第1章

概述

学习目标

学习本章之后，你应当能够：

- 描述有关机密性、完整性和可用性的关键安全要求；
- 讨论亟待解决的安全威胁、安全攻击的类型，给出不同类型计算机和网络资产面临这几类威胁和攻击的例子；
- 总结计算机安全的基本要求；
- 解释基本安全设计原则；
- 讨论攻击面和攻击树的用途；
- 理解全面安全策略的主要内容。

本章是计算机安全的概述。首先，本章讨论计算机安全的定义。本质上，计算机安全讨论的是那些与计算机相关的、容易遭受各种威胁的资产，以及保护这些遭受威胁的资产所采取的各种措施。因此，本章的 1.2 节简要概述用户和系统管理者希望保护的计算机相关资产分类，并研究这些资产所面临的各种威胁和攻击，以及应对这些威胁和攻击的措施。从 1.3 到 1.5 的三节基于三个不同的观点分析了可以应对这些威胁和攻击的措施。在 1.6 节列举了计算机安全的策略。

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）我们需要保护什么样的资产？

（2）这些资产是如何受到威胁的？

（3）我们可以做些什么来应对这些威胁？

1.1 计算机安全的概念

1.1.1 计算机安全的定义

NIST 内部 / 机构间报告 NISTIR 7298（关键信息安全术语表，2019 年 7 月）定义术语计算机安全（computer security）如下：

计算机安全：保证计算机处理和存储的信息的机密性、完整性和可用性的措施和控制方法，其中信息包括硬件、软件、固件、信息数据与通信。

这个定义介绍了处于计算机安全核心地位的三个关键目标。

- **机密性**（confidentiality）。这个术语包含两个相关概念。
  - —**数据机密性**[①]：确保隐私或机密信息不被非授权的个人利用，或被泄露给非授权的个人。
  - —**隐私性**。确保个人能够控制或影响与自身相关的信息收集和存储，也能够控制这些

① RFC 4949（网络安全术语表，2007 年 8 月）定义信息为“能够用多种数据形式表现（编码）的事实或想法”；定义数据为“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，特指可以由计算机处理或产生的信息的表示”。安全文献中通常对两者没有进行区分，本书也没有。

信息可以由谁披露或向谁披露。

- **完整性**（integrity）。这个术语包含两个相关概念。
  —**数据完整性：**确保信息和程序只能在指定的和被授权的情况下才能够被改变。
  —**系统完整性：**确保系统在未受损的方式下执行预期的功能，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，并且不能拒绝授权用户的服务请求。

这三个概念形成了经常提到的 **CIA 三元组**（CIA triad）。这三个概念具体体现了对数据、信息和计算服务的基本安全目标。例如，NIST 标准 FIPS 199（联邦信息和信息系统安全分类标准，2004 年 2 月）将机密性、完整性和可用性列为信息和信息系统的三个安全目标。FIPS 199 从需求的角度对这三个目标给出了非常有用的描述，并在每个分类中提出了安全缺失的定义。

- **机密性：**保持对信息访问和披露的限制，包括对个人隐私和专有信息保护的措施。机密性缺失是指非授权的信息披露。
- **完整性：**防范不正当的信息修改和破坏，包括保证信息的抗抵赖性和真实性。完整性缺失是指非授权的信息修改或破坏。
- **可用性：**确保及时可靠地访问和使用信息。可用性缺失是指对信息或信息系统的访问和使用的破坏。

尽管早已确定使用 CIA 三元组来定义安全目标，但是在安全领域，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（见图 1-1）。下面是两个最经常被提到的概念：

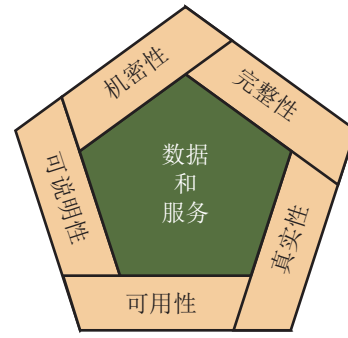

图 1-1　网络和计算机安全的基本要求

- **真实性**（authenticity）：真实性是一种能够被验证和信任的表示真实情况或正确程度的属性，它使得传输、消息和消息源的有效性能够被充分相信。这就意味着要验证用户的身份是否与其所声称的一致，并需要保证到达系统的每一个输入都是来自可信的信息源。
- **可说明性**（accountability）：安全目标要求实体的动作能够被唯一地追踪。这需要支持抗抵赖（non-repudiation）、壁垒（deterrence）、故障隔离、入侵检测和防护，以及事后恢复和诉讼（legal action）。由于真正安全的系统目前还不是一个可以实现的目标，因此，必须能够通过追踪来找到违反安全要求的责任人，系统能够保留其活动记录，允许事后的取证分析用以跟踪安全违规或者为处理纠纷提供帮助。

注意，FIPS 199 将真实性包含在完整性之中。

1.1.2　实例

下面提供一些应用实例来说明刚才所列举的安全要求[①]。基于这些例子，依据对机构或个人

① 这些例子摘自普度大学信息技术安全和保密办公室发布的安全策略文献。

所造成的影响，将安全违规（即机密性、完整性或可用性缺失）分为三个级别，其在 FIPS 199 中的定义如下。

- **低级：**安全缺失对机构运转、机构资产或个人的负面影响有限。例如，机密性、完整性或可用性的缺失可能会导致①任务处理能力在一定程度上退化，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；②机构资产的少许破坏；③少许财务损失；④对个人的少许危害。
- **中级：**安全缺失会给机构运转、机构资产或个人带来严重的负面影响。例如，机密性、完整性或可用性的缺失可能会导致①任务处理能力显著退化，尽管在此期间机构能够完成其主要职责，但其效率显著降低；②机构资产明显损坏；③明显的财务损失；④对个人的明显危害，但不涉及失去生命或者严重危及生命的伤害。
- **高级：**安全缺失会给机构运转、机构资产或个人带来非常严重的，甚至灾难性的负面影响。例如，机密性、完整性或可用性的缺失可能会导致①任务处理能力的严重退化，在此期间机构不能完成其一个或多个主要职责；②机构资产的严重破坏；③严重的财务损失；④对个人严重的、灾难性的危害，包括失去生命或严重危及生命的伤害。

1. 机密性

学生的成绩信息可以视为资产，其机密性对于学生来讲是非常重要的。在美国，这些信息的公布是受家庭教育权利及隐私法（The Family Education Rights and Privacy Act，FERPA）约束的。成绩信息应该只对学生、学生的父母及需要该信息来完成相应工作的员工公开。学生注册信息应该具有中等机密等级，该信息也受 FERPA 约束管理，但可被更多的从事日常管理工作的人看到。相对于成绩信息，学生注册信息受到攻击的可能性更小，如果被披露，导致的损害更小。对于名录信息（如学生或教师名单、院系列表），可以被分配一个低机密等级或者实际上不评级。这些信息一般对公众公开，可以在学校的网站上获得。

2. 完整性

完整性的几个方面可以通过存储在数据库中的医院病人过敏史信息来说明。医生应该相信该信息的正确性和即时性。现在，假定被授权能够查看并可更新该信息的员工（如护士）故意伪造数据以损害医院，数据库则需要快速地恢复到以前的可信状态，并能追查出现的错误，找到责任人。病人过敏史的信息是资产对完整性要求较高的一个例子。不准确的信息会对病人产生严重伤害甚至危及生命，并使医院承担巨大责任。

资产被分配中等完整性要求级别的例子是一个为注册用户提供讨论某些特定话题的论坛（网站）。注册用户或者黑客能够篡改一些内容或者破坏网站。如果论坛仅用于用户娱乐，广告收入很少甚至没有，不用于重要用途（如研究），那么篡改内容或破坏网站造成的潜在威胁并不严重，网站经营者可能会损失一些数据、金钱和时间。

完整性要求较低的例子是匿名网上投票。许多网站（如新闻机构），在用户投票时几乎没有采用任何安全措施。然而，这种投票方式的不准确性和不科学性也是显而易见的。

3. 可用性

越关键的组件或服务，对可用性的要求越高。试想一个为关键系统、应用程序和设备提供认证服务的系统，服务中断会使得访问计算机资源的用户和访问所需资源来执行关键任务的工作人员无能为力，服务不可用会转化成员工丧失生产力、潜在客户丢失等方面的巨大经济损失。

