第1章 chapter 1

计算机安全与网络安全概论

在当今信息化的社会中，人们对计算机网络的依赖日益增强，越来越多的信息和重要数据资源出现在网络中。通过网络获取信息的方式已成为当前主要的信息沟通方式之一，这种趋势还在不断地发展。人们在使用 Internet 网获得诸多便利和好处的同时，也受到了来自黑客、计算机病毒的侵袭和威胁，使个人和单位蒙受了巨大的损失，特别是近年来 Internet 规模爆炸式的增长，网络上各种新业务（如电子政务、电子商务、网络银行和网上购物等）的兴起以及各种专用网络（如金融网、金税网和教育网等）的建设，使得如何保障计算机安全及网络安全已成为目前一个亟待解决的问题。因此，计算机安全及网络安全技术成为当前网络技术的重要研究课题和发展方向。

计算机安全及网络安全主要的研究内容如下：

- 计算机环境安全技术。
- 计算机硬件安全技术。
- 计算机软件安全技术。
- 数据备份与信息安全技术。
- 网络平台安全技术。
- 网络通信安全技术。
- 网络操作系统安全技术。
- 防火墙技术。
- 入侵检测与端口扫描技术。
- 计算机病毒与黑客的防范技术。

本书将对上述内容逐步加以介绍。

本章着重介绍计算机网络安全的基础知识，并对计算机网络安全问题的基本内容进行介绍。

1.1 计算机安全与网络安全

1.1.1 信息安全

1. 信息安全的基本概念

在这里，给信息安全下一个定义如下：

国际标准化组织(ISO)对信息安全的定义为：为数据处理系统建立和采取的技术和管理的安全保护，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。

我国安全保护条例对信息安全的定义为：计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施(含网络)的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。

可以把信息安全保密内容分为实体安全、运行安全、数据安全和管理安全4个方面。

计算机信息系统安全的目标是着力于实体安全、运行安全、信息安全和人员安全。安全保护的直接对象是计算机信息系统，实现安全保护的关键因素是人。

信息安全主要涉及到信息传输的安全、信息存储的安全以及对网络传输信息内容的审计3方面。

1) 信息传输安全系统

- 信息传输加密技术。目的是对传输中的数据流加密，以防止通信线路上的窃听、泄漏、篡改和破坏。如果以加密实现的通信层次来区分，加密可以在通信的三个不同层次来实现，即链路加密(位于OSI网络层以下的加密)、结点加密和端到端加密(传输前对文件加密，位于OSI网络层以上的加密)。

一般常用的是链路加密和端到端加密这两种方式。链路加密侧重在通信链路上而不考虑信源和信宿，是对保密信息通过各链路采用不同的加密密钥提供安全保护。链路加密是面向结点的，对于网络高层主体是透明的，它对高层的协议信息(地址、检错及帧头帧尾)都加密，因此数据在传输中是密文，但在中央结点必须解密得到路由信息。端到端加密则指信息由发送端自动加密，并进入TCP/IP数据包封装，然后作为不可阅读和不可识别的数据穿过互联网，当这些信息一旦到达目的地，将自动重组、解密，成为可读数据。端到端加密是面向网络高层主体的，它不对下层协议进行信息加密，协议信息以明文形式传输，用户数据在中央结点不需解密。

- 数据完整性鉴别技术。目前，对于动态传输的信息，许多协议确保信息完整性的方法大多是收错重传、丢弃后续包的办法，但黑客的攻击可以改变信息包内部的内容，所以应采取有效的措施来进行完整性检验控制。
- 报文鉴别。与数据链路层的循环冗余校验(Cyclic Redundancy Check，CRC)控制类似，将报文名字段(或域)使用一定的操作组成一个约束值，称为该报文的完整性检测向量(Integrated Check Vector，ICV)。然后将它与数据封装在一起进行加密，传输过程中由于侵入者不能对报文解密，所以也就不能同时修改数据并计算新的ICV，这样，接收方收到数据后解密并计算ICV，若与明文中的ICV不同，则认为此报文无效。
- 校验和。一个最简单易行的完整性控制方法是使用校验和，计算出该文件的校验和值并与上次计算出的值比较。若相等，说明文件没有改变；若不等，则说明文件可能被未察觉的行为改变了。校验和方式可以查错，但不能保护数据。
- 加密校验和。将文件分成小块，对每一块计算CRC校验值，然后再将这些CRC值加起来作为校验和。只要运用恰当的算法，这种完整性控制机制几乎无法破

解。但这种机制运算量大，并且昂贵，只适用于那些完整性要求保护极高的情况。

- 消息完整性编码(Message Integrity Code，MIC)。使用简单单向散列函数计算消息的摘要，连同信息发送给接收方，接收方重新计算摘要，并进行比较验证信息在传输过程中的完整性。这种散列函数的特点是任何两个不同的输入不可能产生两个相同的输出。因此，一个被修改的文件不可能有同样的散列值。单向散列函数能够在不同的系统中高效实现。
- 防抵赖技术。它包括对源和目的地双方的证明，常用方法是数字签名，数字签名采用一定的数据交换协议，使得通信双方能够满足两个条件，接收方能够鉴别发送方所宣称的身份，发送方事后不能否认他发送过数据这一事实。比如，通信的双方采用公钥体制，发送方使用接收方的公钥和自己的私钥加密的信息，只有接收方凭借自己的私钥和发送方的公钥解密之后才能读懂，而对于接收方的回执也是同样道理。另外实现防抵赖的途径还有通过可信第三方的认证、使用时间戳、采用一个在线的第三方、数字签名与时间戳相结合等。

鉴于为保障数据传输的安全，需采用数据传输加密技术、数据完整性鉴别技术及防抵赖技术。因此为节省投资、简化系统配置、便于管理、使用方便，有必要选取集成的安全保密技术措施及设备。这种设备应能够为大型网络系统的主机或重点服务器提供加密服务，为应用系统提供安全性强的数字签名和自动密钥分配功能，支持多种单向散列函数和校验码算法，以实现对数据完整性的鉴别。

