第1章 概 述

学习目标

学完本章，读者应该能够：

- 描述机密性、完整性和可用性的主要安全需求。
- 讨论必须处理的安全威胁和攻击类型，给出针对不同类别计算机和网络资产的威胁和攻击的例子。
- 总结计算机安全的功能需求。
- 描述 OSI X.800 安全体系结构。
- 讨论安全威胁和对策的重要趋势。
- 了解一个全面安全策略的主要方面。

本章对计算机安全进行了概述。首先，讨论了计算机安全的含义。从本质上讲，计算机安全讨论的是与计算机相关的容易受到各种威胁的资产，以及保护这些资产所采取的各种措施。因此，1.2 节简要介绍了用户和系统管理员希望保存和保护的计算机相关资产的分类，这些资产可能受到的各种威胁和攻击。然后，在 1.3 节～1.5 节，从三种不同观点出发分析了处理这些威胁和攻击的措施。接着介绍了计算机安全领域的一些最新发展趋势，并用通用术语给出了计算机安全策略。

本章主要关注(实际上也是本书所关注的)如下三个基本问题：

1. 需要保护什么样的资产？
2. 这些资产会受到什么威胁？
3. 如何对抗这些威胁？

1.1 计算机安全概念

1.1.1 计算机安全的定义

NIST 计算机安全手册[NIST95]对术语计算机安全(computer security)的定义如下：

计算机安全 对自动化信息系统提供的保护，以达到保护信息系统资源(包括硬件、软件、固件、信息/数据和通信)的完整性、可用性和机密性的适用的目标。

这个定义中包括计算机安全核心的三个关键目标：

- **机密性(confidentiality)**：这个术语包含了以下两个相关概念。
  - **数据机密性**[①](data confidentiality)：确保私人或机密信息不能由非授权个人使用或不泄露给未授权的个人。

① RFC2828 定义信息为“能够用多种数据形式表示(编码)的事实或思想”，定义数据是“信息的一种特定的物理表示，通常是一个有意义的符号序列；特别指可以由计算机处理或产生的信息的表示”。安全文献中信息和数据通常并没有太大的区别，本书也不对二者进行区分。

  - **隐私性**(privacy)：确保个人能够控制或影响与他们有关的信息的收集和存储，也能够控制或影响这些信息可以由谁披露或者向谁披露。
- **完整性**(integrity)：这个术语包含了以下两个相关概念。
  - **数据完整性**(data integrity)：确保信息和程序只能以指定和授权的方式修改。
  - **系统完整性**(system integrity)：确保系统在未受损的方式下执行其预定的功能，避免对系统进行有意或无意的非授权操作。
- **可用性**(availability)：确保系统能够迅速地进行工作，并且不能拒绝对授权用户的服务。

这三个概念形成了通常提到的 CIA 三元组(CIA triad)，如图 1.1 所示。这三个概念具体体现了对数据以及信息与计算服务的基本安全目标。例如，NIST 的 FIPS199 标准(联邦信息和信息系统的安全分类标准)将机密性、完整性和可用性列为信息与信息系统的三个安全目标。FIPS PUB199 从需求的角度对这三个目标给出了非常有用的描述，并针对每个分类给出了安全缺失时的定义。

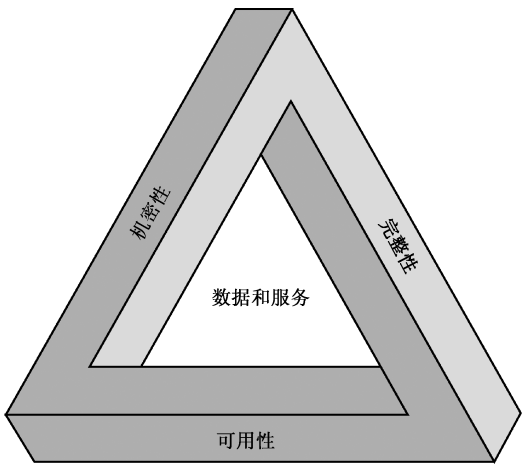

图 1.1　安全需求三元组

- **机密性**：保护对信息访问和泄露的授权限制，包括保护个人隐私和专有信息的措施。机密性缺失是指非授权的信息泄露。
- **完整性**：防范不恰当的信息修改或破坏，包括确保信息的不可否认性和真实性。完整性缺失是对信息非授权的修改或破坏。
- **可用性**：确保及时和可靠地访问和使用信息。可用性缺失是信息或信息系统的访问或使用被破坏。

尽管已确定使用 CIA 三元组来定义安全目标，但在安全领域中，一些人仍认为需要使用额外的概念来对计算机安全进行全面的描述。下面是两个最常提到的概念：

- **真实性**(authenticity)：真实性是一种能够被验证和信任的表示真实的属性，它使得传输、消息或消息源的有效性能够被充分相信。这意味着要验证用户的身份是否与其所声称的一致，每一个到达系统的输入是否来自一个可信的源点。
- **可说明性**(accountability)：一个实体的行为可被唯一追踪到该实体的安全目标，支持抗抵赖(non-repudiation)、威慑(deterrence)、故障隔离、入侵检测和防护，以及事后恢复

和采取法律行动。因为真正安全的系统目前还是不能实现的目标，因此，我们必须能够通过追踪来找到违反安全需求的责任人。系统必须保留他们的活动记录，允许事后取证分析，以跟踪安全违规行为或为解决交易纠纷提供帮助。

注意，FIPS PUB199 将真实性包含在完整性中。

1.1.2 实例

下面通过一些应用程序实例说明刚才列举的要求[①]。在这些例子中，我们将存在安全违规时对机构或个人的影响(即机密性、完整性或可用性缺失)分为三个级别。这些级别定义在 FIPS PUB199 中：

- **低级**：安全缺失会对机构运转、机构资产或个人带来有限的负面影响。有限的负面影响是指，例如，机密性、完整性或可用性缺失可能会：(i)导致任务处理能力一定程度的退化，尽管在此期间机构能够完成其主要职责，但其效率明显降低；(ii)导致机构资产的轻微破坏；(iii)导致轻微的经济损失；(iv)导致轻微的个人伤害。
- **中级**：安全缺失会对机构运转、机构资产或个人带来严重的负面影响。严重的负面影响是指，例如，机密性、完整性或可用性缺失可能会：(i)导致任务处理能力在一定程度上显著退化，尽管在此期间机构能够履行其主要职责，但其效率显著降低；(ii)导致机构资产的显著破坏；(iii)导致显著的经济损失；(iv)导致显著的个人伤害，但不至于丧失生命或严重危及生命。
- **高级**：安全缺失会对机构运转、机构资产或个人带来重大或灾难性的负面影响。重大或灾难性的负面影响是指，例如，机密性、完整性或可用性缺失可能会：(i)导致任务处理能力在一定程度上严重下降或丧失，在此期间机构不能执行其一个或多个主要功能；(ii)导致机构资产的严重破坏；(iii)导致严重的经济损失；(iv)导致严重或灾难性的个人危害，甚至丧失生命或严重危及生命。