通常评定资产具有中等可用性要求的例子是大学的公共网站。网站为现在和未来的学生及捐赠者提供信息。此站点并不是该大学信息系统的关键组成部分，但是如果不可用，则会引发一些尴尬的局面。

电话号码簿网上查询程序可被分配低可用性要求。尽管服务暂时中断会令人不快，但还可以通过其他方法（如纸质的号码簿或接线员）来获取有关信息。

1.1.3　计算机安全面临的挑战

计算机安全既迷人又复杂。原因如下：

（1）计算安全问题并不像初学者想象的那样简单。安全需求看起来是非常直接的，实际上大多数主要安全服务需求都可以用含义明确的一个术语来标识，如机密性、认证、抗抵赖性和完整性等。然而，满足这些需求的机制可能非常复杂，要充分理解可能会涉及相当细致的推理论证。

（2）在开发某种安全机制或算法时，必须始终考虑对这些安全特征的潜在攻击。很多情况下，成功的攻击往往是通过一种完全不同的方式来观察问题的，从而探测机制中不可预见的弱点。

（3）鉴于第 2 点所述的原因，用于提供特定服务的程序（procedure）通常是与直觉相反的。通常情况下，安全机制的设计是复杂的，不能单纯地通过需求来判定方法是否可用。只有在充分考虑各种不同的威胁后，安全机制的设计才是有道理的。

（4）对于已经设计出的各种安全机制，明确其适用场景是非常必要的。无论是在物理布局层面（如网络中的哪些节点需要特定的安全机制），还是在逻辑层面（如网络体系结构如 TCP/IP 中的哪一层或哪几层应该采取安全机制），这一点都是非常重要的。

（5）安全机制通常包含不止一种算法或协议，还要求参与者拥有一些机密信息（如加密密钥），这就产生了一系列问题，如创建、分发和保护该机密信息。此处存在对通信协议的信任问题，协议的行为可能会使开发安全机制的工作复杂化。例如，如果安全机制的正确运行要求对从发送者到接收者的消息传输时间设置时限，那么任何引入各种可变的、不可预见延迟的协议或网络都可能会使时限变得毫无意义。

（6）计算机安全，从本质上讲，就是利用安全脆弱性进行破坏的攻击者和尽力阻止攻击的设计者或管理者之间的一场智力的较量。攻击者的主要优势在于他只需要找到一个安全脆弱性（或称为漏洞）即可，而管理者必须找到且消除所有的安全弱点才能得到真正的安全。

（7）部分用户和系统管理者有这样一种自然的倾向——在安全保障失效之前，很少有人能够看到安全投入所带来的好处。

（8）安全要求定期甚至持续地对系统进行监视，但是在目前注重时效、超负荷运转的系统环境中很难做到这一点。

（9）安全性通常还是事后考虑的问题——在系统设计完成后才加入系统，而没有作为设计过程中的一个有机组成部分来看待。

（10）许多用户甚至安全管理者认为，牢固的安全性有碍于信息系统或信息使用的高效性和用户操作的友好性。

在本书中，当我们分析各种不同的安全威胁和安全机制时，上述所列举的这些难题将会经常遇到。

1.1.4 一个计算机安全模型

先介绍一些贯穿本书的有用术语。表 1-1 给出了这些术语的定义，图 1-2 基于文献 [CCPS12a]，展示了其中一些术语之间的关系。先从用户和所有者希望保护的**系统资源**（system resource）或**资产**（asset）说起。计算机系统资源的分类如下。

- **硬件：**包括计算机系统和其他数据处理、存储和通信的设备。
- **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，也包括与安全相关的数据，如口令文件。
- **通信设施和网络：**包括局域网和广域网的通信线路、网桥、路由器等。

在安全语境中，我们关心的是系统资源的**脆弱性**（vulnerabilities）。[NRC02] 列出了有关计算机系统或网络资产脆弱性的一般分类：

- 系统资源可能被恶意**损坏**（corrupted），以至于做出不当的操作或者给出错误的应答。例如，存储的数据值被不正当地修改而使之与原始值不同。
- 系统资源可能被**泄露**（leaky）。例如，某人本来不能通过网络访问某些或全部可用信息，但他却获得了这种访问权限。
- 系统资源可能变得**不可用**（unavailable）或非常慢。即使用系统或网络变得不可能或不现实。

这三种脆弱性类型分别对应本节前面所提到的完整性、机密性和可用性三个概念。

表 1-1 计算机安全术语定义

敌手（威胁主体）（adversary（threat agent））：进行或意图进行有害活动的个人、团体、组织或政府。 **攻击**（attack）：任何试图收集、干扰、否认、降级或破坏信息系统资源或信息本身的恶意活动。 **对策**（countermeasure）：一个设备或者技术，旨在降低不良或者对抗性活动的运行效率，或者防止间谍活动、蓄意破坏、盗窃、对敏感信息或信息系统的非授权访问与使用。 **风险**（risk）：衡量一个实体受到潜在的情况或事件威胁的程度，通常与下面两个因素有关：①如果该情况或事件发生所产生的不利影响；②发生的可能性**安全策略**（security policy）一组用于提供安全服务的标准。它定义并限制了数据处理设备的活动，以维护系统与数据的安全状态。 **系统资源（资产）**（system resource（asset））：一个主要应用程序、通用支持系统、高影响程序、物理设施、关键任务系统、人员、设备或者逻辑相关的一组系统。 **威胁**（threat）：任何通过信息系统、有可能对组织运营（包括任务、职能、形象或声誉）、组织资产、个体、其他组织、国家造成不利影响的情况或者事件，包括非授权访问、破坏、披露、信息修改和 / 或拒绝服务。 **脆弱性**（vulnerability）：信息系统、系统安全程序、内部控制或者实现中存在的弱点，这些弱点可能会被威胁源利用或者触发。

注：此表摘自 William Stallings 的《计算机安全：原理与实践》（第四版），©2019。经皮尔森教育公司（纽约）许可重新印刷和电子复制。

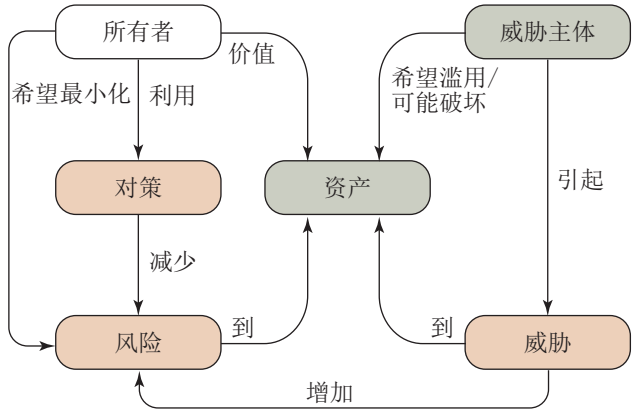

图 1-2　计算机安全术语之间的关系

与系统资源的各种安全脆弱性相对应的是利用这些安全脆弱性产生的**威胁**（threat）。威胁表示对资产的潜在安全危害。**攻击**（attack）是被实施的威胁，即威胁行为，攻击如果成功，将导致不期望的安全侵害或威胁后果。执行攻击的主体被称为攻击者或者**威胁主体**（threat agent）。可以将攻击分为两类。

- **主动攻击**（active attack）：试图改变系统资源或影响其运行。
- **被动攻击**（passive attack）：试图从系统中学习或利用信息，但不影响系统资源。

也可以根据攻击的发起位置对攻击进行分类。

- **内部攻击**（inside attack）：由安全边界内部的实体（“内部人”）发起的攻击。内部人是指已被授权访问系统资源，但以未经授权方许可方式使用资源的内部实体。
- **外部攻击**（outside attack）：由系统安全边界外部的非授权用户或非法使用者（“外部人”）发起的攻击。在 Internet 网络上，潜在的外部攻击者包括业余的恶作剧者及有组织的罪犯、国际恐怖分子和敌对政府等。