2) 信息存储安全系统

在计算机信息系统中存储的信息主要包括纯粹的数据信息和各种功能文件信息两大类。对纯粹数据信息的安全保护，以数据库信息的保护最为典型。而对各种功能文件的保护，终端安全很重要。

(1) 数据库安全。

对数据库系统所管理的数据和资源提供安全保护，其安全功能如下：

- 物理完整性。即数据能够免于物理方面破坏的问题，如掉电、火灾等。
- 逻辑完整性。能够保持数据库的结构，比如对一个字段的修改不至于影响其他字段。
- 元素完整性。包括在每个元素中的数据是准确的。
- 数据的加密。数据以密文形式存储和传输，需要时再进行解密。
- 用户鉴别。确保每个用户被正确识别，避免非法用户入侵。
- 可获得性。指用户一般可访问数据库和所有授权访问的数据。
- 可审计性。能够追踪到谁访问过数据库。

要实现对数据库的安全保护，一种选择是安全数据库系统，即系统的设计、实现、使用和管理等各个阶段都要遵循一套完整的系统安全策略；二是以现有数据库系统所提供的功能为基础构建安全模型，旨在增强现有数据库系统的安全性。

(2) 终端安全。

主要解决计算机终端信息的安全保护问题，其安全功能如下：

- 基于口令密码算法的身份验证，防止非法使用机器。

- 自主和强制存取控制，防止非法访问文件。
- 多级权限管理，防止越权操作。
- 存储设备安全管理，防止非法软盘复制和硬盘启动。
- 数据和程序代码加密存储，防止信息被窃。
- 预防病毒，防止病毒侵袭。
- 严格的审计跟踪，便于追查责任事故。

3）信息内容审计系统

实时对进出内部网络的信息进行审计，以防止或追查可能的泄密行为。因此，为了满足国家保密法的要求，在某些重要或涉密网络，应该安装使用审计系统。

2. 信息安全的特点

- 相对性。没有绝对的安全，只有相对的安全。其安全程度与面临的安全风险大小、安全防护人力、物力投入多少相关。
- 综合性。信息安全并非一个单纯的技术层面的问题，它还涉及到管理、意识和国家法律等多个层面，因此，信息安全其实是一个综合性的问题，各个环节紧密衔接在一起。
- 产品多样性。防黑客的产品不能用来防病毒，不同强度控制不同风险，不能仅指望靠单一的网络安全产品来做到一劳永逸。
- 动态性。今天安全不等于明天就安全，在前一段时间看来是较为安全的问题随着黑客技术的发展也会暴露出原来未检测到的漏洞，所以需要对黑客行为模式进行不断提炼，在技术上的及时跟进和维护支持非常重要。
- 不易管理性。显然安全保护越好，就越不方便，而我们不能限制网络带来的优势，因此投资、安全和便捷之间需要平衡，通过将不同技术控制手段和管理的结合来实现。
- 黑盒性。信息与网络的不安全性是相对透明的，也就是说，信息安全与网络安全是具有黑盒性的。信息安全与网络安全工具和设备在运行时对用户是不可见的，到底能防多少黑客、系统受多少伤害、是否带来新的不安全因素，包括整个安全体系都是很模糊的，用户不知如何管理，本书将提到的网络安全资源管理平台就可以给管理人员一片感性的天地。

3. 信息安全的三个层面

信息安全是要保证信息的完整性、可用性和保密性。当前，信息安全可以分为 3 个层面：网络安全、系统安全以及信息数据安全。

网络层安全问题的核心在于网络是否得到控制，一旦危险的访问者进入企业网络，后果是不堪设想的。这就要求网络能够对所有来访者进行分析，判断来自这一 IP 地址的数据是否安全，以及是否会对本网络造成危害；同时还要求系统能自动将危险来访拒之门外，并对其进行自动记录，使其无法再次入侵。

系统层面的安全问题，主要是病毒对于网络的威胁。病毒的危害已是人尽皆知了，

它就像是暗藏在网络中的不定时炸弹，系统随时都有可能遭到破坏而导致严重后果甚至造成系统瘫痪。因此企业必须做到实时监测，随时查毒、杀毒，不能有丝毫的懈怠与疏忽。

信息数据是安全问题的关键，要求保证信息传输的完整性、保密性等。这一安全问题所涉及的是使用系统中的资源和数据的用户是否是真正被授权的用户，这就要求系统能够对网络中流通的数据信息进行监测、记录，并对使用该系统信息数据的用户进行身份认证，以保证信息安全。

目前，针对这3个层面而开发出的信息安全产品主要包括杀毒软件、防火墙、安全管理、认证授权和加密等。其中以杀毒软件和防火墙应用最为广泛。

1.1.2 计算机安全

1. 计算机安全的基本概念

1946年，计算机问世的初期，人们关注的是如何提高计算机的计算处理能力、运算速度和存储能力，并没有过多地考虑到计算机安全的问题。以后，随着多用户、多进程计算机的出现，众多用户使用同一台计算机运行不同的进程，由此产生了计算机账户管理和资源分配等需求，因此出现了身份认证和访问控制，开始在操作系统中设置专门的用户口令文件和用户账户文件，并在用户登录时引发身份认证进程。计算机还为不同的用户设置专用目录和公用目录，根据预先分配用户的权限来控制其访问范围。从而引入了计算机安全的概念，20世纪70年代初出现的UNIX操作系统就具备了这样的安全机制。实质上，计算机安全是研究如何预防和检测计算机系统用户的非授权行为。

计算机安全是以信息安全为基础的，也即是以信息的存储、访问、传输的安全为宗旨的安全机制。将在后面的内容中介绍。

2. 计算机安全的基本内容

计算机安全主要分为3大部分：硬件安全、软件安全及数据安全。

硬件安全主要是指计算机及其外围设备的安全，尤其是存储设备的安全显得最为重要。因为在计算机中，诸多的重要数据(比如个人隐私、企业营销信息和国家机密等)，都是存放在存储设备上的，一旦这些存储设备遭到攻击或破坏，后果是不堪设想的。

