第 1 章　网络安全概述

本章简要介绍了计算机网络安全的基本概念，并阐述了网络安全从通信安全到信息安全再发展为信息安全保障的历程。作为网络安全的设计方法，掌握本章所阐述的几大安全原则并将其运用到后面章节的各种具体的技术设计中，将对网络安全的设计具有重要意义。

通过本章的学习，读者应掌握以下内容:

- 理解网络安全的基本概念和术语
- 了解目前主要的网络安全问题和安全威胁
- 了解网络和信息安全的重要性
- 了解国内外的信息安全保障体系

1.1　网络安全的基本概念

在互联网上最著名的搜索引擎中搜索“网络安全”这个词，共查到 80,000,000 余条记录，搜索“Net Safe”这个词，共查到 1,300,000,000 余条记录，而搜索“电视”这个词，共查到 100,000,000 余条记录。由此可见，网络安全随着互联网的发展，正逐渐成为人们生活中密不可分的一部分，而且越来越重要。

1.1.1　网络安全的定义及相关术语

1. 网络安全的定义

在解释网络安全这个术语之前，首先要明确计算机网络的定义，计算机网络是地理上分散的多台自主计算机互联的集合，这些计算机遵循约定的通信协议，使用通信设备、通信介质及网络软件共同实现信息交换、资源共享等功能。

所以，从广义上说，网络安全包括网络硬件资源及信息资源的安全性。硬件资源包括通信线路、通信设备（交换机、路由器等）、主机等，要实现信息快速、安全的交换，一个可靠的物理网络是必不可少的。信息资源包括维持网络服务运行的系统软件和应用软件，以及在网络中存储和传输的用户信息数据等。信息资源的保密性、完整性、可用性、真实性等是网络安全研究的重要课题，也是本书涉及的重点内容。

从用户角度看，网络安全主要是保障个人数据或企业的信息在网络中的保密性、完整性、不可否认性，防止信息的泄露和破坏，防止信息资源的非授权访问。对于网络管理者来说，网

络安全的主要任务是保障合法用户正常使用网络资源，避免病毒、拒绝服务、远程控制、非授权访问等安全威胁，及时发现安全漏洞，制止攻击行为等。从教育和意识形态方面，网络安全主要是保障信息内容的合法与健康，控制含不良内容的信息在网络中的传播。

可见网络安全的内容是十分广泛的，不同的人群对其有不同的理解。在此对网络安全下一个通用的定义：网络安全是指保护网络系统中的软件、硬件及信息资源，使之免受偶然或恶意的破坏、篡改和泄露，保证网络系统的正常运行、网络服务不中断。

2. 网络安全的属性

在美国国家信息基础设施（NII）的文献中，给出了网络安全的 5 个属性：可用性、机密性、完整性、可控性和可审查性。这 5 个属性适用于国家信息基础设施的各个领域，如教育、娱乐、医疗、运输、国家安全、通信等。

- 保密性：信息不泄露给非授权用户、实体或过程，或供其利用的特性。
- 完整性：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修改、不被破坏和丢失的特性。
- 可用性：可被授权实体访问并按需求使用的特性，即当需要时能否存取所需的信息。例如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。
- 可控性：对信息的传播及内容具有控制能力。
- 可审查性：出现安全问题时提供依据与手段。

1.1.2 网络安全现状

近年来，随着网络安全事件的频频发生，人们对外部入侵和互联网的安全日益重视，但来自内部网络的攻击却越演越烈，内网安全已成为企业管理的隐患。信息资料被非法泄露、复制、篡改，往往给各行业企事业单位造成重大损失。而如何使内部网络始终处于安全、可靠、保密的环境之下运行，帮助企业各类业务统一优化、规范管理，保障各类业务正常安全运行等一系列的问题困扰着各行业企、事业单位的 IT 部门。

1. 资产管理失控

在现代化大型企业中，拥有数以百计的客户端等 IT 资产是常见的事情。由于客户端分布分散，资产统计与维护十分困难。另外，企业为员工提供的软硬件资产是要求员工在工作的环境下，为企业创造价值，可是很多员工却把这些资产滥用，甚至挪为私用，管理不善的笔记本、CPU、内存，甚至网卡、主板、硬盘等都被使用者更换掉，导致不必要的信息数据泄露。

