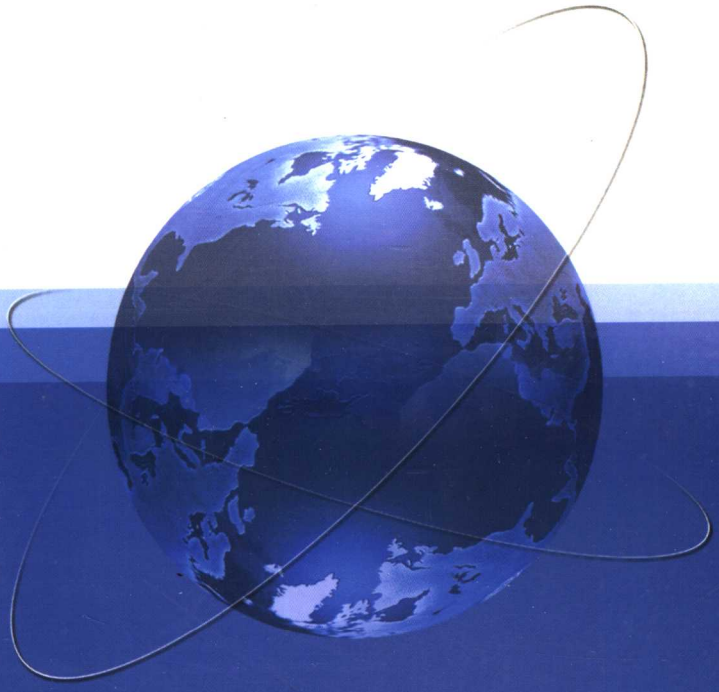
21世纪高职高专规划教材

网络安全技术



陈 卓 主编

机械工业出版社
CHINA MACHINE PRESS

21世纪高职高专规划教材

网络安全技术

主　编	湖北工业大学	陈　卓
副主编	天津中德职业技术学院	马　强
	山东日照职业技术学院	袁　泉
	湖北工业大学	陈晓炜
参　编	湖北工业大学	欧阳勇
	山东日照职业技术学院	唐海和
	山东日照职业技术学院	李　杰

机械工业出版社

本教材是21世纪高职高专规划教材之一，书中介绍了网络安全的基本理论和常用的安全技术，在网络安全的基本理论方面主要介绍了密码学的基本知识，具体包括：对称密码算法、公钥密码算法、鉴别技术和数字签名等；在常用的安全技术方面主要介绍了网络安全协议、防火墙技术、入侵检测技术、病毒防护、操作系统安全和网络环境物理安全以及一些常用网络安全工具的使用。

本教材根据2年制和3年制高职高专计算机网络技术专业的需要，并考虑了计算机专业及相关专业的要求，内容丰富，文字浅显易懂，可作为高职高专计算机网络以及计算机应用等专业的教材，也可作其他相关专业的教材以及计算机爱好者的自学参考书。

图书在版编目（CIP）数据

网络安全技术/陈卓主编. —北京：机械工业出版社，2004.8

21世纪高职高专规划教材

ISBN 7-111-15068-6

Ⅰ.网… Ⅱ.陈… Ⅲ.计算机网络—安全技术—高等学校：技术学校—教材 Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2004）第081422号

机械工业出版社（北京市百万庄大街22号 邮政编码100037）

策划编辑：余茂祚 责任编辑：余茂祚

封面设计：饶 薇 责任印制：石 冉

三河市宏达印刷有限公司印刷·新华书店北京发行所发行

2004年8月第1版第1次印刷

787mm×1092mm 1/16·9.75印张·237千字

定价：16.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

本社购书热线电话（010）68993821、88379646

21世纪高职高专规划教材

编委会名单

前　言

本书是根据教育部教高[2000]2 号文件精神，由中国机械工业教育协会和机械工业出版社组织全国 80 多所院校编写的 21 世纪高职高专规划教材之一。

随着电子信息产业的迅速崛起，互联网、电子商务如雨后春笋，发展之快令各行业为之侧目，目前，互联网已遍及全球 180 多个国家，为 1 亿多用户提供多样化的网络与信息服务。随着网络的深入发展，人们也逐渐意识到网络安全的重要性。现今，网络攻击活动越演越烈，从美国微软、雅虎、亚马哈到中国的新浪，黑客的攻击无处不在。据统计，全球每 20s 发生一次黑客攻击，每日出现 5～10 种新病毒，病毒总数目目前已达 40000 种，黑客攻击手段多达 1500 种。20 世纪 80 年代，美国在互联网上的损失每年达 50 亿美元，到 20 世纪 90 年代每年损失已达到 70 亿美元，甚至更多，仅 2000 年 2 月 7 日至 10 日 3 天就损失了 12 亿美元。

