第 1 章 信息系统安全概述

信息技术的发展带动了全球信息化的发展，从而使信息基础设施成为社会基础设施中必不可少的关键基础设施，与此同时，网络信息系统的安全问题也逐渐引起人们的重视。不解决信息安全问题，不强化网络化的信息安全保障，信息化将得不到可持续的健康发展。

在现实应用中，信息系统已由传统意义上的存放和处理信息的独立系统演变为互相连接、资源共享的系统集合，也就是说，信息系统同时也是一个网络系统。此外信息安全是一个极大的技术领域，本书的侧重点在于网络中的信息安全，因此为叙述和理解方便，本书中信息系统也被称为网络信息系统。

本章首先分析安全问题的起因及信息系统面临的各种攻击，然后介绍网络信息系统的安全需求、安全服务及知名的安全评估标准，使大家对网络信息系统的安全问题有个大致的了解。鉴于加密技术在处理安全问题时的广泛应用，本章最后对加密功能的实施进行了探讨。

1.1 网络信息系统的脆弱性

所谓网络信息系统，是指互相连接起来的独立自主的计算机信息系统的集合。网络信息系统中的计算机能够方便地交换信息、共享资源。随着现代通信技术和计算机技术的不断发展，计算机网络的规模以前所未有的速度快速增长，信息共享应用日益广泛和深入。不难发现，以个人计算机（PC）为中心的计算方式，正在向以网络为中心的计算方式发展。

网络信息系统促使了科学、技术、文化、教育和生产的快速发展，为提高现代人的生活质量提供了极大的便利。随着网络经济和网络社会时代的到来，网络将会进入一个

无处不有、无所不用的境地，经济、文化、军事和社会活动将会强烈地依赖网络，但任何一项技术在发展过程中都必然会产生自己的对立面，当然人类终究又会找出解决的办法。网络在带来资源共享的同时也带来了安全问题，这是天生的一对矛盾，因特网固有的跨国界性、无主管性、不设防性和缺少法律约束性既为各国带来机遇，也带来了巨大的风险。目前作为国家重要基础设施的网络信息系统的安全性已经成为关系国家主权和安全、社会的稳定、民族文化的继承和发扬的重要问题。其重要性，正随着全球信息化步伐的加快而变得越来越重要，所以网络信息系统的安全性问题也逐渐成为计算机网络中的研究焦点。

从技术的角度看，网络信息系统是脆弱的，主要原因有 3 个方面。

第一个方面是由于网络的开放性。首先，业务基于公开的协议，协议的体系和实现是公开的，其中的缺陷很可能被众多熟悉协议的程序员所利用；其次，所有信息和资源通过网络共享，远程访问使得各种攻击无须到现场就能得手；此外，基于主机上的社团彼此信任的基础是建立在网络连接之上的，同传统方式（如相貌、声音等）完全不同，容易假冒。网络的开放性决定了网络信息系统的脆弱性是先天的。

其次就是组成网络的通信系统和信息系统的自身缺陷。现有的商用计算机系统（包括通用和专用操作系统及各种应用系统）存在许多安全性问题，它们在客观上导致了计算机系统在安全上的脆弱性。由于人们的认知能力和实践能力的局限性，在系统设计和开发过程中会产生许多的错误、缺陷和遗漏，成为安全隐患，而且系统越大、越复杂，这种安全隐患越多。1999 年安全应急响应小组论坛（Forum of Incident Response and Security Teams，FIRST）的专家指出：程序每千行中至少有一个缺陷，随着系统的功能越做越强大，复杂性也不断增加，错误会越来越多。到 2001 年，《应用密码学》的作者 Bruce Schneier 指出每千行程序至少有 5～10 个缺陷。

通过下面一组数据（见表 1.1）可以看出，系统中存在着大量的隐藏的漏洞，进而可知网络信息系统中弱点和隐患是普遍存在的。此外用户使用时系统配置本身和用来提供保护的安全系统的配置也可能存在问题。

表 1.1 微软通用操作系统的安全性估计

操作系统	推出年份	代码行数(万)	估计缺陷数(万)
Windows 3.1	1992	300	1.5～3
Windows 95	1995	500	2.5～5
Windows NT4.0	1996	1650	8.25～16.5
Windows 98	1998	1800	9～18
Windows 2000	2000	3500～5000	17.5～35