2. 外接设备滥用

市场战略规划、产品价格体系、自主研发的核心技术等商业机密成为企业目前关注的重点。如何保证企业数据信息的安全性，降低安全风险，这些问题亟待解决。同时公司的软驱、光驱、USB、并口、串口等各种外部存储设备滥用带来的一系列信息安全隐患，增加商业机密外泄机率，如何对网内计算机各种外接设备进行控制，并防止利用移动存储设备进行数据文件的拷贝？

3. 补丁管理混乱

每隔一段时间微软发布修复系统漏洞的更新版本，但很多终端用户不了解系统补丁状态，不能及时使用这些更新修复系统（打补丁）。网络规模越来越庞大，网络管理员要保证每台终端及时、全面地安装响应更新，统一进行补丁的下载、分析、测试和分发，工作量很大且很难实现，从而为蠕虫与黑客入侵保留了通道。

4. 病毒蠕虫入侵

由于补丁更新不及时，网络滥用、移动设备（如笔记本电脑）和新增设备未经过安全检查和处理非法接入等因素导致内网病毒泛滥、黑客入侵、网络阻塞、数据损坏丢失等不安全因素，而且无法找到灾难的源头以迅速采取隔离等处理措施，给我们的内网安全带来了巨大的隐患，从而为正常业务带来灾难性的持续影响。

5. 违规上网行为

“水能载舟亦能覆舟”，互联网在帮助企业提高生产力、促进企业发展，并为人们的生活与工作带来便捷性的同时也带来很多安全隐患;而企业内部却存有各种与工作无关的非许可性上网行为现象，如泡论坛、写博客、在线聊天、发私人邮件，甚至长时间访问非法网站等已经司空见惯，然而信息的机密性、健康性、政治性等问题也随之而来。

6. 网络流量异常

P2P 下载、看电影、玩游戏、炒股票以及访问如色情、赌博等具有高度安全风险的网页，企业员工于互联网上的应用可谓五花八门，如果员工长期沉迷于这些应用，在成为企业生产效率的巨大杀手的同时，都在抢占着有限的带宽资源，并可能造成网速缓慢、信息外泄的可能。面对日益紧张的带宽资源，若无法了解客户端流量应用信息，一旦发生流量异常，IT 运维人员无法及时了解流量异常情况。

7. IP 地址随意更改

企业网络中由于用户原因造成使用管理混乱；网管人员无法知道 IP 地址的使用、IP 同 MAC 地址的绑定情况及网络中 IP 分配情况；没有严格的管理策略，员工随意设置 IP 地址，可能造成 IP 地址冲突、关键设备发生异常。若出现恶意盗用、冒用 IP 地址以谋求非法利益，后果将更为严重。如何防止单位内部员工私自更改个人计算机的 IP 地址和 MAC 地址上网，导致与其他员工的 IP 冲突，从而保证企业员工的正常办公。

8. 安全设备成摆设

为了保障企业网络安全，“堵漏洞、砌高墙、防外攻、防内贼，防不胜防”，防火墙越“砌”越“高”，入侵检测越做越复杂，病毒库越来越庞大，身份系统层层设保，却依然无法应对层出不穷网络安全威胁，难道那么多安全产品都是摆设？企业已有如防火墙、IDS 入侵检测系统、防病毒系统、网闸、加密系统等各种安全设备，但是各自为政，无法协同工作，导致单独系统的信息孤岛。如何真正地保障业务系统的安全，并将各种安全设备进行综合管理。

1.2　主要的网络安全威胁

由于计算机信息系统已经成为信息社会另一种形式的“金库”和“保密室”，成为一些人窥视的目标；再者，由于计算机信息系统自身所固有的脆弱性，使计算机信息系统面临威胁和攻击的考验，而计算机信息系统的安全主要体现在计算机网络的安全上，保护网络安全的最终目的就是保护计算机信息系统的安全。计算机网络的安全同时来自内、外两个方面。

1.2.1　外部威胁

1. 自然灾害

计算机网络是一个由用传输介质连接起来的地理位置不同的计算机组成的“网”，易受火灾、水灾、风暴、地震等破坏及环境（温度、湿度、振动、冲击、污染）的影响。目前，不少

计算机机房并没有防震、防火、防水、避雷、防电磁泄漏或干扰等措施，接地系统也疏于周到考虑，抵御自然灾害和意外事故的能力较差。日常工作中因断电使设备损坏、数据丢失的现象时有发生。