机密性 学生的成绩信息可以看作是一种资产，其机密性对学生来说被认为是非常重要的。在美国，这类信息的发布是受家庭教育权利和隐私法案(FERPA)管理的。成绩信息应该只提供给学生、他们的家长以及需要这些信息完成本职工作的员工。学生注册信息具有中等机密等级，虽然它也受 FERPA 保护，但这个信息可以被更多的从事事务性工作的人看到。相对于成绩信息，学生注册信息受到攻击的可能性更小，如果泄露，造成的危害也更小。名录信息(如学生或教师名单、院系列表)可以被分配一个低保密等级或实际上没有任何等级。这种信息一般对公众公开，可以从学校的网站上获得。

完整性 完整性的若干方面可以用存储在数据库中的医院病人过敏信息的例子来加以说明。医生应该相信该信息的正确性和即时性。现在，假设被授权能够查看和更新此信息的职工(例如，护士)故意伪造数据，这会对医院利益造成危害。此时，数据库需要迅速恢复到以前的可信状态，并应该能跟踪追查到错误的责任人。病人过敏信息是一个对完整性要求比较高的信息资产的例子。不准确的信息可能会对病人造成严重伤害甚至导致病人死亡，使医院承担巨大的责任。

---

① 这些例子摘自美国普度大学信息技术安全和隐私办公室出版的安全策略文献中。

一个中等级别完整性要求的资产例子是网站，其为注册用户提供了讨论特定话题的论坛。无论是注册用户还是黑客都可以伪造一些条目或丑化网站。如果论坛仅用于用户娱乐，广告收入很少或根本没有，也不用于一些重要用途，如研究，那么可能的损害并不严重。网站经营者可能仅会承受数据、经济和时间上的损失。

一个低完整性要求的例子是匿名网上投票。许多网站，如新闻机构，向用户进行民意调查却很少有安全保障。然而，这种民意调查的不准确性和不科学性也是很好理解的。

可用性　越关键的组件或者服务，所要求的可用性级别越高。考虑一个为关键系统、应用程序和设备提供鉴别服务的系统。服务中断会导致用户无法访问计算资源，工作人员无法访问他们执行关键任务所需要的计算资源。服务的损失会转化为工作人员工作效率降低、潜在的客户流失等方面的巨大经济损失。

一个通常会被看作具有中等可用性要求的资产的例子是一所大学的公共网站，该网站为当前和未来的学生和捐助者提供信息。虽然这样的网站不是大学信息系统的关键部分，但是它的不可用也会引起一些尴尬。

电话号码簿网上查询程序被归类为低可用性要求等级。虽然其暂时不可用会令人不快，但还可以通过一些其他方式来获取有关信息，如硬拷贝的号码簿或接线员。

1.1.3　计算机安全的挑战

计算机安全既使人着迷，同时也很复杂。一些原因如下：

1. 计算机安全问题并不像初学者看起来那么简单。安全需求看起来是非常直接的，事实上，大多数主要安全服务需求都可以用含义明确的一个词语标签给出：机密性、鉴别、抗抵赖和完整性。但用来满足这些要求的机制可能相当复杂，要理解它们也许涉及相当细致的推理论证。
2. 开发一个特定的安全机制或算法，必须始终考虑对这些安全特性的潜在攻击。在许多情况下，成功的攻击往往是通过以完全不同的方式观察问题而设计的，从而利用机制中不可预见的弱点。
3. 鉴于上述第 2 点原因，用于提供特定服务的规程（procedure）往往是违反直觉的。通常，安全机制的设计是复杂的，不能简单地通过一个特定的安全要求来判断是否需要如此详尽的措施。只有考虑到威胁的各方面而精心设计的安全机制才是合理的。
4. 对于已经设计出的各种安全机制，需要决定其适用场合。这包含物理位置（例如，在网络中的哪些点需要特定的安全机制）和逻辑意义［例如，在一个架构，如 TCP/IP（传输控制协议/互联网协议）的哪一层或哪几层应该采取安全机制］两个层面。
5. 安全机制通常涉及多种特定算法或协议。它们也要求参与者拥有一些秘密信息（例如，加密密钥），这就产生了该秘密信息的产生、分配和保护的问题。这里可能存在对通信协议的信赖问题，通信协议的行为也许会使安全机制的开发工作复杂化。例如，如果安全机制的正常运作需要对消息从发送端到接收端的传输时间设置时限，那么任何协议或网络引入的可变的、不可预测的延迟都可能会导致此类时限失去意义。
6. 从本质上讲，计算机安全是攻击者试图找到漏洞与设计者或管理员尽力阻止破坏之间的智力较量。攻击者有着很大优势，他或她只需要找到一个安全弱点，而设计师必须找到并消除所有的安全弱点，才能实现真正的安全。

7. 部分用户和系统管理者有一种自然的倾向：在安全故障出现之前，他们认为安全投资几乎没有收效。
8. 安全需要定期的、甚至长期的监测，这在今天短期和超载的环境中是一个困难。
9. 安全往往是在设计完成后被纳入系统之中的，而没有作为设计过程必不可少的一个组成部分来看待。
10. 很多用户(甚至安全管理员)认为，坚固的安全性有碍于信息系统或者信息使用的高效性和用户操作的友好性。

在本书中，当我们调查各种安全威胁和机制时，将会经常遇到上述列举的这些难题。

1.1.4 计算机安全模型

现在，我们介绍一些本书的有用术语，这些术语源自 RFC2828——“Internet 安全术语”①。表 1.1 给出了术语的定义，图 1.2[CCPS09a]说明了其中一些术语之间的关系。我们先从用户或者所有者希望保护的系统资源(system resource)或资产(asset)的概念说起。计算机系统的资产可分类如下：

- **硬件**：包括计算机系统以及其他数据处理、数据存储和数据通信设备。
- **软件**：包括操作系统、系统实用程序和应用程序。
- **数据**：包括文件和数据库，以及与安全相关的数据，比如口令文件。
- **通信设施和网络**：局域网和广域网的通信链路、网桥、路由器等。

表 1.1 计算机安全术语

敌手(威胁代理)(Adversary (threat agent))
攻击系统的实体，或对系统的威胁。

攻击(Attack)
一个来自智能威胁的对系统安全性的攻击，即故意试图逃避安全服务(尤其是在方法或技术的意义上)违反系统安全策略的智能行为。

对策(Countermeasure)
用于减少威胁或脆弱性，消除或者阻止攻击、把可能会导致的危害降至最低、发现和报告攻击以便采取调整行动的动作、设备、程序或技术。

风险(Risk)
损失的期望值，表示一个特定威胁利用一个特定脆弱性带来一个特定有害结果的概率。

安全策略(Security Policy)
一组规则和惯例，指定或调节一个系统或机构如何提供安全服务，以保护敏感和关键的系统资源。

系统资源(资产)(System Resource (Asset))
包含在信息系统中的数据；或系统所提供的服务；或系统能力，如处理能力或通信带宽；或系统设备项目(即一个系统组件：硬件、固件、软件或文档)；或安置系统操作和设备的设施。

