免费提供电子教案

高等院校规划教材

信息管理与信息系统系列

网络与信息安全技术

陈广山　等编著

机械工业出版社
CHINA MACHINE PRESS

高等院校规划教材·信息管理与信息系统系列

网络与信息安全技术

陈广山　等编著

机 械 工 业 出 版 社

本书从网络与信息安全技术出发，介绍计算机网络安全的基本理论，常用的信息安全技术及安全措施。全书共分10章，主要内容包括网络信息安全概论、黑客与攻击技术、计算机病毒、信息加密与鉴别技术、防火墙与入侵检测技术、操作系统的安全、Web的安全、数据与数据库安全、网络信息安全工程以及实验。

本书理论与实验并重，所涉及的各项技术都配有相应的实验。为了突出实验的实用性和可操作性，本书所用的工具都可在Internet上免费获得。本书每章都配有习题，以指导读者深入地进行学习。

本书可作为高等学校计算机及相关专业的教材，也可作为信息安全及管理人员的参考书。

图书在版编目(CIP)数据

网络与信息安全技术/陈广山等编著. —北京：机械工业出版社，2007.7
(高等院校规划教材·信息管理与信息系统系列)
ISBN 978-7-111-21822-7

Ⅰ.网… Ⅱ.陈… 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(2007)第099943号

机械工业出版社(北京市百万庄大街22号 邮政编码100037)
责任编辑：张宝珠
责任印制：杨 曦
三河市国英印务有限公司印刷
2007年7月第1版·第1次印刷
184mm×260mm·17.25印张·426千字
0001－5000册
标准书号：ISBN 978-7-111-21822-7
定价：25.00元

凡购本书，如有缺页，倒页，脱页，由本社发行部调换
销售服务热线电话：(010)68326294
购书热线电话：(010)88379639 88379641 88379643
编辑热线电话：(010)88379739

出版说明

计算机技术的发展极大地促进了现代科学技术的发展，明显地加快了社会发展的进程。因此，各国都非常重视计算机教育。

近年来，随着我国信息化建设的全面推进和高等教育的蓬勃发展，高等院校的计算机教育模式也在不断改革，计算机学科的课程体系和教学内容趋于更加科学和合理，计算机教材建设逐渐成熟。在“十五”期间，机械工业出版社组织出版了大量计算机教材，包括“21世纪高等院校计算机教材系列”、“21世纪重点大学规划教材”、“高等院校计算机科学与技术‘十五’规划教材”、“21世纪高等院校应用型规划教材”等，均取得了可喜成果，其中多个品种的教材被评为国家级、省部级的精品教材。

为了进一步满足计算机教育的需求，机械工业出版社策划开发了“高等院校规划教材”。这套教材是在总结我社以往计算机教材出版经验的基础上策划的，同时借鉴了其他出版社同类教材的优点，对我社已有的计算机教材资源进行整合，旨在大幅提高教材质量。我们邀请多所高校的计算机专家、教师及教务部门针对此次计算机教材建设进行了充分的研讨，达成了许多共识，并由此形成了“高等院校规划教材”的体系架构与编写原则，以保证本套教材与各高等院校的办学层次、学科设置和人才培养模式等相匹配，满足其计算机教学的需要。

本套教材包括计算机科学与技术、软件工程、网络工程、信息管理与信息系统、计算机应用技术以及计算机基础教育等系列。其中，计算机科学与技术系列、软件工程系列、网络工程系列和信息管理与信息系统系列是针对高校相应专业方向的课程设置而组织编写的，体系完整，讲解透彻；计算机应用技术系列是针对计算机应用类课程而组织编写的，着重培养学生利用计算机技术解决实际问题的能力；计算机基础教育系列是为大学公共基础课层面的计算机基础教学而设计的，采用通俗易懂的方法讲解计算机的基础理论、常用技术及应用。

本套教材的内容源自致力于教学与科研一线的骨干教师与资深专家的实践经验和研究成果，融合了先进的教学理念，涵盖了计算机领域的核心理论和最新的应用技术，真正在教材体系、内容和方法上做到了创新。另外，本套教材根据实际需要配有电子教案、实验指导或多媒体光盘等教学资源，实现了教材的“立体化”建设。本套教材将随着计算机技术的进步和计算机应用领域的扩展而及时改版，并及时吸纳新兴课程和特色课程的教材。我们将努力把这套教材打造成为国家级或省部级精品教材，为高等院校的计算机教育提供更好的服务。

对于本套教材的组织出版工作，希望计算机教育界的专家和老师能提出宝贵的意见和建议。衷心感谢计算机教育工作者和广大读者的支持与帮助！

机械工业出版社

前　言

今天，网络已经成为人们生活不可缺少的一部分，网络信息系统也给企事业组织和个人带来了很大的方便。但是病毒和黑客等不安全因素却给网络造成了相当的威胁，网络安全已经成为一个不容忽视的社会问题。本书的目的是帮助读者理解信息安全的重要意义，了解信息安全的基础知识，掌握安全防范的常用安全技术、策略和方法。

