职业技术教育软件人才培养模式改革项目成果教材

网络安全

吴金龙　蔡灿辉　王晋隆　编

高等教育出版社

职业技术教育软件人才培养模式改革项目成果教材

网络安全

吴金龙　蔡灿辉　王晋隆　编

高等教育出版社

内容提要

本书是职业技术教育软件人才培养模式改革项目成果教材。本书用通俗易懂的语言阐述网络安全所涉及的方方面面的问题。

本书内容主要包括网络安全概述、网络安全基础、黑客攻击与防范、Web 系统安全、网络攻击常见的手段与防御措施、计算机病毒、防火墙技术、数据加密技术与应用、入侵检测系统、无线网络安全和虚拟专用网(VPN)。

本书适合高等职业学校、高等专科学校、成人高校、示范性软件职业技术学院及本科院校举办的二级职业技术学院、继续教育学院以及民办高校使用,也可作为工程技术人员学习网络安全知识的参考书。

图书在版编目(CIP)数据

网络安全/吴金龙,蔡灿辉,王晋隆编. —北京:高等教育出版社,2004.4

ISBN 7-04-013901-4

Ⅰ.网… Ⅱ.①吴…②蔡…③王… 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(2003)第123562号

出版发行	高等教育出版社	购书热线	010-64054588
社　　址	北京市西城区德外大街4号	免费咨询	800-810-0598
邮政编码	100011	网　　址	http://www.hep.edu.cn
总　　机	010-82028899		http://www.hep.com.cn
经　　销	新华书店北京发行所		
印　　刷	北京奥隆印刷厂		
开　　本	787×1092　1/16	版　　次	2004年4月第1版
印　　张	14.5	印　　次	2004年4月第1次印刷
字　　数	340 000	定　　价	18.50元

本书如有缺页、倒页、脱页等质量问题,请到所购图书销售部门联系调换。

职业技术教育软件人才培养模式改革项目成果教材编审委员会

出版说明

信息产业是国民经济和社会发展基础性、战略性产业。加快发展信息技术和信息产业，以信息化带动工业化，以信息化促进工业化，是当前和今后我国产业结构调整发展的战略重点。软件产业是信息产业的核心，加快软件人才培养是加快软件产业发展的先决条件。为适应经济结构战略性调整及软件产业发展的需要，加快培养各类软件应用性人才，在国家改革和发展委员会、教育部的指导和支持下，福建省从2002年开始，在全国率先举办软件类高等职业技术教育，拟以办学模式和人才培养模式改革为重点，积极探索有水平、有质量、有特色的软件高职教育发展的新路子。

在软件类高等职业技术教育改革和建设过程中，福建省坚持教育创新，把改革教学内容和课程体系，加强专业建设、教材建设和教学队伍建设作为工作的重点。目前，根据软件行业发展趋势、就业环境和软件高等职业技术教育的办学特点，经组织专家论证和审定，福建省高校首批开设了可视化编程、Web应用程序设计、软件测试、网络系统管理员、网络构建技术、数据库管理员、图形/图像制作、多媒体制作、计算机办公应用等9个软件高职专业，制订了较为科学合理的人才培养方案。为配合支持软件类高职教育的改革和建设，福建省教育厅聘请软件教育有关专家、学者和著名软件企业的高级工程技术人员成立了“职业技术教育软件人才培养模式改革项目成果教材编审委员会”，以“抓好试点规划，实施精品战略”为指导方针，认真吸取国内外软件技术发展成果，根据软件企业对人才培养提出的新要求和软件高职的办学特点，认真处理好教材的统一性与多样化、基本教材与辅助教材、学历教育教材与认证培训教材的关系，以组织开展软件高职公共基础课、专业基础课和专业主干课教材的建设为重点，同时扩大品种，实现教材系列配套，在此基础上形成特色鲜明、优化配套的软件高等职业技术教育教材体系。

