工业和信息化普通高等教育“十二五”规划教材

21世纪高等教育计算机规划教材

COMPUTER

信息安全技术与应用

Technology and Application of Information Security

彭新光 王峥 主编

张辉 郭昊 朱晓军 编著

- 知识体系全面——基本理论、原理、技术、应用和典型案例
- 教材内容丰富——信息安全保障法规、标准与核心技术应用
- 培养工程技能——集成、配置、评估、维护和开发保障系统

人民邮电出版社
POSTS & TELECOM PRESS

工业和信息化普通高等教育“十二五”规划教材
21世纪高等教育计算机规划教材

COMPUTER

信息安全技术与应用

Technology and Application of Information Security

彭新光 王峥 主编
张辉 郭昊 朱晓军 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

信息安全技术与应用 / 彭新光，王峥主编 ；张辉，郭昊，朱晓军编著. -- 北京 ：人民邮电出版社，2013.3
21世纪高等教育计算机规划教材
ISBN 978-7-115-30247-2

Ⅰ. ①信… Ⅱ. ①彭… ②王… ③张… ④郭… ⑤朱… Ⅲ. ①信息安全－高等学校－教材 Ⅳ. ①G203

中国版本图书馆CIP数据核字(2013)第015149号

内 容 提 要

本书从信息安全基础理论、工作原理、技术应用和工程实践多个方面对信息安全技术进行了全面与系统的介绍，内容覆盖了当前信息安全领域的核心技术，包括信息安全概述、密码技术、身份认证、访问控制、防火墙、攻击技术分析、入侵检测、病毒防治、安全通信协议、邮件系统安全和无线网络安全。书中介绍的各种信息安全技术可直接应用于网络信息系统安全保障工程。

本书采用理论、原理、技术和应用为主线的层次知识体系撰写风格，不仅可作为高等院校计算机、软件工程、物联网工程、网络工程、电子商务等相关专业教材，也适用于信息安全技术培训或信息安全工程技术人员使用。

21 世纪高等教育计算机规划教材

信息安全技术与应用

◆ 主　　编　彭新光　王　峥
编　　著　张　辉　郭　昊　朱晓军
责任编辑　邹文波

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京鑫正大印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：17.75　　2013 年 3 月第 1 版
字数：462 千字　　2013 年 3 月北京第 1 次印刷

ISBN 978-7-115-30247-2

定价：35.00 元

读者服务热线：(010)67170985　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前　言

随着网络应用的普及和信息化建设的快速推进，网络基础设施与信息系统已经渗透到社会的政治、经济、文化、军事、意识形态和社会生活的各个方面。特别是随着近年来电子商务、电子政务、办公自动化和企事业单位信息化建设的飞速发展，网络攻击、计算机病毒、特洛伊木马、网络窃听、邮件截获、滥用特权等各种恶意行为频繁发生。针对重要信息资源和网络基础设施的蓄意破坏、篡改、窃听、假冒、泄露、非法访问等入侵行为对国家安全、经济和社会生活造成了极大的威胁，因此，信息安全已成为当今世界各国共同关注的焦点。我国网络基础设施和信息系统安全保障建设远滞后于信息化发展，尽管安全意识不断增强，但缺乏信息安全防护措施。特别是国家强制实施信息安全等级保护工作以来，越来越多的相关专业技术人员需要学习和掌握信息安全技术与应用技能。

信息安全是一个涉及计算机科学、网络技术、软件工程、通信技术、密码技术、法律、法规、管理、教育等多个领域的复杂系统工程。本书按照信息安全基础理论、工作原理、技术应用和工程实践层次体系结构组织教学内容。对当前信息安全领域的核心技术进行了全面与系统地介绍，内容包括信息安全概述、密码技术、身份认证与访问控制、防火墙工作原理及应用、攻击技术分析、入侵检测系统、病毒防治、安全通信协议、电子邮件系统安全和无线网络安全。在强调基础理论和工作原理的基础上，注重安全解决方案、选择、集成、配置、评估、维护和管理信息安全保障系统的工程实践技能。为方便读者学习、分析、设计和实践信息安全技术，多数应用实例均取自优秀的信息安全开源项目。在撰写风格上力求做到深入浅出、概念清晰和通俗易懂。

此外，本书配有电子课件，教师可以根据课时需要进行裁减。本书配套的教学课件可从人民邮电出版社教学服务与资源网（www.ptpedu.com.cn）免费下载。

本书由彭新光和王峥任主编，负责全书体系结构、内容范围、撰写风格的制订以及统稿、编著等组织工作，全书由陈俊杰教授主审。全书共分 10 章，其中第 1 章、第 6 章、第 10 章由彭新光编写，第 2 章、第 5 章、第 7 章由王峥编写，第 3 章由郭昊编写，第 4 章、第 8 章由张辉编写，第 9 章由朱晓军编写。

