



北京市高等教育精品教材立项项目

计算机网络安全

计算机网络技术
与应用系列教材

Network Security

戴 红 王海泉 黄 坚 编著



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

<http://www.phei.com.cn>

北京市高等教育精品教材立项项目

计算机网络技术与应用系列教材

计算机网络安全

Network Security

戴 红 王海泉 黄 坚 编著

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

本书全面系统地介绍计算机网络安全的基本概念、基本状况、基本理论与原理、基本技术及其实现方法。主要内容包括：加密技术（包括对称加密技术、不对称加密技术和单向哈希函数），数字签名的实现，密钥管理技术，网络攻击关键技术，身份认证技术，防火墙技术，入侵检测技术，VPN 技术等安全技术，以及与 Internet 提供的主要服务（WWW 服务、电子邮件服务、电子商务服务）相关的安全问题，网络操作系统 Windows NT、Windows 2000 和 UNIX 的安全性问题，计算机病毒基础知识及常规病毒防治方法，数据备份系统的组成、设备选择、备份方式及常用备份实施方法，网络管理的相关概念及网络管理协议——简单网络管理协议等内容。

本书以注重实用为原则，将理论知识与实际技术实现相结合，力图做到易懂、易学、易用。本书可作为高等院校高职高专、本科计算机及相关专业的课程教材，也可供网络工程、网络管理、信息管理等相关领域的工程技术人员参考。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有，侵权必究。

图书在版编目（CIP）数据

计算机网络安全/戴红，王海泉，黄坚编著. —北京：电子工业出版社，2004.9

（计算机网络技术与应用系列教材）

ISBN 7-121-00273-6

I. 计… II. ①戴…②王…③黄… III. 计算机网络—安全技术—高等学校—教材 IV. TP393.08

中国版本图书馆 CIP 数据核字（2004）第 086339 号

责任编辑：冉 哲

印 刷：北京大中印刷厂

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

经 销：各地新华书店

开 本：787×980 1/16 印张：14.25 字数：312 千字

印 次：2004 年 9 月第 1 次印刷

印 数：5 000 册 定价：18.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zltz@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

丛 书 序

网络技术的飞速发展,带来了全球信息资源与技术不可逆转的网络化发展趋势。网络技术对人类的影响是全方位、多层次的,以计算机网络技术为核心的计算机应用已广泛渗透到各个行业,成为影响科技、经济和文化发展的核心因素,并使社会的生产方式、工作方式乃至生活方式都发生了深刻变化。

随着网络应用的普及和网络技术的不断发展,网络人才的需求量与日俱增,网络人才的培养也日益受到关注。进入 21 世纪,无论从全球经济一体化对人才需求的角度看,还是从企业核心技术岗位向网络技术和信息技术迅速提升的角度看,根据网络技术应用人才的需要以及按职业特定要求设计课程的人才培养模式的需要,使发展网络技术应用型高等职业教育势在必行。然而,目前所用教材多为国外版教材的引进与翻译,现有的国内版教材在适用性、新颖性、系统性方面也有一定的局限性,真正适用于我国高等职业教育,适用于培养高素质技术应用型人才,将网络技术、基础知识与专业技能紧密结合教学模式的教材尚不多见。为此,尽快出版一套适用于计算机网络技术高等职业教育人才培养模式的教材成为当务之急。

作为北京市高等教育“十五”发展规划中“精品教材工程”的组成部分之一,《计算机网络技术与应用系列教材》于 2001 年底立项,2002 年开始启动。本系列教材主要包含以下内容:《Windows NT 网络系统管理教程》,《网络数据库技术》,《TCP/IP 网络技术(基于 Windows 2000)》,《计算机网络安全》和《网络信息资源管理与检索》。在编写过程中,我们以培养技术应用能力和职业素质教育为主线,力争打破以理论教学为本位、为目标、为标准的普通高等教育的教学模式,建立真正以培养技术应用型人才为目标的高等职业教育教学模式,以能力为本位设计教材体系和教学内容,尽量避免理论内容过于追求系统性、完整性、严密性的现象,以及实践内容演示性多而实际操作少、高新技术含量低的现象,加强实训教学内容,各章均设置实训内容,以强化技术应用能力的培养。整套教材力求思路清晰、结构合理、内容丰富、资料翔实,既反映和吸收本专业领域的最新进展,又融入我们自己的研究成果,使之具有较强的科学性、新颖性和实用性。