第三个原因是由于黑客（hacker）及病毒等恶意程序的攻击

其实早期(20 世纪 60～70 年代）的黑客(hacker)是褒义的,他们是独立思考、奉公守法的计算机迷，他们享受智力上的乐趣，对解放和普及计算机技术做出了重大贡献，培养了一批信息革命的先驱。典型的代表是微软公司的盖茨、苹果公司的伍兹和乔布斯，他们的大本营在 MIT、硅谷、斯坦福等计算机人才云集的地方。而当今的黑客是指那些专门闯入计算机系统、网络、电话系统和其他通信系统，具有不同的目的（政治的、商业的、或者仅仅出于恶作剧的目的），非法地入侵和破坏系统、窃取信息的攻击者，他们被早期的黑客称为破坏者（cracker)。现在随着网络的发展，由于存在大量公开的黑客站点，所以获得黑客工具非常容易，黑客技术也越来越易于掌握，这导致网络面临的威胁也越来越大。

大家熟知的计算机病毒是指能利用系统进行自我复制和传播，通过特定事件触发破坏系统的程序，根据其自我复制和传播的方式分为引导型、文件型、宏病毒、邮件传播等类型。

除了上述几种类型外还有下述其他有害程序。

1. 程序后门

后门就是信息系统中未公开的通道，在用户未授权的情况下，系统的设计者或其他人可以通过这些通道出入系统而不被用户发觉比如，监测或窃听用户的敏感信息，控制系统的运行状态等。后门通常是指某些特定输入序列的数码或某个特定用户 ID)或一个不可能事件序列能激活的数码

后门的形成可以有几种途径：黑客通过侵入一个信息系统而在其中设置后门，如安放后门程序或修改操作系统的相关部分等；一些不道德的设备生产厂家或程序员在生产过程中在设备中留下后门。以上两种后门的设置显然是恶意的另外，信息系统的一个重要特征是对用户的友好快速服务，其中远程服务是最受欢迎的方式。远程服务一般具备两个特征：远程信息检测和远程软件加载。这两种特征看起来不是恶意的，但实际上，用户一般不知道厂家或其他人在检测系统的何种信息或在加载何种软件，所以很容易被恶意利用；显然这也是一种后门。因此信息系统中后门是普遍存在的。

后门一旦被原来的程序员利用，或者被有意或无意的人发现将会带来严重的后果。如可利用后门在程序中建立隐蔽通道，植入一些隐蔽的恶意程序，进而可以非法访问系统和网络，达到窃取、篡改、伪造和破坏信息的目的

2. 特洛伊木马

特洛伊木马的名字起源于希腊神话，指冒充正常程序的有害程序，或包含在有用程

序中的隐藏代码，当用户运行的时候将造成破坏，如间接实现非授权用户不能直接实现的功能或毁坏数据等。特洛伊木马不能自我复制和传播。

3.“细菌”程序

“细菌”程序是不明显危害系统或数据的程序，其惟一目的就是复制自己。本身没有破坏性，但通过不停地自我复制，能耗尽系统资源，造成系统死机或拒绝服务。

4. 蠕虫

蠕虫是指通过某种网络载体，利用网络连接关系从一个系统蔓延到另一个系统的程序。系统中，网络蠕虫一旦被激活，其行为与病毒或细菌类似。其中最有名的莫过于“莫里斯蠕虫”病毒，它是第一个对因特网造成严重破坏的恶意程序。

更值得一提的是网络的出现改变了传统恶意病毒程序的传播方式，不仅加快了攻击手段和病毒的传播速度，扩大了危害范围，而且增强了攻击的破坏力。

综上所述，尽管计算机网络已从 20 世纪 70 年代中期用于科研和学术目的的美国国防部(DOD)的阿帕网(ARPA,即现在的 DARPANET)迅速发展到现在商用的庞大的因特网(Internet)，提供了各种各样的应用，但其技术基础是不安全的。下面将分析网络面临的主要威胁和可能遭受的攻击，目的是全面了解网络信息系统的脆弱性及所面临的危险，提高安全意识。

.1.1 网络信息系统的主要威胁

现有的网络信息系统都不可避免地存在安全缺陷，为了便于理解，本节从典型的 TCP/IP 网络 5 层参考模型入手，描述在各协议层次上网络信息系统可能遭受到的一些典型的安全威胁。

1. 物理层

到目前为止，大部分的网络连接设备采用的是双绞线和铜缆，它们不可避免的会产生电磁干扰(EMI)和电磁辐射，如果有足够的设备和耐心，完全可以接收到通信链路中传输的信号并加以还原，窃取重要信息，甚至插入，删除信息。无线信道的安全性更加脆弱，几乎不可避免的会遭受被窃听或劫持等攻击。采用光纤方式，由于传输的是光信号而不是电信号，不会产生电磁辐射，安全性能有所提高，但仍然面临被截断或搭线的威胁。