计算机系统硬件安全有两个含义，其一是保护硬件系统免遭攻击，其二是保护硬件系统免遭破坏。前者指的是如何防止系统遭到攻击，后者指的是对于一旦硬件遭到攻击后，如何恢复原有数据的问题。

软件安全指的是对各种应用软件进行访问权限的设置，没有授权的用户是不能访问该软件的。

数据安全指的是对数据的存储、访问、传输的保密与安全。

数据的存储安全类似于计算机硬件安全，其一是保护数据免遭攻击，其二是保护数据免遭破坏，其三是对数据进行加密。

数据的访问安全指的是对用户设置数据的访问权限，不同权限的用户的访问范围是

不一样的，对于没有权限的用户，是不能随意访问数据的。

数据的传输安全指的是保护数据在传输过程中免遭窃听、窃取、篡改和破坏。

后面将要介绍，计算机安全是以信息安全为基础的，也即是以信息的存储、访问和传输的安全为宗旨的安全机制。

1.1.3 网络安全

1. 网络安全管理的意义

随着人类社会生活对 Internet 需求的日益增长，网络安全逐渐成为 Internet 及各项网络服务和应用进一步发展的关键问题，特别是 1993 年以后 Internet 开始商用，通过 Internet 进行的各种电子商务业务日益增多，加之 Internet/Intranet 技术日趋成熟，很多组织和企业都建立了自己的内部网络并与 Internet 连接。电子商务应用和企业网络中的商业秘密均成为攻击者的目标。

随着 Internet 的发展，网络安全技术也在与网络攻击的对抗中不断发展。从总体上看，经历了从静态到动态、从被动防范到主动防范的发展过程。计算机网络安全是一个非常复杂的问题，安全问题不仅仅是技术方面的问题，它还涉及人的心理、社会环境以及法律等多方面内容。

在计算机网络系统中，多个用户共处在一个大环境中，系统资源是共享的，用户终端可直接访问网络和分布在各用户处理机中的文件、数据和各种软件、硬件资源。随着计算机和网络的普及，政府、军队的核心机密和重要数据、企业的商业机密、甚至是个人的隐私都存储在计算机网络中，不法之徒千方百计的“闯入”和破坏，使有关方面蒙受了巨大的损失。

综上所述，网络安全技术主要用于保证网络环境中各种应用系统和信息资源的安全，防止未经授权的用户非法登录系统，非法访问网络资源，窃取信息或实施破坏。网络系统安全主要侧重于攻击行为和特征的检测和阻断、系统防护和灾难恢复方面的研究。主要技术有防火墙、访问控制、入侵检测、漏洞扫描、身份认证、灾难恢复和安全管理等。

2. 计算机网络安全的有关概念

- 安全与保密。计算机网络安全是指网络系统中用户共享的软、硬件等各种资源是否安全，使其不受到有意无意的破坏，不被非法入侵等。研究计算机网络安全问题必然要涉及到保密问题，但安全与保密却不是等同的两个概念。在研究网络安全问题时，针对非法侵入、盗窃机密等方面的安全问题要用保密技术加以解决。保密是指为维护用户自身利益，对资源加以防止非法侵入和防止盗取，即使非法用户盗取到了资源也识别不了的方法。
- 风险与威胁。风险是指损失的程度，威胁是指对资产构成威胁的人、物、事及想法。其中资产是进行风险分析的核心内容，它是系统必须保护的，网络系统中的资产主要是数据。威胁会利用系统所暴露出的弱点和要害之处对系统进行攻击，威胁包括有意和无意两种。

- 敏感信息。敏感信息是指那些丢失、滥用、被非法授权人访问或修改的信息，是泄露、破坏、不可使用或修改后会对你造成损失的信息。
- 脆弱性。脆弱性是指在系统中安全防护的弱点或缺少用于防止某些威胁的安全防护。脆弱性与威胁是密切相关的。
- 控制。控制是指为降低受破坏可能性所做的努力。

3. 安全管理的基本内容

安全管理包括安全特征的管理和管理信息的安全。

安全特征的管理提供安全的服务，以及安全机制变化的控制，直至物理场地、人员的安全，病毒防范措施操作过程的连续性，灾难事故时恢复措施的计划与实施等内容，管理信息的安全是保障管理信息自身的安全。安全管理提供的主要功能包括：

- 安全告警管理。
- 安全审计跟踪功能管理。
- 安全访问控制管理。

4. 保护网络系统的基本要素

1）安全策略

制定对系统进行有效管理的安全策略。网络系统的安全策略包括下述内容：

- 使用口令登录进行访问控制。
- 制定网络操作系统和用户应用程序的安全控制。
- 对付系统备份、灾难系统和数据恢复的安全机制。
- 网络系统的重要资源(如服务器、路由器、交换机和软件等)的物理安全策略。
- 明确网络安装和维护的软件硬件人员的职责及网络访问级别。
- 在进行网络外部访问时维护网络完整性的策略。

2）防火墙

将非法信息和非法入侵人员挡在“墙外”的一种技术。

在计算机网络系统中，“防火墙”是用来限制和隔离网络用户的某些工作的一种特殊技术，安全系统对外来造访者可以通过防火墙技术来实现安全保护。

防火墙实质上是用“包过滤”技术来实现的，将对内部网络造成威胁或危害的外来“数据包”挡在墙外。

3）记录

将网络运行情况详细记录下来，以便事后进行分析。

系统必须能自动记录网上的每项活动，系统管理员则采取一些特殊手段对这些记录信息进行处理，以便获得所需信息来定位和特征化入侵行为。

4）脆弱性评价

详细分析系统的脆弱性，及时改进。

5）物理保护

物理保护指的是对计算机网络的物理设备和通信介质进行有效的保护。主要防止

搭线窃取网络数据。

6）注册登录

注册登录的限制。

1.2 计算机网络面临的安全问题

1.2.1 网络脆弱性分析

计算机网络尤其是互联网络，由于网络分布的广域性、网络体系结构的开放性、信息资源的共享性和通信信道的共用性，而使计算机网络存在严重的脆弱点。它们是网络安全的隐患。给攻击型的威胁提供了可乘之机，对于网络安全来说，找到和确认这些脆弱点是至关重要的。