最后，**对策**（countermeasure）是指对付攻击所采取的任何手段。理想情况下，可以设计一种对策来**阻止**（prevent）特定类型的攻击。在某些情况下，当阻止不可能或在某些情况下失效时，对策的目标就是**检测**（detect）攻击，并从攻击造成的影响中**恢复**（recover）。在执行安全对策后，对策本身可能会引入新的脆弱性，残余的脆弱性可能还存在。这些脆弱性可能被威胁主体利用，表现为资产的残余**风险**（risk）。资产所有者将通过制定其他约束来寻求最小化风险。

1.2　威胁、攻击和资产

下面开始更详细地了解威胁、攻击和资产。首先弄清必须要处置的安全威胁的类型，然后给出一些针对不同类型资产的威胁类型的例子。

1.2.1　威胁与攻击

表 1-2 基于 RFC 4949，描述了四种威胁后果，并列出了导致每一种后果的威胁行为类型。

表 1-2 威胁后果及导致每种后果的威胁行为类型（基于 RFC 4949）

威胁后果	威胁行为（攻击）
非授权泄露：实体未经授权而获得对数据访问的情况或事件	**暴露：**敏感数据被直接泄露给非授权实体 **截获：**非授权实体直接访问在授权的源和目的地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（但不一定是包含在通信中的数据）的威胁活动 **入侵：**非授权实体通过躲避系统安全保护措施来获得对敏感数据的访问
欺骗：导致授权实体接受虚假数据并相信其正确性的情况或事件	**冒充：**非授权实体通过佯装成授权实体来访问系统或执行恶意行为 **伪造：**以虚假数据欺骗授权实体 **抵赖：**一个实体通过虚伪地否认对行为的责任而欺骗另一个实体
破坏：中断或阻止系统服务和功能正确运行的情况或事件	**失能：**通过禁用系统组件来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来对系统运行进行非期望的改变 **阻碍：**通过阻止系统运行来中断系统服务交付的威胁活动
篡夺：导致系统服务或功能被非授权实体控制的情况或事件	**盗用：**实体对系统资源采取非授权的逻辑或物理控制 **误用：**导致系统组件执行对系统安全有害的功能或服务

（1）**非授权泄露**（unauthorized disclosure）是对机密性的威胁。下面的攻击类型会导致此类威胁后果。

- **暴露**（exposure）：这种类型的威胁、动作可能是故意的，如内部人蓄意泄露敏感信息（如信用卡卡号）给外部人；也可能是由于个人、硬件或软件的错误导致其他实体获得非授权的敏感数据。这种情况的实例有很多，如一些大学不经意将学生的机密信息公布在网上。
- **截获**（interception）：在通信环境中，拦截是最普遍的一种攻击方式。在共享式局域网（LAN）如无线 LAN 或广播以太网中，任何连接到 LAN 的设备都能接收到期望发送给其他设备的数据包的副本。在网络上，有目的的黑客能够访问电子邮件通信流量和其他数据传输情况。所有这些情况都为非授权访问数据创造了可能。
- **推理**（inference）：通信流量分析是众所周知的例子，敌手通过观察网络的通信流量模式得到信息，如网络中特定主机间的通信流量。另一个例子是，具有某数据库受限访问权的用户，可以通过组合重复查询的结果推理出细节信息。
- **入侵**（intrusion）：入侵的例子是敌手通过克服系统的访问控制保护，得到对敏感数据的非授权访问。

（2）**欺骗**（deception）是对系统完整性或数据完整性的威胁。下面的攻击类型会导致此类威胁后果。

- **冒充**（masquerade）：冒充的一个例子是非授权用户通过佯装成授权用户访问系统。如果非授权用户知道其他用户的注册 ID 和密码的话，这种情况是很容易发生的。另一个例子是恶意代码程序，如特洛伊木马，看上去是在执行有用或预期的功能，实际上获得了系统资源的非授权访问或者欺骗用户执行其他恶意逻辑操作。

- **伪造**（falsification）：指更改或替换有效数据，或将虚假数据引入文件或数据库。例如，学生可能在学校数据库中更改其成绩。
- **抵赖**（repudiation）：在这种情况下，用户会否认发送数据，或者否认接收或拥有数据。

（3）**破坏**（disruption）是对可用性或系统完整性的威胁。下面的攻击类型会导致此类威胁后果。

- **失能**（incapacitation）：是对系统可用性的攻击，这是对系统硬件进行物理破坏或损坏的结果。更具代表性的恶意软件，如特洛伊木马、病毒或蠕虫，能够通过这种方式使系统功能丧失或部分服务不可用。
- **损坏**（corruption）：是对系统完整性的攻击。在此情景下，恶意软件可能使得系统资源或服务以不期望的方式工作，或者用户通过非授权方式访问系统，修改某些功能。后者的一个例子是用户在系统中设置后门逻辑，使其能以非正常程序访问系统及其资源。
- **阻碍**（obstruction）：阻碍系统运行的一种方式是通过中断通信链路，或者更改通信控制信息来干扰通信。另一种方式是通过对通信流量或处理器资源施加额外的负担使系统过载。

（4）**篡夺**（usurption）是对系统完整性的威胁。下面的攻击类型会导致此类威胁后果。

- **盗用**（misappropriation）：这包括服务窃取。一个例子是分布式拒绝服务攻击，恶意软件被安装在很多主机上，这些主机将作为向目标主机发送通信流量的平台。在这种情况下，恶意软件将非授权使用处理器和操作系统资源。
- **误用**（misuse）：误用经常是由恶意代码引起的，或者是由获得对系统非授权访问的黑客造成的。这两种情况下安全功能会被禁用或被阻碍。

1.2.2　威胁与资产

计算机系统资产可以分为硬件、软件、数据及通信线路与网络。本小节将简单描述这四个类别，并将其与 1.1 节介绍的完整性、机密性和可用性的概念联系起来（见图 1-3 和表 1-3）。

1. 硬件

对计算机系统硬件主要的威胁是对其可用性的威胁。硬件最容易受到攻击，但对自动化控制最不敏感。威胁包括意外地或蓄意地对设备进行破坏和偷盗。个人计算机和工作站的盛行及局域网的广泛使用增加了硬件出现损失的可能性，如偷盗 USB 设备导致机密性受损。这些威胁需要采用物理或管理方面的安全措施来处理。

2. 软件

软件包括操作系统、实用程序和应用程序。对于软件主要的威胁是对软件可用性的攻击。软件，尤其是应用软件通常很容易被删除，也可能被修改或被破坏导致不能使用。谨慎的软件配置管理，包括对软件最新版本的备份，能够使其保持高可用性。更难处理的问题是对软件进行修改，使其虽仍能运行，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归属这一类。最后一个问题是保护软件不被非授权拷贝，尽管采取了某些对策，但总的来说软件的非授权拷贝问题还没有根本解决。