2. 数据链路层

数据监听是数据链路层最常见的攻击手段。目前的局域网基本上都采用以广播为技术基础的以太网，各主机处于同一信任域，传输信息可以相互监听。因此，只要接入以太网上的任一节点，就可以捕获在这个以太网上发送的所有数据包，从而窃取关键信息，这是以太网所固有的安全隐患。要解决这个问题，首先，应当尽可能地划分网段，将非授权用户与敏感的网络资源相互隔离，从而防止可能的非法监听。其次，以交换式集线器代替广泛使用的共享式集线器，减少数据监听的设备基础。再者，还可以运用虚拟局域网(VLAN)技术，把所有服务器和用户节点都放置在各自的虚拟局域网内，将以太网通信变为点对点通信，互不干扰。

3. 网络层

TCP/IP 协议是 20 世纪 90 年代以来发展最为迅速的协议，尽管它们在网络互联方面取得了巨大的成功，但是由于 TCP/IP 在设计之初并没有考虑到安全性问题，因此在协议层次上具有相当多的安全漏洞网络层典型的安全问题有：

- IP 欺骗，伪造 IP 地址以获取非法权利；
- 利用源路由选项，侦听数据；
- 对路由协议，如 RIP 等进行攻击；
- 利用 ICMP 的 Redirect 报文破坏路由机制。

为了尽可能解决这些安全性问题，Internet 的技术管理机构 IETF(Internet Engineering Task Force)提出了一种新版本 IP 协议——IPv6，通过 IP 数据包首部后面的扩展首部实现安全特性，在鉴别和保密两个方面制定了一系列标准、并强制性地要求支持这些安全标准。

4. 传输层

TCP 协议的实现给黑客们留下了攻击空间，它的 3 次握手建链方式，成为实现 SYN Flooding 拒绝服务攻击方式的基础，而且 TCP 连接很容易被欺骗、截取和破坏。除此之外，伪造 TCP/UDP 中的源地址、源端口也是一种常见的地址欺骗方式。

5. 应用层

应用层存在认证、访问控制、完整性、保密性等所有安全问题。如应用层的很多协议缺少严格的加密认证机制，DNS 便是一例。DNS 提供主机名与 IP 地址的映射关系，它从出现以来就缺乏加密认证机制，所以黑客很容易在监听，伪造的基础上进行攻击。

其他比较常见的网络软件与网络服务的漏洞有：NFS 的 RPC 调用、Finger 漏洞、匿名 FTP 和远程登录,等等。

1.1.2 攻击的种类

对网络信息系统的攻击来自很多方面，这些攻击可以宏观地分为人为攻击和自然灾害攻击。它们都会对通信安全构成威胁，但是精心设计的人为攻击威胁最大，也最难防备。本节主要分析人为攻击的情况。

对网络信息系统的人为攻击，通常都是通过寻找系统的弱点，以非授权方式达到破坏、欺骗和窃取数据等目的。采用不同的分类标准（如攻击手段、攻击目标等），会得出不同的分类结果。

美国国家安全局在 2000 年 9 月发布的《信息保障技术框架(IATF)》3.0 版中将攻击分为以下 5 类：被动攻击、主动攻击、物理临近攻击、内部人员攻击和软硬件配装攻击。下面分别介绍这 5 类攻击的特点。

1. 被动攻击

被动攻击是在未经用户同意和认可的情况下将信息或数据文件泄露给系统攻击者，但不对数据信息做任何修改。通常包括监听未受保护的通信、流量分析、解密弱加密的数据流、获得认证信息（如密码）等。其中流量分析情况比较微妙，假如通过某种手段，如加密屏蔽了消息内容或其他通信量，使得攻击者从截获的消息中无法得到消息的真实内容，但攻击者还能通过观察这些数据包的模式，分析出通信双方的位置、通信的次数及消息的长度等信息，而这些信息可能对通信双方来说是敏感的，不希望被攻击者得知。这种分析称为流量分析。

被动攻击常用的手段有下列几种。

(1) 搭线监听

搭线监听是最常用的手段，将导线搭到无人值守的网络传输线上进行监听。只要所搭的监听设备不影响网络负载平衡，网络站点上是无法发现的。通过解调和正确的协议分析，完全可以掌握通信的全部内容。

