”和“1”的集合构成的软件以及存储其中的数据——不属于硬件。毕竟，你无法进入计算机内部抓出来一些比特(bits)和字节(bytes)！

1. 处理器

中央处理单元(Central Processing Unit，CPU)通常称为处理器或微处理器，是计算机的神经中枢，是控制所有主要操作的芯片(或多处理器系统中的芯片)，直接执行或协调复杂的计算工作，从而使计算机执行其预期任务。令人惊讶的是，尽管 CPU 允许计算机执行非常复杂的任务，但 CPU 本身却只能执行一组有限的计算和逻辑操作。操作系统和编译器负责将用高级编程语言设计的软件转换为 CPU 能理解的简单汇编语言指令。这种功能范围的限制是有意而为之的，它可使 CPU 以超快的速度执行计算和逻辑操作。



注意：

要了解多年来计算技术进步的程度，请参阅介绍摩尔定律的文章：
http://en.wikipedia.org/wiki/Moore's_law

2. 执行类型(Execution Types)

随着计算机处理能力的提高，用户需要更高级的功能，以使这些系统能够以更高的速率处

理信息并能同时管理多个功能。计算机工程师设计了如下几种方法来满足这些要求。



提示：

乍一看，术语“多任务”“多核”“多处理”“多程序”和“多线程”看起来几乎相同。然而，它们却描述了非常不同的方法来解决“同时做两件事”的难题。我们强烈建议你花时间研究这些术语之间的区别，直到你觉得已经理解为止。

多任务 过去，大多数系统并不是真正的多任务处理，它们依靠操作系统来模拟多任务处理，方法是仔细地构造发送到 CPU 执行的命令序列。当处理器在以几千兆赫兹的速度工作而嗡嗡作响时，很难说它是在任务之间切换还是在同时处理两个任务。单核多任务系统能在任意给定时间处理多个任务或进程。

多核 今天，大多数 CPU 都有多个内核。这意味着以前单独的 CPU 或微处理器芯片，现在是一个可能包含两个、四个、八个或几十个可以同时运行的独立执行内核的芯片。

多处理 在多处理环境中，多处理器计算系统(即具有多个 CPU 的系统)利用多个处理器的处理能力来完成多线程应用程序的执行。例如，一个数据库服务器可能在包含四个、六个或更多处理器的系统上运行。如果数据库应用程序同时接收到许多条单独的查询命令，它可能会将每个查询命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，最常见的多处理系统有两种类型，即 SMP 和 MPP。刚才描述的场景，其中一台计算机包含多个处理器，这些处理器被同等对待并由单个操作系统控制。这被称为对称多处理(Symmetric Multiprocessing, SMP)。在 SMP 中，处理器不仅共享通用操作系统，还共享通用数据总线和内存资源。在这类设计中，系统可使用大量处理器。幸运的是，这类计算能力足以驱动大多数系统。

某些计算密集型操作，例如那些支持科学家和数学家研究的计算操作，需要比单个操作系统更强大的处理能力。大规模并行处理(Massively Parallel Processing, MPP)技术最适合执行这种类型的操作。MPP 系统容纳数百甚至数千个处理器，每个处理器都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安排它们进行处理的软件遇到计算密集型任务时，会将任务的责任指派给单个处理器。该处理器随后将任务分解为可管理的部分，并将它们分发给其他处理器执行。那些处理器将其结果返回给协调处理器，协调处理器将结果组装并返回给提出请求的应用程序。MPP 系统非常强大(不用说，也非常昂贵！)并且应用于有大量计算或基于计算的研究中。

多处理的两种类型都有独特优点，适用于不同类型的情况。SMP 系统擅长以极高的速率处理简单操作，而 MPP 系统非常适合处理庞大、复杂和计算密集的任务，这些任务适合分解并分配到多个子任务进行处理。

多程序 多程序设计类似于多任务处理。它由操作系统协调，在单个处理器上模拟同时执行两个任务，达到提高操作效率的目的。大多数情况下，多程序设计是一种批处理或序列化多个进程的方法，这样当一个进程因等待外设而停止时，其状态将被保存，并且下一个进程将开始处理。等到批处理中的其他所有进程都有机会执行然后因等待外设而停止时，第一个程序会返回处理。对于任何单个程序，此方法会导致完成任务的显著延迟。但对批处理中的所有进程而言，完成所有任务的总时间缩短了。

多程序设计被认为是一种相对过时的技术，除遗留系统外，目前很少使用。多程序设计和多任务处理有两个主要区别：

- 多程序设计通常在大型系统(如大型机)上使用,而多任务处理则在个人计算机(PC)操作系统(如 Windows 和 Linux)上使用。
- 多任务通常由操作系统协调,而多程序设计需要编写专门的软件,这种软件通过操作系统协调自己的活动和执行。

多线程 多线程允许在单一进程中执行多个并发任务。多任务处理多个任务时占用多个进程;与多任务处理不同,多线程允许多个任务在单一进程中运行。线程是一个独立的指令序列,可与属于同一父进程的其他线程并行执行。多线程通常用于多个活动进程之间频繁上下文切换消耗过多开销且效率降低的应用程序。在多线程中,线程之间的切换产生的开销要小得多,因此效率更高。自 2002 年发布 Xeon 处理器以来,许多英特尔 CPU 都采用了称为超线程的专有多线程技术,该技术能将每个物理内核虚拟化为两个处理器,以便实现任务的并发调度。例如,在现代 Windows 实现中,在单一进程中从一个线程切换到另一个线程所涉及的开销约为 40~50 条指令,而且不需要大量的内存传输。相比之下,从一个进程切换到另一个进程涉及 1000 条或更多条指令,并且需要大量的内存传输。

使用多线程处理的一个很好的例子就在一个字处理程序中同时打开多个文档。这种情况下,实际上并没有运行字处理程序的多个实例,这对系统的要求会很高。相反,每个文档都由这个字处理程序进程中的单独线程来处理,并且在任何给定时刻由字处理程序软件选择它所要处理的线程。

对称多处理系统在操作系统级别使用线程。与刚刚描述的字处理示例一样,操作系统还包含许多线程用来控制分配给它的任务。在单处理器系统中,操作系统(OS)一次向处理器发送一个线程以供执行。SMP 系统向每个可用处理器发送一个线程以便并发执行。

3. 处理类型

许多高安全性的系统控制着分配了不同安全级别的信息的处理工作,例如美国政府将与国防有关的信息指定了分类级别:未分类、敏感、机密、秘密和绝密。设计计算机时必须遵循这种分类,这样它们就不会无意地向未经授权的接收者泄露信息。

计算机架构师和安全策略管理员在处理器级别以两种不同的方式解决了这个问题。一种是通过策略机制,另一种是通过硬件解决方案。下面探讨每个选项:

单一状态 单一状态系统需要使用策略机制来管理不同级别的信息。在这种类型的方案中,安全管理员批准处理器和系统一次只能处理一个安全级别的信息。例如,某个系统可能被标记为仅处理秘密信息。然后,该系统的所有用户必须被批准处理秘密级别的信息。这将使保护系统上正在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身上。

多状态 多状态系统能够实现更高级别的安全性。这些系统经过认证,可使用专门的安全机制同时处理多个安全级别,如下一节“保护机制”中所述。这些机制旨在防止信息跨越不同的安全级别。一个用户可能正在使用多状态系统来处理秘密级别的信息,而另一个用户同时正在处理绝密级别的信息。技术机制防止在两个用户之间交叉处理信息,从而防止跨越安全级别处理信息。

在实际应用中,多状态系统由于实现必要的技术机制的费用高,相对不太普及。实现技术机制的费用有时是合理的;但当你处理非常昂贵的资源(如大规模并行系统)时,获得多个系统的成本,远超过在单个此类系统上实现启用多状态操作所需的额外安全控制的成本。

4. 保护机制

如果计算机没有运行，它就是一堆什么也不干的塑料、硅和金属。当计算机运行时，它管理一个运行时环境，该环境表示操作系统和任何可能处于活动状态的应用程序的组合。当运行时，计算机还能够根据用户的安全权限允许访问文件和其他数据。在该运行时环境中，必须集成安全信息和控件以保护操作系统本身的整体性。管理允许哪些用户访问特定的数据项、授权或拒绝对此类数据请求的操作等。运行中的计算机在运行时实现和处理安全性的方式可以大致描述为保护机制的集合。以下是各种保护机制的描述，例如保护环、操作状态和安全模式。



提示：

由于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非常重要，因此你应该了解这里涉及的所有三种机制——环、操作状态和安全模式——的定义以及它们的行为机制。这些内容非常重要，所以这三种保护机制相关的细节问题都有可能出现在考试中。

保护环 保护环是一个古老却好用的方案。它可以追溯到 Multics 操作系统时代所做的工作。这个实验性的操作系统是在贝尔实验室、麻省理工学院和通用电气公司的合作下于 1963 年至 1969 年间设计和建造的。它在霍尼韦尔(Honeywell)的实施中实现了商业用途。Multics 在计算领域留下了两个影响深远的遗产。首先，它启发了一个更简单、更易于理解的操作系统的创建——称为 Unix(一个关于单词 Multics 的游戏)。其次，它在 OS 设计中引入了保护环的概念。

从安全角度看，保护环将操作系统中的代码和组件(以及应用程序、实用程序或在操作系统控制下运行的其他代码)组织成同心环，如图 9.1 所示。进入圆环内部越深，与占用特定环的代码相关的权限级别就越高。虽然最初的 Multics 实现允许多达七个环(编号为 0 到 6)，但大多数现代操作系统使用四个环的模型(编号为 0 到 3)。

作为最内层的环，环 0 具有最高的特权级别，并且基本上可访问任何资源、文件或内存位置。操作系统中始终驻留在内存中的部分(因此可根据需要随时运行)称为内核。它占用环 0 并可抢占在任何其他环上运行的代码。操作系统的其余部分——作为各种任务请求、执行的操作、进程切换等而进出内存的那些部分占用环 1。环 2 在一定程度上也有特权，是 I/O 驱动程序和系统实用程序驻留的地方；它们能访问应用程序和其他程序本身无法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最外层的环 3。

环模型的本质在于优先级、特权和内存分段。任何想要执行的进程都必须排队等待(挂起的进程队列)。环编号最低的进程总比环编号较高的进程提前运行。较低编号环中的进程与较高编号环中的进程相比可访问更多资源并能更直接地与操作系统交互。在较高编号的环中运行的进程通常必须向较低编号环中的处理程序或驱动程序请求它们所需的服务，这有时称为中介访问模型。在其最严格的实现中，每个环都有自己关联的内存段。因此，来自较高编号环中的进程对较低编号环中的地址的任何请求必须调用与该地址相关联的环中的辅助进程。在实践中，许多现代操作系统仅将内存分为两个段：一个用于系统级访问(环 0 到 2)，通常称为内核模式或特权模式，另一个用于用户级的程序和应用程序(环 3)，通常称为用户模式。

从安全性角度看，环模型使操作系统能够保护和隔离自己，免受用户和应用程序的影响。它还允许在具有高特权的操作系统组件(例如内核)和操作系统的低特权部分(例如操作系统的其他部分，以及驱动程序和实用程序)之间实施严格的边界限制。在此模型中，直接访问特定资源只能在特定环内执行；同样，某些操作(例如进程切换、终止和调度)仅允许在某些环内执行。



图 9.1 在常用的四环模型中，保护环将操作系统分为环 0 到 2 中的内核、组件和驱动程序以及在环 3 上运行的应用程序和其他程序

进程占用的环决定了其对系统资源的访问级别(并决定它必须从较低编号、更高特权环中的进程请求哪种资源)。进程可直接访问对象，只要它们位于进程自己的环内或当前边界之外的某个环中(例如，这意味着环 1 的进程可以直接访问自己环内的资源以及与环 2 和 3 关联的资源，但它不能访问仅与环 0 相关联的任何资源)。中介访问机制即前面提到的驱动程序或处理程序请求的方法通常称为系统调用，且往往涉及调用特定系统或用于将请求传递给内环以进行服务的编程接口。然而，在任何此类请求得到满足之前，被调用环必须检查以确保调用进程具有正确的凭据和授权，从而能访问数据和执行满足请求所涉及的操作。

进程状态 进程状态也称为操作状态，进程状态是进程可能在其中运行的各种执行形式。对操作系统而言，在任何给定时刻它都处于两种模式之一：以特权、完全访问模式运行，称为监督状态；或在与用户模式相关的所谓问题状态下运行。其权限较低并且所有的访问请求在被准许或拒绝之前必须检查授权凭据。后者之所以被称为问题状态，不是因为问题一定会发生，而是因为用户访问的非特权性意味着可能会发生问题，系统必须采取适当的措施来保护安全性、完整性和保密性。

进程在操作系统的处理队列中排队等待执行，当处理器可用时它们将被安排执行。由于许多操作系统允许进程仅以固定增量或块的形式占用处理器时间，因此在进程创建时，它首次进入处理队列；如果一个进程在占用完其整个处理时间(称为时间片)仍未完成的情况下，它将返回到处理队列中等待下一轮继续执行。此外，进程调度程序通常选择最高优先级的进程来执行，因此到达队列的前端并不总能保证对 CPU 的访问(因为进程可能在最后一刻被另一个具有更高优先级的进程抢占)。

根据进程是否正在运行，它可能处于以下几种状态：

就绪状态 在就绪状态下，进程准备在被调度执行时立刻恢复或开始处理。进程在这个状态时如果 CPU 可用，它将直接转换到运行状态；否则，它会处于就绪状态直到 CPU 可用。这意

意味着该进程具有立即开始执行所需的所有内存和其他资源。

等待状态 等待也可以被理解为“等待某种资源”，也就是说，该过程已经准备好继续执行但在它可以继续处理之前需要等待设备或访问请求(某种中断)提供的服务(例如，一个要求从文件中读取记录的数据库应用程序必须等待找到并打开该文件，并找到正确的记录集)。一些参考资料将此状态标记为阻塞状态，因为在某个外部事件发生前，会阻止该进程进一步执行。



提示：

运行状态通常也称为问题状态。但不要将单词“问题”与错误相联系。相反，可以把问题状态看作像解决数学问题以便获得答案一样。但请记住，它被称为问题状态是因为可能会发生问题或错误。就像解决数学问题可能出错一样，问题状态与监督状态隔离，因此任何可能发生的错误都不会轻易影响整个系统的稳定性；它们只影响发生错误的进程。

运行状态 运行中的进程在 CPU 上执行并持续运行，直到完成、时间片到期或者由于某种原因而被阻塞(通常是因为它产生了一个中断来访问设备或网络，并等待该中断提供服务)。如果时间片结束但是进程没有完成，则返回就绪状态并进入队列中排队；如果进程因等待资源可用而阻塞，则进入等待状态并进入队列中排队。

监管状态 当进程必须执行需要大于问题状态特权集的特权操作时，才使用监督状态，包括修改系统配置、安装设备驱动程序或修改安全设置。基本上，在用户模式(环 3)或问题状态中未出现的任何功能都会在监管模式中执行。

停止状态 当进程完成或必须终止时(因为发生错误、需要的资源不可用或者无法满足资源请求)，它将进入停止状态。此时，操作系统将收回分配给该进程的所有内存和其他资源，并根据需要重新分配给其他进程使用。

图 9.2 显示了这些不同状态如何相互关联，新进程总是转换到就绪状态。从那里开始，准备好的进程总是转换到运行状态。在运行时，如果进程完成或终止，进程可以转换到停止状态；如果等待下一个时间片就返回到就绪状态；或转移到等待状态，直到其挂起的资源请求得到满足。当操作系统要决定下一个运行的进程时，它会检查等待队列和就绪队列，并获取最高优先级的作业准备运行(因此，等待的进程中，只有那些请求的资源已得到满足或者准备好服务的作业才会被考虑)。

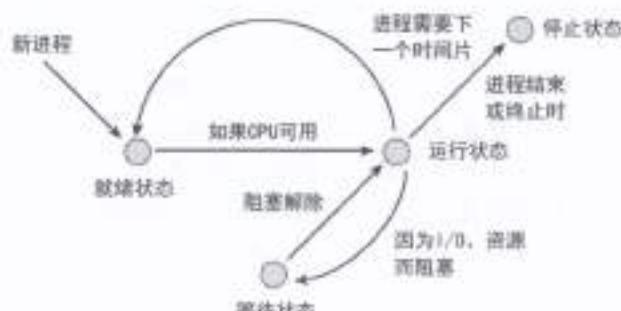


图 9.2 进程调度程序

在图 9.2 中，进程调度程序管理在就绪状态和等待状态下等待执行的进程，并决定当运行

的进程转换到另一个状态(就绪、等待或停止)时将发生什么。

安全模式 美国政府为处理机密信息的系统指定了四种经批准的安全模式。这些将在接下来介绍。在第1章中，我们回顾了美国联邦政府使用的分类系统以及安全许可和访问批准的概念。在这种情况下唯一需要知道的新术语是“知其所需”(need to know)，它是指一种访问授权方案。在该方案中，主体访问客体的权限不仅考虑特权级别，还考虑主体所扮演角色与所涉及数据的相关性(或他们执行的工作)。这表示主体需要访问客体才能正确执行其工作或扮演某些特定角色。那些不需要知道的人，无论他们拥有什么级别的权限，都无法访问该客体。如果你需要回顾这些概念，请在继续学习之前复习第1章中相关知识。在部署安全模式之前，必须存在三个特定元素：

- 分层的强制访问控制(MAC)环境
- 对可以访问计算机控制台的主体的完全物理控制
- 对能进入计算机控制台同一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承包商以外的地方遇到以下模式。但你可能在其他语境中发现这个术语，因此建议你熟记这些术语。

专用模式 专用模式系统基本上等同于本章前面“处理类型”一节描述的单一状态系统。专用系统的用户有下列三个要求：

- 每个用户必须具有允许访问系统处理的所有信息的安全许可。
- 每个用户必须拥有系统处理的所有信息的访问批准。
- 每个用户必须有对系统处理的所有信息具有“知其所需”权限。



注意：

在每种模式的定义中，为简洁起见，我们使用了“系统处理的所有信息”。官方的定义更全面，使用了“处理、存储、传输或访问的所有信息”。如果你想深入研究，请使用互联网搜索引擎查找“Department of Defense 8510.1-M DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Manual”。

系统高级模式 系统高级模式系统的要求略有不同，用户必须满足这些要求：

- 每个用户必须具有允许访问系统处理的所有信息的有效安全许可
- 每个用户必须拥有系统处理的所有信息的访问批准。
- 每个用户必须对系统处理的某些信息具有有效的“知其所需”权限，但不要求对系统处理的所有信息都具有有效的“知其所需”权限。

注意，专用模式和系统高级模式之间的主要区别在于，在系统高级模式中，所有用户不必对计算设备上处理的所有信息都具有“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，但该用户可以访问前者的所有数据，而对后者的一些数据的访问却受到限制。

分隔模式 分隔模式系统进一步弱化了这些要求：

- 每个用户必须具有允许访问系统处理的所有信息的有效安全许可。
- 每个用户必须具有他们在系统上访问的任何信息的访问批准。

- 每个用户必须具有他们将在系统上访问的所有信息的有效的“知其所需”权限。

请注意，分隔模式系统和系统高级模式系统之间的主要区别在于：分隔模式系统的用户不一定具有对系统上所有信息的访问批准。但系统高级模式和专用系统的相同之处在于，系统的所有用户仍必须具有适当的安全许可。在一种称为分隔模式工作站(Compartmented Mode Workstations, CMW)的模式的特殊实现中，具有必要许可的用户可同时处理多个分隔区中的数据。

CMW 要求在客体上设置两种形式的安全标签：敏感度级别和信息标签。敏感度级别描述了必须在什么级别保护客体。敏感度级别在所有四种模式中都很常见。信息标签可防止数据过度分类并将附加信息与对象相关联，这有助于正确和准确地标记与访问控制无关的数据。

多级模式 政府对多级模式系统的定义与上一节中给出的技术定义非常相似。但是，为保持一致性，我们将使用术语“许可”“访问批准”和“知其所需”来表达：

- 某些用户不具有访问系统所处理的全部信息的有效安全许可，因此，通过检查主体的许可级别是否能控制客体的敏感性标签来控制访问。
- 每个用户必须对系统上要访问的所有信息都具有访问批准。
- 每个用户必须对系统上要访问的所有信息都具有一个有效的“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：当从专用系统向下移到多级系统时，控制访问系统的用户类型的管理要求会逐步降低。但这并没有降低限制个人访问的重要性，因此用户只能获得他们有合法权限访问的信息。如上一节所述，只需要将执行这些要求的负担从管理人员(他们采用物理方式限制对计算机的访问)转移到硬件和软件上(它们控制多用户系统中的每个用户可访问哪些信息)。



注意：

多级安全模式也称为受控安全模式。

根据所需的安全许可、“知其所需”权限以及处理来自多个许可级别的数据(Process Data from Multiple Clearance Levels, 缩写为 PDMCL)的能力，表 9.1 总结和比较了这四种安全模式。比较所有四种安全模式时，通常认为多级模式暴露出最高级别的风险。

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

如果所有用户必须具有相同的安全许可，则安全许可为“相同”，否则为“不同”。如果不适用且未使用，或虽然使用“知其所需”，但所有用户对系统上的所有数据都具有“知其所需”权限，则“知其所需”权限为“无”，如果访问受到“知其所需”权限的限制，则“知其所需”权限为“是”。如果使用了 CMW 实现，则 PDMCL 为“是”，否则 PDMCL 为“无”。

5. 操作模式

现代处理器和操作系统旨在支持多用户环境。在多用户环境中，单个计算机用户不会被授予访问系统的所有组件或存储在其上的所有信息的权限。因此，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 CPU 在执行用户应用程序时使用的基本模式。在此模式下，CPU 只允许执行其全部指令集中的部分指令。这样做是为了防止用户由于执行设计不当的代码或无意误用该代码而意外损害系统。它还可保护系统及其数据免受恶意用户的攻击。恶意用户可能尝试执行旨在绕过操作系统采取的安全措施的指令，或者可能错误地执行某些操作导致未授权访问、损害系统或有价值的信息资产。

通常，用户模式内的进程在称为虚拟机(VM)的受控环境中执行。虚拟机是由 OS 创建的模拟环境，为程序执行提供安全有效的运行场所。每个 VM 都与其他所有 VM 隔离，并且每个 VM 都有自己的系统分配的内存地址空间，宿主应用程序可使用它们。特权模式(即内核模式)中的模块负责创建和支持 VM，并防止一个 VM 中的进程干扰其他 VM 中的进程。

特权模式 CPU 还支持特权模式，该模式旨在使操作系统能访问 CPU 支持的所有指令。此模式有许多名称，确切的术语因 CPU 制造商而异。下面列出一些常见名称：

- 特权模式
- 监管模式
- 系统模式
- 内核模式

无论你使用哪个术语，基本概念都是相同的：这种模式给在 CPU 上执行的进程授予了广泛权限。因此，设计合理的操作系统不允许任何用户应用程序在特权模式下执行。出于安全性和系统完整性的目的，只有那些作为操作系统本身组件的进程才能在特权模式下执行。



提示：

不要将处理器模式与任何类型的用户访问权限混淆。高级处理器模式有时称为特权或监管模式，这一事实与用户的角色没有任何关系。所有用户(包括系统管理员)的应用程序都以用户模式运行。当系统管理员使用系统工具更改系统配置时，这些工具也以用户模式运行。当用户应用程序需要执行某个特权操作时，它会使用系统调用将该请求传递给操作系统。操作系统会对请求进行评估，然后拒绝或者批准请求。如果批准，则在用户控制范围外的某个特权模式的进程中执行该请求。

6. 存储器(Memory)

系统中第二个重要的硬件组件是存储器(Memory)，它是计算机用于保存需要随时可用的信息的存储库。有许多不同类型的存储器，每种存储器都适用于不同的目的。我们将在后续章节中详细介绍。

只读存储器

顾名思义，只读存储器(ROM)是可以读取但不能更改的内存(不允许写入)。标准 ROM 芯片的内容在工厂里“烧入”，最终用户根本无法改变它。ROM 芯片通常包含“引导”信息，是计

算机在从磁盘加载操作系统前用于启动的信息。引导信息包括每次启动 PC 时都会运行大家熟悉的开机自检(Power-On Self-Test, POST)系列诊断程序。

ROM 的主要优点是不能被修改。用户或管理员的错误不会意外地清除或修改此类芯片的内容。这个属性使得 ROM 非常适合组织协调计算机中最核心的工作。

有一种类型的 ROM，管理员在某种程度上可修改它。它被称为可编程只读存储器(Programmable Read-Only Memory, PROM)，下面将描述它的几种子类型：

可编程只读存储器 基本的可编程只读存储器(PROM)芯片在功能上类似于 ROM 芯片，但有一个例外。在制造过程中，PROM 芯片的内容不像标准 ROM 芯片那样在工厂“烧入”。相反，PROM 包含特殊功能，允许最终用户稍后烧入芯片的内容。但烧入过程具有类似结果：一旦将数据写入 PROM 芯片，就再也不能更改。烧入后，PROM 芯片的功能基本上和 ROM 芯片一样。

PROM 芯片为软件开发人员提供了在高速定制内存芯片上永久存储信息的机会。PROM 通常用于需要某些定制功能的硬件应用程序，但一旦编程完成就很少改变。

可擦除可编程只读存储器 由于 PROM 芯片较高的成本以及软件开发人员在编写代码后不可避免地需要修改代码，导致人们开发出了可擦除 PROM(EPROM)。EPROM 有两个主要的子类别，即 UVEPROM 和 EEPROM(见下一项内容)。紫外线 EPROM(UVEPROM)可以用光擦除。这些芯片有一个小窗口，当用特殊的紫外光照射时可擦除芯片上的内容。擦除后，最终用户可将新信息烧入 UVEPROM，就像以前它从未写过一样。

电可擦除可编程只读存储器 一个更灵活、更友好的 UVEPROM 替代方案是电子可擦除 PROM(EEPROM)，它使用传递到芯片引脚的电压来强制擦除。

闪存 闪存是 EEPROM 的衍生概念。它是一种非易失性存储介质，可通过电子方式擦除和重写。EEPROM 和闪存的主要区别在于必须完全擦除后 EEPROM 才能重写，而闪存可按块或页擦除和写入。NAND 闪存是最常见的闪存类型。它广泛用于存储卡、优盘、移动设备和 SSD(固态硬盘)。

随机存取存储器

随机存取存储器(Random Access Memory, RAM) 是可读写存储器，包含计算机在处理过程中使用的信息。RAM 仅在持续供电时才能保留其内容。与 ROM 不同，当计算机断电后，RAM 中存储的所有数据都会消失。因此，RAM 仅适用于临时存储。关键数据不应只存储在 RAM 中；备份副本应该始终在另一个存储设备上保存，以防止在突然断电时发生数据丢失。以下是 RAM 的类型：

实际存储器 实际内存(也称为主内存)通常是计算机可用的最大 RAM 存储资源。它通常由许多动态 RAM 芯片组成，因此必须由 CPU 定期刷新(有关此主题的更多信息，请参见边栏“动态 RAM 与静态 RAM”)。

高速缓存 RAM 计算机系统包含许多缓存，当存在重复使用的可能时，这些缓存通过从较慢的设备获取数据将其临时存储在更快的设备中来提高性能，这就是缓存 RAM。处理器通常包含一个板载的超高速缓存，用于保存它即将运行的数据。高速缓存 RAM 可称为 L1、L2、L3 甚至 L4 缓存(L 为级别的缩写)。许多现代 CPU 包括多达三级的片上高速缓存。一些高速缓存(通常为 L1 和/或 L2)专用于单个处理器内核，而 L3 可以是内核之间共享的高速缓存。一些 CPU 涉及 L4 高速缓存，其可能位于主板/母板上或 GPU(图形处理单元)上。同样，实际存储器通常包含存储在磁性介质或 SSD 上的信息的高速缓存。这个存储链继续向下经过内存/存储设备的

层次结构，使计算机能够通过保存接下来可能使用的数据来提高性能(无论是 CPU 指令、数据提取、文件访问还是其他操作)。

许多外围设备也有板载高速缓存，以减少它们给 CPU 和操作系统造成的存储负担。例如，许多高端打印机包含大量 RAM 缓存，因此操作系统可快速将整个作业假脱机打印到打印机。之后，处理器可忘记打印作业；它不必被迫等待打印机实际生成所请求的输出，一次块地给打印机输入数据。打印机可预先处理其板载缓存中的信息，从而释放 CPU 和操作系统以处理其他任务。许多存储设备(如硬盘驱动器(HDD)、固态驱动器(SSD)和某些优盘)都包含缓存，以帮助提高读写速度。但在断开连接或断电前，必须将这些高速缓存存储到永久或二级存储区域，以避免高速缓存中驻留的数据丢失。



真实场景

动态 RAM 与静态 RAM

目前主要有两种类型的 RAM：动态 RAM 和静态 RAM。大多数计算机包含这两种类型 RAM 的组合，并将它们用于不同目的。

为存储数据，动态 RAM 使用一系列电容器，即保持电荷的微小电子设备。这些电容器保持电荷(表示存储器中的比特 1)或不保持电荷(表示比特 0)。但由于电容器会随着时间的推移自然放电，因此 CPU 必须花时间刷新动态 RAM 的内容，以确保比特 1 不会无意中更改为比特 0，从而改变存储器中的内容。

静态 RAM 使用更复杂的技术，一种称为触发器的逻辑设备。对于所有意图和目的而言，它只是一个 ON/OFF 开关，必须从一个位置移到另一个位置才能将比特 0 更改为比特 1，反之亦然。更重要的是，只要不断电，静态存储器就会保持其内容不变，并且不会因定期刷新操作而给 CPU 带来开销。

因为电容器比触发器价格便宜，所以动态 RAM 比静态 RAM 便宜，但静态 RAM 运行速度比动态 RAM 快得多。对系统设计人员来说，这是个性能与价格权衡的问题。他们将静态 RAM 和动态 RAM 模块结合起来使用，在成本与性能之间取得了适当的平衡。

寄存器(Registers)

CPU 还包括数量有限的板载存储器，称为寄存器。它为算术逻辑单元(CPU 的大脑)在执行计算或处理指令时，提供可直接访问的存储位置。实际上，ALU 要操作的任何数据，除非作为指令的一部分直接提供，否则都必须加载到寄存器中。这种类型内存的主要优点是它是 ALU 本身的一部分，因此它以典型的 CPU 速度与 CPU 保持同步。

存储器寻址(Memory Addressing)

使用内存资源时，处理器必须具有一些引用内存中各个位置的方法。该问题的解决方案称为寻址，并在不同情况下存在多种不同的寻址方案。以下是五种较常见的寻址方案：

寄存器寻址 寄存器是直接集成在 CPU 中的较少的存储位置。当 CPU 需要来自某个寄存器的信息进行操作时，它使用寄存器地址(例如，“寄存器 1”)来访问其内容。

立即寻址 立即寻址本身并不是存储器寻址方案，而是一种数据引用方式，其将数据作为指令的一部分提供给 CPU。例如，CPU 可能会处理命令“将寄存器 1 中的值加 2”。这条命令使用两种寻址方案。第一个是立即寻址：告诉 CPU 要添加数字 2 且不需要从内存某种位置检

索该数值，它是作为命令的一部分提供的。第二个是寄存器寻址：告诉 CPU 从寄存器 1 中取得数值。

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提供给 CPU。此地址必须与正在执行的指令位于相同的存储器页面上。直接寻址比立即寻址更灵活，因为存储器位置的内容的修改相对容易，而立即寻址中硬编码的数据需要重新编程才能更改。

间接寻址 间接寻址使用的方案类似于直接寻址。但作为指令的一部分提供给 CPU 的存储器地址并不包含 CPU 用作操作数的实际数值。相反，指令中的内存地址所指内存中包含另一个内存地址(可能位于不同的页面上)。CPU 读取间接地址来确定所需数据驻留的地址，然后从该地址取得实际的操作数。

基址+偏移量寻址 基址+偏移量寻址使用存储在 CPU 的某个寄存器中的数值作为开始计算的基址地址。然后，CPU 将随指令提供的偏移量与该基址相加，并从计算出的内存位置取得操作数。

辅助存储器

“辅助存储器”这个术语通常指磁性、光学或基于闪存的介质，或其他存储设备，包含 CPU 不能直接获得的数据。CPU 为了访问辅助存储器中的数据，必须首先由操作系统读取数据并将其存储在实际内存中。但辅助存储器比主存储器便宜得多，并可用来存储大量信息。这种情况下，硬盘、闪存驱动器和光学介质(像光盘(CD)、数字通用光盘(DVD)、蓝光光盘之类)都可以用作辅助存储器。

虚拟内存是一种特殊类型的辅助内存，由操作系统管理，可使其像真实内存一样。最常见的虚拟内存类型是页面文件，由大多数操作系统作为其内存管理功能的一部分进行管理。这种特殊格式的文件包含先前存储在内存中但最近未使用的数据。当操作系统需要访问存储在页面文件中的地址时，它会检查页面是否驻留在内存中(这种情况下可立即访问)或是否已经被交换到磁盘中，这种情况下它会将数据从磁盘读回到实际内存中(此过程称为分页)。

使用虚拟内存是一种使计算机运行的廉价方式，使计算机运行时好像具有比实际安装的更多的真实内存。它的主要缺点是：在主存储器和辅助存储器之间交换数据时进行的分页操作相对较慢(内存工作在纳秒级、磁盘系统工作在微秒级，通常这意味着差三个数量级!)。并且产生大量的计算机开销，导致整个系统的速度降低。随着更大容量实际物理 RAM 的使用，对虚拟内存的需求正在减少，而且通过使用闪存卡或 SSD 来存储虚拟内存分页文件也可降低虚拟内存的性能损失。

存储器的安全问题

存储设备存储并处理数据，其中一些可能非常敏感。因此，理解各种类型的存储器并了解它们如何存储和保留数据至关重要。任何可能保留敏感数据的存储设备都应在出于某种原因被允许离开你的组织之前，进行清除。这对于辅助存储器和 ROM、PROM、EPROM、EEPROM 设备来说尤其重要，因为这些设备在断电后仍可保留数据。

但存储器数据保持问题不仅限于那些设计用于保留数据的存储器类型。请记住，静态和动态 RAM 芯片是通过使用电容和触发器来存储数据的(参见边栏“动态 RAM 与静态 RAM”)。从技术角度看，断电后这些电子元件在有限时段内仍可能保留一些电量。理论上，技术经验丰富的人可针对这些组件采用电子手段，将设备上存储的部分数据读取出来。不过，这需要大量

的技术专业知识，而且除非你的对手拥有令人难以置信的雄厚资金，否则这不太可能构成威胁。

当系统关闭或 RAM 被拔出主板时，有一种攻击方法会冻结内存芯片以延迟驻留数据的衰减。参见 http://en.wikipedia.org/wiki/Cold_boot_attack。甚至还有一些攻击专注于内存映像转储或系统崩溃转储以提取加密密钥。请参见 www.lostpassword.com/hdd-decryption.htm。

