第1章 概 览

The combination of space, time, and strength that must be considered as the basic elements of this theory of defense makes this a fairly complicated matter. Consequently, it is not easy to find a fixed point of departure.

—*On War*, Carl Von Clausewitz

学习目标

通过本章的学习后应具备以下能力：

- 描述密钥安全需求的保密性、完整性和可用性。
- 讨论需要解决的安全威胁和攻击的类型，并举例说明作用于不同计算机和网络上各种类型的安全威胁和攻击。
- 总结计算机安全的功能性需求。
- 描述 OSI 的 X.800 安全框架。

本书集中讨论两大领域：一是密码算法和协议，它们有着广泛的应用；二是网络和 Internet 安全，它们大量地依赖密码技术。

密码算法和协议又可以分为 4 个主要的领域：

- **对称加密**：用于加密任意大小的数据块或数据流的内容，包括消息、文件、加密密钥和口令。
- **非对称加密**：用于加密小的数据块，如加密密钥或者数字签名中使用的 Hash 函数值。
- **数据完整性算法**：用于保护数据块(如一条消息)的内容免于被修改。
- **认证协议**：有许多基于密码算法的认证方案，用来认证实体的真实性。

网络和 Internet 安全领域涉及阻止、防止、检测和纠正信息传输中出现的安全违规行为的措施。它所包含的内容相当广泛。为使读者对本书中讨论的领域有所了解，我们先举几个有关安全违规行为的例子：

(1)用户 A 向用户 B 传送文件,该文件包含不能泄密的敏感信息(如工资单),用户 C 无权读取该文件,但他能够监视传输过程并截获该文件。

(2)网络管理员 D 向其管辖的计算机 E 传输一条消息,命令计算机 E 更新权限文件以允许一批新用户可访问 E。用户 F 截获并修改该消息,如增加或删除一些用户,然后再将消息转发给 E,而 E 误以为是管理员 D 发来的消息并按照消息的内容更新权限文件。

(3)上例中,用户 F 也可以不截获消息,而是按自己的意愿构造消息并发送给 E,同样 E 误以为是管理员 D 发来的消息并更新权限文件。

(4)雇员事先未得到警告就被解雇。人事经理向服务器系统发送消息以注销该雇员的账号,账号注销后,服务器将发送通知到该雇员的文件中以确认注销。该雇员可以截获并延时发送人事经理发的消息,直至他有足够的时间访问服务器来获取敏感信息,然后再转发这条消息,以注销账号。雇员的这些活动在相当长时间内不会被察觉。

(5)顾客向股票经纪人发送消息,请求完成各种交易,后来这些投资失败而顾客否认发送过该消息。

尽管上述举例不能穷尽所有可能的安全威胁类型,但它们说明了网络安全所关注的范围。

1.1 计算机安全概念

1.1.1 计算机安全的定义

NIST 的《计算机安全手册》[NIST95]针对计算机安全这一术语的定义如下:

计算机安全

对于一个自动化的信息系统,采取保护措施确保信息系统资源(包括硬件,软件,固件,信息/数据和通信)的完整性、可用性和保密性。

这个定义引进了处于计算机安全核心地位的 3 个关键目标:

- **保密性**(Confidentiality):这个术语包含了两个相关的概念:
  数据[①]保密性:确保隐私或者秘密信息不向非授权者泄露,也不被非授权者所使用。
  隐私性:确保个人能够控制或确定与其自身相关的哪些信息是可以被收集、被保存的、这些信息可以由谁来公开以及向谁公开。
- **完整性**(Integrity):这个术语包含两个相关的概念:
  数据完整性:确保信息和程序只能以特定和授权的方式进行改变。
  系统完整性:确保系统以一种正常的方式来执行预定的功能,免于有意或者无意的非授权操纵。
- **可用性**(Availability):确保系统能工作迅速,对授权用户不能拒绝服务。

这 3 个概念形成了被经常称道的 CIA 三元组。这 3 个概念体现了数据,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)将保密性,完整性

① RFC 4949 定义信息为“事实和想法,可以用各种形式的数据进行表示”,而定义数据为“用特定物理表示的信息,通常是一串有意义的符号序列,特别的是可以由计算机处理和产生信息的表示”。安全文献一般不做这种区分,本书也不做区分。

和可用性作为信息和信息系统的三个安全目标。FIPS 199 从安全需求和安全缺失的角度对这三个目标做了刻画。

- **保密性**：对信息的访问和公开进行授权限制，包括保护个人隐私和秘密信息。保密性缺失的定义是信息的非授权泄露。
- **完整性**：防止对信息的不恰当修改或破坏，包括确保信息的不可否认性和真实性。完整性缺失的定义是对信息的非授权修改和毁坏。
- **可用性**：确保对信息的及时和可靠的访问和使用。可用性的缺失是对信息和信息系统访问和使用的中断。