1. 网络漏洞

不设防的网络会有成百上千个漏洞和后门。机器设备、计算机硬件和软件、网络系统，甚至有些安全产品本身就存在安全漏洞。

2. 电磁辐射

电子设备工作过程都有电磁辐射产生。电磁辐射在网络中表现出两方面的脆弱性。一方面，电磁辐射能够破坏网络中传输的数据，这种辐射的来源有两个方面，网络周围电子电气设备产生的电磁辐射和试图破坏数据传输而预谋的干扰辐射源；另一方面，网络的终端、打印机或其他电子设备在工作时产生的电磁辐射泄露，即使用不太先进的设备，在近处甚至远处都可以将这些数据，包括在终端屏幕上显示的数据接收下来，并且重新恢复。

3. 线路窃听

无源线路窃听通常是一种没有检测的窃听，它通常是为了获取网络中的信息内容。有源线路窃听是对信息流进行有目的的变形，能够任意改变信息内容，注入伪造信息，删除和重发原来的信息。也可以用于模仿合法用户，或通过干扰阻止和破坏信息传输。

4. 串音干扰

串音的作用是产生传输噪音，噪音能对网络上传输的信号造成严重的破坏。

5. 硬件故障

硬件故障势必造成软件中断和通信中断，带来重大损害。

6. 软件故障

通信网络软件一般用于建立计算机和网络的连接。程序里包含有大量的管理系统

安全的部分，如果这些软件程序受到损害，则该系统就是一个极不安全的系统。

7. 人为因素

系统内部人员的非法活动，如系统操作员、工程技术人员和管理人员盗窃机密数据或破坏系统资源。利用制度不健全或管理不严盗窃存有机密数据的媒体，甚至直接破坏网络系统。

8. 网络规模

网络安全的脆弱性和网络的规模有密切关系。网络规模越大，其安全的脆弱性越大。资源共享与网络安全也是矛盾的，随着网络发展和资源共享增强，安全问题也越突出。

9. 网络物理环境

这种类型脆弱性是属于计算机设备防止自然灾害的领域，比如火灾和洪水。也包括一般的物理环境的保护，像机房的安全门、人员出入机房的规定等。物理环境安全保护的范围不仅包括计算机设备和传输线路，也包括一切可以移动的物品，比如打印数据的打印纸和装有数据和程序的磁盘。

10. 通信系统

通信系统始终是最严重的脆弱性课题。对于一般的通信系统，获得存取权是相对简单的，并且机会总是存在的。一旦信息从生成和存储的设备发送出去，它将给攻击型的威胁提供了巨大的突破口。

1.2.2 网络面临的威胁

网络安全潜在威胁形形色色，有人为和非人为的、恶意的和非恶意的、内部攻击和外部攻击等。对网络安全的威胁主要表现在非授权访问、冒充合法用户、破坏数据完整性、干扰系统正常运行、利用网络传播病毒和线路窃听等方面。安全威胁主要利用以下途径，系统存在的漏洞；系统安全体系的缺陷；使用人员的安全意识薄弱；管理制度的不健全。

安全威胁可分为故意的（如系统入侵）和偶然的（如将信息发到错误地址）两类。故意威胁又可进一步分成被动威胁和主动威胁两类，被动威胁只对信息进行监听和窃取，而不对其修改和破坏；主动威胁则要对信息进行故意篡改和破坏，使合法用户得不到可用信息。网络安全主要有以下几种：

1. 基本的安全威胁

网络安全具备 4 个方面的特征，即机密性、完整性、可用性及可控性。下面的 4 个基本安全威胁直接针对这 4 个安全目标。

- 信息泄露。信息泄露给某个未经授权的实体。这种威胁主要来自窃听、搭线等信

息探测攻击。

- 完整性破坏。数据的一致性由于受到未授权的修改、创建、破坏而损害。
- 拒绝服务。对资源的合法访问被阻断。拒绝服务可能由以下原因造成，攻击者对系统进行大量的、反复的非法访问尝试而造成系统资源过载，无法为合法用户提供服务；系统物理或逻辑上受到破坏而中断服务。
- 非法使用。某一资源被非授权人以授权方式使用。

2. 主要渗入威胁

- 假冒。即某个实体假装成另外一个不同的实体。这个未授权实体以一定的方式使安全守卫者相信它是一个合法实体，从而获得合法实体对资源的访问权限。这是大多数黑客常用的攻击方法。如甲和乙同为网络上的合法用户，网络能为他们服务。丙也想获得这些服务，于是丙向网络发出："我是乙"。
- 篡改。乙给甲发了如下一份报文："请给丁汇 10000 元钱，乙"。报文在转发过程中经过丙，丙把报文改为"请给丙汇 10000 元钱，乙"。结果是丙而不是丁收到了这 10000 元钱。这就是报文篡改。
- 旁路。攻击者通过各种手段发现一些系统安全缺陷，并利用这些安全缺陷绕过系统防线渗入到系统内部。
- 授权侵犯。对某一资源具有一定权限的实体，将此权限用于未被授权的实体，也称"内部威胁"。