围绕存储器的安全最重要的问题之一是：控制在计算机使用过程中谁可访问存储在存储器中的数据。这主要是操作系统的责任，也是本章前面部分描述的各种处理模式下的主要存储器的安全问题。在本章后面的“基本安全保护机制”一节中，你将学习如何使用进程隔离原则，来确保进程无法读取或写入未分配给它们的存储器空间。如果你在多级安全环境中运行，那么特别需要注意的是：要确保有足够的保护措施来防止安全级别之间发生不必要的存储器内容泄露，泄露可能通过直接访问存储器或隐蔽通道发生(稍后将对隐蔽通道进行详细讨论)。

7. 存储设备(Storage)

下面将讨论的是第三类计算机系统组件：数据存储设备(Storage)。这些设备用于存储计算机在写入后随时可使用的信息。将首先讨论一些与存储设备相关的常用术语，然后研究与数据存储相关的一些安全问题。

主存储设备与辅助存储设备

主存储设备和辅助存储设备的概念可能有些混乱，特别是与主存储器和辅助存储器相比时。有一种简单方法可分清这些概念，其实它们是一样的！主存储器(也称为主存储设备)是计算机用于在运行时保存 CPU 可用的必要信息的 RAM。辅助存储器(或辅助存储设备)包括所有熟悉且每天都使用的长期存储设备。辅助存储器由磁性和光学介质组成，例如硬盘(HDD)、固态硬盘(SSD)、闪存驱动器、磁带、CD、DVD 和闪存卡等。

易失性存储设备与非易失性存储设备

尽管你之前可能没听说过使用“易失性”这个术语来描述存储设备，但我们在讨论存储器时已经熟悉了易失性的概念。存储设备的易失性只是衡量电源关闭时其丢失数据的可能性。断电后，设计用来保留其数据的设备(例如磁性介质)属于非易失性设备，而设计为丢失其数据的设备(例如静态或动态 RAM 模块等)属于易失性设备。回顾上节讨论的内容：复杂的技术有时能够在断电后从易失性存储器中提取数据，因此两者之间的界限有时也不是那么清晰。

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类型的寻址系统从设备内的任何位置立即读取(并且有时写入)数据。几乎所有主存储设备都是随机存取设备。你可使用存储器地址访问存储在 RAM 芯片内任何位置的信息，而不必读取此位置前的物理存储的数据。大多数辅助存储设备也是随机存取设备。例如，硬盘驱动器使用可移动磁头系统，允许你直接移动到磁盘上的任何位置，而不会旋转通过存储在其前面磁道上存储的所有数据；同样，CD 和 DVD 设备使用光学扫描器，可将自己定位在盘片表面的任何位置。

另一方面，顺序存储设备不提供这种灵活性。它们要求在到达所需位置之前读取(或加速经过)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。为存取存储在磁带中间位置的数据，磁带驱动器必须物理地扫描整个磁带(即使它不一定需要处理以快进模式经过的数据)，直到它到达所希望的位置。

显然，顺序存储设备的存取速度比随机存取存储设备慢得多。但此刻你会再次面临成本/收益决策。许多顺序存储设备可在相对便宜的介质上保存大量数据。这个特性使磁带驱动器特别适合与灾难恢复/业务连续性计划相关的备份任务(请参阅第 3 章和第 18 章)。在备份时，你经常需要存储大量数据，而很少需要访问存储的信息。这种情况下只需要使用顺序存储设备就好了！

8. 存储介质的安全

上一节讨论了主存储设备相关的安全问题。关于辅助存储设备的安全性有三个主要问题，这些也映射出了对主存储设备安全的关注：

- 即使在数据被删除后，数据仍可保留在辅助存储设备上。这种情况称为数据残留。大多数精通技术的计算机用户都知道，即使在删除文件后，也可以使用工具软件从磁盘中恢复文件。从技术角度看，也可以从已重新格式化的磁盘中恢复数据。如果确实想要从辅助存储设备中删除数据，则必须使用专门的实用程序来破坏设备上的所有数据痕迹，或破坏或销毁辅助存储设备本身，并使其无法被修复(通常称为净化)。
- 固态硬盘 SSD 在净化方面有一个独特问题。“SSD 耗损均衡”意味着通常存在未标记为“存活”的数据块，当它被关闭复制为“降低磨损水平块”时仍然保留了数据的副本。这意味着传统的零擦除作为 SSD 的数据安全措施是无效的。
- 辅助存储设备还很容易被盗。经济损失不是主要因素(毕竟，备份磁带或硬盘驱动器的成本没多少钱)，但机密信息的丢失会带来很大的风险。如果有人将你的商业机密复制到可移动介质上并带离公司，那么它的价值远高于介质本身的成本。因此，有必要使用全盘加密来降低未经授权的实体访问数据的风险。由于其损耗均衡技术，在将任何数据存储到 SSD 之前对 SSD 进行加密是一种很好的安全措施。这会降低将明文数据存储在休眠块中的可能性。幸运的是，许多 HDD 和 SSD 设备本身都提供加密功能。
- 访问存储在辅助存储设备上的数据，是计算机安全专业人员面临的最重要的问题之一。对于硬盘，通常可通过组合操作系统的访问控制来保护数据。可移动介质带来了更大挑战，通常需要使用加密技术来保护它们。
- 由于可用性也是安全三要素之一，因此必须选择能够在所需时间长度内保留数据的介质。例如，备份磁带可能会在数据保留期终止之前降级。此外，用于辅助存储的技术也可能过时，从而很难恢复/读取使用过时技术存储的数据。

9. 输入和输出设备

输入和输出设备通常被视为基本的原始外围设备，并在它们停止正常工作前通常不会受到太多关注。然而，即使这些基本设备也会给系统带来安全风险。安全专业人员应该意识到这些风险，并确保采取适当的控制措施来降低这些风险。接下来将介绍特定的输入和输出设备带来的一些风险。

显示器

监视器似乎相当安全。毕竟，它们只是显示操作系统提供的数据。关闭它们后，数据会从屏幕上消失而且无法恢复。但一种称为 TEMPEST 的技术可能危害监视器上显示的数据的安全性。通常，阴极射线管(CRT)监视器很容易产生辐射，而液晶显示器(LCD)监视器外泄的程度要

小得多(有些研究声称辐射太低不足以泄露关键数据)。

TEMPEST 是一种技术，可从远处甚至从另一个位置读取每个监视器产生的电子辐射(称为 Van Eck 辐射)，从远处读取电子辐射这个过程称为 Van Eck 入侵。该技术还可用于阻止此类活动。各种实验表明：可使用停靠在街边的货车中的此类设备，轻松地读取办公楼内的显示器屏幕上的内容。遗憾的是，防止 Van Eck 辐射所需的保护控制措施实施起来很昂贵(需要大量的铜！)并且使用起来很麻烦。可以说，任何显示器的最大风险仍然是肩窥或是相机上的长焦镜头。肩窥的概念就是：有人可用眼睛或摄像机看到你屏幕上的内容。记住，肩窥是桌面显示器、笔记本电脑显示器、平板电脑和手机的风险关注点。

打印机

虽然比较简单，但打印机也可能存在安全风险。根据你组织采用的物理安全控制措施，带走打印形式的敏感信息可能比用闪存或磁性介质带走敏感信息要容易得多。如果打印机是共享的，用户可能忘记取走打印出来的敏感信息，因而容易受到窥探。许多现代打印机也在本地存储数据，通常存储在硬盘驱动器上，有些则无限期地保留着打印的副本。打印机通常暴露在网络上以便访问，并且通常没有被设计成一个安全的系统。但是，根据打印机的型号不同，有很多配置设置可用来提供一定级别的合理的安全网络打印服务。这些配置设置包括数据加密传输以及在和打印机交互之前先进行身份验证等。这些都是组织安全策略能很好地解决的问题。

键盘/鼠标

键盘、鼠标和类似的输入设备也不能免受安全漏洞的影响。所有这些设备都容易受到 TEMPEST 技术的监控。此外，键盘容易受到不太复杂的“窃听”的影响。可将一个简单设备放在键盘内或其连接电缆旁边，以拦截所有击键操作并使用无线电信号将它们发送到远程接收器。这与使用 TEMPEST 技术监测具有相同的效果，但可用更便宜的装备完成。此外，如果你的键盘和鼠标是无线的(包括蓝牙)，无线电信号也可能被截获。

调制解调器

随着无处不在的宽带和无线网络的出现，调制解调器正在成为过时且少见的计算机组件。如果你的组织仍在使用旧设备，则调制解调器可能是硬件配置的一部分。用户系统中存在调制解调器通常是安全管理人员最大的困境之一。调制解调器允许用户在网络中创建不受控制的接入点。在最糟糕的情况下，如果配置不当，它们可能产生极其严重的安全漏洞，使外部人员能绕过所有网络边界保护机制并直接访问网络资源。更糟的是，调制解调器创建了一个备用出口通道，内部人员可使用该通道把组织的数据泄露到外部。但请记住，只有当调制解调器可以连接到可操作的固定电话线上时，这个漏洞才能被利用！

除非出于业务原因确实需要调制解调器，否则应该认真考虑在组织的安全策略中彻底禁用调制解调器。在这些情况下，安全管理人员应该知道所有调制解调器在网络中的物理和逻辑位置，确保它们的配置正确，并确保采取适当的保护措施以防止其被非法使用。

9.1.2 固件

固件(Firmware)在某些领域中也称为微码，是用于描述存储在 ROM 芯片中的软件的术语。这种类型的软件很少更改(实际上，如果它存储在真正的 ROM 芯片而不是 EEPROM/EEPROM 上

的话，就永远不会更改了），经常用来驱动计算设备的基本操作。有两种类型的固件：主板上的 BIOS 以及通用的内部和外部设备固件。

1. BIOS 和 UEFI

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，用于启动计算机并从磁盘加载操作系统。BIOS 包含在固件设备中，计算机在引导时会立即访问它。在大多数计算机中，BIOS 存储在 EEPROM 芯片上以便于版本更新。更新 BIOS 的过程称为“刷新 BIOS”。

曾经发生过一些恶意代码被嵌入 BIOS/固件的事件。还有一种称为 phlashing 的攻击，它会安装官方 BIOS 或固件的恶意变体版本，将远程控制或其他恶意功能引入设备。

自 2011 年以来，大多数系统制造商已使用统一可扩展固件接口(Unified Extensible Firmware Interface, UEFI)取代了主板上的传统 BIOS 系统。UEFI 是一种硬件和操作系统之间更高级的接口，它保留了对传统 BIOS 服务的支持。

2. 设备固件

许多硬件设备(例如打印机和调制解调器)也需要一些有限的处理能力来完成其任务，同时最小化操作系统本身的负担。在许多情况下，这些“迷你”操作系统完全包含在它们所在设备上的固件芯片中。与计算机的 BIOS 一样，设备固件也常存储在 EEPROM 设备中，因此可以根据需要进行更新。

9.2 基于客户端的系统

基于客户端的漏洞会使用户及其数据和系统面临攻击和破坏的风险。客户端攻击是任何能够损害客户的攻击。在讨论攻击时，通常假设主要目标是服务器或服务器端组件。客户端或客户端攻击指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示例是恶意网站，它将恶意移动代码(例如 applet)传输到运行在客户端且有漏洞的浏览器上。客户端攻击可发生在任何通信协议上，而不仅是超文本传输协议(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

上面介绍过，代理是从用户系统发送的代码对象，用于查询和处理存储在远程系统上的数据。applet 执行相反的功能，这些代码对象由服务器发送到客户端以便执行某些操作。实际上，applet 实际上是独立的微型程序，这些程序的执行独立于发送它们的服务器。万维网的竞技场正在不断变化。如今 applet 的使用并不像 2010 年初那样普遍。但是，applet 并没有从 Web 上消失，大多数浏览器仍然支持它们(或仍然有支持它们的附加组件)。因此，即使组织在内部或公共 Web 设计中没有使用 applet，你的 Web 浏览器也可能在浏览公共 Web 时遇到它们。

假设有一个 Web 服务器为 Web 用户提供了各种金融工具。其中一个工具可能是抵押计算器，它处理用户的财务信息，并根据贷款的本金和期限以及借款人的信用信息提供每月抵押付款。远程 Web 服务器可向本地系统发送一个 applet，使其自己能执行这些计算，而不是在服务

端处理这些数据并将结果返回给客户端系统。这为远程服务器和最终用户提供了许多好处：

- 处理压力被转移到客户端，释放 Web 服务器上的资源且可以处理更多来自用户的请求。
- 客户端可使用本地资源生成数据，而不必等待远程服务器的响应。许多情况下，这可更快地响应输入数据的更改。
- 在设计合理的 applet 中，Web 服务器不会接收作为输入提供给小程序的任何数据，因此可维护用户财务数据的安全性和隐私性。

然而，就像代理一样，applet 引入了许多安全问题。它们允许远程系统将代码发送到本地系统运行。安全管理员必须采取措施，确保发送到其网络上系统的代码安全并正确地屏蔽恶意活动。此外，除非逐行分析代码，否则最终用户永远无法确定 applet 中是否包含特洛伊木马组件。例如，抵押计算器确实可能在最终用户不知情或准许的情况下将敏感的财务信息发送到 Web 服务器。

下面介绍两个常见的 applet 示例：Java applet 和 ActiveX 控件。

Java applet Java 是由 Sun Microsystems(现在由 Oracle 拥有)开发的独立于平台的编程语言。Java 在很大程度上已经被现代应用程序所取代，并且大多数浏览器不再直接支持它。但是，你仍然应该对 Java 有基本的了解，因为它可能仍在内部使用或在组织实现的特定浏览器中得到支持。虽然现代网页设计已经很少使用 Java，但这并不意味着 Java 已经从互联网上消失了。大多数编程语言都使用编译器来生成定制的应用程序，以便在特定的操作系统下运行。这导致一个应用程序需要使用多个编译器，来为它支持的每个平台都生成一个版本。Java 通过引入 Java 虚拟机(JVM)解决了这个限制。每个运行 Java 代码的系统都会下载其操作系统支持的 JVM 版本。然后，JVM 将 Java 代码转换为该特定系统可执行的代码格式。这种方案的最大优点是代码可以在操作系统之间共享而不必修改。Java applet 是通过 Internet 传输的简短 Java 程序，用于在远程系统上执行各种操作。

在 Java 平台的设计过程中，安全性是最重要的考虑因素，Sun 公司的开发团队创建了“沙箱”概念，对 Java 代码的特权进行限制。沙箱将 Java 代码对象与操作系统的其余部分隔离开来，并对这些对象可以访问的资源实施严格的规则。例如，沙箱会禁止 Java applet 从不是分配给它的内存区域中检索信息，从而阻止 applet 窃取该信息。遗憾的是，虽然沙箱减少了可通过 Java 发起的恶意事件的形式，但仍然存在其他许多已经被广泛利用的漏洞。

ActiveX 控件 ActiveX 控件是微软对 Sun Java applet 的回应产品。它们以与 java applets 类似的方式运行，但可使用多种语言实现，包括 Visual Basic、C、C++ 和 Java。Java applet 和 ActiveX 控件之间有两个主要区别。首先，ActiveX 控件使用 Microsoft 公司专有的技术，因此只能在 Microsoft 公司浏览器的系统上运行。其次，ActiveX 控件不受 Java applet 上的沙箱限制的约束。它们对 Windows 操作环境具有全部的访问权限，并可执行许多特权操作。因此，在决定下载和执行哪些 ActiveX 控件时，必须采取特殊的预防措施。一些安全管理员采取了比较苛刻的态度，禁止从除少数几个受信任站点之外的所有站点中下载任何 ActiveX 内容。

Internet Explorer 11 仍支持 ActiveX，但跟随 Windows 10 发布的 Microsoft 最新浏览器 Edge 不包含对 ActiveX 的支持。这表明微软正逐步淘汰 ActiveX。

9.2.2 本地缓存

本地缓存是临时存储在客户端上以供将来重复使用的任何内容。一个典型的客户端上有许多本地缓存，包括地址解析协议(Address Resolution Protocol, ARP)缓存、域名系统(Domain Name System, DNS)缓存和 Internet 文件缓存。ARP 缓存中毒是由攻击者响应 ARP 广播查询并返回伪造的回复造成的。如果客户端在有效回复之前接收到错误回复，则使用错误回复来填充 ARP 缓存，并将有效回复作为外部公开的查询而丢弃。ARP 缓存的动态内容，无论是中毒还是合法，都将保留在缓存中直到超时(通常不到 10 分钟)。ARP 用于将互联网协议(IP)地址解析为适当的 MAC 地址，以便组成用于数据传输的以太网报头。一旦一个 IP 到 MAC 的映射离开缓存，攻击者就会在客户端重新执行 ARP 广播查询时获得另一个毒害 ARP 缓存的机会。

ARP 缓存中毒的第二种形式是创建静态 ARP 条目。这是通过执行 ARP 命令完成的而且必须在本地执行。但这很容易通过一个脚本来实现，该脚本通过特洛伊木马、缓冲区溢出或社会工程攻击在客户端上执行。静态 ARP 条目是永久性的，即使系统重新启动后也是如此。一旦发生 ARP 中毒，无论是针对永久性条目还是动态条目，从客户端传输的数据流量都将被发送到非预期的系统。这是由于 IP 地址被映射到错误的或不同的硬件地址(即 MAC 地址)造成的。ARP 缓存中毒或只是 ARP 中毒是建立中间人攻击的一种方法。

另一种执行中间人攻击的流行方法是通过 DNS 缓存中毒。与 ARP 缓存类似，一旦客户端收到来自 DNS 的响应，该响应将被缓存以备将来使用。如果可将伪造的信息输入到 DNS 缓存中，那么重定向通信就非常容易。有许多方法可执行 DNS 缓存中毒，包括主机(HOSTS)中毒、授权 DNS 服务器攻击、缓存 DNS 服务器攻击、DNS 查找地址更改以及 DNS 查询欺骗。

HOSTS 文件是静态文件并可在支持 TCP/IP 的系统上找到，其中包含域名及其关联 IP 地址的硬编码索引。HOSTS 文件现在是在基于动态查询的 DNS 系统之前使用的，但它仍可作为后备措施或强制解析的手段。管理员或黑客可向 HOSTS 文件添加内容，以建立 FQDN(完全限定域名)与所选 IP 地址之间的关系。如果攻击者能将伪造的信息存储到 HOSTS 文件中，那么当系统启动时，HOSTS 文件的内容将被读入内存，这些伪造的信息将被优先使用。与动态查询不同，动态查询最终将因超时而从缓存中清除。HOSTS 文件中的条目是永久性的。

授权的 DNS 服务器攻击的目标是改变其原始主机系统(主授权 DNS 服务器)上 FQDN 的主记录。主授权 DNS 服务器托管区域文件或域数据库。如果此原始数据集被更改，则最终这些更改将在整个 Internet 上传播。但是，对授权 DNS 服务器的攻击通常会很快被发现，因此很少会导致大范围的漏洞利用。因此，大多数攻击者都专注于缓存 DNS 服务器。缓存 DNS 服务器是用来缓存来自其他 DNS 服务器的 DNS 信息的任何 DNS 系统。大多数公司和 ISP 为其用户提供缓存 DNS 服务器。缓存 DNS 服务器上托管的内容不会被全球的安全社区所关注，而是由本地运营者维护。因此，对缓存 DNS 服务器的攻击可能会在很长一段时间后才被发现。有关如何攻击缓存 DNS 服务器的详细信息，请参阅 <http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html> 上的“Kaminsky DNS 漏洞的图解说明”。虽然这些攻击都集中在 DNS 服务器上，但它们最终会影响客户端。客户端执行动态 DNS 解析后，从授权 DNS 服务器或缓存 DNS 服务器接收的信息将临时存储到客户端的本地 DNS 缓存中。如果该信息是伪造的，则客户端的 DNS 缓存就中毒了。

DNS 中毒的第四个示例是向客户端发送替换过的 IP 地址作为 DNS 服务器，为客户端提供

解析查询服务。DNS 服务器地址通常通过动态主机控制协议(DHCP)分发给客户端，但也可静态分配。即使 IP 配置信息的所有其他元素都已由 DHCP 分配，仍可在本地轻松地更改静态分配的 DNS 服务器地址。可通过脚本(类似于前面提到的 ARP 攻击)或通过破坏 DHCP 来发起更改客户端的 DNS 服务器查找地址的攻击。一旦客户端使用错误的 DNS 服务器，查询就会发送到黑客控制的 DNS 服务器，服务器将返回中毒的结果。

DNS 中毒的第五个例子是 DNS 查询欺骗。发生这种攻击时，黑客能窃听客户端发送给 DNS 服务器的查询。然后攻击者发回一个包含虚假信息的回复。如果客户端接受虚假回复，则会将该信息放入其本地 DNS 缓存中。当真实回复到达时，它将被丢弃，因为原始查询已经被响应。无论执行这五种 DNS 攻击手段中的哪一种，虚假条目都将写入客户端的本地 DNS 缓存中。因此，所有 IP 通信都将被发送到错误的端点。这样黑客就可以通过操纵该错误端点然后将流量转发到正确的目的地来建立中间人攻击。

关于本地缓存的第三个关注领域是临时 Internet 文件或 Internet 文件缓存。这是从 Internet 网站下载的文件的临时存储，这些文件由客户端实用程序保存，供当前和将来使用。大多数情况下，此缓存包含网站内容，但其他 Internet 服务也可使用文件缓存。各种漏洞利用方法，例如拆分响应攻击，可能导致客户端下载内容并将其存储在缓存中，但这些内容并不是所请求网页中的预期元素。移动代码脚本攻击也可用于在缓存中写入虚假内容。一旦缓存中的文件中毒，即使合法的 Web 文档调用缓存中的内容，也会激活恶意内容。

减轻或解决这些攻击并不总是那么简单或直接。没有一个简单的补丁或更新可以防止利用这些漏洞对客户端进行攻击。这是因为这些攻击利用了内置到各种协议、服务和应用程序中的正常和适当的机制。因此，防范这类攻击不仅要给缺陷打补丁，更要关注攻击的监测和预防。通常作为开始，应使操作系统和应用程序与各自供应商的补丁保持同步。接下来，安装主机入侵检测和网络入侵检测工具来监视这些类型的滥用情况。定期查看 DNS 和 DHCP 系统的日志，以及本地客户端系统日志以及可能的防火墙、交换机和路由器日志，以查找异常或可疑事件的条目。

组织应使用拆分 DNS 系统(也称为水平拆分 DNS、视图拆分 DNS 和脑拆分 DNS)。拆分 DNS 是部署一个供公共使用的 DNS 服务器，另外单独部署一个供内部使用的 DNS 服务器。公共 DNS 服务器上的区域文件中的所有数据都可由公众通过查询或探测访问。但内部 DNS 仅供内部使用。只有内部系统才会被授权与内部 DNS 服务器进行交互。通过阻止传输控制协议(TCP)和用户数据报协议(UDP)的入站端口 53 来禁止外部人员访问内部 DNS 服务器。TCP53 用于区域传输(其中包括大多数 DNS 服务器到 DNS 服务器的通信)，UDP53 用于查询(就是任何向 DNS 服务器发送查询的非 DNS 系统)。内部系统可配置为仅与内部 DNS 服务器交互，或者可允许它们向外部 DNS 服务器发送查询(这要求防火墙必须是状态检测防火墙，配置为允许将一个已批准的出站查询的响应返回到内部系统)。

9.3 基于服务端的系统

基于服务端(可能也包括客户端)的系统安全，关注的重要领域是数据流控制的问题。数据流是进程之间、设备之间、网络之间或通信通道之间的数据移动。数据流管理不仅要确保以最小延迟或延时进行高效的传输，还要使用散列确保可靠的吞吐率、使用加密确保保密性。数据

流控制还要确保接收系统不会因流量而过载，尤其是出现连接丢失或遭受恶意(甚至是自己造成的拒绝服务的情况)。当发生数据溢出时，数据可能丢失或损坏，或者可能触发重新传送的要求。这些结果是不符合要求的，通常通过实施数据流控制以防止这些问题的发生。数据流控制可由路由器和交换机等网络设备提供，也可由网络应用和服务提供。

负载均衡器用于在多个网络链路或网络设备之间传播或分配网络流量负载。负载均衡器可能提供对数据流的更多控制。负载均衡的目的是获得更优化的基础设施利用率、响应时间最小化、吞吐量最大化、减少过载并消除瓶颈。尽管可在多种场景下使用负载均衡，但常见的用途是在服务器场或集群的多个成员之间分配负载。负载均衡器可能使用各种技术来执行负载分配，包括随机选择、循环、负载/利用率监控和首选项。

拒绝服务(Denial-Of-Service, DoS)攻击可能对数据流控制造成严重危害。监控 DoS 攻击并实施缓解措施非常重要。有关这些攻击和潜在防御机制的讨论，请参阅第 12 章和第 17 章。

9.4 数据库系统安全

数据库安全性是任何使用大量数据作为重要资产的组织的重要组成部分。如果没有在数据库安全方面所做的工作，可能会导致业务中断并泄露机密信息。对于 CISSP 考试来说，你必须了解与数据库安全性相关的几个主题。这些主题包括聚合、推理、数据挖掘、数据仓库和数据分析。

9.4.1 聚合

SQL 提供了许多函数，这些函数可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。此过程称为聚合(Aggregation)。聚合也有安全漏洞。聚合攻击用来收集大量较低安全级别或较低价值数据项，并将它们组合在一起以生成具有更高安全级别或有价值的数据项。

SQL 的这些功能虽然非常有用，但也会对数据库中信息的安全性造成风险。例如，假设一名低级军事记录员负责更新基地之间的人员和设备的调配记录。作为其职责的一部分，可向该记录员授予查询和更新人员表所需的数据库权限。

军方可能没有考虑到个人调动请求(换句话说，琼斯中士从基地 X 调到基地 Y)是机密信息。记录员可访问该信息，因为他需要它来处理琼斯中士的调动。但是，通过使用聚合函数，记录员可计算出全球每个军事基地的部队人数，这些武装力量的级别通常是被严密保护的军事机密，但低级别的记录员可通过在大量未分类数据记录中使用聚合函数来推断出这些内容。

因此，严格控制对聚合函数的访问并充分评估它们可能向未经授权的人披露的潜在信息，对于数据库安全管理员来说非常重要。

9.4.2 推理

推理(Inference)攻击造成的数据库安全问题与数据聚合威胁造成的问题类似。推理攻击指组合若干非敏感信息以获取本应该属于更高分类级别的信息。然而，推理攻击利用的是人类思维的推理能力而不是现代数据库平台的原始计算能力。

推理攻击的一个常见例子是大公司的会计，他们可检索公司的工资总支出，以便在给高层的报告中使用，但不允许查看个别员工的工资。会计通常必须使用过去的有效日期来准备报告，因此可获得过去一年中任何一天的工资总额。假如，这位会计还必须知道各个员工的雇用和解聘日期，并可访问这些信息，这就为推理攻击打开了大门。如果某个员工是在特定日期雇用的唯一人员，则会计现在可检索该日期和前一天的工资总额，就可推断出该员工的工资，而这本应该是会计不能直接访问的敏感信息。

与聚合类似，针对推理攻击的最佳防御措施是对授予单个用户的权限始终保持警惕。此外，也可故意混淆数据来防止敏感信息的推理。例如，如果会计人员只能检索四舍五入到“百万”位的工资信息，那么他们可能无法获得有关个别员工的任何有用信息。最后，还可使用数据库分区来帮助阻止这些攻击。

9.4.3 数据挖掘和数据仓库

许多公司使用大型数据库(称为数据仓库)来存储来自各种数据库的大量信息，以便与专门的分析技术一起使用。由于存储限制或数据安全性问题，数据仓库常包含通常在生产数据库中不存储的详细历史信息。

数据字典通常用于存储关于数据的关键信息，包括用途、类型、来源、关系和格式。数据库管理系统(DBMS)软件读取数据字典以确定试图访问数据的用户的访问权限。

数据挖掘技术允许分析人员搜索数据仓库并寻找潜在的相关信息。例如，分析人员可能发现冬季时对灯泡的需求总是增加，然后使用这些信息来规划定价和促销策略。数据挖掘技术导致了数据模型的开发，数据模型可用于预测未来的活动。

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。元数据不仅仅是数据挖掘操作的结果；其他功能或服务也可以生成元数据。可将数据挖掘操作中的元数据视为数据浓缩。它也可以是超集、子集或更大数据集的代表。元数据可以是数据集中重要的、有意义的、相关的、不正常的或异常的元素。

元数据的一个常见安全示例是安全事件报告。事件报告是通过使用安全审核数据挖掘工具从审核日志的数据仓库中提取的元数据。大多数情况下，元数据的价值或敏感度(由于泄露)比数据仓库中的大量数据更高。因此，元数据存储在称为数据集市的更安全的容器中。

数据仓库和数据挖掘对安全专业人员来说意义重大，主要原因有两个。首先，如前所述，数据仓库包含大量易受聚合和推理攻击的潜在敏感信息，安全从业者必须确保有足够的访问控制和其他安全措施来保护这些数据。其次，当数据挖掘用于开发基于统计异常的入侵检测系统的基线时，它实际上可作为安全工具使用。数据挖掘用于“搜索”与安全相关的大量数据，以查找可能表明正在进行攻击、损害或破坏的异常事件。

9.4.4 数据分析

数据分析是检查原始数据的科学，其重点是从大批量信息集中提取出有用信息。数据分析的结果可能集中在与正常或标准项目相比的重要异常值或异常，所有数据项的摘要，或一些有兴趣的信息的提取和组织。随着越来越多的组织从其客户和产品中大量收集数据，数据分析是一个不断发展的领域。要处理的大量信息需要一整套新的数据库结构和分析工具。它甚至获得

了“大数据”的昵称。

大数据是指数据集合已变得非常巨大，以至于传统的分析或处理方法变得无效果、效率低下且不充分。大数据涉及许多挑战，包括收集、存储、分析、挖掘、传输、分发和结果呈现。如此大量的数据可能揭示细微的差别和特质，而普通数据集是无法解决的。从大数据中学习的潜力是巨大的，但处理大数据的负担同样很大。随着数据量的增加，数据分析的复杂性也会增加。大数据分析需要在大规模并行或分布式处理系统上运行高性能的分析。在安全性方面，组织正在努力收集更详尽的事件数据和访问数据。收集这些数据的目的是评估合规性、提高效率和检测违规行为。

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种设计用于同时执行大量计算的计算系统。但并行数据系统通常远超出基本的多处理能力。它们通常包含的概念是将大型任务划分为更小的元素，然后将每个子元素分配到不同的处理子系统进行并行计算。这种实现基于这样的想法：某些问题如果可分解成可同时工作的较小任务，则可更有效地解决。并行数据处理可通过使用不同的 CPU 或多核 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还必须关注性能、功耗和可靠性/稳定性问题。

在多处理或并行处理的领域内有几个部分。第一个部分关于非对称多处理(AMP)和对称多处理(SMP)。在 AMP 中，处理器通常彼此独立地工作。通常，每个处理器都有自己的 OS 和/或任务指令集。在 AMP 下，处理器可配置为仅执行特定代码或对特定任务进行操作(或者允许特定代码或任务仅在特定处理器上运行；在某些情况下可能称为亲和性)。在 SMP 中，每个处理器共享一个公共的操作系统和内存。处理器集合还可在单一任务、代码或项目上共同工作。AMP 的一种变体是大规模并行处理(MPP)，其中许多 SMP 系统被链接在一起，以便在多个链接系统中的多个进程上处理单一主任务。MPP 传统上涉及多个机箱，但现代 MPP 通常在同一芯片上实现。

大规模并行数据系统的舞台仍在不断发展。许多管理问题可能尚未发现，而对于已知的问题仍在寻找解决方案。大规模并行数据管理可能是管理大数据的关键工具，通常涉及云计算、网格计算或对等计算解决方案。下面将介绍这三个概念。

9.5 分布式系统和端点安全

计算已经从主机/终端模型(用户可以物理分布，但所有功能、活动、数据和资源都驻留在单个集中式系统上)发展为客户端/服务器模型(用户操作独立的、功能齐全的台式计算机，但是仍要访问网络服务器上的服务和资源)，安全控制和概念必须随之发展。这意味着客户端具有计算和存储功能，众多的服务器通常也具有相同的功能。客户端/服务器模型网络的概念也称为分布式系统或分布式体系结构。因此，安全性必须在所有地方解决，而不是只在单个集中的主机上。从安全角度看，这意味着由于处理和存储分布在多个客户端和服务器上进行，因此必须妥善地保障和保护所有这些计算机。它还意味着客户端和服务器之间的网络链接(某些情况下，这些链接可能不仅仅是本地链接)也必须受到保障和保护。在评估安全体系结构时，请务必包含对

与分布式体系结构相关的需求和风险的评估。

分布式体系结构比完整的主机/终端系统更容易出现意想不到的漏洞。桌面系统包含可能存在暴露风险的敏感信息，因此必须加以保护。个人用户可能缺乏一般的安全知识或意识，因此底层架构必须弥补这些不足。桌面PC、工作站和笔记本电脑都可提供访问分布式环境中其他位置上关键信息系统的途径，因为用户需要访问网络上的服务器和服务才能完成工作。由于允许用户计算机访问网络及其分布的资源，组织还必须认识到：如果这些用户计算机被滥用或受到攻击，它们可能成为威胁。必须正确评估并解决这类软件和系统的漏洞以及威胁。

通信设备也提供有害的分布式环境入口。例如，连接到桌面计算机的调制解调器也连接到组织的网络，这会使该网络容易受到拨号攻击。客户端系统上的无线适配器也存在被用来创建开放网络的风险。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、特洛伊木马等的风险。台式机、笔记本电脑、平板电脑、移动电话和工作站以及相关磁盘或其他存储设备可能无法防范物理入侵或被盗。最后，当数据仅存储在客户端计算机上时，可能无法使用适当的备份进行保护(通常，虽然服务器进行常规的备份，但客户端计算机却不是这样)。

你应该看到，上述一系列分布式体系结构中的潜在漏洞，意味着这类环境需要许多安全措施来实现适当的安全性，并确保消除、减轻或修复此类漏洞。客户必须遵守对其内容和用户活动实施保护的政策。其中包括：