目前，我国网络的安全防护能力还很弱，存在极大的风险和危险。信息产业基础薄弱，严重依赖国外，信息犯罪在我国有发展蔓延的趋势，全社会的信息安全意识也急待提高。有专家称国内仍有许多网站处于“不设防状态”，等于为入侵者洞开方便之门，使人不能不为当前的网络安全现状忧虑。

然而，由于很多网民和网络使用者对直接的经济损失还感受不深，还没有认识到网络安全的重要性。人们对信息安全的意识从无到有、由浅入深，似乎还有很长的路要走。但应该了解网络系统世界中有关安全的基本情况，知道网络上的个人数据和通信记录随时都有可能被公之于众或被滥用，防患于未然是很有必要的。

在信息飞速发展的今天，没有安全就意味挨打，更不会有发展。网络安全关系到国家的主权和安全，这是一个必须正视的问题。因此，构筑面向 21 世纪的国家信息安全保障体系，无疑具有十分重要的战略意义。

时代需要网络，网络需要安全。

但是网络本身技术性较强，网络安全涉及的理论比较生涩难懂，可能这是初入此道者翻了几本书后的共同心理。正是在这种情况下，我们根据高职高专计算机网络技术专业的需要，并考虑了计算机专业及相关专业的要求，编写了这本教材。本书力求以通俗的语言和清晰的叙述方法，向读者介绍计算机网络安全的基本理论和常用的安全技术。

本书内容共分 9 章。

第 1 章为计算机网络安全概述，主要介绍了计算机网络安全的定义、面临的主要威胁，网络安全的基本需求：机密性、完整性、可用性、不可否认性等，以及构建网络安全体系结构的主要技术、网络安全的级别分类、我国网络安全现状。

第 2 章我们将学习密码学的历史与发展、密码学的基本概念、密码算法的分类，学习几种有代表性的古典密码，还将学习对称密码算法和非对称密码算法的原理。

第 3 章仍然属密码技术范畴，我们将学习数据的鉴别技术、数字签名和身份认证技术。

第 4 章介绍网络中常用的网络安全协议，网络安全协议的种类繁多，本书将主要介绍其中的 SSL、IPSec、PGP 协议。

第 5 章介绍网络防火墙技术的基本原理、分类、以及相关的主要技术，我们将了解到：防火墙不能解决所有的安全问题，防火墙只是整个安全策略的一部分。

第 6 章将学习计算机网络病毒的特性、传播途径以及病毒的预防和查杀的知识。

在第 7 章，将介绍入侵检测技术的定义、功能、分类等知识。

第 8 章介绍操作系统安全和网络环境的物理安全。

最后，在第 9 章将介绍几种常用的网络安全工具。

每章内容后都附有小结和复习思考题，帮助读者对基本理论和关键技术的掌握，同时还附有上机练习，帮助读者能学以致用，尽快进入实用状态。

本教材参考学时为 48 学时。建议理论教学 38 学时、上机学时 10 个学时。可作为 2 年制和 3 年制高职高专计算机网络技术专业、计算机应用专业及相关专业的教材以及计算机爱好者自学使用。

本教材第 1 章和第 2 章由陈卓编写；第 3 章和第 4 章由陈晓炜编写；第 5、6、7、8、9 章分别由李杰、唐海和、袁泉、欧阳勇、马强编写，陈卓作为主编对全书进行了统编和最后定稿。

在本书的编写和出版过程中，得到了机械工业出版社余茂祚教授的热情帮助；山东日照职业技术学院、天津中德职业技术学院、湖北工业大学职教学院也提供了的大力支持；此外，凌世焰高工对本书提出了许多宝贵意见，谨在此一并表示衷心感谢；最后感谢张正文先生的大力帮助，使得本书得以早日付梓，在此致以谢意。

在向读者们热情推荐本书的同时，我们也深深感到计算机网络安全的理论、技术以及应用可谓“博大精深”，网络安全新技术如雨后春笋，书中如有错误和疏漏，敬请各位同仁批评指正，并提出宝贵意见。

编 者

目　录

第1章　计算机网络安全概述

21世纪的今天，信息技术的迅猛发展使得计算机网络这一人类伟大的发明已经广泛地深入到社会的各个角落，人们利用网络存储数据、处理图像、遨游网际、互发电子邮件等，充分地享用网络带来的无可比拟的功能和智慧。计算机网络已经成为社会发展进步的重要标志，它的应用遍及国家的政府、军事、科技、文教等各个领域。其中存储、传输和加工处理的信息有许多涉及政府宏观调控决策、商业经济信息、银行资金转账、股票证券、能源资源数据、科研数据等重要内容。

与此同时，无情的事实表明，除非我们把计算机锁在一个密闭的房间里，并且没有任何计算机与之相连，使其对外界的访问受到隔离，否则该计算机系统就会时刻处于危险之中，随时都可能面临黑客的攻击、少数网民的恶作剧以及个别居心叵测分子的作祟，同时，计算机网络实体还要经受诸如水灾、火灾、地震、电磁辐射等自然灾害的考验。