本软件系列教材适用于本科院校、高职高专院校、成人高校及继续教育学院的软件高职类专业及相关专业使用。

职业技术教育软件人才培养模式改革项目成果教材编审委员会

二〇〇三年五月

前　言

随着因特网的普及和发展，人们在享受网络给工作、学习和生活带来便利的同时，也常常会遇到黑客攻击、病毒感染、信息丢失等令人麻烦的事情。因此，计算机网络安全已经在世界许多国家引起特别的重视，成为网络与通信技术、信息安全技术和应用数学等多门学科的研究领域。

由于因特网本身安全性设计的缺陷及其开放性的应用环境，使网络安全变得十分脆弱。一些黑客正是利用网络存在的安全漏洞向网络系统不断地发起攻击。不管黑客或网络攻击者出于何种目的，目前一些黑客的恶意攻击正成为全球新的公害。因此，认识黑客、了解黑客、防御黑客的入侵，从技术上剖析黑客的种种攻击手段，让普通网民，特别是年轻的大学生及网络管理人员对黑客技术和网络安全漏洞有一个大致的了解，从而把因网络安全问题引起的损失降到最低限度，这就是编写本书的目的。需要指出的是，任何对他人网络实施的攻击行为并由此造成的损失，都是我国有关法律所不允许的，攻击者应当承担相应的法律责任。由此可见，网络安全不仅是一个技术问题，更是一个社会问题和法律问题，必须靠全体网民来共同维护。

本书使用通俗易懂的语言，围绕网络安全的各种问题以及解决这些问题的相关技术进行讲述。全书共11章，各章内容如下：

第1章是网络安全概述，包括网络安全的意义和本质、网络安全面临的威胁、网络安全的特性和基本需求、网络安全机制和管理策略、计算机网络安全等级。

第2章介绍网络安全基础，包括因特网的安全缺陷、TCP/IP协议的IP安全机制、TCP/IP协议的TCP安全机制、UDP协议和UDP安全性分析。

第3章介绍黑客攻击与防范，包括因特网上的踩点、因特网上的扫描、Windows NT/2000的查点、UNIX的查点、BGP路由器的查点。

第4章介绍网络操作系统安全，包括Windows 9x的安全、Windows NT的安全、Windows 2000的安全、UNIX的安全。

第5章介绍Web系统安全，包括Web技术概述、CGI的安全、IIS与ASP的安全、Web体系结构与安全性。

第6章介绍网络攻击常见的手段与防御措施，包括拒绝服务攻击、欺骗攻击、电子邮件攻击。

第7章介绍计算机病毒，包括计算机病毒概述、病毒原理及检测方法、宏病毒、网络病毒、典型病毒介绍、常用反病毒软件产品介绍。

第8章介绍防火墙技术，包括防火墙的基本概念、防火墙的攻击与防范、现代防火墙安全技术。

第9章介绍数据加密技术与应用，包括数据加密概述、DES密码算法、RSA密码算法、鉴别、PGP数据加密系统。

第10章介绍入侵检测系统，包括入侵检测系统概述、入侵检测系统的应用问题、入侵检测系统的产品及其发展趋势。

第11章介绍无线网络安全和VPN，包括无线通信网络概述、无线网络常见的弱点及攻击手段、无线网络安全对策、虚拟专用网络。

本书第1章～第6章、第9章～第11章由吴金龙编写；第7章由王晋隆编写；第8章由蔡灿辉编写；全书由吴金龙统稿。在本书的编写过程中，还得到了王美珍老师、傅金枝老师和韩秋锋、鲁斌、陈荣鑫等研究生的帮助，在此向他们表示感谢。

本书涉及的许多网络安全案例，来自编者自己的教学实践并参考了大量书籍、文献，在此向上述书籍、文献的作者表示感谢。

本书面向高职高专学生，也可供大学本科网络安全的教学人员和其他工程技术人员参考。由于编者水平有限，书中可能存在疏漏或不足之处，请专家和读者批评指正。

编者 于泉州国立华侨大学

2003年10月

目　录

第1章　网络安全概述

学习目标

- 正确理解网络安全的意义和本质
- 掌握网络安全面临的各种威胁
- 熟悉网络安全的基本需求
- 熟练掌握网络安全机制和管理策略
- 了解计算机网络安全等级

在信息化社会中，随着计算机网络与通信的发展和普及，人们以网络方式获取信息、储存信息和交流信息的活动越来越多，网络的重要性和对社会的影响也越来越大。特别是因特网的出现，电子商务、网络教育和各种新兴业务的兴起，使人类社会再也离不开网络了。网络正在逐步改变人们的工作方式和生活方式，成为当今社会发展的一个重要特征。