在编写此书的过程中，邀请了多位信息安全企业专家审定教学内容，他们提供了许多建设性意见。陈俊杰教授认真审阅了全书，提出了许多宝贵修改意见。冯秀芳教授和李海芳教授对本书的编写也给予了大力支持和热心帮助，谨向他们表示衷心的感谢。

尽管编著者尽心尽力编写各章内容，但信息安全技术涉及的知识面十分广泛，书中难免存在一些缺点和错误，恳请广大读者批评指正。

编著者

2012 年 12 月

目　录

第1章 信息安全概述

随着 Internet 迅猛发展和网络社会化的到来，网络已经无所不在地影响着社会的政治、经济、文化、军事、意识形态和社会生活的各个方面。同时在全球范围内，针对重要信息资源和网络基础设施的入侵行为和企图入侵行为的数量仍在持续不断增加，网络攻击与入侵行为对国家安全、经济和社会生活造成了极大的威胁。因此，信息安全已成为世界各国当今共同关注的焦点。

1.1 信息安全基本概念

1.1.1 信息安全定义

安全在字典中的定义是为防范间谍活动或蓄意破坏、犯罪、攻击而采取的措施，将安全的一般含义限定在网络与信息系统范畴，信息安全就是为防范计算机网络硬件、软件、数据偶然或蓄意破坏、篡改、窃听、假冒、泄露、非法访问和保护网络系统持续有效工作的措施总和。

1. 信息安全保护范围

信息安全、网络安全与计算机系统安全和密码安全密切相关，但涉及的保护范围不同。信息安全所涉及的保护范围包括所有信息资源，计算机系统安全将保护范围限定在计算机系统硬件、软件、文件和数据范畴，安全措施通过限制使用计算机的物理场所和利用专用软件或操作系统来实现。密码安全是信息安全、网络安全和计算机系统安全的基础与核心，密码安全是身份认证、访问控制、拒绝否认和防止信息窃取的有效手段。信息安全、网络安全、计算机系统安全和密码安全的关系如图 1.1 所示。

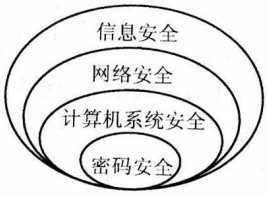

图 1.1 信息安全保护范围

2. 信息安全侧重点

事实上，信息安全也可以看成是计算机网络上的信息安全，凡涉及网络信息的可靠性、保密性、完整性、有效性、可控性和拒绝否认性的理论、技术与管理都属于信息安全的研究范畴，只是不同人员或部门对信息安全关注的侧重点有所不同。信息安全研究人员更关注从理论上采用数学方法精确描述安全属性，通过安全模型来解决信息安全问题。信息安全工程人员从实际应用角度对成熟的信息安全解决方案和新型信息安全产品更感兴趣，他们更关心各种安全防范工具、操作系统防护技术和安全应急处理措施。信息安全评估人员较多关注的是信息安全评价标准、安全等级划分、安全产品测评方法与工具、网络信息采集以及网络攻击技术。网络安全管理或信息安全管理人员通常更关心信息安全管理策略、身份认证、访问控制、入侵检测、网络与系统安全审计、信息安全

应急响应、计算机病毒防治等安全技术，因为他们负责配置与维护网络信息系统在保护授权用户方便访问信息资源的同时，必须防范非法访问、病毒感染、黑客攻击、服务中断、垃圾邮件等各种威胁，一旦系统遭到破坏、数据或文件丢失后，能够采取相应的信息安全应急响应措施予以补救。对国家安全保密部门来说，必须了解网络信息泄露、窃听和过滤的各种技术手段，避免涉及国家政治、军事、经济等重要机密信息的无意或有意泄露；抑制和过滤威胁国家安全的反动与邪教等意识形态信息传播，以免给国家造成重大经济损失，甚至危害到国家安全。对公共安全部门而言，应当熟悉国家和行业部门颁布的常用信息安全监察法律法规、信息安全取证、信息安全审计、知识产权保护、社会文化安全等技术，一旦发现窃取或破坏商业机密信息、软件盗版、电子出版物侵权、色情与暴力信息传播等各种网络违法犯罪行为，能够取得可信的、完整的、准确的、符合国家法律法规的诉讼证据。军事人员则更关心信息对抗、信息加密、安全通信协议、无线网络安全、入侵攻击、网络病毒传播等信息安全综合技术，通过综合利用信息安全技术夺取网络信息优势；扰乱敌方指挥系统；摧毁敌方网络基础设施和信息系统，以便赢得未来信息战争的决胜权。也许最关注信息安全问题的是广泛使用计算机及网络的个人或企业用户，在网络与信息系统为工作、生活和商务活动带来便捷的同时，他们更关心如何保护个人隐私和商业信息不被窃取、篡改、破坏和非法存取，确保网络信息的保密性、完整性、有效性和拒绝否认性。