尽管 CIA 三元组足以定义安全目标，但是许多从事安全领域研究的人认为还需要其他概念来定义才更全面。下面是其中两个被提及较多的概念：

- **真实性(Authenticity)**：一个实体是真实性的、是可被验证的和可被信任的特性；对传输信息来说，信息和信息的来源是正确的。也就是说能够验证该用户是否是他声称的那个人，以及系统的每个输入是否均来自可信任的信源。
- **可追溯性(Accountability)**：这一安全目标要求实体的行为可以唯一追溯到该实体。这一属性支持不可否认性、阻止、故障隔离、入侵检测和预防、事后恢复，以及法律诉讼。因为无法得到真正安全的系统，我们必须能够把安全泄露追查到负有责任的一方。系统必须保留他们的活动记录，以允许事后的审计分析来跟踪安全事件或者解决争执。

1.1.2　例子

下面提供一些应用的例子来展示刚才列举的一些要求[①]。对于这些例子，如果发生了安全泄露事件(保密性，完整性或可用性的缺失)，我们使用三个层次说明对组织和个人的影响。这些层次定义在 FIPS PUB 199 里。

- **低**：这种损失对组织的运行，组织的资产或者个人的负面影响有限。有限的负面影响是指，例如，保密性、完整性或可用性的缺失可能(1)导致执行使命的能力在一定程度上和时期内的降级，这期间仍能完成主要的功能，但功能的效果会可见地降低；(2)导致资产的较小损失；(3)导致很小的经济损失；(4)导致对个人的很小伤害。
- **中**：这种损失对组织的运行，组织的资产和个人有严重的负面影响。严重的负面影响是指，例如，这种损失可以(1)导致执行使命的能力在一定程度上和时期内的显著降级，这期间仍能够完成主要的功能，但功能的效果会显著降低；(2)导致资产的显著损失；(3)导致显著的经济损失；(4)导致对个人的显著伤害，但不包括丧命或者严重威胁生命安全的伤害。
- **高**：这种损失对组织的运行，资产和个人有严重的或者灾难性的负面影响。严重的或灾难性的负面影响是指，例如，这种损失可以(1)导致执行使命的能力在一定程度上和时期内的严重降级，这期间不能完成主要的一项或多项功能；(2)导致大部分资产的损失；(3)导致大部分经济的损失；(4)导致对个人的严重或灾难性的伤害，包括丧命或者严重威胁生命安全的伤害。

保密性：学生的分数信息是一种资产，它的保密性被学生们认为是非常重要的。在美国，这种

① 这些例子来自 Purdue 大学信息技术安全与隐私办公室发表的安全政策文献。

信息的发布受家庭教育权和隐私权法案(FERPA)管理。学生的分数仅由学生自己,他们的父母以及需要这些信息来完成工作的学校雇员可以得到。学生的注册信息有中等程度的保密等级。尽管注册信息仍然受 FERPA 管理,但这些信息可以以天为单位被更多人看到,它比起分数信息更少受到攻击,即使受到攻击,损失也比较小。目录信息,如学生,老师,院系名单可列为低保密等级或者无须保密。这些信息对公众自由开放,可以在学校网页上发布。

完整性:存储在医院数据库内的病人的过敏信息的例子可以说明完整性的几个方面。医生应该能够信任这些信息是新的、正确的。现在假设一个有权查看和更新这些信息的雇员(比如护士)有意篡改了数据而造成医院的损失。这个数据库需要快速恢复到可以信任的状态,而且应该能把这些错误追溯到负有责任的那个人。这个例子说明病人的过敏信息是对完整性要求很高的一种资产。不准确的信息可以导致对病人的伤害甚至是造成病人死亡,从而使医院担负重大的责任。

对资产的完整性有中等要求的例子是 Web 站点,这些站点提供论坛供用户注册来讨论一些特定的话题。无论是注册用户还是黑客都不能篡改某些项或者丑化网站。如果网站仅仅是为了用户的娱乐,很少或没有广告收入,也不是用于如科研等重要的事情,那么潜在的危害就不是那么严重。网站的主人可能承受一些数据、经济和时间上的损失。

一个对完整性要求低的例子是匿名在线民意调查。许多 Web 站点,如新闻机构,为他们的用户提供几乎没有监管的这类民意调查。然而,这类民意调查的不准确性和非科学性早已为大家所理解。

可用性:一个部件或服务越关键,可用性的要求就越高。考虑一个为关键系统、应用和设备提供认证服务的系统,服务的瘫痪将导致顾客不能访问计算资源,员工不能访问他们执行重要任务所需要的资源。由于员工生产率的损失和顾客潜在的损失,使得服务的缺失转换为大量的经济损失。