- 必须对电子邮件进行过滤，使其不会成为恶意软件感染的载体；电子邮件还应遵守管理正当使用且限制潜在责任的政策。
- 必须创建下载/上传策略，以便过滤传入和传出的数据并阻止可疑的内容。
- 系统必须受到可靠的访问控制约束，这可能包括多因素身份验证和/或生物识别，以限制对最终用户设备的访问并防止对服务器和服务的未授权访问。
- 应使用受限用户界面机制并安装数据库管理系统，限制和管理对关键信息的访问，这样用户对敏感资源可进行必要但最少的访问。
- 文件加密可能适用于存储在客户端计算机上的文件和数据(实际上，驱动器级加密对于笔记本电脑和其他移动计算设备来说是一个好主意，因为这些设备可能在组织的场所之外丢失或被盗)。
- 必须分离和隔离在用户和监管模式下运行的进程，这样可防止对高权限进程和功能进行未经授权和有害的访问。
- 应该创建保护域，以便某个客户端遭受的危害不会自动危害整个网络。
- 应清楚地标明磁盘和其他敏感材料的安全等级或组织敏感性；程序流程和系统控制应结合起来，以帮助保护敏感材料免受不必要的未授权的访问。
- 应备份桌面计算机上的文件以及服务器上的文件。理想情况下，应使用某种集中形式的备份实用程序，该实用程序与客户端代理软件一起使用以识别和捕获客户存储在安全备份存储归档中的文件。
- 桌面用户需要定期进行安全意识培训，以保持正确的安全意识；有关潜在的威胁要通知他们，并指导他们正确地处理这些威胁。
- 台式计算机及其存储介质需要防范环境危害(如温度、湿度、断电/电压波动等)。
- 桌面计算机应该包含在灾难恢复和业务连续性计划中，是为了能让用户恢复在其他系统上工作，桌面计算机可能与组织内的其他系统和服务一样重要(或者更重要)。

- 在分布式环境中使用内置和自定义软件的开发人员也需要考虑安全性，包括使用正式的开发和部署方法，例如代码库、变更控制机制、配置管理以及补丁和更新部署。

通常，保护分布式环境意味着要了解它们所面临的漏洞并采用适当的安全控制措施。这些措施的范围可以从技术解决方案和控制延伸到风险管理的政策和程序，力求限制或避免损失、破坏、有害的泄露等。

在应对漏洞和威胁时，对于对策原则的正确理解是非常重要的。第 2 章讨论了一些具体的对策原则。但共同的一般性原则是纵深防御。纵深防御是一种常见的安全策略，用于提供防止各种攻击形式的多层的保护性屏障。可合理地假设，通过一个由防火墙、IDS 和负责任的管理人员强化的网络传送有问题的流量或数据，肯定比仅使用一个防火墙的网络更难。为什么不把防御措施加倍呢？纵深防御(又称多层次防御和防御多样性)是在字面上或理论上的同心圆中使用多种类型的访问控制。这种分层安全形式有助于组织避免单一的安全态势。单一的或加固的心态是相信单一的安全机制能充分提供所需的全部安全性。不幸的是，每个单独的安全机制都会有缺陷或绕过方法，迟早会被黑客发现和利用。只有通过对策的智能组合，才能抵御重大的和持久的破坏图谋。

9.5.1 基于云的系统和云计算

云计算是一个流行的术语，是一个计算概念，指通过网络连接在其他地方(而不是本地)执行处理和存储。云计算通常被认为是基于 Internet 的计算或远程虚拟化。最终，处理和存储仍然发生在某个地方的计算机上，但区别在于本地操作者不再需要在本地具有该容量或能力。这还允许更大的用户组根据需求来利用云资源。从最终用户的角度看，所有计算工作现在都在“云中”执行，因此计算的复杂性与他们无关。

云计算是虚拟化、互联网、分布式架构以及可随处访问数据和资源的需求的自然延伸和发展。但它确实存在一些问题，包括隐私问题、合规困难、开源与封闭式解决方案的使用、开放标准的采用以及基于云的数据是否切实地受到保护(甚至能否保护)。虚拟机管理程序(也称为虚拟机监视器)是创建、管理和操作虚拟机的虚拟化组件。运行虚拟机管理程序的计算机称为主机操作系统，在虚拟机管理程序支持的虚拟机中运行的操作系统称为客户操作系统。

Type-I 虚拟机管理程序是原生或裸机管理程序。在此配置中，没有主机操作系统；相反，虚拟机管理程序直接安装到通常主机操作系统安装的硬件上。Type-I 虚拟机管理程序常用来支持服务器虚拟化。这允许最大限度地利用硬件资源，同时消除由主机 OS 引起的任何风险。

Type-II 虚拟机管理程序是托管管理程序。在这种配置中，在硬件上安装一个标准的常规 OS，然后将虚拟机管理程序作为一个软件应用程序安装。Type-II 虚拟机管理程序通常用于桌面部署，功能包括：客户操作系统提供安全的沙箱区域来测试新代码、允许执行遗留的应用程序、支持来自备用操作系统的应用程序以及为用户提供对主机 OS 功能的访问等。

云存储的概念是指使用云供应商提供的存储容量作为托管组织数据文件的方法。云存储可当作一种备份方式或用来支持在线数据服务。云存储可能符合成本效益原则，但它并不总是高速或低延迟。大多数组织还没有将云存储视为物理备份介质解决方案的替代品，而是作为组织数据保护的补充。此外，使用云存储可能涉及额外的风险，因为组织的数据存储在另一个设施中的设备上并且受第三方控制。

弹性是指虚拟化和云解决方案根据需要扩展或收缩的灵活性。与虚拟化有关，主机弹性意

意味着可在需要时引导其他硬件主机，然后将虚拟化服务的工作负载分布到新的可用容量上。随着工作负载变小，你可从不需要的硬件中分离出虚拟化服务，然后关闭它以节省电力并减少热量。

此处列出了云计算的一些概念：

平台即服务 平台即服务(Platform as a Service, PaaS)的概念是将计算平台和软件解决方案提供为虚拟的或者基于云的服务。从根本上讲，这种类型的云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包)。PaaS 的主要吸引力在于避免必须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(Software as a Service, SaaS)是 PaaS 的衍生产品。SaaS 提供对特定软件应用程序或套件的按需在线访问而不需要本地安装。多数情况下，很少有本地硬件和操作系统的限制。SaaS 可实现为订阅服务(如 Microsoft Office 365)、即用即付服务或免费服务(如 Google Docs)。

基础设施即服务 基础设施即服务(Infrastructure as a Service, IaaS)使 PaaS 模式又向前迈进了一步，不仅提供按需运营解决方案，还提供完整的外包选项。这可以包括实用程序或计量计算服务、管理任务自动化、动态扩展、虚拟化服务、策略实施和管理服务以及托管/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软件或基于数据的服务/解决方案，而不必在本地安装大量硬件。

市场上还有许多其他“X 即服务”产品，每种产品都有各自潜在的漏洞和优势。不同的云计算公司可能会按照自己的方式定义或标记其服务。因此，仔细比较和对比每个提供商提供的功能和选项非常重要。

本地部署解决方案是传统的部署概念，组织拥有硬件、购买软件许可证，并且通常在他们自己的建筑物内操作和维护系统。本地部署解决方案不像云服务那样具有持续的每月订阅成本，但由于获得硬件和软件许可证的前期初始成本以及持续的运营管理成本，因此可能更昂贵。本地部署解决方案提供完全的定制化：提供本地安全控制、不需要 Internet 连接并且提供对更新和变更的本地控制。但它们也需要对更新和变更进行大量的管理，需要本地备份和管理，并且扩展更具挑战性。

托管解决方案是一种部署概念，其中组织必须购买软件许可证，然后操作和维护软件。托管服务提供商拥有、运营和维护支持组织软件的硬件。

云解决方案是一种组织与第三方云提供商签订合同的部署概念。云提供商拥有、运营和维护硬件和软件。组织按月支付费用(通常基于每个用户计算)以使用云解决方案。大多数本地环境都可创建或重建为仅限于云的解决方案。

可按如下几种方式部署云服务。

私有云 私有云(private cloud)是企业内部网络中的云服务并与 Internet 隔离。私有云仅供内部使用。虚拟私有云是由公有云提供商提供的服务，该提供商提供公有云或外部云的独立子部分，供组织内部专用。换句话说，组织将其私有云外包给外部提供商。

公有云 公有云(public cloud)是一种可供公众访问的云服务，通常通过 Internet 连接。公有云服务可能需要某种形式的订阅或按使用次数付费，或者也可能免费提供。虽然公有云中组织或个人的数据通常与其他客户的数据保持分离和隔离，但云的总体目的或用途对所有客户来说都是相同的。

混合云 混合云(hybrid cloud)是私有云和公有云组件的混合体。例如，组织可以托管专用

于内部使用的私有云，但会将一些资源分配到公有云，供公众、业务合作伙伴、客户、外部销售人员等使用。

社区云 社区云(*community cloud*)是由一组用户或组织维护、使用和支付用于利益共享的云环境，例如协作和数据交换。与独立访问私有云或公有云相比，这可节省一些成本。

云计算是虚拟化、互联网、分布式架构以及可随处访问数据和资源的需求的自然延伸和发展。但它确实存在一些问题，包括隐私问题、合规困难、开源与封闭式解决方案的使用、开放标准的采用以及基于云的数据是否切实地受到保护(甚至能否保护)。

云解决方案通常具有较低的前期成本、较低的维护成本、供应商维护的安全性和可扩展的资源，并且通常可从任何地方(通过互联网)获得高级别的正常运行时间和可用性。但云解决方案不允许客户控制操作系统和软件(如更新和配置变更)，提供最小的定制，没有互联网连接时通常将无法访问。此外，云提供商的安全策略可能与组织的安全策略不匹配。

云计算和虚拟化(尤其在云中进行虚拟化时)会产生严重风险。一旦敏感、机密或私有数据离开组织范围，它就离开了组织安全策略和组合的基础设施所给予的保护。云服务商及其人员可能不遵从与组织相同的安全标准。实际上，许多云供应商提供的环境比大多数组织自己能维护的环境更安全。云提供商通常拥有安全工程师、运营和测试人员等资源，而许多中小型(甚至大型)组织根本负担不起。在采用云服务前，调查云服务的安全性非常重要。

随着行业法规负担的增加，例如 2002 年的 SOX 法案(Sarbanes - Oxley Act，萨班斯-奥克斯利法案)、HIPAA 法案(Health Insurance Portability and Accountability Act，健康保险流通与责任法案)以及 PCI DSS(Payment Card Industry Data Security Standards，支付卡行业数据安全标准)，必须确保云服务提供足够保护以保持合规性。此外，云服务供应商可能无法将你的数据存储在主要物理位置的附近。事实上，他们可能将数据分布存储在很多地方，其中一些地点可能位于你的原籍国之外。可能有必要向云服务合同中添加限制条款，要求仅将数据存放在特定的逻辑和地理边界内。

研究云服务使用的加密解决方案非常重要。你是否将数据发送给它们之前进行预加密，或者仅在到达云平台后才加密？加密密钥存储在哪里？你的数据与其他云用户的数据之间是否进行隔离？加密错误会泄露你的数据或使你的数据无法恢复。

从云中恢复或复原数据的方法是什么、速度怎么样？如果本地系统出现故障，那么如何让环境恢复正常？还要考虑云服务是否有灾难恢复解决方案。如果遇到灾难，它恢复和复原服务以及访问你的云资源的计划是什么？

其他问题包括：进行调查的难度、对数据销毁的担忧，以及如果当前的云计算服务商停业或被其他组织收购会发生什么。

快照是虚拟机的备份。它们提供一种从错误或有问题的更新中快速恢复的方法。备份整个虚拟系统而不是等效的本机硬件安装的系统通常更便捷。

虚拟化不会降低操作系统的安全管理要求。因此，补丁管理仍然是必不可少的。修补或更新虚拟化操作系统与传统硬件安装的操作系统的过程相同，还有一个好处，即你可在不关闭服务的情况下修补系统或交换活动系统。另外，不要忘记你还需要更新虚拟化主机。

当使用虚拟化系统时，保护主机的稳定性非常重要。这通常意味着避免将主机用于托管虚拟化元素之外的任何其他目的。如果主机的可用性受到损害，则虚拟系统的可用性和稳定性也会受到损害。

虚拟化系统应该进行安全测试。虚拟化操作系统的测试采用与硬件安装的操作系统相同的

方式，例如漏洞评估和渗透测试。但是，虚拟化产品可能会引入其他独特的安全问题，因此需要调整测试过程以包括这些特性。

云访问安全代理(Cloud Access Security Broker, CASB)是一种实施安全策略的解决方案，可在本地安装也可以基于云。CASB 的目标是在云解决方案和客户组织之间实施适当的安全措施。

安全即服务(Security as a Service, SECaas)是一个云提供商概念，其中通过在线实体或由在线实体向组织提供安全性。SECaas 解决方案的目的是降低在本地实施和管理安全性的成本和开销。SECaas 通常实现为不需要专用本地硬件的纯软件安全组件。SECaas 安全组件可包括各种安全产品，包括身份验证、授权、审计/记账、反恶意软件、入侵检测、合规性和漏洞扫描、渗透测试和安全事件管理。

云共享责任模型的概念是，当组织使用云解决方案时，提供商和客户之间存在安全性和稳定性责任的划分。不同形式的云服务(例如 SaaS, PaaS 和 IaaS)可能具有不同级别或划分点的共享责任。SaaS 解决方案将大部分管理负担置于云提供商的肩上，而 IaaS 的管理责任则更倾向于客户。在选择使用云服务时，重要的是要考虑管理、故障排除和安全管理的细节以及如何在云提供商和客户之间分配、划分或共享这些职责。

9.5.2 网格计算

网格计算是一种并行分布式处理形式，它将大量处理节点松散地分组，以实现特定处理目标。网格成员可随机进入和离开网格。通常，网格成员只有在其处理能力不对本地工作造成负担时才加入网格。当系统处于空闲状态时，它可加入网格组，下载一小部分工作，然后开始计算。当系统离开网格时，它会保存其工作并可将完成或部分工作元素上传回网格。已经开发了网格计算的许多有趣用途，包括寻找智能外星人、执行蛋白质折叠、预测天气、地震建模、规划财务决策和解决素数等众多项目。

网格计算最大的安全问题是每个工作包的内容可能会暴露给外界。许多网格计算项目对全世界开放，因此对谁可运行本地处理应用程序并参与网格项目并没有限制。这也意味着网格成员可保留每个工作包的副本并检查其内容。因此，网格项目不太可能保护保密性，不适用于私有、机密或专有数据。

网格计算在计算能力方面也会随时发生很大变化。工作包有时不会被返回、返回迟到或返回时已经损坏。这需要大量的返工，并导致项目整体以及各个网格成员的速度、进度、响应性和延迟的不稳定性。对时间敏感的项目可能没有足够的计算时间来按指定的时间截止期限内完成。

网格计算通常使用中央核心服务器来管理项目、跟踪工作包并且集成返回的工作分段。如果中央服务器过载或脱机，则可能发生彻底故障或网格崩溃。但是，通常当中央网格系统不可访问时，网格成员完成其当前的本地任务，然后定期轮询以发现中央服务器何时重新联机。还存在这样的一个潜在风险：可利用被控制的中央网格服务器来攻击网格成员或欺骗网格成员执行恶意操作。

9.5.3 对等网络

对等网络(Peer to Peer, P2P)技术是网络和分布式应用程序解决方案，可在点对点之间共享

任务和工作负载。这类似于网格计算：主要区别在于 P2P 没有中央管理系统，其所提供的服务通常是实时的，而不是计算能力的集合。P2P 的常见示例包括许多 VoIP 服务，例如 Skype、BitTorrent(用于数据/文件分发)和 Spotify(用于流媒体音频/音乐分发)。

P2P 解决方案的安全问题包括对盗版受版权保护材料的感知诱导、窃听分布式内容的能力、缺乏集中控制/监督/管理/过滤以及服务消耗所有可用带宽的可能性。

注意：



第 6 章和第 7 章中详细介绍了密码系统。

9.6 物联网

智能设备是一系列移动设备，通常通过安装应用程序为用户提供大量的自定义选项，并可利用设备上或云端的人工智能(AI)处理。可贴上“智能设备”标签的产品不断扩大，已经包括的产品有智能手机、平板电脑、音乐播放器、家庭助理、极限运动相机和健身追踪器。

物联网(IoT)是一个新的子类别，甚至是一类新的智能设备，它们通过互联网连接，以便为家庭或办公室环境中的传统或新装置或设备提供自动化、远程控制或 AI 处理。物联网设备有时是对本地和手动执行了数十年的功能或操作的革命性改进，你希望继续使用这些功能或操作。其他物联网设备只不过是昂贵的花哨小玩意儿，在使用后没多久就被遗忘和/或丢弃。与物联网相关的安全问题涉及访问控制和加密。通常情况下，物联网设备不是以安全为核心概念设计的，甚至是事后才考虑。这已经导致许多家庭和办公室网络安全攻击事件。此外，一旦攻击者可以远程访问或控制了物联网设备，他们就可以访问被攻陷的网络上的其他设备。在选择安装物联网设备时，请评估设备的安全性以及供应商的安全信誉。如果新设备无法满足或接受你现有的安全基线，那么请不要仅为了华而不实的小工具而使安全性陷入危险。

一种可能的安全实施方案是将物联网设备部署在单独划分的网络中，且该网络与主网络保持独立和隔离。此配置通常称为三个哑路由器(请参阅 <https://www.grc.com/sn/sn-545.pdf> 或 <https://www.pcper.com/reviews/General-Tech/Steve-Gibsons-Three-Router-Solution-IOT-Insecurity>)。

虽然我们常将智能设备和物联网与家庭或个人使用相关联，但它们也是每个组织关注的问题。这在一定程度上是因为员工会在公司内部甚至组织的网络上使用移动设备。网络专业人员关注的另一个问题是许多物联网或网络自动化设备正在添加到业务环境中。这包括环境控制，如供暖、通风和空调(Heating, Ventilation And Air Conditioning, HVAC)管理、空气质量控制、碎片和烟雾探测、照明控制、门自动化、人员和资产跟踪，以及消耗品库存管理和自动重新排序(如咖啡、快餐、打印机墨粉、纸张和其他办公用品)。因此，智能设备和物联网设备都是现代业务网络中的潜在元素，需要适当的安全管理和监督。有关智能设备和物联网设备正确安全管理重要性的更多信息，请参阅“物联网 NIST 计划”，网址为 <https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot>。

9.7 工业控制系统

工业控制系统(Industrial Control System, ICS)是一种控制工业过程和机器的计算机管理设备。ICS 广泛用于各行各业，包括制造、加工、发电和配电、供水、污水处理和炼油。有几种形式的 ICS，包括分布式控制系统(DCS)、可编程逻辑控制器(PLC)以及监控和数据采集(SCADA)。

DCS 单元通常存在于工业过程计划中，其中从单个位置收集数据并实施对大规模环境的控制的需求是必不可少的。DCS 的一个重要方面是控制元件分布在受监控的环境中，例如生产车间或生产线，并且集中监控位置在收集状态和性能数据的同时也从这些局部控制器发送命令。DCS 本质上是模拟的或数字的，这取决于正在执行的任务或被控制的设备。例如，液体流量值 DCS 会是模拟系统，而电压调节器 DCS 可能是数字系统。

PLC 单元实际上是高效的单用途或专用数字计算机。它们通常用于各种工业机电操作的管理和自动化，例如控制装配线上的系统或大型数字灯显示器(例如体育场内或拉斯维加斯大道的巨型显示系统)。

SCADA 系统可作为独立设备运行，也可与其他 SCADA 系统联网，或与传统 IT 系统联网。大多数 SCADA 系统都设计成只有很少的人机界面。通常，它们使用机械按钮和旋钮或简单的 LCD 屏幕界面(类似于在商用打印机或 GPS 导航设备上可能看到的)。但是，联网的 SCADA 设备可能具有更复杂的远程控制软件接口。

从理论上讲，SCADA、PLC 和 DCS 单元的静态设计及其最小的人机接口应该使系统能够完全抵抗损害或修改。因此，这些工业控制设备中，特别是在过去，几乎没有考虑安全性。但近年来，工业控制系统出现了一些众所周知的攻击事件；例如，Stuxnet 有史以来第一次将 rootkit 投放到位于核设施的 SCADA 系统中。许多 SCADA 供应商已开始在其解决方案中实施安全性改进，以防止或至少减少未来的危害。然而，在实践中，SCADA 和 ICS 系统通常仍然安全性差、易受攻击并且不经常更新，并且设计中未考虑安全性的旧版本仍然在广泛使用。

9.8 评估和缓解基于 Web 系统的漏洞

基于 Web 的系统中存在各种各样的应用程序和系统漏洞与威胁，并且范围不断扩大。漏洞包括与可扩展标记语言(XML)和安全关联标记语言(SAML)相关的问题，以及开放 Web 应用安全项目(Open Web Application Security Project, OWASP)中所讨论的许多其他问题。

OWASP 是一个非营利性安全项目，专注于提高在线或基于 Web 的应用程序的安全性。OWASP 不仅是一个组织，也是一个大型社区，它们共同努力，自由地共享与更好的编码实践和更安全的部署架构相关的信息、方法、工具和技术。有关 OWASP 和参与社区的更多信息，请访问 www.owasp.org。OWASP 组织在 https://www.owasp.org/index.php/Web_Application_Security_Testing_Cheat_Sheet 上维护了评估 Web 服务安全性的建议指南。OWASP 还在 https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf 维护 Web 应用程序最重要的十大攻击的列表。这两个文档都是规划组织 Web 服务的安全评估或渗透测试的合理起点。

任何安全评估都应从侦察或信息收集开始。这一步骤是收集尽可能多的有关目标的信息，

以供后续步骤使用。这通常包括查看每个托管网页、发现正在使用的自动化技术、查找不应发布的信息以及检查配置和安全漏洞。然后评估站点的配置管理(例如文件处理、使用中的扩展、备份、在客户端代码中查找敏感数据)，并评估站点的传输安全性(例如检查安全套接字层(SSL)/传输层安全(TLS)版本支持，评估密码套件、cookie/会话 ID/令牌管理以及对伪造请求的敏感性)。

Web 安全评估中的下一步是评估身份验证和会话管理。然后评估站点的加密以及用于数据验证和清理的方法。Web 安全评估还应包括检查 DoS 防御、评估风险响应以及测试错误处理。

这只是对 Web 安全评估概念的概述，因为 CISSP 考试并不期望你成为专业的渗透测试人员，但你应该大致了解安全评估的概念。如果你对此主题感兴趣，欢迎你从 OWASP 指南中了解有关 Web 安全评估的更多信息。

注入、XML 利用、跨站脚本(XSS)和 CSRF 都属于“OWASP 十大 Web 风险”之列。

注入攻击指允许攻击者向目标系统提交代码以便修改其操作和/或损害并破坏其数据集。存在各种潜在注入攻击。通常，注入攻击是以其利用的后端系统的类型或传递(注入)到目标上的有效载荷的类型命名的。注入示例包括 SQL 注入、LDAP 注入、XML 注入、命令注入、HTML 注入、代码注入和文件注入。本节将详细介绍其中的一些内容。

从组织的角度看，SQL 注入攻击甚至比 XSS 攻击风险更高(参见下一节)，因为 SQL 注入攻击的目标是组织资产，而 XSS 攻击的目标是网站的客户或访问者。SQL 注入攻击使用意外的输入来更改或危害 Web 应用程序。但 SQL 注入攻击不是使用此输入来欺骗用户，而是使用它来获取对底层数据库和相关资产的未授权访问。

在 Web 时代的早期，所有网页都是静态的或者是不变的。网站管理员创建了包含信息的网页，并将其放在 Web 服务器上，用户可使用 Web 浏览器检索它们。Web 很快就超越了这个模型，因为用户希望根据个人需求访问定制化信息。例如，银行网站的访问者不仅对包含银行位置、营业时间和服务信息的静态页面感兴趣，还希望能检索包含有关其个人账户信息的动态内容。显然，网站管理员不可能在 Web 服务器上为每个用户创建包含其个人账户信息的页面。对于一家大型银行，这需要使用最新信息来维护数百万个页面。这就是动态 Web 应用程序发挥作用的地方。

Web 应用程序利用数据库在用户发出请求时按需创建内容。在银行示例中，用户登录 Web 应用程序，提供账号和密码。然后，Web 应用程序从银行的数据库中检索当前账户信息，并使用它立即创建包含用户当前账户信息的网页。如果该用户一个小时后返回，则 Web 服务器重复该过程，从数据库获取更新过的账户信息。

这对安全专业人员意味着什么？Web 应用程序增加了传统安全模型的复杂性。Web 服务器作为可公共访问的服务器，位于与其他服务器隔离的单独网络区域，通常称为非军事区(DMZ)。另一方面，数据库服务器不用于公共访问，因此它属于内部网络或至少与 DMZ 分离的安全子网。Web 应用程序需要访问数据库，因此防火墙管理员必须创建允许从 Web 服务器访问数据库服务器的规则。此规则为 Internet 用户创建了访问数据库服务器的潜在路径。

如果 Web 应用程序正常运行，它只允许对数据库的授权请求。但是，如果 Web 应用程序存在缺陷，则可能允许个人通过使用 SQL 注入攻击以意外和未经授权的方式篡改数据库。这些攻击允许恶意个体直接针对底层数据库执行 SQL 事务。SQL 注入攻击可能使攻击者绕过身份验证、从数据库表中泄露机密数据、更改现有数据、向数据库添加新记录、销毁整个表或数据库，甚至通过某些数据库功能获得命令行式访问(例如命令 shell 存储过程)。

可使用两种技术来保护 Web 应用程序免受 SQL 注入攻击。

执行输入验证 输入验证允许你限制用户在表单中输入的数据类型。输入注入或操纵攻击

有很多形式。需要多种防御方法，包括白名单和黑名单过滤器。应该采用的输入净化的主要形式包括限制输入的长度、过滤已知的恶意内容模式以及转义元字符。

限制账户权限 Web 服务器使用的数据库账户应具有可能的最小特权集。如果 Web 应用程序只需要检索数据，那么它应该只具有该能力。

元字符

元字符是已赋予特殊编程含义的字符。因此，它们具有标准字符所没有的特殊意义。有很多常见的元字符，但典型的例子包括单引号和双引号、开/闭方括号、反斜杠、分号、&符号、插入符号、美元符号、点号、垂直条(或管道符号)、问号、星号、加号、开/闭花括号以及开/闭圆括号：

```
" [ ] \ ^ $ , + ? * { }
```

转义元字符是将元字符标记为普通字符或常用字符(如字母或数字)的过程，从而消除了它们的特殊编程功能。这通常通过在字符前添加反斜杠(\&)来实现，但根据编程语言或执行环境，有许多方法可转义元字符。

基本上，SQL 注入是用于处理前端(通常是 Web 服务器)和后端数据库之间交互的脚本的一个漏洞。如果脚本是防御性的，并且包含要转义(作废或拒绝)元字符的代码，将无法进行 SQL 注入。

LDAP 注入是输入注入攻击的一种变体；但攻击重点是 LDAP 目录服务的后端而不是数据库服务器。如果 Web 服务器前端使用脚本根据用户的输入来生成 LDAP 语句，则 LDAP 注入可能是一种威胁。就像 SQL 注入一样，输入净化和防御性编码对于消除这种威胁至关重要。

XML 注入是 SQL 注入的另一种变体，其中后端目标是 XML 应用程序。同样，输入净化是消除这种威胁所必需的。

目录遍历/命令注入

目录遍历是一种攻击，它使攻击者能跳出 Web 根目录结构，进入 Web 服务器主机操作系统托管的文件系统的其他任何部分。历史上，此攻击的常见版本是针对由 Windows NT 4.0 Server 托管的 IIS 4.0。该攻击使用修改后的 URL 经由 Web 根目录遍历到主 OS 文件夹中，以便访问命令提示符可执行文件。

下面是一个例子：

```
http://victim.com/scripts/..%c0%af.../%c0%af.../%c0%af.../%c0%af.../..%c0%af.../%c0%af.../..%c0%af.../..%c0%af.../winnt/system32/cmd.exe?/c+tftp+1+get+exploit:exe
```

此 URL 包含“更改为父目录”(change to parent directory)命令的 Unicode 编码，在 ASCII 中为 ./. 并且注意它还使用元字符百分比(%). 此 URL 不仅执行了目录遍历，还使攻击者获得了执行命令注入的能力。该示例显示了命令注入执行了普通文件传输协议(TFTP)Get 操作，以将漏洞利用工具下载到受害的 Web 服务器上。可使用任何能在 IIS 服务的特权下执行并在 URL 的限制内指定的命令。该示例执行一个列出 C 根目录文件的命令。但是通过微小的调整，可以使用 TFTP 命令将黑客工具下载到目标系统，然后启动这些工具，以授予更大的远程控制或真正的命令 shell 访问权限。可通过元字符转义或过滤来阻止此类攻击。

XML 利用是一种编程攻击的形式，用于伪造发送给访问者的信息，或者导致他们的系统在未经授权的情况下泄露信息。关于 XML 攻击越来越受关注的一个领域是安全关联标记语言(SAML)。SAML 滥用通常集中在基于 Web 的身份验证方面。

SAML 是一种基于 XML 的约定，用来组织和交换在安全域之间的用于认证与授权通信的详细信息，通常使用 Web 协议。SAML 通常用来提供基于 Web 的 SSO(单点登录)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，他们可能会绕过身份验证并获得对站点的未授权访问。

跨站脚本(XSS)是一种恶意代码注入攻击形式，攻击者可攻击 Web 服务器并将自己的恶意代码注入发送给其他访问者的内容中。黑客已发现了许多巧妙方法，可通过公共网关接口(CGI)脚本、Web 服务器软件漏洞、SQL 注入攻击、帧利用、DNS 重定向、cookie 劫持以及许多其他形式的攻击将恶意代码注入网站。成功的 XSS 攻击可能导致身份盗窃、凭据盗窃、数据盗窃、经济损失或在来访的客户端上植入远程控制软件。

对于网站管理员来说，针对 XSS 的防御包括维护已安装补丁的 Web 服务器、使用 Web 应用程序防火墙、运行基于主机的入侵检测系统(Host-Based Intrusion Detection System, HIDS)、审核可疑活动。最重要的是，在服务器端验证输入长度、执行恶意内容和元字符过滤。作为 Web 用户，你可通过及时给系统打补丁、运行反病毒软件以及避免非主流网站来防范 XSS。某些 Web 浏览器有一些附加组件，例如适用于 Firefox 的 NoScript 和适用于 Chrome 的 uBlock Origin，它们只允许执行你选择的脚本。

跨站请求伪造(Cross-Site Request Forgery, XSRF)本质上是一种与 XSS 类似的攻击。但是，使用 XSRF 攻击的重点是来访用户的 Web 浏览器，而不是要访问的网站。XSRF 的主要目的是欺骗用户或用户的浏览器执行超出预期或不会被授权的操作。这可能包括退出会话、上传网站 cookie、更改账户信息、下载账户详细信息、进行购买等。有一种形式的 XSRF 感染受害者的系统，其恶意软件一直处于休眠状态，直到访问特定的网站时才激活。然后，恶意软件伪造用户的请求，以欺骗 Web 服务器并对 Web 服务器和/或客户端执行恶意操作。

使用 XSRF 的漏洞利用的一个例子是 Zeus，它会隐藏在受害者的系统上，直到用户访问他们的在线银行网站；然后，在检查账户余额并确定了银行账号后，这些详细信息将被发送给攻击控制者，后者将向另一家银行发起 ACH 汇款。因此，这是恶意软件的一个例子，它会直接从受害者的账户中窃取资金。

网站管理员可通过在连接的客户端请求敏感或有风险的操作时，要求确认或重新认证来实施针对 XSRF 的预防措施。这可能包括要求用户重新输入密码、通过短信或电子邮件向用户发送代码，这些代码然后必须返回给网站、触发基于电话呼叫的验证，或者解答 CAPTCHA(Completely Automated Public Turing Test to Tell Computers and Humans Apart)。CAPTCHA 是一种区分人类和软件机器人的机制。另一种潜在的保护机制是向每个 URL 请求和会话建立添加随机化字符串(称为 nonce)，并检查客户端 HTTP 请求头引用防止欺骗。最终用户可形成更安全的习惯，例如运行反恶意软件扫描程序、使用 HIDS、运行防火墙、避免非主流网站、始终从站点注销(而不是关闭浏览器或关闭选项卡或转到另一个 URL)、给浏览器打补丁以及定期清除临时文件(和缓存的 cookie)。

有关 XSS 和 CSRF 的其他内容，请参见第 21 章。

9.9 评估和缓解移动系统的漏洞

随着智能手机和其他移动设备越来越顺畅地与互联网以及企业网络进行交互，它们呈现出越来越大的安全风险。当个人拥有的设备被允许进入和离开安全设施而没有限制、监督或控制时，潜在的危害是巨大的。

恶意内部人员可以通过各种存储设备将恶意代码从外部引入到内部，包括移动电话、音频播放器、数码相机、存储卡、光盘和通用串行总线(USB)驱动器。这些相同的存储设备可用于泄露或窃取内部机密和私有数据(维基解密的大部分内容来源于此)。恶意内部人员可执行恶意代码，访问危险网站或故意执行有害的活动。

注意：



可使用以下任何术语来引用个人拥有的设备：便携式设备、移动设备、个人移动设备(Personal Mobile Device, PMD)、个人电子设备(Personal Electronic Device, PED)、便携式电子设备(Portable Electronic Device，简写形式也为 PED)以及个人拥有的设备(Personally Owned Device, POD)。

移动设备通常包含敏感数据，如联系人、短信、电子邮件以及可能的笔记和文档。任何具有相机功能的移动设备都可拍摄敏感信息或位置的照片。移动设备的丢失或被盗可能意味着个人和/或公司机密的泄露。

移动设备是黑客和恶意代码的共同目标。以下这些措施很重要：不要在便携式设备中保存敏感信息，运行防火墙和反病毒产品(如果可用)，保持系统锁定和/或加密(如果可能)。

许多移动设备还支持 USB 连接，可用于与桌面和/或笔记本计算机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，移动设备也无法避免窃听。使用类型合适的精密设备，大多数手机通话都能被窃听，更不用说 15 英尺内的任何人都可听到你的谈话内容。尤其在公共场所，一定要小心打电话时谈论的内容。

移动设备上提供了广泛的安全功能。但对一个功能的支持和“正确配置并启用这个功能”不是一回事。只有在安全功能生效时才能获得安全保障。请务必检查所有需要的安全功能是否在你的设备上按预期运行。

Android

Android 是一款基于 Linux 的移动设备操作系统，于 2005 年被 Google 收购。2008 年，第一批安装了 Android 的设备向公众开放。Android 源代码是通过 Apache 许可证开源的，但大多数设备还包括专有软件。虽然主要用于手机和平板电脑，但 Android 也正被广泛用于各种设备，包括电视、游戏机、数码相机、微波炉、手表、电子阅读器、无线电话和滑雪护目镜。