1.1.2 信息安全目标

信息安全的最终目标就是通过各种技术与管理手段实现网络信息系统的可靠性、保密性、完整性、有效性、可控性和拒绝否认性。可靠性（reliability）是所有信息系统正常运行的基本前提，通常指信息系统能够在规定的条件与时间内完成规定功能的特性。可控性（controllability）是指信息系统对信息内容和传输具有控制能力的特性。拒绝否认性（no-repudiation）也称为不可抵赖性或不可否认性，是指通信双方不能抵赖或否认已完成的操作和承诺，利用数字签名能够防止通信双方否认曾经发送和接收信息的事实。在多数情况下，信息安全更侧重强调网络信息的保密性、完整性和有效性。

1. 保密性

保密性（confidentiality）是指信息系统防止信息非法泄露的特性，信息只限于授权用户使用。保密性主要通过信息加密、身份认证、访问控制、安全通信协议等技术实现，信息加密是防止信息非法泄露的最基本手段。口令加密可以防止密码被盗，保护密码是防止信息泄露的关键。如果密码以明文形式传输，在网络上窃取密码是一件十分简单的事情。事实上，大多数信息安全防护系统都采用了基于密码的技术，密码一旦泄露，就意味着整个安全防护系统的全面崩溃。机密文件和重要电子邮件在 Internet 上传输也需要加密，加密后的文件和邮件即使被劫持，尽管多数加密算法是公开的，但由于没有正确密钥进行解密，劫持的密文仍然是不可读的。此外，机密文件即使不在网络上传输，也应该进行加密；否则，窃取密码就可以获得机密文件。对机密文件加密可以提供双重保护。

2. 完整性

完整性（integrity）是指信息未经授权不能改变的特性，完整性与保密性强调的侧重点不同。保密性强调信息不能非法泄露，而完整性强调信息在存储和传输过程中不能被偶然或蓄意修改、删除、伪造、添加、破坏或丢失，信息在存储和传输过程中必须保持原样。信息完整性表明了信息的可靠性、正确性、有效性和一致性，只有完整的信息才是可信任的信息。影响信息完整性的因素主要有硬件故障、软件故障、网络故障、灾害事件、入侵攻击、计算机病毒等，保障信息完

整性的技术主要有安全通信协议、密码校验、数字签名等。实际上，数据备份是防范信息完整性受到破坏时的最有效恢复手段。

3. 有效性

有效性（availability）是指信息资源容许授权用户按需访问的特性，有效性是信息系统面向用户服务的安全特性。信息系统只有持续有效，授权用户才能随时、随地根据自己的需要访问信息系统提供的服务。有效性在强调面向用户服务的同时，还必须进行身份认证与访问控制，只有合法用户才能访问限定权限的信息资源。一般而言，如果网络信息系统能够满足保密性、完整性和有效性 3 个安全目标，信息系统在通常意义下就可认为是安全的。

1.1.3　信息安全模型

为了实现信息安全目标，安全研究人员希望通过构造信息安全理论模型获得完整的信息安全解决方案。早期的信息安全模型主要从安全操作系统、信息加密、身份认证、访问控制、服务安全访问等方面来保障网络信息系统的安全性，但信息安全解决方案是一个涉及法律、法规、管理、技术和教育等多个因素的复杂系统工程，单凭几个安全技术不可能保障网络信息系统的安全性。事实上，安全只具有相对意义，绝对的安全只是一个理念，任何安全模型都不可能将所有可能的安全隐患都考虑周全。因此，理想的信息安全模型永远不会存在。

由 Internet 安全系统公司（Internet security systems，ISS）提出的著名 PPDR（policy protection detection response）信息安全模型在国际上公认为具有一定的可操作性，ISS 公司最早提出的是 PDR（protection detection response）模型，PPDR 模型是 PDR 模型的改进版。许多信息安全公司出于商业策略考虑，也分别提出了各自的信息安全模型，但本质内容仍然来自 PPDR 模型。包括 ISS 公司也将 PPDR 模型改版为 PADIMEE 模型，PADIMEE 分别表示策略（policy）、评估（assessment）、设计（design）、履行（implementation）、管理（management）、应急响应（emergency response）和教育（education）。

PPDR 信息安全模型如图 1.2 所示，包括安全策略、保护、检测和响应四个部分。安全策略是 PPDR 模型的核心，是围绕安全目标、依据信息系统具体应用、针对信息安全等级在信息安全管理过程中必须遵守的原则。安全策略的制定与实施依赖于安全技术、安全管理和法律法规，先进的信息安全技术为信息安全防范提供了技术保障；严格的信息安全管理为实施安全策略提供了基础；完善的法律法规为制定信息安全策略提供了坚强后盾。