全书共分 10 章。第 1 章对信息安全的基本概念、威胁网络信息安全的因素、网络安全的基本原则、信息安全的等级和标准、信息安全法规及信息安全的发展趋势等内容进行了介绍。第 2 章首先介绍了黑客的概念和黑客守则，然后对常用的黑客攻防技术进行了说明，主要包括扫描、监听、缓冲区溢出、拒绝服务、IP 欺骗、Web 欺骗和木马等技术。第 3 章讲述了计算机病毒的概念、特征、分类、基本原理以及计算机病毒的检测和防范等知识。第 4 章介绍了信息加密的发展过程、传统和现代信息加密技术，主要介绍了 DES 和 RSA 算法的基本原理和实现方法；同时对鉴别技术也进行了介绍，主要对数字签名、数字证书、身份认证等内容进行了重点介绍。第 5 章主要介绍了防火墙和入侵检测系统的基本概念、技术、原理和发展趋势等内容。第 6 章对常用操作系统的安全进行了讲述，包括 Windows 2000 Server、UNIX、Linux 常见的漏洞、基本安全措施、安全策略以及安全配置等基础知识。第 7 章对 Web 的安全性进行了研究，主要对服务器的安全和客户端的安全进行了介绍，并对 Web 中常见的安全问题进行了分析。第 8 章对数据和数据库的安全问题和安全机制进行了简单介绍。第 9 章主要介绍网络信息安全工程，针对目前企业信息系统、电子政务和电子商务中的安全问题进行了分析。第 10 章为实验，主要针对信息安全中的常用技术应用和常用工具的使用方法进行了介绍，目的是使读者清楚信息安全是一个具体的问题，是一个具有可操作性的现实问题。

本书第 10 章中所介绍的实验都在 Windows 2000 Server 网络环境下成功实现，相应的工具都可从 Internet 上免费获得。为了使学生加深对基本知识的理解和掌握，每章后附有习题，书末附有部分习题的参考答案。

参加本书编写的还有白雪、肖玉兰、张伟、高明东。

书中难免存在不妥之处，请读者原谅，并提出宝贵意见。需要本书课件的读者，请到 http://www.cmpbook.com 下载。

编　者

目　录

第1章　网络信息安全概论

21世纪是一个信息文明的新世纪，信息技术已经成为一个国家的政治、军事、经济和文教等事业发展的决定因素。但是，目前的网络环境中却蛰伏着诸多不安全的因素，信息文明还面临着许多威胁和风险，网络信息安全问题业已成为制约信息化发展的瓶颈，是事关一个国家生存和发展的重要问题，其重要性随着全球信息化进程的加快而显得越来越重要。

本章是网络与信息安全的引导篇，将主要介绍网络信息安全的基本概念、基本原则、安全体系结构、安全等级与标准、安全法规和网络安全现状与展望等知识，使读者掌握必要的网络与信息安全基础知识，理解信息安全的重要意义，提高信息安全意识。

1.1　网络信息安全

信息系统是指互相连接起来的独立自主的计算机信息系统的集合。计算机信息系统是由计算机及其相关的和配套的设备、设施构成的，并按一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。今天的信息系统已由传统意义上的存放和处理信息的独立系统演变为互相连接、资源共享的系统的集合。也就是说，信息系统同时也是一个网络系统。安全问题是信息系统的研究和应用中必须要解决的问题，具有重要的理论和现实意义。

1.1.1　网络信息安全概念

网络信息系统促进了科学、技术、文化、教育等事业的快速发展，给人类的生产、生活带来了极大的方便，信息技术也自然地嵌入到政治、军事、经济文化和社会活动之中。然而，目前的网络信息系统还存在着各种各样不容忽视的安全问题，它是一个关系到国家安全和主权、社会稳定、民族文化的继承和发扬的重要问题。

1. 网络信息安全的定义

网络信息安全是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多学科的边缘学科。从广义上讲，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络信息安全所要研究的领域。通用的定义为：网络信息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，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统能够连续、可靠、正常地运行，网络服务不中断。

2. 网络信息安全的含义

值得注意的是，网络信息安全是一个相对的概念，是指在信息安全期内保证其在传输和存储时不被非法访问。绝对的安全是不存在的，其意义与所保护的对象有关，在不同的环境会有不同的解释。

(1) 信息系统安全

信息系统安全即信息处理和传输系统的安全。包括计算机机房环境的保护，法律、政策的

保护，计算机结构设计上的安全考虑，硬件系统的可靠、安全运行，操作系统和应用软件的安全，数据库系统的安全，电磁信息泄露的防护等。它侧重于保证系统正常的运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免由于电磁泄露而产生信息泄露、干扰他人或受他人干扰。其本质是保护系统的合法操作和正常运行。