(2) 无线截获

对难于搭线监听的可以用无线截获方法得到信息，通过高灵敏接收装置接收网络站点辐射的电磁波或网络连接设备辐射的电磁波，通过对电磁信号的分析恢复原数据信号从而获得网络信息。尽管有时数据信息不能通过电磁信号全部恢复，但可能得到极有价值的情报。有些网络通信是通过无线传送的，此时无线截获与搭线监听有同样功效。

(3) 其他截获

用程序和病毒截获信息是计算机技术发展出的新型手段，在通信设备或主机中预留程序代码或施放病毒程序后，这些程序会将有用的信息通过某种方式发送出来。

被动攻击不易被发现，常是主动攻击的前期阶段。由于被动攻击不会对被攻击的信息做任何修改，留下的痕迹很少，或者根本没有留下痕迹，因而非常难以检测。抗击这种攻击的重点在于预防，具体措施包括使用虚拟专用网（VPN）、采用加密技术保护网络以及使用加保护的分布式网络等

2. 主动攻击

主动攻击涉及某些数据流的篡改或虚假流的产生。这些攻击可分为以下 4 个子类：假冒、重放、篡改消息和拒绝服务。

(1)假 冒

假冒指的是某个实体（人或系统）假扮成另外一个实体，以获取合法用户的权利和特权。

(2)重 放

重放即攻击者对截获的某次合法数据进行复制，以后出于非法目的重新发送，以产生未授权的效果。

(3) 篡改消息

篡改消息指一个合法消息的某些部分被改变、删除，或者消息被延迟或改变顺序，以产生未授权的效果。如修改数据文件中的数据，将“允许甲执行某操作”改为“允许乙执行某操作”。

(4) 拒绝服务

拒绝服务即常说的 DoS(deny of service)，会导致对通信设备的正常使用或管理被无条件地拒绝。通常是对整个网络实施破坏，如用大量无用信息将资源（如通信带宽、主机内存等）耗尽，以达到降低性能、中断服务的目的。这种攻击也可能有一个特定的目标，如到某一特定目的地（如安全审计服务）的所有数据包都被阻止。大家一定还记得 2000 年 2 月在全球范围内引起了巨大震动的安全事件：Yahoo、Amazon、eBay 等著名网站相继遭受到攻击导致服务中断，攻击者采用的攻击方式就是拒绝服务攻击。

主动攻击的特点与被动攻击正好相反。被动攻击虽然难以检测，但可采用措施有效地防止，而要绝对防止主动攻击是十分困难的，因为这需要随时随地对所有的通信设备和通信活动进行物理和逻辑保护。因此防止主动攻击的主要途径是检测，以及能从此攻击造成的破坏中及时地恢复，同时检测还具有某种威慑效应，在定程度上也能起

到防止攻击的作用。具体措施包括自动审计、入侵检测和完整性恢复等

3. 物理临近攻击

物理临近攻击指未授权个人以更改、收集或拒绝访问为目的而物理接近网络、系统或设备。这种接近可以是秘密进入或公开接近，或两种方式同时使用。

4. 内部人员攻击

内部人员攻击可以是恶意的或非恶意的。恶意攻击是指内部人员有计划地窃听、偷窃或损坏信息，或拒绝其他授权用户的访问。联邦调查局（FBI）的评估显示 80% 的攻击和入侵来自组织内部。内部人员知道系统的布局、有价值的数据放在何处及何种安全防范系统在工作，这种攻击最难于检测和防范。

非恶意攻击则通常由粗心、缺乏技术知识或为了“完成工作”等无意间绕过安全策略但对系统产生了破坏的行为造成。

5. 软硬件配装攻击

又称分发攻击指在软硬件的生产工厂内或在产品分发过程中恶意修改硬件或软件。这种攻击可能给一个产品引入后门程序等恶意代码，以便日后在未获授权的情况下访问信息或系统。

需要说明的是，在现实世界中，一次成功的攻击过程会综合几种攻击手段。通常是采用被动攻击手段来收集信息，制定攻击步骤，然后通过主动攻击来达到目的。此外，人为攻击所造成的危害程度取决于被攻击的对象，与所采用的攻击手段无关。

1.2 安全需求和安全服务

通过上面的分析，可以得知网络信息系统的安全性是很脆弱的，需要采取措施加以保护。那么网络信息系统的安全需求包括什么内容？该采取什么措施来保护网络的安全？密码又有什么作用？