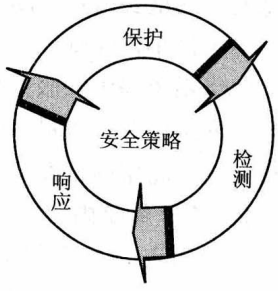

图 1.2　PPDR 信息安全模型

安全保护是网络安全的第一道防线，包括安全细则、安全配置和各种安全防御措施，能够阻止决大多数网络入侵和危害行为。安全细则是在安全策略基础上根据不同网络应用制定的规章制度，安全配置主要是在安全策略指导下确保服务安全与合理分配用户权限，安全防御措施主要包括信息加密、身份认证、访问控制、防火墙、病毒防治、风险评估、虚拟专用网（virtual private network，VPN）等安全防范组件。入侵检测是网络信息安全的第二道防线，目的是采用主动出击方式实时检测合法用户滥用特权、第一道防线遗漏的攻击、未知攻击和各种威胁信息安全的异常行为，通过安全监控中心掌握整个网络与信息系统的运行状态，采用与安全防御措施联动方式尽可能降低威胁网络与信息系统安全的风险。发现恶意攻击或威胁信息安全的异常行为以后，应急响应能够在信息系统受到危害之前，采用用户定义或自动响应方式及时阻断进一步的破坏活动。通过详细

记录入侵过程为入侵跟踪和计算机取证奠定基础，应急响应通常还包括数据和系统恢复措施，最大程度地减小破坏造成的损失。

1.1.4 信息安全策略

信息安全策略是保障机构信息安全的指导文件，一般而言，信息安全策略包括总体安全策略和具体安全管理实施细则。总体安全策略用于构建机构信息安全框架和战略指导方针，包括分析安全需求、分析安全威胁、定义安全目标、确定安全保护范围、分配部门责任、配备人力物力、确认违反策略的行为和相应的制裁措施。总体安全策略只是一个安全指导思想，还不能具体实施，在总体安全策略框架下针对特定应用制定的安全管理细则才规定了具体的实施方法和内容。

1. 安全策略总则

无论是制定总体安全策略，还是制定安全管理实施细则，都应当根据信息安全特点遵守均衡性、时效性和最小限度共性原则。

（1）均衡性原则

由于软件漏洞、协议漏洞、管理漏洞和网络威胁永远不可能消除，信息安全必定是计算机网络的永恒主题。无论制定多么完善的信息安全策略，还是使用多么先进的信息安全技术，信息安全也只是一个相对概念，因为世上没有绝对的安全系统。此外，信息系统易用性和效能与安全强度是一对天生的矛盾。夸大信息安全漏洞和威胁不仅会浪费大量投资，而且会降低信息系统易用性和效能，甚至有可能引入新的不稳定因素和安全隐患。忽视信息安全比夸大信息安全更加严重，有可能造成机构或国家重大经济损失，甚至威胁到国家安全。因此，信息安全策略需要在安全需求、易用性、效能和安全成本之间保持相对平衡，科学制定均衡的信息安全策略是提高投资回报和充分发挥网络及信息系统效能的关键。

（2）时效性原则

由于影响信息安全的因素随时间有所变化，导致信息安全问题具有显著的时效性。例如，信息系统用户增加、信任关系发生变化、网络规模扩大、新安全漏洞和攻击方法不断暴露都是影响信息安全的重要因素。因此，信息安全策略必须考虑环境随时间的变化。

（3）最小化原则

网络系统提供的服务越多，安全漏洞和威胁也就越多。因此，应当关闭信息安全策略中没有规定的网络服务；以最小限度原则配置满足安全策略定义的用户权限；及时删除无用账号和主机信任关系，将威胁信息安全的风险降至最低。

2. 安全策略内容

一般而言，大多数网络都是由网络硬件、网络连接、操作系统、网络服务和数据组成，网络安全管理员或信息安全管理员负责安全策略的实施，网络用户则应当严格按照安全策略的规定使用网络提供的服务。因此，在考虑网络与信息系统整体安全问题时应主要从网络硬件、网络连接、操作系统、网络服务、数据、安全管理责任和网络用户几方面着手。

（1）硬件物理安全

核心网络设备和服务器应当设置防盗、防火、防水、防毁等物理安全设施以及温度、湿度、洁净、供电等环境安全设施，位于雷电活动频繁地区的网络基础设施必须配备良好的防雷与接地装置，每年因雷电击毁网络设施的事例层出不穷。在规划物理安全设施时可参考《GB/T 21052—2007 信息系统物理安全要求》、《GB/T 22239—2008 信息系统安全等级保护基本要求》等国家技术标准。

核心网络设备和服务器最好集中放置在中心机房，其优点是便于管理与维护，也容易保障设

备的物理安全，更重要的是能够防止直接通过端口窃取重要资料。防止信息空间扩散也是规划物理安全的重要内容，除光纤之外的各种通信介质、显示器以及设备电缆接口都不同程度地存在电磁辐射现象，利用高性能电磁监测和协议分析仪有可能在几百米范围内将信息复原，对于涉及国家机密的信息必须考虑电磁泄露防护技术。例如，铺设电缆采用金属导管屏蔽，计算机和显示器最好使用符合美国瞬态电磁脉冲辐射标准（transient electromagnetic pulse emanation standard，TEMPEST）的产品，尽可能减小因电磁辐射导致失密的危险，TEMPEST 是美国国家安全部制定的计算机信息泄漏安全防护标准。我国也先后颁布了国家公共安全保密标准《GGBB1—1999 信息设备电磁泄漏发射限值》、《GGBB2—1999 计算机信息系统设备电磁泄漏发射测试方法》和国家保密标准《BMB5—2000 涉密信息设备使用现场的电磁泄漏发射防护要求》。