对资产的可用性要求中等的一个例子是大学的公共网站;这样的网站为现有的和潜在的学生和捐助人提供信息。这样的网站不能算是大学信息系统的关键部分,但它的不可用仍然会给大学造成窘境。

在线电话目录查询应用可以划分为可用性要求低的例子。尽管服务的临时缺失是一件恼人的事情,但有其他办法获得这些信息,如纸质的电话号码簿或者接线员。

1.1.3 计算机安全的挑战

计算机和网络安全很吸引人也很复杂。原因如下所述。

(1)安全对初学者而言并没有想象的那么简单。安全的要求看上去很直观;的确,对安全服务的大部分要求都可以用其含义不言自明的单词给出,如保密性、认证,不可否认或完整性。但是满足这些要求的机制却非常复杂,理解它们需要缜密的推理。

(2)当设计一个特别的安全机制或算法时,一定要考虑各种各样潜在的攻击。以与设计完全不同的方式看问题往往可以使攻击成功,这样做通常是利用了设计的机制中没有预料到的弱点。

(3)根据第二点,设计安全机制的过程通常采用逆向思维。安全机制是复杂的,从要求的陈述里并不能明显地看出需要精心的设计,只有当威胁的各个方面被考虑到时,对精心设计的复杂机制的需求就变得易于理解了。

(4)设计好各种安全机制后,接下来是决定在哪里使用这些安全机制。包括物理位置(例如,

网络的什么地方需要某一安全机制)和逻辑位置(例如，像 TCP/IP 这样的网络协议的哪一层或哪几层)。

(5)安全机制所使用的算法或协议通常不止一个。这些算法和协议需要参与者使用一些秘密信息(如加密密钥)，这就带来对秘密信息的产生、分发和保护等问题。它们所依赖的通信协议可能会使开发安全机制的过程变得复杂。例如，安全机制要正常行使功能需要对消息的传输时间设定限制，而任何协议和网络都存在不确定且不可预测的延迟，从而使得那个时间限制变得毫无意义。

(6)计算机和网络安全本质上是一场入侵者和设计者(或管理员)之间的智力战争。入侵者努力要找到漏洞，而设计者或管理员努力要封堵漏洞。入侵者的优势在于他或她仅仅需要找到一个弱点，而设计者必须找到并根除所有的弱点来获得完全的安全。

(7)用户和系统管理员有一种倾向，直到发生了安全事件，才意识到安全投资可以带来收益。

(8)安全需要经常的，甚至是不断的监管，而这在当今短期、负荷过重的环境里是难以做到的。

(9)绝大多数情况下，安全仍然是一种事后措施，当系统设计完成以后，再来把安全机制增加到系统里。而不是作为整个系统设计过程的一个主要部分。

(10)许多用户，甚至是安全管理员认为强的安全不利于信息系统高效工作、有碍于用户友好操作，或不利于对信息的使用。

本书中，随着对各种安全威胁和机制的考察，会以多种方式遇到上面列举的各种困难。

1.2　OSI 安全框架

为了有效评价一个机构的安全需求，以及对各种安全产品和政策进行评价和选择，负责安全的管理员需要某种系统的方法来定义对安全的要求并刻画满足这些要求的措施。在集中式数据处理环境下做到这一点已经非常困难。随着局域网和广域网的使用，这一问题变得更加复杂。

为此，ITU-T[①] 推荐方案 X.800，OSI 安全框架，给出了一种系统化的定义方法[②]。对安全人员来说，OSI 安全框架是提供安全的一种组织方法。而且，因为这个框架是作为国际标准而开发的，所以许多计算机和通信的服务商已经开发了与 OSI 安全框架的安全特性相适应的产品和服务。

对于我们来说，OSI 安全框架实际上是对本书将要涉及的许多概念做了一个尽管抽象但非常有用的综述。OSI 安全架构主要关注安全攻击、安全机制和安全服务。可以简短地定义如下。

- **安全攻击**：任何危及信息系统安全的行为。
- **安全机制**：用来检测、阻止攻击或者从攻击状态恢复到正常状态的过程(或实现该过程的设备)。
- **安全服务**：加强数据处理系统和信息传输的安全性的一种处理过程或通信服务。其目的在于利用一种或多种安全机制进行反攻击。

在文献中，术语“威胁”和“攻击”差不多是用来指相同的事情的。表 1.1 列出了 RFC 4949(互联网安全术语表)给出的定义。

---

① 国际电信联盟(ITU)电信标准化组(ITU-T)是一个联合国资助的机构，主要是开发与长途通信、开放系统互连(OSI)有关的各种标准，这些标准也称为建议。

② OSI 安全架构是在 OSI 协议框架范围内开发的，协议框架在附录 H 中给出。然而，本章的目的不需要理解 OSI 协议框架。

表 1.1 威胁和攻击(RFC 4949)