1.2.1 网络信息系统安全的基本需求

网络信息系统安全的内容包括了系统安全和信息安全两个部分。系统安全主要指网络设备的硬件、操作系统和应用软件的安全；信息安全主要指各种信息的存储、传输的安全。网络安全通常依赖于两种技术：一是传统意义上的存取控制和授权，如访问控制表技术、口令验证技术等；二是利用密码技术实现对信息的加密、身份鉴别等。

国际标准化组织（International Standardization Organization，ISO）对“计算机安全”的定义是：“为数据处理系统建立和采用的技术和管理上的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露”。此概念偏重于静态信息保护，而且没有考虑网络的因素另一种考虑了网络因素的定义是：“保护网络系统中的各种资源不因偶然或恶意的原因而遭到占用、毁坏、更改和泄露，系统能够连续正常运行。这些资源包括计算机和网络设备、存储介质、软件、数据等”，此定义侧重于动态意义的描述。鉴于现有的网络系统是不断发展，动态变化的，本书采用第二种定义

网络信息系统安全的具体含义会随着“角度”的变化而变化。比如：从用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络 上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私，同时也避免其他用户的非授权访问和破坏。

从网络运行和管理者角度说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“后门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。

而对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，对国家造成巨大损失

一般认为可以从以下 5 个方面定义网络信息系统安全的基本需求。

1. 保密性(confidentiality)

保密性是指信息不泄露给非授权用户、实体和过程，不被非法利用。上文提到的被动攻击中的监听、流量分析就是对系统的保密性进行攻击

由于系统无法确认是否有未授权的用户窃听网络上的数据，这就需要使用一种手段来对数据进行保密处理。通常采用数据加密技术来实现这一目标的，加密后的数据能够保证在传输、使用和转换过程中不被第三方非法获取数据经过加密变换后，明文转换成密文，只有经过授权的合法用户，使用被授予的正确密钥，通过解密算法才能将密文还原成明文。反之，未经授权的用户因不掌握解密算法或解秘密钥，无法获取原文的信息，从而限制了其对加密数据的访问，维护了数据的保密性。当然加密算法必须有足够的复杂度，以排除从密文中破译出消息的可能性。

除了使用各种加密技术外，数据的存储保密性也可通过访问控制的方法来实现网络和系统管理员根据不同的数据类型和应用需求，对数据和用户进行分类，配置不同的访问模式。这种访问控制不难实现，许多带安全机制的操作系统都具有这种功能，如 UNIX，Windows NT 等，但早期的 DOS 和 Windows 95 不具有这种功能。

2. 完整性(Integrity)

完整性是指数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被非法修改、破坏和丢失，并且能够判别出数据是否已被改变。其目的就是保证信息系统上的数据处于一种完整和未受损的状态，不会因有意或无意的事件而被改变或丢失。上文提到的主动攻击中的篡改即是对系统的完整性进行破坏。

可采用加密、数字签名和散列函数（hash function）来保护数据的完整性。最常用的为散列函数，散列函数也译为杂凑函数、哈希函数，通常表示为函数 $h=H(M)$，其输入 M 为任意长度的消息，输出 h 为长度固定的消息摘要。本书的第 8 章中对散列函数的特性、功能、算法等有详细的描述。

3. 可用性(availability)

可用性是指可被授权实体访问并按需求使用的特性，即当需要时授权者总能够存取所需的信息，攻击者不能占用所有的资源而妨碍授权者的使用。网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

可用性中的按需使用可通过鉴别技术来实现，即每个实体都的确是其所宣称的那个实体。但要保证系统和网络中能提供正常的服务，除了备份和冗余配置外，目前没有特别有效的方法。

4. 可控性(controllability)

可控性是指可以控制授权范围内的信息流向及行为方式，对信息的传播及内容具有控制能力。

为保证可控性，首先系统能够控制谁能够访问系统或网络上的数据，以及如何访问（是只读还是可以修改等），通常通过访问控制列表等方法来实现；其次需要对网络上的用户进行验证，可通过握手协议和鉴别进行身份验证；最后要将用户的所有活动记录下来便于查询审计。

5. 不可否认性(non-repudiation)