灾害轻则造成业务工作混乱，重则造成系统中断，甚至造成无法估量的损失。例如，1999年8月吉林省某电信业务部门的通信设备被雷击中，造成惊人的损失；还有某铁路计算机系统遭受雷击，造成设备损坏、铁路运输中断等。

2. 黑客

计算机信息网络上的黑客攻击事件愈演愈烈，已经成为具有一定经济条件和技术专长的形形色色攻击者活动的舞台。黑客破坏了信息网络的正常使用状态，造成可怕的系统破坏和巨大的经济损失。

3. 计算机病毒

计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能、毁坏数据、影响计算机使用并能自我复制的一组计算机指令或者程序代码。

“计算机病毒”将自己附在其他程序上，在这些程序运行时进入到网络系统中进行扩散。一台计算机感染上病毒后，轻则系统工作效率下降，使部分文件丢失，重则造成系统死机或毁坏，使全部数据丢失。1999年4月26日，CIH病毒在全球造成的危害足以显露计算机病毒的可怕。

据一份市场调查报告表明，我国约有 90%的网络用户曾遭到过病毒的侵袭，并且其中大部分因此受到损失。病毒危害的泛滥说明了计算机系统和人们在安全意识方面的薄弱。

4. 垃圾邮件和黄毒泛滥

一些人利用电子邮件地址的“公开性”和系统的“可广播性”进行商业、宗教、政治等活动，把自己的电子邮件强行“推入”别人的电子邮箱，甚至塞满别人的电子邮箱，强迫别人接收他们的垃圾邮件。

国际互联网的广域性和自身的多媒体功能也给黄毒的泛滥提供了可乘之机。

5. 经济和商业间谍

通过信息网络获取经济、商业情报和信息的威胁大大增加。大量的国家和社团组织上网，在丰富网上内容的同时，也为外国情报收集者提供了捷径，通过访问公告牌、网页及内部电子邮箱，利用信息网络的高速信息处理能力，进行信息分析以获取情报。

6. 电子商务和电子支付的安全隐患

计算机信息网络的电子商务和电子支付的应用给人们展现了美好前景，但网上安全措施和手段的缺乏阻碍了它的快速发展。

7. 信息战的严重威胁

所谓信息战，就是为了国家的军事战略而采取行动，取得信息优势，干扰敌方的信息和信息系统，同时保卫自己的信息和信息系统。这种对抗形式的目标不是集中打击敌方的人员或战斗技术装备，而是打击敌方的计算机信息系统，使其神经中枢似的指挥系统瘫痪。

信息技术从根本上改变了进行战争的方法，信息武器已成为继原子武器、生物武器、化学武器之后的第四类战略武器。

在海湾战争中，信息武器首次进入实战。伊拉克的指挥系统吃尽了美国的苦头：购买的智能打印机被塞进了一片带有病毒的集成电路芯片，加上其他因素，最终导致系统崩溃，指挥失灵，几十万伊军被几万联合国维和部队俘虏。美国的维和部队还利用国际卫星的全球计算机

网络，为其建立军事目的的全球数据电视系统服务。所以，未来国与国之间的对抗首先来自信息技术的较量。网络信息安全应该成为国家安全的前提。

8. 计算机犯罪

计算机犯罪是利用暴力和非暴力形式，故意泄漏或破坏系统中的机密信息，以及危害系统实体和信息安全的不法行为。《中华人民共和国刑法》对计算机犯罪做了明确定义，即利用计算机技术知识进行犯罪活动，并将计算机信息系统作为犯罪对象。

利用计算机犯罪的人通常利用窃取口令等手段，非法侵入计算机信息系统，利用计算机传播反动和色情等有害信息，或实施贪污、盗窃、诈骗和金融犯罪等活动，甚至恶意破坏计算机系统。

1.2.2　内部威胁

由于计算机信息网络是一个“人机系统”，所以内部威胁主要来自使用的信息网络系统的脆弱性和使用该系统的人。外部的各种威胁因素和形形色色的进攻手段之所以起作用，是由于计算机系统本身存在着脆弱性，抵御攻击的能力很弱，自身的一些缺陷常常容易被非授权用户不断利用，外因通过内因起变化。