威胁
破坏安全的潜在可能,在环境、能力、行为或事件允许的情况下,它们会破坏安全造成危害。也就是说,威胁是脆弱性被利用而可能带来的危险
攻击
对系统安全的攻击,它来源于一种具有智能的威胁,也就是说,有意违反安全服务和侵犯系统安全策略的(特别是在方法或技巧方面的)智能行为

1.3 安全攻击

X.800 和 RFC 4949 都使用了一种有效的方式来对安全攻击进行分类,即被动攻击和主动攻击。被动攻击试图了解或利用系统的信息但不影响系统资源。主动攻击试图改变系统资源或影响系统运作。

1.3.1 被动攻击

被动攻击(参见图 1.1)的特性是对传输进行窃听和监测。攻击者的目标是获得传输的信息。信息内容的泄漏和流量分析就是两种被动攻击。

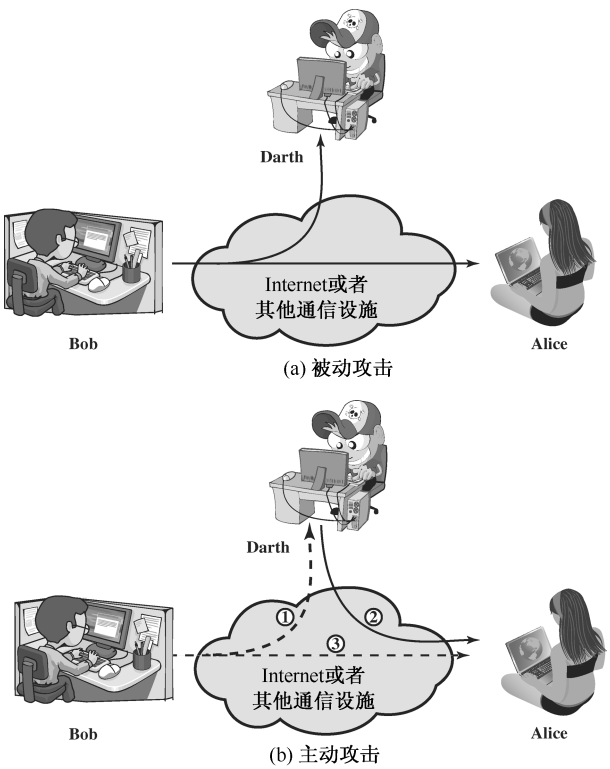

图 1.1 安全攻击

信息内容泄露攻击很易理解。电话、电子邮件消息和传输的文件都可能含有敏感或秘密的信息。我们希望能阻止攻击者获得传输的内容。

第二种被动攻击是流量分析,有些微妙。设想我们已有一种方法来隐藏消息内容或其

他信息流量，使得攻击者即使捕获了消息也不能从消息里获得信息。加密是隐藏内容的常用技巧。即使我们恰当地进行了加密保护，攻击者仍可能获得这些消息模式。攻击者可以决定通信主机的身份和位置，可以观察传输消息的频率和长度。这些信息可以用于判断通信的性质。

被动攻击由于不涉及对数据的更改，所以很难觉察。典型的情况是，信息流表面上以一种常规的方式在收发，收发双方谁也不知道有第三方已经读了信息或者观察了流量模式。然而，通过加密的手段阻止这种攻击却是可行的。因此处理被动攻击的重点是预防，不是检测。

1.3.2　主动攻击

主动攻击[参见图 1.1(b)]包括对数据流进行修改或伪造数据流，可分为四类：伪装、重播、消息修改和拒绝服务。

伪装是指某实体假装别的实体[图 1.1(b)的路径 2 是有效的]。伪装攻击通常还包含其他形式的主动攻击。例如，捕获认证信息，并在真的认证信息之后进行重播，这样没有权限的实体通过冒充有权限的实体从而获得额外的权限。

重播是指将获得的信息再次发送以产生非授权的效果(路径 1、2、3 有效)。

消息修改指修改合法消息的一部分或延迟消息的传输或改变消息的顺序以获得非授权的效果(路径 1、2 有效)。例如，将消息“Allow John Smith to read confidential file *accounts*”修改为“Allow Fred Brown to read confidential file *accounts*”。

拒绝服务阻止或禁止对通信设施的正常使用或管理(路径 3 有效)。这种攻击可能有具体的目标。比如，某实体可能会查禁所有发向某目的地(如安全审计服务)的消息。拒绝服务的另一种形式是破坏整个网络，它或者是使网络失效，或者是使其过载以降低其性能。