3. 主要植入威胁

- 计算机病毒。计算机病毒是一种会"传染"其他计算机程序并具有破坏能力的程序，"传染"是通过修改其他程序来把自身复制进去完成的。比如"特洛伊木马(Trojan horse)"，是一种执行超出程序定义之外的程序，如一个编译程序除了执行编译任务以外，还把用户的源程序偷偷地复制下来，这种编辑程序就是一个特洛伊木马。
- 陷门。在某个系统或某个文件中预先设置"机关"，诱你掉入"陷门"之中，一旦你提供特定的输入时，允许你违反安全策略，将自己机器上的秘密自动传送到对方的计算机上。

典型的安全威胁如表 1-1 所示。

表 1-1 典型的网络安全威胁

威　胁	描　述
授权侵犯	为某一特定目的被授权使用某个系统的人，将该系统用作其他未受权的目的
窃听	在监视通信的过程中获得信息
电磁泄露	从设备发出的辐射中泄露信息
信息泄露	信息泄露给未授权实体

续表

威　胁	描　述
物理入侵	入侵者绕过物理控制而获得对系统的访问权
重放	出于非法目的而重新发送截获的合法通信数据
资源耗尽	某一资源被故意超负荷使用，导致其他用户的服务中断
完整性破坏	对数据的未授权创建、修改或破坏造成一致性损坏
人员疏忽	一个授权人出于某种动机或由于粗心将信息泄露给未授权的人

1.2.3 网络安全的基本技术

网络安全是对付威胁、克服脆弱性及保护网络资源的所有措施的总称，涉及政策、法律、管理、教育和技术等方面的内容。网络安全是一项系统工程，针对来自不同方面的安全威胁，需要采取不同的安全对策。从法律、制度、管理和技术上采取综合措施，以便相互补充，达到较好的安全效果。技术措施是最直接的屏障，目前常用而有效的网络安全技术对策有如下几种：

1. 数据加密技术

加密是所有信息保护技术措施中最古老、最基本的一种手段。加密的主要目的是防止信息的非授权泄漏。加密方法多种多样，在信息网络中一般是利用信息变换规则把可读的信息变成不可读的信息。既可对传输信息加密，也可对存储信息加密，把计算机数据变成一堆乱码数据。现代密码算法不仅可以实现加密，还可以实现数字签名、身份认证和报文完整性鉴别等功能，能有效地对抗截获、非法访问、破坏信息的完整性、冒充、抵赖和重放等威胁，因此，密码技术是信息网络安全的核心技术。

2. 数字签名技术

数字签名机制提供了一种鉴别方法，以解决伪造、抵赖、冒充和篡改等安全问题。数字签名采用一种数据交换协议，使得数据的收发双方能够满足三个条件，接受方能够鉴别发送方所宣称的身份；发送方事后不能否认他发送过数据这一事实；接收方事后不能伪造数字签名。数据签名一般采用非对称加密技术，发送方对整个明文进行加密变换，得到一个值，将其作为签名。接收者使用发送者的公开密钥对签名进行解密运算，如其结果为对方身份，则签名有效，证明对方身份是真实的。

3. 鉴别技术

鉴别的目的是验明用户或信息的正身。对实体声称的身份进行唯一地识别，以便验证其访问请求或保证信息来自或到达指定的源和目的。鉴别技术可以验证消息的完整性，有效地对抗冒充、非法访问、重放等威胁。按照鉴别对象的不同，鉴别技术可以分为消息源鉴别和通信双方相互鉴别；按照鉴别内容的不同，鉴别技术可以分为用户身份鉴

别和消息内容鉴别。鉴别的方法很多，利用鉴别码验证消息的完整性；利用通行字、密钥、访问控制机制等鉴别用户身份，防止冒充、非法访问。当今最佳的鉴别方法是数字签名，利用单方数字签名，可实现消息源鉴别、访问身份鉴别、消息完整性鉴别。利用收发双方数字签名，可同时实现收发双方身份鉴别、消息完整性鉴别。

4. 访问控制技术

访问控制的目的是防止非法访问。访问控制是采取各种措施保证系统资源不被非法访问和使用。一般采用基于资源的集中式控制、基于源和目的地址的过滤管理以及网络签证技术等技术来实现。

5. 安全审计技术

计算机安全审计是通过一定的策略，利用记录和分析历史操作事件发现系统的漏洞并改进系统的性能和安全。

6. 防火墙技术

防火墙技术是建立在现代通信网络技术和信息安全技术基础上的应用性安全技术，越来越多地应用于专用网络与公用网络的互连环境中。在大型网络系统与因特网互连的第一道屏障就是防火墙。防火墙通过控制和监测网络之间的信息交换和访问行为来实现对网络安全的有效管理，其基本功能为过滤进、出网络的数据；管理进、出网络的访问行为；封堵某些禁止行为；记录通过防火墙的信息内容和活动；对网络攻击进行检测和告警。

7. 入侵检测技术

网络入侵检测技术也叫网络实时监控技术，它通过硬件或软件对网络上的数据流进行实时检查，并与系统中的入侵特征数据库进行比较，一旦发现有被攻击的迹象，立刻根据用户所定义的动作做出反应，如切断网络连接，或通知防火墙系统对访问控制策略进行调整，将入侵的数据包过滤掉等。

通过入侵检测技术，可监视登录到系统用户的一切行为，当用户试图对系统造成安全威胁时，自动发出报警或切断网络。

8. 端口扫描技术

网络安全扫描技术是为使系统管理员能够及时了解系统中存在的安全漏洞，并采取相应防范措施，从而降低系统的安全风险而发展起来的一种安全技术。利用安全扫描技术，可以对局域网络、Web 站点、主机操作系统、系统服务以及防火墙系统的安全漏洞进行扫描，系统管理员可以了解在运行的网络系统中存在不安全的网络服务，在操作系统上存在可能导致遭受缓冲区溢出攻击或者拒绝服务攻击的安全漏洞，还可以检测主机系统中是否被安装了窃听程序，防火墙系统是否存在安全漏洞和配置错误等。