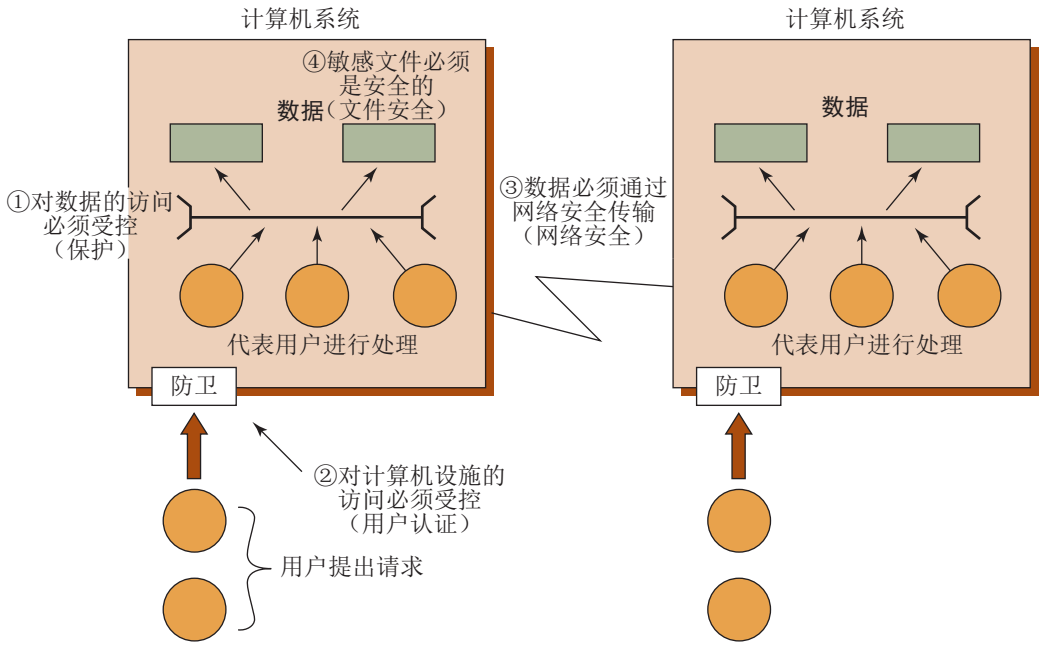

图 1-3　计算机安全的范围

注：本图描述了物理安全之外的安全问题，包括控制对计算机系统的访问、保护通信系统上传输的数据及保护存储的数据。

表 1-3　计算机系统资产的威胁举例

	可用性	机密性	完整性
硬件	设备被偷盗或禁用，因而拒绝提供服务	未加密的 USB 设备被盗	一个门传感器被替换成另一个，无论门的实际位置如何，该传感器均会在特定时间发送关闭状态
软件	程序被删除，拒绝用户访问	软件的非授权拷贝	正在运行的程序被修改，使其在执行过程中失败或执行一些非预期的任务
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潜在的深层次的数据	修改已有文件或伪造新文件
通信线路和网络	消息被破坏或被删除；通信线路或网络不可用	消息被读取；消息的流量模式被观察	消息被修改、延迟、重新排序或复制；伪造虚假消息

3. 数据

硬件和软件安全通常由计算中心的专家关注，或者由个别个人计算机用户关注。一个更加普遍的问题是数据安全，包含由个人、团体或商业组织控制的文件或其他形式的数据。

关于数据方面的安全问题是广泛的，包含可用性、机密性和完整性。就可用性而言，主要关注的是被偶然或恶意破坏的数据文件。

对于机密性的主要威胁是非授权读取数据文件或数据库。与其他的计算机安全领域相比，数据或许需要进行更多的研究，付出更多的努力。一种对机密性不太明显的威胁是进行数据分

析并在使用提供概括和聚集信息（aggregate information）的所谓统计数据库的过程中表现出来的。假定已有的聚集信息不会威胁有关个人的隐私，但随着对统计数据库使用量的增加，个人信息泄露的可能性也会增加。从本质上讲，组成个体的特征可以通过细致的分析识别出来。例如，如果一张表记录着被访者 A、B、C、D 的收入总和，另一个表记录着被访者 A、B、C、D、E 的收入总和，那么两个收入总和的差值将是 E 的收入。如果进一步要求合并数据集，隐私信息泄露问题还会加剧。许多情况下，为了保持不同聚集级别的一致性，在匹配多个数据集时，需要访问个体单元。因而，个体单元作为隐私问题的主体，在数据集处理的不同阶段都可以获得。

最后，数据完整性在大多数安装过程中都是核心关注的问题，修改数据文件产生的后果可能很小，也可能很严重。

4. 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者影响其运行。

（1）**被动攻击**（passive attack）的本质是窃听或监视数据传输，攻击者的目标是获取传输的数据信息。被动攻击的两种形式是消息内容泄露和流量分析。

（2）**消息内容泄露**（release of message content）很容易理解。电话通话、电子邮件消息和传输的文件中都有可能包含敏感或机密信息。我们希望能阻止对手了解传输的内容。

另一种被动攻击即**流量分析**（traffic analysis）更加巧妙。假设有一种方法可以隐藏消息内容或其他信息流量，使得攻击者即使捕获了该消息也不能从消息中提取出信息。通常用来隐藏内容的技巧是加密。即使我们恰当地进行了加密保护，对手仍可能获得这些消息的模式。对手可以确定出通信主机的位置和身份，并能观察到正被交换的消息的频率和长度。这些信息对于判断已发生的通信的性质很有帮助。

被动攻击由于不涉及对数据的修改，所以很难察觉。通常，消息流量表面上以正常的方式发送和接收，收发双方都不知道有第三方已经读取该消息或者观察了流量模式。尽管如此，还是能够阻止这些攻击的，通常使用加密的方法来实现。因此，对付被动攻击的重点是阻止而不是检测。

主动攻击（active attack）包含对数据流进行篡改或伪造数据流，它可以划分为四类：重放、冒充、篡改消息和拒绝服务。

（1）**重放**（replay），涉及被动获取数据单元并在稍后重传，以产生非授权的效果。

（2）**冒充**（masquerade），发生在一个实体假装成另一个实体的场景。冒充攻击通常包含其他主动攻击形式中的一种。例如，捕获认证序列，并在有效的认证序列发生之后重放，这样就可以使具有很少特权的授权实体通过冒充具有更多特权的实体从而获得这些额外的特权。

（3）**篡改消息**（modification of message），简单地说，是指合法消息的某些部分被篡改，或者消息被延迟或被重新排序，从而产生非授权效果。例如，将内容为“ 允许 Abigail Flores 读取机密文件账户（Allow Abigail Flores to read confidential file accounts.）”的消息篡改为“允许 Isidora Martinez 读取机密文件账户（Allow Isidora Martinez to read confidential file accounts.）”。

（4）**拒绝服务**（denial of service）可以阻止或禁止对通信设施的正常使用或管理。这种攻击可能有具体的目标。例如，一个实体可能禁止所有发向某个目的地（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，使网络失效或利用信息使其过载从而降低其性能。

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，但却有办法防范。而主动攻击却很难绝对地防范，因为要实现这个目的就要对所有通信设施和路径进行不间断的物理

保护。所以重点在于检测主动攻击并从其导致的破坏或延迟中恢复过来。由于检测本身具有威慑作用，所以它也可以对防范起到一定作用。

1.3 安全功能要求

对于减少脆弱性并处理系统资产威胁的对策，可以通过很多种方法对其进行分类和描述。本节从功能要求角度分析了对策，遵循 FIPS 200（联邦信息和信息系统最低安全要求，2006 年 3 月）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 安全要求

访问控制（access control）：限制信息系统只能由授权用户或以授权用户名义执行的进程或设备（包括其他信息系统）访问，限制授权用户被允许执行的事务和功能的类型。
意识和培训（awareness and training）：①确保信息系统的管理者和用户能够意识到与他们的活动相关的安全风险，以及与信息系统安全相关的法律、法规和政策；②确保通过充分的培训个人能够承担与信息安全相关的任务和职责。
审计和可说明性（audit and accountability）：①最大限度地创建、保护和保留信息系统审计记录，用于监视、分析、调查和报告不合法的、非授权的或不正当的信息系统活动；②确保个人信息系统用户的活动能被唯一追踪，以便他们对自己的行为负责。
认证[①]**、认可和安全评估**（certification，accreditation and security assessment）：①定期评估机构的信息系统的安全控制措施，确定该控制措施在其应用中是否有效；②制订并实施用来纠正机构信息系统的不足、减少或消除其脆弱性的行动计划；③对机构信息系统及相关的信息系统连接的运行授权；④实时监视信息系统的安全控制措施，确保控制措施的持续有效性。
配置管理（configuration management）：①在各个系统开发生命周期中，建立和维护组织信息系统（包括硬件、软件、固件和文档）的基线配置和清单；②建立和执行在机构信息系统中部署的信息技术产品的安全配置。
应急规划（contingency planning）：建立、维护和实施针对机构信息系统的应急响应、备份操作和灾后恢复的计划，确保在紧急情况下关键信息资源的可用性和操作的持续性。
识别与认证（identification and authentication）：标识信息系统用户和以用户名义进行的进程或设备，认证（或验证）这些用户、进程或设备的身份，以此作为允许访问机构信息系统的先决条件。
事故响应（incident response）：①建立对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；②跟踪、记载并将事故报告给适当的组织官员及管理机构。
维护（maintenance）：①对机构信息系统进行定期、及时的维护；②对实施信息系统维护所用到的工具、技术、机制和人员提供有效的控制。
介质保护（media protection）：①保护信息系统介质（包括纸质和数字介质）；②限制授权用户访问信息系统介质上的信息；③在销毁或者放弃再次使用之前，消除或破坏信息系统介质。
物理和环境保护（physical and environmental protection）：①限制授权个体对信息系统、设备和各自操作环境的物理访问；②保护信息系统的物理厂房和支持信息系统的基础设施；③提供对信息系统的支持设施；④保护信息系统免受环境危害；⑤对包含信息系统的场所提供适当的环境控制措施。
规划（planning）：制订、记录、定期更新和实施机构信息系统的安全计划，其中应描述信息系统中现有的或规划中的安全控制措施以及个人访问信息系统的行为规则。