主动攻击与被动攻击相反。被动攻击虽然难以被检测到但可以防止。另一方面，因为物理通信设施，软件和网络本身潜在弱点的多样性，主动攻击难以绝对地预防，但容易检测。所以重点在于检测并从破坏或造成的延迟中恢复过来。因为检测主动攻击有一种威慑效果，所以也可在某种程度上阻止主动攻击。

1.4　安全服务

X.800 将安全服务定义为通信开放系统的协议层提供的服务，从而保证系统或数据传输有足够的安全性。也许在 RFC 4949 中可找到一种更清楚的定义：是一种由系统提供的对系统资源进行特殊保护的处理或通信服务；安全服务通过安全机制来实现安全策略。

X.800 将这些服务分为 5 类共 14 个特定服务(参见表 1.2)。我们下面将逐类进行讨论[①]。

1.4.1　认证

认证服务与保证通信的真实性有关。在单条消息的情况，如一条警告或报警信号，认证服务功能是向接收方保证消息来自所声称的发送方。对于正在进行的交互，如终端和主机连接，就涉及两个方面。首先，在连接的初始化阶段，认证服务保证两个实体是可信的，也就是说，每个实

① 信息安全文献中使用的许多术语尚未达成广泛的一致。例如，完整性有时是指信息安全性的多个方面。认证有时既用来指身份验证，又用来指本章中列出的各种数据完整性功能。我们这里使用的术语与 X.800 和 RFC 4949 是相一致的。

体都是他们所声称的实体。其次，认证服务必须保证该连接不受第三方的干扰：这种干扰是指，第三方能够伪装成两个合法实体中的一个进行非授权传输或接收。

表 1.2 安全服务(X.800)

认证	**数据完整性**
保证通信的实体是它所声称的实体	保证收到的数据的确是授权实体所发出的数据(即没有修改、插入、删除或重播)
同等实体认证	**具有恢复功能的连接完整性**
用于逻辑连接时为连接的实体的身份提供可信性	提供一次连接中所有用户数据的完整性。检测整个数据序列内存在的修改、插入、删除或重播，且试图恢复之
数据源认证	**无恢复的连接完整性**
在无连接传输时保证收到的信息来源是声称的来源	同上，但仅提供检测，无恢复
访问控制	**选择域连接完整性**
阻止对资源的非授权使用(即这项服务控制谁能访问资源，在什么条件下可以访问，这些访问的资源可用于什么)	提供一次连接中传输的单个数据块内用户数据的指定部分的完整性，并判断指定部分是否有修改、插入、删除或重播
数据保密性	**无连接完整性**
保护数据免于非授权泄露	为单个无连接数据块提供完整性保护,并检测是否有数据修改。另外，提供有限的重播检测
连接保密性	**选择域无连接完整性**
保护一次连接中所有的用户数据	为单个无连接数据块内指定域提供完整性保护；判断指定域是否被修改
无连接保密性	**不可否认性**
保护单个数据块里的所有用户数据	防止整个或部分通信过程中，任一通信实体进行否认的行为
选择域保密性	**源不可否认**
对一次连接或单个数据块里指定的数据部分提供保密性	证明消息是由特定方发出的
流量保密性	**宿不可否认性**
保护那些可以通过观察流量而获得的信息	证明消息被特定方收到

X.800 还定义了以下两个特殊的认证服务。

- **同等实体认证**：为连接中的同等实体提供身份确认。如果处于不同系统中的两个实体实行相同的协议则考虑他们为对等的，例如，位于两个通信系统中的两个 TCP 模块。对等实体认证用于连接的建立或数据传输阶段。该服务想提供这样的保证：一个实体没有试图进行伪装或对以前的连接进行非授权重播。
- **数据源认证**：为数据的来源提供确认。但对数据的复制或修改并不提供保护。这种服务支持电子邮件这样的应用，在这种应用的背景下，通信实体间没有预先的交互。

1.4.2 访问控制

在网络安全中，访问控制是一种限制和控制那些通过通信连接对主机和应用进行访问的能力。为此，每个试图获得访问控制的实体必须被识别或认证后才能获取其相应的访问权限。

1.4.3 数据保密性

保密性是防止传输的数据遭到被动攻击。关于数据传输，可以有几层保护。最广泛的服务在一段时间内为两个用户间所传输的所有用户数据提供保护。例如，如果两个系统间建立了 TCP 连接，则这种广泛的保护将防止在 TCP 连接上传输的任何用户数据的泄露。也可以定义一种较窄的保密性服务，可以是对单条消息或对单条消息内某个特定的范围提供保护。这种细化比起