概括来说,本系列教材的特色之处表现在:

① 根据首都经济发展需要,配合北京市高职高专重点、试点专业的建设,遵循新的教育理念和办法,填补高职、高专计算机网络技术专业教材的空白。

② 计算机网络技术的发展日新月异,硬件不断升级换代,软件产品层出不穷,为了适应网络技术飞速发展的需要,全面更新教材内容和学科体系,增强教学内容的新颖性、针对性、应用性、实用性,以适应 21 世纪计算机网络技术发展对人才与知识结构提出的新要

求,具有较强的新颖性和时代气息。

③ 面向计算机网络技术高等职业技术教育,使专业基础课和专业主干课教材配套。

本系列教材的作者都是具有多年网络技术应用实践经验和教学经验的中青年教师,这套书不仅是他们多年实践教学改革经验的总结,也是他们最新研究成果的结晶。

本系列教材既适合于高等院校、成人教育、高职高专院校的计算机网络技术、计算机应用、信息管理与信息系统等专业作为教材使用,也可供计算机网络技术自学者学习参考。

本系列教材能列入“北京市高等教育精品教材立项项目”并及时出版,要衷心感谢市教委领导的大力支持,衷心感谢电子工业出版社领导及编辑的大力支持与积极配合。

限于认知和水准,书中可能存在疏漏和失当之处,敬请专家、学者及各位读者海涵斧正。

饶伟红

2002年11月

前 言

随着计算机网络技术的广泛应用和飞速发展,计算机信息网络已成为现代信息社会的基础设施。它作为进行信息交流、开展各种社会活动的基础工具,已深入到人们工作和生活当中。同时,计算机安全问题也随之日益突出,计算机病毒扩散、网络黑客攻击、计算机网络犯罪等违法事件的数量迅速增长。安全问题已成为人们普遍关注的问题。

本书是“北京市高等教育精品教材立项项目”——《计算机网络技术与应用系列教材》中的一本。本书分5大部分共10章。第1部分为概述。其中第1章介绍计算机网络安全的基本概念、基本术语,目前网络系统自身的不安全因素及所面临的威胁,主要防范措施和策略,以及计算机网络安全的评价和管理标准。第2部分为密码学。其中第2章介绍密码学基础知识,包括对称加密技术、不对称加密技术和单向哈希函数3种加密技术,以及数字签名的实现和密钥管理技术的基本概念和方法。第3部分为网络安全。其中第3章介绍网络攻击技术的基本原理和关键技术;第4章介绍现有网络安全技术所能解决的问题和适用情况,以及身份认证技术、防火墙技术、入侵检测技术、加密/解密技术、VPN技术及其他安全技术的基本概念和实现方法;第5章介绍WWW服务、电子邮件服务、电子商务服务的工作原理和安全机制及它们存在的安全问题和解决防护策略,并描述了安全电子交易模型及其工作过程;第6章介绍网络管理的相关概念及目前广泛运用的网络管理协议——简单网络管理协议。第4部分为系统安全。其中第7章介绍网络操作系统Windows NT、Windows 2000和UNIX系统的安全性及如何进行基本的安全设置;第8章介绍计算机病毒的基础知识及常规的病毒防治方法;第9章介绍数据备份的概念、方法及企业和个人用户的数据备份策略。第5部分为无线网络安全。其中第10章对无线网络的基本概念、基本安全技术、安全漏洞及安全措施进行了简单阐述。为了配合教学,本书在每章后都附有复习题和实训题,以巩固学习效果。