① 译者注：本书的 authentication 和 certification 根据习惯，均译为“认证”。authentication 也可译为“鉴别”，指确保实体是它所声称的实体，如身份认证；certification 指可交付件是否符合规定需求所给出的正式保证陈述的规程，如产品认证（在第 1 章和第 27 章出现）。请读者根据上下文加以区分。

续表

人员安全（personnel security）：①确保机构（包括第三方服务提供者）中处于责任岗位的个人是可信赖的，并满足已建立的该岗位的安全准则；②保证在职工离职和调动等人事活动前后，机构信息和信息系统是受保护的；③对不能遵守机构的安全策略和程序的职工，制定正式的制裁方法。

风险评估（risk assessment）：定期评估机构运行（包括任务、职能、形象或声誉）、机构资产和个人的风险，这是根据机构信息系统的运行及机构信息的相关处理、存储或传输得出的。

系统和服务获取（systems and service acquisition）：①分配足够的资源来充分保护机构信息系统；②在系统开发生命周期中考虑信息安全问题；③使用软件用法和安装限制；④确保第三方提供充分的安全措施来保护机构外包的信息、应用或服务。

系统和通信保护（system and communications protection）：①在信息系统的外边界和关键内边界上监视、控制和保护机构通信（即机构信息系统的信息传输或接收）；②利用架构设计、软件开发技术和系统工程原理来提高机构信息系统的信息安全的有效性。

系统和信息完整性（system and information integrity）：①及时地识别、报告和纠正信息和信息系统的缺陷；②在机构信息系统的适当位置提供恶意代码防护；③监视信息系统安全报警和警告，并采取适当的行动作为响应。

FIPS 200 中列举出的要求，涵盖了针对安全脆弱性和威胁的多种措施。可以将其粗略地分成两类：一类要求采取计算机安全技术措施（涵盖在本书的第一部分和第二部分），要么仅包含硬件或软件，要么二者都包含；另一类基本上是管理措施（在本书的第三部分出现）。

每一个功能领域可能都会涉及计算机安全技术措施和管理措施。主要涉及计算机安全技术措施的功能领域包括访问控制、识别与认证、系统与通信保护、系统与信息完整性。主要涉及管理措施和程序的功能领域包括意识与培训，审计与可说明性，认证、认可和安全评估，应急规划，维护，物理和环境保护，规划，人员安全，风险评估，系统和服务获取。同时包含在计算机安全技术措施和管理措施中的功能领域包括配置管理、事故响应和介质保护。

值得注意的是，FIPS 200 中的大多数功能要求领域主要是管理问题或者至少有重要的管理组件，这与纯软件或硬件解决方案是相对的。对此一些读者可能会觉得很新鲜，这一点并没有在许多计算机和信息安全的书籍中体现出来。但正如一个计算机安全专家所言，“如果你认为技术可以解决安全问题，那么你并不理解安全问题，也并不理解技术”[SCHN00]。本书反映出将技术和管理方法结合起来才能取得有效计算机安全的必要性。

FIPS 200 针对技术和管理方面的核心关注领域给出了非常有用的概述，这些都与计算机安全相关。本书努力涵盖所有这些领域。

1.4　基本安全设计原则

尽管经历了多年的研究和发展，但是系统地排除安全漏洞、防止所有未经授权的操作的安全设计和实现技术还没有开发出来。由于缺少完备的技术，因此制定一系列被广泛认可的设计原则以指导保护机制的开发是非常必要的。美国国家安全局 (NSA) 和美国国土安全部 (DHS) 联合创建的信息保障 / 网络防御国家卓越学术中心（The National Centers of Academic Excellence in Information Assurance/Cyber Defense）列出了以下基本安全设计原则：

- 经济机制（economy of mechanism）原则。
- 安全缺省设置（fail-safe default）原则。
- 绝对中介（complete mediation）原则。
- 开放式设计（open design）原则。

- 特权分离（separation of privilege）原则。
- 最小特权（least privilege）原则。
- 最小共用机制（least common mechanism）原则。
- 心理可接受性（psychological acceptability）原则。
- 隔离（isolation）原则。
- 封装（encapsulation）原则。
- 模块化（modularity）原则。
- 分层（layering）原则。
- 最小惊动（least astonishment）原则。

前八项原最早被列入文献 [SALT75]，并经历了时间的考验。本节将简要地讨论上述每一个原则。

（1）**经济机制原则**，指嵌在硬件和软件的安全机制的设计要尽可能简单、短小。这是因为简单、短小的设计更易于进行彻底的测试和验证；复杂的设计则为敌手发现和利用可能难以提前发现的微小缺陷提供了更多的机会。设计机制越复杂，包含可利用缺陷的可能性越大。简单的机制则很难发现可利用的缺陷，并且只需较少的维护。此外，由于配置管理问题的简化，更新或替代一个简单机制也不会太烦琐。然而在实践中，这可能是最难遵守的原则。随着硬件和软件新功能的需求不断增加，安全设计任务越来越复杂。所以最好的办法是在进行系统设计时牢记此原则，尽量降低不必要的复杂性。

（2）**安全缺省设置原则**，指访问控制应当基于许可而不是排除。即缺省的情形是不能进行访问的，而保护方案可以识别在什么情况下访问是被允许的。缺省的选择基于许可时，这种方式能比另一种方式更好地识别故障。如果一个机制中的设计或实现出现了故障，在安全环境下（基于许可）能很快发现这一问题，因为在该模式下会被拒绝访问。相反地，如果故障出现在以排除作为访问控制的环境下，这个故障可能很久都不会被发现并被正常地继续使用，因为默认是允许访问的。实际上，大多数文件存取系统都基于这一原则，客户端 / 服务器系统中所有被保护的服务也都基于这一原则。

（3）**绝对中介原则**，指每一次访问都应当依据访问控制机制进行检查。系统不应该依赖于从缓存中检索到的访问命令。在设计持续运行的系统时，这一原则要求：如果访问命令被提示是将来被用到的，那么如何改变优先级顺序将在被仔细权衡后再传递给本地存储器。文件访问系统则是遵守这一原则的例子。然而，通常情况下，一旦用户打开了一个文件，就不会检查权限（permission）是否发生更改。为彻底实现绝对中介，用户每次读取文件的一个字段或记录，或者数据库中的一个数据项时，系统都必须进行访问控制。这一资源密集（即占用大量资源）的方法很少被使用。

（4）**开放式设计原则**，指安全机制的设计应当开放而非保密。例如，虽然加密密钥是保密的，但加密算法应对外公开以供公众审查。这样算法就能被许多专家审查，用户就能对其更加信任。这是美国国家标准技术局（National Institute of Standards and Technology，NIST）标准化加密计划与哈希算法计划所遵循的理念，它使得 NIST 批准的算法被广泛采用。

（5）**特权分离原则**，在文献 [SALT75] 中，特权分离原则是针对限定资源的访问需要多特权属性的这一情况定义的。多因素用户认证就是一个很好的例子，它需要用多种技术，如同时拥有口令和智能卡，才能对用户授权。这一原则也应用于任何一项技术，只要程序能被分成

多个部分，而每个部分受限于各个部分的特定权限（specific privilege）只能执行一个特定的任务。特权分离可以减轻计算机安全攻击的可能造成的破坏。这可以通过下面的例子说明：将一个进程的高特权操作转移给另一个进程并运行该进程去完成具有更高特权要求的任务。日常见到的各种界面都是通过更低权限（lower-privileged）的进程执行的。

（6）**最小特权原则**，是指每个进程和系统用户都应当使用完成某项任务所必需的最少特权集进行操作。很好利用这一原则的例子就是基于角色的访问控制（将在第 4 章详细阐述）。系统安全策略可以识别或定义出不同的进程或用户角色。每一个角色仅被分配完成其功能所必须的许可权。每个许可都指定了一个针对特定资源的访问权（例如，读写访问一个特定的文件或目录，又如连接访问给定的主机和端口等）。除非明确地授予了权限，用户或进程都不能访问受保护的资源。更一般地说，任何一个访问控制系统都应该允许每一个用户仅具有其被授予的特权。最小特权原则具有暂时性。例如，具有特殊权限的系统程序或管理员应当仅在必要时使用这些特权；进行常规的活动时，这些特权应当被收回。如果没有妥善地处理就容易引发意外事件。