（1）软件工程的复杂性和多样性使得软件产品不可避免地存在各种漏洞。世界上没有一家软件公司能够做到其开发的产品设计完全正确，而且没有缺陷，这些缺陷正是计算机病毒蔓延和黑客“随心所欲”的温床。

（2）电磁辐射也可能泄漏有用信息。已有试验表明，在一定的距离以内接收计算机因地线、电源线、信号线或计算机终端辐射导致的电磁泄漏产生的电磁信号，可复原正在处理的机密或敏感信息，如“黑客”们利用电磁泄漏或搭线窃听等方式可截获机密信息，或通过对信息流向、流量、通信频率和波段等参数的分析，推断出有用信息，如用户口令、账号等重要信息。

（3）网络环境下电子数据的可访问性对信息的潜在威胁比对传统信息的潜在威胁大得多。

非网络环境下，任何一个想要窃密的人都必须先解决潜入秘密区域的难题；而在网络环境下，这个难题已不复存在，只要有足够的技术能力和耐心即可。

（4）不安全的网络通信信道和通信协议。信息网络自身的运行机制是一种开放性的协议机制。网络节点之间的通信是按照固定的机制，通过协议数据单元来完成的，以保证信息流按“包”或“帧”的形式无差错地传输。那么，只要所传的信息格式符合协议所规定的协议数据单元格式，那么，这些信息“包”或“帧”就可以在网上自由通行。至于这些协议数据单元是否来自真正的发送方，其内容是否真实，显然无法保证。这是在早期制定协议时，只考虑信息的无差错传输所带来的固有的安全漏洞，更何况某些协议本身在具体的实现过程中也可能会产生一些安全方面的缺陷。对一般的通信线路，可以利用搭线窃听技术来截获线路上传输的数据包，甚至重放（一种攻击方法）以前的数据包或篡改截获的数据包后再发出（主动攻击），这种搭线窃听并不比用窃听器听别人的电话困难多少。对于卫星通信信道而言，则既需要有专门的接收设备（类似于电视信号的地面接收器），又要求有较高的技术安装设备（如天线方位和角度的调整及其他参数的设置等）。

（5）内部人员的不忠诚、人员的非授权操作和内外勾结作案是威胁计算机信息网络安全的重要因素。

“没有家贼，引不来外鬼”就是这个道理。他们或因利欲熏心，或因对领导不满，或出

于某种政治、经济或军事的特殊使命，从机构内部利用权限或超越权限进行违反法纪的活动。统计表明，信息网络安全事件中 60%～70%起源于内部。我们要牢记“防内重于防外”。

1.2.3 网络安全威胁的主要表现形式

网络中的信息和设备所面临的安全威胁有着多种多样的具体表现形式，而且威胁的表现形式随着硬件技术的不断发展，也在不断地进化。这里将一些典型的危害网络安全的行为总结如表 1-1 所示。

表 1-1 威胁的主要表现形式

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授权的目的
旁路控制	攻击者发掘系统的缺陷或安全弱点，从而渗入系统
拒绝服务	合法访问被无条件拒绝和推迟
窃听	在监视通信的过程中获得信息
电磁泄漏	从设备发出的电磁辐射中泄漏信息
非法使用	资源被某个未授权的人或以未授权的方式使用
信息泄露	信息泄露给未授权实体
完整性破坏	对数据的未授权创建、修改或破坏造成数据一致性损害
假冒	一个实体假装成另一个实体
物理侵入	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的拷贝
否认	参与通信的一方事后否认曾经发生过此次通信
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被中断
业务流分析	通过对业务流模式进行观察（有、无、数量、方向、频率），而使信息泄露给未授权实体
特洛伊木马	含有觉察不出或无害程序段的软件，当它被运行时，会损害用户的安全
陷门	在某个系统或文件中预先设置的“机关”，使得当提供特定的输入时，允许违反安全策略
人员疏忽	一个授权的人出于某种动机或由于粗心将信息泄露给未授权的人