正当人们在惊喜计算机网络带来的开放性、共享性、可靠性和便捷性的同时，利用计算机网络进行犯罪的活动却层出不穷。它已严重地危害社会的发展和国家的安全。因此，网络通信和信息安全已经成为信息科学的一个重要研究领域，日益受到人们的关注。

网络安全是一门涉及计算机科学、网络技术、通信技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性技术。网络安全的实现不仅要靠先进的技术，而且要靠严格的安全管理、严肃的法律制约和普及的安全教育。因此，从普及安全知识的角度出发，本章要讲述的内容包括：

- 网络安全的意义和本质
- 网络安全面临的威胁（重点）
- 网络安全的基本需求
- 网络安全机制和管理策略（难点）
- 计算机网络安全等级

1.1　网络安全的意义和本质

网络安全是一个涉及社会、国家、企业和个人生活的方方面面的重要问题。网络安全从其本质上来讲，就是网络上硬件设备和信息系统的安全。随着因特网的普及和发展，社会生活节奏的

加速，信息本身就等同于时间、财富、生命和生产力。现代社会的一个重要特征，就是信息的网络化，谁破坏了网络，谁就破坏了信息；反过来说，谁保护了网络，谁就保护了信息。因此，从广义角度理解，凡是涉及网络信息的保密性、完整性、可用性、真实性以及可控性的相关技术和理论都是网络安全所要研究的问题。从国家和社会的角度看，网络安全关系到国家的主权和声誉、社会的繁荣和稳定、民族文化的继承和发扬等一系列重大问题；从企业和个人的角度看，网络安全涉及个人隐私、商业利益和品牌声誉等无形资产不受侵犯的严重问题。在电子商务时代，保护这些无形资产甚至比保护有形资产还要重要。试想，如果一个员工到处散布关于“某公司的网络遭到攻击，所有资料全部被毁”的消息，那将会造成什么样的影响?! 信息有时候比金子还贵，信息可以将一个企业毁掉，也可以救活一个企业。当然，如果花在保护信息方面的金钱比信息的成本还要高，那么有谁愿意花费100万美元去保护20万美元的东西呢?

网络安全不是一件孤立的事情。实质上安全是相对的，不安全是绝对的。安全只是人、规章制度和技术的完美结合，是三者之间相互作用的最高点。安全是一个过程，不是一个产品。总之，安全是一种“买不到”的东西。即插即用并提供足够安全的体系是不存在的。但是，制定一个安全的规章制度，采用安全的防护设备，雇用安全技术素质高的人员，建立一个安全的防护体系，却是每个单位的计算机网络管理人员和网络用户必须选择的安全通道。

网络安全教育的目的关系到两个方面的问题。一是如何正确看待网络安全漏洞，增强安全意识，消除对网络的恐惧感；二是积极对待网络安全的公开性讨论。安全与不安全因素的斗争，实际上是多种技术的较量。安全问题的最终解决在于提高人的道德素质和防范意识，自觉抵制利用计算机进行各类犯罪活动的诱惑。将网络安全建立在法律约束之下的自律行为的基础上，才是实现网络安全的根本出路。

1.2 网络安全面临的威胁

“威胁”是指尚未发生但只要发生就会造成伤害或损失的事件。计算机网络所面临的威胁有三种：硬件安全、软件安全和数据安全。硬件包括网络中的各种设备及其元配件、接插件及线缆等；软件包括网络操作系统、各种驱动程序、通信软件及其他应用软件；数据包括系统的配置文件、日志文件、用户资料、各种重要的敏感数据库及其网络上两台机器之间的通信内容等机密信息。