(2) 系统信息安全

系统信息安全包括用户口令鉴别，用户存取权限控制，数据存取权限、方式控制，安全审计，安全问题跟踪，计算机病毒防治，数据加密等。

(3) 信息传播安全

信息传播安全主要指传播后果的安全，包括信息过滤、不良信息的过滤等，侧重于防止和控制非法、有害信息传播产生的后果，避免在公共信道上信息传输时产生信息失控的现象，以维护信息道德、法律和国家的利益。

(4) 信息内容安全

信息内容安全侧重于保护信息的保密性、真实性和完整性。避免攻击者利用系统的安全漏洞进行窃听、假冒、诈骗等有损于合法用户的行为，以保护用户的利益和隐私。

可见，如果从普通用户、网络管理员、安全保密部门、教育以及社会意识形态等不同的角度来理解，网络信息安全的含义也会有差别。本书所涉及的网络信息安全的含义是通过各种计算机、网络、加密技术和信息安全技术，保护在公共通信网络中传输、交换和存储的信息的机密性、完整性和真实性，并对信息的传播及内容具有控制能力。

1.1.2 网络信息安全的特征

1. 保密性

保密性是指信息不被泄露给非授权的用户、实体或进程，不被非法利用。信息的保密性包括传输过程中的保密性和存储时的保密性。

数据在传输过程中可以被窃听和分析，这就需要用加密技术对原始明文进行处理，加密后的密文能够保证在传输、使用和转换的过程中不被第三方非法获取，即使获取了也无法破解，只有掌握解密密钥的合法用户才能将其恢复成明文，从而确保数据的保密性；存储时的保密性可以通过访问控制来实现，管理员可以根据不同的数据类型和应用需求，对用户和数据进行分类，设置成不同的访问模式。

2. 完整性

完整性是指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不被非法修改、破坏和丢失，并且能够判别出数据是否已被改变。其目的是保证信息系统上的数据处于一种完整和未受损的状态，不会因有意或无意的事件而被改变或丢失。一旦数据的完整性不保，则其可用性必将丧失。

数据的完整性可通过访问控制、数据备份和冗余设置来实现。

3. 可用性

可用性是指可被授权实体访问并按需求使用的特性，即当需要时授权者总能够存取所需要的信息，攻击者不能占用所有的资源而妨碍授权者的使用。拒绝服务攻击、病毒等都可以破坏数据的可用性。

其中，按需使用可通过认证和鉴别技术来实现，以保证每个实体的真实、可靠性，但要确保

实时、正常的服务似乎是不太可能的，除了备份和冗余设置技术以外，目前还没有找到更有效的办法。

4. 不可否认性

不可否认性(也称不可抵赖性)是对通信双方信息真实性的安全要求，信息行为人要对自己的行为负责，即通信双方均不可抵赖。包括：源发证明，它给信息接收者提供证据，使发送者谎称未发送过这些信息或者否认它的内容的企图不能得逞；交付证明，它给信息发送者提供证据，使接收者谎称未接收过这些信息或者否认它的内容的企图不能得逞。