9. 网络嗅探技术

网络嗅探是利用计算机的网络接口截获目的地及其他计算机数据报文的一种技术。它工作在网络的最底层，把网络传输的全部数据记录下来。以帮助网络管理员查找网络漏洞和检测网络性能，还可以分析网络的流量，以便找出所关心的网络中潜在的问题。

10. 病毒诊断与防治技术

病毒对计算机及网络造成的威胁是极大的，一个安全的计算机网络系统，必须要有强大的病毒诊断能力和防范措施。

11. 黑客防范技术

“黑客”就是非法入侵者，他对计算机网络的威胁也是不可估量的。黑客的防范技术有防火墙技术、口令保护技术、“堡垒主机”技术和“蜜罐”技术。

1.2.4 网络安全的基本功能

一个安全的计算机网络系统，通常是由下列功能组成的。

1. 身份识别

身份识别是安全系统应具备的最基本功能。这是验证通信双方身份的有效手段。用户向其系统服务时，要出示自己的身份证明。例如在进入一个系统或进程时，需要提交 User ID(用户名)和 Password(口令)。系统应具备检查用户身份的能力，对于用户的输入，能够明确判别该输入是否来自合法用户。

2. 存取权限控制

存取权限的基本任务是，防止非法用户进入系统及防止合法用户对资源的非法使用。在开放系统中，网上资源的使用应制定一些规定：一是定义哪些用户可以访问哪些资源；二是定义可以访问的用户各自具备的读、写操作等权限。

3. 保护数据完整性

主要通过消息摘要算法保护数据的完整性。

4. 审计追踪

通过系统日志记录的数据，对一些关键数据进行统计分析，当系统出现安全问题时能够追查原因。

5. 密钥管理

密钥安全管理有两方面的含义：一是对密钥的产生、存储、传送和定期更换进行有效地控制并引入密钥管理机制；二是对密钥进行加密，即是要求密钥必须经加密处理后方

能允许通过公共网络(如 Internet)进行传播。

1.3 系统安全策略

在规划和建设一个网络之前,必须要明确哪些资源、服务类型需要保护,并要求明确其保护的重要程度和防护对象,这就是所谓的安全策略。安全策略是由一组规则组成的,是对系统中所有与安全相关元素的活动做出的一些限制。

由于系统安全是由信息安全、计算机安全和网络安全组成的,在本节中,将依次介绍这 3 个方面的安全策略,其中重点是网络安全策略。

1.3.1 信息安全策略

1. 信息安全策略的定义

信息安全策略是一组规则,它们定义了一个组织要实现的安全目标和实现这些安全目标的途径。信息安全策略可以划分为两个部分,问题策略(issue policy)和功能策略(functional policy)。问题策略描述了一个组织所关心的安全领域和对这些领域内安全问题的基本态度。功能策略描述如何解决所关心的问题,包括制定具体的硬件和软件配置规格说明、使用策略以及雇员行为策略。信息安全策略必须有清晰和完全的文档描述,必须有相应的措施保证信息安全策略得到强制执行。在组织内部,必须有行政措施保证既定的信息安全策略被不打折扣地执行,管理层不能允许任何违反组织信息安全策略的行为存在,另一方面,也需要根据业务情况的变化不断地修改和补充信息安全策略。

2. 信息安全策略框架

信息安全策略框架包括以下内容:

- 加密策略。描述组织对数据加密的安全要求。
- 使用策略。描述设备使用、计算机服务使用和雇员安全规定、以保护组织的信息和资源安全。
- 线路连接策略。描述诸如传真发送和接收、模拟线路与计算机连接、拨号连接等安全要求。
- 反病毒策略。给出有效减少计算机病毒对组织威胁的一些指导方针,明确在哪些环节必须进行病毒检测。
- 应用服务策略。定义应用服务提供者必须遵守的安全方针。
- 审计策略。描述信息审计要求,包括审计小组的组成、权限、事故调查、安全风险估计、信息安全策略符合程度评价、对用户和系统活动进行监控等活动的要求。
- 电子邮件使用策略。描述内部和外部电子邮件接收、传递的安全要求。
- 数据库策略。描述存储、检索和更新等管理数据库数据的安全要求。
- 非军事区域策略。定义位于“非军事区域”(demilitarized zone)的设备和网络分区。

- 第三方的连接策略。定义第三方接入的安全要求。
- 敏感信息策略。对于组织的机密信息进行分级，按照它们的敏感度描述安全要求。
- 内部策略。描述对组织内部的各种活动安全要求，使组织的产品服务和利益受到充分保护。
- Internet 接入策略。定义在组织防火墙之外的设备和操作的安全要求。
- 口令防护策略。定义创建，保护和改变口令的要求。
- 远程访问策略。定义从外部主机或者网络连接到组织的网络进行外部访问的安全要求。
- 路由器安全策略。定义组织内部路由器和交换机的安全配置。
- 服务器安全策略。定义组织内部服务器的安全配置。
- VPN 安全策略。定义通过 VPN 接入的安全要求。
- 无线通信策略。定义无线系统接入的安全要求。

1.3.2 计算机安全策略

计算机安全策略主要研究的是如何预防和检测计算机系统用户的非授权行为。换句话说，计算机安全是关于对信息和资源的控制访问。

1. 计算机安全的结构

一个完整的计算机系统是由计算机硬件、软件、应用程序、资源（主体）和用户（客体）组成的。在这里，将用二维空间结构图来描述计算机安全的结构，如图 1-1 所示。

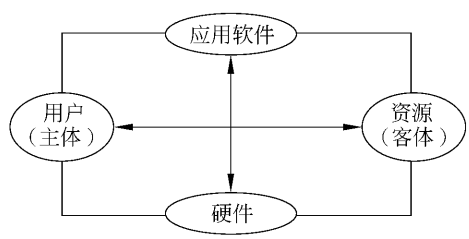

图 1-1 计算机安全结构图

在图 1-1 中，横轴代表安全策略的重点，纵轴代表具有保护机制的计算机系统层次。

2. 控制重点

计算机安全的重点是保证数据的完整性策略，可以用下列规则进行描述。

- 数据项的格式和内容。比如，一条规则可以规定账目数据库中的余额域必须包括一个整数（典型的实例是，银行活期存款中规定一张存折的余额不能小于 1 元）。这个规则并不依赖于访问数据项的用户或者作用在数据项上的操作。
- 规定作用在一个数据项上所有可能的操作。比如，一条规则可以规定只有开户、查询余额、取款和存款操作，可以访问账目数据库中的余额项，并且只有银行工作人员允许执行“开户”操作。
- 规定访问一个数据项的用户。比如，一条规则可以规定只有账户的持有者和银行工作人员才可以访问账目数据库。