（7）**最小共用机制原则**，指在设计时应当最小化不同用户共享的功能，以提高彼此的安全性。这一原则有助于减少非预期的通信路径的数量、减少所有用户共同依赖的硬件和软件数量，因此更易发现是否存在安全隐患。

（8）**心理可接受性原则**，指安全机制不应该过度干涉用户的工作，同时也要满足那些用户授权访问的要求。如果安全机制阻碍了对资源的可用性或可访问性，用户就可能选择关闭这些机制。安全机制应当尽可能地对系统用户透明，或者最小化给用户带来的不便。除了不妨碍用户或者不引起过多的负担，安全实施过程还必须反映出用户理想的保护模式。如果保护程序对用户来说无意义，或者用户必须将其对保护的愿望强行转变为许多各种不同的协议，那么用户很可能会犯错误。

（9）**隔离原则**，这一原则应用于三种环境。第一，公共访问系统应当与重要的资源（数据、进程等）分离，以免泄露或被篡改。在信息的敏感性或重要性很高时，组织就会限制存储数据的系统数量，并在物理上或逻辑上对其进行隔离。物理隔离应当确保一个组织中的公共访问信息资源与重要信息之间没有物理上的连接。为实现逻辑隔离的要求，在公共系统和负责保障重要信息安全性的安全系统之间应当建立层次化的安全服务与安全机制。第二，个人用户的进程和文件应当与他人的相隔离，除非对于不进行隔离有明确的要求。所有的现代操作系统都为这种隔离提供了便利，以保证个人用户有分离的、隔离的进程空间、存储空间和文件空间，通过阻止非授权的访问来实现对系统的安全保护。第三，从阻止对安全机制访问的意义上说，安全机制也应当被隔离。例如，逻辑访问控制可能提供了一个将加密软件与主机系统其他部分相隔离的方法，用以保护加密软件不被篡改，密钥不被替代或泄露。

（10）**封装原则**，可以视为基于面向对象功能的一种特殊形式的隔离。封装提供安全是通过如下方式实现的：将一组过程和数据对象封装在其自身的域中，以使数据对象的内部结构仅能被受保护的子系统中的过程访问，并且这些过程也只能通过特定的域的入口点被调用。

（11）**模块化原则**，在安全的背景下是指将各个安全功能开发成分离的、受保护的模块，也指使用模块化架构进行安全机制的设计和实现。关于使用分离的安全模块，设计目标就是提供公共安全功能和服务，如将需要加密功能的所有内容集合成公共模块。具体来说，大量的协议和应用程序都使用加密功能，但并不是在每个协议或应用程序中都需要实现这一功能，一个

更加安全的设计是开发一个能够被大量协议和应用程序调用的公共的加密模块来实现。这样，设计和实现工作就集中到这一公共加密模块的安全设计与实现上了，包括模块免遭篡改的保护机制。关于模块化架构的使用，每个安全机制都应支持向新技术的移植或者新功能的升级，而无须重新设计整个系统。安全设计应当模块化，以使安全设计的各个部分可以分别进行升级，而无须对整个系统进行修改。

（12）**分层原则**，指的是使用多重的、重叠的保护办法，强调的是信息系统的人员、技术和操作方面。通过使用多重的、重叠的保护方法，任何单一的保护方法失效或规避都不会将系统置于不受保护的状况。阅读全书会发现，分层方法通常被用来在敌手与受保护的信息或服务之间提供多重障碍。这一技术通常也被称为深度防御（defense in depth）。

（13）**最小惊动原则**，指程序或用户界面的响应方式应当尽可能小地出乎用户的意料，不至于惊吓到用户。例如，认证机制对用户来讲应当足够透明，使用户直观理解安全目标与所提供的安全机制之间是如何对应的。

1.5 攻击面和攻击树

第 1.2 节给出了关于计算机和网络系统安全威胁和攻击的概述。本书第 8.1 节将更加详细地介绍攻击的本质和带来安全威胁的敌手的类型。本节将详细介绍对评估和分类威胁非常有用的两个概念：攻击面和攻击树。

1.5.1 攻击面

攻击面是由系统中可访问的和可被利用的脆弱点构成的 [BELL16, MANA11, HOWA03]。以下是攻击面的例子：

- 对外开放的 Web 及其他服务器的端口，以及监听这些端口的代码；
- 在防火墙内可用的服务；
- 处理传入的数据、电子邮件、XML、办公文档和工业级定制数据交换格式的代码；
- 接口、SQL 和 Web 表单；
- 对敏感信息有访问权限的员工，这些敏感数据可能会受到社会工程学的攻击。

攻击面可以按如下方式分类。

- **网络攻击面：**网络攻击面是指企业网、广域网或者 Internet 中的脆弱点，包括网络协议中的脆弱点，例如，利用这些脆弱点进行拒绝服务攻击、通信线路破坏和各种不同形式的入侵攻击。
- **软件攻击面：**软件攻击面是指应用程序、实用程序或操作系统代码中的漏洞，尤其是 Web 服务器软件中的漏洞。
- **人为攻击面：**人为攻击面是指员工或者外部人员（如社会工程学、人为错误和受信任的内部人员）引起的脆弱点。

攻击面分析是评估系统威胁规模和严重性的有效技术。对这些脆弱点进行系统的分析可使开发者和安全分析师知道哪些安全机制是必须的。一旦攻击面被定义，设计人员就能找到减小攻击面的方法，从而使敌手的入侵更加困难。攻击面也可以为设置测试优先级、加强安全措施、修改服务或应用程序等提供指导。

图 1-4 显示了使用分层或深度防御和减少攻击面之间在降低安全风险中的相互关系。

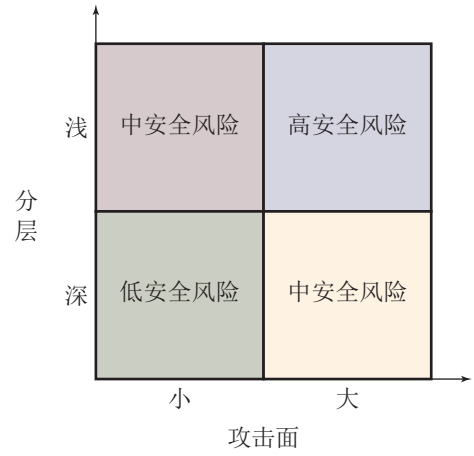

图 1-4　深度防御和攻击面

1.5.2　攻击树

攻击树是一个分支型的、层次化的数据结构，表示了一系列利用安全漏洞进行攻击的潜在技术[MAUW05,MOOR01,SCHN99]。作为攻击目标的安全事件是这个树的根节点，攻击者迭代地、递增地达到这个目标的途径可以用这棵树的分支和子节点来表示。每一个子节点都定义了一个子目标，每一个子目标都可能有一系列的，进一步的子目标，等等。从根节点沿着路径向外延伸的最终节点，也就是叶子节点，代表了发起一个攻击的不同方式。除叶子节点外的每一个节点，都是与节点（AND-node），或者是或节点（OR-node）。若想达成与节点表示的目标，该节点的所有子节点所代表的子目标都要求被实现；若想达成或节点表示的目标，则只需完成其中至少一个子目标即可。分支可以用代表难度、代价或其他攻击属性的值标注，以便与可选择的攻击进行比较。

使用攻击树的动机是有效地利用存在于攻击模式中的有效信息。诸如 CERT（计算机应急响应小组）等组织发布了安全建议，这些安全建议能够促进关于一般攻击策略和特定攻击模式的知识体系的发展。安全分析师利用攻击树可以用结构化的形式记录安全攻击，用以揭示主要的安全漏洞。攻击树对系统和应用程序的设计，以及对对策的选取和强化都具有指导作用。