威胁(Threat)
潜在的安全侵害，存在于可能违反安全并造成损害的环境、能力、行为或事件的情况下。也就是说，威胁是可能利用脆弱性的潜在危险。

脆弱性(Vulnerability)
系统设计、实施、运行和管理中的缺陷或弱点，可被利用来破坏系统的安全策略。

来源：自 RFC 2828，“Internet 安全术语表”，2000 年 5 月。

① 见第 0 章 RFC 的解释。

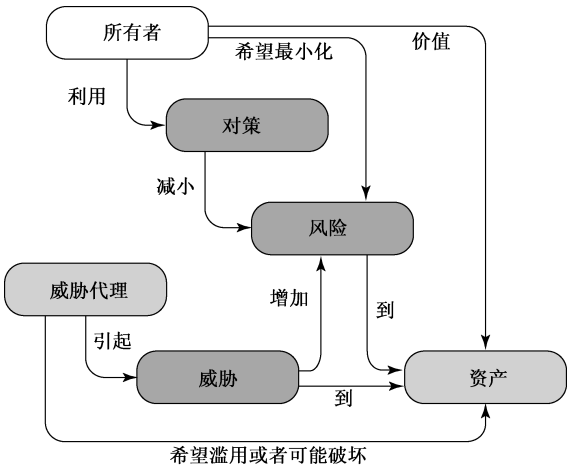

图 1.2　安全概念及其关系

在安全语境中，我们关注的是系统资源的脆弱性。[NRC02]列出了下列计算机系统或网络资产脆弱性的通用类别：

- 系统资源可能被恶意损坏，以至于做出不当的操作或者给出错误的应答。例如，存储的数据值被不恰当地修改而不同于其原始值。
- 系统资源可能被泄露。例如，不应该访问部分或全部信息的人通过网络获得这样的访问。
- 系统资源可能变得不可用，或者非常慢。也就是说，无法使用系统或网络。

这三种类型的脆弱性对应本节在前面列举的完整性、机密性和可用性的概念。

与系统资源的各类脆弱性对应的是能够利用这些脆弱性的威胁。威胁代表对资产可能的安全危害。攻击(attack)是指被实施的威胁(威胁行为)，如果成功的话，会导致不期望的安全危害或威胁后果。执行攻击的代理称为攻击者或威胁代理(threat agent)。我们可以把攻击区分为以下两种类型。

- **主动攻击**：试图改变系统资源或影响其运行的攻击。
- **被动攻击**：试图获悉或使用系统信息，但不影响系统资源的攻击。

也可以根据攻击的来源对攻击进行分类：

- **内部攻击**：由安全边界内的实体(“内部人员”)发起的攻击。被授权访问系统资源的内部人员，以未授权的方式使用它们。
- **外部攻击**：外部非授权或非法用户(“外部人员”)发起的攻击。在 Internet 上，潜在的外部攻击者从业余恶作剧者到有组织的罪犯、国际恐怖分子和敌对政府。

最后，对策是对付安全性攻击所采取的任何手段。理想情况下，可以设计出防止特定类型攻击的对策。在某些情况下，当防止不可能或失效时，目标是检测攻击，然后从攻击的影响中恢复。对策本身可能会引入新的安全脆弱性。在任何情况下，执行安全对策后都会遗留一些脆弱性。这些脆弱性可能被威胁代理利用，表现为资产的残余风险级别。资产所有者将通过制定其他约束以尽量减少这种风险。

1.2 威胁、攻击和资产

现在，我们对威胁、攻击和资产给出更详细的分析。首先，介绍必须处理的各类安全威胁，然后给出一些针对不同类别资产的威胁类型的例子。

1.2.1 威胁和攻击

表 1.2 在 RFC2828 的基础上介绍了四种类型的威胁后果，并列出了导致每一种威胁后果的攻击类型。

非授权泄露是对机密性的威胁。以下类型的攻击会导致这种威胁后果：

- **暴露**：这可能是故意的，如内部人员蓄意泄露敏感信息(如信用卡号)给外部人员。它也可能是一个人为的、硬件或软件错误，从而导致其他实体获得非授权的敏感数据。已经有不少这样的实例，如一些大学不经意地把学生的敏感信息公布在网络上。
- **截获**：截获是通信环境中的一个常见攻击。在共享式局域网络(LAN)中，如无线 LAN 或广播以太网上，连接到 LAN 的任何移动设备都可以接收到发给其他设备的数据包的副本。在 Internet 上，一个有目的的黑客可以获取电子邮件流量和其他数据传输。所有这些情况会导致潜在的对数据的非授权访问。
- **推理**：通信量分析是大家熟知的推理的例子。敌手通过对网络模式或通信量的观察获取信息，如网络上特定主机之间的通信量。另一个例子是，从用户只有有限访问的数据库中推理详细信息，这是通过组合多次查询的结果而实现的。
- **入侵**：入侵的例子是敌手克服系统的访问控制保护获得对敏感数据的非授权访问。

欺骗是对系统的完整性或数据的完整性的威胁。以下类型的攻击可以导致这种威胁后果：

- **冒充**：冒充的一个例子是非授权用户试图通过冒充授权用户获得对系统的访问，如果非授权用户知道一个授权用户的登录 ID 和口令，就可能发生这种情况。另一个例子是恶意软件，如木马，看起来像是执行有用或者预期的功能，实际上获得了对系统资源的非授权访问或诱骗用户执行其他恶意逻辑。
- **伪造**：指改变或者替换一个文件或数据库中的有效数据，或引入虚假数据。例如，学生可能会更改他或她在学校数据库的成绩。
- **抵赖**：在这种情况下，用户可以否认曾经发送数据，或者用户否认接收或处理数据。

破坏是一种对系统可用性或完整性的威胁。以下类型的攻击可以导致这种威胁后果：

- **丧失能力**：这是一种对系统可用性的攻击，会导致物理破坏或系统硬件损坏的结果。更典型的是恶意软件，如特洛伊木马、病毒或蠕虫，可能以这样一种方式工作，如禁用系统或某些服务。
- **损坏**：这是一种对系统完整性的攻击。在此上下文中，恶意软件可能以这样的方式运行，使系统资源或服务以非预期的方式运行。或者，用户可能获得对系统的非授权访问，修改它的一些功能。后者的一个例子是用户在系统中设置后门逻辑，通过非正常程序提供对系统及其资源的后续访问。

- **阻碍**：阻碍系统运行的方法之一，通过禁用通信链路或更改通信控制信息干扰通信。另一种方式是对通信流量或处理资源施加过多的负担使系统超载。

篡夺：是对系统完整性的一个威胁。以下类型的攻击可以导致这种威胁后果：

- **盗用**：这包括服务窃取。一个例子是分布式拒绝服务攻击，恶意软件被安装在大量主机上，这些主机被用作向目标主机加载流量的平台。在这种情况下，恶意软件非授权地使用处理器和操作系统资源。
- **误用**：无论是恶意软件还是黑客获得对系统的非授权访问都会发生误用。在这两种情况下，安全功能可以被禁用或阻碍。

表 1.2　威胁后果及导致每种后果的威胁行为的类型

威胁后果	威胁行为(攻击)
非授权泄露 实体未经授权获得对数据的访问的情况或事件	**暴露**：敏感数据被直接泄露给非授权的实体 **截获**：非授权实体直接访问授权的源和目的之间传输的敏感数据 **推理**：非授权实体通过基于特征的推理或通信产品间接访问敏感数据(但不一定是通信中的数据)的威胁动作 **入侵**：非授权的实体绕过系统的安全保护措施获得对敏感数据的访问
欺骗 导致授权实体收到虚假数据并相信其真实性的情况和事件	**冒充**：非授权实体冒充授权实体以获得对系统的访问或执行恶意行为 **伪造**：以虚假数据欺骗授权实体 **抵赖**：一个实体通过虚假地否认对行为的责任而欺骗另一个实体
破坏 中断或阻止系统的服务和功能正确运行的情况或事件	**丧失能力**：通过禁用系统组件阻止或中断系统运行 **损坏**：通过对系统功能或数据的不利修改对系统运行进行不期望的改变 **阻碍**：通过阻止系统运行来中断系统服务交付的威胁行为
篡夺 导致非授权实体控制系统服务或功能的情况或事件	**盗用**：实体非授权地逻辑或物理控制系统资源 **误用**：导致系统组件执行对系统安全有害的功能或服务