本书由北京联合大学应用文理学院教师戴红编写第1章、第5章、第7章和第10章,由北京航空航天大学软件学院教师王海泉、黄坚分别编写第2章、第3章、第4章、第6章和第8章、第9章,全书由戴红审核统稿。在本书的编写过程中,得到了北京市高等教育精品教材指导委员会和北京联合大学应用文理学院教材指导委员会的大力支持,在此表示衷心感谢。

由于作者水平有限,时间仓促,书中难免会有错误和不妥之处,恳请读者批评指正。

作 者
2004年8月

目 录

第 1 部分 概 述

第 1 章 计算机网络安全概述	(2)
1.1 计算机网络安全简介	(2)
1.2 计算机网络所面临的威胁	(6)
1.2.1 人为威胁	(6)
1.2.2 非人为威胁	(8)
1.3 计算机网络安全的主要研究内容	(9)
1.3.1 安全措施的研究	(9)
1.3.2 主要计算机网络安全产品介绍	(10)
1.3.3 安全管理的研究	(11)
1.4 计算机网络安全技术和策略	(13)
1.4.1 安全技术	(13)
1.4.2 安全策略	(16)
1.5 计算机网络安全评价准则、管理标准和法律法规	(17)
1.5.1 评价准则	(17)
1.5.2 管理标准	(24)
1.5.3 法律法规	(24)
习题 1	(28)

第 2 部分 密 码 学

第 2 章 密码学基础	(30)
2.1 密码学	(30)
2.2 对称加密	(31)
2.2.1 基本概念	(31)
2.2.2 数据加密标准 DES 算法	(33)
2.2.3 实用软件介绍	(37)
2.3 不对称加密	(40)
2.3.1 基本概念	(40)
2.3.2 RSA 算法	(41)
2.4 单向哈希函数	(43)
2.5 数字签名	(44)

2.6 密钥管理	(45)
2.6.1 数字证书	(45)
2.6.2 认证中心	(46)
2.6.3 PKI 简介	(47)
习题 2	(48)

第3部分 网络安全

第3章 系统攻击及网络入侵模式	(50)
3.1 安全隐患的产生	(50)
3.2 网络入侵技术简介	(52)
3.2.1 网络入侵	(52)
3.2.2 网络入侵技术介绍	(53)
3.3 系统入侵一般模式	(55)
3.4 一次入侵过程	(57)
习题 3	(60)
第4章 网络安全技术	(61)
4.1 身份认证技术	(61)
4.1.1 个人特征的身份证明技术	(61)
4.1.2 一次一密认证机制	(62)
4.1.3 Kerberos 认证系统	(62)
4.1.4 X.509 认证系统	(64)
4.2 访问控制技术	(65)
4.2.1 访问控制分类	(66)
4.2.2 访问控制应用类型	(67)
4.3 防火墙技术	(68)
4.3.1 防火墙基本功能	(68)
4.3.2 防火墙分类	(69)
4.3.3 防火墙使用环境	(69)
4.3.4 ISA 防火墙的安装、配置和管理	(73)
4.4 入侵检测技术	(79)
4.4.1 入侵检测系统分类	(79)
4.4.2 入侵分析技术	(81)
4.4.3 入侵检测工具介绍	(82)
4.5 其他技术介绍	(84)
习题 4	(85)
第5章 Internet 应用的安全性分析	(86)
5.1 WWW 的安全性分析	(86)

5.1.1 概述	(86)
5.1.2 Web 的安全性	(88)
5.1.3 WWW 客户端安全性	(88)
5.2 电子邮件的安全性	(92)
5.2.1 电子邮件系统原理	(92)
5.2.2 电子邮件服务的安全性	(93)
5.2.3 电子邮件安全协议	(95)
5.2.4 通过 Outlook Express 发送安全电子邮件	(97)
5.2.5 加密软件 PGP	(98)
5.3 电子商务安全	(104)
5.3.1 电子商务概述	(104)
5.3.2 安全电子交易	(105)
习题 5	(108)
第 6 章 网络管理的原理与实现	(109)
6.1 网络管理基本概念	(109)
6.1.1 网络管理概述	(109)
6.1.2 网络管理系统的模型和要素	(110)
6.2 简单网络管理协议	(111)
6.2.1 概述	(111)
6.2.2 命令和报文	(112)
6.2.3 管理信息数据库	(113)
6.2.4 SNMP 存在的安全问题	(114)
6.2.5 防范基于 SNMP 的远程扫描	(117)
习题 6	(118)