不可否认性通常用数字签名技术来实现。

5. 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，对信息的传播及内容具有控制能力。

可控性可通过访问控制等技术来实现。

1.1.3 网络信息安全技术

1. 主动防御技术

(1) 数据加密

加密技术被认为是解决网络安全问题的最好途径，是目前最有效的数据保护的手段。

(2) CA 认证

CA 中心是具有权威性和公正性的第三方信任机构，采用 PKI 公共密钥基础架构技术，提供网络身份认证服务，确保通信双方的真实、可靠。

(3) 访问控制

访问控制主要分为自主访问控制和强制访问控制两种，即通过身份认证来控制用户对资源的访问和通过规定主体对客体的操作权限来保证信息的安全。

(4) 虚拟网络技术

使用 VPN 或 VLAN 技术，通过网段的划分、控制数据流向等手段来实现防范的目的。

(5) 入侵检测技术

入侵检测是使用软件(或硬件)技术监视和分析网络信息系统中发生的事件，当系统受到攻击时，它可以检测出来并做出积极的响应。

2. 被动防御技术

(1) 防火墙技术

防火墙是一种置于可信网络与不可信网络之间的安全防御系统，可以认为是一种访问控制机制，用于控制非授权的访问进出防火墙。

(2) 安全扫描

可自动检测远程或本地主机安全弱点的程序，用于观察网络的工作情况、收集主机的信息。

(3) 密码检查器

通过口令验证程序检查薄弱的口令。

(4) 安全审计

在网络信息系统中有记录与安全相关事件的日志文件，可供日后调查、分析、追查有关不

信任的人，发现系统安全的弱点和漏洞等。

(5) 路由过滤

路由器中的过滤器对所接收的每一个数据包根据包过滤规则做出允许或拒绝的决定。

(6) 安全管理技术

通过制定规章制度和条例等安全策略来减少人为因素对网络信息系统的影响。

1.2 威胁网络信息安全的因素

1.2.1 物理威胁

1. 偷窃

网络信息安全中的偷窃包括设备偷窃、信息偷窃和服务偷窃等内容。如果计算机中有黑客感兴趣的信息，那么他们就可以采用将计算机偷走的办法，或者通过监视器偷窥计算机中的信息。偷窃攻击比网络入侵更直接，而且容易得多。

2. 废物搜寻

废物搜寻是指在被扔掉的打印材料、废弃软盘等废物中搜寻所需要的信息。在计算机中，还包括从未抹掉有用信息的软盘、硬盘，甚至从光盘上获得有用的资料，除非物理上对其进行粉碎。

3. 身份识别错误

非法建立文件或记录，企图把它们作为有效的、正式生产的文件或记录。如对具有身份鉴别特征的物品(如护照、执照、出生证明或加密的安全卡)进行伪造，属于身份识别发生错误的范畴。这种行为对网络数据构成了巨大的威胁。

4. 间谍行为

间谍行为是为了省钱或获取有价值的机密，采用不道德的手段来获取信息的一种行为。

1.2.2 漏洞威胁

1. 不安全服务

由于缺陷或错误使系统本身存在漏洞，这些问题可能导致一些服务程序绕过安全系统，从而对信息系统造成不可预料的损失。

2. 配置和初始化错误

服务器的关闭或重新启动可能是不可避免的，当服务器启动时系统要重新初始化，如果安全系统没有随之正确的初始化，就会留下安全漏洞而被人利用。类似的问题在木马程序修改了系统的安全配置文件时也会发生。

3. 乘虚而入

计算机之间的通信是通过特定的端口来实现的。如在 FTP 服务中，用户暂时停止了与某个系统的通信，但由于该端口仍处于激活状态，那么，其他用户就可以乘虚而入，利用这个端口与这个系统通信，这样就会绕过例行的申请和安全检查程序。

1.2.3 身份鉴别威胁

1. 口令圈套

口令圈套是网络安全的一种诡计，与冒名顶替有关。常用的口令圈套通过一个编译代码模块来实现，它运行起来和登录屏幕一模一样，被插入到正常的登录过程之前，最终用户看到的只是先后两个登录屏幕，第一次登录失败了，所以用户被要求再输入用户名和口令。实际上，第一次登录并没有失败，它将登录数据（如用户名和口令）写入到这个数据文件中，留待使用。

2. 口令破解

口令破解就是通过某种策略对口令进行分析和猜测，在该领域中已形成许多能提高成功率的技巧。

3. 编辑口令

编辑口令需要依靠操作系统漏洞。如果企业内部的人，建立了一个虚设的账户或修改了一个隐含账户的口令，那么，任何知道那个账户的用户名和口令的人便可以访问该主机了。

4. 算法考虑不周

口令验证系统必须在满足一定的条件下才能正常工作，这个验证过程需要通过某种算法来实现。如果算法考虑不周全，验证的过程和结果就不可靠，以前就曾发生过入侵者采用超长的字符串破解口令算法，从而成功地进入网络信息系统的案例。

1.2.4 有害程序威胁

1. 病毒

病毒是一种把自己的拷贝附着于其他正常程序上的一段代码。通过这种方式，病毒可以进行自我复制，并随着它所附着的程序在网络及计算机之间传播。

2. 特洛伊木马

特洛伊木马是一种远程控制工具，一旦被安装到某台主机上，该主机便可以被监视和控制。特洛伊木马可以在该主机上上传、下载文件，偷窥私人文件、密码及口令信息，甚至能够摧毁数据。中了特洛伊木马的主机，其一切秘密都会暴露在别人面前，隐私将不复存在。

3. 代码炸弹

代码炸弹是一种具有杀伤力的代码，当满足预设的条件时，代码炸弹就被触发并产生破坏性结果。代码炸弹不会像病毒那样四处传播，程序员将代码炸弹写入软件中，使其产生一个不能被轻易找到的安全漏洞，一旦该代码炸弹被触发后，只有该程序员能解除，因此他可以借此勒索和敲诈，甚至有时受害者并不知道他们被敲诈了，即便他们有疑心也无法证实自己的猜测。

1.2.5 网络连接威胁

1. 窃听

对通信过程进行窃听可达到收集信息的目的，通过检测从连线上发射出来的电磁辐射就能拾取所要的信号。为了使机构内部的通信有一定的保密性，可以使用加密技术来防止信息被解密。