广泛的方法用处要少，而且实现起来更复杂昂贵。

保密性的另一个方面是防止流量分析。这要求攻击者不能观察到消息的源和宿、频率、长度或通信设施上的其他流量特征。

1.4.4　数据完整性

与保密性一样，完整性可应用于消息流、单条消息或消息的指定部分。同样，最有用也最直接的方法是对整个数据流提供保护。

用于处理消息流、面向连接的完整性服务保证收到的消息和发出的消息一致，没有复制、插入、修改、更改顺序或重播。该服务也涉及对数据的破坏。因此，面向连接的完整性服务处理消息流的修改和拒绝服务两个问题。另一方面，无连接的完整性服务，仅仅处理单条消息，而不管大量的上下文信息，其通常仅仅防止对单条消息的修改。

我们可以区分有恢复和无恢复的服务。因为完整性服务和主动攻击有关，我们更关心检测而不是阻止攻击。如果检测到完整性遭破坏，那么服务可以简单地报告这种破坏，并通过软件的其他部分或人工干预来恢复被破坏部分。另外，我们下面会看到，有些机制可用来恢复数据完整性。通常，自动恢复机制是一种更具吸引力的选择。

1.4.5　不可否认性

不可否认性防止发送方或接收方否认传输或接收过某条消息。因此，当消息发出后，接收方能证明消息是由声称的发送方发出的。同样，当消息接收后，发送方能证明消息确实由声称的接收方收到。

1.4.6　可用性服务

X.800 和 RFC 4949 都定义可用性为：根据系统的性能说明，能够按被授权系统实体的要求访问或使用系统和系统资源的性质(即当用户请求服务时，若系统能够提供符合系统设计的这些服务，则系统是可用的)。许多攻击可导致可用性的损失或减少。一些自动防御措施，如认证、加密，可对付某些攻击。而其他的一些攻击需要一些物理措施来阻止或恢复分布式系统中要素可用性的损失。

X.800 将可用性视为和各种安全服务相关的性质。但是，单独说明可用性服务是颇有意义的。可用性服务确保系统的可用性。这种服务处理由拒绝服务攻击引起的安全问题。它依赖于对系统资源的恰当管理和控制，因此依赖于访问控制服务和其他安全服务。

1.5　安全机制

表 1.3 列出了 X.800 中定义的安全机制。由表可知，这些安全机制可分成两类：一类在特定的协议层实现，如 TCP 或应用层协议，另一类不属于任何的协议层或安全服务。本书将会在适当的时候讨论这些机制，在此除了讨论加密的定义外不详论之。X.800 区分可逆和不可逆加密机制。可逆加密机制只是一种加密算法，数据可以加密和解密。不可逆加密机制包括 Hash 算法和消息认证码，用于数字签名和消息认证应用。

基于 X.800 中的定义，表 1.4 给出了安全服务和安全机制的关系。

表 1.3 安全机制(X.800)

特定安全机制	普遍的安全机制
可以并入适当的协议层以提供一些 OSI 安全服务	不局限于任何特定的 OSI 安全服务或协议层的机制
加密 运用数学算法将数据转换成不可知的形式。数据的变换和还原依赖于算法和零个或多个加密密钥	**可信功能** 据某些标准被认为是正确的功能(如根据安全策略所建立的标准)
数字签名 附加于数据单元之后的一种数据,它是对数据单元的密码变换,以使得(如接收方)可证明数据源和完整性,并防止伪造	**安全标签** 资源(可能是数据单元)的标志,命名或指定该资源的安全属性
访问控制 对资源行使访问控制的各种机制	**事件检测** 检测与安全相关的事件
数据完整性 用于保证数据单元或数据单元流的完整性的各种机制	**安全审计跟踪** 收集可用于安全审计的数据,它是对系统记录和行为的独立回顾和核查
认证交换 通过信息交换来保证实体身份的各种机制	**安全恢复** 处理来自安全机制的请求,如事件处理、管理功能和采取恢复行为
流量填充 在数据流空隙中插入若干位以阻止流量分析	
路由控制 能够为某些数据选择特殊的物理上安全的路线并允许路由变化(尤其是在怀疑有侵犯安全的行为时)	
公证 利用可信的第三方来保证数据交换的某些性质	

表 1.4 安全服务与机制间的联系

	机制							
服务	加密	数字签名	访问控制	数据完整性	认证交换	流量填充	路由控制	公证
同等实体认证	Y	Y			Y			
数据源认证	Y	Y						
访问控制			Y					
保密性	Y						Y	
流量保密性	Y					Y	Y	
数据完整性	Y	Y		Y				
不可否认性		Y		Y				Y
可用性				Y	Y			

1.6 网络安全模型

我们要讨论的大多数通信模型如图 1.2 所示,通信一方要通过 Internet 将消息传送给另一方,那么通信双方,称为交互的主体,必须协调努力共同完成消息交换,我们可以通过定义 Internet 上从源到宿的路由以及通信主体共同使用的通信协议(如 TCP/IP)来建立逻辑信息通道。