在手机和平板电脑中使用 Android 可以进行广泛的用户定制；你可以安装 Google Play 商店应用以及来自未知外部源(例如亚马逊的 App Store)的应用，并且许多设备支持用定制的或修改版本替换默认版本的 Android 系统。但当 Android 在其他设备上使用时，它的实现更像是一个静态系统。

无论是否静态，Android 都有许多安全漏洞。这些漏洞包括暴露于恶意应用程序、运行恶意网站脚本以及允许不安全的数据传输。Android 设备通常会被提升为 root 权限(破坏了其安全性和访问限制)，以便给予用户对设备底层的配置设置的完全 root 级别访问权限。提升为 root 权限会增加设备的安全风险，因为所有正在运行的代码都继承了 root 权限。

随着新的更新发布，Android 的安全性得到了改善。用户可以调整许多配置项的设置，以减少漏洞和风险。此外，用户还可安装能向平台添加附加安全功能的应用程序。

iOS

iOS 是 Apple 的移动设备操作系统，可在 iPhone、iPad 和 Apple TV 上使用。iOS 没有授权给任何非 Apple 硬件使用。因此，Apple 可完全控制 iOS 的特性和功能。然而 iOS 也不是静态环境，因为用户可从 Apple App Store 安装超过 200 万个应用程序中的任何一款。此外，通常可越狱 iOS(打破 Apple 的安全和访问限制)，允许用户从第三方安装应用程序并获得对底层设置的最大控制权限。越狱 iOS 设备会降低其安全性并使设备面临潜在的危害。用户可调整设备设置以提高 iOS 设备的安全性，并安装许多可增加安全功能的应用程序。

9.9.1 设备安全

设备安全性涉及可用于移动设备的潜在安全选项或功能的范围。并非所有便携式电子设备(PED)都具有良好的安全功能。即使设备具有安全功能，除非启用并正确配置，否则这些功能没有任何价值。在做出购买决定前，请务必考虑新设备的安全选项。

1. 全设备加密

一些移动设备，包括便携式计算机、平板电脑和移动电话，可提供设备加密。如果设备的大多数或所有存储介质都可被加密，这通常是一个值得启用的功能。但加密并不能保证数据的安全，特别是如果设备在已解锁时被盗或者系统本身具有已知的后门攻击漏洞。

当使用网络电话(VoIP)服务时，可在移动设备上进行语音加密。与到传统固定电话或典型的移动电话的 VoIP 连接相比，在计算机类设备之间的 VoIP 服务更可能提供加密选项。当语音对话被加密时，窃听将变得毫无价值，因为对话的内容是无法解密的。

2. 远程擦除

当设备丢失或被盗后，执行设备远程擦除或远程清除变得越来越普遍。通过远程擦除，你可远程删除设备中的所有数据(甚至包括配置设置)。擦除过程可通过移动电话服务或有时通过任何互联网连接触发。但远程擦除不能保证数据的安全。窃贼可能很聪明，可阻止设备联网而触发擦除功能，然后就可将数据导出。另外，远程擦除主要是删除操作。使用反删除或数据恢复工具通常可恢复已擦除设备上的数据。为确保远程擦除能破坏数据而无法恢复，应该对设备进行加密。这样，反删除操作只能恢复出加密数据，而攻击者将无法解密这些数据。

3. 锁定(Lockout)

移动设备上的锁定类似于公司工作站上的账户锁定。当用户在重复尝试后未能提供其凭据时，账户或设备将被禁用(锁定)一段时间或直到管理员清除锁定标志。

移动设备可能提供锁定功能，但仅在设置了屏幕锁定时才会启用。另外，通过简单的屏幕滑动来访问设备不能提供足够的安全性，因为这并没有进行身份验证过程。随着身份验证失败次数的增加，某些设备会触发更长的延迟。某些设备在触发持续几分钟的锁定之前允许一定次数的尝试(例如三次)。其他设备会触发持久锁定，并需要使用其他账户或主密码/代码才能重新获得对设备的访问权限。

4. 锁屏

锁屏旨在防止有人随意拿起来就能使用你的手机或移动设备。但大多数锁屏都可通过在键盘显示屏上滑动图案或键入数字来解锁。这些都不是真正的安全操作，屏幕锁定可能有绕过的方法，例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 电缆连接到设备，锁屏也不一定能保护设备。

锁屏通常在闲置超过一定时间后触发。如果系统闲置几分钟，大多数 PC 会自动触发受密码保护的屏幕保护程序。同样，许多平板电脑和手机会在 30~60 秒后触发锁屏并调暗或关闭显示屏。锁屏功能可确保设备处于无人看管状态或丢失或被盗时，其他任何人都无法访问你的数据或应用程序。要解锁设备，必须输入密码(或 PIN 码)、绘制图案、使用眼球或面部识别、扫描你的指纹或使用接近设备环或片。NFC(Near-Field Communication，近场通信)或 RFID(Radio-Frequency Identification，射频识别)都属于接近设备。



注意：

近场通信(NFC)是在邻近的设备之间建立无线电通信的标准。它允许你通过将设备接触在一起或将它们放在彼此相距几英寸的范围内来执行设备之间的自动同步和关联。NFC 通常出现在智能手机和许多移动设备配件上。它通常用来执行设备到设备数据交换、建立直接通信，或访问更复杂的服务，例如通过 NFC 与无线接入点链接来访问 WPA2(WiFi Protected Access 2)加密无线网络。NFC 是一种基于无线电的技术，因此存在漏洞。针对 NFC 的攻击包括中间人、窃听、数据操纵和重放攻击。

5. GPS

许多移动设备包括全球定位系统(Global Positioning System, GPS)芯片，以支持定位服务(例如导航)并从中受益，因此可以跟踪这些设备。GPS 芯片本身通常只是接收 GPS 卫星信号的接收器。但移动设备上的应用程序可记录设备的 GPS 位置，然后将其报告给在线服务。你可使用 GPS 跟踪来监控自己的移动，跟踪其他人(例如未成年人或送货人员)的移动，或追踪被盗设备。但要使 GPS 跟踪能工作，移动设备必须能连接到互联网或无线电话服务，并通过该服务来传送其位置信息。

6. 应用程序控制

应用程序控制是一种设备管理解决方案，能够限制可将哪些应用程序安装到设备上。它还可用于强制安装特定应用程序或强制执行某些应用程序的设置，以支持安全基线或维护其他形式的合规性。应用程序控制限制了用户安装来自未知来源或提供与工作无关功能的应用程序的能力，它可减少设备对恶意应用程序的暴露。

7. 存储分隔

存储分隔用于人为地在存储介质上划分各种类型或数据值。在移动设备上，设备制造商和/or 服务提供商可使用存储分隔将设备的 OS 和预装的应用与用户安装的应用和用户数据隔离。一些移动设备管理系统进一步强制存储分隔，以便将公司数据和应用与用户数据和应用隔离。

8. 资产跟踪

资产跟踪是用于维护对库存(例如已部署的移动设备)监督的管理过程。资产跟踪系统可以是被动的或主动的。被动系统依靠资产本身定期向管理服务签到，或者每当员工到达工作岗位时，设备被检测到位于办公室中。主动系统使用轮询或推送技术向设备发送查询以引发响应。

你可使用资产跟踪来验证设备是否仍由指定的授权用户拥有。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扩展到硬件库存管理之外，可以监控设备上已安装的应用程序、应用程序使用情况、存储的数据和数据访问。你可使用此类监控来验证是否符合安全准则，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”可描述硬件资产跟踪(如前一主题中所讨论的)。然而，它也可以指使用移动设备跟踪仓库或存储柜中的库存。大多数移动设备都有摄像头。使用移动设备的相机，应用程序可拍摄照片或扫描条形码来跟踪实物商品。这些具有 RFID 或 NFC 功能的移动设备能与使用电子标记的对象或其容器进行交互。

10. 移动设备管理

移动设备管理(Mobile Device Management, MDM)是一种软件解决方案，用来完成一个充满挑战的任务，即管理员工用于访问公司资源的无数移动设备。MDM 的目标是提高安全性、提供监控、启用远程管理以及支持故障排除。很多 MDM 解决方案支持各种设备，并可跨多个服务提供商进行操作。你可使用 MDM 借助无线连接(通过运营商网络)和 Wi-Fi 连接推送或删除应用程序、管理数据以及强制执行配置设置。MDM 可用于管理公司拥有的设备以及个人拥有的设备(例如，在自带设备[Bring Your Own Device, BYOD]环境中)。

11. 设备访问控制

如果锁定手机能提供真正的安全性，在手机或其他移动设备上设置一个强大的密码将是一个好主意。但是许多移动设备并不安全，因为即使使用强密码，设备仍可通过蓝牙、无线或 USB 电缆访问。如果特定的移动设备在启用系统锁定时阻止对设备的访问，则这是一个值得设置的功能。可设置为在空闲一段时间后自动触发或者手动触发。当你同时启用设备密码和存储加密时，通常会更有优势。

你应该考虑减少未经授权访问移动设备的任何方法。许多 MDM 解决方案可以强制锁屏配置并防止用户禁用该功能。

12. 可移动存储

很多移动设备支持可移动存储。某些设备支持 microSD 卡，可用于扩展移动设备上的可用存储空间。然而，大多数移动电话需要移除背板并且有时需要移除电池才能添加或移除存储卡。较大的移动电话、平板电脑和笔记本电脑可能支持位于设备侧面易于访问的卡槽。

许多移动设备还支持外部 USB 存储设备，例如闪存驱动器和外部硬盘驱动器。这些可能需要特殊的 OTG(on-the-go) 电缆。

此外，还有移动存储设备可以通过板载无线接口，基于蓝牙或 Wi-Fi 提供对存储数据的访问。

13. 关闭不使用的功能

虽然启用安全功能至关重要，但删除应用程序和禁用与业务任务或个人使用无关的功能也很重要。启用的功能和已安装应用程序的范围越广，攻击或软件缺陷对设备和/或其包含的数据造成损害的可能性越大。遵循常见的安全措施(例如加固)可减少移动设备的攻击面。

9.9.2 应用安全

除了管理移动设备的安全性外，你还需要关注这些设备上使用的应用程序和功能。台式机或笔记本电脑系统上的大多数软件安全问题和安全常识都适用于移动设备。

1. 密钥管理

在涉及密码技术时，密钥管理始终是一个问题。大多数密码系统的失败都是由于密钥管理而不是因为算法。好的密钥选择取决于随机数的质量和可用性。大多数移动设备必须依赖于本地较差的随机数生产机制或通过无线链路访问更强大的随机数生成器(Random Number Generator, RNG)。一旦创建密钥，就需要以尽量减少丢失或损害的方式来存储密钥。密钥存储的最佳选择通常是可移动硬件或使用可信平台模块(Trusted Platform Module, TPM)，但这些在手机和平板电脑上都很少见。

2. 凭据管理

在中心位置存储凭据称为凭据管理。鉴于各种互联网站点和服务的广泛性，每个站点和服务都有自己特定的登录要求，使用唯一的名称和密码可能是一种负担。凭据管理解决方案提供了一种安全存储大量凭据集的方法。当需要解锁数据集时，这些工具通常使用主凭据集(首选多因素)，某些凭据管理选项甚至可为应用和网站提供自动登录选项。

3. 身份验证

移动设备或移动设备上的身份验证通常相当简单，尤其是对于移动电话和平板电脑。但是，滑屏或模式访问不应被视为真正的身份验证。只要可能，请使用密码、个人身份识别码(PIN)、眼球或面部识别、扫描指纹或使用接近设备(NFC 或 RFID 环或卡)等进行身份验证。如果能正确实施，这些设备验证手段对于小偷来说是很难绕过的。如前所述，谨慎的做法是将设备验证与设备加密结合起来以阻止通过连接电缆访问存储的信息。

4. 地理位置标记

具有 GPS 支持的移动设备在拍照时，能将地理位置以纬度和经度的形式嵌入照片中，还可嵌入拍摄照片的日期时间信息。这允许潜在的攻击者(或愤怒的前任)查看来自社交网络或类似网站的照片，并确定拍摄照片的时间和地点。这种地理标记也可用于恶意目的，例如确定一个人什么时候进行正常的日常活动。

一旦标有地理标记的照片上传到互联网上，潜在的网络跟踪者可能会获得比上传者预期的更多的信息。

5. 加密

加密通常是防止未经授权访问数据的有效保护机制，无论是存储中还是在传输中。大多数移动设备提供某种形式的存储加密。如果可用，则应启用它。一些移动设备提供对通信加密的本地支持，大多数移动设备可运行附加软件(应用程序)为数据会话、语音呼叫和/或视频会议加密。

6. 应用白名单

应用程序白名单是一种安全选项，可禁止未经授权的软件执行。白名单也称为默认拒绝或隐式拒绝。在应用程序安全中，白名单会阻止任何和所有软件(包括恶意软件)执行，除非它位于预先批准的例外列表(白名单)中。这与典型的设备安全立场有很大的不同，即默认情况下允许执行，通过例外列表(也称为黑名单)拒绝执行。

由于恶意软件的增长，应用程序白名单方法是保留下来的少数选项之一，它可切实保护设备和数据。但包括白名单在内的任何安全解决方案都是不完美的。所有已知的白名单解决方案都可通过内核级漏洞和应用程序配置问题来绕过。

9.9.3 BYOD 关注点

BYOD(Bring Your Own Device，自带设备)是一项策略，允许员工将自己的个人移动设备投入工作，并使用这些设备连接，经由公司网络连接到业务资源和/或互联网。尽管 BYOD 可以提高员工士气和工作满意度，但它会增加组织的安全风险。如果 BYOD 策略是开放的，则允许任何设备连接到公司网络。并非所有移动设备都具有安全功能，因此这种策略允许不符合要求的设备进入生产网络。强制要求使用特定设备的 BYOD 策略可以降低此风险，但它反过来可能会要求公司为无法自行购买兼容设备的员工购买设备。以下各节将讨论其他许多 BYOD 问题。

BYOD 策略有多种替代方案，包括 COPE、CYOD、企业拥有和 VDI。

公司拥有个人启用(Company-Owned, Personally Enabled, COPE)指组织购买设备并将其提供给员工。然后，每个用户都可自定义设备并将其用于工作活动和个人活动。COPE 使组织可以准确选择组织网络上允许的设备——特别是可以配置为符合安全策略的设备。

自选设备(Choose Your Own Device, CYOD)指为用户提供已获准设备的列表，可从中选择要使用的设备。如果实施 CYOD，则员工可从已获准的列表(BYOD 的变体)购买自己的设备，或者公司可以为员工购买设备(COPE 的变体)。

企业拥有移动设备的战略是指公司购买符合安全策略的合规移动设备。这些设备将专门用

于公司用途，并且用户不应该在设备上执行任何个人任务。这通常要求员工携带第二个设备以供个人使用。

虚拟桌面基础设施(Virtual Desktop Infrastructure, VDI)是一种降低终端设备的安全风险和性能要求的方法，通过由用户远程访问托管在中央服务器上的虚拟机来实现。VDI 已被应用到移动设备中，并已广泛应用于平板电脑和笔记本电脑。它是一种在中央服务器上保留存储控制、获得访问更高级别的系统处理和其他资源的手段，并允许低端设备超越其硬件限制获得软件支持和服务。

这导致提出了虚拟移动基础设施(Virtual Mobile Infrastructure, VMI)，其中移动设备的操作系统在中央服务器上虚拟化。因此，传统移动设备的大多数动作和活动不再发生在移动设备本身。与使用标准移动设备平台相比，远程虚拟化使组织能获得更好的控制和安全性。还可使个人拥有的设备与 VDI 交互，而不会增加风险。这个概念需要一个专用的隔离无线网络来限制 BYOD 设备直接与公司资源进行交互，而不是通过 VDI 解决方案。

用户需要了解在工作中使用自己的设备的好处、限制和后果。阅读和签署 BYOD、COPE、CYOD 等策略，以及参加培训计划了解概况以培养合理的安全意识。

1. 数据所有权

当个人设备用于业务工作时，可能将个人数据和业务数据混为一体。有些设备支持存储分隔，但并非所有设备都能提供按数据类型隔离的功能。建立数据所有权可能很复杂。例如，如果设备丢失或被盗，公司可能希望触发远程擦除，清除设备中的所有有价值信息。但是，员工通常会对此产生抵触情绪，尤其是在有希望找到或归还设备的情况下。擦除可以删除所有业务和个人数据，这对个人可能是个重大损失——特别是如果设备最终找回，因为擦除似乎是一个过度反应。应建立明确的数据所有权策略。某些 MDM 解决方案可提供数据隔离/分隔，也支持业务数据清理，而不会影响个人数据。

有关数据所有权的移动设备策略应该解决移动设备的备份问题。业务数据和个人数据应该受到备份解决方案的保护——可以是设备上所有数据的单一解决方案，也可以是每类数据的单独解决方案。这可以降低远程擦除事件以及设备故障或损坏时数据丢失的风险。

2. 所有权支持

当员工的移动设备出现失败、故障或损坏时，谁负责设备的维修、更换或技术支持？移动设备策略应该定义公司将提供哪些支持，哪些留给个人支持，并且如果涉及服务供应商，还要考虑哪些由供应商支持。

3. 补丁管理

移动设备策略应该定义个人拥有的移动设备的补丁管理手段和机制。用户是否负责安装更新？用户应该安装所有可用的更新吗？组织是否应该在设备安装之前测试更新？是通过服务提供商更新还是通过 Wi-Fi 处理更新？是否有不能使用的移动操作系统版本？需要什么补丁或更新级别？

4. 反病毒管理

移动设备策略应规定是否要在移动设备上安装反病毒、防恶意软件和反间谍软件扫描程序。

该策略应指明建议使用哪些产品/应用，以及这些解决方案的设置。

5. 取证

移动设备策略应解决与移动设备相关的取证(forensics)和调查问题。用户需要知道，如果发生安全违规或犯罪活动，他们的设备可能也会被涉及。策略要求将从这些设备收集证据。一些证据收集过程可能具有破坏性，而且一些法律调查要求没收设备。

6. 隐私

移动设备策略应该涉及隐私和监控。当个人设备用于商业任务时，用户经常会失去在工作中使用他们的移动设备之前所享有的部分或全部隐私。员工可能需要同意对他们的移动设备进行跟踪和监控，即使不在公司财产范围和工作时间之内。在 BYOD 下使用的个人设备应被个人视为准公司财产。

7. 入职/离职(On-boarding/Off-boarding)

移动设备策略应解决个人移动设备入职和离职程序问题。移动设备入职程序包括安装安全、管理和生产应用程序，以及实施安全和高效的配置。移动设备离职程序包括正式擦除业务数据以及删除任何特定业务的应用程序。某些情况下，可以规定完整的设备擦除和恢复出厂设置。

8. 遵守公司策略

移动设备策略应明确指出：使用个人移动设备进行业务活动时，员工也要遵守公司策略。员工应将移动设备视为公司财产，因此即使在非办公场所和非工作时间也要遵守所有限制。

9. 用户接受度

移动设备策略中关于工作中使用个人设备的所有要素都需要明确和具体。对于许多用户而言，在公司政策下实施的限制、安全设置和 MDM 跟踪要比他们预期的更复杂。因此，在允许个人设备进入生产环境前，组织应该努力充分地解释移动设备策略的细节。只有在员工表示同意和接受后(通常需要签名)，才允许他们的设备进入生产环境。

10. 架构/基础设施考虑

在实施移动设备策略时，组织应评估其网络和安全设计、体系结构和基础设施。如果每个员工都携带个人设备，那么网络上的设备数量可能会翻倍。这需要计划处理 IP 分配、通信隔离、数据优先级管理、增强的入侵检测系统(IDS)/入侵预防系统(IPS)监控负载、在内部和任何互联网链路上增加的带宽消耗。大多数移动设备都支持无线，因此这可能需要一个更健壮的无线网络来处理 Wi-Fi 拥塞和干扰。移动设备策略需要考虑由此触发的额外基础设施成本。

11. 法律问题

公司律师应评估移动设备的法律问题。在执行业务任务时使用个人设备可能意味着增加了责任负担和数据泄露风险。移动设备可以让员工满意，但对组织而言，这可能不是一项有价值或具有成本效益的事情。

12. 可接受使用策略

移动设备策略应该参考公司的可接受使用策略，或者包括专注于独特问题的移动设备特定版本。随着个人移动设备在工作中的使用，信息泄露、分散注意力以及访问不适当内容的风险在不断增加。员工应该注意，工作中的主要目标是完成生产任务。

13. 机载摄像头/视频

移动设备策略需要解决带有相机的移动设备的问题。某些环境禁用任何类型的相机。这将要求移动设备不能有相机。如果允许使用相机，则应明确记录并向员工解释何时可使用和不可使用相机。移动设备可当作存储设备，向外部提供商或服务提供备用的无线连接路径，还可用于收集泄露机密信息或装备的图像和视频。

9.10 评估和缓解嵌入式设备和信息物理系统的漏洞

嵌入式系统是作为大系统的一部分而实现的计算机系统。嵌入式系统通常是围绕一组有限的特定功能设计的，这些特定功能与将其作为组件的较大产品相关。它的组件可与构成典型计算机系统的组件相同，也可能是微控制器(具有板载内存和外围端口的集成芯片)。嵌入式系统的示例包括联网的打印机、智能电视、HVAC 控制、智能电器、智能恒温器、车辆娱乐/驾驶员辅助/自动驾驶系统和医疗设备。

与嵌入式系统类似的另一个概念是静态系统(又称静态环境)。静态环境是一组不变的条件、事件和环境。从理论上讲，一旦理解，就会知道静态环境不会提供新的或令人惊讶的元素。静态 IT 环境是任何旨在保持不被用户和管理员改变的系统。目标是防止(或至少减少)用户变更降低安全性或影响功能操作的可能性。

在技术方面，静态环境是为特定需求、能力或功能配置的应用程序、操作系统、硬件集或网络，然后设置为保持不变。尽管使用了术语“静态”，其实并没有真正的静态系统。硬件故障、硬件配置更改、软件错误、软件设置更改或漏洞利用总可能改变环境，从而导致非预期的操作参数或实际的安全入侵。

9.10.1 嵌入式系统和静态系统的示例

支持网络的设备是指具有本机联网功能的任何类型的便携式或非便携式设备。这通常假设所讨论的网络是无线类型的网络，主要是由移动通信公司提供的网络。但它也可指连接到 Wi-Fi 的设备(特别是当它们可以自动连接时)、从无线电信服务(例如移动热点)共享数据连接的设备以及具有 RJ-45 插孔的设备(以接收用于有线连接的标准以太网电缆)。支持联网的设备包括智能手机、移动电话、平板电脑、智能电视、机顶盒或 HDMI 桥流媒体播放器(如 Roku 播放器、亚马逊 Fire TV 或谷歌 Android TV/Chromecast)、联网的打印机、游戏系统等。

注意：

某些情况下，支持联网的设备可能包括支持蓝牙、NFC 和其他基于无线电的连接技术的设备。此外，一些供应商提供的设备可为自身没有联网功能的设备添加网络连接的功能。这些附加设备本身可能被视为支持网络的设备(或更具体地说，是能支持网络的设备)，并且它们组合成的增强设备可能被视为支持联网的设备。

网络物理系统指提供计算手段来控制物理世界中的某些东西的设备。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多关注于物理世界的结果而非计算方面。网络物理设备和系统本质上是机器人和传感器网络中的关键元素。基本上，任何可导致在现实世界中发生运动的计算设备都被认为是机器人元件，而能检测物理条件(如温度、光、运动和湿度)的任何设备都是传感器。网络物理系统的示例包括提供人体增强或辅助功能的假肢、车辆中的防碰撞、空中交通管制协调、机器人手术的精确性、危险条件下的远程操作，还包括车辆、设备、移动设备和建筑物的节能。

网络物理系统、嵌入式系统和网络设备的另一个扩展是物联网(IoT)。如前所述，物联网是可通过互联网相互通信或与控制台通信的设备集合，以便影响和监控现实世界。物联网设备可能被标记为智能设备或智能家居设备。在办公楼中发现的许多工业环境控制理念正在为小型办公室或个人住宅提供更多消费者可用的解决方案。物联网不仅限于静态定位设备，还可与陆地、空中或水上交通工具或移动设备联合使用。物联网设备通常是静态系统，因为它们只能运行制造商提供的固件。

大型机是高端计算机系统，用于执行高度复杂的计算并提供批量数据处理。较早的大型机可能被视为静态环境，因为它们通常围绕单个任务设计或支撑单个关键任务的应用程序。这些配置没有提供显著的灵活性，但它们确实实现了高稳定性和长期操作。许多大型机能够运行数十年。

现代大型机更灵活，通常用于提供高速计算能力以支持众多虚拟机。每个虚拟机都可用于托管一个独特的操作系统，从而支持各种应用程序。如果现代大型机实现为提供对一个 OS 或应用程序的固定或静态支持，则可将其视为静态环境。

游戏控制台(无论是家庭系统还是便携式系统)都是静态系统的潜在例子。游戏机的操作系统通常是固定的，只有在供应商发布升级系统时才会更改。此类升级通常是 OS、应用程序和固件改进的混合。虽然游戏机功能通常集中在玩游戏和媒体上，但现代游戏机可能为一系列改善和第三方应用程序提供支持。应用支持越灵活，开放性越强，静态系统就越少。

车载计算系统可包括用于监控发动机性能并优化制动、转向和悬架的部件，但还可包括与驾驶、环境控制和娱乐相关的仪表板元件。早期的车载系统是静态环境，很少或根本没有为业主/司机提供调整或更改的能力。现代车载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应用程序。

9.10.2 保护嵌入式和静态系统的方法

大多数嵌入式和静态系统的设计重点是成本最小化和实现非常特别的功能，这通常会导致安全性降低以及升级或修补程序出现问题。由于嵌入式系统控制着物理世界中的行为方式，因此安全漏洞可能给人员和财产造成伤害。

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。虽然它们可能没有像通用计算机那样广泛的攻击面，也没有面临那么多风险，但它们仍然需要适当的安全治理。

1. 网络分段

网络分段涉及控制联网设备之间的流量。完整(或物理)的网络分段是指当网络与所有外部通信隔离时，因此只能在分段网络内的设备之间进行事务处理。你可使用虚拟局域网(VLAN)或通过其他流量控制手段对交换机强制执行逻辑网络分段，包括 MAC 地址、IP 地址、物理端口、TCP 端口、UDP 端口、协议或应用程序筛选、路由和访问控制管理。网络分段可用于隔离静态环境，以防止更改和/或漏洞影响静态环境。

2. 安全层

当具有不同分类或敏感级别的设备被组合在一起并与其他具有不同级别的组隔离时，就存在安全层。这种隔离可以是绝对的或单向的。例如，较低级别可能不能启动与较高级别的通信，但较高级别可启动与较低级别的通信。隔离也可以是逻辑的或物理的。逻辑隔离要求在数据和数据包上使用分类标签，这必须得到网络管理、操作系统和应用程序的慎重对待和强制执行。物理隔离需要在不同安全级别的网络之间实现网络分段或空间隔断。

3. 应用防火墙

应用程序防火墙是一种设备、服务器附件、虚拟服务或系统过滤器，它为服务和所有用户定义了一组严格的通信规则。它的目的是作为一个特定于应用程序的服务器端防火墙，以防止特定于应用程序的协议和有效负载攻击。

网络防火墙是一种硬件设备，通常称为装置，专为通用网络过滤而设计。网络防火墙旨在为整个网络提供广泛保护。

这两种类型的防火墙都很重要，并且许多情况下可能是相关的。每个网络都需要网络防火墙。许多应用服务器需要应用防火墙。但是，使用应用程序防火墙通常不会否定对网络防火墙的需求。你应该结合使用这两个防火墙，让它们相互补充，而不要将它们看作竞争性解决方案。

4. 手动更新

应该在静态环境中使用手动更新，以确保仅执行经过测试和授权的更改。使用自动更新系统将允许未经测试的更新引入未知的安全性降低。

5. 固件版本控制

与手动软件更新类似，严格控制静态环境中的固件非常重要。固件更新应该仅在测试和评审后手动、降低实施。对固件版本控制的监督应侧重于维护稳定的操作平台，同时最大限度地减少停机时间或损害的风险。

6. 包装器

包装器(Wrappers)用于封装或包含其他内容。在安全社区中，包装器与特洛伊木马恶意软件有关是众所周知的。这种包装器用于将一个良性的主机与恶意负载组合在一起。

包装器也用作封装解决方案。某些静态环境可能配置为拒绝更新、更改或安装软件，除非

它们是通过受控通道引入的。这个受控通道可以是特定的包装器。包装器可以包括完整性和身份验证特性，以确保仅将预期的和已授权的更新应用于系统。

7. 监控

即使是嵌入式和静态系统，也应监控性能、违规、合规性和运行状态。其中一些类型的设备可以执行设备自身的监视、审计和日志记录，而其他设备可能需要外部系统来收集活动数据。应该监控组织内的所有设备、装备和计算机，以确保高性能、最短的宕机时间以及检测和阻止违规和滥用行为。

8. 控制冗余和多样性

与任何安全解决方案一样，依赖单一安全机制是不明智的。纵深防御在文字上或理论上的同心圆或层中使用多种类型的访问控制。这种分层安全形式有助于组织避免单一的安全状态。单一的心态是相信单一的安全机制能充分地提供全部所需的安全性。通过具有安全控制的冗余性和多样性，静态环境可避免单个安全功能失败的陷阱；环境有几个机会可以转移、拒绝、检测和阻止任何威胁。不幸的是，没有安全机制是完美的。每个单独的安全机制都会有缺陷或绕过方法，迟早会被黑客发现和利用。

9.11 基本安全保护机制

操作系统内对安全机制的需求可以归结为一个简单事实：软件不应该被信任。第三方软件本质上都是不可信赖的。无论来自谁或来自何处。这并不是说所有软件都是有害的。相反，这是一种保护态度：因为所有第三方软件都是由 OS 创建者之外的其他人编写的，该软件可能会导致问题。因此，将所有非 OS 软件视为具有潜在破坏性，允许 OS 通过使用软件管理保护机制来防止许多灾难性事件的发生。操作系统必须采用保护机制来保持计算环境的稳定性并使进程间彼此隔离。如果没有这些努力，数据的安全性永远是不可靠的，甚至是不可能的。

计算机系统设计人员在设计安全系统时应该遵循一些通用的保护机制。这些原则是管理安全计算实践的更通用安全规则的特定实例。在开发的最初阶段就将安全性引入系统中，将有助于确保整体安全架构的成功和可靠。下面将从两个方面讨论：技术机制和策略机制。

9.11.1 技术机制

技术机制是系统设计人员在其构建系统时可使用的控件。我们将研究 5 种机制：分层、抽象、数据隐藏、进程隔离和硬件分隔。

1. 分层

通过分层过程，可实现与用于操作模式的环模型(前面讨论过)类似的结构，并将其应用于每个操作系统进程。它将过程中最敏感的功能置于核心，由一系列逐渐扩大的同心圆所包围，这些圆带有相应的逐渐降低的敏感度级别(使用稍微不同的方法解释，有时也会使用术语“上层”和“下层”，其中从下层上升到上层时，安全性和特权会降低)。在 OS 体系结构的讨论中，受

保护环的概念很常见，但它并不是唯一的。还有其他方法可以表示相同的基本思想，用“级别”来代替“环”。在这样的系统中，最高级别的特权最高，而最低级别的特权最低。

“级别”与“环”的比较

保护环概念的许多特征和限制也适用于多层或多级系统。假设有一座高层公寓楼。廉租公寓通常位于较低楼层。当你到达中间楼层时，公寓通常更大，并且视野更好。最后，顶层(或最高的几层)是最奢华和最昂贵的(通常被认为是顶层公寓)。通常情况下，如果你住在大楼的廉租公寓中，你将无法乘坐高于廉租公寓最高楼层的电梯。如果你是居住在中层的公寓，除了顶层公寓外，你可以乘坐电梯到任何楼层。如果你是顶层公寓居民，你可乘坐电梯去任何你想去的楼层。你也可以在办公楼和酒店找到这种楼层限制系统。可能还有一部电梯直接在最低层和顶层之间运行，从而绕过所有较低层。但是，如果直达电梯遭到破坏，则其他保护层也将失去价值。

分层或多级系统的顶部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。在保护和访问概念方面，级别、层和环是类似的。术语域(即具有单一特征的客体的集合)也是通用的。

层与层之间的通信只能通过定义明确的特定接口进行，以提供必要的安全性。所有来自外部(不太敏感)层的入站请求在被允许之前都要经过严格的身份验证和授权检查(如果未通过此类检查，则会被拒绝)。使用安全分层类似于使用安全域和基于格的安全模型，因为对特定主体和客体的安全和访问控制是与特定层和特权关联的，当从外层向内层移动时，访问权限会增加。

事实上，单独的层只能通过旨在维护系统安全性和完整性的特定接口相互通信。尽管不太安全的外层依赖于来自更安全内层的服务和数据，但它们只知道这些层的接口，并不知道这些内层的内部结构、特征或其他细节。这样层的完整性得以保持，内层既不知道也不依赖于外层。在任何一对层之间无论存在何种安全关系，都不能篡改另一层(这样可以保护每一层免受任何其他层的篡改)，最后，外层不能违反或覆盖内层强制执行的任何安全策略。

2. 抽象

抽象是面向对象编程领域的基本原则之一。正如“黑箱”理论所说：对象(或操作系统组件)的用户不一定需要知道对象如何工作的细节；用户只需要知道使用对象的正确语法以及作为结果返回的数据类型(即如何发送输入和接收输出)。这往往涉及对数据或服务的中介访问，例如用户模式应用程序使用系统调用来请求管理员模式的服务或数据(根据请求者的凭据和权限可以授予或拒绝此类请求)而不是获得直接无中介的访问。

抽象应用于安全性的另一种方式是引入对象组，有时称为类，其中访问控制和操作权限被分配给对象组而不是基于每个对象。这种方法允许安全管理员轻松地定义和命名组(名称通常与工作角色或职责相关)，并有助于简化权限和特权的管理(当向类添加对象时，就已经赋予对象权限和特权，而不必分别管理每个对象的权限和特权)。

3. 数据隐藏

数据隐藏是多级安全系统中的一个重要特征。它确保在一个安全级别存在的数据对于以不同安全级别运行的进程是不可见的。数据隐藏背后的关键概念是，希望确保那些不需要知道在

一个级别访问和处理数据所涉及细节的人，无法秘密或非法地了解和查看这些细节。从安全角度看，数据隐藏依赖于将客体放在安全容器中，该容器与主体占用的安全容器不同，对不需要了解它们的容器隐藏客体的详细信息。

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单独的内存空间。它还要求操作系统强制执行这些边界，从而阻止一个进程读取或写入属于另一个进程的数据。使用这种技术有两个主要优点：