近年来，计算机犯罪案件急剧上升，各国的计算机系统特别是网络系统面临着很大的威胁，并成为严重的社会问题之一，据美国联邦调查局的报告，计算机犯罪是商业犯罪中最大的犯罪类型之一，每笔犯罪的平均金额为45000美元，每年计算机犯罪造成的经济损失高达100亿美元，加之国际互联网络的广域性、开放性和可扩展性，计算机犯罪也已成为具有普遍性的国际问题。由此可见，计算机的安全问题，尤其是计算机网络的安全问题，已经到了不可小视，必须深入探讨研究的非同小可的时候了。

1.1　引言

1.1.1　计算机网络安全的定义

当你遨游在Internet浩瀚无际的信息海洋时，你就会发现计算机只有同网络相连，才是名副其实的计算机，从一定意义上讲，“网络就是计算机”，“计算机就是网络”，两者密不可分。随着计算机网络的飞速发展，这一关于计算机的现代理念已经越来越得到人们的认可。因此，要给计算机网络安全下定义，首先要了解“计算机安全”的概念。

国际标准化组织(ISO)将“计算机安全”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”，此定义偏重于静态信息的保护。

也曾有人将“计算机安全”定义为：“计算机的硬件、软件和数据受到保护，不因偶然和恶意的原因而遭到破坏、更改和泄露，系统连续正常运行。”该定义着重于动态意义描述。

综合上述计算机安全的定义以及计算机和网络的密切关系，我们可以给“计算机网络安全”作如下定义：“保护计算机网络系统中的硬件、软件及其数据不受偶然或者恶意原因而遭到破坏、更改、泄露，保障系统连续可靠地正常运行，网络服务不中断。”

1.1.2　计算机网络面临的安全威胁

为什么计算机网络如此容易受到侵害？主要存在于两个方面的问题：一方面，资源共享是计算机网络的重要特点，这对于无数的计算机用户无疑是天大的好事，否则，网络也不会

受到人们的如此青睐。但也正是因为“共享”，却被一些别有用心者钻了空子，使得网络信息及网络设备的安全受到了种种不同程度的威胁；另一方面，从网络协议结构设计看，如今使用最广泛的网络协议是TCP / IP协议，它是在资源管理及网络技术均不成熟的情况下设计的。它的主要设计目标是互联、互通、共享，而不是安全。实践证明，该协议中已被发现有许多安全漏洞和隐患，这是因为研制者在设计初并没有过多考虑网络的安全性能。因此，计算机技术，包括网络技术，虽然已经从过去的研究阶段进入了商品实用阶段，但是它的技术基础却是不安全的，有其脆弱的一面，这是我们不可否认的客观事实。

知己知彼，百战不殆。下面我们通过计算机网络上两个用户的通信来考察一下网络面临的主要威胁。

(1) 截获：当发方通过网络与接收方通信时，如果不采取任何保密措施，那么其他人，就有可能截获并偷听到他们的通信内容，如图 1-1 所示。

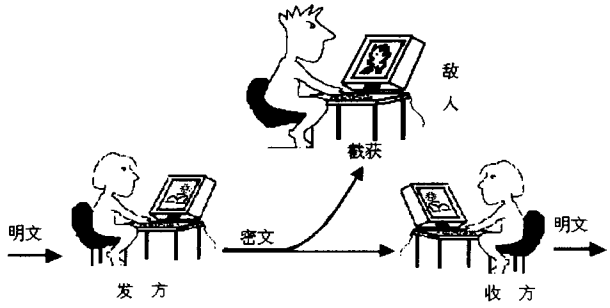


图 1-1 消息被截获

（2）篡改：未授权方不仅获得了访问而且篡改了内容。随着信息技术的发展，信息处理与计算能力得到了极大的提高，敌人对保密通信体制的攻击，除了原来的“截获-破译”外，在很多场合，特别是在实时性要求不太高的情况下，对手可采用在信道中间插入一个非法设备，对原来的信息进行诸如删除、添加、修改等活动。例如：A 给 B 发如下消息：“请立即汇款 1 万元，A”，报文在转发的过程中，被 C 篡改成“请立即给 C 汇款 10 万元，A”；或者 C 将 A 发送给 B 的“请原地待命”改成“请马上撤退”，都会给 A、B 之间带来无法挽回的损失，如图 1-2 所示。