由此可以得到一个结论，计算机系统的安全保护策略是保护计算机操作系统和数据的安全。

3. 计算机系统的保护机制

一个完整的计算机系统应由硬件、操作系统、服务、应用程序和外围环境组成。可以将其保护机制想象成一个个同心圆，如图 1-2 所示。

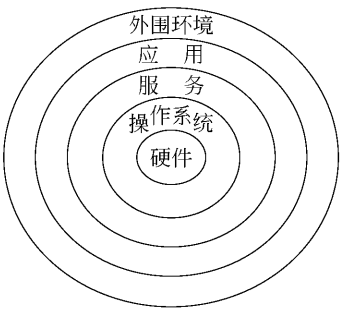

图 1-2 计算机系统的保护机制

从图 1-2 可看出，计算机系统的保护是分层次的，比如，硬件级的安全保护只涉及到硬件的保护，而涉及不到操作系统的保护，反过来说，操作系统层次的保护既能保护操作系统层次，又能保护硬件层次，然而，操作系统层次的保护也涉及不到服务层及应用层的保护。从而可以得到一个结论，硬件级的保护级别最低，而应用层的保护级别最高，也就是说，当考虑应用层的保护时，除了要考虑保护应用层以外，还要考虑服务层、操作系统层及硬件层的保护。另外，恶劣的外围环境（如电压不稳定、电磁干扰严重、机房潮湿、机房有火灾隐患等）会导致数据的损坏、各种服务不能正常工作，甚至造成硬件损坏，因此，外围环境也是计算机系统安全保护最重要的内容。

4. 集中式控制与分布式控制

计算机系统的安全策略可分为集中式控制和分布式控制两种，所谓集中式控制，就是将计算机系统所有安全问题都集中在一个被称为中央实体的控制中心进行，而分布式控制则是将系统安全分别托付给系统中的各个成员或部分成员。

集中式控制的优点是便于安全监测和管理，缺点是控制中心容易造成瓶颈。鉴此，在实际应用中通常使用的是分布式控制策略，它能有效地解决瓶颈问题，但值得注意的是，系统中不同成员之间的策略一致性问题。

1.3.3 网络安全策略

网络安全策略的目的是决定一个计算机网络组织机构如何保护企业内部网络及其信息，其策略通常包括两部分内容，总体策略和具体的规则。总体策略用于阐明安全策略的总体思想，而具体的规则用于说明什么是被允许的，什么是被禁止的。

1. 网络安全策略的等级

通常将网络安全策略划分成如下 4 个等级：

- 一切都是禁止的。
- 一切未被允许的都是禁止的。
- 一切未被禁止的都是允许的。
- 一切都是允许的。

第 1 种策略是最高保护策略，其实现方法是切断内部网络与外部网络的联系。这种策略能有效地防止内部网络遭受外来的攻击，但也把内部网络与外界隔绝，不能与外界

沟通和信息交流，在通常情况下是一种不可取的策略。

第2种策略是开放（允许）部分有限的资源，而对于未明确开放的资源，是禁止访问的。

第3种策略是禁止部分资源的访问，而对于未明确禁止的资源，是允许访问的。

第4种是没有安全保护的策略，其实现手段是把内部网络的全部资源完全对外开放，不加任何保护。这种策略通常也是不可取的。

2. 网络安全策略的内容

一个实用的网络安全策略包括下述内容：

- 网络管理员的安全策略。该策略要求在每台主机上使用专门的安全措施，登录用户名称，监测和记录过程等，还可以限制在网络连接中所有的主机不能运行应用程序。
- 网络用户的安全策略。该策略要求用户每隔一段时间必须改变其用户操作口令；口令必须符合安全标准形式；并定时或不定时进行检测，以了解其账户是否被别人访问过。
- 网络资源的安全策略。该策略明确规定哪些人可以访问网络资源，并规定哪些资源是可以访问的，哪些资源是禁止访问的。
- 安全检测策略。该策略主要用于当检测出安全问题时的应急处理措施。

3. 网络安全机制

网络安全机制有身份认证机制、授权机制、访问控制机制、数据加密机制、数据完整性机制、数字签名机制、报文鉴别机制、路由控制机制和业务流填充机制等。

比如“授权机制”是针对不同用户授以不同的资源访问权限的一种安全访问机制。其具体内容如下：

- 一致性。对资源的控制没有二义性，各种定义之间不能相互冲突。
- 统一性。对所有资源要求集中进行管理，安全策略必须统一。
- 审计功能。对所有授权用户都能进行审计跟踪检查。

习 题 1

1. 信息安全保密的内容是什么？
2. 信息安全内容有哪几个方面？
3. 信息安全的特点是什么？
4. 计算机的安全机制是什么？
5. 安全管理的主要功能是什么？
6. 网络安全的主要技术有哪些？
7. 网络安全策略有哪些等级？
8. 网络安全策略的内容是什么？