影响网络安全的因素很多。有些因素是人为的，有些因素是非人为的。人为的因素又可以分为无意的失误和恶意的攻击。非人为的因素包括自然灾害如地震、雷击、洪水或其他不可抗拒的天灾。此外，网络设备的自然损坏、硬盘或其他存储设备的老化、无规则的停电引起的设备故障等。这种安全威胁只破坏信息的完整性和可用性，无损信息的秘密性。人为的无意失误包括误操作引起的文件删除、硬盘被格式化，或者掉电引起的系统中断、崩溃；由于网络管理员技术素质不高，安全访问权限分配不当造成的漏洞；用户安全意识不强，口令设置不妥或随意与他人共享网络资源等不良习惯都会给网络安全带来威胁。人为的恶意攻击，往往来自企业之间的网络间谍和网上黑客等，这才是计算机网络安全面临的最大威胁。这些人的攻击和计算机犯罪行为又可以分为两类。一类是主动攻击，它以各种手段有选择地破坏信息的完整性和可用性；另一类

攻击是被动攻击，它以各种方式截获、窃取或破译网络重要的机密信息，虽然它不影响网络的正常工作，但将导致机密信息的严重泄露。网络操作系统、网络编程软件的各种缺陷和漏洞，恰好又成为这些人进行攻击的首选目标。

有时候，信息的泄露原因并非是人为造成的，也不是敌人发现了什么安全漏洞。真正的原因是计算机网络设备工作时所产生的电磁发射，它包括辐射和传导发射。这两种电磁发射可被高灵敏度的接收设备接收并进行分析还原。因此，计算机网络设备和信息安全应当符合瞬时电磁脉冲辐射标准(TEMPEST)。20 世纪 80 年代，美国已将此标准用于生产军用通信设备中。

还有，网络用户可能在不知不觉中造成显示器因静电产生很高的电压，击穿大规模集成电路，或者产生放电火花，酿成火灾。

总之，计算机网络的安全因素是错综复杂的，正如一场火灾的原因一样，可能是雷电引发的；也可能是管理人员操作不当或乱扔烟头引起的；还有可能是电气设备老化或老鼠咬破导线引发的短路现象导致的火灾；当然，也不能排除人为故意放火的犯罪行为。

综上所述，网络安全面临的威胁因素如图 1-1 所示。

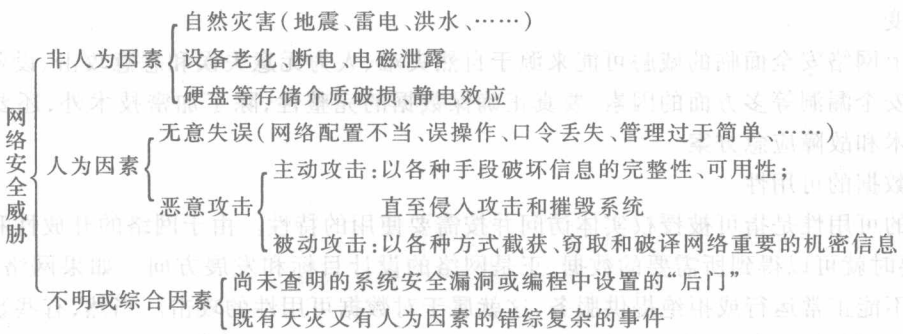

图 1-1 网络安全面临的威胁因素分析

1.3 网络安全的特性和基本需求

1.3.1 网络安全的特性

众所周知，计算机网络不同于一般的单机系统。网络安全不同于一般的计算机系统安全。在某种程度上，封闭性、独占性有利于保证系统信息的安全。但是，计算机网络设备的互联性、网络资源的共享性、网络技术的开放性、网络应用的灵活性、从根本上决定了网络系统是不安全的。从网络发展历史看，网络安全和信息安全并未得到充分的考虑。目前使用的网络协议 TCP/IP 及其相应的网络安全产品，主要有两大类：开放型(如数据加密)及被动防卫型(如防火墙)。它们是根据网络安全的基本需求而设计和应用的。