（2）网络连接安全

网络连接安全主要考虑网络边界的安全，如内部网（intranet）与外部网（extranet）、Internet 公用网络有连接需求，使用防火墙和入侵检测技术双层安全机制来保障网络边界的安全。内部网安全主要通过操作系统安全和数据安全策略来保障，由于网络地址转换（network address translator，NAT）技术能够对 Internet 屏蔽内部网地址，必要时也可以考虑使用 NAT 保护内部网私有 IP 地址。

对信息安全有特殊要求的内部网最好使用物理隔离技术保障网络边界的安全，根据安全需求，可以采用固定公用主机、双主机或一机两用等不同物理隔离方案。固定公用主机与内部网无连接，专用于访问 Internet，虽然使用不够方便，但能够确保内部主机信息的保密性。双主机在一个机箱中配备了两块主板、两块网卡和两个硬盘，双主机在启动时由用户选择内部网或 Internet 连接，较好地解决了安全性与方便性的矛盾。一机两用隔离方案由用户选择接入内部网或 Internet，但不能同时接入两个网络。虽然成本低廉、使用方便，但仍然存在泄密的可能性。

（3）操作系统安全

操作系统安全应重点考虑计算机病毒、特洛伊木马（Trojan horse）和入侵攻击威胁。计算机病毒是隐藏在计算机系统中的程序，具有自我繁殖、相互感染、激活再生、隐藏寄生、迅速传播特点，以降低计算机系统性能、破坏系统内部信息或破坏计算机系统运行为目的。截至目前，已发现有两万多种不同类型的病毒。病毒传播途径已经从移动存储介质转向 Internet，病毒在网络中以指数增长规律迅速扩散，诸如邮件病毒、Java 病毒和 ActiveX 病毒给网络病毒防治带来新的挑战。

特洛伊木马与计算机病毒不同，特洛伊木马是一种未经用户同意私自驻留在正常程序内部，以窃取用户资料为目的的间谍程序。目前，并没有特别有效的计算机病毒和特洛伊木马程序防治手段，主要还是通过提高病毒防范意义，严格安全管理，安装优秀防病毒、杀病毒、特洛伊木马专杀软件来尽可能减少病毒与木马入侵机会。操作系统漏洞为入侵攻击提供了条件，因此，经常升级操作系统、防病毒软件和木马专杀软件是提高操作系统安全性的最有效、最简便方法。

（4）网络服务安全

目前网络提供的电子邮件、文件传输、Usenet 新闻组、远程登录、域名查询、网络打印和 WWW（world wide web）服务都存在大量的安全隐患，虽然用户并不直接使用域名查询服务，但域名查询通过将主机名转换成主机 IP 地址为其他网络服务奠定了基础。由于不同网络服务的安全隐患和安全措施不相同，应当在分析网络服务风险的基础上，为每一种网络服务分别制定相应的安全策略细则。

（5）数据安全

根据数据机密性和重要性的不同，一般将数据分为关键数据、重要数据、有用数据和非重要

数据，以便对不同类型数据采取不同的保护措施。关键数据是指直接影响信息系统正常运行或无法再次得到的数据，如操作系统和关键应用程序等。重要数据是指具有很高机密性或高使用价值的数据，如国防或国家安全部门涉及国家机密的数据；金融部门涉及用户的账目数据等。有用数据一般指信息系统经常使用但可以从其他地方复制的数据，非重要数据则是很少使用而且很容易得到的数据。由于任何安全措施都不可能保证网络信息系统绝对安全或不发生故障，在信息安全策略中除考虑重要数据加密之外，还必须考虑关键数据和重要数据的备份。

目前，数据备份使用的介质主要是磁带、硬盘和光盘，因磁带具有容量大、技术成熟、成本低廉等优点，大容量数据备份多选用磁带存储介质。随着硬盘价格不断下降，网络服务器都使用硬盘作为存储介质，目前流行的硬盘数据备份技术主要有磁盘镜像和冗余磁盘阵列（redundant arrays of inexpensive disks，RAID）。磁盘镜像技术能够将数据同时写入型号与格式相同的主磁盘和辅助磁盘，RAID 是专用服务器广泛使用的磁盘冗错技术。大型网络常采用光盘库、光盘阵列和光盘塔作为存储设备，但光盘特别容易被划伤，导致数据读出错误，数据备份使用更多的还是磁带和硬盘存储介质。