1.2.4 网络出现安全威胁的原因

引起网络的安全问题的原因，可以归纳为以下几种。

1. 薄弱的认证环节

网络上的认证通常是使用口令来实现的，但口令有公认的薄弱性。网上口令可以通过许多方法破译，其中最常用的两种方法是把加密的口令解密和通过信道窃取口令。例如，UNIX 操作系统通常把加密的口令保存在一个文件中，而该文件普通用户即可读取。该口令文件可以通过简单的拷贝或其他方法得到。一旦口令文件被闯入者得到，他们就可以使用解密程序对口令进行解密，然后用它来获取对系统的访问权。

2. 系统的易被监视性

用户使用 Telnet 或 FTP 连接他在远程主机上的账户，在网上传的口令是没有加密的。入侵者可以通过监视携带用户名和口令的 IP 包获取它们，然后使用这些用户名和口令通过正常

渠道登录到系统。如果被截获的是管理员的口令，那么获取特权级访问就变得更容易了。成千上万的系统就是被这种方式侵入的。

3. 易欺骗性

TCP 或 UDP 服务相信主机的地址。如果使用“IP Source Routing”，那么攻击者的主机就可以冒充一个被信任的主机或客户。使用“IP Source Routing”，采用以下操作可把攻击者的系统假扮成某一特定服务器的可信任的客户。

4. 有缺陷的局域网服务和相互信任的主机

主机的安全管理既困难又费时。为了降低管理要求并增强局域网，一些站点使用了诸如 NIS 和 NFS 之类的服务。这些服务通过允许一些数据库（如口令文件）以分布式方式管理以及允许系统共享文件和数据，在很大程度上减轻了过多的管理工作量。但这些服务带来了不安全因素，可以被有经验闯入者利用以获得访问权。如果一个中央服务器遭受到损失，那么其他信任该系统的系统会更容易遭受损害。

5. 复杂的设置和控制

主机系统的访问控制配置复杂且难以验证，因此偶然的配置错误会使闯入者获取访问权。一些主要的 UNIX 经销商仍然把 UNIX 配置成具有最大访问权的系统，这将导致未经许可的访问。

许多网上的安全事故原因是由于入侵者发现的弱点造成的。由于目前大部分的 UNIX 系统都是从 BSD 获得网络部分的代码，而 BSD 的源代码又可以轻易获得，所以闯入者可以通过研究其中可利用的缺陷来侵入系统。存在缺陷的部分原因是因为软件的复杂性，而没有能力在各种环境中进行测试。有时候缺陷很容易被发现和修改，而另一些时候除了重写软件外几乎不能做什么（如 Sendmail）。

6. 无法估计主机的安全性

主机系统的安全性无法很好的估计。随着一个站点主机数量的增加，确保每台主机的安全性都处在高水平的能力却在下降。只用管理一台系统的能力来管理如此多的系统就容易犯错误。另外，系统管理的作用经常变换并行动迟缓，这导致一些系统的安全性比另一些要低。这些系统将成为薄弱环节，最终将破坏这个安全链。

1.3　网络安全措施

1.3.1　安全技术手段

1. 物理措施

例如，保护网络关键设备（如交换机、大型计算机等），制定严格的网络安全规章制度，采取防辐射、防火及安装不间断电源（UPS）等措施。

2. 访问控制

对用户访问网络资源的权限进行严格的认证和控制。例如，进行用户身份认证，对口令加密、更新和鉴别，设置用户访问目录和文件的权限，控制网络设备配置的权限等。

3. 数据加密

加密是保护数据安全的重要手段。加密的作用是保障信息被人截获后不能读懂其含义。防止计算机网络病毒，安装网络防病毒系统。

4. 网络隔离

网络隔离有两种方式：一种是采用隔离卡来实现的；另一种是采用网络安全隔离网闸实现的。隔离卡主要用于对单台机器的隔离，网闸主要用于对于整个网络的隔离。

5. 其他措施

其他措施包括信息过滤、容错、数据镜像、数据备份和审计等。近年来，围绕网络安全问题提出了许多解决办法，如数据加密技术和防火墙技术等。数据加密是对网络中传输的数据进行加密，到达目的地后再解密还原为原始数据，目的是防止非法用户截获后盗用信息。防火墙技术是通过对网络的隔离和限制访问等方法来控制网络的访问权限。