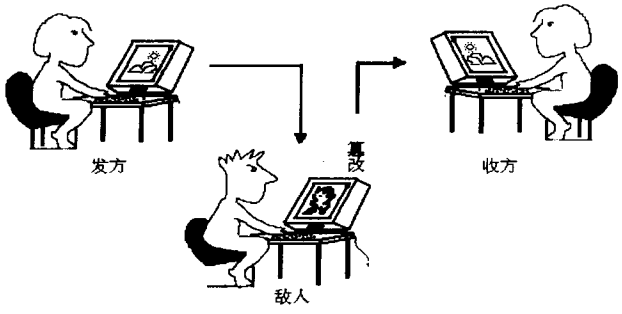


图 1-2 消息被篡改

（3）抵赖：这是通信双方之间可能发生的安全隐患，例如 A 否认自己曾经给 B 发出过的报文（如签发的支票）。在电子商务系统中特别需要提供抗抵赖服务。

（4） 病毒危害：计算机病毒也是计算机网络面临的主要威胁之一。所谓病毒（Viruses）是指一段可执行的程序代码，通过对其他程序进行修改，可以“感染”这些程序，使它们含有该病毒程序的一个复制，有的病毒还具备引发损坏和植入攻击的能力。由于网络的设计目标是资源共享，所以网络是计算机病毒滋生的理想家园，随着 Internet 的发展，大大地加速了病毒的传播速度。

（5）拒绝服务：拒绝服务 DoS（Denial of Service）是一种破坏性的攻击方式，其目的旨在使目的主机陷入停顿或无意义的繁忙，从而使合法用户无法正常使用资源，造成网络效率降低甚至瘫痪。例如：Ping 风暴是一种常用的 DoS 攻击方法，只要多人约定在某个时刻同时对目标主机使用 Ping 程序，就可能耗尽目标主机的网络带宽和处理能力，造成网络效率急剧降低或瘫痪。

1.2 计算机网络安全的基本需求

面对计算机网络面临的威胁，人们对计算机网络中的数据安全提出了以下安全需求：

1．数据的机密性　首先人们意识到的是信息保密。在传统信息环境中，普通人通过邮政系统发送信件，为了个人隐私还要装上信封。可是到了使用数字化的信息的今天，以 0、1 比特串编码在网上传来传去，连个“信封”都没有，我们发的电子邮件都是“明信片”，那还有什么秘密可言，因此，就提出了信息安全中数据的机密性的需求。

数据的机密性是指数据不被未授权者获取，机密性可以保护被传输的数据免受如图 1-1 所示的截获攻击。

2．数据的完整性　在网络环境中如何防止信息被黑客篡改，或者说信息被移花接木后怎样才可以被察觉呢？人们提出了网络中数据的完整性的需求。

数据的完整性是指保证真实的数据从发送方到达接收方。在经过网络传输后的数据，必须与传输前的内容与形式完全一样，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，数据在传输的过程不会被有意或无意的事件所改变、破坏和丢失。系统需要一种方法来确认数据在此过程中没有被改变。

3．数据的可用性　数据的可用性是授权者可以随时使用信息的服务特性，即攻击者不能占用资源而阻碍授权者的工作。由于互联网络是开放性网络，需要时就可以得到所需要的数据，这是网络设计和发展的基本目标，因此数据的可用性要求系统当用户需要时能够存取所需要的数据，或者说能够得到系统提供的服务。如果一个合法用户需要得到系统或网络服务时，系统和网络不能提供正常的服务，那么就像文件资料被锁在保险柜里，开关和密码系统因混乱而不能取出一样，虽然数据完好无损地存在于系统之中，却眼看着拿不出来。例如，网络环境下拒绝服务、破坏网络和系统的正常运行等都属于对数据可用性的攻击。

4．不可抵赖和不可否认　是指用户不能抵赖自己曾做出的行为，也不能否认曾经接到对方的信息，这在网络交易系统如电子商务中十分重要。

另外，保护网络硬件资源不被非法占有和破坏，软件资源免受病毒的侵害，都构成了整个信息网络上的安全需求。

1.3 主要的网络安全技术

1．网络安全的基石——密码技术　构建网络安全的体系结构离不开密码技术，没有密

码技术的支撑，网络安全无从谈起。密码理论是网络安全的重要基石，是保护网络信息安全的核心与关键技术，随着通信和计算机技术发展起来的现代密码学，不仅在解决信息的机密性，而且在解决信息的完整性、可用性和抗抵赖性方面发挥着不可替代的作用。本书在第2、3章将介绍密码学中的加密技术、鉴别和数字签名等技术。

数据加密可以用来实现数据的机密性，使得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，将明文转换成密文，只有经过授权的合法用户，使用与发送方共享的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密钥，无法获得原文的信息。数据加密可以说是许多安全措施的基本保证。

对于数据的完整性，可以采用鉴别技术来实现，鉴别技术也是密码学的主要应用领域之一。为了防止数据在传输过程中被非法篡改、删除、产生，只需在通信介质两端进行密码学鉴别变换。鉴别技术就像明查秋毫的大法官，通过对鉴别算法产生的消息鉴别码的比对，立刻就能发现接收到的数据是否被作过手脚，常用的鉴别算法有MD5、SHA等。