（6）安全管理责任

由于人是制定和执行信息安全策略的主体，所以在制定信息安全策略时，必须明确信息安全管理责任人。小型网络与信息系统可由网络管理员兼任信息安全管理职责，但大型网络、电子政务、电子商务、电子银行或其他要害部门的网络信息系统应配备专职信息安全管理责任人。信息安全管理采用技术与行政相结合的手段主要对授权、用户和资源进行管理，其中授权是信息安全管理的重点。安全管理责任包括行政职责、网络设备、网络监控、系统软件、应用软件、系统维护、数据备份、操作规程、安全审计、病毒防治、入侵跟踪、恢复措施、内部人员、网络用户等与网络安全相关的各种功能。

（7）网络用户安全责任

信息安全不仅仅是信息安全管理员的事，网络用户对信息安全也负有不可推卸的责任。网络用户应特别注意不能私自将调制解调器（modem）接入 Internet；不要下载未经安全认证的软件和插件；确保本机没有安装文件和打印机共享服务；不要使用脆弱性口令；经常更换口令等。

1.2 信息安全漏洞与威胁

1.2.1 软件漏洞

软件漏洞（flaw）是指在设计与编制软件时没有考虑对非正常输入进行处理或错误代码而造成的安全隐患，软件漏洞也称为软件脆弱性（vulnerability）或软件隐错（bug）。软件漏洞产生的主要原因是软件设计人员不可能将所有输入都考虑周全，因此，软件漏洞是任何软件存在的客观事实。软件产品通常在正式发布之前，一般都要相继发布 α 版本、β 版本和 γ 版本供反复测试使用，目的就是为了尽可能减少软件漏洞。

根据卡内基梅隆大学软件工程研究所计算机应急响应协作中心（CERT coordination center）截止到 2008 年的软件漏洞和攻击事件统计报告，1995 年仅有 171 起软件漏洞报告，2006 年则上升到 8064 起软件漏洞报告。随着软件设计技术水平的提高和人们对信息安全事件的重视，2008 年软件漏洞报告下降到 6058 件，并逐步趋于稳定。针对软件漏洞的攻击，1998 年仅发生了 6 起，

2003 年就发生了 137 529 起攻击事件。由于各种自动攻击工具在网络上随处可见，CERT 认为统计攻击事件已经没有太多意义，从 2004 年开始转向电子犯罪统计。软件漏洞和攻击事件统计趋势分别如图 1.3 和图 1.4 所示。

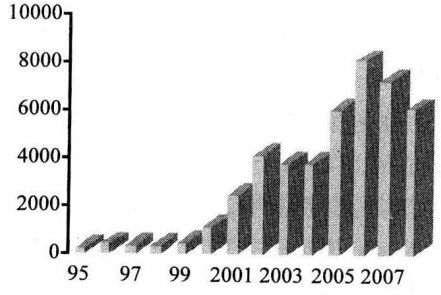

图 1.3　软件漏洞趋势图

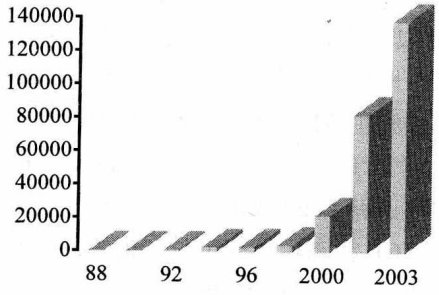

图 1.4　攻击事件趋势图

缓冲区溢出、特殊字符组合和操作系统多任务竞争是最常见的软件漏洞，除非正常输入和错误代码造成的软件漏洞之外，通常将软件配置不当造成的安全隐患也归类到软件漏洞范畴，如操作系统缺省配置、脆弱性口令、系统后门等都是攻击首选的安全漏洞。不同软件、同一软件的不同版本或不同运行环境其软件漏洞各自都不相同，因此，脱离具体软件和运行环境讨论软件漏洞毫无意义。此外，软件漏洞具有时效性特点，随着软件的广泛使用，软件漏洞将不断暴露出来。软件商通常会发布软件补丁修补已发现的软件漏洞，或在新版本中予以纠正。新版本软件在纠正旧版本软件的同时，有可能引入新的软件漏洞。随着软件使用时间的推移，已暴露的软件漏洞会不断消亡，新的软件漏洞将不断出现。

1.2.2　网络协议漏洞

网络协议漏洞类似于软件漏洞，是指网络通信协议不完善而导致的安全隐患。截止到目前，Internet 上广泛使用的 TCP/IP 协议族几乎所有协议都发现存在安全隐患，包括数据链路层（data link layer）的地址解析协议（address resolution protocol，ARP）、逆向地址解析协议（reverse address resolution protocol，RARP）；网络层（network layer）的网际协议（internet protocol，IP）、Internet 控制报文协议（internet control messages protocol，ICMP）、Internet 组管理协议（internet group management protocol，IGMP）；传输层（transport layer）的传输控制协议（transfer control protocol，TCP）、用户数据报协议（user datagram protocol，UDP）、可靠数据协议（reliable data protocol，RDP）；应用层（application layer）的域名系统（domain name systems，DNS）、文件传输协议（file transfer protocol，FTP）、超文本传输协议（hyper text transfer protocol，HTTP）、简单邮件传输协议（simple message transfer protocol，SMTP）、远程登录协议（Telnet）等。