第 4 部分 系统安全

第 7 章 网络操作系统的安全性分析和管理	(120)
7.1 Windows NT 的安全性	(120)
7.1.1 Windows NT 的安全体系	(120)
7.1.2 Windows NT 的安全漏洞及安全设置	(124)
7.2 Windows 2000 的安全性	(128)
7.2.1 Windows 2000 的安全体系	(128)
7.2.2 Windows 2000 的安全隐患	(131)
7.2.3 Windows 2000 的安全策略和配置	(132)
7.3 UNIX 的安全性	(147)
7.3.1 UNIX 的安全体系	(147)
7.3.2 UNIX 的基本安全设置及安全管理	(149)

习题 7	(157)
第 8 章 计算机病毒及其防治	(158)
8.1 计算机病毒基础知识	(158)
8.1.1 计算机病毒的概念	(158)
8.1.2 计算机病毒的产生背景	(158)
8.1.3 计算机病毒的发展简史	(159)
8.1.4 计算机病毒的特征	(162)
8.1.5 计算机病毒的表现形式	(164)
8.1.6 计算机病毒的技术分析	(165)
8.2 计算机病毒防治知识	(170)
8.2.1 预防计算机病毒感染	(170)
8.2.2 反病毒技术及产品	(171)
8.2.3 灾后重建	(181)
习题 8	(182)
第 9 章 数据备份技术	(183)
9.1 数据备份概述	(183)
9.1.1 数据失效	(184)
9.1.2 备份	(185)
9.2 企业数据备份方案设计	(187)
9.2.1 数据备份需求分析	(187)
9.2.2 备份系统的组成	(188)
9.2.3 存储设备	(188)
9.2.4 备份服务器及备份软件	(190)
9.2.5 数据备份方式	(191)
9.3 个人数据的备份	(192)
9.3.1 个人数据备份设备和软件	(192)
9.3.2 Windows 2000 自带的备份功能	(193)
9.3.3 Norton Ghost 2003 软件的使用方法	(196)
习题 9	(202)

第 5 部分 无线网络安全

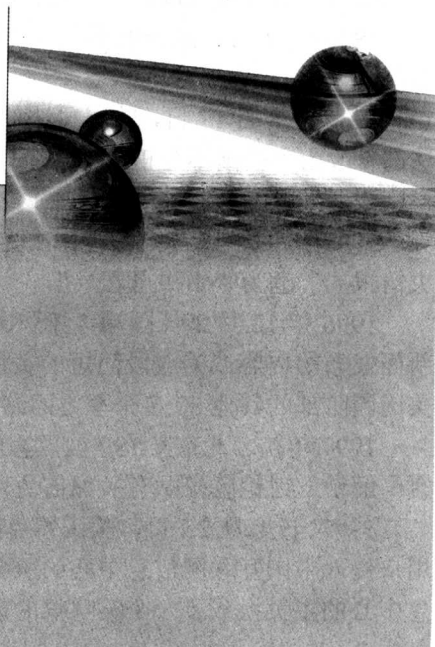
第 10 章 无线网络安全技术	(204)
10.1 概述	(204)
10.1.1 无线网络的定义	(204)
10.1.2 无线网络技术	(205)
10.1.3 无线局域网的组成	(206)

10.2 无线网络安全基本技术.....	(207)
10.2.1 访问控制.....	(207)
10.2.2 数据加密.....	(209)
10.3 无线网络安全问题.....	(210)
10.3.1 无线网络安全隐患.....	(210)
10.3.2 无线网络安全措施.....	(211)
习题 10.....	(212)
附录 A 计算机网络安全技术资源.....	(213)
参考文献.....	(216)