来源：基于 RFC2828。

1.2.2　威胁和资产

计算机系统的资产可以被归类为硬件、软件、数据、通信线路和网络。在本小节中，我们简要介绍一下这四类资产，并把它们与(见图 1.3 和表 1.3)1.1 节中介绍的完整性、机密性和可用性的概念联系起来。

表 1.3　对计算机和网络资产的威胁举例

	可用性	机密性	完整性
硬件	设备被盗或禁用，因而拒绝提供服务		
软件	程序被删除，拒绝用户访问	对软件的非授权复制	修改运行程序，使其在执行过程中失败或执行一些不期望的任务
数据	文件被删除，拒绝用户访问	非授权读取数据。分析统计数据来揭露隐含数据	修改已有的文件或伪造新文件
通信线路	消息被破坏或删除，通信线路或网络不可用	消息被读取，消息的通信模式被观察到	消息被修改、延迟、重新排序，或复制。伪造虚假消息

硬件　对计算机系统硬件的主要威胁是对其可用性的威胁。硬件最容易受到攻击，且对自动控制最不敏感。威胁包括意外和故意损坏设备以及盗窃。个人计算机和工作站的流行和局域网的广泛使用，增加了该领域遭受损失的可能性。盗窃 CD-ROM 和 DVD 会导致机密性受损。应对这些威胁需要采取物理和行政的安全措施。

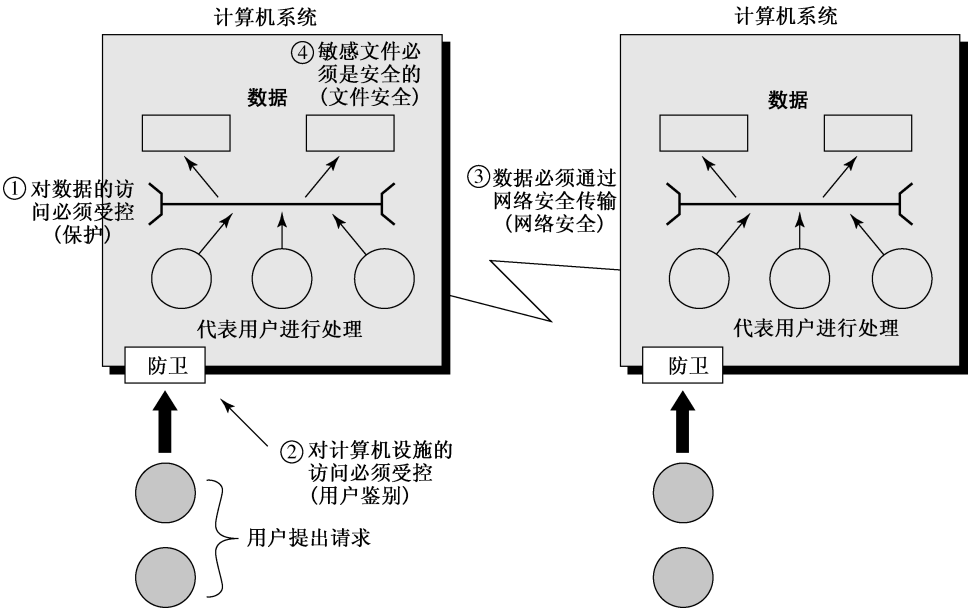

图 1.3 计算机安全的范围(说明:本图描绘的安全问题,除了物理安全,包括控制对计算机系统的访问,保护通信系统的数据传输,保护存储数据)

软件 软件包括操作系统、实用工具和应用程序。对软件的主要威胁是对软件可用性的攻击。软件,特别是应用软件,往往容易被删除。软件也可能被更改或被损坏而不能使用。谨慎的软件配置管理(包括备份软件的最新版本)能够保持其高度可用性。更难处理的一个问题是对软件的修改,程序虽然可以运行,但与以前的行为大不相同,这是对软件完整性/真实性的威胁。计算机病毒及相关攻击就属于这一类。最后一个问题是保护软件不被盗版。虽然某些措施是可用的,但总的来说,软件的非授权复制问题还一直没有得到解决。

数据 硬件和软件安全通常由计算中心的专家或个人电脑用户关注。一个更普遍的问题是数据的安全性,其中包括由个人、团体和企业机构控制的文件和其他形式的数据。

数据方面的安全问题是广泛的,涵盖可用性、机密性和完整性。就可用性而言,值得关注的是数据文件,它可能发生意外或恶意的损坏。

对机密性最主要的威胁是非授权读取数据文件或数据库,与计算机安全其他领域相比,这个领域也许一直需要进行更多的研究和付出更多的努力。一个不太明显的机密性威胁涉及数据分析,这体现在提供概括或汇总信息的所谓统计数据库的使用中。假定已有的汇总信息不会威胁个人隐私。然而,由于统计数据库使用的增长,个人信息泄露的可能性越来越高。从本质上讲,组成个体的特征通过仔细分析可以识别出来。例如,如果一个表记录了受访者 A、B、C 和 D 的收入总额,而另一个表记录了 A、B、C、D 和 E 的总收入,两个汇总之间的差就是 E 的收入。对合并数据集合的期望的日益增长更激化了这个问题。许多情况下,匹配几个数据集时,为了保持不同汇总级别的一致性,需要访问每个单元。因此,个体单元作为隐私关注的主体,在数据集处理各阶段都是可获得的。

最后,数据完整性是大多数安装中的一个主要问题。对数据文件的修改产生的后果可能很小也可能很严重。

通信线路和网络　网络安全攻击可以划分为被动攻击和主动攻击。被动攻击会企图了解或利用系统信息，但不影响系统资源。主动攻击则试图改变系统资源，或影响它们的运行。

被动攻击具有窃听、监视传输的性质。攻击者的目标是获取传输的信息。两种类型的被动攻击是消息内容泄露和流量分析。

消息内容泄露很容易理解。电话通话、电子邮件和传输文件都可能包含敏感或机密信息。我们希望能阻止敌手了解传输的内容。

第二种类型的被动攻击是流量分析，其更加巧妙。假设我们有办法隐藏消息的内容或其他信息流量，这样，即使攻击者捕获了消息，也不能从该消息中提取出信息。通常用来隐藏消息内容的技术是加密。即使我们恰当地进行了加密保护，敌手仍然可能观察到这些消息的模式。敌手可以确定通信主机的位置和身份，并能观察到被交换消息的频率和长度。这些信息对于判断正在发生的通信的性质可能是有用的。

被动攻击很难觉察，因为它们不涉及对数据的修改。通常，信息流量表面上以正常的方式发送和接收，收发双方都没有意识到第三方已读取该消息或观察到通信模式。尽管如此，通过使用加密的方法防止这些攻击是可行的。因此，对付被动攻击的重点是预防，而不是检测。