应用程序在 IEEE802.3 以太网（ethernet）标准上采用 TCP/IP 传送数据时，用户数据通过传输层、网络层、数据链路层都要分别添加 TCP、IP 和载波监听多路访问/冲突检测（carrier sense multiple access/collision detect，CSMA/CD）首部信息。由于 IP 分组封装在 CSMA/CD 帧内，位于数据链路层的网络接口驱动程序并不清楚有 IP 地址，而且也不理解 IP 地址格式。主机在数据链路层采用 48 位介质访问控制（medium access control，MAC）硬件地址实现数据通信，因此，在数据通信之前，必须首先获得目标主机的 MAC 地址，源和目标主机的 MAC 地址封装在 CSMA/CD 帧头内，最终才能通过物理层介质达到传送数据的目的。ARP 的主要任务就是通过查询本机 ARP 缓冲表来获取目标 IP 地址对应的 MAC 地址，主机传送数据前，首先查询 ARP 缓冲表，如检索

到目标 IP 地址，则将对应的 MAC 地址封装在帧头内。否则，在网段内发送一个 ARP 询问广播包，具有目标 IP 地址的主机将回送一个包含 MAC 地址的 ARP 应答包，源主机提取目标 MAC 地址并将其保存到 ARP 缓冲表。正是 ARP 的应答与地址映射机制导致了安全隐患，ARP 应答分组完全可以假冒路由器、文件服务器或数据库服务器 IP 地址，目标为某台主机的 MAC 地址。接收 ARP 虚假应答分组的主机将路由器、文件服务器或数据库服务器 IP 地址错误地映射成指定主机的 MAC 地址，结果是发往路由器、文件服务器或数据库服务器的分组全部传送到某台指定的主机，这种利用 ARP 应答与地址映射机制漏洞实施的攻击称为缓冲中毒攻击（cache poisoning）。

针对 TCP 三次握手（three-way handshake）初始连接和应答每个接收报文安全漏洞，TCP 漏洞典型攻击有 Land 攻击、会话劫持（hijack）攻击、TCP 序列号猜测攻击、同步洪流攻击（SYN flood）、TCP 状态转移和定时器拒绝服务攻击等。UDP fraggle 拒绝服务攻击是针对 UDP 漏洞的典型攻击之一，将目标 IP 地址设置成目标网络的广播地址，通过伪造目标网络中某主机 UDP 广播报文，广播域内所有主机会给目标主机发送错误消息，目标主机将被错误消息所淹没，导致目标主机发生拒绝服务。Smurf 攻击利用 ICMP 回复漏洞和 IP 地址欺骗能够使广播域内数据流量巨增，从而导致目标主机拒绝为正常请求服务。ICMP 与 IP 都位于网络层，但 ICMP 报文是封装在 IP 分组中传输的。Smurf 攻击类似于 UDP fraggle 拒绝服务攻击，伪造源 IP 地址并将目标 IP 地址设置成目标网络的广播地址，通过向广播域发送类型为 8、代码为 0 的回应请求（echo）ICMP 报文，由于广播域内的所有主机都向伪造的 IP 地址发送回应消息，大量回应消息不仅充斥广播域，而且将淹没目标主机。

截止到 2012 年 6 月，专门从事安全漏洞名称标准化的公共漏洞披露机构（common vulnerability and exposures，CVE）已发布了 53 623 个不同的安全漏洞，新的安全漏洞仍在不断披露。

1.2.3 安全管理漏洞

软件漏洞和网络协议漏洞是天生具有的，但由于安全管理疏漏产生的安全漏洞则完全是人为因素造成的。信息安全技术只是保证信息安全的基础，信息安全管理才是发挥信息安全技术的根本保证。因此，信息安全问题并不是一个纯技术问题，从信息安全管理角度看，信息安全首先应当是管理问题。事实上，国际标准化组织（international standardization organization，ISO）将网络管理划分为故障、性能、配置、记账和安全管理五个领域，表明安全管理是网络管理的重要组成部分。

由于计算机网络包含各种网络设施、服务器、工作站、网络终端等设备，每个设备又可能安装了不同操作系统和应用软件，各自都具有不同的安全隐患。因此，计算机网络和信息系统的安全隐患由大量子系统安全隐患聚集而成，导致信息安全隐患数量庞大且十分复杂，提高了信息安全管理的技术难度与成本，容易造成更多的安全管理疏漏。