对于通信中的抵赖行为，在密码学中可以采用“数字签名”来解决。数字签名的目的是使发送者把签了名的消息发送给接收者以后，便不能否认其签名的消息；而接收者能够验证发送者的签名，但不能伪造。数字签名的作用类似于传统的手写签名，一旦双方就消息的内容和消息的来源发生了争执，应能向仲裁者提供出有效的证据，证明是一方抵赖还是另一方诬告。

2．网络安全协议　通过前面的介绍，我们知道采用密码技术可以提供数据的机密性、完整性、抗抵赖等安全服务，那么这些安全服务如何在网络中系统地实施呢？我们知道OSI参考模型是用7层概念功能层的方法来描述网络的结构，但因特网体系结构TCP/IP只用了4层，TCP/IP本身并没有考虑网络的安全问题，于是人们提出了若干网络安全协议试图在TCP/IP的各个层面上来解决其安全问题，本书将主要介绍其中的SSL、IPSec、PGP协议。虽然不必人人都是安全协议的专家，但是，了解网络安全协议的基本知识有助于建立一套完整的安全体系结构，这样在具体的安全方案的实施中，可以根据实际的安全需求很方便地在操作系统和路由器中进行安全配置。

3．网络安全的大门——防火墙技术　防火墙是插在内部网与不安全的外部网络之间的一个隔离层，它通过建立受控的连接来形成一道安全的屏障，它隔离内部网与外部网，使内部网有选择地与外部网进行信息交换，阻止外界对内部资源的非法访问。防火墙增强了内部网络的安全性，用户可以安全地使用网络，更好地利用网络的资源。比较常用的防火墙有：包过滤防火墙、代理服务器（也叫应用级网关）、电路级网关、规则检测防火墙等。

防火墙也有自身的限制，这些缺陷包括：

1）定义数据包过滤器会比较复杂，并且随着过滤器数目的增加，路由器的吞吐量会下降，因此防火墙可能会是潜在的瓶颈。

2）防火墙无法阻止绕过防火墙的攻击。

3）防火墙无法阻止来自内部的威胁。

因此，防火墙不能解决所有的安全问题，防火墙只是整个安全策略的一部分。

4．入侵检测　入侵检测是防火墙的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力(包括安全审计、监视、进攻识别和响应)，提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息，并分析这些信息，了解网络中是否

有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。

5. 网络病毒防护　面对病毒的猖獗，需要建立起有效的技术措施，能从病毒传染的各种可能途径入手，不受病毒种类和变形的限制，能够防、杀结合，甚至能够安全运行受病毒感染的程序，保证网络系统的有效、正常运行。

6. PKI　PKI 是 Public Key Infrastructure 的缩写，即“公开密钥基础设施”，是一种遵循既定标准的密钥管理平台，它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系。

完整的 PKI 系统必须具有权威认证机关(CA)、数字证书库、密钥备份及恢复系统、证书作废系统、应用接口等基本构成部分，构建 PKI 也将围绕着这五大系统来着手构建。PKI 技术可运用于众多领域，其中包括：虚拟专用网络（VPN）、安全电子邮件、Web 交互安全及倍受瞩目的电子商务安全领域，基于网络环境下数据加密/签名的应用将越来越广泛，PKI 作为技术基础可以很好地实现通行于网络的统一标准的身份认证，其中既包含有线网络，也涵盖了无线通信领域。可以预见，PKI 的应用前景将无比广阔。

7. 虚拟专用网（VPN）技术　虚拟专用网是一种在公用网络中实现专用网络功能的技术。在 VPN 中，任意两个节点之间的连接并无专用网所需的物理链路，而是利用公众网的资源动态组成。这种公众网可以是 ATM、帧中继网、IP 网，从而形成逻辑上的专用网络。目前，因特网已成为全球最大的网络基础设施，几乎延伸到世界的各个角落，于是基于因特网的 VPN 技术越来越受到广泛关注。

1.4　网络的安全管理问题

除了依靠以上先进的技术，网络安全还离不开严格的网络安全管理。各网络使用机构、企业和单位应建立相应的严格的信息安全管理办法，加强内部管理，建立审计和跟踪体系，提高整体的信息安全意识。

你也许花了不少的钱买了安全设备，但如果你将它束之高阁，或不按它的安全规范合理操作，认为有了安全的设备就会安全，而没有在落实上下功夫，那么再好的设备也不安全。

世界上现有的很多信息系统仍然缺少安全管理员，缺少信息系统安全管理的技术规范，缺少定期的安全测试与检查，更缺少安全审计。我国许多企业的信息系统已经使用许多年，但计算机的系统管理员与用户的注册不少还处于默认状态。

另一方面，也可以说网络的安全问题是天生的，网络由各种服务器、工作站、终端等集群而成，所以整个网络天然地继承了它们各自的安全隐患。各种服务器各自运行着不同的操作系统，各自继承着自身系统的不同安全特性。随着计算机及通信设备组件数目的增大，积累起来的安全问题将十分复杂。