当今世界处于信息时代，计算机和信息技术的发展成为这个时代前进的主要推动力之一。随着计算机和信息技术的发展，特别是计算机网络技术的发展和广泛应用，计算机系统的安全、信息的安全及网络系统的安全问题正越来越受到人们的普遍关注。尤其是在人们享受着网络带来的资源共享和信息交换便利的同时，也承受着因人为的蓄意攻击、人为的失误和自然灾害等不安全因素所造成的损失、混乱和破坏。在网络系统下的信息安全问题已成为社会各界所关注的热点问题。

第 1 部分

概 述



第1章 计算机网络安全概述

本章介绍计算机网络安全的基本概念、基本术语,列举目前计算机网络系统自身的不安全因素及其所面临的威胁,对计算机网络安全的研究内容进行探讨。另外,还介绍目前计算机网络安全所采取的主要防范措施和策略,以及计算机网络安全的评价、管理标准和相关法律法规。

1.1 计算机网络安全简介

作为信息时代的主角——信息已成为人类最宝贵的资源之一,经济的发展、社会的进步、国家的安全都越来越依赖于对信息资源的占有和保护。而以 Internet 为代表的网络系统已成为承载、传播信息的主要媒体。网络的开放性、自由性和全球性使我们在最大限度拥有信息的同时,也为如何确保网络系统的安全以及其上的信息自身的安全,提出了新的课题。我们来看一些数据。

1996 年初,美国旧金山的计算机安全协会与联邦调查局在一次联合调查统计中称:有 53%的企业受到过计算机病毒的侵害,42%的企业的计算机系统在过去的 12 个月被非法使用过。而五角大楼的一个研究小组称美国一年中遭受的攻击就达 25 万次之多。

1996 年 2 月,刚开通不久的 CHINANET 受到某高校的一个研究生的攻击,且攻击得逞。

1996 年 8 月 17 日,美国司法部的网络服务器遭黑客入侵,并将其主页上的“美国司法部”改为“美国不公正部”,将司法部部长的照片换成了阿道夫·希特勒,将司法部徽章换成了纳粹党徽。

1996 年 9 月 18 日,黑客再次光顾美国中央情报局的网络服务器,将其主页上的“中央情报局”改为“中央愚蠢局”。

1996 年 12 月 29 日,黑客侵入美国空军的全球网网址,将其主页中有关空军介绍、新闻发布等内容改为一段简短的黄色录像,并声称美国政府所说的一切都是谎言,迫使美国国防部的其他 80 多个军方网站一度关闭。

1997 年初,北京某 ISP 被黑客成功侵入,并在清华大学“水木清华”BBS 站的“黑客与解密”讨论区张贴有关如何免费通过该 ISP 进入 Internet 的文章。

1997 年 4 月 23 日,美国得克萨斯州内查德逊地区西南贝尔互联网公司的某个 PPP 用户侵入中国互联网信息中心的服务器,破译该系统的 ShutDown 账户,把中国互联网信息中心的主页换成了一个笑嘻嘻的骷髅头。

2000年3月,攻击者针对Microsoft(微软)的以色列网站发起了一次拒绝服务型攻击。

2000年3月,美国中央情报局主管未否认名为ECHELON的大规模情报收集系统的存在。

2000年,包括微软的Internet Explorer 5.0、ISS(互联网安全系统)公司的RealSecure网络入侵检测软件在内的多种软件被公布存在缺陷和漏洞。

2001年,我国有73%的计算机曾感染病毒,到了2002年上升到近84%,2003年上半年又增加到85%。而微软的官方统计数据称,2002年因网络安全问题给全球经济造成的直接损失高达130亿美元。

2003年8月12日,一种叫做“冲击波”的计算机病毒开始袭击计算机用户,有数字统计表明,至少有数十万台计算机受到袭击。

.....