但许多安全管理漏洞只要提高安全管理意识完全可以避免，如常见的系统缺省配置、脆弱性口令、信任关系转移等。系统缺省配置主要考虑的是用户友好性，但方便使用的同时也就意味着更多的安全隐患。许多系统采用 123456 作为默认口令，用 Administrator 或 ChangMe 作为默认用户名，这些系统缺省配置很容易被猜测。许多用户习惯用用户名或用户名的变形、自己或亲友生日、电话号码、身份证或员工号码、常用单词等作为口令，事实上，这些口令都是典型的脆弱性口令。假设用出生 19××（0～99）年××（1～12）月××日（1～31）8 位数字作为口令，但可能的组合数只有 100×12×31=37200，一般口令破解软件每秒至少可以搜索 4 万种组合。通常 8 位以上、字母大小写和数字混用的口令才是安全口令。

信息安全管理是在信息安全策略指导下为保护网络与信息系统不受内外各种威胁而采取的一系列信息安全措施，信息安全策略则是根据信息安全目标和网络应用环境，为提供特定安全级别保护而必须遵守的规则。因此，信息安全策略与网络应用环境密切相关，不同的应用环境需要制定不同的安全策略。如果将信任区的安全策略应用到非信任区，必然会产生众多的安全管理漏洞。如果将非信任区的安全策略应用到信任区，又会造成不必要的资金浪费。由此可见，信息安全是相对的，是建立在信任基础之上的，绝对的信息安全永远不存在。信任区与非信任区，或者安全区与非安全区的边界是基于信任关系划定的，在安全区内应当相信系统管理人员和内部用户不会滥用特权，并且具有良好的职业道德。但是当信任关系发生变化时，安全管理必须进行及时调整，否则会大大降低整个网络的安全性。

1.2.4　信息安全威胁来源

信息安全威胁是指事件对信息资源的可靠性、保密性、完整性、有效性、可控性和拒绝否认性可能产生的危害，信息安全威胁根据威胁产生的因素可以分为自然和人为两大类。因自然因素产生的信息安全威胁主要有硬件故障、软件故障、电源故障、电磁干扰、电磁辐射和各种不可抗拒的自然灾害，电磁辐射并不影响信息的完整性和有效性，但破坏了信息的保密性，物理故障及自然灾害主要破坏了信息的完整性和有效性。人为因素导致的信息安全威胁又可以根据是否有意分为意外损坏和蓄意攻击两类，意外损坏主要包括偶然删除文件、格式化硬盘、带电拔插、系统断电等各种操作失误，操作失误主要影响了信息的完整性和有效性，对保密性影响不大。蓄意攻击则是有意利用软件漏洞、协议漏洞和管理漏洞试图饶过信息安全策略破坏、篡改、窃听、假冒、泄露和非法访问信息资源的各种恶意行为，包括网络攻击、计算机病毒、特洛伊木马、网络窃听、邮件截获、滥用特权等多种类型，信息安全威胁分类及破坏目标如图 1.5 所示。

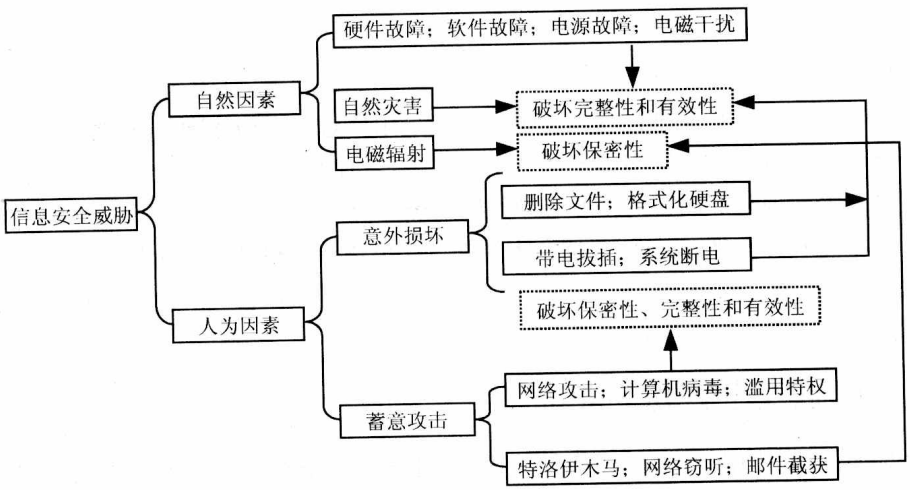

图 1.5　信息安全威胁分类及破坏目标

根据信息安全威胁来自网络边界内部或外部，蓄意攻击还可以分为内部攻击和外部攻击，由于内部人员位于信任范围内，熟悉敏感数据的存放位置、存取方法、网络拓扑结构、安全漏洞及防御措施，而且多数机构的安全保护措施都是防外不防内，因此，决大多数蓄意攻击来自内部而不是外部。因内部人员角色经常变动，内部人员界定比较困难，一般而言，软件开发人员、系统维护人员、授权用户、网络管理员、安全管理员、系统管理员、数据库管理员等属于内部人员，