这意味着要制定一个有效的安全管理策略。如某公司的信息应当由管理者们做出决策，确定哪些信息是可共享的，哪些信息是内部机密，不得泄露，以免对公司利益造成损害。

安全管理必须回答下列基本问题：需要保护什么？为什么需要保护?怎样保护？何时保护？在哪里保护？显然上述问题有的涉及安全技术，而有的是管理者的决策。另外，安全性和使用方便性又是一对矛盾，两者不可兼得，强调了安全性，使用方便将受影响；强调使用

方便，则安全性可能减弱，这也需要管理者做出决策。国际标准化组织把网络管理划分为五个领域，分别是：故障、性能、配置、记账和安全。“故障管理”负责检测或发现异常的网络运转，隔离并控制网络问题。“性能管理”负责分析网络出错率及网络吞吐率，以建立合理、优化的网络运行状态。“配置管理”负责检测物理的和逻辑的配置，了解和控制网络状态。“记账管理”负责搜集资源、处理资源和利用数据。“安全管理”负责控制各种对网络的访问。

此外，网络运行的环境、操作人员的管理也是网络安全管理的重要方面。不得不正视这样的一个事实，网络用户大多数不具备计算机的专业知识，他们只是将计算机视为一个工具，由于他们缺乏安全操作的常识或对安全不够重视，他们在安全操作方面的失误往往造成对网络的侵害，如将上网口令取为自己的或亲朋的姓名、生日、出生地等易猜信息，或者将口令随意标在机器上、机器旁的纸片上及自己的记事簿上或贴在机房里。再如，有多少用户在暂时离开办公桌，去开一个短会、去吃饭或去卫生间时会关闭应用系统呢？当一个系统未关闭而被非法用户侵入时，它的全部权力将被无保留地非法盗用。虽然我们无法完全模仿入侵者如黑客们的全部手段，但必须正视这一事实：我们工作活动的空间正是黑客们游荡、窥测的地方。

1.5 计算机网络安全的级别分类

1.5.1 信任计算机标准评估准则（TCSEC）

从 1981 年起，美国国防部计算机安全中心就开始全面研究计算机系统所处理的机密信息的保护要求和控制手段。1985 年开发出计算机安全标准：《可信任计算机标准评估准则》（TCSEC：Trusted Computer Standards Evaluation Criteria），因为封面为桔色也叫桔皮书，其中的一些计算机安全级别被用来评价一个计算机系统的安全性。自从 1985 年它成为美国国防部的标准以来，就一直没有改变过，多年来一直是评估多用户主机和操作系统的主要方法，其他子系统(如数据库和网络等)也一直是用桔皮书来解释评价的。

桔皮书就计算机系统的安全性程度，分为若干安全级别，依照安全等级由低到高的顺序是：D 级安全、C 级安全、B 级安全、A 级安全。

1. D 级安全　D 级是最低的安全级别，拥有这个级别的系统是可用的最低安全形式。其硬件缺乏保护，操作系统容易受到损害，用户和存储器在计算机上的信息少有身份验证控制访问权限。属于这个级别的操作系统有：MS-DOS、Windows 和 Macintosh System 7.x 等操作系统，它们不区分用户，无法确定谁在敲击键盘，对硬盘上的信息几乎可以不受限制地访问。然而，这并不意味着此类操作系统不向用户提供任何安全功能，而仅仅表示那种操作系统不具备更高级别的安全功能。它们提供简单的用户识别、验证、审核，也有一些访问控制和加密等功能，只是不如 C 级的操作系统。

2．C 级安全　C 级有两个安全子级别，即 C1 级和 C2 级。

（1）C1 级安全：C1 级安全又称自由选择性安全保护(Discretionary Security Protection)级别，它描述了一种典型的在 UNIX 系统上的安全级别。这种级别的系统对硬件提供了某种程度的保护，用户拥有注册账号和口令系统，通过账号和口令来识别用户是否合法，并决定用户对程序和数据有什么样的访问权，但其硬件受到损害的可能性仍然存在。

用户拥有的访问权是指对文件的访问权。文件的拥有者和超级用户(Root)可以改动文件中的访问属性，从而对不同的用户给予不同的访问权，例如，让文件拥有者具有读写和执行

的权力，而给其他用户只分配读的权力。

另外，许多日常的管理工作由超级用户来完成，他有很大的权力，所以他的口令一定要保存好，不能共享。

C1 级安全保护的不足之处在于用户能直接访问操作系统的超级用户。C1 级不能控制进入系统的用户的访问级别，所以用户可以将系统中的数据任意移走，他们可以控制系统配置，获取比系统管理员允许的更高权限，如改变和控制用户名。