不可否认性是指信息的行为人要对自己的信息行为负责，不能抵赖自己曾有过的行为，也不能否认曾经接到对方的信息。这在交易系统中十分重要。

通常将数字签名和公证机制一同使用来保证不可否认性。数字签名是手写签名的功能模拟，其实是一个函数，输入为所保护的消息的所有比特位及一个秘密密钥，输出

为一个数值，其正确性可通过另一个密钥来检验本书的第 9 章将对数字签名的特性、功能、标准等进行详细描述。

1.2.2 安全服务

如何才能满足网络信息系统安全的基本需求呢？通常将为加强网络信息系统安全性及对抗安全攻击而采取的一系列措施称为安全服务。

安全服务的主要内容包括安全机制、 安全连接、安全协议和安全策略等，能在一定程度上弥补和完善现有操作系统和网络信息系统的安全漏洞。

关于安全服务与有关机制的一般描述，可参见 ISO 制定的国际标准 ISO7498-2：《信息处理系统开放系统互连基本参考模型第 2 部分——安全体系结构》。该标准为开放系统互连(Open Systems Interworking，OSI ）描述了安全体系结构的基本参考模型，并确定在参考模型内部可以提供这些安全服务与安全机制的位置（该标准在 1995 年被我国引进为国家标准 GB/T9387.2—1995）。

ISO7498—2 中定义了 5 类可选的安全服务

鉴别(authentication)

鉴别用于保证通信的真实性，证实接收的数据就来自所要求的源方，包括对等实体鉴别和数据源鉴别。数据源鉴别连同无连接的服务一起操作，而对等实体鉴别通常与面向连接的服务一起操作，一方面可确保双方实体是可信的（即每个实体都的确是他们宣称的那个实体），另一方面可确保该连接不被第三方干扰（如假冒其中的一方进行非授权的传输或接收）。

2. 访问控制(access control)

访问控制用于防止对网络资源的非授权访问，保证系统的可控性。访问控制可以用于通信的源或目的，或是通信链路上的某一地方。一般用在应用层，有时希望为子网提供保护，可在传输层实现访问控制

3. 数据保密（data confidentiality)

数据保密用于保护数据以防止被动攻击，服务可根据保护范围的大小分为几个层次。其中最广义的服务可保护一定时间范围内两个用户之间传输的所有数据；较狭义的服务包括对单个消息的保护或对一个消息中某个特定字段的保护，不过同广义服务比起来，这种服务用处较小，代价可能更高。

4. 数据完整性(data integrity)

数据完整性用于保证所接收的消息未经复制、插入、篡改、重排或重放，即用于对付主动攻击。此外还能对遭受一定程度毁坏的数据进行恢复。同数据保密性一样，数据完整性可用于一个消息流、单个消息或一个消息中的所选字段，同样，最为有用和直接的方法是对整个流的保护。

5. 不可否认(non-repudiation)

不可否认用于防止通信双方中的某一方抵赖所传输的消息。即消息的接收者能够证明消息的确是由消息的发送者发出的，而消息的发送者能够证明这一消息的确已被消息的接收者接收了。

这 5 类安全服务同上节中的安全需求的 5 个方面基本对应。

1.2.3 安全服务的实施位置

表 1.2 列出了协议栈各层中可提供的安全服务。从表 1.2 可以看出，应用层可以提供所有的安全服务，而同一种安全服务也可以在网络的好几层中实施，但实施后提供的安全保障有各自的优缺点，实际应用中采用哪种方式应取决于应用（程序）对安全保密的要求，以及用户自己的实际需要。

表 1.2 协议栈各层中可提供的安全服务

安全服务	TCP/IP 协议层			
	数据链路层	网络层	传输层	应用层
对等实体鉴别	—	Y	Y	Y
数据源鉴别	—	Y	Y	Y
访问控制服务	—	Y	Y	Y
连接保密性	Y	Y	Y	Y
无连接保密性	Y	Y	Y	Y
选择域保密性	—	—	—	Y
流量保密性	Y	Y	—	Y
有恢复功能的完整性	—	—	Y	Y
无恢复功能的完整性	—	Y	Y	Y
选择域连接完整性	—	—	—	Y
无连接完整性	—	Y	Y	Y

续表

安全服务	TCP/IP 协议层			
	数据链路层	网络层	传输层	应用层
选择域非连接完整性	—	—	—	Y
源发方不可否认	—	—	—	Y
接收方不可否认	—	—	—	Y