1.3.2 网络安全的基本需求

(1) 数据的保密性

由于网络系统无法确认是否有未经授权的用户截取数据或非法使用数据,这就要求使用某种手段对数据进行保密处理。数据保密可以分为网络传输保密和数据存储保密。对机密敏感的数据使用各种加密技术,将明文转换为密文,只有经过授权的合法用户才能利用密钥将密文还原成明文。反之,未经授权的用户无法获得所需信息。这就是数据的保密特性。

此外,网络管理员通过配置不同数据的访问模式,也可以防止非法用户对敏感数据的存取。既不能访问,也不能利用相关的数据。

(2) 数据的完整性

数据的完整性是指数据未经授权不能进行改变的特性。在网络传输和存储的过程中,系统必须保证数据不被篡改、破坏和丢失。因此,网络系统要有某种安全机制来确认数据在此过程中没有被改变。

实际上网络安全面临的威胁可能来源于自然灾难、人为无意失误和恶意攻击、设备故障或不可预测的安全漏洞等多方面的因素,要真正确保数据的完整性,除了加密技术外,还要使用多种预防性技术和故障应急方案。

(3) 数据的可用性

数据的可用性是指可被授权实体访问并按需要使用的特性。由于网络的开放性和资源的共享性,需要时就可以得到所需要的数据,正是网络的设计目标和发展方向。如果网络遭受攻击,造成系统不能正常运行或拒绝提供服务,这就属于对数据可用性的攻击。当然,有些数据是要求付费才能被调用的一种“有偿服务”数据。

(4) 数据的可控性

数据的可控性是指在其控制授权范围内具有信息流向及行为方式的控制能力。这种控制能力体现在三个方面:

首先,采用访问控制表对用户访问系统或网络上的数据加以授权,不同级别的用户权力不同。

其次,通过握手协议和数据加密方式进行身份验证,确保用户身份的真实性。

最后,对用户所有的网络活动记录在案,以便为事故的预测、报警、原因查询、定位以及实时处理提供可靠依据;或者为正常操作进行统计、计费等审计。合法用户不能否认自己做出的行为或曾收到的信息。系统的资源不被非法占有,或者免遭病毒破坏,都是数据安全链条不可缺少的一环。

1.4 网络安全机制和管理策略

根据网络安全的基本需求,可以采用如下安全机制,并制定相应的管理策略。

1.4.1 网络安全机制

网络安全机制各种各样,但最常见的有以下几种:

(1) 数据加密机制

数据加密是网络安全的核心技术。加密技术不仅应用于数据的存储和传输的过程中,而且应用于程序的执行中。软件的安全主要依靠良好的加密措施。

网络中的数据加密,除了选择加密算法和密钥外,主要问题是选择采用何种加密方式,是链路层加密、结点间加密还是端对端加密。实际上,OSI 协议的多个层次上都可以实现数据加密。加密算法可分为对称密钥算法和非对称密钥算法。对称密钥属于单密钥体制,即加密密钥和解密密钥相同。如按操作和运算的方法不同,它又可分为序列密码或流密码(stream cipher)算法和分组密码算法两种。序列密码每次运算一位,分组密码(block cipher)每次运算一分组。分组长度越长密码的可靠性越高。公开密钥加密,即非对称密钥算法,使用两把密钥,一把公开密钥用于加密,一把私人密钥用于解密。它解决了分组密码加密方法中复杂的密钥分发问题,简化了密钥的管理。

加密算法除了提供信息的保密性之外,还能与其他技术相配合,例如 Hash 函数,以便保证数据的完整性。公开密钥加密技术可有效地增强加密强度和抗分析破译的能力。

(2) 访问控制机制

访问控制机制是按事先确定的规则防止未经授权的用户或用户组非法使用系统资源。当一个用户企图非法访问未经授权的资源时,系统访问控制机制将拒绝这一企图,并向审计跟踪系统报告,审计系统发出报警并形成部分追踪审计信息。