- 它可防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。
- 它保护进程的完整性。如果没有这样的控制，设计不佳的进程可能出现混乱并将数据写入分配给其他进程的内存空间，从而导致整个系统变得不稳定，而不仅仅影响错误进程的执行。在更具恶意的情况下，进程可尝试（甚至可能成功）读取或写入其范围之外的内存空间，侵入或攻击其他进程。

许多现代操作系统通过在每个用户或每个进程的基础上实现虚拟机来满足进程隔离的需求。虚拟机向用户或进程提供处理环境，包括内存、地址空间和其他关键系统资源和服务，允许该用户或进程表现得好像具有对整个计算机的唯一独占访问权一样。这允许每个用户或进程独立操作，而不需要识别可能在同一机器上同时活动的其他用户或进程。作为对操作系统提供的系统中介访问的一部分，它以用户模式映射虚拟资源和访问，以便使用监督模式调用来访问相应的真实资源。这不仅使程序员更轻松，还保护个人用户和进程不受其他用户和进程影响。

5. 硬件分隔

硬件分隔的目的与进程隔离类似，它阻止了对属于不同进程/安全级别的信息的访问。主要区别在于硬件分隔通过使用物理硬件控制，而不是操作系统强加的逻辑进程隔离控制来满足这些要求。这种实现很少，并且它们通常仅限于国家安全实施，其中额外的成本和复杂性被所涉及信息的敏感性和未授权访问或泄露的固有风险所抵消。

9.11.2 安全策略和计算机架构

安全策略指导组织中的日常安全运营、流程和过程，也在设计和实现系统时发挥着重要作用。无论系统是完全基于硬件、完全基于软件还是两者的组合，都同样适用。这种情况下，安全策略的作用是告知和指导特定系统的设计、开发、实现、测试和维护。因此，这种安全策略要紧紧围绕具体的实施工作而展开（虽然它可能由其他类似的工作改编而来，但应尽可能准确、完整地反映当前的工作目标）。

对于系统开发人员，安全策略最好以文档的形式出现，该文档定义了一组描述系统应该如何管理、保护和分发敏感信息的规则、实践和过程。阻止信息从较高安全级别流向较低安全级别的安全策略称为多级安全策略。在开发系统时，应该设计、构建、实施和测试安全策略，因为它涉及所有适用的系统组件或元素，包括以下任何一个或全部：物理硬件组件、固件、软件以及组织如何与系统交互并使用系统。总之，在项目的整个生命周期都需要考虑安全性。如果仅在最后才实施安全，通常都会失败。

9.11.3 策略机制

与任何安全计划一样，也应建立安全策略机制。这些机制是基本的计算机安全原则的扩展，但本节中描述的应用程序是特定于计算机体系结构和设计领域的。

1. 最小特权原则

第13章讨论最小特权的一般安全原则以及它如何应用于计算系统的用户。该原理对于计算机和操作系统的应用也很重要，尤其是将其应用于系统模式时。在设计操作系统进程时，应该始终确保它们尽可能以用户模式运行。在特权模式下执行的进程数量越多，恶意个人可利用以获得对系统的监督访问的潜在漏洞数量就越多。通常，最好使用API来请求监督模式服务，或者当用户模式应用请求时将控制权交给可信、受到良好保护的监督模式进程，而不是将这些程序或进程一起提升到监督模式。

2. 特权分离

特权分离原则建立在最小特权原则之上。它需要使用粒度化的访问权限：也就是说，每种类型的特权操作都有不同的权限。这允许设计者授予一些进程来执行某些监督功能的权限，而不允许它们不受限制地访问系统。它还允许对照访问控制来检查对服务或资源访问的各个请求，并基于发出请求的用户的身份或用户所属的组成用户的安全角色，授予或拒绝这些请求。

可将职责分离视为对管理员应用最小特权原则。在大多数中型到大型组织中，有许多管理员，每个管理员都有不同的指定任务。因此，通常很少或没有个人管理员需要所有环境或者基础设施的完全访问权限。例如，用户管理员不必具有重新配置网络路由、格式化存储设备或执行备份功能的权限。

职责分离也是用于防止在分配访问权限和工作任务时发生利益冲突的工具。例如，那些负责编码的人员不应该同时负责测试和编写代码。同样，那些负责账户支付工作的人员不能同时负责账户的收款工作。有许多这样的工作或任务冲突，可以通过适当的职责分离来实现安全的管理。

3. 问责制

问责制(accountability)是任何安全设计的重要组成部分。许多高安全性系统包含强制对特权功能进行个人问责的物理设备(例如纸和笔记录的访问者日志和不可修改的审计踪迹)。但是，一般而言，此类功能依赖于系统监视资源和配置数据的活动和交互的能力，并保护生成的日志免受不必要的访问或更改，以便它们提供该系统上的每个用户(包括具有高级别权限的管理员或其他可信任的个人)准确可靠的历史记录。除了需要可靠的审计和监控系统来支持问责制外，还必须有一个灵活的授权系统和无懈可击的身份验证系统。

9.12 常见的架构缺陷和安全问题

没有安全架构是完整且完全安全的。每个计算机系统都有弱点和漏洞。安全模型和体系结

构的目标是尽可能多地解决已知的弱点。基于这一事实，必须采取纠正措施来解决安全问题。下面介绍与安全体系结构漏洞相关的影响计算机系统的一些常见安全问题。你应该了解每个问题以及它们是如何降低系统的整体安全性的。一些问题和缺陷相互重叠，并以创造性的方式攻击系统。虽然以下讨论涵盖了最常见的缺陷，但该列表并非详尽无遗。攻击者非常聪明。

9.12.1 隐蔽通道

隐蔽通道是一种用于在通常不用于通信的路径上传递信息的方法。由于此路径通常不用于通信，因此它可能不受系统正常安全控制的保护。使用隐蔽通道提供了一种违反、绕过或损害安全策略且不会被检测到的手段。隐蔽通道是安全架构漏洞的重要示例之一。

正如你可能想象的那样，隐蔽通道与公开通道相反。公开通道是已知的、预期的、已授权的、经过设计的、受监视的和受监控的通信方法。

有两种基本类型的隐蔽通道：

时间隐蔽通道 时间隐蔽通道通过改变系统组件的性能或以可预测的方式修改资源的时间来传达信息。使用时间隐蔽通道通常是秘密地传输数据的方法，并且非常难以检测。

存储隐蔽通道 存储隐蔽通道通过将数据写入公共存储区域来传送信息，其中另一个进程可以读取它。在评估软件的安全性时，请努力寻找那些写入其他进程可以读取的任何内存区域的进程。

两种类型的隐蔽通道都依赖于使用通信技术与其他未经授权的主体交换信息。因为隐蔽通道超出了正常数据传输环境，所以检测它可能很困难。对任何隐蔽通道活动最好的防御措施就是实施审核和分析日志文件。

9.12.2 基于设计或编码缺陷的攻击和安全问题

某些攻击可能源于糟糕的设计技术、有问题的实现实践和过程或者糟糕或不充分的测试。有些攻击可能是故意的设计决策导致的，如代码中包含的用于绕过访问控制、登录的特殊入口点，或者开发过程中添加到代码中的其他安全检查，在代码投入生产的时候没有去除。由于显而易见的原因，这些出口点被恰当地称为后门，因为它们通过设计绕过了安全措施(稍后的“维护钩子和特权程序”一节中介绍)。需要进行广泛的测试和代码审查才能发现这种隐蔽的访问方式，这些方法在开发的最后阶段很容易删除，但在测试和维护阶段却很难检测到。

虽然功能测试对于商业代码和应用程序来说很常见，但是仅在过去几年中，对安全问题的单独测试才获得了关注和可信度，这主要得益于广泛宣传的病毒和蠕虫攻击、SQL 注入攻击、跨站脚本攻击以及偶尔对广泛使用的公共网站的损毁或破坏。你可通过 https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf 查看 OWASP 十大 Web 应用程序安全风险报告。

接下来将介绍安全架构的常见攻击源或漏洞，这些漏洞可能归因于设计、实现、预发布代码清理或彻底的编码错误等的失败。虽然它们是可以避免的，但是发现和修复这些缺陷需要从项目开发之初就进行有安全意识的严格设计，并且需要花费额外的时间和精力进行测试和分析。这有助于解释软件安全的可悲状态，但它并不能成为借口！

人类永远不会编写出绝对安全(没有缺陷)的代码。在整个应用开发周期中实施的源代码分

析工具将最大限度地减少生产版本中缺陷的数量，并且在生产发布之前发现的缺陷的处置成本也会比较低。代码审查和测试的概念将在第15章中介绍。

1. 可信恢复

当一个未预料的系统崩溃发生并随后恢复时，可能会有两个危及其安全控制的机会。许多系统将安全控制卸载作为其关闭过程的一部分。可信恢复可确保在发生崩溃时所有安全控制保持完整无缺。在可信恢复期间，系统确保在禁用安全控制情况下不会有访问的机会。即使是恢复运行阶段，所有控件都完好无损时也不会有访问的机会。

例如，假设一个系统崩溃了，而数据库事务正在往磁盘中写数据，而且这个数据库分类为最高机密。一个未受保护的系统可能允许未经授权的用户在将临时数据写入磁盘之前访问该临时数据。而支持可信恢复的系统可确保即使在崩溃期间也不会发生数据保密性违规。这个过程需要仔细规划，处理系统故障的过程也应当就详明的。虽然自动恢复程序可能构成整个恢复的一部分，但仍可能需要人工干预。显然，如果需要这样的人工操作，对执行恢复的人员进行适当的识别和身份验证同样重要。

2. 输入和参数检查

最臭名昭著的安全漏洞之一是缓冲区溢出。当程序员未能充分验证输入数据时，尤其是当他们没有对软件接受的输入数据量施加限制时，就会发生这种漏洞。由于此类数据通常存储在输入缓冲区中，因此当超出缓冲区的正常最大尺寸时，额外的数据就称为溢出。因此，当有人试图提供恶意指令或代码作为程序输入的一部分时产生的攻击类型称为缓冲区溢出。遗憾的是，在许多系统中，这种溢出数据通常由处于高特权级别的遭受攻击的系统直接执行，或者在接受这个输入的进程具有的任何特权级别上执行。对于几乎所有类型的操作系统，包括Windows、Unix、Linux和其他操作系统，缓冲区溢出都会暴露出一些最明显和最深刻的机会，可以对任何已知安全漏洞进行破坏和攻击。

负责缓冲区溢出漏洞的责任方始终是程序员，其代码允许未净化或非净化的输入。尽职尽责的程序员可以完全消除缓冲区溢出，但前提是程序员在将所有输入和参数存储到任何数据结构之前检查所有输入和参数(并限制可以提供多少数据作为输入)。正确的数据验证是消除缓冲区溢出的唯一方法。否则，发现缓冲区溢出会导致常见的关键安全更新模式，必须应用于受影响的系统以关闭攻击点。

3. 维护钩子和特权程序

维护钩子是进入系统的入口点。只有系统开发人员才知道。这样的入口点也称为后门。虽然维护钩子的存在明显违反了安全策略，但它们仍然在许多系统中出现。后门的最初目的是为了维护原因或者当常规访问被意外地禁用时，可保证提供对系统的访问。问题是这种类型的访问绕过了所有安全控制，并且知道后门存在的任何人都可以自由地访问。必须明确禁止此类入口点并监视审核日志，以发现可能表明未经授权的管理员访问的任何活动。

另一个常见的系统漏洞是执行程序的实践，其执行期间的安全级别进行了提升。必须仔细编写和测试此类程序，以便它们不允许任何退出和/或入口点存在，以防主体具有更高的安全等级。确保所有在高安全级别运行的程序只能由适当的用户访问，并且对他们进行加固以防止滥用。一个很好的例子是 Unix/Linux OS 环境中的 root 所有的可写可执行脚本。这个重大的安全

漏洞经常被忽视：任何人都可以修改脚本，它将在 root 用户上下文中执行，允许创建用户，从而导致后门访问。

4. 增量攻击

某些形式的攻击以缓慢、渐进的增量发生，而不是通过明显或可识别的尝试来破坏系统安全性或完整性。两种这样的攻击形式是数据欺骗(data diddling)和 salami 攻击。

当攻击者获得对系统的访问权并在存储、处理、输入、输出或事务期间对数据进行小的、随机的或增量的更改，而不是明显地更改文件内容或损坏或删除整个文件时，就会发生数据欺骗。除非文件和数据受加密保护，或者除非每次读取或写入文件时例行地执行和应用某种完整性检查(例如校验和或消息摘要)，否则很难检测到这些更改。加密文件系统、文件级加密技术或某种形式的文件监控(包括由应用程序执行的完整性检查，例如 Tripwire 和其他文件完整性监控[FIM]工具等)通常可提供足够的保证，确保没有数据欺骗正在进行。通常认为由内部人员发起的数据欺骗攻击比外部人员(即外部入侵者)更频繁。显而易见的是，由于数据欺骗是一种改变数据的攻击，因此它被认为是主动攻击。

所有已发表的报道都说，salami 攻击更神秘。salami 攻击是指对账户中的资产或具有财务价值的其他记录系统性地进行削减，其中非常小的金额会定期和例行地从余额中扣除。比方说，这种攻击可能被解释为每次将香肠放入切片机时，只要付费客户访问，就会从香肠上偷取一个非常薄的切片。实际上，尽管没有关于此类攻击的文档示例，但大多数安全专家承认 salami 攻击是可能的，特别是当组织内部人员可能参与时。只有通过适当的职责分离和对代码的适当控制，组织才能完全防止或消除这种攻击。设置金融交易监控器以跟踪非常小的资金或其他有价物品的转移，应该对检测此类活动有帮助；定期向员工通报的做法应该有助于阻止这种攻击的尝试。



注意：

如果你想要以一种有趣的方法来了解 salami 攻击或 salami 技术，请观看电影《办公室空间》《运动鞋》和《超人 III》，你也可以阅读《连线》(Wired)杂志 2008 年发表的一篇关于分析此类攻击的文章：<https://www.wired.com/2008/05/man-allegedly-b/>。

9.12.3 编程

我们已经提到了编程中最大的缺陷：缓冲区溢出，如果程序员未能检查或净化输入数据的格式和/或大小，就会发生缓冲区溢出。程序还存在其他潜在缺陷。任何不能正常处理任何异常的程序都有进入不稳定状态的危险。在程序提高安全级别以执行正常任务后，可以巧妙地使程序崩溃。如果攻击者成功地使程序在正确的时间崩溃，他们可以获得更高的安全级别并导致对系统的保密性、完整性和可用性的破坏。

所有直接或间接执行的程序必须经过全面测试，以符合安全模型。确保安装了所有软件的最新版本，并了解任何已知的安全漏洞。由于每种安全模型和每种安全策略都不同，因此必须确保你执行的软件不超过你允许的权限。编写安全代码很困难，但它肯定可能的。确保你使用的所有程序在设计时都考虑了安全问题。有关代码评审和测试的更多信息，请参阅第 15 章。

9.12.4 计时、状态改变和通信中断

计算机系统以严格的精度执行任务。计算机擅长执行可重复的任务。攻击者可以根据任务执行的可预测性来开展攻击。一个算法的常见事件顺序是检查资源是否可用，然后在允许的情况下访问它。检查时间(Time Of Check, TOC)是主体检查客体状态的时间。在返回客体进行访问之前，可能需要做出几个决定。当决定访问该客体时，该过程在使用时间(Time Of Use, TOU)访问它。TOC 和 TOU 之间的差异有时足够大，以至于攻击者可以根据自己的需要用另一个客体替换原始客体。检查时间到使用时间(Time Of Check to Time Of Use, TOCTTOU)攻击通常称为竞争条件，因为在使用之前攻击者正在与合法进程竞争以替换客体。

一个经典的TOCTTOU攻击是：数据文件在其身份被验证之后且在读取数据之前被替换了。通过将一个真实的数据文件替换为攻击者选择和设计的另一个文件，攻击者可采用多种方式控制程序的执行。当然，攻击者必须深入了解受攻击的程序和系统。

同样，当资源状态或整个系统发生变化时，攻击者可以尝试在两个已知状态之间采取行动。通信中断也给攻击者提供了可能试图攻击的短暂停窗口。每当对资源进行操作前都要先检查资源的状态时，在检查和操作之间的短暂停中都存在着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予以解决。TOCTTOU 攻击、竞争条件攻击和通信中断被称为状态攻击，攻击针对的是时间、数据流控制和从一个系统状态到另一个系统状态的转换。

9.12.5 技术和过程集成

评估和理解系统架构中的漏洞非常重要，尤其是在技术和过程集成方面。由于在制作新的和独特的业务功能的过程中，多种技术和复杂流程相互交织在一起，因此经常出现新的问题和安全隐患。随着系统的集成，应该关注潜在的单点故障以及面向服务的体系结构(SOA)中浮现出的弱点。SOA 使用现有独立的且不同的软件服务构建新的应用程序或功能。最终的应用程序通常是个新应用；因此，它的安全问题是未知的、未经测试的和未保护的。所有新的部署，特别是新的应用程序或功能，在被允许进入生产网络或公共互联网之前，需要进行彻底审查。

9.12.6 电磁辐射

因为计算机硬件是由各种电子元件构成的，许多计算机硬件设备在正常操作期间都会发射电磁(Emit Electromagnetic, EM)辐射。与其他计算机或外围设备通信的过程中产生的电磁波可以被拦截。通过拦截和处理来自键盘和计算机监视器的电磁辐射，甚至可重新创建键盘输入或监视器输出的数据。你还可在数据通过网段时被动地检测和读取网络数据包(即实际上不用电缆连接)。这些辐射泄漏可能会导致严重的安全问题，但通常很容易解决。

消除电磁辐射拦截的最简单方法是通过电缆屏蔽或导管减少辐射，并通过应用物理安全控制来阻止未经授权的人员和设备过于靠近设备或电缆。通过降低信号强度并增加敏感设备周围的物理缓冲区，可以大大降低信号拦截的风险。

如前所述，有几种 TEMPEST 技术可防止 EM 辐射窃听。这些包括法拉第笼、干扰或噪音发生器和控制区。法拉第笼是一种特殊外壳，可用作 EM 容器。当使用法拉第笼时，没有 EM

信号可以进入或离开封闭区域。干扰或噪声发生器的思想是：当干扰太大时很难或不可能检索到某个信号。因此，通过广播自己的干扰，可以防止不希望的 EM 拦截。此概念的唯一问题是必须确保干扰不会影响你自己设备的正常运行。确保这一点的一种方法是使用控制区，这就是用于阻止故意广播干扰的法拉第笼。例如，如果你想在办公室的几个房间内使用无线网络但不允许在其他地方使用无线网络，则可将这些房间封装在一个法拉第笼中，然后在控制区外部放置几个噪声发生器。这将允许指定房间内进行正常的无线网络连接，但完全阻止在指定区域之外的任何地方正常使用和窃听。

9.13 本章小结

设计安全计算系统是一项复杂的任务，许多安全工程师把他们的全部职业生涯都献给了理解信息系统的最深层的工作并确保支持在当前环境中安全运行所需的核心安全功能。许多安全专业人员不一定需要对这些原则有深入的了解，但他们至少应该对这些基本原理有宽泛的理解，以推动增强组织内部安全性的过程。

这种理解始于对硬件、软件和固件的调查以及这些部分如何融入安全难题中。了解通用的计算机和网络组织、体系结构和设计的原理非常重要，包括寻址(物理的和符号的)、地址空间和内存空间之间的区别以及机器类型(真实、虚拟、多状态、多任务、多程序、多处理、多处理器和多用户)。

此外，安全专业人员必须充分了解运行状态(单一状态、多状态)，操作模式(用户模式、监管模式、特权模式)，存储类型(主存储、辅助存储、真实存储器、虚拟存储器、易失性存储器、非易失性存储器、随机存取、顺序存取)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、问责制)。

无论一个安全模型多么复杂，都会存在攻击者可以利用的漏洞。有些缺陷，如缓冲区溢出和维护钩子，是由程序员引入的，而另外一些缺陷，如隐蔽通道，则是架构设计问题。重要的是要了解这些问题的影响，并在适当的时候修改安全体系结构以进行弥补。

9.14 考试要点

能够解释多任务、多线程、多处理和多程序设计之间的差异。多任务处理是在计算机上同时执行多个应用程序，并由操作系统管理。多线程允许在单个进程中执行多个并发任务。多处理使用多个处理器来提高计算能力。多道程序设计类似于多任务处理，但在大型机系统上进行，需要特定的编程。

了解单一状态处理器和多状态处理器之间的差异。单一状态处理器一次只能在一个安全级别运行，而多状态处理器可同时在多个安全级别运行。

描述美国联邦政府批准的用于处理机密信息的四种安全模式。专用模式要求所有用户对存储在系统上的所有信息都有适当的许可、访问权限、“知其所需”要求。系统高级模式消除了“知其所需”的要求。分隔模式消除了“知其所需”的要求和访问权限要求。多级模式消除了所有三个要求。

解释大多数现代处理器使用的两种操作模式。用户应用程序在称为用户模式的有限指令集中运行。操作系统在特权模式下执行受控操作，也称为系统模式、内核模式和监管模式。

描述计算机使用的不同类型的内存。ROM 是非易失性的，不能由最终用户写入。最终用户只能将数据写入 PROM 芯片一次。可通过使用紫外光擦除 EPROM/UVEPROM 芯片，然后写入新的数据。EEPROM 芯片可以用电流擦除，然后写入新的数据。RAM 芯片是易失性的，当计算机断电后其内容会丢失。

了解内存组件相关的安全问题。存储器组件存在一些安全问题：断电后数据可能保留在芯片上，并且控制多用户系统中的存储器访问。

描述计算机使用的存储设备的不同特征。主存储器与内存相同。辅助存储器由磁性、闪存和光学介质组成，在 CPU 可使用数据之前必须先将其读入主存储器。随机存取存储设备可以在任何点读取，而顺序存取设备需要在访问所需位置之前扫描物理存储的所有数据。

了解关于辅助存储设备的安全问题。关于辅助存储设备存在三个主要的安全问题：可移动介质可用来窃取数据，必须应用访问控制和加密来保护数据，即使在文件删除或介质格式化之后数据也可以保留在介质上。

理解输入和输出设备可能带来的安全风险。输入输出设备可能受到偷听和窃听，用于将数据带出组织，或用于创建未经授权的、不安全的进入组织系统和网络的入口点。准备好识别并缓解这些漏洞。

理解固件的用途。固件是存储在 ROM 芯片上的软件。在计算机层面，它包含启动计算机所需的基本指令。固件还可用于诸如打印机之类的外围设备中，为其提供操作指令。

能够描述进程隔离、分层、抽象、数据隐藏和硬件分隔。进程隔离确保各个进程只能访问自己的数据。分层在一个过程中创建了不同的安全领域，并限制了它们之间的通信。抽象为程序员创建了“黑盒”接口，不必了解算法或设备的内部工作原理。数据隐藏可防止从不同的安全级别读取信息。硬件分隔使用物理控件强制执行进程隔离。

理解安全策略如何推动系统设计、实施、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、实施、测试和维护。

理解云计算。云计算是一种流行的术语，是计算的概念，指的是通过网络连接在其他地方而不是本地执行处理和存储的计算概念。云计算通常被认为是基于互联网的计算。

理解与云计算和虚拟化相关的风险。云计算和虚拟化，特别是结合使用时，会产生严重风险。一旦敏感、机密或私有数据离开了组织的范围，也就离开了组织安全策略和组合的基础设施所给予的保护。云服务供应商及其人员可能不遵守与你的组织相同的安全标准。

理解虚拟机管理程序。虚拟机管理程序（也称为虚拟机监视器（VMM））是创建、管理和操作虚拟机的虚拟化组件。

理解 Type-I 虚拟机管理程序。Type-I 虚拟机管理程序是原生或裸机管理程序。在此配置中，没有主机操作系统；相反，虚拟机管理程序直接安装到通常主机操作系统安装的硬件上。

Type-II 虚拟机管理程序。Type-II 虚拟机管理程序是托管管理程序。在这种配置中，在硬件上安装一个标准的常规 OS，然后将虚拟机管理程序作为一个软件应用程序安装。

定义 CASB。云访问安全代理（CASB）是一种实施安全策略的解决方案，可以在本地安装也可以基于云。

理解 SECaaS。安全即服务（SECaaS）是一个云提供商概念，其中通过在线实体或由在线实体向组织提供安全性。

理解智能设备。智能设备是一系列移动设备，通常通过安装应用程序为用户提供大量的自定义选项，并可利用设备上或云端的人工智能(AI)处理。

理解 IoT。物联网(IoT)是一个新的子类别，甚至是一类新的智能设备，它们通过互联网连接，以便为家庭或办公室环境中的传统或新装置或设备提供自动化、远程控制或 AI 处理。

理解移动设备安全。设备安全性涉及可用于移动设备的一系列潜在安全选项或功能。并非所有便携式电子设备(PED)都具有良好的安全功能。PED 安全功能包括全设备加密、远程擦除、锁定、锁屏、GPS、应用控制、存储分隔、资产跟踪、库存控制、移动设备管理、设备访问控制、可移动存储以及关闭不使用的功能。

理解移动设备应用安全。需要保护移动设备上使用的应用程序和功能。相关概念包括密钥管理、凭据管理、身份验证、地理标记、加密、应用程序白名单和可传递信任。

理解 BYOD。BYOD(Bring Your Own Device)是一项策略，允许员工将自己的个人移动设备投入工作，并使用这些设备或通过公司网络连接到业务资源和/或互联网。尽管 BYOD 可提高员工士气和工作满意度，但它会增加组织的安全风险。相关问题包括数据所有权、支持所有权、补丁管理、反病毒管理、取证、隐私、入职/离职、遵守公司策略、用户接受度、架构/基础架构考虑因素、法律问题、可接的使用策略以及机载摄像头/视频。

理解嵌入式系统和静态环境。嵌入式系统通常是围绕一组有限的特定功能设计的，这些特定功能是与其作为组件的较大产品相关的。静态环境是为特定需求、能力或功能配置的应用程序、操作系统、硬件集或网络，然后设置为保持不变。

理解嵌入式系统和静态环境安全问题。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。这些技术可以包括网络分段、安全层、应用防火墙、手动更新、固件版本控制、包装器以及控制冗余和多样性。

理解最小特权原则、特权分离和问责制原则如何适用于计算机体系结构。最小特权原则确保只有最少数量的进程被授权在监督模式下运行。权限分离增加了安全操作的粒度。问责制确保存在审计踪迹以追溯操作的来源。

能够解释什么是隐蔽通道。隐蔽通道是一种用于在通常不用于通信的路径上传递信息的方法。

理解缓冲区溢出和输入检查是什么。当程序员在将数据写入特定内存位置之前未能检查输入数据的大小时，会发生缓冲区溢出。事实上，任何验证输入数据的失败都可能导致安全受到破坏。

描述安全架构的常见缺陷。除了缓冲区溢出之外，程序员还可以在部署后在系统上留下后门和特权程序。即使设计很好的系统也容易受到 TOCTTOU 攻击的影响。任何状态更改都可能成为攻击者破坏系统的潜在机会之窗。

9.15 书面实验

1. 列举三个标准的基于云的“X 即服务”选项，并简要描述它们。
2. 系统处理分类信息的四种安全模式是什么？
3. 说出三对用于描述存储的方面或特性的名称。
4. 列出分布式体系架构中发现的一些漏洞。

9.16 复习题

1. 许多 PC 操作系统提供了使其能够支持在单处理器系统上同时执行多个应用程序的功能。用什么术语来描述这种能力？
 - A. 多程序
 - B. 多线程
 - C. 多任务
 - D. 多进程
2. 什么技术为组织提供了对 BYOD 设备的最佳控制？
 - A. 应用白名单
 - B. 移动设备管理
 - C. 加密可移动存储
 - D. 地理位置标记
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。其中一个应用程序是一个文字处理程序，它同时管理两个线程。另外两个应用程序仅使用一个执行线程。在任何给定时间处理器上运行了多少个应用程序线程？
 - A. 1
 - B. 2
 - C. 3
 - D. 4
4. 什么类型的美国联邦政府计算系统要求访问系统的所有个人都需要知道该系统处理的所有信息？
 - A. 专用模式
 - B. 系统高级模式
 - C. 分隔模式
 - D. 多级模式
5. 嵌入式系统中在标准 PC 中并不常见的安全风险是什么？
 - A. 软件缺陷
 - B. 访问互联网
 - C. 控制物理世界中的机制
 - D. 电力流失
6. 以下哪项描述了社区云？
 - A. 由一组用户或组织维护、使用和支付的云环境，用于共享利益，例如协作和数据交换。
 - B. 企业内部网络中的云服务，与互联网隔离。
 - C. 通过互联网连接向公众开放的云服务。
 - D. 一种云服务，部分托管在组织内供企业内部使用，并使用外部服务向外部人员提供资源。

7. _____是作为大系统的一部分而实现的计算机的概念，系统通常是围绕一组有限的特定功能(如管理、监控和控制)设计，这些特定功能与其所属的较大产品相关。
- A. IoT
 - B. 应用装置
 - C. SoC
 - D. 嵌入式系统
8. 下列哪种类型的存储器在从计算机中移除后可能会保留信息，因此存在安全风险？
- 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(例如笔记本电脑)上丢失数据的风险的最有效方法是什么？
- A. 定义一个强登录密码
 - B. 最大限度地减少存储在移动设备上的敏感数据
 - C. 使用电缆锁
 - D. 加密硬盘
10. 什么类型的电气元件是动态 RAM 芯片的主要构建模块？
- A. 电容
 - B. 电阻
 - C. 触发器
 - D. 晶体管
11. 以下哪个存储设备最有可能需要加密技术才能在网络环境中维护数据的安全性？
- A. 硬盘
 - B. 备份磁带
 - C. 可移动驱动器
 - D. RAM
12. 在以下的_____安全模式中，可以确保所有用户都拥有系统处理的所有信息的访问权限，但不一定需要知道所有这些信息。
- A. 专用模式
 - B. 系统高级模式
 - C. 分隔模式
 - D. 多级模式
13. 手机窃听最常被忽视的方面与以下哪项有关？
- A. 存储设备加密
 - B. 锁屏
 - C. 无意中听到的对话
 - D. 无线网络
14. 什么类型的存储设备通常用于包含计算机的主板 BIOS？
- A. PROM
 - B. EEPROM

- C. ROM
- D. EPROM

15. 什么类型的内存可直接供 CPU 使用，并且通常是 CPU 的一部分？

- A. RAM
- B. ROM
- C. 寄存器
- D. 虚拟内存

16. 你是一位零售商组织的 IT 安全经理，该组织刚刚上线了一个电子商务网站。你聘请了几位程序员来编写代码，这些代码是新的 Web 销售系统的支柱。但是，你担心新代码虽然运行良好，但可能不安全。你将开始审查代码、系统设计和服务体系结构，以跟踪问题和关注点。你希望找到以下哪一项以防止或防范 XSS？

- A. 输入验证
- B. 防御式编码
- C. 允许脚本输入
- D. 元字符转义

17. _____ 形式的攻击利用程序在将输入存储到内存之前未对其接收的数据进行长度限制，从而导致执行任意代码。

- A. ARP 中毒
- B. XSS
- C. 域名劫持
- D. 缓冲区溢出

18. 什么安全原则有助于防止用户访问分配给其他用户运行的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. 哪种安全原则要求只有最少数量的操作系统进程能在监督模式下运行？

- A. 抽象
- B. 分层
- C. 数据隐藏
- D. 最小特权

20. 哪种安全原则采用进程隔离的概念并使用物理控件实现它？

- A. 硬件分割
- B. 数据隐藏
- C. 分层
- D. 抽象

物理安全要求

本章涵盖的 CISSP 认证考试主题包括：

✓ 域 3：安全架构和工程

- 3.10 站点与设施设计的安全原则
- 3.11 实现站点与设施安全控制
 - 3.11.1 配线间/中间布线设施
 - 3.11.2 服务器间/数据中心
 - 3.11.3 介质存储设施
 - 3.11.4 证据存储
 - 3.11.5 受限区与工作区安全
 - 3.11.6 基础设施与 HVAC
 - 3.11.7 环境问题
 - 3.11.8 火灾预防、探测与消防

✓ 域 7：安全运营

- 7.15 物理安全的实现与管理
 - 7.15.1 边界安全控制
 - 7.15.2 内部安全控制

物理与环境安全主题在几个知识域中都会涉及，但主要出现在知识域 3 与知识域 7 中。在 CISSP 认证考试的通用知识体系(CBK)中，这两个知识域的多个子章节都会介绍与设施安全相关的主题与议题，包括基本原则、设计与实现、防火、边界安全、内部安全等。

物理安全的目的是防护来自真实世界的威胁。下面列出最常见的物理威胁：火与烟雾，水(漫水/降水)，地壳运动(地震、滑坡、火山爆发)，风暴(大风、雷电、雨、雪、冰雹、结冰)，破坏/损坏公物，爆炸/破坏，建筑物倒塌，有毒物质，基础设施故障(供电、供气、供水、供暖、冷气)，设备故障，偷盗，人力损失(罢工、生病、访问、交通)。

本章深入探讨这些威胁并讨论针对这些威胁的保护及防范措施。很多情况下，需要制定灾难恢复计划或业务连续性计划，以应对严重的物理安全威胁(如爆炸、破坏或自然灾害)。第 3 章和第 18 章详细介绍这些主题。

10.1 站点与设施设计的安全原则

有一点是显而易见的：假如没有对物理环境的控制，任何管理的、技术的或逻辑的访问控制技术都无法提供足够的安全性。如果怀有恶意的人员获取了对设施及设备的物理访问权，那么他们可进行肆意破坏或窃取、更改数据，为所欲为。物理控制是安全防护的第一条防线，而人员是最后一道防线。

实现与维护物理安全涉及很多方面。其中一个关键因素是选择与设计能够放置 IT 基础设施、能够为组织的运营活动提供保护的安全场所。选择或设计安全设施的过程都始于计划。

10.1.1 安全设施计划

“安全设施计划”需要列出组织的安全需求，并突出保障安全所使用的方法及技术。该计划是通过称为关键路径分析的过程来完成的。“关键路径分析”是一项系统性工作，用于找出关键应用、流程、运营以及所有必要支撑元素间的关系。例如，一台在网上销售产品的电子商务服务器，需要有互联网接入、计算机硬件、电力、温度控制、存储设备等。

如果关键路径分析正确，就能完整绘制出组织正常运行所必要的相互依赖、相互作用的图像。分析完成后，会生成需要保护项目的列表。设计安全 IT 基础设施的第一步，要满足组织环境及信息设备的安全要求。这些基本要求包括：电力、环境控制(建筑、空调、供暖、湿度控制等)，以及供水/排水。