说明："Y"表示可以提供，"—"表示不能提供

下面具体讨论一下在协议栈的各层提供安全服务的优点和缺点。

1. 应用层

应用层的安全措施只能在通信两端的主机系统上实施。在应用层提供安全保障主要有下述几个方面的优点。

安全策略和措施通常是基于用户制定的，因而能很容易地访问用户的一些鉴别数据，如私人密钥等。

对用户想要保护的数据具有完整的访问权，因而能很方便地提供一些服务，如不可否认服务。

不必依赖操作系统来提供这些服务，可根据应用程序的需求自由扩展，因而能满足一些特殊的安全需求。通常，应用程序对操作系统中实施的功能只有使用权，没有控制权。

由于应用程序对数据的实际含义有着充分的理解，可以区分在同一通道上传输的某些具体数据的安全性要求，因此可很方便地据此采用相应的安全措施。

应用层安全的缺点在于：对每个应用都需要单独设计一套安全机制，而现有的应用必须进行相应的改动后才能提供安全保障。这样导致的后果：一是效率太低；二是对现有系统的兼容性太差；三是改动的程序太多，出现错误的概率大增，为系统带来更多的安全漏洞。

2. 传输层

传输层上的安全同样只可在端系统中实现。与应用层安全相比，在传输层提供安全服务的好处是能为其上的各种应用提供安全服务，提供了更加细化的基于进程对进程的安全服务，这样现有的和未来的应用可以很方便地得到安全服务，而且在传输层的安全服务内容有变化时，只要接口不变，应用程序就不必改动。

然而由于传输层很难获取关于每个用户的背景数据，实施时通常假定只有一个用

户使用系统，所以很难满足针对每个用户的安全需求。

具体的传输层安全服务内容取决于具体的协议，而通常每种安全传输协议都需要密钥管理，因此这种过程可能会重复多次。

3. 网络层

网络层安全在端系统和路由器上都可以实现。

在网络层实现安全服务具有多方面的优点。主要优点是透明性，能提供主机对主机的安全服务，因而安全服务的提供不要求传输层和应用层做改动，也不必为每个应用设计自己的安全机制；其次是网络层支持以子网为基础的安全，子网可采用物理分段或逻辑分段，因而可很容易实现 VPN 和内联网，防止对网络资源的非法访问；第三个方面是由于多种传送协议和应用程序可共享由网络层提供的密钥管理架构，密钥协商的开销大大降低。

在网络层提供安全服务的缺点是无法实现针对用户和用户数据语义上的安全控制。

4. 数据链路层

数据链路层能提供的安全服务种类较少，常用的方式是用硬件设备对所有的通信数据进行加密。这样做的最大好处是整个分组（包括分组头信息）都被加密，但由于需要对所有的通信数据进行加密（包括路由数据），因此只有在专用链路上才能很好地工作，而且进行通信的两个实体必须在物理上连接到一起，中间不能有转接点，因此使用范围有限。

这种安全模型的典型应用就是自动柜员机（ATM），所有机器均通过专用线路连接到中心办公室。

1.2.4 安全机制

安全机制是实现安全服务的技术手段，表现为操作系统、软硬件功能部件、管理程序以及它们的任意组合。网络信息系统的安全是一个系统的概念，为了保障整个系统的安全可以采用多种机制。

ISO 7498-2 中定义了 8 类安全机制。

加密机制(encryption)；

数字签名机制(digital signature mechanisms)；

访问控制机制(access control mechanisms)；

数据完整性机制 (data integrity mechanisms)；

鉴别机制(authentication mechanisms)；

通信业务填充机制（traffic padding mechanisms)；

路由控制机制(routing control mechanisms)；

公证机制(notarization mechanisms)

一种安全机制可以提供多种安全服务，而一种安全服务也可采用多种安全机制。安全服务与安全机制之间的关系如表 1.3 所示

表 1.3　安全服务与安全机制的关系

机制/服务	保密性	完整性	鉴别	访问控制	不可否认
加密	Y	Y	Y	—	—
数字签名	—	Y	Y	—	Y
访问控制	—	—	—	Y	—
数据完整性	—	Y	—	—	Y
鉴别	—	—	Y	—	—
业务填充	Y	—	—	—	—
路由控制	Y	—	—	—	—
公证	—	—	—	—	Y

说明："Y"表示可以提供，"—"表示不能提供

其中加密机制有着最广泛的实际应用，并且可以提供最大限度的安全性。其主要应用是防止对保密性、完整性和鉴别的破坏。

这 8 种机制中，除业务填充和路由控制外，其余的 6 种都同密码算法有关，因此说密码算法是网络信息系统安全的核心技术。

1.3　安 全 策 略

上节介绍了安全服务与安全机制，但在实际应用中，到底应该采取什么样的安全机制，提供什么样的安全服务呢？这时需要根据网络信息系统的情况，定义好安全需求，制定相应的安全策略，然后由安全策略来决定采用何种方式和手段来保证网络系统的安全。即首先要清楚自己需要什么，制定恰当的满足需求的策略方案，然后才考虑技术上如何实施。