在需要保护信息传输以防攻击者威胁消息的保密性、真实性等的时候,就会涉及信息安全,任何用来保证安全的方法都包含两个方面:

- 与待发送信息安全相关的变换。如对消息加密,它打乱消息使得攻击者不能读懂消息,或者将基于消息的编码附于消息后,用于验证发送方的身份。

- 双方共享某些秘密信息，并希望这些信息不为攻击者所知。如加密密钥，它配合加密算法在消息传输之前将消息加密，而在接收端将消息解密①。

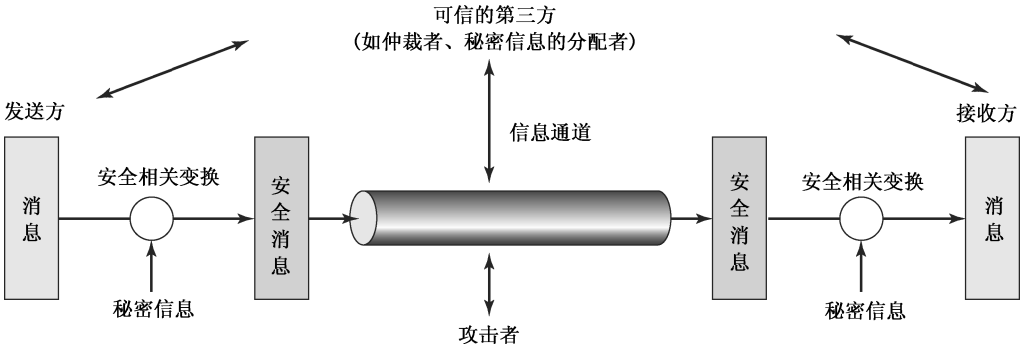

图 1.2　网络安全模型

为了实现安全传输，可能需要有可信的第三方。例如，第三方负责将秘密信息分配给通信双方，而对攻击者保密，或者当通信双方关于信息传输的真实性发生争执时，由第三方来仲裁。

上述模型说明，设计安全服务应包含下列 4 个方面的内容：

(1)设计一个算法，它执行与安全相关的变换。该算法应是攻击者无法攻破的。
(2)产生算法所使用的秘密信息。
(3)设计分配和共享秘密信息的方法。
(4)指明通信双方使用的协议，该协议利用安全算法和秘密信息实现安全服务。

本书的第一部分至第五部分讨论的是安全机制和服务，它们遵循图 1.2 所示的模型，但是，还有其他与安全有关的情形不完全符合该模型，本书也会讨论这些内容，它们的一般模型如图 1.3 所示，该模型希望保护信息系统不受有害的访问，大多数读者都熟悉黑客引起的问题，黑客试图渗入到通过网络可访问的系统，他可能没有恶意、只是对闯入或进入计算机系统感到满足。入侵者可能是一个不如意的雇员，想进行破坏，或者是一个罪犯，想利用计算机获利(如获取信用卡号或者进行非法的资金转账)。

另一种类型的有害访问是在计算机系统中加入程序，它利用系统的弱点来影响应用程序和实用功能程序，如编辑程序和编译程序。对程序的威胁有以下两种。

- **信息访问威胁**：以非授权用户的名义截获或修改数据。
- **服务威胁**：利用计算机中的服务缺陷禁止合法用户使用这些服务。

病毒和蠕虫是两种软件攻击，这些攻击可通过磁盘进入系统，如果磁盘上的应用软件中隐藏有害程序。这些攻击也可以通过网络进入系统。网络安全更关心的是通过网络进入系统的攻击。

对付有害访问所需的安全机制分为两大类(参见图 1.3)。第一类称为看门人功能，它包括基于口令的登录过程，该过程只允许授权用户的访问，还包括监控程序，该程序负责检测和阻断蠕虫、病毒以及其他类似的攻击。一旦非法用户或软件获得了访问权，那么由各种内部控制程序组成的第二道防线就监视其活动、分析存储的信息，以便检测非法入侵者。这些问题将会在第六部分讨论。