访问控制可分为高层访问控制和低层访问控制。高层访问控制通过检查用户口令、用户权限和资源属性加以实现;低层访问控制则通过通信协议中的某些特征信息进行识别和判断,例如路由器上的数据包过滤规则,就是阻止非法用户的访问控制。

(3) 数据完整性机制

数据完整性包括两种形式:数据单元的完整性和数据单元序列的完整性。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或篡改。保证数据单元完整性的一般做法是发送方在有数字签名的文件上用单向哈希(Hash)函数产生一个标记,接收方在收到文件后,也用相同的 Hash 函数处理一遍。如果接收方与发送方产生的标记相同,就可以确定在传输过程中数据没有被修改过,保持了完整的数据。

数据单元序列的完整性是指发送方在发出数据前,应将数据分割为按序列号编排的许多单元数据,待数据传输到接收方时还能依照原有的序列,保持序列编号的连续性和时间标记的正确性。这样,就可以防止丢失、重复、乱序或假冒数据单元的情况产生。

同样,数据在存储过程中也应保持完整未损状态。

(4) 数字签名机制

数字签名机制是对数据加密机制和数据完整性机制的重要补充,也是解决网络通信安全问题的有效方法。数字签名机制涉及下列问题:

· 否认 发送方事后不承认自己曾发送过某份文件或答应过某件事。接收方也可否认自己

曾接收某份文件或做过某件事。

· 伪造 接收方伪造某份文件,声称它来自发送方。

· 冒充 网上某个用户冒充别人的身份收发信息。

· 篡改 接收方私自篡改发送方发出的信息内容。

数字签名机制保证数据具有可证实性(authentic)、不可否认性(nonrepudiated)、不可伪造性(unforgeable)和不可重用性(unreusable)。通常人们通过辨别相貌、声音和笔迹来确定某个人的身份,获取手稿上的签名图章等作为证据,但在网络上,原始的方法却不可行。因此,数字签名机制显得格外重要。

(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认双方彼此的身份。交换鉴别技术有多种,常见的方法有三类:

· 口令鉴别

发送方提供口令以证明自己的身份,接收方根据口令以检测对方的身份。

· 数据加密鉴别

将交换的数据加密后进行传送,只有合法的用户才能通过自己掌握的密钥解密,得出明文并确认发送方是掌握另一个密钥的人。有时候,数据加密常与时间标记、同步时钟、双方或多方握手协议、数字签名和公证机构等配合使用,以使身份鉴别更加可靠。

· 实物属性鉴别

利用通信双方的固有特征或所拥有的实物属性进行身份鉴别。例如指纹识别、声谱识别、身份卡识别等。

(6) 流量填充机制

流量填充机制主要用于对付窃听者的流量分析。攻击者常常通过网络中某一路径的信息流量和流向的变化,判断将会发生的某些事件,或从中提取军事上、商业上的敏感信息。为了对付这种攻击,在某些站点间持续地传送一些伪随机数据,以保持信息流量的基本稳定。

流量填充机制包括掩盖通信的频度、报文的长度、报文的格式和报文的地址。为了掩盖报文地址,一般采用物理层的链路加密方式,而伪报文的发送可在网络高层协议中实现。为了掩盖报文的格式,常采用带反馈的加密方式,并使所有报文都扩充到同一长度。

(7) 路由控制机制

在广域网中,特别是因特网中的通信,路由控制机制可以使信息的发送方选择特殊的路由,以保证数据安全。路由控制机制实际上就是控制信息的流向。这种控制,可以由用户提出申请,在自己的程序中设计安全路由标志;也可以由网络安全控制机构在检测出不安全路由后,通过动态调整路由表,选择安全的路径。

(8) 公证机制

公证机制的设立是为了解决通信双方由于诚信问题产生的纠纷,同时也便于解决由于系统故障引起的信息丢失、破坏或延误等有关的责任问题。通常需要有一个各方都能信任的仲裁机构,以确保双方的争执获得公平的解决。

为使公证机构得到必要的信息,通信各方的信息交换都必须由公证机构进行中转。显然,公证机构本身的安全可靠性和诚实可信度又必须处于严格的控制之中。