主动攻击涉及数据流的修改或伪造数据流，它可以划分为四类：消息的重放、假冒、篡改和拒绝服务。

重放涉及数据单元的被动捕获及其后续的重发，以产生非授权的效果。

当一个实体假装成另一个不同的实体时就发生了**冒充**。冒充攻击通常涉及其他形式的主动攻击。例如，有效的身份鉴别序列发生之后，鉴别序列可被捕获和重放，从而使拥有较少特权的实体冒充另一个有额外特权的实体，并获得这些特权。

简单地说，**篡改消息**意味着一个合法消息的某些部分被改变，或消息被延迟或重新排序，从而产生非授权的后果。例如，一条消息“允许 John Smith 读取机密文件账户”被修改为“允许 Fred Brown 读取机密文件的账户”。

拒绝服务阻止或禁止通信设施的正常使用或管理。这种攻击通常有一个具体的目标。例如，一个实体可能禁止所有发送到一个特定目标(如安全审计服务)的消息。另一种形式的拒绝服务是破坏整个网络，使网络失效或超载，从而降低其性能。

主动攻击表现出与被动攻击相反的特征。被动攻击虽然难以检测，但可以采取措施防止它们。另一方面，要完全阻止主动攻击是非常困难的，因为要达到这个目的，就要对所有的通信设施和路径进行不间断的物理保护。因此，目标是检测主动攻击，并从其所导致的破坏或延迟中恢复过来。由于检测具有威慑作用，它也可以对防范起到一定作用。

1.3　安全功能需求

有许多方式可以分类和描绘减少脆弱性并处理系统资产威胁的对策。分析其中的几种方法对于本书其余内容的展开是很有价值的。我们将在本节和接下来的两节完成这个工作。本节分析对策的功能需求，遵循 FIPS PUB200(联邦信息和信息系统的最低安全要求)定义的分类方法。该标准列举了 17 个安全相关的领域，涉及保护信息系统及其处理、存储和传输的信息的机密性、完整性和可用性。这些领域定义在表 1.4 中。

表 1.4 安全需求

访问控制：限制信息系统只能由授权用户或代表授权用户的进程或设备(包括其他信息系统)访问，限制授权用户允许执行的事务和功能类型
意识和培训：(i)确保机构信息系统的管理者和使用者都了解他们活动的安全风险及适用的安全性法律、法规和政策；(ii)确保人员得到充分的培训,以便承担信息安全相关任务和职责
审计与可说明性：(i)建立、保护和保留信息系统的审计记录，以便对非法的、未授权的或不适当的信息系统活动进行监测、分析、调查和报告；(ii)确保个人信息系统的用户活动都可以被唯一追踪到这些用户，使得他们能够为自己的行为负责
认证、认可和安全性评估：(i)定期评估机构信息系统的安全控制措施，确定该控制措施在应用中是否有效；(ii)开发和实施旨在纠正机构信息系统的缺陷并减少或消除其脆弱性的行动计划；(iii)对机构信息系统及相关信息系统连接的运行授权；(iv)实时监控信息系统的安全控制，确保控制措施的持续有效性
配置管理：(i)建立和维护贯穿在各个机构信息系统开发生命周期中的基线配置和清单(包括硬件、软件、固件和文档)；(ii)为机构信息系统采用的信息技术产品建立和实施安全配置
应急计划：建立、维护和实施机构信息系统的应急响应、备份操作和灾后恢复计划，以确保紧急情况下关键信息资源的可用性和连续性
事故响应：(i)建立机构信息系统的运行事故处理能力，包括充分的准备、检测、分析、遏制、恢复和用户响应活动；(ii)跟踪、记录并将事故报告给恰当的机构官员和/或管理机构
维护：(i)定期和及时地维护机构信息系统；(ii)提供用于进行信息系统维护的有效的控制工具、技术、机制和人员
介质保护：(i)保护信息系统纸质和数字化介质；(ii)限制授权用户访问信息系统介质上的信息；(iii)废弃或再次使用前对信息系统介质进行杀毒或销毁
物理和环境保护：(i)限制授权个体对信息系统、设备和相应运行环境的物理访问；(ii)保护信息系统的物理厂房和支撑基础设施；(iii)为信息系统提供配套支持设施；(iv)防止环境对信息系统的危害；(v)为包含信息系统的设施提供适当的环境控制措施
规划：开发、归档、定期更新和实施机构信息系统的信息安全计划，其描述了信息系统的合适及计划的安全控制措施以及个人访问信息系统的行为规则
人员安全：(i)确保机构(包括第三方服务提供商)内担任相应职位的责任人士是值得信赖的，并符合这些职位既定的安全标准；(ii)确保一些人事活动的终止和变换的过程中或之后，机构信息和信息系统是受到保护的；(iii)对不符合机构的安全策略和程序的人员采取正式制裁
风险评估：定期评估机构运行(包括任务、职能、图像或声誉)、机构资产和个人的风险，根据机构信息系统运行和相关的机构信息处理、存储或传输得出
系统和服务获取：(i)分配足够的资源，以充分保护机构信息系统；(ii)在系统开发生命周期中纳入信息安全方面的考虑；(iii)采用软件使用和安装限制；(iv)确保第三方供应商采取足够的安全措施，以保护机构外包的信息、应用程序或服务
系统和通信保护：(i)在信息系统的外部边界和关键的内部边界，监督、控制和保护的机构通信(即机构信息系统发送或接收的信息)；以及(ii)采用架构设计、软件开发技术和系统工程原理，提高机构信息系统信息安全的有效性
系统和信息的完整性：(i)确定、报告并及时纠正信息和信息系统的缺陷；(ii)在机构信息系统的恰当位置提供恶意代码防护；(iii)监测信息系统的安全警报和公告,并采取适当的行动作为响应

列举在 FIP PUB200 中的需求，包含了针对安全脆弱性和威胁的多种对策。我们可以把这些对策粗略地分为两大类：一类要求计算机安全技术的措施(包括在本书的第一部分和第二部分)，要么仅包含硬件或软件，要么两者都包含；另一类基本是管理措施(第三部分涉及)。

每个功能领域都可能涉及计算机安全的技术措施和管理措施。主要要求计算机安全技术措施的功能领域包括：访问控制、标识和鉴别，系统和通信保护，系统和信息的完整性。主要涉及管理控制和程序的功能领域包括：意识和培训，审计和可说明性，认证、鉴定和安全评估，应急计划，维护，物理和环境保护，规划，人员安全，风险评估以及系统和服务的获得。计算机安全技术措施和管理控制都涉及的功能领域包括：配置管理，事件响应和介质保护。

值得注意的是，FIP PUB200 中的功能需求大部分或者主要是管理问题，或者至少有一个重要的管理组件，而不是纯粹的软件或硬件解决方案。这对一些读者可能是新的，并没有反映在许多计算机和信息安全的书籍上。但是，正如一个计算机安全专家指出的，“如果你认为技术可以解决安全问题，那么不是你不明白问题，就是你不了解技术”[SCHN00]。本书反映了用技术和管理相结合的方法来实现有效的计算机安全。