1.3.2 安全防范意识

拥有网络安全意识是保证网络安全的重要前提。许多网络安全事件的发生都和缺乏安全防范意识有关。对于网络用户来说，提高网络安全防范意识是解决安全问题的根本。具体地说，凡是来自于网上的东西都要持谨慎态度。

1.3.3 主机安全检查

要保证网络安全，进行网络安全建设，第一步首先要全面了解系统，评估系统安全性，认识到自己的风险所在，从而迅速、准确地解决内网安全问题。由安天实验室自主研发的国内首款创新型自动主机安全检查工具，彻底颠覆传统系统保密检查和系统风险评测工具操作的繁冗性，一键操作即可对内网计算机进行全面的安全保密检查及精准的安全等级判定，并对评测系统进行强有力的分析处置和修复。

1.4 网络安全标准与体系

安全服务是由网络安全设备提供的，它为保护网络安全提供服务。保护信息安全所采用的手段称为安全机制。安全服务和安全机制对安全系统设计者有不同的含义，但对安全分析来说其含义是相同的。所有的安全机制都是针对某些安全攻击威胁而设计的，它们可以按不同的方式单独使用，也可组合使用。合理地使用安全机制，会在有限的投入下最大限度地降低安全风险。

1.4.1 可信计算机系统评价准则简介

为实现对网络安全的定性评价，美国国防部所属的国家计算机安全中心（NCSC）在 20 世纪 90 年代提出了网络安全性标准（DoD5200.28-STD），即可信任计算机标准评估准则（Trusted Computer Standards Evaluation Criteria），也叫橘皮书（Orange Book），认为要使系统免受攻击，对应不同的安全级别，硬件、软件和存储的信息应实施不同的安全保护。安全级别对不同类型的物理安全、用户身份验证（Authentication）、操作系统软件的可信任性和用户应用程序进行了安全描述，标准限制了可连接到你的主机系统的系统类型。

网络安全性标准将网络安全性等级划分为 A、B、C、D 四类，其中，A 类安全等级最高，D 类安全等级最低。

1.4.2 国际安全标准简介

数据加密的标准化工作在国外很早就开始了。比如，1976 年美国国家标准局就颁布了“数

据加密标准算法（DES）”。1984 年，国际标准化组织 ISO/TC97 决定正式成立分技术委员会，即 SC20，开展制定信息技术安全标准工作。从此，数据加密标准化工作在 ISO/TC97 内正式蓬勃展开。经过几年的努力，根据技术发展的需要，ISO 决定撤消原来的 SC20，组建新的 SC27，并在 1990 年 4 月瑞典斯德哥尔摩年会上正式成立 SC27，其名称为“信息技术－安全技术”。SC27 的工作范围是信息技术安全的一般方法和信息技术安全标准体系，包括确定信息技术系统安全服务的一般要求、开发安全技术和机制、开发安全指南、开发管理支撑文件和标准。

1.4.3　我国安全标准简介

我国信息安全研究经历了通信保密、计算机数据保护两个发展阶段，正在进入网络信息安全的研究阶段。通过学习、吸收、消化 TCSEC 的原则进行了安全操作系统、多级安全数据库的研制，但由于系统安全内核受控于人，以及国外产品的不断更新升级，基于具体产品的增强安全功能的成果，难以保证没有漏洞，难以得到推广和应用。在学习借鉴国外技术的基础上，国内一些部门也开发研制了一些防火墙、安全路由器、安全网关、黑客入侵检测、系统脆弱性扫描软件等。但是，这些产品安全技术的完善性、规范化实用性还存在许多不足，特别是在多平台的兼容性及安全工具的协作配合和互动性方面存在很大距离，理论基础和自主的技术手段也需要发展和强化。

以前，国内主要是等同采用国际标准。目前，由公安部主持制定、国家技术标准局发布的中华人民共和国国家标准 GB 17895－1999《计算机信息系统安全保护等级划分准则》已经正式颁布。该准则将信息系统安全分为 5 个等级，分别是自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。主要的安全考核指标有身份认证、自主访问控制、数据完整性、审计、隐蔽信道分析、客体重用、强制访问控制、安全标记、可信路径和可信恢复等，这些指标涵盖了不同级别的安全要求。