与关键路径分析同等重要的是评估完整或潜在的技术融合。“技术融合”指的是各种技术、解决方案、实用程序及系统，随时间的推移而发展、合并的趋势。这通常会造成多个系统执行相似或冗余的任务，或是一个系统取代另一个系统的特殊功能。虽然在某些情况下，这可提高效率、节约成本，但也容易产生单点故障，从而成为黑客及入侵者更有价值的目标。如果语音、视频、传真与数据传输都共享一个传输通道，而不是各自采用独立的通道，那么入侵者或小偷只需要破坏主通道就可以切断所有通信。

信息安全人员应参与站点与设施的设计。否则，物理安全的很多重要方面可能会被忽视，而这些方面又是逻辑安全至关重要的基础。只有安全人员参与物理设施设计，才能确保组织的长期安全目标，不仅在策略、人员与设备上，同时在建筑本身也获得强有力的支撑。

10.1.2 站点选择

站点的选择应基于组织的安全需求。成本、位置及规模都很重要，但是始终应该优先考虑安全要求。当选择地点建造设施或利用现有建筑时，一定要仔细检查其所处位置的各个方面。

确保资产安全很大程度上取决于站点的安全性，这涉及大量的注意事项及环境元素。站点位置与施工建造在整个选址过程中起着至关重要的作用。如果把站点选在易发生骚乱、抢劫、入室盗窃、破坏公共财产的地方或犯罪高发区，都是非常糟糕的选择，因为这些情况难以把控。在选择站点时，还要注意远离供电线路故障区、龙卷风/飓风区以及其他自然灾害多发区，因为这些灾害难以避免。

此外，还要重点考虑站点是否靠近其他建筑物与商业区。要评估这些地方会吸引哪些人的

注意，是否会对组织的正常运行及设施产生影响。如果附近的商业吸引的游客太多、产生大量的噪音与震动、处理危险物质，这些都会给雇员与建筑带来危险。此外，还要考虑附近是否有应急事件响应人员以及其他一些因素。一些公司有财力购买或建造自己的园区，以隔离开附近的不利因素，实现更严格的访问控制与监视。但不是每个公司都具备这样的财力，只能在可负担的范围内进行选择。

最低限度要确保建筑物的设计，能承受较为极端天气条件的考验，并能阻止或迟滞明显的入侵企图。在分析中，不仅要注意门窗这些易受攻击的入口点，也应评估可能会遮盖非法闯入行为的障碍物(如树木、灌木或人造物体)。

10.1.3 可见度

可见度很重要。周围地形地貌如何？在不被发现的情况下，开车或步行是否很容易接近设施？周围区域的组成也很重要，附近是否有居民区、商业或工业区？本地的犯罪率是多少？距离最近的应急服务机构(消防队、医院、警察)有多远？附近是否存在特殊的危险源(化工厂、无家可归者收容所、大学、建筑工地等)？

10.1.4 自然灾害

另一个需要考虑的是该地区是否会遭受自然灾害的影响。是否易于发生地震、泥石流、沉降、火灾、洪水、飓风、龙卷风、落石、雪、雨、结冰、潮湿、高温、极寒等自然灾害？要做好应对自然灾害的准备，以确保 IT 环境或能抵御灾害，或可以方便地维修。前文提到，第 3 章与第 18 章介绍业务连续性与灾备计划。

10.1.5 设施设计

在设计建筑设施时，必须清楚组织所需的安全级别。在开始施工前必须计划、设计好恰当的安全级别。

需要重点考虑的因素包括：可燃性、火警等级、建筑材料、负载率、布局，以及对墙、门、天花板、地板、HVAC、电力、供水、排水、燃气等项目的控制。暴力入侵、紧急通道、门禁、出入口方向、警报的使用以及传导性是其他需要重点评估的方面。应按照保护 IT 基础架构与人员的原则，对设施中的每一元素从正反两方面进行评估(如，水和空气是从设施内部往外部正向流动的)。

在“安全体系统结构”里提到一个很好的想法，常称为 CPTED(通过环境设计预防犯罪)。其指导思想是通过构建物理环境和周边设施，来降低甚至打消潜在入侵者的犯罪企图。国际 CPTED 协会网站 www.cpd.net 是这一主题很好的信息来源，Oscar Newman 的 *Creating Defensible Space* 一书也是关于该主题的，该书由 HUD 的政策发展与研究办公室出版，可从 www.defensiblespace.com/book.htm 免费下载)。

10.2 实现站点与设施安全控制

物理安全中的安全控制可以分为三大部分：管理类、技术类与现场类。由于访问控制技术也分为同样的三大类，所以要重点关注这些控制的物理安全。“管理类物理安全控制”包括：设施建造与选择、站点管理、人员控制、安全意识培训以及应急响应与流程。“技术类物理安全控制”包括：访问控制、入侵检测、警报、闭路电视监控系统(Closed-Circuit Television, CCTV)、监视、HVAC 的电力供应以及火警探测与消防。“现场类物理安全控制”包括：围栏、照明、门锁、建筑材料、捕人陷阱、警犬与警卫。

 **真实场景**

公司与个人财产

许多商业环境中都配备可见及不可见的物理安全控制。在邮局、便利店和机房的某些区域经常能看到。这些访问控制无处不在，甚至会出现在普通人的生活里，比如封闭的社区或安全的公寓小区。

Alison 是一家专业从事数据管理技术公司的安全分析员。该公司有一名室内安全人员(保安、管理员等)，职责是处理物理安全风险。

Brad 在公司停车场遭遇了一次私家车被盗事件。他问 Alison 有没有看到或记录下有人闯入他的汽车。但是，被盗的是私人物品而不是公司财产，Alison 无法控制、阻止雇员的财产损失。这虽令 Brad 不满，但他也清楚 Alison 负责保护的是公司的、而不是他个人的财产。在什么情况下，安全措施可公私兼顾？答案是：在任何涉及或可能涉及公司资产的地方。如果停在公司停车场的是 Brad 使用的公司车辆，那么 Alison 可能要为 Brad 物品的意外损失提供一些补偿，但即便如此，Alison 也不必为此承担过多责任。另一方面，关键人物也是重要资产(大多数企业的高管、在敏感岗位工作的安全分析师、国家元首等)，保护及保安措施通常要兼顾他们的人身和财产安全，这也是资产保护、降低风险的内容。当然，如果雇员或他们的随身财产面临较严重的威胁，就有必要在停车场安装门禁与监控设备。简而言之，如果发生入室盗窃带来的损失超过安装安防设备的费用，那么这些安全措施还是有必要的。

在为环境设计物理安全时，需要注意各类控制的功能顺序，顺序如下：

- (1) 呵阻(威慑)
- (2) 阻挡
- (3) 监测
- (4) 延迟

部署安全控制首先是要“吓阻”(例如，使用边界限制)入侵者接近物理资产的企图。如果吓阻无效，应“阻挡”(如采用上锁的门)入侵者接触物理资产。如果阻挡失效，“监测”系统应及时发现入侵行为(如，使用运动传感器)，同时“延迟”措施应尽量迟滞入侵者的闯入，以便安保人员有充分时间做出响应(如加固资产)。在部署物理安全控制时，重要的是要记住这个顺序：首先是吓阻，然后是阻挡，接着是监测，最后是延迟。

10.2.1 设备故障

无论组织选择、购买与安装的设备质量如何，发生故障都在所难免。清楚这一点并及时做出准备，有利于确保 IT 基础设施的可用性，也可保护信息资产的完整性与可用性。

预防设备故障可采用多种形式。在一些非关键场合，只要知道在 48 小时内从哪里能购买到配件，并进行更换就足够了。在其他一些情况下，则必须在现场维修更换设备。需要牢记，维修系统并恢复到可用状态的响应时间与付出的费用是成比例的。这些费用包括：存储、运输、预购置以及负责现场安装与恢复工作专家的费用。还有一些情况无法在现场进行维修更换工作。对于这种情况，与硬件厂商签订服务水平协议(Service-Level Agreement, SLA)是非常重要的。SLA 中清楚写明了发生设备紧急故障时厂商的响应时间。

老旧的硬件应安排定期进行更换和/或维修。维修时间的安排应基于每个硬件预先估计的 MTTF (Mean Time To Failure, 平均故障时间)与 MTTR (Mean Time To Repair, 平均恢复时间)，或是业界最佳实践的硬件管理周期。MTTF 是特定操作环境下所预计的设备典型功能周期。MTTR 是对设备进行修复所需的平均时间长度。在预计的灾难性故障发生之前，设备常常要经过多次维修。要确保所有设备在其 MTTF 失效之前得到及时更换。另一种度量方法是 MTBF (Mean Time Between Failures, 平均故障间隔时间)，这是发生第一次故障与第二次故障之间时间的估值。如果 MTTF 和 MTBF 值相同或接近，制造商通常只列出 MTTF 来同时表示这两个值。

设备送修时，需要有替代件或备份件做临时之用。通常，在进行维修前出现小故障是可以接受的，但等到出现大问题才进行维修更换就难以接受了。

10.2.2 配线间

在过去，配线间(wiring closet)只是用于整理楼宇通信电缆信息模块(punch-down blocks)的小机柜。今天，配线间虽仍用于线路整理的目的，但同时也成为一类重要的基础设施。现代配线间将整栋建筑或某一楼层的网络电缆，连接到放置其他重要设备的地方。这些设备包括布线板、交换机、路由器、局域网(LAN)扩展器与主干通道。配线间其他更专业的名称包括综合布线间(premises wire distribution room)、中间布线设施(Intermediate Distribution Facilities, IDF)。在配线间中常放置一个或多个配线架(见图 10.1)。

由于线缆最大有效长度的限制，更大的建筑中需要更多的配线间。普通铜芯双绞线线缆最大有效长度是 100 米。但在电磁噪声环境中，这种有效长度会减少很多。配线间也是方便连接多个楼层的地方。在这种多层建筑中，配线间通常位于不同楼层正对的上下方。

配线间也常用于存放、管理建筑物中其他多种重要设施的布线，包括警报系统、断路器面板、电话信息模块、无线接入点与视频系统(包括安全摄像头)。

配线间的安全非常重要。配线间的大部分安全措施都集中在防止非法的物理访问。如果非法的入侵者进入该区域，他们可能会窃取设备、拉断电缆，甚至安装监听设备。因此，配线间的安全策略应包括如下一些基本规则：

- 不要使用配线间作为一般的储物区。
- 配备充足的门锁，必要时采用生物因素。



图 10.1 一个典型的配线间

- 保持该区域整洁。
- 该区域中不能存储易燃品。
- 配备视频监控设备，监视配线间内的活动。
- 使用开门传感器进行日志记录。
- 钥匙只能由获得授权的管理员保管。
- 对配线间进行常规的现场巡视以确保其安全。
- 将配线间纳入组织的环境管理和监控中，既能够确保合适的环境控制和监视，也是为了及时发现类似水情和火警的危险。

同样重要的是，将配线间安全策略与访问限制告知大楼的物业管理部门，可进一步减少非法的访问企图。

配线间只是综合布线管理策略(cable plant management policy)中的一个元素。综合布线是互连线缆与连接装置(如跳线箱、接线板和交换机)的集合，它们组建起物理网络。综合布线的元素包括：

接入设施(entrance facility)：也称为分界点，这也是(通信)服务商的电缆连接到建筑物内部网络的接入点。

设备间(equipment room)：这是建筑物的主布线间，通常是与接入设施连接或相邻。

骨干配线系统(backbone distribution system)：为设备间和通信间提供电缆连接，包括跨层连接。

通信机房(telecommunications room)：也成为布线间，通过为组网设备和布线系统提供空间，来满足大型建筑中不同楼层和部分间的连接需要。也充当骨干配线系统和水平配线系统间的连接点。

水平配线系统(horizontal distribution system)：提供通信机房与工作区域间的连接，通常包括：布线、交叉连接模块、布线板以及硬件支持设施(如电缆槽、电缆挂钩与导管)。

10.2.3 服务器间与数据中心

服务器间、数据中心、通信机房、布线柜、服务器柜以及 IT 机柜是封闭的、受限的和受保护的空间，用来放置重要的服务器与网络设备。集中式服务器间环境不需要适宜人员常驻(与人的相容性不好)。事实上，服务器间与人相容性越差，就越能提供保护，越能抵御偶然的与明确的攻击。可通过如下措施来实现与人的不相容性：采用哈龙(Halotron)、热原(PyroGen)或者哈龙替代物作为火警探测及灭火系统、低温、低照明或无照明、狭窄的设备空间。服务器机房的设计应充分利用 IT 基础设施的优点，同时要阻止非法人员的访问或干预。

服务器间应该位于建筑的核心位置。尽可能避免将服务器间设置在建筑物的一楼、顶楼或地下室。此外，服务器间应远离水、燃气与污水管道。这些管道存在较大的泄漏风险，可导致严重的设备损坏与停机。

提示：服务器间的墙壁应具备至少一小时的耐火等级。



真实场景

使服务器无法访问

有一个笑话在信息安全界广为流传：断开网络连接，密封在没有门窗房间里的计算机才是最安全的。这虽是笑话，但也道出了实情，其中也蕴含着讽刺。

Carlos 在一家金融银行公司操作安全程序与平台，他非常熟悉单向(one-way)系统及不可见设备(Unreachable Devices)。敏感的商业交易在瞬间完成，任何一个错误操作都会给数据及相关设备带来严重风险。

根据 Carlos 的经验，他知道那些最不易接近与最不友好的地方放置的是最有价值资产，所以他将很多机器存放在一个单独的银行金库中。除非是一个天才的窃贼，同时兼备熟练开锁工与意志坚定电脑黑客的本领，否则很难突破他的安全防线。

并不是所有的商业应用及程序，都能产生如此极端的防护效果。如果没有 Carlos 那样的金库，如何才能让一台服务器难以接近呢？一间没有窗户，只有一个出入口，访问受限的内部房间是个不错的选择。关键在于首先选择一个访问受限的空间，然后在入口设置障碍(尤其是限制非法进入)。房间门口的闭路电视监控系统以及内部的运动探测器可对出入人员进行监视。

对许多组织来说，其数据中心和服务器间相同的。对另外一些组织，数据中心则是外部的一个单独区域，里面部署了大量的后端 PC 服务器、数据存储设备与网络管理设备。数据中心可能靠近主办公区，也可能是位置较远的一栋独立建筑。数据中心可能是组织单独拥有与管理，也可能租用的是数据中心提供商的服务。一个数据中心可能是单租户配置，也可能是多租户配置。不管有什么差异，除了服务器间是重点，还要关注其他很多相关的概念。

在很多数据中心与服务器室中，采用各种技术的访问控制来管理物理访问。这些包括但不限于：智能卡/哑卡，接近式读卡器，生物识别，入侵检测系统(IDS)，以及基于纵深防御的设计。

1. 智能卡

“智能卡”(smartcard)既可以是一种信用卡大小的身份标识、徽章，也可以是带嵌入式磁

条、条形码、集成芯片的安全通行证。其中包含合法权持有者的信息，用来进行识别与/或身份验证目的。一些智能卡甚至可进行信息处理，或在记忆芯片中存储一定数量的数据。下面是几条与智能卡有关的短语与术语：

- 包含集成电路(IC)的身份令牌
- 处理器 IC 卡
- 支持 ISO 7819 接口的 IC 卡

智能卡通常被视为一种完整的安全解决方案，但这不意味着单纯依靠智能卡本身就可以高枕无忧了。与任何单一的安全机制一样，智能卡也存在弱点与脆弱性。智能卡可能会成为物理攻击、逻辑攻击、特洛伊木马攻击，或社会工程攻击的牺牲品。大多数情况下，一张智能卡工作在多因素配置下。如果这样，即使智能卡被盗或遗失，都不会被冒用。智能卡中最常用的多因素形式是 PIN 码。有关智能卡的详细内容会在第 13 章中进行介绍。

记忆卡(memory cards)是带机器可读磁条的 ID 卡，类似于信用卡、借记卡或 ATM 卡，记忆卡内可以存储少量的数据，但不能像智能卡一样处理数据。记忆卡经常充当一类双因素控制功能：该卡是“你所有的”，同时卡的个人身份识别码(PIN)是“你所知的”。但是，记忆卡易于拷贝与复制，所以不能在安全环境中作验证之用。

2. 接近式读卡器

除了智能卡/哑卡，接近式读卡器也可以用来控制物理访问。接近式读卡器(proximity reader)可能是一种无源装置、感应供电装置或应答器。接近装置由授权用户佩戴或持有。当接近装置通过读卡器时，读卡器能够确定持有者的身份，也可判断持有者是否获得了进入授权。无源装置反射或改变读卡器的电磁场，读卡器能够探测到电磁场的改变。

无源装置中缺少有源电子器件，它只是一块具有特殊性质的小磁铁(比如 DVD 上常见的防盗装置)。场供电装置内装有电子器件，当装置通过读卡器产生的电磁场时，电子器件就会启动。这些装置实际上是利用电磁场产生的电能给自己供电(如读卡器，只需要将门禁卡在离读卡器只有几英寸远的地方晃动几下，就可打开房门)。应答器是一种自供电装置，其发出的信号被读卡器接收。工作原理类似于常见的按钮(如车库门开关与密钥卡)。

除了智能卡/哑卡与接近式读卡器，还可通过射频识别(RFID)及生物识别访问控制设备进行物理访问管理。生物识别装置的内容可参见第 13 章。此外，还有其他一些装置，如链条锁，也可以保护设备的安全。

3. 入侵检测系统

入侵检测系统(IDS)既有自动的，也有人工的，主要用于探测：入侵、破坏或攻击企图；是否使用了未经授权的入口；是否在未授权及非正常时间内发生了特殊事件。监视真实活动的入侵检测系统包括：保安、自动访问控制、动作探测器以及其他专业监视技术。这些将在 10.3.2 节的“动作探测器”与“入侵警报”中详细讨论。

物理入侵检测系统也称“盗贼警报”。其作用是探测非法活动并通知安保人员(内部保安或是外部的执法人员)。最常见的一类系统，使用的是由一种金属箔条构成的简单电路(干式接触开关)，一般安装在入口点用于探测门窗是否打开。

只有与入侵警报相连，入侵检测才会发挥应有的作用。入侵警报会通知安保人员出现了物理安全漏洞。

任何入侵检测及警报系统都有两个致命的弱点：电源与通信。如果系统失去电力供应，警报将无法工作。因此，一个可靠的检测与警报系统，应该配备电力充足的备用电池，以确保系统 24 小时都能正常工作。

如果通信线路被切断，警报也会失效，因为无法通知安保人员，请求应急服务。因此，一个可靠的检测与警报系统，应配备“心跳传感器”进行线路监视。心跳传感器的功能是通过持续或周期性测试信号，来检查通信线路是否正常。如果接收站检测不到心跳信号，就自动触发报警。这两种措施都用来防止入侵者绕过探测与警报系统。

4. 访问滥用

无论使用哪种形式的物理访问控制，都需要配备保安人员或其他监视系统，来防止滥用、伪装及捎带。通过物理访问控制滥用的事例，可以演示如何打开安全大门，绕过门锁或访问控制。“伪装”(Masquerading)是冒用他人的安全 ID 来获得访问权限。“捎带”(piggybacking)是采取跟随他人的方式穿过安全门或通道，从而躲过人员鉴别及授权机制。可以通过审计踪迹与保留访问日志的手段来发现滥用行为。

即使对于物理访问控制，审计踪迹与访问日志也是有效的技术手段。日志既可由安保人员手工记录，也可在具备访问控制技术条件(例如智能卡与特定的接近读卡器)下自动进行记录。审计踪迹与访问日志记录里的信息包括：事件发生的时间、身份验证过程的结果(成功或失败)、安全门打开的持续时间等。除了电子或纸质记录，还应该采用闭路电视监控系统(CCTV)或安全探头来监视各个入口点。CCTV 记录的事件视频信息，可以与审计踪迹及访问日志信息结合起来进行对比参照。这对于还原入侵、破坏或攻击事件的全过程至关重要。

5. 发射安全

很多电子设备发出的电信号或产生的辐射可能会被非法人员侦听。这些信号可能包含机密、敏感或个人数据。常见的发射装置有无线网络设备与移动电话。此外，还有很多其他设备也容易被拦截。这些设备包括监视器、调制解调器以及内驱与外驱(硬盘、U 盘、光盘等)。针对这些设备，非法用户可侦听来自这些装置的电磁或无线频率信号(统称为“发射”)，从而提取出机密信息。

很显然，如果组织内设备发出的信号能被外面的人员侦听到，就需要采用相应的安全保护措施。用于防护发射攻击的方法及技术称为 TEMPEST 措施。TEMPEST 最初是源于政府的一个研究课题，目的是为了保护电子设备，免受核爆炸所产生的电磁脉冲(Electromagnetic Pulse, EMP)的破坏。现在已经扩展成一项监视发射、防止侦听的通用研究课题。TEMPEST 现在是涵盖多种防护措施的正式名称。

TEMPEST 措施包括：法拉第笼、白噪声与控制区。

“法拉第笼”是覆盖在盒子、活动房屋或是整栋建筑外的金属网，金属网完整覆盖物体外部的各个截面(前后左右上下)。金属网充当电磁干扰(EMI)-吸收电容(也是为什么以 Michael Faraday 这样一个电磁学研究先驱命名的原因)，用来阻止电磁信号的进入或发出。法拉第笼阻挡 EM 信号非常有效。在现实中，法拉第笼中的移动电话无法正常工作，电台与电视也接收不到信号。

“白噪声”简单地说就是通过发射无线噪声来覆盖并隐藏真实的电磁信号。白噪声可以是来自于其他非保密信号源的真实信号，也可以是某个特定频率的恒定信号，或是一个随机变量

信号(如电台或电视台间的白噪声)，甚至可以是导致侦听设备失效的混杂信号。白噪声部署在保护区域的边界，向外进行发射效果最好，这样既不干扰内部的正常通信又可起到保护作用。



注意：

白噪声指能淹没没有意义信息的随机噪声、信号或程序。范围覆盖从耳朵可听到的声音到不可见的电子传输，甚至是故意伪造的线路或流量噪声，以达到掩盖信号源或破坏侦察设备的目的。

“控制区”是第三种类型的 TEMPEST 措施，“控制区”采用单一的法拉第笼、白噪声或二者组合，对环境中某个特定区域进行保护，而其他区域则不受影响。一个控制区可以是一个房间，一层楼，或是整栋建筑。在控制区内，必要的设备(如无线网络、移动电话、广播和电视)可以正常发射和接收电磁信号。控制区外，使用各种 TEMPEST 措施来阻挡与防止发射侦察。

10.2.4 介质存储设施

介质存储设施用于安全存储空白介质、可重用介质及安装介质。无论是硬盘、闪存设备、光盘或是磁带，各种介质都应进行严格保护以免被盗或受损。新的空白介质也要防止被偷或被植入恶意软件。

可擦写介质(如 U 盘、闪存卡或移动硬盘)，要防止被偷或进行数据残余恢复。“数据残余”是指存储设备经过标准删除或格式化操作后依然残留的数据。这些操作只清除了目录结构，并将簇区标记为可用，却并没有将簇区中存储的数据完全删除。使用简单的反删除工具或数据恢复扫描器就可以恢复这些数据。限制对于介质的访问并使用安全擦除工具可以减少此类风险。

要保护安装介质免于被盗或植入恶意软件的危险。这样能够保证在需要安装软件时，有介质可用并且是安全的。

下面列出实现介质安全存储设施的一些方法：

- 将存储介质保存在上锁的柜子或保险箱里。
- 介质存放在上锁的柜子里，并指定专人进行管理。
- 建立登入/登出制度，跟踪库中介质的查找、使用与归还行为。
- 可重用介质归还时，执行介质净化与清零过程(使用全零这样的无意义数据进行改写)，清除介质中的数据残余。
- 采用基于 hash 的完整性检查机制，来校验文件的有效性，或验证介质是否得到彻底净化，不再残留以前的数据了。

对安全要求高的组织，有必要在介质上打上安全提示标签，以标识其使用等级，或在介质上使用 RFID/NFC 资产追踪标记。使用介质存储柜也非常重要，其作用相当于一个保险柜而不是简单的办公室货架。介质更高等级的保护要求还包括：防火、防水、防磁以及温度监视与保护。

10.2.5 证据存储

不仅是执法部门，对于所有组织来说，证据存储正越来越变得有必要。随着网络安全事件不断攀升，保留日志、审计记录以及其他数据事件记录变得日益重要。同时，也有必要保存磁

盘镜像及虚拟机快照便于以后对比。这样不仅有利于内部的公司调查，也有助于执法部门的取证分析。保存可能作为证据的数据，不论对内部的公司调查，还是执法部门的网络犯罪调查都至关重要。

安全证据存储的要求：

- 使用与生产网络完全不同的专用存储系统。
- 如果没有新数据需要存入，应让存储系统保持离线状态。
- 关闭存储系统与互联网的连接。
- 跟踪证据存储系统上的所有活动。
- 计算存储在系统中所有数据的 hash 值。
- 只有安全管理员与法律顾问才能访问。
- 对存储在系统中的所有数据进行加密。

此外，根据不同的管理条例、行业要求或合同义务，对于证据存储系统还有其他一些安全要求。

10.2.6 受限区与工作区安全

内部区安全包括工作区域与访客区域，应进行认真的设计与配置。设施内的所有区域不能是整齐划一的访问等级。对存放高价值或重要性高资产区域的访问，应受到更严格的限制。任何进入设施的人可使用休息室及公共电话，但不能进入敏感区域，只有网络管理员与安全人员才能进入服务器间。有价值及保密资产应处于设施的保护核心或中心，也应将注意力集中在物理保护环的中心。这样的配置，保证了只有不断获得更高级的授权，才能逐级进入设施中更敏感的区域。

墙与隔断能够用于分隔相似但不同的工作区域。这种分隔可防止无意的肩窥(shoulder surfing)或偷听行为。肩窥是指通过偷窥操作者显示器及键盘操作来收集信息的行为。使用封闭墙壁能够分隔出不同敏感及保密等级的区域(墙壁应该避开天花板悬吊或脆弱部分，墙壁是不同安全等级区域间难以逾越的障碍)。

每个工作区都应按照 IT 资产分级进行评估与分级。只有获得许可或具备工作区访问权限的人员才允许进入。不同目的及用途的区域应分配不同的访问及限制级别。区域内可访问的资产越多，对进入区域人员及其活动的限制规定就越重要。

设施的安全设计应反映对内部安全实现及运营的支持。除了正常工作区内人员的管理，还需要进行访客管理与控制。检查一下是否建立了访客陪护制度？现有哪些形式的访客控制措施？除了钥匙门锁这些基本的物理安全工具，是否配备了陷阱、视频探头、日志记录、安全警卫及 RFID ID 标签这些安全机制。

一个安全受限工作区的实例是敏感隔间信息设施(Sensitive Compartmented Information Facility, SCIF)。政府与军事承包商经常使用 SCIF，建立进行高敏感数据存储与计算的安全环境。SCIF 的目的是存储、检查以及更新敏感的隔离信息(Sensitive Compartmented Information, SCI)。隔离信息是一种机密信息，对 SCIF 内数据的访问受到严格限制，只对那些有特定业务需要并获得授权的人员开放。这通常是由人员的许可等级与 SCI 的准入等级来确定。大多数情况下，SCIF 禁止在安全区内使用拍照、摄像或其他记录设备。SCIF 既可建造在陆地设施里，也可在飞行器或漂浮平台里。SCIF 既可是一个永久性建筑也可是一临时性设施。SCIF 通常处于一

个建筑中，而完整的建筑也可成为一个 SCIF。

10.2.7 基础设施与 HVAC

电力公司的电力供应并不是持续和洁净的，大多数电子设备需要洁净的电力才能正常工作。电压波动引起的设备损坏时有发生。许多组织采用各种方法，来改善各自的电力供应。“不间断电源”(Uninterruptible Power Supply, UPS)是一种自充电电池，可为敏感设备提供持续洁净的电力供应。UPS 从墙上的插座里获取电力，并将电力存储在电池里，再将电池里存储的电力供给所连接的设备。这称为双变换 UPS。UPS 还有一个附带功能，也常作为卖点：在主电源断电的情况下依然可供电。根据 UPS 的容量与所连接的设备，供电时间可从几分钟到几小时不等。从电网供电切换到电池供电瞬间完成，对设备的电力供应不会中断。

另一种形式的 UPS 是在线交互式(line-interactive)UPS。该类型系统有浪涌保护器、电池充电逆变器以及位于电网电源及设备间的电压调节器。在正常条件下，电池是离线的。如果电网停电，设备可以通过电池逆变器及电压调节器获取不间断的电力供应。

后备电池或容错(fail-over)电池并不是一种形式的 UPS，因为电网停电时，电力供应从电网切换到后备电池上，通常需要有一小段时间，在这期间，设备完全失去了电力供应。

另一种保证设备不受电压波动损害的方法，是使用带浪涌保护器的接线板。浪涌保护器里有一个保险丝，如果电压波动大到会对设备造成损坏时，保险丝就会熔断。但是，一旦浪涌保护器中的保险丝或电路断开，电流也完全中断了，浪涌保护器只能用于瞬时断电不会对设备造成损害的场合。否则就应使用 UPS。

如果在低压或停电的情况下，仍然需要维持一段时间的正常运营，就应该配备电力发电机。当检测到电力供应中断时，发电机会自动打开。大部分发电机都使用液态燃油或气体燃料，需要定期进行维护，以确保使用安全可靠。电力发电机可以作为电源的替代或备份。

有关电力的问题有很多。下面列出一些应该了解的电力术语：

- 故障(Fault): 瞬时断电。
- 停电(Blackout): 完全失去电力供应。
- 电压骤降(Sag): 瞬时低电压。
- 低电压(Brownout): 长时低电压。
- 尖峰(Spike): 瞬时高电压。
- 浪涌(Surge): 长时高电压。
- 合闸电流(Inrush): 通常是接入电源(主电源、替代/副电源)。
- 噪声(Noise): 持续稳定干扰电力供应的波动或者扰动。
- 瞬态(Transient): 短时的线路噪声扰动。
- 洁净(Clean): 无波动纯电力。
- 接地(Ground): 电路中接地导线。

出现电力故障时，确定故障点的位置非常重要，如果故障出现在电表箱以外，应该有电力公司来修理解决。否则其他内部问题都需要自己解决。

1. 噪声

噪声的危害不仅会影响设备的正常工作，还可能干扰通信、传输以及播放的质量。电流产

生的噪声能够影响任何使用电磁传输机制的数据通信，比如电话、手机、电视、音频、广播及网络。

有两种类型的“电磁干扰”(Electromagnetic Interference, EMI)：普通模式与穿透模式。“普通模式噪声”是由电源火线与地线间的电压差或操作电气设备而产生的。“穿透模式噪声”则是由火线与零线间的电压差或操作电气设备产生的。

“无线电频率干扰”(Radio-Frequency Interference, RFI)是另一种噪声与干扰源，它像 EMI 一样能够干扰很多系统的正常工作。范围广泛的普通电器都会产生 RFI，如荧光灯、电缆、电加热器、电脑、电梯、电机以及电磁铁，所以在部署 IT 系统和其他设施时，一定要注意周围电器的影响。

保护电源与设备免受噪声影响，为 IT 设施提供正常的生产与工作环境十分重要。保护的措施有：提供充足的电力供应、正确的接地、采用屏蔽电缆、远离 EMI 和 RFI 发射源。

2. 温度、湿度与静电

除了电力因素，对环境的保护还包含对 HVAC 系统的控制。放置电脑的房间温度通常要保持在华氏 60~75 度之间(摄氏 15~23 度)。此外，有一些对环境温度要求苛刻的设备需要的温度低到华氏 50 度，还有一些要求环境温度超过华氏 90 度。电脑房间内的湿度应保持在 40%~60%。湿度太高会腐蚀电脑中的配件，湿度太低会产生静电。即使铺设了防静电地板，在低湿度的环境中依然可能产生 20 000 伏的静电放电电压。正如在表 10.1 所示，即使是最低等级的静电放电电压也足以击毁电子设备。

表 10.1 静电电压与破坏力

静电电压	可能造成的破坏
40	损坏敏感电路和其他电子部件
1 000	干扰显示器工作
1 500	破坏硬盘上存储的数据
2 000	系统突然关机
4 000	打印机塞纸或是部件损坏
17 000	电路永久性损坏

3. 关于水的问题(如漏水、洪水)

水的问题，如漏水和洪水，也应在环境安全策略及程序中得到解决。水管漏水不是每天都会发生，可是一旦发生就会带来非常大的损失。

水电不相容，如果电脑进了水，特别是处于运行状态时，肯定会对系统造成破坏。此外，如果水遇到电还会增加附近人员的触电风险。在任何可能的情况下，服务器间、数据中心与关键电脑设备都要远离水源或水管的位置。在关键系统的周围，还需要安装漏水探测绳。如果设备周围发生渗水事故，漏水探测绳会发出警报提醒相关人员。

如果想减少紧急情况的发生，还需要知道水阀及排水系统的位置。除了监视水管漏水，还需要评估设施处理大暴雨或附近发生洪水的能力。建筑是位于山上还是在山谷里？是否具备足够的排水能力？本地是否有发洪水或堰塞湖的历史？服务器间是不是设置在地下室或顶楼？

10.2.8 火灾预防、探测与消防

不能忽视火灾的预防、探测与消防。任何安全与保护系统的首要目标是保障人身的安全。除了人员的安全以及设计火灾探测与消防系统的目的，还为了将火、烟及热量造成的损失(特别是对IT基础设施的损失)降到最低，还要减少灭火剂的使用。

标准的火灾预防与灭火知识培训，主要是关于火灾三要素，也可表示成火灾三角形(参见图10.2)。三角形的三个角分别是火、热量与氧气。三角形中心表示的是这三个要素间发生的化学反应。火灾三角形重点揭示出：只要消除三角形中四项的任何一项，火灾就能被扑灭。不同的灭火剂针解决火不同方面的问题：

- 水是为了降低温度减少热量。
- 碳酸钠及其他干粉灭火剂是阻断燃料的供应。
- 二氧化碳是为了抑制氧气的供应。
- 哈龙替代物与其他不可燃气体干扰燃烧的化学反应和/或抑制氧气供应。