安全策略是指在一个特定的环境中，为保证提供一定级别的安全保护所必须遵守

的规则。安全策略通常包括两个重要的组成部分。

- 严格的管理：各网络使用机构、企业和单位应根据本单位的具体情况建立相应的信息安全管理办法，加强内部管理，建立审计和跟踪体系，提高整体信息安全意识
- 先进的技术：先进的安全技术是信息安全的根本保障。用户须首先对面临的威胁进行风险评估，根据评估报告和所需的安全保护级别决定其需要的安全服务种类，选择相应的安全机制，然后集成先进的安全技术，最后还要定期升级相关的技术。

具体安全策略如下所述。

1. 采用什么样的安全保障体系

安全是一个相对的概念，相对于不同的网络系统的具体需求不同，而且安全措施的采用无疑是与运行效率相矛盾的，因为它会占用网络系统资源，降低正常服务的运行效率。因此在设计网络系统时，需要根据关键业务的各个方面的实际需要，在安全性和效率 上进行权衡。

2. 确定网络资源的职责划分

根据网络资源的职责确定哪些人允许使用某一设备，如用户如何授权访问，如允许哪些用户使用、允许何时使用、分别允许哪些操作；采用什么样的登录方式（远程和本地登录),授权(或禁止)哪些用户访问哪些系统程序和应用程序,授权(或禁止)访问哪些数据，并制定授权方式和程序。

3. 制定使用规则

包括用户口令的设置规则，应多长时间内更改口令；用户是自身提供备份还是由网络服务提供者提供等，此外如何在保护用户的隐私与网络管理人员为诊断、处理问题而收集用户信息之间进行均衡。

4. 制定日常维护规程

包括如何配置网络系统的安全检测程序，采用什么检测方式、检测手段和检测哪些方面的内容等。

5. 确定在检测到安全问题或系统遭到破坏时应采用什么样的相应措施

如对发生在本局域网内部的安全问题，是否应逐级过滤、隔离；在系统遭到破坏时是否启动自动恢复等。

系统安全性包括数据安全性、通信安全性和信息安全性等等各个环节，是一个整

体，整个系统的安全性等同于其中最薄弱环节的安全性，因此针对系统的特点制定合理的安全策略是很重要的。

1.4 信息系统安全评估标准

实际上，人们经常需要了解一个网络信息系统的安全状况，衡量和评价一个网络信息系统安全性的一个重要准则就是安全评价标准鉴于网络信息系统安全的重要性，各国和相关的国际标准化组织纷纷制定了一系列的评价标准，下面简单地介绍几种主要的标准。

.4.1 美国的彩虹系列(Rainbow Series)

1985 年美国国防部计算机安全中心开发出计算机安全标准：可信任计算机标准评估规则（Trusted Computer Standards Evaluation Criteria Orange Book，TCSEC），即大家通常所说的橘皮书，描述了不同类型的物理安全、操作系统软件的可信度，说明了如何创建不同系统的安全需求等。它是第一个信息安全评估标准，多年来它一直是评估多用户主机和小型操作系统的主要方法。其缺点是由于提出的时间早，以单机为主要考虑对象，以加密为主要手段，对网络系统和数据库的安全需求没有考虑。

后来美国国防部计算机安全中心更名为国家计算机安全中心（National Computer Security Center，NCSC），将计算机安全方面的有关文件汇编成册，形成彩虹系列文集，橘皮书是其中的一份重要文件。

在彩虹系列文集中，共有 3 种形式的文件：标准文件、解释性文件和指导性文件标准文件是其中的核心，如橘皮书，其他文件都是围绕标准文件进行标准要求的解释和安全原则的建议指导。其中红皮书（Trusted Network Interpretation of TCSEC）说明了在网络环境下橘皮书的各项要求。蓝皮书（Vendor Guide of Trusted Product Evaluation）给出了产品评估的要求和基本步骤该标准将安全分为 4 个方面：安全政策、可说明性、安全保障和文档，从以上 4 个方面划分为 7 个安全级别，从低到高依次为 D、C1、C2、B1、B2、B3 和 A 级。其中 A 级意味着绝对可信网络安全，B 级代表完全可信网络安全(B1、B2、B3)，C 级则表明可信网络安全（C1、C2），而 D 级意味着不可信的网络安全。

1. D 级

D 级是最低的安全级别。该级别说明整个系统都是不可信的。对于硬件来说，没