1.5　网络安全机制

安全机制是一种用于解决和处理某种安全问题的方法，通常分为预防、检测和恢复 3 种类型。网络安全中的绝大多数安全服务和安全机制都是建立在密码技术基础之上的，它们通过密码学方法对数据信息进行加密和解密来实现网络安全的目标要求。

一个或多个安全机制的运用与实现便构成一种安全策略。在网络安全中，常把密码函数运用到安全策略中的某个环节上，通过数据加密可以把需要保护的敏感数据的敏感性减弱，从而降低危险。在网络上采用下列机制，才能维护网络的安全。

1. 加密机制

加密是提供信息保密的核心方法。按照密钥的类型不同，加密算法可分为对称密钥算法和非对称密钥算法两种。按照密码体制的不同，又可以分为序列密码算法和分组密码算法两种。加密算法除了提供信息的保密性之外，它和其他技术结合，如 Hash 函数，还能提供信息的完整性。

加密技术不仅应用于数据通信和存储，也应用于程序的运行，通过对程序的运行实行加密保护，可以防止软件被非法复制，防止软件的安全机制被破坏，这就是软件加密技术。

2. 访问控制机制

访问控制可以防止未经授权的用户非法使用系统资源，这种服务不仅可以提供给单个用

户，也可以提供给用户组的所有用户。访问控制是通过对访问者的有关信息进行检查来限制或禁止访问者使用资源的技术，分为高层访问控制和低层访问控制。高层访问控制包括身份检查和权限确认，是通过对用户口令、用户权限、资源属性的检查和对比来实现的。低层访问控制是通过对通信协议中的某些特征信息的识别、判断，来禁止或允许用户访问的措施。如在路由器上设置过滤规则进行数据包过滤，就属于低层访问控制。

3. 数据完整性机制

数据完整性包括数据单元的完整性和数据序列的完整性两个方面。

（1）数据单元的完整性是指组成一个单元的一段数据不被破坏和增删篡改，通常是把包括有数字签名的文件用 Hash 函数产生一个标记，接收者在收到文件后也用相同的 Hash 函数处理一遍，看看产生的标记是否相同就可以知道数据是否完整。

（2）数据序列的完整性是指发出的数据分割为按序列号编排的许多单元时，在接收时还能按原来的序列把数据串联起来，而不要发生数据单元的丢失、重复、乱序、假冒等情况。

4. 数字签名机制

数字签名机制主要解决以下安全问题：

（1）否认。事后发送者不承认文件是他发送的。

（2）伪造。有人自己伪造了一份文件，却声称是某人发送的。

（3）冒充。冒充别人的身份在网上发送文件。

（4）篡改。接收者私自篡改文件的内容。

数字签名机制具有可证实性、不可否认性、不可伪造性和不可重用性。

5. 交换鉴别机制

交换鉴别机制是通过互相交换信息的方式来确定彼此的身份。用于交换鉴别的技术有以下几种：

（1）口令。由发送方给出自己的口令，以证明自己的身份，接收方则根据口令来判断对方的身份。

（2）密码技术。发送方和接收方各自掌握的密钥是成对的。接收方在收到已加密的信息时，通过自己掌握的密钥解密，能够确定信息的发送者是掌握了另一个密钥的那个人。在许多情况下，密码技术还和时间标记、同步时钟、双方或多方握手协议、数字签名、第三方公证等相结合，以提供更加完善的身份鉴别。

（3）特征实物。如 IC 卡、指纹、声音频谱等。

6. 公证机制

网络上鱼龙混杂，很难说相信谁不相信谁。同时，网络的有些故障和缺陷也可能导致信息的丢失或延误。为了免得事后说不清，可以找一个大家都信任的公证机构，各方交换的信息都通过公证机构来中转。公证机构从中转的信息里提取必要的证据，日后一旦发生纠纷，就可以据此做出仲裁。

7. 流量填充机制

流量填充机制提供针对流量分析的保护。外部攻击者有时能够根据数据交换的出现、消失、数量或频率而提取出有用信息。数据交换量的突然改变也可能泄露有用信息。例如，当公司开始出售它在股票市场上的份额时，在消息公开以前的准备阶段中，公司可能与银行有大量通信。因此对购买该股票感兴趣的人就可以密切关注公司与银行之间的数据流量以了解是否可以购买。