第2章 chapter 2

计算机环境安全技术

2.1 环境安全概述

计算机周边环境的好坏直接影响计算机及其外围设备的性能及工作，也直接涉及网络设施的安全，因此，要保护计算机及网络的安全，环境的安全是至关重要的。

计算机环境安全的内容有计算机机房场地、温度、湿度、洁净度、静电、电磁干扰、采光照明和噪声等的安全技术，本章将逐步加以介绍。

2.1.1 计算机机房安全

1. 计算机机房安全的内容

- 计算机机房的设备防护。火灾及防护措施、机房的防水、机房的防物理、化学、生物灾害、硬件防盗。
- 计算机机房安全供电系统。供电故障对计算机系统的影响、电源故障类型、供电系统的技术要求、计算机系统供配电技术、电源安全要点。
- 计算机机房安全接地系统。计算机机房的接地种类及其作用、计算机机房的接地系统、计算机接地装置的安装要求、接地工艺、接地电阻的测量。

2. 机房位置

计算机设备应该有足够的摆放空间，可以放置在任何一层楼，但由于一楼太潮湿、顶楼易漏雨并易遭受雷击，所以，机房不宜设在一楼和顶楼。

计算机设备应该被安放在拥有坚固结构的楼层，具有多重安全出口，并且拥有冗余电力供应。

环境安全结构策略还要考虑到的是冗余电力供应的可行性。冗余电力供应包括为设备提供电力的电力公司、不间断电源 UPS 以及一切与之相关的事项。策略必须反映出物理和经济现实，同时也要考虑到对保护业务运作的必要条件。

3. 锁和防护设施

如果要确保信息被存放在安全的房间里面，就不能不考虑门和其他防护设施。破旧

的门可能会成为物理安全程序中的脆弱之处。

防火门和防火设施可以防止或减少损失，它们可以防止外面的火势蔓延到屋内，也可以防止屋里的火冲到屋外，火可能在扩散之前就熄灭了。这些门应该是密封的，甚至可以考虑用自动关闭功能的门，这样可以更有效地防火。关于这些门的策略不仅要考虑到它们的用途，还要注意这些门不能长期保持打开状态。

4. 环境支持

环境的每一个方面都可以有对应的策略。知道如何控制静电，保持适当的湿度、温度和空气质量。

2.1.2 环境保护机制

在制订环境保护策略前，应首先对一些环境或措施有所了解，然后针对自身的情况，对相关的策略做出一个正确的定位。环境保护涉及到的主要机制和措施由空调系统、防静电和防火等方面构成，下面将作详细的介绍。

放置服务器的区域应该有足够的环境控制系统，包括温度和湿度控制以及防止静电的有效措施。

1. 温度

计算机系统内有许多元器件，不仅散热量大而且对高温、低温非常敏感。环境温度过高容易引起硬件损坏，温度太低时，有些设备工作不正常或无法正常启动。机房温度一般应控制在冬季(20±2)℃、夏季(23±2)℃，温度变化率≤5℃/h。

2. 湿度

机房内相对湿度过高会使电气部分绝缘性降低，金属锈蚀加快；而相对湿度过低会引起静电的积聚，使计算机内信息丢失、损坏芯片，使外部设备工作不正常等。机房内的相对湿度一般控制在(50±5)%。湿度控制与温度控制都应与空调联系在一起，由空调系统集中控制。机房内应安装温、湿度显示仪，随时观察、监测。

3. 粉尘

计算机及其外部设备是精密的设备，磁头的缝隙、磁头与磁盘之间读写时的间隙都非常小，一粒小小的尘埃相对这个间隙就像是一座大山，它会影响寻道的准确性，甚至划伤磁盘，严重地影响计算机系统的正常工作。因此，机房必须采取一定的除尘、防尘措施，以保证设备稳定地工作。

机房内一般应采用乙烯类材料装修，避免使用挂毯、地毯等吸尘材料。人员进出门应有隔离间，并应安装吹尘、吸尘设备，排除进入人员所带的灰尘。空调系统进风口应安装空气滤清器，并应定期清洁和更换过滤材料，以防灰尘进入。同时进风压力要大，房间要密封，使室内空气压力高于室外，这样灰尘不会进入室内。

房内的尘埃要求低于0.5nm；对于开机时机房内的噪音，在中央控制台处测量时应

小于 70dB。

4. 其他

洁净度。要求符合标准 Ashrae 52～76，空气中大于 0.5nm 的尘粒每立方米应少于 10 000 粒。

噪声。关闭主设备的条件下，在工作人员正常办公位置处测量不高于 68dB。

机房单位面积的冷负荷为 257W/(m^2h)。

系统控制室单位时间换气数≥23 次/h。

数据中心机房单位时间换气数≥22 次/h。

2.2 环境安全保护

2.2.1 空调系统

计算机房内空调系统是保证计算机系统正常运行的重要设备之一。通过空调系统使机房的温度、湿度和洁净度得到保证，从而使系统能正常工作。重要的计算机系统安放处应有单独的空调系统，计算机房的空调较一般的空调有更苛刻的要求。它应具有供风、加热、冷却、减湿和空气除尘的能力。

空调系统的送风量应取下列 3 种数据中的最大值。

- 室内总送风量的 5%。
- 按工作人员每人 40m^3/h。
- 维持室内正压所需风量。

主机房的空调送风系统，应设初效、中效两级空气过滤器，中效空气过滤器计数效率应大于 80%，末级过滤装置宜设在正压端或送风口。

主机房在冬季需送冷风时，可取室外新风作冷风源。

计算机机房空气调节控制装置应满足计算机系统对温度、湿度以及粉尘对正压的要求。

空调设备的选择如下：

- 空调设备的选用应符合运行可靠、经济和节能的原则。
- 空调系统应设消声装置。
- 空调系统和设备选择应根据计算机类型、机房面积、发热量及对温、湿度和空气含尘浓度的要求综合考虑。
- 空调冷冻设备宜采用带风冷冷凝器的空调机。当采用水冷机组时，对冷却水系统冬季应采取防冻措施。
- 空调和制冷设备宜选用高效、低噪声、低振动的设备。
- 空调制冷设备的制冷能力，应留有 15%～20%的余量。
- 当计算机系统需长期连续运行时，空调系统应有备用装置。