① 第二部分讨论的公钥密码中，只需发送方或者接收方拥有秘密信息。

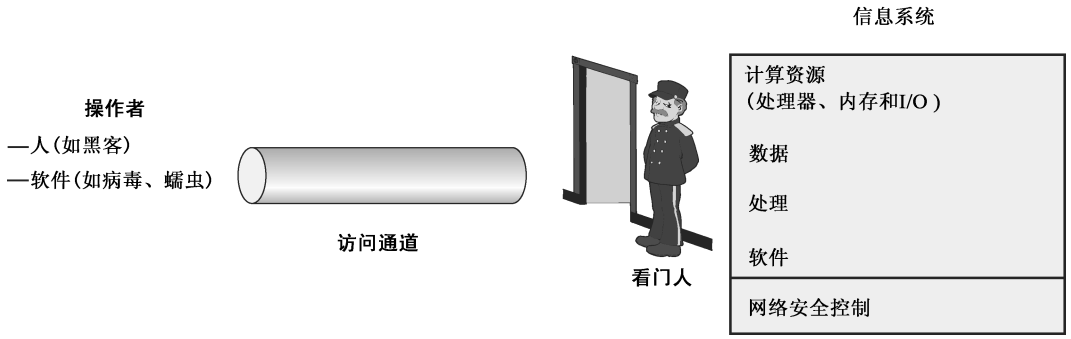

图 1.3 网络访问安全模型

1.7 推荐读物

参考文献[STAL12]提供了计算机和网络安全方面的广泛介绍。[SCHN00]对从事计算机和网络安全的实践者来说是很有价值的读物。该书讨论了技术，特别是密码学，在提供安全方面的局限性。该书认为还需要考虑硬件和软件实现、网络及从事安全与攻击的人员等因素。

读一些有关计算机安全的引论性的论文是有用的。它们提供了一种从历史的观点来理解现在的工作和想法。可以读的论文有[WARE79]，[BROW72]，[SALT75]，[SHAN77]以及[SUMM84]。两篇稍近一些的论文[ANDR04]，[LAMP04]则简短地介绍了计算机安全。参考文献[NIST95](290 页)则是该主题大全式的文章。另一篇好的论文是[NRC91]。参考文献[FRAS97]也很有用。

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 Computeing in the Information Age*. Washington, D. C.: National Academy Press, 1991.

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

SCHN00 Schneier, B. *Secrets and Lies: Digital Security in a Networked World*. New York: Wiley 2000.

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

STAL12 Stallings, W., and Brown, L. *Computer Security*. Upper Saddle River, NJ: Prentice Hall, 2012.

SUMM84 Summers, R. "An Overview of Computer Security." *IBM Systems Journal*, Vol. 23, No. 4, 1984.

WARE79 Ware, W., ed. *Security Controls for Computer Systems*. RAND Report 609-1. October 1979.

1.8　关键术语、思考题和习题

关键术语

访问控制	拒绝服务	被动威胁
主动威胁	加密	重放
认证	完整性	安全攻击
真实性	入侵者	安全机制
可用性	伪装	安全服务
数据保密性	非否认性	流量分析
数据完整性	OSI 安全框架	

思考题

1.1　OSI 安全框架是什么?

1.2　被动和主动安全威胁的区别是什么?

1.3　列出并简短地定义被动和主动安全攻击的种类。

1.4　列出并简短地定义安全服务的种类。

1.5　列出并简短地定义安全机制的种类。

习题

1.1　考虑一个自动取款机(ATM),用户为其提供个人身份码(PIN)和账户访问的卡。给出有关这个系统的安全性,完整性和可用性要求的例子,就每一个例子说明要求的重要性程度。

1.2　以电话交换系统为例重做习题 1.1。电话交换系统根据呼叫用户呼叫的电话号码通过交换网络路由呼叫。

1.3　考虑为各种组织产生文档的桌面发布系统。

(a)给出一种发布类型的例子,此时对存储数据的安全性是最重要的。

(b)给出一种发布类型的例子,此时对存储数据的完整性是最重要的。

(c)给一个例子,其对系统可用性的要求是最重要的。

1.4　对于下面的资产,当发生保密性,可用性和完整性损失时,分别为其产生的影响划分低、中和高等级,并陈述理由。

(a)在自己的网络服务器上管理公开信息的组织。

(b)法律执行组织管理极端敏感的调查信息。

(c)金融机构管理例行的行政信息(非隐私信息)。

(d)合同签订机构的大单收购信息系统,包含敏感、预投标阶段的合同信息和例行的行政信息。请分别评价这两份信息资产的影响情况以及整个信息系统的影响情况。

(e)发电厂包含有 SCADA(监管控制和数据获取)系统,该系统负责为军事设施提供电力分发。SCADA 系统包含有实时传感器数据和例行的行政信息。请分别评价这两份信息资产的影响情况以及整个信息系统的影响情况

1.5　类似于表 1.4,画一个矩阵来表明安全服务和安全攻击的关系。

1.6　类似于表 1.4,画一个矩阵来表明安全机制和安全攻击的关系。

1.7　阅读 1.7 节所引用的经典论文,写一篇 500 ~ 1000 字的论文(或 8 ~ 12 页的 PowerPoint 幻灯片展示)总结在这些论文出现的关键概念并强调对大多数或全部论文通用的概念。