这些数字可谓触目惊心。人类发展史上技术最先进、破坏最严重的安全问题在网络上威胁着人们的工作和生活。

1. 信息系统安全的6大基本要素

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等的综合性学科。网络安全是一个内涵丰富的概念,从不同的角度和不同的应用环境有不同的解释。本质上来说,网络安全就是网络系统上的信息安全。信息系统的安全性应包括以下6个基本要素。

1) 保密性

保密性是指确保信息不暴露给未授权的人或程序。换句话说,信息除拥有者和被授权使用的人外,其他人不能有意或无意地获取。某些信息,如个人私有信息和企业内部资料、有关政府和国家的机密等,对保密性的要求尤为重要。

2) 完整性

完整性也称真实性,是指只有得到授权的人或程序才能修改数据,同时能够识别数据是否已经被修改。当信息在网络上存储、传输时,确保不被有意或无意地插入、删除、修改、伪造、重排、重放等。交通运输、金融贸易等应用场合中信息的完整性若遭受破坏,就可能会造成重大的经济损失。

3) 可用性

可用性是指得到授权的人或程序可以按照需要访问数据,即使在网络部分受损或需要降级使用时,仍能为授权用户提供有效服务。

4) 可控性

可控性是指可以控制授权范围内的信息流向及行为方式,对网络信息的传播及内容具有控制能力。用户对网络信息系统所提供的服务具有随机性、实时性和多角度等要求,网络系统除了能够对用户的身份进行识别及确认外,还应对用户的访问

权限和方式进行控制。

5) 可靠性

可靠性是指网络信息系统能够在规定条件下和规定的时间内完成规定功能的特性，是系统安全的最基本要求之一，是所有网络信息系统的建设和运行目标。可靠性主要表现在硬件可靠性、软件可靠性、人员可靠性、环境可靠性等方面。硬件可靠性最为直观和常见。软件可靠性是指在规定的时间内，程序成功运行的概率。人员可靠性是指人员成功地完成工作或任务的概率。人员可靠性在整个系统可靠性中扮演重要角色，因为系统失效的大部分原因是人为差错造成的。因此，人员的教育、培养、训练和管理以及合理的人机界面是提高可靠性的重要方面。环境可靠性是指在规定的环内，保证网络成功运行的概率。这里的环境主要是指自然环境和电磁环境。

6) 可审查性

可审查性是指对出现的网络安全问题提供调查的依据和手段。其最为重要的组成特点之一就是不可抵赖性，也称为不可否认性，是指在网络信息系统的信息交互过程中，确信参与者的真实同一性，即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。用户在系统进行某项运作后，若事后能提出证明，而无法加以否认，便具备不可否认性。

2. 计算机网络安全的定义

计算机网络安全是计算机安全概念在网络环境下的扩展。因此，在介绍计算机网络安全以前首先需要了解计算机安全的基本概念。

1) 计算机安全

国际标准化组织曾建议将计算机安全定义为：“计算机系统受到保护，计算机系统的硬件、软件、数据不被偶然或故意地泄露、更改和破坏。”计算机网络安全可以分为实体安全、运行安全和信息安全3个方面。

- 实体安全包括环境安全、设备安全和媒体安全3个方面。
- 运行安全包括风险分析、审计跟踪、备份与恢复、应急处理4个方面。
- 信息安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密和鉴别7个方面。

2) 计算机网络安全

计算机网络安全（简称网络安全）是指网络系统的硬件、软件及其系统中的数据受到保护，不被偶然或者恶意地破坏、更改、泄露，系统连续可靠地正常运行，网络服务不中断。对于一般用户而言，是指保证其在网络上的私人信息或商业信息内容的安全保密性和完整性；对于网络运行和管理者而言，网络安全的侧重点为信息处理和传输系统的安全性、网络信息的可用性和可控性；对于安全保密部门而言，则注重的是信息的机密性和可控性；而从社会、道德和教育的角度来说，对网络信息内容的可控性，是目前要解决的主要问题。

总之，凡涉及到网络上信息的保密性、完整性、可用性、可控性和可审查性及网络

系统自身的可靠性的相关技术和理论都是网络安全所要研究的领域。其涉及层面包含技术和管理两个方面,技术方面主要侧重于防范外部非法用户的攻击,管理方面则侧重于内部人为因素的管理。

在评估网络的安全性时,因其是计算机安全概念在网络环境下的扩展,所以往往要先假设其安全性完全依赖于计算机系统的安全性,再根据计算机系统安全性的准则确定网络的安全级别。