FIPS PUB 200 提供了计算机安全技术和管理方面主要关注领域的有用总结。本书努力涵盖所有这些领域。

1.4　开放系统安全体系结构

为了有效评价一个机构的安全需求，并评估和选择各种安全产品和策略，负责安全的经理需要一种系统化的方式定义安全需求和描述满足这些要求的方法。在集中数据处理环境中这是非常困难的，随着局域网和广域网的使用，该问题被放大。

ITU-T 推荐标准 X.800，即“OSI 安全体系结构(Security Architecture for OSI)”，定义了这样一种系统化的方法。OSI 安全体系结构作为一种机构提供安全的任务的方式，对于管理者是非常有用的。此外，因为这个体系结构是作为国际标准开发的，计算机和通信厂商已经为其产品和服务开发出符合该结构化定义的服务和机制的安全特征。尽管 X.800 重点关注的是网络和通信安全，但其提出的概念也适用于计算机安全。

对我们而言，OSI 安全体系结构为本书将要涉及的许多概念提供了一个有用的抽象介绍。OSI 安全体系结构重点关注安全攻击、安全机制和安全服务，可以简要定义如下：

- **安全攻击**：任何危害机构所拥有的信息的安全性的行为。
- **安全机制**：用于检测、防范或从安全攻击恢复的机制。
- **安全服务**：增强数据处理系统和机构信息传输的安全性的服务。

这些服务是为了对抗安全攻击的，它们采用了一种或多种安全机制来提供该服务。

1.2 节中的对通信线路和网络的威胁小节是基于 X.800 的安全威胁分类的。接下来的两节回顾基于 X.800 架构的安全服务和机制。

国际电信联盟(ITU)电信标准化部门(ITU-T)是联合国资助的机构，主要开发与电信和开放系统互连(OSI)有关的标准和建议，称为推荐标准，请参见附录 C。

1.4.1　安全服务

X.800 将安全服务定义为：通信开放系统通信协议层提供的一种服务，用来确保系统或者数据传输的充分安全性。RFC2828 中的定义也许更为清晰：由系统提供的对系统资源进行特定类型的保护的处理或通信服务；实施安全策略的安全服务由安全机制实现。

X.800 把这些服务分成 6 类共 14 个具体服务(见表 1.5)。我们依次讨论每个类别[①]。需要记住的是，在相当程度上，X.800 关注的是分布式、网络化系统，因此更强调单一系统的计算机安全之上的网络安全。即便如此，表 1.5 还是安全服务的一个有用列表。

---

① 安全文献中使用的许多术语尚未达成广泛的一致。例如，术语“完整性”有时用来指信息安全的所有方面。鉴别一词有时被用来指验证实体的身份，又用来指本章列在完整性下面的各种功能。我们这里的用法与 X.800 和 RFC2828 是一致的。

鉴别 鉴别服务确保通信是真实的。对于一条消息(如警告或报警信号)而言，鉴别服务的功能是向接收者保证消息来自其所声称的发送方。对于正在进行的交互，如终端与主机的连接，涉及收、发双方。首先，在连接初始化时，鉴别服务确保两个实体是真实的，也就是说，每一个实体是它所声称的实体。其次，鉴别服务必须保证连接不被第三方以这样的方式干扰，也就是第三方伪装成合法双方之一，进行非授权的发送或接收。

表 1.5 安全服务

鉴别	数据完整性
确保通信实体是它所声称的实体。	确保接收到的数据与授权实体发送的是完全一样的(即无篡改、插入、删除或重放)。
对等实体鉴别 用于为与一个逻辑连接相关的连接实体的身份提供可信性。	**带恢复的连接完整性** 对一个连接上的所有用户数据提供完整性，检测一个完整数据序列中的任何篡改、插入、删除或重放，并试图恢复。
数据原发鉴别 用于无连接的传输，确保所接收到的数据的来源是所声称的。	**无恢复的连接完整性** 同上，但仅提供检测而无恢复。
访问控制	**选择字段连接完整性** 提供一次连接中传输的数据块中的用户数据选择字段的完整性，并确定选择字段是否已被篡改、插入、删除或者重放。
防止未经授权使用资源(即，该服务控制谁能访问某个资源，在什么条件下可以访问，允许如何访问)。	**无连接的完整性** 提供单一无连接的数据块的完整性保护，可检测数据篡改。此外，可提供有限的重放检测。
数据机密性	**选择字段连接完整性** 提供单一无连接数据块选择字段的完整性保护；确定选定的字段是否已被篡改。
防止非授权的数据泄露。	**抗抵赖**
连接机密性 保护一个连接的所有用户数据。	一个通信中，防止参加全部或部分通信的实体之一否认其行为。
无连接机密性 保护单一数据块中的所有用户数据。	**原发抗抵赖** 证明消息由指定的实体发送。
选择字段机密性 对一个连接或者单一数据块上用户数据的选择字段提供机密性。	**接收抗抵赖** 证明消息被指定的实体接收。
通信流量机密性 防止通过观察通信流量而获得信息。	
可用性	
确保未因影响网络的事件而拒绝对网络元素、存储的信息、信息流、服务和应用的授权访问。灾难恢复解决方案也包括在此类中。	

来源：摘自 X.800，“OSI 安全体系结构”。

标准中定义的两个具体的鉴别服务是：

- **对等实体鉴别：**提供一个连接中对等实体的身份验证。若两个实体在不同的系统中实现了相同的协议(例如，分别处于两个通信系统中的两个 TCP 用户)，被认为二者是对等的。对等实体鉴别适用于连接建立或数据传输阶段。它试图证明实体没有进行假冒或非授权地重放以前的连接。
- **数据原发鉴别：**提供数据单元的来源验证，但它不提供防止复制或修改数据单元的保护。这种类型的服务支持电子邮件之类的通信实体没有事先交互的应用。

访问控制 在网络安全语境中，访问控制是限制和控制通过通信链路访问主机系统和应用程序的能力。要做到这一点，试图获得访问的每个实体必须首先被识别或鉴别，这样才能获得相应的访问权限。

数据机密性　在网络安全语境中，机密性是防止传输数据受到被动攻击。就数据传输的内容而言，保护可以分为若干级别。最广义的服务是保护一段时间内两个用户间传送的所有数据。例如，若两个系统之间建立了一个 TCP 连接，这个广义的保护可以防止在 TCP 连接上传输的任何用户数据的泄露。也可以定义一个更狭义的服务形式，包括单个消息甚至一个消息特定字段的保护。这种狭义保护不如广义保护有用，而且实现起来更加复杂和昂贵。

机密性的另一个方面是防止对通信流量进行分析。这要求攻击者观察不到一个通信设施上传输的流量的信源、信宿、频率、长度或其他特征。

数据完整性　在网络安全语境中，数据完整性与数据机密性一样，可以应用于消息流、单个消息或消息的选定字段。同样，最有用也最简单的方法是对整个数据流的保护。

面向连接的完整性服务处理消息流，用来确保接收到的消息与发送的消息一致，未被复制、插入、修改、重排序或重放。数据的破坏也包含在这项服务中。因此，面向连接的完整性服务可以解决消息流的篡改和拒绝服务问题。另一方面，无连接的完整性服务处理单个信息，而不考虑任何更大范围的上下文，一般仅用来防止消息篡改。