图 1-5（基于 [DIMI07] 中的一幅图）是一个网银认证应用的攻击树分析例子。根节点是攻击者的目标，即破解用户账户。树中具有阴影的方框部分为叶子节点，代表了构成攻击的事件。树中的白框部分通常是由一个或多个特定的攻击事件（叶子节点）组成的。注意在这棵树中，除了叶子节点的所有节点都是或节点（OR-node）。生成这棵树进行分析时，要考虑与认证相关的以下三部分。

- **用户终端和用户（user terminal and user，UT/U）：**这种攻击把用户设备作为攻击目标，包括可能涉及的令牌，如智能卡或其他口令生成器，也可能是用户的各种操作。
- **通信信道（Communication channel，CC）：**此类攻击主要集中在通信线路。
- **网银服务器（Internet banking server，IBS）：**此类攻击主要针对网银应用所在的服务器进行离线攻击。

共有五类攻击可以被识别，每种攻击都利用了以上三个部分中的一个或多个。

- **获取用户凭证（user credential compromise）：**这种策略可用于针对攻击面中的许多元素，包括程序性攻击（procedural attack）。例如，监视用户的行为以获取个人识别码（PIN）或其他凭证，或者盗取用户的令牌或手写记录。敌手可能会通过使用多种令牌窃取工具来获取令牌信息，例如，破解智能卡或暴力破解 PIN。另一种可能的策略是嵌入恶意软件以获取用户的登录名及口令。敌手可能会通过通信信道（嗅探）来获取凭证信息。最后，敌手还可能通过多种手段与目标用户进行通信，如图 1-5 所示。

- **命令注入（injection of commands）：**此类攻击中，入侵者能够截取 UT 与 IBS 之间的通信信息。许多方法都能用来冒充合法的用户，从而获取银行系统的访问权限。
- **猜测用户凭证（user credential guessing）：**[HILT06] 中记载，通过发送随机用户名和口令的方法暴力攻击银行认证方案是可行的。攻击机制是基于分布式僵尸个人计算机，这些计算机上托管基于用户名或者口令计算的自动化程序。
- **违反安全策略（security policy violation）：**例如，员工违反银行的安全政策，再加上访问控制与日志机制的薄弱，可能会引发内部安全事件，暴露客户的账户信息。
- **利用已知的认证会话（use of known authenticated session）：**此类攻击会说服用户或强制用户通过预先设置的会话 ID 连接 IBS。一旦用户通过了服务器的认证，攻击者就可以利用已知的会话 ID 向 IBS 发送数据包，冒充用户的身份信息。

图 1-5 给出了有关网银认证应用中不同类型攻击的一个概览。从这棵攻击树出发，安全分析师可以评估每个攻击的风险，并使用上一节（第 1.4 节）中列出的设计原则来设计全面的安全设施。[DIMO07] 很好地说明了该设计工作的结果。

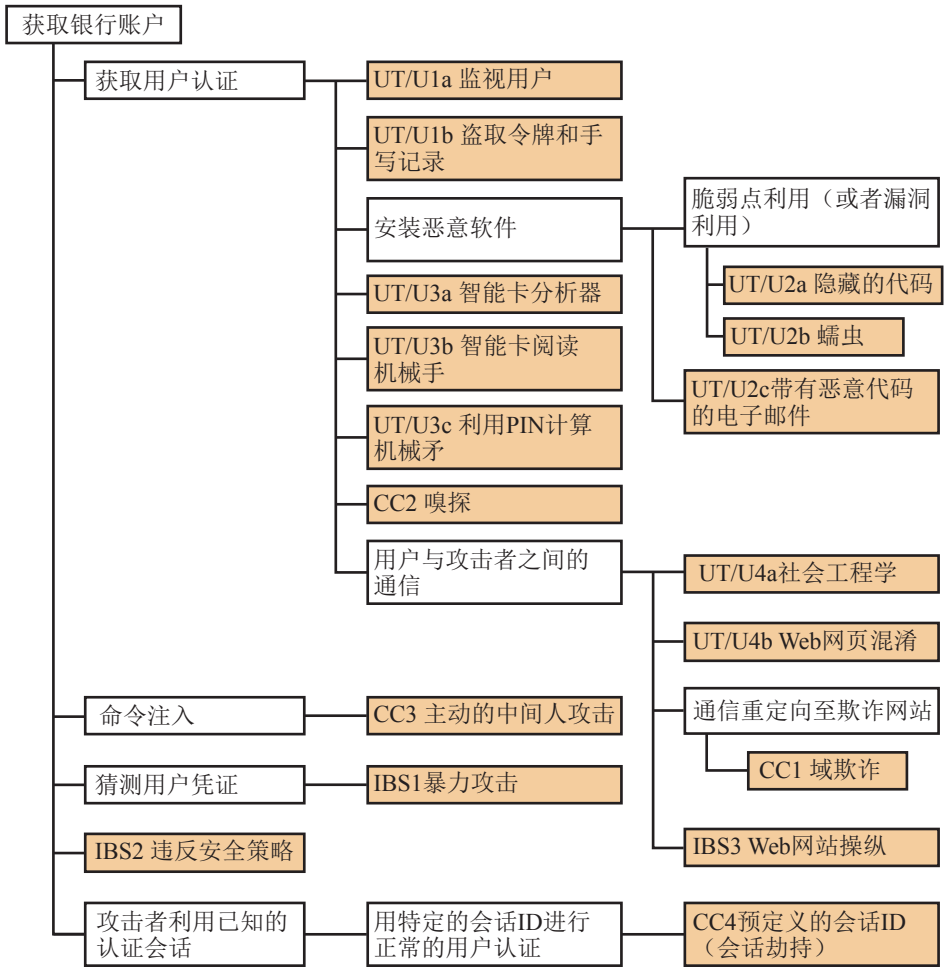

图 1-5　网银认证的攻击树

1.6　计算机安全策略

下面简要归纳一下为提供计算机安全所采用的总体策略，以总结本章的内容。[LAMP04]提出的全面安全策略涉及以下三个方面。

- **规范 / 策略**（specification/policy）：安全策略应该要实现什么？
- **实施 / 机制**（implementation/mechanism）：安全策略是如何实现的？
- **正确性 / 保证**（correctness/assurance）：安全策略是否确实起作用了？

1.6.1　安全策略

设计安全服务和安全机制的第一步是开发安全策略。其中包含计算机安全领域对术语安全策略（security policy）有不同的用法。至少，安全策略是系统期望行为的非形式化描述[NRC91]。这种非形式化策略应参考安全性、完整性和可用性的要求。更有用的是，安全策略是一份规则与实践的形式化陈述，规定或规范了系统及组织如何提供安全服务来保护敏感和关键的系统资源（RFC 4949）。这种形式化安全策略有助于通过系统的技术控制措施及管理和运行控制措施来予以实施。

在制定安全策略时，安全管理者需要考虑如下几个因素：

- 需要保护的资产的价值；
- 系统的脆弱性；
- 潜在的威胁和可能的攻击。

进一步地，管理者必须权衡下列问题：

- **易用性与安全**（ease of use versus security）：几乎所有安全措施都会在易用性方面做出一定的牺牲，正如下面几个例子所描述的那样。访问控制机制要求用户记住口令，此外可能还要执行其他的访问控制操作；防火墙及其他网络安全措施可能会降低可用的传输容量、减慢响应时间；病毒检测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故障。
- **安全成本与失效—恢复成本**（cost of security versus cost of failure and recovery）：除易用性和性能成本外，实施和维护安全措施是直接的经济成本。所有这些成本必须与缺乏某种安全措施所导致的安全失效和恢复的成本相均衡。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违规导致的损害，还要考虑风险，即特定威胁利用特定脆弱性造成特定有害结果的可能性。

因此，安全策略是一个可能受到法律要求影响的商业决策。

1.6.2　安全实施

安全实施涉及四个互为补充的行动步骤。

（1）**预防**（prevention）：理想的安全策略是使任何攻击都不能成功。尽管这并不是在所有情况下都可行，但对于众多威胁，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，而且采取适当措施防止对加密密钥的非授权访问，那么对传输数据机密性的攻击就能做到预防。

（2）**检测**（detection）：在多数情况下，绝对的保护是不可行的，但是检测安全攻击是可

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，拒绝服务攻击使得通信或处理器资源被消耗以至于合法用户不能使用。

（3）**响应**（response）：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），系统能做出响应，终止攻击并预防进一步的危害。