在1989年提出的ISO 7498—2标准中,ISO提出了层次型的安全体系模型结构(如图1.1所示),成为网络安全的经典模型。

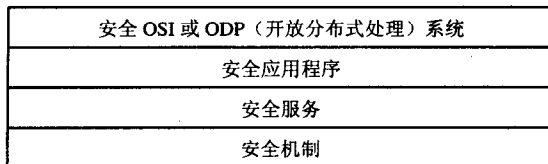


图 1.1 ISO 安全体系的层次模型

3. 计算机网络安全的发展过程

自第一代电子计算机出现以来,随着计算机技术的发展和应用领域的扩大,计算机系统及其相关系统的安全性问题逐渐引起人们的注意。

20世纪50年代,计算机尚未普及,安全问题并未受到重视。

到了20世纪70年代,计算机得到广泛应用。一些重要信息开始采用计算机来处理,开始出现以窃取信息为目的的计算机犯罪,人们开始意识到安全的重要性,研究并制定了一系列的计算机安全法律、法规和防护手段。1976年,美国学者提出的公开密钥密码体制在克服了网络信息系统密钥管理困难的同时,解决了数字签名问题,并可用于身份认证,它是当前研究的热点。1977年,美国国家标准局(NBS)颁布了国家数据加密标准(DES)。

20世纪80年代,美国国防部基于军事计算机系统的保密需要,在20世纪70年代的基础理论研究成果——计算机保密模型(Bell & Lapadula模型)的基础上,制定了《可信计算机系统评价准则》(TCSEC),形成了安全信息系统体系结构的最早原则。

20世纪90年代以来,计算机网络安全问题得到进一步的深化。英、法、德、荷4国提出了包括保密性、完整性、可用性概念在内的“信息技术安全评价准则”(TISFC)。

近年来,6国7方(美国国家安全局和国家技术标准研究所、加、英、法、德、荷)共同提出了《信息技术安全评价通用准则》(The Common Criteria for Information Technology Security Evaluation,简称通用准则或CC)。CC综合了国际上已有的评审准则和技术标准的精华,给出了安全评价的框架和原则要求。

1.2 计算机网络所面临的威胁

网络系统正面临着各种各样的危险。攻击者的目的有很多种，例如，造成整个系统瘫痪，造成间歇停机，造成随机数据差错，盗窃大量信息，盗用服务，进行非法监视和收集情报，引入假电文和提取数据用于欺诈等。

目前，计算机网络系统所面临的威胁主要表现为两大类。

1.2.1 人为威胁

1. 人为的无意失误

1) 安全配置不当造成的安全漏洞

系统管理员设置资源访问控制的失误，会导致一些资源被偶然或故意地破坏。另外，用户安全意识不强、口令选择不慎、将自己的账号随意转借或与别人共享等都会给网络安全造成威胁。

2) 无意的信息泄露

合法用户进入安全进程后中途离开而给非法用户提供可乘之机，口令密钥等保管不善而为他人非法获得，造成网络信息保密性的破坏。

3) 操作失误

删除文件、格式化硬盘、线路拆除等操作失误，系统掉电、“死机”等系统崩溃引起信息缺失，从而造成网络信息完整性和可用性的破坏。

2. 人为的恶意攻击

这是计算机网络所面临的最大威胁，对手的攻击和计算机犯罪同属此类。此类攻击又可以分为两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性，是纯粹的信息破坏。这类积极攻击者通常截取网上信息包，对其进行更改使之失效，或者故意篡改信息，或者登录系统占用大量网络资源从而导致资源消耗，损害合法用户的利益。这类攻击者的破坏作用最大。另一种是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息，这类攻击者称为消极攻击者。两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄露。人为恶意攻击具体可表现在以下几个方面。

1) 非授权访问

未经同意而使用网络或计算机资源被看做非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或者擅自扩大权限，越权访问信息等。其主要表现形式有：假冒，身份攻击，非法用户进入网络系统进行违法操作，合法用户以未授权方式进行操作等。