我们需要区分有恢复和无恢复的服务。因为完整性服务与主动攻击有关，我们更关注检测，而不是防范。如果检测到完整性被破坏，该服务可能只是简单地报告违规，如果要从违规中恢复，需要软件的其他部分或人为干预。另外，还有一些恢复数据完整性的机制，我们将在随后谈到。通常，自动恢复机制是一种更具吸引力的选择方案。

抗抵赖　抗抵赖可以防止发送者或接收者否认发送的消息。因此，当消息被发送后，接收者可以证明宣称的发件人发送过消息。同样，当消息被接收后，发送方可以证明宣称的接收者确实收到了消息。

可用性　X.800 和 RFC2828 都将可用性定义为：按照系统的性能规范，能够根据授权实体需求访问和使用系统或系统资源的特性(即，如果用户请求服务时，系统能根据其设计提供服务，则系统是可用的)。多种攻击可能导致可用性的缺失或下降。一些攻击可用自动防御措施来对付，如鉴别和加密，而另一些则需要物理措施阻止或恢复可用性损失。

X.800 将可用性看作是与各种安全服务相关的一个特性。X.805，“端到端通信系统的安全体系结构(Security Architecture for Systems Providing End-to-End Communications)”，明确提到可用性服务。可用性服务是保护系统以确保其可用性的服务。该服务解决了拒绝服务攻击引起的安全问题。它依赖于适当的管理和系统资源控制，从而依赖于访问控制服务和其他安全服务。

1.4.2　安全机制

表 1.6 列出了 X.800 中定义的安全机制。这些机制分为两类，一类在一个特定的协议层(如 TCP 或应用层协议)上实现，另一类不针对任何具体协议层或安全服务。这些机制将在本书的相关章节详细介绍，在此，除了对加密的定义加以说明外，其他内容不予详细描述。X.800 区分可逆加密机制和不可逆加密机制。可逆加密机制是允许数据加密之后再被解密的加密算法。不可逆加密机制，包括哈希算法和消息鉴别码，用于数字签名和消息鉴别应用。

表 1.6 安全机制(X.800)

具体的安全机制	普适安全机制
可结合到适当的协议层,以提供某些 OSI 安全服务。	不针对任何特定的 OSI 安全服务或协议层的机制。
加密 使用数学算法将数据转换成不易于理解的形式。数据的变换和随后的恢复依赖于算法和零个或多个加密密钥。	**可信功能** 就某些准则(例如根据安全策略建立的准则)而言被认为是正确的功能。
数字签名 附加到数据单元之后的数据,或是对数据单元的加密变换,以便数据单元的接收者证明数据单元的来源和完整性,并防止伪造(如被接收方伪造)。	**安全标签** 绑定到资源(可能是数据单元)上的标记,指定该资源的安全属性。
访问控制 实施对资源的访问权的各种机制。	**事件检测** 检测与安全相关的事件。
数据完整性 确保数据单元或者数据流的完整性的各种机制。	**安全审计踪迹** 收集用于安全审计的数据,这是对系统记录和活动的独立的审查和分析。
鉴别交换 通过信息交换旨在确保实体身份的机制。	**安全恢复** 处理来自安全机制(如事件处理和管理功能)的请求,并采取恢复措施。
流量填充 将若干位插入到数据流间隙以阻止流量分析。	
路由控制 对特定的数据启用物理安全的路由,并允许路由变化,特别是当怀疑安全被违反时。	
公证 使用一个可信的第三方,以确保数据交换的某些属性。	

1.5 计算机安全趋势

为了评估各种威胁的相对严重程度和计算机安全性的各种方法的相对重要性,参考一些机构的经验是有用的。一个由计算机安全协会(Computer Security Institute, CSI)实施和提供的有用的调查是 2010/2011 年度 CSI 计算机犯罪和安全调查[CSI10]。受访者包括超过 350 个总部设在美国的公司、非营利机构和公共部门机构。

图 1.4 给出了受访者所经历的 9 大类的攻击类型①。最值得一提的是恶意软件攻击的数量庞大且不断增长。值得注意的是大多数种类的攻击表现出有点下降的趋势。CSI 报告推测,这是由于很大程度上的机构安全技术的提高。

图 1.5 显示了各类机构对抗威胁所采用的安全技术。几乎普遍使用的两个是防火墙和杀毒软件。

这两个软件的流行反映了多种因素:

- 这些技术的成熟度意味者安全管理员非常熟悉这些产品,并对其有效性充满信心。
- 因为这些技术是成熟的,并且有许多厂商提供支持,成本趋向于非常合理,并且用户界面友好。
- 这些技术对抗的威胁在安全管理员面临的最重要的威胁之中。