（4）**恢复**（recovery）：恢复的一个实例是使用系统备份。如果数据的完整性被损坏，可用重新装载以前正确的数据备份。

1.6.3 保证和评估

计算机安全服务和机制的“用户”（如系统管理者、销售者、消费者和终端用户）都希望相信安全措施能够按照预期的目标正常工作。也就是说，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。这些想法引入了保证和评估的概念。

（1）**保证**（**assurance**）是信息系统的一个属性，为系统的运行提供了可靠的依据，从而实现了系统的安全策略，这包括系统设计和系统实现。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？”，保证表示为置信度，而不是设计或实现是否正确的形式化证明。就目前关于设计与实现的证明情况看，越过置信度而达到绝对证明是不可能的。人们在开发定义需求、描述设计与实现的形式化模型，以及运用逻辑和数学技巧来处理这些问题方面已经做了很多工作。但是，保证依然停留在一个置信度层面。

（2）**评估**（evaluation）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，可能还包括形式化分析或数学技术。该领域的核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）并为产品比较提供广泛支持的评估准则。

1.7 标准

本书中所描述的许多安全技术和应用已被指定为标准。此外，这些标准已被拓展为涵盖管理实践、安全机制和服务的总体架构。我们利用正在使用的最重要的或正在制定的标准来描述计算机安全的各个方面。各种组织都在致力于制定或推广这些标准，一些最重要（截止到当前）的组织如下。

- **美国国家标准与技术研究所（National Institute of Standard and Technology，NIST）：** NIST 是美国联邦政府的一个机构，负责制定美国政府使用的度量科学、标准和技术，也负责推动美国私营企业的创新。尽管是一个美国国家机构，NIST 的联邦信息处理标准（NIST federal information processing standards，FIPS）与特别出版物（special publications，SP）有着国际范围的影响力。
- **Internet 协会（Internet Society，ISOC）：** ISOC 是一个专业的成员联盟，拥有世界性的组织成员和个人成员。在解决 Internet 未来面临的问题上，它处于领导者的地位，同时它也是制定各种 Internet 基础设施标准组织的管理机构。这些组织包括 Internet 工程任务组（Internet Engineering Task Force，IETF）和 Internet 结构委员会（Internet Architecture Board，IAB）。这些组织制定 Internet 标准和相关细节。所有的这些内容以请求评论文档（requests for comments，RFC）的形式公布。
- **电信标准化部门（ITU-T）：** 国际电子通信联盟（International Telecommunication Union，

ITU）是一个联合国机构，各国政府和私营企业在它的领导下一起协调全球的电子通信网络和服务。ITU 的电子通信标准化部门（Telecommunication Standardization Sector，ITU-T）是 ITU 的三大部门之一。ITU-T 的任务是制定覆盖所有电子通信领域的标准。ITU-T 的标准被称为推荐标准（recommendation）。

- **国际标准化组织（ISO）：**国际标准化组织（ISO）[①] 是一个由全球 140 多个国家的国家标准组织参加的世界联盟。ISO 是一个非政府组织，负责推动标准化的发展，促进国际间的商品和服务的交换，发展全球在知识、科学、技术和经济活动方面的合作。ISO 的工作促使国际间的协议作为国际标准发布。

附录 C 对这些组织进行了更详细的讨论。本书末尾提供了书中引用的 ISO 和 NIST 文档列表。

1.8　关键术语、复习题和习题

1.8.1　关键术语

访问控制（access control）	拒绝服务（denial of service）	入侵（intrusion）
主动攻击（active attack）	破坏（disruption）	隔离（isolation）
敌手（adversary）	经济机制（economy of mechanism）	分层（layering）
资产（asset）	封装（encapsulation）	最小惊动（least astorishment）
保证（assurance）	评估（evaluation）	最小共用机制（least common mechanism）
攻击（attack）	暴露（exposure）	最小特权（least privilege）
攻击面（attack surfaces）	安全缺省设置（fail-safe default）	冒充（masquerade）
攻击树（attack trees）	伪造（falsification）	盗用（misappropriation）
认证（certification）	失能（incapacitation）	误用（misuse）
真实性（authenticity）	推理（inference）	模块化（modularity）
可用性（availability）	内部攻击（inside attack）	阻碍（obstruction）
绝对中介（completc mediation）	完整性（integrity）	开放式设计（open design）
机密性（confidentrality）	截获（interception）	外部攻击（outside attack）
损坏（corruption）	安全策略（security policy）	被动攻击（passive attack）
对策隐私（privacy）	特权分离（separation of privilege）	阻止（prevent）
心理可接受性（psychological acctability）	系统资源（system resource）	流量分析（traffic analysis）
重放（replay）	威胁主体（threat agent）	非授权泄露（unauthorized disclosure）
抵赖（repudiation）		篡夺（usurption）
风险（risk）		脆弱性 / 漏洞（vulnerability）

1.8.2　复习题

1. 给出计算机安全的定义。
2. 被动安全威胁和主动安全威胁的区别是什么？
3. 列举并简要定义被动和主动网络安全攻击的分类。

① 译者注：ISO 不是一个缩略词（假如是缩略词就应该写为 IOS），而是一个词，它来自希腊语，是相等（equal）的意思。

4. 列举并简要定义基本的安全设计原则。

5. 解释攻击面和攻击树之间的不同。

1.8.3 习题

1. 思考在自动柜员机（ATM）上，用户提供银行卡和个人标识码（PIN）用于账户访问。给出与系统相关的机密性、完整性和可用性要求的例子，并说明每种情况下要求的重要性等级。

2. 电话交换系统根据呼叫者请求的电话号码通过交换式网络路由呼叫。针对这种情况重复考虑习题 1 的问题。

3. 考虑一个由许多机构使用的打印文档的桌面印刷系统。

（1）给出存储数据的机密性为最高需求的出版物类型的例子。

（2）给出存储数据的完整性为最高需求的出版物类型的例子。

（3）给出系统可用性为最高需求的例子。

4. 对于下列每种资产，分别为机密性、可用性和完整性缺失分配低、中或高影响级别，并证明你的答案。

（1）一个组织管理其 Web 服务器上的公开信息。

（2）执法机构管理极其敏感的调查信息。

（3）金融组织管理日常行政信息（不是与隐私有关的信息）。

（4）一家承包机构用于大量采集数据的信息系统，既包含敏感的、预询价（pre-solicitation）阶段的合同信息，也包含日常管理信息。分别对两个数据集和整个信息系统的影响进行评价。

（5）一家电厂具有监控与数据采集（SCADA）系统，用于控制大型军事基地的电力分配。SCADA 系统既包含实时传感数据，也包含日常管理信息。分别对两个数据集和整个信息系统的影响进行评价。

5. 考虑如下允许访问资源的代码：

```
DWORD dwRet = IsAccessAllowed(…);
if (dwRet == ERROR_ACCESS_DENIED) {
// Security check failed.
// Inform user that access is denied.
} else {
// Security check OK.
}
```

（1）解释程序中存在的安全缺陷。

（2）重写代码以避免缺陷。

提示：考虑安全缺省设置原则。

6. 设计攻击树，目标是获取物理安全中相关内容的访问权限。

7. 假设一个公司在安装在两个建筑内的同一资产上运营，一个建筑是总部，而另一个建筑包含网络和计算机服务。物理安全方面，资产用坚固的围栏在四周进行保护。除此之外，物理安全还包括了前门的警卫。局域网分为总部局域网和网络服务局域网。网络使用者通过防火墙连接 Web 服务器，拨号用户通过拨号可以连接网络服务局域网。请设计一个攻击树，它的根节点代表资产机密的泄露包括物理上的、社会工程学和技术攻击。这个攻击树可以包括与节点（AND-node）和或节点（OR-node）。请设计一个至少包含 15 个叶子节点的树。

8. 阅读一些关于计算机安全的经典教程论文是很有用的，这些论文提供了历史视角，可以帮助我们理解当前的工作与思想。你可以在 Pearson Companion 网站的 Student Support Files 分区（https://pearsonhighered.com/stallings）找到一些精选的经典论文。阅读这些论文，写一篇 500 ～ 1000 字的文章（或包含 8 ～ 12 张幻灯片的 PPT），总结这些经典论文中的关键概念，尤其是在大多数或全部论文中出现的概念。