流量填充机制能够保持流量基本恒定，因此观测者不能获取任何信息。流量填充的实现方法是：随机生成数据并对其加密，再通过网络发送。

8. 路由控制机制

路由控制机制使得可以指定通过网络发送数据的路径。这样，可以选择那些可信的网络节点，从而确保数据不会暴露在安全攻击之下。而且，如果数据进入某个没有正确安全标志的专用网络时，网络管理员可以选择拒绝该数据包。

1.6　网络安全设计准则

安全建设是一个系统工程，网络安全经过若干年的发展后，从初期的单一产品、单一技术，到技术的堆砌和产品的堆砌，但是，安全问题一直没有得到彻底解决。近几年又兴起了风险评估、蜜罐、安全管理等多种概念，这一切的实施和贯彻，都必须落实和反映在最后的网络建设和设计中。

一般而言，网络安全体系的建设和设计应按照“统一规划、统筹安排，统一标准、相互配套”的原则进行，采用先进的“平台化”建设思想，避免重复投入、重复建设，充分考虑整体和局部的利益，坚持近期目标与远期目标相结合。

在进行系统安全方案设计、规划时，应遵循以下原则：

1. 综合性、整体性原则

应用系统工程的观点、方法，分析网络的安全及具体措施。安全措施主要包括行政法律手段、各种管理制度（人员审查、工作流程、维护保障制度等）及专业措施（识别技术、存取控制、密码、低辐射、容错、防病毒、采用高安全产品等）。一个较好的安全措施往往是多种方法适当综合应用的结果。一个计算机网络，包括个人、设备、软件、数据等。这些环节在网络中的地位和影响作用，也只有从系统综合整体的角度去看待、分析，才能取得有效、可行的措施。即计算机网络安全应遵循整体安全性原则，根据规定的安全策略制定出合理的网络安全体系结构。

2. 需求、风险、代价平衡的原则

对任一网络，难以达到绝对安全，也不一定是必要的。对一个网络进行实际额度研究（包括任务、性能、结构、可靠性、可维护性等），并对网络面临的威胁及可能承担的风险进行定性与定量相结合的分析，然后制定规范和措施，确定系统的安全策略。

3. 一致性原则

一致性原则主要是指网络安全问题应与整个网络的工作周期（或生命周期）同时存在，制定的安全体系结构必须与网络的安全需求相一致。安全的网络系统设计（包括初步或详细设计）及实施计划、网络验证、验收、运行等，都要有安全的内容及措施，实际上，在网络建设的开始就考虑网络安全对策，比在网络建设好后再考虑安全措施，不但容易，而且花费也少得多。

4. 易操作性原则

安全措施需要人去完成，如果措施过于复杂，对人的要求过高，本身就降低了安全性。其次，措施的采用不能影响系统的正常运行。

5. 分步实施原则

由于网络系统及其应用扩展范围广阔，随着网络规模的扩大及应用的增加，网络脆弱性

也会不断增加。一劳永逸地解决网络安全问题是不现实的。同时由于实施信息安全措施需要很大的费用。因此分步实施，既可满足网络系统及信息安全的基本需求，也可节省费用开支。

6. 多重保护原则

任何安全措施都不可能绝对安全，都可能被攻破。但是建立一个多层次保护系统，各层保护相互补充，当一层保护被攻破时，其他层保护仍可保护信息的安全。

7. 可评价性原则

如何预先评价一个安全设计并验证其网络的安全性，这需要通过国家有关网络信息安全测评认证机构的评估来实现。

通过前面的网络安全事件，可以了解到目前网络安全面临的问题是比较多的，学习网络安全，就要密切关注网络安全事件发生的起因和形式，进而找出相应的防范措施，尽力使网络变得更安全。

简答题

1. 简明阐述网络安全设计的一致性原则。
2. 简明阐述信息安全保障的 5 个要考虑的因素。
3. 什么是网络安全?
4. 网络面临的安全威胁有哪几种？
5. 网络的安全机制有哪些？
6. 什么是物理安全？它包括哪几方面的内容？
7. 网络安全教育的意义是什么?
8. 计算机信息系统安全保护分为哪 5 个级别?
9. 通过网络检索，结合书中的案例，举例说明有哪几种形式的网络安全事件。
10. 结合自己使用计算机上网的经历，介绍自己上网遇到的网络安全事件，并说明解决的过程。