① 一个完整的列表,包括低发病类别的文件"(攻击类型)Types – of – Attacks. pdf"可在本书的额外内容网站的文档文件夹中得到。

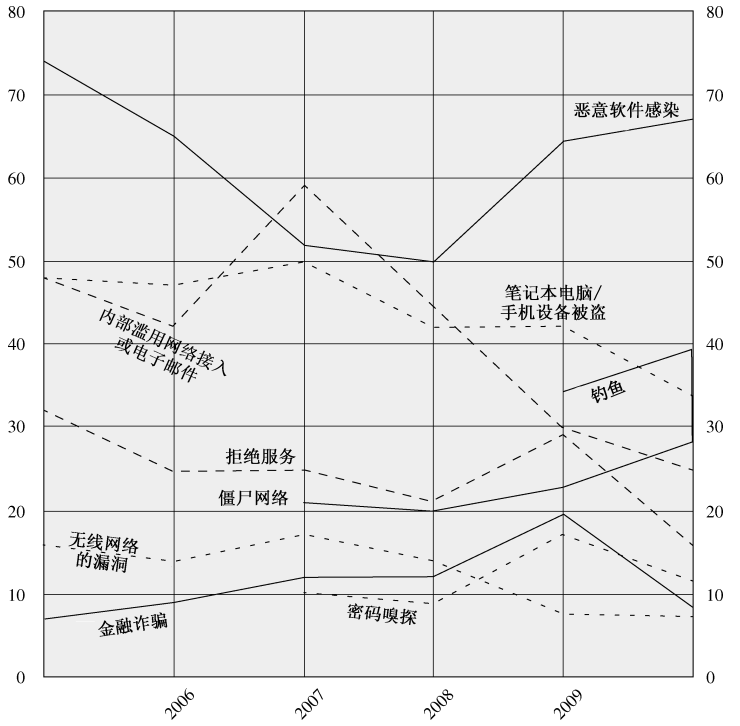

图 1.4　经历的攻击类型(受访者百分比)。资料来源：计算机安全协会2010/2011年度计算机犯罪和安全调查

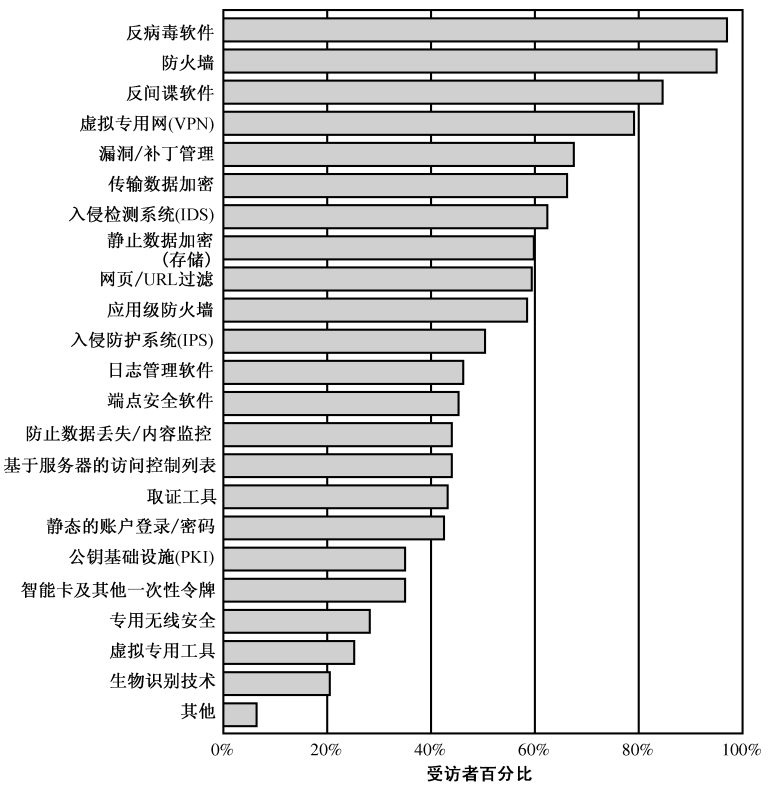

图 1.5　使用的安全技术(资料来源：计算机安全协会 2010/2011 年度计算机犯罪和安全调查)

1.6 计算机安全策略

我们简要归纳一下为提供计算机安全所采用的整体策略并作为本章的总结。[LAMP04]提出全面的安全策略应涉及以下三个方面:

- **规范/策略**:安全方案要实现什么?
- **实施/机制**:安全策略是如何实现的?
- **正确性/保证**:安全策略是否确实起作用了?

1.6.1 安全策略

设计安全服务和机制的第一步是开发一个安全策略。涉及计算机安全的有关方面以多种方式使用术语安全策略。最低限度上,安全策略是期望的系统行为的非形式化描述[NRC91]。这种非形式化策略可以参考安全性、完整性和可用性的要求。更有用的情况下,安全策略是规定或控制系统或机构如何提供安全服务的规则与实践的形式化描述,安全服务以保护敏感和关键的系统资源为目的(RFC2828)。这种形式化安全策略可通过系统的技术控制及管理和运行控制措施予以实施。

在开发安全策略时,安全管理者需要考虑以下几个因素:

- 需要保护的资产的价值。
- 系统的脆弱性。
- 潜在的威胁和攻击的可能性。

进一步讲,管理者必须对下列问题进行权衡:

- **易用性与安全**:实际上,所有的安全措施都会对易用性产生影响。例如,访问控制机制要求用户记住口令,可能还要执行其他访问控制操作。防火墙及其他网络安全措施可能会降低可用的传输容量或者减慢响应时间。病毒检查软件会降低可用的处理能力,并可能由于安全软件和操作系统之间的不正确交互而导致系统崩溃或出现故障。
- **安全成本与失效 – 恢复成本**:除了易用性和性能成本外,实施和维护安全措施有直接的经济成本。所有这些成本必须与缺乏某种安全措施所导致的失效和恢复成本相均衡。安全失效和恢复成本不仅要考虑被保护资产的价值和安全失效造成的损害,而且还要考虑风险。风险是一个特定威胁将会利用某个具有特定有害结果的脆弱性的特定威胁发生的概率。

因此,安全策略是可能受到法律规定影响的商业决策。

1.6.2 安全实施

安全实施涉及四个互补的行动步骤:

- **预防**:理想的安全方案是使攻击不能够成功。尽管这并不是在所有情况下都可行的,但对于广泛的威胁,预防都是一个合理的目标。例如,考虑加密数据的传输。如果使用安全的加密算法,而且采取适当的措施防止对加密密钥的非授权访问,那么就能阻止对传输数据机密性的攻击。
- **检测**:在许多情况下,提供绝对保护是不可行的,但是检测安全攻击却是实际可行的。

例如，设计入侵检测系统来检测是否有非授权用户登录系统。另一个例子是检测拒绝服务攻击，拒绝服务攻击消耗通信或处理资源，以至于合法用户无法使用。

- **响应**：如果安全机制检测到一个正在进行的攻击，如拒绝服务攻击，系统能够做出响应，中止攻击，并防止进一步的危害。
- **恢复**：恢复的一个实例是备份系统的使用，这样一来，如果数据的完整性受到损害，可以重新加载以前的正确的数据备份。

1.6.3　保证和评估

计算机安全服务和机制的“用户”(例如，系统管理者、供应商、客户和最终用户)都希望安全措施能够按照预期的目标正常工作。也就是说，安全用户希望系统的安全基础设施能够满足安全要求并执行安全策略。这些考虑引入了保证和评估的概念。

NIST 计算机安全手册[NIST95]定义**保证**为：一方对技术上和操作上的安全措施按照预期方式工作来保护系统及其处理的信息的相信程度。这包括系统设计和系统实施。因此，保证处理的问题是，“安全系统的设计是否满足其要求”和“安全系统的实现是否符合其规范”。

需要注意的是，保证是由可信程度表示的，而不是根据对设计或实现正确性的形式化证明。鉴于目前的技术水平，超越可信程度达到绝对证明并非不可能，但也是非常困难的。人们在开发定义需求、描述设计与实施的形式化模型，以及运用逻辑和数学技巧来解决这些问题方面已经做了很多工作，但保证依然停留在可信程度层面。

评估是依据某准则检查计算机产品或系统的过程。评估包括测试，可能还涉及形式化分析或数学技术。该领域的中心工作是开发能够应用到任何安全系统(包括安全服务和机制)并对产品比较提供广泛支持的评估准则。

1.7　推荐读物和网站

阅读一些计算机安全方面的经典教程论文是非常有用的，这些文章从历史发展的角度评价了当前的工作和思路，可参考的论文有[WARE79]、[BROW72]、[SALT75]、[SHAN77]和[SUMM84]。两篇最近的计算机安全短篇读物是[ANDR04]和[LAMP04]。[NIST95]给出了对本主题的详细论述(290 页)。另一篇很好的参考文献是[NRC91]。[FRAS97]也非常有用。

有大量的关于计算机安全的材料，包括书籍、论文和在线资源。也许最有用和明确的信息资源是来自标准制定机构以及其工作得到广泛的行业和政府认可的标准和规范。我们在附录 C 中列出了一些最重要的资源。

ANDR04　Andrews, M., and Whittaker, J. “Computer Security.” *IEEE Security and Privacy*, September/October 2004.

BROW72　Browne, P. “Computer Security—A Survey.” *ACM SIGMIS Database*, Fall 1972.

FRAS97　Fraser, B. *Site Security Handbook*. RFC 2196, September 1997.

LAMP04　Lampson, B. “Computer Security in the Real World.” *Computer*, June 2004.

NIST95　National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook*. Special Publication 800-12, October 1995.

NRC91　National Research Council. *Computers at Risk: Safe Computing in the Information Age*. Washington, DC: National Academy Press, 1991.

SALT75　Saltzer, J., and Schroeder, M. “The Protection of Information in Computer Systems.” *Proceedings of the IEEE*, September 1975.

SHAN77　Shanker, K. “The Total Computer Security Problem: An Overview.” *Computer*, June 1977.