图 10.2 火灾三角形

在选择灭火剂时，首先要考虑是针对火灾三角形的哪些方面，该灭火剂的效果如何，还要考虑灭火剂对环境的影响。

除了理解火灾三角形，还需要理解火灾的发展阶段。火灾会经历很多阶段，图10.3介绍了其中最主要的四个阶段。

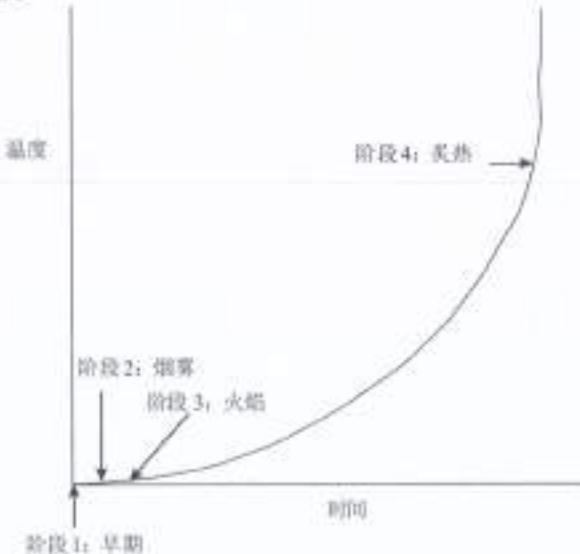


图 10.3 火灾的四个主要阶段

阶段 1：早期阶段这一阶段只有空气电离，没有烟雾产生。

阶段 2：烟雾阶段可以看见有烟雾从着火点冒出。

阶段 3：火焰阶段在这个阶段，用肉眼就能看见火焰。

阶段 4：炙热阶段在阶段 4，火场温度沿着时间轴急剧升高，聚集了大量热量，火场中的任何可燃物都燃烧起来。

火灾发现的越早越容易扑灭，火灾以及灭火剂造成的损失也越小。

防火管理中的一个基础是正确的人员防火意识培训。每个人都应非常熟悉设施中的消防原理；也应熟悉所在主工作区至少两条的逃生通道；还应知晓如何在设施中其他地方发现逃生通道。此外，还应培训人员如何发现与使用灭火器。其他防火或通用应急响应培训内容还包括心肺复苏(CPR)、紧急关机程序以及发现预设集合点或安全验证机制(如语音邮箱)。



提示：

数据中心中的大部分火灾都是由于电源插座过载引起的。

1. 灭火器

有几种类型的灭火器。了解何种类型的灭火器适用于哪些火灾，对于有效扑灭火灾至关重要。如果灭火器使用的不正确，或对火灾的类型不合适，就会适得其反，不仅无法灭火还会让火势蔓延。灭火器只适用于处于早期阶段的火灾。表 10.2 列出了三种常见类型的灭火器。

表 10.2 灭火器类别

类别	类型	灭火剂
A	普通燃烧物	水、硼酸钠(一种干粉或化学药水)
B	液态	二氧化碳、哈龙*、碳酸钠
C	电气火灾	二氧化碳、哈龙*
D	金属	干粉

* 哈龙或 EPA-许可的哈龙替代品。



提示：

水不能用于 B 类火灾，因为会溅出可燃液体，并会让可燃液体漂浮在水上。水也不能用于 C 类火灾，因为存在触电的危险。氧气抑制剂不能用于金属火灾，因为燃烧的金属会产生氧气。

火灾探测系统

为了保护设施免受火灾的影响，需要安装自动火灾探测与消防系统。火灾探测系统的类型有很多。“固定温度探测”系统在环境达到特定温度时会触发灭火装置。触发器通常是一种金属或塑料材质部件，安装在灭火喷淋头上，当温度上升到设定值时，这个部件就会熔化，从而打开喷淋头进行洒水灭火。还有一种触发器使用小玻璃瓶，里面充满了化学物质，当温度升高到设定值时，瓶中的化学物质会快速挥发，产生的过压也会启动灭火装置。“上升率探测”系统是在温度的上升速率达到特定值时启动灭火功能。“火焰驱动”系统依靠火焰的红外热能触发灭火装置。“烟雾驱动”系统使用光电或辐射电离传感器作为触发器。早期(火情)烟雾探测系统，也

称为吸气传感器，能够探测出燃烧非常早期阶段产生的化学物质，从而比使用其他方法更早发现潜在的火情。

大多数火灾探测系统都与火灾响应服务报告系统相连。在启动灭火装置的同时，该系统也会通知当地消防部门并自动发出消息或警报请求援助。

为能充分发挥作用，火灾探头的安装位置也十分重要。房间的吊顶和活动地板中、服务器间、个人办公室、公共区域中都需要安装，HVAC 通风井、电梯井、地下室等地方也不能遗漏。

对于所采用的灭火系统，可以选择水消防系统，也可以选择气体消防系统。在人类相容环境中，水是常用灭火剂，而气体消防系统更适合没有人员驻留的机房。

2. 喷水消防系统

主要有四种喷水灭火系统

“湿管系统”(也称为封闭喷头系统)的管中一直是充满水的。当打开灭火功能时，管中的水会立刻喷洒出来进行灭火。

“干管系统”中充满了压缩气体。一旦打开灭火功能，气体会释放出来，随即供水阀门会打开，管中进水并开始喷洒灭火。

“集水系统”是另一种干管系统，由于采用更粗的管道，因而可以输送的水量更大。集水系统不适用于存放电子仪器与计算机的环境。

“预动作系统”结合了湿管与干管的特点，正常情况下保持干管状态，如果探测到可能的火灾因素(如烟、热量等)，管中会立刻注满水。但是只有环境的热量足以熔化喷淋头上的触发器，管中的水才会释放出来。如果在喷淋头打开之前，火势就被扑灭，系统可以手动进行排空和复位。这也提供一种在喷淋头触发前，能够通过人工干预阻止水管喷水的机制。

预动作系统是最适合人机共存环境的喷水灭火系统。



提示：

喷水灭火系统的最常见故障都是因为人为错误造成的，比如发生火灾了才发现水源关闭了，或是没有发生火灾却打开了喷水功能。

3. 气体消防系统

“气体消防系统”通常比喷水消防系统更有效。然而，气体消防系统不能用在有人员常驻的环境中。气体消防系统会清除空气中的氧气，因而对人员是十分危险的。系统常用的是压缩气体灭火剂，例如二氧化碳、哈龙或 FM-200(一种哈龙替代品)。

哈龙是一种有效的灭火用化合物(通过耗尽氧气，来阻止可燃材料与氧气间的化学变化)，但在华氏 900 度，会分解出有毒气体。所以，哈龙不是环境友好型的(同时，它又消耗臭氧)。1994 年，EPA 在美国停止了哈龙的生产。进口 1994 年后生产的哈龙也不合法。发达国家在 2003 年 12 月 31 日也停止了哈龙 1301、哈龙 1211 以及哈龙 2403 的生产。然而，根据蒙特利尔协议，还可以向哈龙循环利用机构购买哈龙。EPA 寻求将现有库存的哈龙使用完后停止该物质的使用。

由于哈龙存在的缺点，它逐渐被更为生态友好或毒性更小的灭火剂所取代。下面列出的是 EPA 许可使用的哈龙替代品(更详细的信息请见 <http://www.epa.gov/ozone/snap/fire/halonreps.html>)：

- FM-200 (HFC-227ea)

- CEA-410 或 CEA-308
- NAF-S-III (HCFC A 混合物)
- FE-13 (HCFC-23)
- Argon (IG55) 或 Argonite(IG01)
- Inergen (IG541)
- Aero-K(气溶胶形式的微量钾化合物)

也可以用低压水雾来代替哈龙替代品。但此类系统不能在电脑机房或电气设备存储间内使用。低压水雾系统形成的气雾云能快速降低起火区域的温度。

4. 破坏

设计火灾探测与消防系统还要考虑火灾可能带来的污染与损害。火灾的主要破坏因素包括烟、高温，也包括水或碳酸钠这样的灭火剂。烟会损坏大多数存储设备，高温可能会损坏电子或电脑部件。例如，在100华氏度下会损坏磁带，175度会损坏电脑硬件(如CPU和内存)，350度下纸质文件会损坏(会卷边和褪色)。

灭火剂还可能造成短路、腐蚀或设备报废。在设计消防系统时，这些因素都需要考虑。



提示：

发生火灾时，除了火灾本身和灭火剂造成的损害，消防人员在用水管灭火、使用救生斧寻找火源的过程也可能造成损坏。

10.3 物理安全的实现与管理

控制、监视、管理设施访问的物理访问控制手段有很多。范围覆盖从吓阻到探测的多个方面。设施与场所中的各部分、分部或区域也应清楚地划分出公共区、专用区或限制区。每个区域都需要配备侧重点不同的物理访问控制、监视及预防措施。下面讨论这些技术手段，主要用于多种区域的划分、分隔与访问控制，包括边界安全和内部安全。

10.3.1 边界安全控制

建筑或园区是否方便进出这点很重要。单个出口非常利于安全保卫，但多个出口在发生紧急情况时更便于疏散逃生。附近的道路情况如何，有哪些便捷的交通方式(火车、高速公路、机场、船舶)？一天的旅客流量有多少？

出入的方便性受到边界安全需要的制约。访问与使用的需求也应支持边界安全的实现与运营。物理访问控制、人员监视、设备进出、发生事件的审计与日志，这些都是维护组织总体安全的关键因素。

1. 围栏(Fences)、门(Gates)、旋转门(Turnstiles)与捕人陷阱(Mantraps)

“围栏”是一种边界界定装置。围栏清楚地划分出处于特定安全保护级别的内外区域。建造围栏的部件、材料以及方法多种多样，可以是喷涂在地面上的条纹标志，也可以是锁链、铁

丝网、水泥墙，甚至可以是使用激光、运动或热能探测器的不可见边界。不同类型的围栏适用于不同类型的入侵者：

- 3~4 英尺的围栏可吓阻无意穿越者。
- 6~7 英尺高的围栏难以攀爬，可吓阻大多数入侵者。但对于坚定的入侵者无效。
- 8 英尺以上的围栏，外加三层铁丝网甚至可吓阻坚定的入侵者。

“门”是围栏中可控的出入口。吓阻级别的门在功能上必须等同于吓阻级别的围栏，这样才能维持围栏整体的有效性。铰链和门锁要进行加固以防被更改、损坏或移除。当门关闭时，不能有其他额外的可以出入的漏洞。应该将门的数量降到最低。并且每个门都应该处于警卫的监视之下。没有警卫把守的门，可以使用警犬或是闭路电视进行监控。

“旋转门”(如图 10.4 所示)是一种特殊形式的门，其特殊性在于一次只允许一个人通过，并且限制只能朝着一个方向转动。经常用于只能进不能出的场合，或是相反的功能。旋转门在功能上等同于配备安全转门的围栏。

“捕人陷阱”通常是一种配备警卫的内、外双道门机构(如图 10.4 所示)，或是其他类型能防止捎带跟入的物理机关，机关可按警卫的意志控制进入的人员。捕人陷阱的作用是暂时控制目标，进行目标身份的验证和识别。如果目标获得授权可以进入，内部的门就会打开，允许目标进入。如果目标未获授权，内外两道门都保持关闭锁紧状态，直到陪护人员(比较典型的是警卫或者警察)到来，陪同目标离开或者是因为擅自闯入被捕(这称为“延迟特性”)。捕人陷阱通常兼具防止捎带和尾随两种功能。

物理安全的另一个重要部件(尤其对于数据中心、政府设施和高安全组织)是安全隔离桩，其作用是防止车辆的闯入。这些隔离桩可能是固定的永久设施，也可能是在固定的时间或响起警报时，自动从基座升起。隔离桩经常伪装成植物或其他建筑部件。

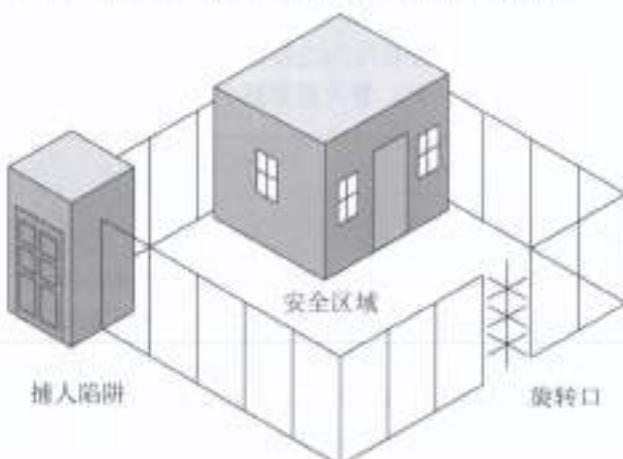


图 10.4 具备捕人陷阱和旋转门的安全物理边界

2. 照明

“照明”也是常用的边界安全控制形式，照明的主要目的是阻止偶然的闯入者、穿越者、盗贼，或是有偷盗企图想趁着黑暗浑水摸鱼的人。但由于照明不是一种强有力的阻止措施，除非在低安全等级场所，否则不能将照明作为主要的或单一的安全防护机制。

照明不应暴露保安、警犬、巡逻岗或是其他类似的安全警卫。照明应与保安、警犬、CCTV

及其他形式的入侵检测或监控机制结合在一起使用。照明一定不能干扰周围居民、道路、铁路、机场等的正常生活与运行。同时，也不能直接或间接照射保安、警犬与监视设备，以免在出现闯入情况时，帮了攻击者的忙。

用于边界保护的照明，一般业界接受的标准是：关键区域的照明强度应达到 2 尺烛光。使用照明的另一个问题是探照灯的位置，使用标准建议灯杆应立在照明区域“盲径”远的距离。例如，如果照明区域的直径是 40 英尺，那么灯杆就应该立在 40 英尺远的位置。

3. 安全警卫与警犬

所有的物理安全控制，无论是静态的威慑，还是主动探测与监控机制，最终都需要人员进行干预，来阻止真实的入侵与攻击行为。安全警卫的职责就在于此。警卫可站在边界或内部，时刻监视着出入口，也可能时刻注视着探测与监控画面。警卫的优点在于他们能够适应各种条件并对各种情况做出反应。警卫能够学习并识别出攻击活动及模式，可以针对环境的变化做出调整，能够做出决策并发出判断指令。当现场需要进行快速情况处理与决策时，安全警卫的作用就显得独一无二。

然而，不幸的是，安全警卫并不是完美无缺。部署、维持及依靠安全警卫也存在诸多不利方面。不是所有环境与设施都适合安全警卫。这可能是由于环境与人的不相容，也可能是由于设施的布局、设计、位置与构造的限制。而且不是所有的安全警卫都可靠。预筛选、团队建设与训练并不能保证安全警卫的胜任与可靠。

即使安全警卫最初是可靠的，他们会受伤或生病，也会休假，也可能心不在焉，难以抵御社会工程攻击，也可能因为滥用药物而被解雇。此外，安全警卫通常是在危害到他们自身安全的时候才会提供保护。警卫也并不清楚设施的整体运营，因此也无法做到面面俱到，对每一种情况都会做出反应。最后，安全警卫是很昂贵的。

警犬可以替代安全警卫的作用，经常作为边界安全控制。警犬是一种非常有效的探测与吓阻手段。然而，使用警犬也是有代价的，警犬需要精心喂养，需要昂贵的保险以及认真看护。



真实场景

部署物理访问控制

在现实世界中，需要部署多层次的物理访问控制，管理设施中授权与未授权人员的流动。

最外层的是照明，场所的外侧边界应照射得明亮清晰。这样既有利于轻松识别人员、发现入侵企图，又可以威慑潜在入侵者。紧挨边界，应设置防止非法人员闯入的围栏或围墙。围栏或围墙的入口与出口是特殊的控制点。这些控制点无论是门、旋转门还是捕人陷阱，都应处于CCTV 或警卫的监视之下。隔离柱能防止车辆冲撞入口。所有入口的人员都需要经过识别与验证才允许进入。

在设施内部，应明显划分隔离出敏感性或保密性级别不同的区域。公共区域及访客区域也应如此。当人员从一个区域进入另一个区域时，需要另外的鉴别/验证过程。最敏感的资源与系统应位于设施的中心或核心位置，并只向权限最高的人员开放。

10.3.2 内部安全控制

如果在设施中建立限制区来控制物理安全，就需要采取针对访客的控制措施。通常的做法是为访客指定一名陪护人员，这样访客的出入与活动就会受到密切监视。允许外来人员进入保护区，却没有对其行为进行监控，不利于受保护资产的安全。采用钥匙(key)、密码锁(combination lock)、胸卡(badge)、动作探测器(motion detector)、入侵警报(intrusion alarm)等也是控制访客的有效手段。

1. 钥匙与密码锁

门锁的作用是锁紧关闭的门。门锁的设计与使用是为了防止未经授权人员的出入。“锁”是一种较原始的识别与身份验证机制。拥有了正确的钥匙或密码，就可以视为是获得了授权与进入许可。钥匙锁是最常见、最便宜的物理安全控制装置，常称为“预设锁具”。这些类型的锁具容易打开，这一类针对锁具的攻击，称为“shimming 攻击”。



真实场景

锁具的使用

钥匙还是密码锁——应该如何选择与使用？

常有一些健忘的用户。Elise 总是忘记她的锁密码，Francis 上班时也经常忘带门禁卡，管理员 Gino 处理问题的风格比较悲观，他很想在合适位置，充分发挥密码锁及门禁卡的作用。

在什么场合或条件下使用密码锁，在哪里需要钥匙或门卡？如果有人获取了密码或捡到钥匙，哪一种配置选项会带来极大风险？这些单点故障会不会给受保护资产带来很大风险？

比较典型的情况是，很多组织在设施内的不同区域，采取不同形式的钥匙或密码锁。

例如，钥匙与门禁卡在其共享入口使用(从外部进入大楼、进入内部房间)，密码锁用来控制单一入口的出入(存储间、文件柜等)。

可编程锁与密码锁的控制功能强于预置锁。有些种类的可编程锁能设置多个开锁密码，还有一些配备小键盘、智能卡或带加密功能的数字电子装置。例如，有一种“电子访问控制(EAC)锁”使用了三种部件：一个电磁铁控制门保持关闭状态，一个证书阅读器验证访问者，并使电磁铁失效(打开房门)，还有一个传感器在门关闭后让电磁铁重新吸合。

锁能替代警卫充当边界入口的访问控制设备。警卫可以查验人员身份，打开或关闭大门控制人员出入。锁本身也具备验证功能，也可以允许或限制人员的进入。

2. 胸卡

“胸卡、身份卡以及安全标识”是不同形式的物理身份标识和/或电子访问控制装置。胸卡可以很简单，上面只记录持有者的姓名简单表明持有者的身份(员工还是访客)。也可以像智能卡与令牌装置那样复杂，采用多因素身份验证技术来验证、证明持有者身份，合法的持有者有资格进入设施、特殊的房间或安全工作站。胸卡上通常会贴照片，带存储加密数据的磁条以及个人信息，以便警卫进行身份验证。

胸卡主要在由安全警卫控制的物理访问环境中使用。在这样的情况下，胸卡对于警卫来说

就是可见的身份工具。警卫可通过对比人员与胸卡上的照片来验证身份，然后查找示质的或电子的获授权人员名册，最后确定是否允许持卡人通过。

胸卡也可在配备扫描仪没有警卫看守的环境中使用。在此情况下，胸卡既能用于身份识别也能用于身份验证目的。胸卡用作身份标识时，胸卡先要在设备上刷一下，持卡人再提供一种或多种的身份验证因素，如密码、口令或生物特征(如果使用生物身份验证设备)。胸卡用于身份验证时，持卡人要先提供 ID、用户名等，然后再刷卡进行身份验证。

3. 动作探测器

“动作探测器”或“动作传感器”是一种在特定区域内感知运动或声音的装置。动作探测器的种类很多，包括红外、热量、波动(wave pattern)、电容、光电及被动音频类型。

“红外动作探测器”监视受控区域内的红外照明模式的变化。

“热量动作探测器”监视受控区域内热量级别与模式的变化。

“波动动作探测器”向被监测区域内发射持续的低频超声或高频微波信号，并监视反射信号中的变化与扰动。

“电容动作探测器”感知被监视对象周围电场或磁场的变化。

“光电动作探测器”感知受监视区域内可见光级别的变化。光电动作探测器经常部署在没有窗户、没有光线的内部房间中。

“被动音频动作探测器”监听被监视区域内是否有异常声响。

4. 入侵警报

当动作探测器发现环境中出现异常，会立即触发警报。“警报”是一种独立的安全措施，警报能够启动防护机制，并且/或发出通知信息。

阻止警报(Deterrent Alarms)能启动的阻止手段可能有：关闭附加门锁、关闭房门等。该警报的目的是为了进一步增加入侵或攻击的难度。

驱除警报(Remove Alarms)触发的驱除手段通常包括拉响警报、警铃或打开照明。该类型警报的目的是为了警告入侵者或攻击者，吓阻他们的恶意或穿越行为，迫使他们离开。

通知警报(Notification Alarms)触发时，入侵者/攻击者并无察觉，但系统会记录事件信息并通知管理员、安全警卫与执法人员。事件记录的信息可能是日志文件与/或 CCTV 磁带。此类警报保持静默的原因，是为了让安全人员能及时赶到，并抓住图谋不轨的入侵者。

警报也可以按照其安装的位置进行分类：本地的、中心的、或专有的、辅助的。

本地警报系统(Local Alarm System)发出的警报声必须要足够强(声音可能高达 120 分贝)，以保证在 400 英尺以外也能听清。此外，警报系统通常需要有安全警卫进行保护，以免遭受不法分子的破坏。本地警报系统要发挥作用，必须在附近部署安全保卫团队，以便在响起警报时能迅速做出反应。

中心站系统(Central Station System)通常在本地是静默的，在发生安全事件时，站区外监视代理会收到通知警报，安全团队会及时做出响应。大多数居民安保采用的都是此类系统。大多数中心站系统都是知名的或全国范围的大公司，如 Brinks 和 ADT。“专有系统”(Proprietary System)与中心站系统类似，但是，拥有此类系统的组织，在现场会配备组织专属的安保人员，随时待命对安全事件进行响应。

辅助站(Auxiliary Station)系统可附加到本地或中心警报系统中。当安全边界受到破坏时，应

急服务团队收到警报通知，对安全事件做出响应并及时到达现场。此类服务可能包含消防、警察及医疗救护。

在安全方案中可以包含两种或多种上述的入侵与警报系统。

5. 二次验证机制

在使用动作探测器、传感器与警报时，还应配备二次验证机制。随着设备灵敏度的增加，出现误报的情况也非常频繁。此外，小动物、飞鸟、蚊虫以及授权人员也可能会错误地触发警报。部署两种或多种探测器及传感器系统，或是在两种或多种触发机制连续动作时才发出警报，这样可大幅减少误报，同时提高警报通知真实入侵攻击行为的准确性。

CCTV 是与动作探测器、传感器以及警报相关联的安全技术。然而，CCTV 不是一种自动化探测-响应系统。CCTV 需要有专门人员紧盯监视画面，来发现可疑恶意活动并发出警报。安全摄像头拓展了安全警卫的有效探测距离，因此也扩大了监视的范围。许多情况下，CCTV 不作为主要的探测工具，因为雇用专门的视频监控人员费用太高。但是，CCTV 却可以用于自动系统触发后的二次或后续验证机制。事实上，CCTV 与事件记录信息的关系，和审计与审计踪迹的关系相同。CCTV 是一种预防措施，而检查事件记录信息是一种探测措施。



真实场景

二次验证

如以前真实场景里所述，Gino 面临持续的安全风险，因为 Elise 总是忘记(因而需要记下)密码，而 Francis 则经常忘记把门禁卡丢在哪里。如果有人捡到了门禁卡或知道了密码，并知晓如何使用，会发生什么情况？

Gino 的有利条件在于他预先建立的二次验证机制，这既可能是一套门禁卡使用者的面部识别 CCTV，也可能是监视密码输入的监控系统。记录进出人员活动的录像带，对于进行安全事件调查或发现有预谋的非法进入很有帮助。

很多安全系统一发现正在使用的“可疑用户”或“可疑证件”，就会发出通知消息或警报。但对使用者的处理措施，要看具体的系统设置，以及由此可能带来的风险大小。每当 Elise(或是任何一个使用该证件的人)登入系统或 Francis 使用门禁卡时，都应派附近的巡逻或流动安全警卫进行确认。当然，如果让 Elise 与 Francis 的主管去提醒他们，注意密码及门禁卡的正确保管与使用方法，让他们意识到可能存在的潜在风险，也是不错的做法。

6. 环境与生命安全

物理访问控制以及设施安全保护的一个重要方面，就是要保护环境基本要素的完好及人员生命安全。在任何场合、任何条件下，安全最重要的方面就是保护人身安全。因此，防止人身伤害就成为所有安全方案的首要目标。

保护人员安全有一部分就是要维护设施环境的正常有序。如果在短时间内，失去水、食物、空调及电力供应，暂时可能不会危及人员安全。但一些情况下，如果这些基本要素缺失，可能会产生灾难性后果，可能产生更紧急、更危险的问题。洪水、火灾、有毒物质泄漏以及自然灾害都会威胁人员生命安全以及设施的稳定。物理安全应该首先要保护人员生命安全，然后才恢复环境安全以及使 IT 设备所需的基础设施正常工作。

人员始终都应该处于第一位。只有人员安全的情况下，才能考虑解决业务连续性问题。许多组织采纳居住者紧急计划(Occupant Emergency Plan, OEP)，用于在发生灾难后，指导与协助保护人员安全。OEP 提供指导或讲授各种方法，来降低人身面临的安全威胁，如防止受伤、缓解压力、提供安全监视以及保护财产免受灾害的损失。OEP 不解决 IT 相关或业务连续性问题，只是针对人员与一般财产安全。业务连续性计划(Business Continuity Plan, BCP)与灾难恢复计划(Disaster Recovery Plan, DRP)解决的是 IT 及业务连续性与恢复问题。

7. 隐私责任与法律要求

任何组织的安全策略中，也应保护个人信息的安全。并且该安全策略也必须符合业界以及所在辖区的监管要求。

“隐私”的意思就是要保护个人信息，不泄露给任何未授权的个人或实体。在当今的网络世界里，公共信息与私人信息的界线越来越模糊。例如，有关个人上网习惯的信息是私人的还是公共的？如果未经用户的同意，收集此类信息合法吗？收集信息的组织借此获利，却不分一杯羹给用户合理吗？而且，个人信息的内容可能远不只是上网习惯，也可能包含用户的姓名、地址、电话、种族、宗教信仰、年龄等，可能还有用户的健康及医疗记录、金融记录，甚至是犯罪或违法记录。所有这些信息都属于个人身份信息内容，具体参见美国国家标准与技术研究院(NIST)发布的《保护个人身份信息秘密指南》，在线版本见 <https://csrc.nist.gov/publications/detail/sp/800-122/final>。

任何有雇员的组织都需要与个人隐私打交道。因此，隐私是所有组织的中心问题之一。在任何组织的安全策略里，要将保护个人隐私作为核心任务和目标。

GDPR EU 2016/679 是欧盟的一项专门保护公民及其权利与个人信息的法规。尽管美国尚无类似的法律保护本国公民，很多美国公司已经采用 GDPR 的一些条款来吸引、保护雇员与客户，并借此获得在欧盟国家的运营许可。

GDPR 以及很多其他有关人员隐私保护的话题，已在第 4 章中详细讨论。

8. 监管要求

在行业或辖区内运营的组织，在这两个实体或更多实体范围中的行为必然受到法律要求、限制与规定的约束。这些“法律需求”可能涉及软件的使用许可、雇佣条件限制、对敏感材料的处理以及对于安全法规的遵守。

遵守所有适用的法律要求，也是维持安全的关键一环。一个行业或国家（也可能是一州和城市）的法律要求，必须应视为构建安全的基线与基础。

10.4 本章小结

如果没有对物理环境的控制，采用再多的管理类或技术类逻辑访问控制都徒劳无功。如果恶意的攻击者能够进入设施、接触设备，那么他可以为所欲为。

实现与维护物理安全有几个重要元素。其中的一个核心元素是选择或设计存放 IT 基础设施、充当组织运营场所的建筑。首先要制定计划，列出组织的安全需求，强调实现这些安全需求的方法与机制。计划的制定要通过关键路径分析过程来完成。

用于管理物理安全的安全技术可以分为三大类：管理的、技术和现场的。管理类物理安全控制包括设施建造与选择、场站管理、人员控制、意识培训以及应急响应及程序。技术类物理安全控制包括访问控制、入侵检测、警报、CCTV、监视、HVAC、电力供应以及火灾探测与消防。物理安全的现场控制包括围栏、照明、门锁、建筑材料、捕人陷阱、警犬与警卫。

有很多种类的物理访问技术，主要用于控制、监视以及管理对于设施的访问。功能覆盖从威慑到监测各个级别。例如围栏、门、旋转门、捕人陷阱、照明、安全保安、警犬、钥匙锁、密码锁、胸卡、动作探测器、传感器及警报。

技术类控制经常作为访问控制手段来管理物理访问，主要包括智能卡/哑卡和生物鉴别技术。除访问控制以外，物理安全机制的形式还包括审计踪迹、访问日志与入侵检测系统。

配线间与服务器机房是需要保护的重要基础设施。经常用于放置核心网络设备及其他敏感设备。保护的手段包括各类门锁、监控、访问控制及常规的安全检查。

介质存储安全应具备存储库检出系统、上锁的柜子或保险箱以及可重用介质的净化措施。

物理访问控制及设施安全保护的一个重要方面，是保护环境的基本要素及人身安全。在任何情况及任何条件下，安全的首要目标是保护人。防止伤害是所有安全工作最核心的目标，此外，提供清洁的电源、管理环境也很重要。

火灾的探测与消防也不能忽视。在设计火灾探测与消防系统时，除了保护人的安全，还应将由火、烟雾、高温以及灭火剂造成的损失降到最小，尤其是重点保护IT基础设施。

人的安全永远是第一位的。只有人员安全了才能考虑业务连续性问题。

10.5 考试要点

理解为什么没有物理安全就无安全可言。没有对于物理环境的控制，再多的管理类或技术类/逻辑类访问控制也形同虚设。如果有恶意的人员能够获得设施或设备的物理访问，他们可以破坏设备、窃取更改数据，肆意妄为。

能够列出管理类物理安全控制。举出设施建造与选择、场所管理、人员控制、认知培训以及应急响应与程序的例子。

能够列出技术类物理安全控制。技术类物理安全控制有访问控制、入侵检测、警报、CCTV、监视、HVAC、电力供应以及火灾探测与消防。

能够说出物理安全的现场控制。物理安全的现场控制有围栏、照明、门锁、建筑材料、捕人陷阱、警犬及警卫。

了解控制的功能顺序。首先是威慑，其次是阻挡，然后是监测，最后是延缓。

了解选择站点及设计建造设施的要素。选择站点的关键要素有可见性、周围环境的构成、区域的便利性以及自然灾害的影响等。设施设计建造的关键要素，是在建造前要理解组织需要的安全级别，并为此制定周详的计划。

了解如何设计与设置安全工作区。设施中的所有区域不会是相同的访问等级。区域中所放置资产价值或重要度越高，对该区域的访问就应受到越严格的限制。高价值及保密资产应位于设施保护的核心或中心。同时，中央服务器或计算机房应不适宜人常驻。

理解配线间的安全要点。配线间是放置整栋或单层网络电缆的地方，这些电缆将其他重要的设备，如配线架、交换机、路由器、LAN扩展器以及主干通道连接起来。配线间安全的重点

是防止非法进入。如果非法入侵者进入该区域，他们可能会偷盗设备，割扯电缆，甚至会植入监听设备。

理解在安全设施中如何应对访客。若设施中划分了限制区域控制物理安全，就有必要建立访客处理机制。通常是为访客指派一个陪护人员，随身监视访客的出入与活动。如果允许外来者进入保护区域，却没有对其活动进行有效跟踪控制，可能会损害受保护资产的安全。

了解用于管理物理安全的三大类安全控制，并能举出每一类的例子。管理物理安全的安全控制分为三类：管理类、技术类和现场类。理解每一类的使用场合和方法，能够列出每一种的例子。

理解介质存储的安全要求。应设计介质存储设施来安全存储空白介质、可重用介质以及安装介质。需要防护的重点是偷盗、腐烂以及残余数据恢复。介质存储设施保护措施包括：带锁的柜子或保险箱，指定保管员/托管员，设置检入/检出流程，进行介质净化。

理解证据存储的重点。证据存储常用于保存日志、磁盘镜像、虚拟机快照以及其他恢复用数据、内部调查资料及取证调查资料。保护手段包括专用/单独的存储设施、离线存储、活动追踪、hash 管理、访问限制及加密。

了解对于物理访问控制的常见威胁。无论采用哪种形式的物理访问控制，都必须配备安全保卫或其他监视系统，以防止滥用、伪装及捎带。滥用物理访问控制包括打开安全门、绕开门锁或访问控制。伪装是使用其他人的安全 ID 进入设施。捎带则是尾随在其他人身后通过安全门或通道，以躲避身份识别和授权。

理解审计踪迹与访问日志的要求。审计踪迹与访问日志是一种对物理访问控制非常有用的工具。它们既可以由安全保卫手工进行填写，也可以由访问控制设备(智能卡、接近式读卡器)自动记录。同时，还要考虑在入口处安装监视 CCTV。通过 CCTV 可将审计踪迹记录、访问日志与视频监控资料进行对比，这些信息对于重建入侵、破坏与攻击事件全过程至关重要。

理解对于洁净电力的需求。电力公司的电力供应并不一直是持续与洁净的。大多数电子设备需要洁净的电力才能正常工作。因为电力波动而导致的设备损坏时有发生。很多组织采用多种形式来管理各自的电力供应。UPS 是一种自充电电池，能为敏感设备提供持续洁净的电源。甚至在主要电力供应中断的情况下，依然能够持续供电，供电时间从几分钟到几小时不等，时间的长短主要依靠 UPS 的容量及所接设备的数量。

了解与电力相关的常用术语。知道下列术语的定义：故障、停电、电压骤降、低电压、尖峰、浪涌、合闸电流、噪声、瞬态、洁净及接地。

理解对环境的控制。除了电力供应，环境的控制还包括对 HVAC 的控制。主要计算机房的温度应保持在华氏 60~75 度之间(摄氏 15~23 度)。机房的湿度应保持在相对湿度 40%~60%。温度太高可能腐蚀机器，湿度太低可能产生静电。

了解静电的有关知识。即使在抗静电地毯上，如果环境湿度过低，依然可能会产生 20 000 伏的静电放电电压。即使是最低级别的静电放电电压也足以摧毁电子设备。

理解对漏水与洪水管理的要求。在环境安全策略及程序中，应包含对漏水与洪水问题的解决方法。虽然管道漏水不会天天发生，可是一旦发生带来的后果则是灾难性的。水电不容，如果计算机系统进了水，特别是在运行状态，注定会损坏系统。任何可能的情况下，本地服务器机房及关键计算机设备都应远离水源或输水管道。

理解火灾探测及消防系统的重要性。不能忽视火灾探测及消防。任何安保系统的首要目标都是保护人员不受伤害。除了保护人，火灾探测与消防系统还应将由火、烟、高温以及灭火材料造成的损坏降到最低，尤其要保护 IT 基础设施。

理解火灾探测及消防系统可能带来的污染与损害。火灾的破坏因素不但包括火和烟，还有灭火剂，例如水或碳酸钠。烟会损坏大多数存储设备。高温则会损坏任何电子及计算机部件。灭火剂会导致短路、初级腐蚀或造成设备失效。在设计消防系统时，这些因素必须考虑进去。