（2）C2 级安全：C2 级以 C1 级标准为基础，除了具有 C1 级包含的特性外，C2 级系统还具有访问控制环境（Controlled-Access Environment)的权力。该环境具有进一步限制用户执行某些命令或访问某些文件的权限，而且还加入了身份认证级别。另外，系统对发生的事件加以审计(Audit)，并写入日志当中，如什么时候开机，哪个用户在什么时候从哪儿登录等等，这样通过查看日志，就可以发现入侵的痕迹，如多次登录失败，也可以大致推测出可能有人想强行闯入系统。审计除了可以记录下系统管理员执行的活动以外，还加入了身份认证级别，这样就可以知道谁在执行这些命令。

能够达到 C2 级的常见操作系统有：UNIX、XENIX、Novell 3.0、Windows NT 等。

3. B 级安全　B 级安全也叫强制性安全保护，包括三个子级别，即 B1、B2 和 B3。

（1）B1 级安全：B1 级即标志安全保护(Labeled Security Protection)，是支持多级安全(如秘密和绝密)的第一个级别，这个级别说明一个处于强制性访问控制之下的对象(如磁盘或文件服务器目录)，系统不允许文件的使用者修改其许可权限，这种用户标识和加密标志的双重保护，加强了系统信息的安全性。

B1 级的计算机安全措施，视操作系统而定，政府机关和安全承包商们是 B1 级计算机系统的主要拥有者。

（2）B2 级安全：B2 级安全叫做结构保护(Structured Protection)，它要求计算机系统中所有的对象都要加上标签，而且给设备(磁盘、磁带及终端)分配单个或多个安全级别，它是提供较高安全级别的对象与另一个较低安全级别的对象相互通信的第一个级别。

（3）B3 级安全：B3 级安全称做安全域级别(Security Domain)，使用安装硬件的办法来保护域，例如内存管理硬件用于保护安全域免遭无授权访问或其他安全域对象的修改，该级别也要求用户的终端通过一条可信任途径连到该系统上。

4. A 级安全　A 级安全也称验证设计(Verify Design)，是当前桔皮书中规定的最高安全级别，它包含了一个严格的设计、控制和验证过程。与前面提到的各个级别一样，该级别包含了较低级别的所有特性。其设计必须是从数学上经过验证的，而且必须进行对秘密通道和可信任分布的分析。可信任分布(Trusted Distribution)的含义是硬件和软件在传输过程中要受到保护，以防止破坏整个安全系统，即所有部件来源必须有安全保证，在销售和运输过程中受到严密跟踪。

1.5.2　ITSEC 和 C C

TCSEC 桔皮书带动了国际计算机安全的评估研究，20 世纪 90 年代初西欧四国（英国、法国、荷兰、德国）联合提出了信息技术安全评价标准（ITSEC)，ITSEC 又称为欧洲白皮书，它除了吸收 TCSEC 的成功经验外，首次提出了信息安全的保密性、完整性、可用性的概念。他们的工作成为欧共体信息安全计划的基础，并对国际信息安全的研究、实施带来深刻的影响，ITSEC 也定义了 7 个安全级别。

美国为了保持它们在制定准则方面的优势，不甘心 TCSEC 的影响被 ITSEC 取代，它们采取联合其他国家共同提出新的评估准则的办法体现他们的领导作用，1991 年 1 月宣布了制定通用安全评估准则的计划，它的全称是 Common Criteria for IT Security Evaluation（简称 CC）。制定的国家涉及到六国七方，它们是美国的国家标准及技术研究所（NIST）和国家安全局（NSA），欧洲的荷兰、法国、德国、英国，北美的加拿大。CC 标准因为吸收了各先进国家对现代信息系统信息安全的经验与知识，将会对未来信息安全的研究与应用带来重大影响。

1.6 我国计算机网络安全概况

我国在 20 世纪 80 年代特别是进入 20 世纪 90 年代以来，计算机网络应用飞速发展，网络以其独特的优越性日益深入社会各方面并影响到我国的国民经济、政府事务、科研教育事业等各行各业。现实中各种资金、财物和社会资料乃至个人隐私等都转化为计算机数据在网络上流通，网络正在逐步成为整个国家政府机构运转的命脉和社会活动的支柱。

1.6.1 网络安全方面存在的主要困难和问题

我国网络安全面临的主要困难和问题主要存在以下几个方面：

1）计算机应用水平低，资源共享不易，在此基础上构造安全保护体系比较困难。我国的计算机网络工程建设，大都处于各部门自行规划、封闭建设、低水平重复的情况，缺乏统一制定的计算机网络协议标准、规范，造成网络技术落后，互联困难，资源无法共享，在安全方面将影响建立统一的安全保护体系。

2）人才缺乏，特别是高级的系统安全管理人员缺乏。系统安全管理人员是复合型人才，网络的发展需要大批既熟悉专门业务，又精通计算机网络技术，具有丰富网络工程建设经验的工程技术人员、管理人员。而在我国由于计算机及网络技术是一种在近十年内才开始且发展迅速的综合技术领域，没有一定的积累过程，人才非常缺乏，在此基础上，既懂系统管理技术，又熟悉安全技术的系统安全管理人员很少。

3）安全意识薄弱，安全管理不落实。不少部门仍存在“重应用、轻安全”的倾向，缺乏制度或有了制度也没有很好落实。

4）信息服务刚刚起步，如 Internet 服务提供商（ISP）的经营、管理机制尚不够成熟，安全管理机制更是有待建立和健全。

5）安全产品国产化较低，直接影响我国信息主权安全和国家利益，不利于提高我国自主信息安全技术水平的提高。如加密产品历来都是国家安全的组成部分，西方发达国家尤其是美国，一直将加密产品列为出口限制产品，因此，我们的安全产品寄希望于进口既不现实，也极不安全。

1.6.2 我国网络安全技术水平

我国的网络安全技术虽然与世界先进水平有不小的差距，但毕竟已经起步并形成相当的规模，在以下方面与发展中国家相比具有一定的水平。

1．规范网络安全保护及安全产品的管理和检测认证　这方面的工作得到的国家的重视，近年来进展较快，主面有以下几个方面：

1）制定了一系列有关计算机安全的国家标准，并产生了一批有关计算机安全的规范性技术文件。国家标准主要有：《计算机信息系统安全专用产品分类原则》（GA163-1997）、《计

算机机房用活动地板技术条件》(GB6650—1986)、《计算机场地安全要求》(GB/T9361—1988)、《电子设备雷击保护导则》(GB/T7450—1987)、《信息技术设备的无线电干扰》(GB9254—1998)等。有关技术规范性文件有《军用通信设备及系统安全要求》、《军队通用计算机信息系统使用安全要求》等。

2）在计算机信息系统（包括网络）中实行安全等级保护，这已在《中华人民共和国计算机信息系统安全保护条例》中作了规定，1999 年 9 月 13 日，国家质量技术监督局发布了由公安部组织制定的强制性国家标准《计算机信息系统安全保护等级划分准则》，并于 2001 年 1 月 1 日实施，这意味着我国有了自己的等级保护制度，我国计算机网络安全管理构架正在日趋完善。

2．安全产品的研制和生产　近年来计算机网络安全产品的研制与生产在我国已逐步形成产业，主要有网络防火墙、入侵检测系统、计算机病毒防治产品和加密设备等。例如早在 1997 年 4 月 9 日，我国自行研制的网络防火墙“网络卫士”，通过国务院信息化工作领导小组主持的技术鉴定，为我国的网络安全提供了必要的技术手段。计算机病毒防治产品的研制和生产在我国得到迅速发展，1989 年，著名的“小球”病毒侵入我国后，公安部计算机安全监察司研制并免费提供能检测清除“小球”、“大球”等几种病毒的工具软件。随后病毒防治软、硬件迅速作为商品推向市场，至今已是琳琅满目。虽然这些产品与国外产品相比有一些差距，但它们在许多方面比较适合中国的国情，仍是很受欢迎。

1996 年 10 月 19 日，深圳桑达实业股份有限公司与清华大学计算机网络系统组合作研制开发的 SED-08 路由器通过电子部主持的鉴定。SED-08 路由器是我国自行设计开发的产品，它实现了互联、路由、管理、带宽优化、防火墙等功能，达到了国际同档产品先进水平，是国内首次研制成功的具有自主知识产权的路由器产品。

中国科学院信息安全中心与惠普公司合作，建立了“中科院信息安全中心——惠普公司演示中心”，该中心向国内广大用户介绍和演示惠普公司的安全产品，另外双方在信息安全领域达成合作，将在惠普公司的平台上开发出具有中国自主版权的信息安全产品。中国科学院信息安全中心在惠普公司的平台上成功开发了一系列信息安全产品：“智能卡安全平台”、“防火墙”、“代理服务器”和“Internet 安全集成系统”等。

但是在网络安全管理工具、大型加密工具等方面的产品近年还主要是外国公司占据市场。

3．安全研究、学术活动和研究机构　近年来随着计算机网络的普及，计算机安全研究、学术活动也日益活跃。自 1986 年以来，中国计算机安全专业委员会、计算机安全保密学会每年都联合举办一届“全国计算机安全技术交流会”，有力地促进了我国计算机安全管理和技术水平的提高，此外，中国还加入了国际计算机安全技术委员会。

国内有关计算机安全研究机构也相继成立，比较著名的有：中国科学院信息安全技术工程研究中心，中国科技大学研究生院信息安全国家重点实验室等。

中国人民银行对计算机安全从管理到技术进行了系统的研究，两项研究项目被列入国家“八五”重点科技攻关项目并取得成功。

计算机安全技术在我国正通过各种方式日益普及，包括利用 Internet 开设网络安全知识普及的网站，如国家信息中心信息安全处、中国信息协会信息安全专业委员会在网上开设的“中国计算机安全”网站（http://infosec.cei.gov.cn）等。