理解人员隐私与安全。任何情况和任何条件下，安全最重要的方面都是保护人。因此，防止人身伤害是所有安全工作的首要目标。

10.6 书面实验

1. 哪种装置可用于设置组织的边界同时可阻止无意的穿越行为？
2. 基于哈龙的消防技术有什么问题？
3. 消防部门紧急来访后，会留下什么潜在问题？

10.7 复习题

1. 下面哪一个是安全的最重要方面？
 - A. 物理安全
 - B. 入侵检测
 - C. 逻辑安全
 - D. 认知培训
2. 哪种方法可识别出组织对于新设施的需求？
 - A. 逻辑文件审计
 - B. 关键路径分析
 - C. 风险分析
 - D. 发明
3. 哪一类的基础设施处于多个楼层的相同位置，并提供方便的手段将各个楼层的网络设备连接在一起？
 - A. 服务器机房
 - B. 配线间
 - C. 数据中心
 - D. 介质柜
4. 下面哪一类不是致力于安全的设施或场所设计元素？
 - A. 分隔出工作和访客区域
 - B. 限制对更高价值或重要性区域的访问
 - C. 保密资产位于设施的核心或中心
 - D. 设施中的所有地方具有相同的访问权限
5. 要维护最有效率及安全的服务器机房，下面的那一条不必为真？
 - A. 必须与人相容
 - B. 必须使用非水消防系统

- C. 湿度必须要保持在 40%~60%之间
D. 温度必须要保持在华氏 60~75 度之间
6. 对存有可重用可移动介质的存储设施来说，下列哪一种不是典型的安全手段？
A. 设置保管员或托管员
B. 采用检入/检出流程
C. Hashing
D. 对归还的介质做净化处理
7. 下列哪一项是经常由保安警卫的双层门结构，能够暂时扣留进入者，直到通过了身份验证才予以放行？
A. 大门
B. 旋转门
C. 捕人陷阱
D. 接近式探测器
8. 下列哪个是最常见的边界安全设备或技术？
A. 安全警卫
B. 围栏
C. CCTV
D. 照明
9. 下列那一条不是安全警卫的不足之处？
A. 安全警卫通常不了解设施的运营范围
B. 不是所有的环境和设施都适用安全警卫
C. 不是所有安全警卫都可靠
D. 预筛查、团结和训练并不能保证安全警卫的能力和可靠
10. 下列哪一条是水消防系统失效最常见的原因？
A. 缺水
B. 人
C. 离子化探测器
D. 把探测器装在吊顶里
11. 哪一种是最常见也是最便宜的物理访问控制装置？
A. 照明
B. 安全警卫
C. 钥匙锁
D. 围栏
12. 哪一种类型的动作探测器，能感知到被监视物体周围电场或磁场的改变？
A. 波动
B. 光电
C. 热量
D. 电容
13. 下列哪一类不是由物理安全触发的安全警报？
A. 预防类

- B. 阻止类
- C. 驱除类
- D. 通知类

14. 无论采用哪一种物理访问控制，以下哪种行为不能通过配备安全警卫或其他监视系统来防止？

- A. 携带
- B. 间谍
- C. 伪装
- D. 滥用

15. 所有安全工作的首要目标是什么？

- A. 预防信息泄露
- B. 保持完整性
- C. 人身安全
- D. 维持可用性

16. 计算机房中湿度的理想范围是？

- A. 20%~40%
- B. 40%~60%
- C. 60%~75%
- D. 80%~90%

17. 静电电压达到多少时，会对硬盘中存储的数据造成损害？

- A. 4 000
- B. 17 000
- C. 40
- D. 1500

18. B类灭火器不会使用下面的哪种灭火剂？

- A. 水
- B. 二氧化碳
- C. 哈龙或可接受的哈龙替代物
- D. 碳酸钠

19. 哪一类水消防系统最适合计算机设备？

- A. 湿管系统
- B. 干管系统
- C. 预动作系统
- D. 集水系统

20. 在发生火灾或触发消防系统时，下列哪一类不会计算机设备造成损害？

- A. 高温
- B. 灭火剂
- C. 烟雾
- D. 照明

安全网络架构和保护网络组件

本章涵盖的 CISSP 认证考试主题包括：

- ✓ 域 4：通信与网络安全
 - 4.1 在网络架构中实施安全设计原则
 - 4.1.1 OSI 模型和 TCP/IP 模型
 - 4.1.2 互联网协议(IP)网络
 - 4.1.3 多层协议的含义
 - 4.1.4 融合协议
 - 4.1.5 软件定义网络
 - 4.1.6 无线网络
 - 4.2 安全的网络组件
 - 4.2.1 硬件操作
 - 4.2.2 传输介质
 - 4.2.3 网络访问控制(NAC)设备
 - 4.2.4 端点安全
 - 4.2.5 内容分发网络

计算机和网络涉及通信设备、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、数据和人员。本章讨论开放系统互连(OSI)模型，该模型是网络、布线、无线连接、传输控制协议/互联网协议(TCP/IP)和相关协议、网络设备和防火墙的基础。

CISSP 认证考试在“通信与网络安全”域涉及与网络组件(即网络设备和协议)相关的主题，特别是网络组件如何运行及其与安全的相关性。本章和第 12 章将讨论这些知识。请务必阅读并研究这两章中的材料，确保完整了解 CISSP 认证考试的基本内容。

11.1 OSI 模型

协议可通过网络在计算机之间进行通信。协议是一组规则和限制，用于定义数据如何通过网络介质传输(例如双绞线、无线传输等)。在网络发展的早期，许多公司都有自己的专有协议，这意味着不同供应商的计算机之间通信很困难或者根本不能通信。为消除这个问题，国际标准化组织(ISO)在 20 世纪 80 年代早期开发了开放系统互连(OSI)参考模型。具体而言，ISO 7498

定义了 OSI 参考模型(更常用的名称是 OSI 模型)。了解 OSI 模型及其与网络设计、部署和安全性的关系对于准备 CISSP 考试至关重要。

为在网络体系结构中正确实现安全设计原则,充分理解计算机通信中涉及的所有技术非常重要。从硬件、软件到协议、加密等,需要了解许多细节、标准以及要遵循的程序。此外,安全网络架构和设计的基础是对 OSI 和 TCP/IP 模型以及一般的 IP 网络的全面了解。

11.1.1 OSI 模型的历史

OSI 模型不是第一个也不是唯一一个尝试简化网络协议或建立通用通信标准的模型。事实上,当今最广泛使用的 TCP/IP 协议(基于 DARPA 模型,现在也称为 TCP/IP 模型)是在 20 世纪 70 年代早期开发的。OSI 模型直到 20 世纪 70 年代后期才开发出来。

开发 OSI 协议是为给所有计算机系统建立通用的通信结构或标准。实际 OSI 协议从未被广泛采用,但 OSI 协议和 OSI 模型背后的理论很容易被接受。OSI 模型用作协议描述了理想硬件上运行的理想抽象框架或理论模型。因此,OSI 模型已成为一个共同参考。

11.1.2 OSI 功能

OSI 模型将网络任务分为七个不同的层。每层负责执行特定任务或操作,以支持在两台计算机之间交换数据(即网络通信)。这些层始终自下而上编号(参见图 11.1),用名称或层号来表示;例如,第 3 层称为网络层。每一层都按特定顺序排列,以表明信息如何通过不同层次交流传递。每一层直接与上面的层以及下面的层通信,也与通信系统的对等层通信。

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
物理层	1

图 11.1 OSI 模型的表示

OSI 模型是网络产品供应商的开放式网络架构指南。该标准或指南为开发新协议、网络服务甚至硬件设备提供共同的基础。通过使用 OSI 模型,供应商能确保其产品与其他公司的产品集成,并得到各种操作系统的支持。如果所有供应商都开发自己的网络框架,那么不同厂商的产品之间几乎不可能互操作。OSI 模型的真正好处在于表达了网络的实际运行方式。

最现实的意义是,网络通信是通过物理连接发生的(无论物理连接是铜缆上的电子、光纤上的光子还是通过空气传输的无线电信号)。物理设备建立电子信号可从一台计算机传递到另一台

计算机的通道。这些物理设备通道只是 OSI 模型定义的七种逻辑通信类型中的一种。OSI 模型的每一层通过逻辑信道与另一台计算机上的对等层进行通信。这使得基于 OSI 模型的协议能通过识别远程通信实体以及验证所接收数据的来源来支持一种身份验证。

11.1.3 封装/解封

基于 OSI 模型的协议采用“封装”机制。封装是将每个层从上面的层传递到下面的层之前为每个层接收的数据添加头部，也可能添加尾部。当消息被封装在每一层时，前一层的头和有效载荷组合成当前层的有效载荷。当数据通过 OSI 模型层从应用层下移到物理层时发生封装。数据从物理层到应用层向上移动时的逆操作称为解封。封装/解封过程如下：

- (1) 应用层创建一条消息。
- (2) 应用层将消息传递给表示层。
- (3) 表示层通过添加信息头来封装消息。信息通常仅在消息的开头(称为头部)添加；但某些层还会在消息末尾添加内容(称为尾部)，如图 11.2 所示。

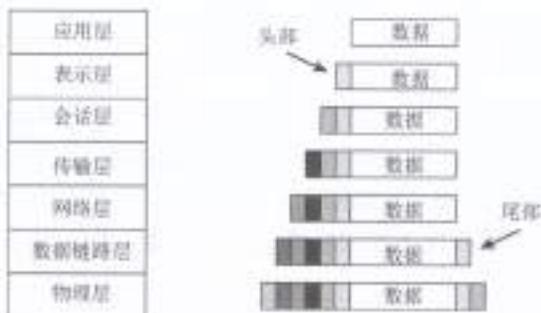


图 11.2 OSI 模型封装的示意图

- (4) 向下传递消息并添加特定层的信息的过程将一直持续到消息到达物理层。
- (5) 在物理层，消息被转换为用比特表示的电脉冲，并通过物理连接传输。
- (6) 接收计算机从物理连接中捕获比特，在物理层中重新创建消息。
- (7) 物理层将消息从位转换为数据链路帧，将消息发送到数据链路层。
- (8) 数据链路层剥离其信息并将消息发送到网络层。
- (9) 执行解封过程直到消息到达应用层。
- (10) 当邮件到达应用程序层时，邮件中的数据将发送给目标收件人。

每层删除的信息包含指令、校验和等，只能由最初添加或创建信息的对等层理解(参见图 11.3)。此信息用于创建逻辑通道，使不同计算机上的对等层能够通信。



图 11.3 OSI 模型对等层逻辑信道示意图

发送到协议栈第七层的信息被称为数据流。它保留数据流的标签(有时是 PDU 的标签)，直至它到达传输层(第 4 层)，在那里被称为段(TCP)或数据报(UDP 协议)。在网络层(第 3 层)中，它被称为数据包。在数据链路层(第 2 层)中，它被称为帧。在物理层(第 1 层)中，数据已被转换为比特，以通过物理连接介质传输。图 11.4 显示了每个层如何通过此过程更改数据。



图 11.4 OSI 模型数据名称

11.1.4 OSI 模型层次

了解 OSI 模型每个层的功能和职责将有助于你了解网络通信的功能、了解如何针对网络通信进行攻击以及如何保护网络通信安全。下面将从底层开始逐层讨论。



注意：

有关 TCP/IP 堆栈的更多信息，请在 Wikipedia(<http://en.wikipedia.org>)上搜索 TCP/IP。

记住 OSI 要充分利用 OSI，首先必须能以正确顺序记住七层的名称。记忆它们的一种常用方法是用每层名称的首字母创建一个助记符，以便更容易记住。最受欢迎的方式是用“Please Do Not Teach Silly People Acronyms”每个单词的首字母分别代表 OSI 的七层，此助记符是从物理层到应用层的。从应用层到物理层的助记符是“All Presidents Since Truman Never Did Pot”每个单词首字母。还有许多其他的 OSI 记忆方案；你只需要知道它们是自上而下还是自下而上即可。

1. 物理层

物理层(第 1 层)接受来自数据链路层的帧，并将帧转换为比特，以便通过物理连接介质进行传输。物理层还负责从物理连接介质接收比特并将它们转换为数据链路层使用的帧。

物理层包含设备驱动程序，它告诉协议如何使用硬件来传输和接收比特。位于物理层的电气规范、协议和接口的标准如下所示：

- EIA/TIA-232 和 EIA/TIA-449
- X.21
- 高速串行接口(HSSI)
- 同步光纤网络(SONET)
- V.24 和 V.35

物理层通过设备驱动程序和这些标准来控制吞吐率、处理同步、管理线路噪声和介质访问，并确定是采用数字信号、模拟信号还是光脉冲通过物理硬件接口传输或接收数据。

在第 1 层(物理层)运行的网络硬件设备是网卡(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所有其他端口(集线器)发送信号或放大信号以支持更大的传输距离(中继器)。

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适当的传输格式。正确格式由网络硬件和技术决定。如以太网(IEEE 802.3)、令牌环(IEEE 802.5)、异步传输模式(ATM)、光纤分布式数据接口(FDDI)和铜线分布式数据接口(CDDI)。但是，只有以太网仍是现代网络中常用的数据链路层技术。在数据链路层中，存在基于特定技术的协议，这些协议将数据包转换为格式正确的帧。格式化帧后，将其发送到物理层进行传输。

下面列出数据链路层中的一些协议：

- 串行线路互联网协议(Serial Line Internet Protocol, SLIP)
- 点对点协议(Point-to-Point Protocol, PPP)
- 地址解析协议(Address Resolution Protocol, ARP)
- 第二层转发(Layer 2 Forwarding, L2F)
- 第二层隧道协议(Layer 2 Tunneling Protocol, L2TP)
- 点对点隧道协议(Point-to-Point Tunneling Protocol, PPTP)
- 综合业务数字网(Integrated Services Digital Network, ISDN)

对数据链路层内的数据处理包括将硬件源和目标地址添加到帧。硬件地址是 MAC 地址，它是一个 6 字节(48 位)的二进制地址并以十六进制表示法编写(如 00-13-02-1F-58-F5)。前 3 个字节(24 位)地址表示网卡制造商。这称为组织唯一标识符(OUI)。OUI 在电气和电子工程师协会(IEEE)注册，并控制其发行。OUI 可用于通过 IEEE 网站发现网卡的制造商。网址是 <http://standards.ieee.org/regauth/oui/index.shtml>。最后 3 个字节(24 位)表示制造商分配给该接口的唯一编号。在同一本地以太网广播域中，没有两个设备可拥有相同的 MAC 地址，否则会发生地址冲突。这是确保企业私有网络中所有 MAC 地址都唯一的好办法。虽然 MAC 地址的设计

应使它们唯一。但供应商错误会产生重复的 MAC 地址。发生这种情况时，必须更换网卡硬件或将 MAC 地址修改成不冲突的地址。



EUI-48 至 EUI-64

几十年来，MAC 地址一直是 48 位，类似的寻址方法是 EUI-48。EUI 代表扩展唯一标识符。最初的基于 IEEE 802 的 48 位 MAC 以太网寻址方案采纳 Xerox 最早的寻址方法。MAC 地址通常用于识别网络硬件，而 EUI 用于识别其他类型的硬件以及软件。

IEEE 认为 MAC-48 是一个过时方案，应弃用并转而支持 EUI-48。

此外，还有从 EUI-48 转换为 EUI-64 的措施。这为未来全球采用 IPv6 以及网络设备和网络软件包数量的指数级增长做好了准备，所有这些都需要一个唯一的标识符。

MAC-48 或 EUI-48 地址可用 EUI-64 表示。在 MAC-48 的情况下，在 OUI(前 3 个字节)和唯一 NIC 规范(最后 3 个字节)之间添加两个额外的 FF:FF 八位字节；例如，cc:cc:cc:FF:FF:ee:ee:ee。在 EUI-48 情况下，另外两个八位字节是 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，你应该熟悉地址解析协议(ARP)。ARP 用于将 IP 地址解析为 MAC 地址。使用 MAC 地址将网段上的流量从其源系统定向到其目标系统。

ARP 作为以太网帧的有效载荷携带，属于第 2 层协议。认为 ARP 属于第 3 层也是有意义的，但 ARP 不能作为真正的第 3 层协议运行，因为它不使用源/目的地寻址方案来引导其报头中的通信(类似于 IP 报头)。相反，它取决于以太网的源和目标 MAC 地址。ARP 不是真正的第 3 层，也不是真正的全 2 层协议，因为它依赖于以太网提供服务，因此它最多是依赖第 2 层协议。OSI 模型是概念模型，而不是对真实协议的严格描述。因此，ARP 并不适合 OSI 组织。

数据链路层包含两个子层：逻辑链路控制(LLC)子层和 MAC 子层。有关这些子层的详细信息对于 CISSP 考试并不重要。

在第 2 层(数据链路层)运行的网络硬件设备是交换机和网桥。这些设备支持基于 MAC 的流量路由。交换机在一个端口上接收帧，并根据目标 MAC 地址将其发送到另一个端口。MAC 地址目的地用于确定帧是否通过网桥从一个网络传输到另一个网络。

3. 网络层

网络层(第 3 层)负责给数据添加路由和寻址信息。网络层接受来自传输层的段，并向其添加信息以创建数据包。该数据包包括源和目标 IP 地址。

路由协议位于此层，包括以下内容：

- 互联网控制消息协议(Internet Control Message Protocol, ICMP)
- 路由信息协议(Routing Information Protocol, RIP)
- 开放最短路径优先(Open Shortest Path First, OSPF)
- 边界网关协议(Border Gateway Protocol, BGP)
- 互联网组管理协议(Internet Group Management Protocol, IGMP)

- 互联网协议(Internet Protocol, IP)
- 互联网协议安全(Internet Protocol Security, IPsec)
- 网络数据包交换(Internetwork Packet Exchange, IPX)
- 网络地址转换(Internetwork Packet Exchange, NAT)
- IP 简单密钥管理(Simple Key Management for Internet Protocols, SKIP)

网络层负责提供路由或传递信息，但它不负责验证信息是否传递成功(这是传输层的责任)。网络层还管理错误检测和节点数据流量(即流量控制)。

非 IP 协议

非 IP 协议是在 OSI 网络层(第 3 层)用来替代 IP 的协议。过去非 IP 协议被广泛使用。然而随着 TCP/IP 的主导和成功，非 IP 协议已成为专用网络的范畴。三种最受认可的非 IP 协议是 IPX、AppleTalk 和 NetBEUI。

IPX 是 20 世纪 90 年代 Novell NetWare 网络上常用的(尽管不是严格要求的)IPX/SPX 协议套件的一部分。AppleTalk 是由 Apple 开发的用于 Macintosh 系统联网的一套协议，最初于 1984 年发布。自 2009 年 Mac OS X v10.6 发布以来，已不再支持 AppleTalk。IPX 和 AppleTalk 都是使用“IP 到备用协议”网关的盲区网络(盲区是使用备用网络层协议而不是 IP 协议的网段)的 IP 替代方案。NetBIOS 扩展用户界面(NetBEUI，又名 NetBIOS Frame 协议或 NBF)是最广为人知的于 1985 年开发的 Microsoft 协议，用于支持文件和打印机共享。Microsoft 通过设计 TCP/IP 上的 NetBIOS(NBT)，在现代网络上启用对 NetBEUI 的支持。还支持服务器消息块(SMB)的 Windows 共享协议，也称为通用互联网文件系统(CIFS)。NetBEUI 作为低层协议不再被支持；只有它的 SMB 和 CIFS 变体仍在使用中。当私有网络中使用非 IP 协议时，存在潜在的安全风险。由于非 IP 协议很少见，因此大多数防火墙无法对这些协议执行数据包标头、地址或有效载荷内容过滤。因此，当涉及非 IP 协议时，防火墙通常必须阻止或允许所有。如果你的组织依赖于仅使用非 IP 协议运行的服务，那么你可能不得不承担通过防火墙传递所有非 IP 协议的风险。这个问题主要存在于当非 IP 协议在专用网络内的网段之间遍历时。但非 IP 协议可封装在 IP 中，以便通过互联网进行通信。在封装情况下，IP 防火墙很少能对此类封装执行内容过滤，因此必须将安全性设置为允许所有或者拒绝所有。

路由器和桥接路由器(brouter)属于在第 3 层运行的网络硬件设备。路由器根据速率、跳数、首选项等确定数据包传输的最佳路径。路由器使用目标 IP 地址来指导数据包的传输。桥接路由器主要在第 3 层工作，但必要时也可在第 2 层工作，会首先尝试路由，如果路由失败则默认为桥接。

路由协议

路由协议有两大类：距离矢量和链路状态。距离矢量路由协议维护目标网络的列表，以及以跳数度量的方向和距离度量(即到达目的地的路由器的数量)。链路状态路由协议维护所有连接网络的拓扑图，并以此映射来确定到目的地的最短路径。距离矢量路由协议的常见示例是 RIP，而链路状态路由协议的常见示例是 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。它接受PDU(可指代协议数据单元、分组数据单元或有效载荷数据单元——即在网络层之间传递的信息或数据的容器)，来自会话层的PDU被转换为段。传输层控制如何寻址或引用网上的设备，在节点(也称为设备)之间建立通信连接并定义会话规则。会话规则指定每个段可包含多少数据，如何验证传输的数据的完整性，以及如何确定数据是否已丢失。会话规则是通过握手过程建立的，因此通信设备都遵循该规则(请参考稍后讨论的传输层协议TCP的SYN/ACK三次握手)。

传输层在两个设备之间建立逻辑连接，并提供端到端传输服务以确保数据传输。该层包括用于分段、排序、错误检查、控制数据流、纠错、多路复用和网络服务优化的机制。以下协议在传输层中运行：

- 传输控制协议(Transmission Control Protocol, TCP)
- 用户数据报协议(User Datagram Protocol, UDP)
- 顺序数据包交换(Sequenced Packet Exchange, SPX)
- 安全套接字层(Secure Sockets Layer, SSL)
- 传输层安全(Transport Layer Security, TLS)

5. 会话层

会话层(第5层)负责建立、维护和终止两台计算机之间的通信会话。它管理对话规则或对话控制(单工、半双工、全双工)，建立分组和恢复的检查点，并重传自上次验证检查点以来失败或丢失的PDU。以下协议在会话层内运行：

- 网络文件系统(Network File System, NFS)
- 结构化查询语言(Structured Query Language, SQL)
- 远程过程调用(Remote Procedure Call, RPC)
- 通信会话可以按下列三种不同的控制模式之一运行：
 - 单工 单向通信。
 - 半双工 双向通信，但一次只能有一个方向发送数据。
 - 全双工 双向通信，可以同时向两个方向发送数据。

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循OSI模型的任何系统都能理解的格式。它对数据强加了通用或标准化的结构和格式规则。表示层还负责加密和压缩。因此，它充当网络和应用程序之间的接口。该层允许各种应用程序通过网络进行交互，并通过确保两个系统都支持的数据格式来实现。大多数文件或数据格式在此层运行，包括图像、视频、声音、文档、电子邮件、网页、控制会话等格式。下面列出表示层中的一些格式标准：

- 美国信息交换标准码(American Standard Code for Information Interchange, ASCII)
- 扩展二进制编码十进制交换模式(Extended Binary-Coded Decimal Interchange Mode, EBCDICM)

- 标签图像文件格式(Tagged Image File Format, TIFF)
- 联合图像专家组(Joint Photographic Experts Group, JPEG)
- 动态图像专家组(Moving Picture Experts Group, MPEG)
- 乐器数字接口(Musical Instrument Digital Interface, MIDI)



真实场景

如此多的协议，如此多的层

有七层和超过 50 个协议，记住每个协议所在的层似乎令人生畏。可创建卡牌，在每张卡牌的正面写下协议名，背面写层名。洗牌后，将每个协议的卡牌放在代表其假定层的堆中。放置完所有协议后，通过查看卡牌背面的层名来检验是否放置正确。重复此过程，直至你能正确放置每张卡牌为止。

7. 应用层

应用层(第 7 层)负责将用户应用程序、网络服务或操作系统与协议栈连接。它允许应用程序与协议栈通信。应用层确定远程通信伙伴是否可用且可访问，还确保有足够的资源来支持所请求的通信。

应用程序不在此层内：相反，这里可找到传输文件、交换消息、连接到远程终端等所需的协议和服务。在该层中可找到许多特定应用程序的协议，例如：

- 超文本传输协议(Hypertext Transfer Protocol, HTTP)
- 文件传输协议(File Transfer Protocol, FTP)
- 行打印后台程序(Line Print Daemon, LPD)
- 简单邮件传输协议(Simple Mail Transfer Protocol, SMTP)
- 远程登录(Telnet)
- 普通文件传输协议(Trivial File Transfer Protocol, TFTP)
- 电子数据交换(Electronic Data Interchange, EDI)
- 邮局协议版本 3(Post Office Protocol version 3, POP3)
- Internet 消息访问协议(Internet Message Access Protocol, IMAP)
- 简单网络管理协议(Simple Network Management Protocol, SNMP)
- 网络新闻传输协议(Network News Transport Protocol, NNTP)
- 安全远程过程调用(Secure Remote Procedure Call, S-RPC)
- 安全电子交易(Secure Electronic Transaction, SET)

有一个在应用层工作的网络设备或服务，即网关。但应用层网关是特定类型的组件，充当协议转换工具。例如，IP 到 IPX 网关从 TCP/IP 获取入站通信，并将它们转换为 IPX/SPX 以进行出站传输。应用层防火墙也在此层运行。其他网络设备或过滤软件可观察或修改该层的流量。

11.2 TCP/IP 模型

TCP/IP 模型(也称为 DARPA 或 DOD 模型)仅由四层组成,而 OSI 参考模型则为七层。TCP/IP 模型的四个层是应用层(也称为进程)、传输层(也称为主机到主机)、互联网层(也称为网络互联)和链路层(尽管使用网络接口,有时也使用网络访问)。图 11.5 显示了它们与 OSI 模型的七个层的比较。TCP/IP 协议套件是在创建 OSI 参考模型之前开发的。OSI 参考模型的设计者注重确保他们的模型与 TCP/IP 协议套件适配,因为开发 OSI 模型时 TCP/IP 协议套件已在网络中建立部署。



图 11.5 将 OSI 模型与 TCP/IP 模型进行比较

TCP/IP 模型的应用层对应于 OSI 模型的第 5、6 和 7 层。TCP/IP 模型的传输层对应于 OSI 模型的第 4 层。TCP/IP 模型的互联网层对应于 OSI 模型的第 3 层。TCP/IP 模型的链路层对应于 OSI 模型中的第 1 层和第 2 层。

通过 OSI 模型对等层名称调用 TCP/IP 模型层已成为常见做法。TCP/IP 模型的应用层已使用了与 OSI 模型相同的名称,因此容易理解。TCP/IP 模型的主机到主机层有时称为传输层(OSI 模型的第 4 层)。TCP/IP 模型的互联网层有时被称为网络层(OSI 模型的第 3 层)。TCP/IP 模型的链路层有时称为数据链路或网络接入层(OSI 模型的第 2 层)。



注意：

由于 TCP/IP 模型层名称和 OSI 模型层名称可互换使用,因此了解在各种上下文中选用模型非常重要。除非另有说明,否则始终假设以 OSI 模型为基础,因为它是使用最广泛的网络参考模型。

TCP/IP 协议套件概述

最广泛使用的协议套件是 TCP/IP,但它不仅是一个协议,而且是一个包含许多单独协议的协议栈(见图 11.6)。TCP/IP 是一种基于开放标准的独立于平台的协议。然而,这既有优势又有

缺点。TCP/IP 几乎支持所有操作系统，但会消耗大量系统资源并且相对容易被入侵，因为它的设计初衷是易用性而不是安全性。



图 11.6 TCP/IP 四层协议及其组件

可使用系统之间的虚拟专用网络(VPN)链接来保护 TCP/IP。VPN 链接经过加密，可增强隐私、保密性和身份验证，并保持数据完整性。用于建立 VPN 的协议有 PPTP、L2TP、SSH、OpenVPN(SSL/TLS VPN)和 IPsec。提供协议级安全性的另一种方法是使用 TCP 封装器。TCP 封装器是一种可作为基本防火墙的应用程序，它通过基于用户 ID 或系统 ID 限制对端口和资源的访问。使用 TCP 封装器是一种基于端口的访问控制。

1. 传输层协议

TCP/IP 的两个主要传输层协议是 TCP 和 UDP。TCP 是一种面向连接的全双工协议，而 UDP 是一种无连接单工协议，在两个系统之间使用端口建立通信连接。TCP 和 UDP 都有 65 536 个端口。由于端口号是 16 位二进制数，因此端口总数为 2^{16} 或 65 536，编号为 0 到 65 535。端口只是通信链路两端在传输层内传输数据时同意使用的地址编号。端口允许单个 IP 地址同时支持多个通信，每个通信使用不同端口号。IP 地址和端口号的组合称为套接字。

这些端口中的前 1024 个(0-1023)称为众所周知的端口或服务端口。这是因为对它们支持的服务进行了标准化分配。例如，端口 80 是 Web(HTTP)流量的标准端口，端口 23 是 Telnet 的标准端口、端口 25 是 SMTP 的标准端口。这些端口是专门预留给服务器用的(换句话说，不能用作客户端请求的源端口)。你可在稍后的“通用应用层协议”部分找到需要了解的端口列表。

端口 1024-49 151 称为已注册的软件端口。这些端口具有一个或多个专门在 IANA(互联网编号分配机构，网址是 www.iana.org)注册的网络软件产品，以便为尝试连接其产品的客户提供标准化的端口编号系统。

端口 49 152-65 535 被称为随机、动态或临时端口。它们通常被客户端随机地临时用作源端口。在初始服务或注册端口之外在客户端和服务器之间协商数据传输管道时，一些网络服务

也使用这些随机端口，例如 FTP。

端口号

IANA 建议将端口 49 152~65 535 用作动态和/或专用端口。但并非所有操作系统都遵守此规定。网址 <https://www.cymru.com/jtk/misc/ephemeralports.html> 列举了操作系统用于随机端口的各种范围的示例。关键是除了较低的 0~1023 端口只保留供服务器使用外，任何其他端口都可用作客户端源端口。只要它尚未在该本地系统上使用即可。

TCP 在 OSI 模型的第 4 层(传输层)上运行。它支持全双工通信，面向连接，并采用可靠的会话。TCP 面向连接，在两个系统之间使用握手过程来建立通信会话。完成该握手过程后，建立可支持客户端和服务器之间的数据传输的通信会话。三次握手过程(图 11.7)如下：

- (1) 客户端将 SYN(同步)标记的数据包发送到服务器。
- (2) 服务器以 SYN/ACK(同步和确认)标记的数据包响应客户端。
- (3) 客户端以 ACK(确认)标记的数据包响应服务器。

通信会话完成后，有两种方法可断开 TCP 会话。首先，最常见的是使用 FIN(完成)标记的数据包。一旦所有数据被传输，会话的每一侧都将发送 FIN 标记的分组，触发对方用 ACK 标记的分组进行确认。因此，需要四个数据包来优雅地终止 TCP 会话。其次是使用 RST(重置)标记的数据包，这导致会话立即或突然终止(请参阅稍后有关 TCP 标头标志的讨论)。

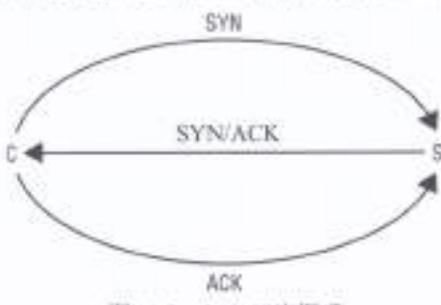


图 11.7 TCP 三次握手

TCP 传输的段用序列号标记。这允许接收器通过将接收的段重新排序来重建原始通信，不管它们被接收的顺序如何。通过 TCP 会话传送的数据定期通过确认进行验证。通过将 TCP 报头的确认序列值设置为在传输窗口内从发送方接收的最后序列号，接收方将确认发送回发送方。在发送确认分组前发送的分组数称为发送窗口。数据流通过“滑动窗口”机制来控制。TCP 能在发送确认之前使用不同大小的窗口(换句话说，发送的数据包数量不同)。较大窗口允许更快的数据传输，但它们应该只用在丢失或损坏数据最少的可靠连接上。当通信连接不可靠时，应使用较小窗口。当需要数据传输时，应采用 TCP。滑动窗口的大小动态变化，因为 TCP 会话的可靠性在使用时会发生变化。在未接收到传输窗口所有分组的情况下，不发送确认。超时后，发送者将再次发送整个传输窗口的数据包。

与 UDP 相比，TCP 报头相对复杂。TCP 报头长度为 20~60 个字节。此报头分为几个部分或字段，如表 11.1 所示。

表 11.1 TCP 报头结构(按报头从头到尾排序)

大小	字段
16	源端口
16	目的端口
32	序列号
4	数据偏移
4	保留供将来使用
8	标志(见表 11.2)
16	窗口大小
16	校验和
16	紧急指针
变量	多种选择：必须是 32 位的倍数

所有这些字段都有独特的参数和要求，其中大部分都超出了 CISSP 考试的范围。但你应该熟悉标志字段的详细信息。标志字段可包含一个或多个指定的标志或控制位。这些标志指示 TCP 数据包的功能，并请求接收方以特定方式响应。标志字段长度为 8 位。每个位置代表单个标志或控制设置。每个位置的值可设置为 1 或者 0。有些条件可同时启用多个标志(如 TCP 三次握手中的第二个数据包可设置 SYN 和 ACK 标志)。表 11.2 详细说明了标志控制位。

表 11.2 TCP 报头标志字段值

标志位指示符	名称	描述
CWR	拥塞窗口减少	用于管理拥塞链路上的传输
ECE	ECN-Echo(显式拥塞通知)	用于管理拥塞链路上的传输；参阅 RFC 3168
URG	紧急	表示紧急数据
ACK	确认	确认同步或关闭请求
PSH	推送	表示需要立即将数据推送给应用
RST	重置	导致立即断开 TCP 会话
SYN	同步	用新的序列号请求同步
FIN	完成	请求正常关闭 TCP 会话

另一个重要消息是 TCP 的 IP 头协议字段值是 6(0x06)。协议字段值是在每个 IP 数据包的报头中找到的标签或标志，它告诉接收系统它是什么类型的数据包。IP 报头的协议字段指示下一个封装协议的标识(换句话说，来自当前协议层的有效载荷中包含的协议，如 ICMP 或 IGMP，或下一层，如 TCP 或 UDP)。把它设想成是从冰箱里拿出的用屠夫纸包裹的神秘肉类包装上的标签。没有标签，你必须打开并检查以弄清楚它是什么。但使用标签，你可快速搜索或过滤以查找感兴趣的项目。有关其他协议字段值的列表，请访问 www.iana.org/assignments/protocol-numbers。