“十二五”职业教育国家规划教材
经全国职业教育教材审定委员会审定

普通高等职业教育 计算机系列规划教材

信息安全技术与实施(第2版)

◆ 武春岭 主编

NETWORK

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

配备电子课件

“十二五”职业教育国家规划教材
经全国职业教育教材审定委员会审定

普通高等职业教育计算机系列规划教材

信息安全技术与实施

（第2版）

武春岭　主　编

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书作为信息安全知识普及与技术推广教材，涵盖信息安全概念、信息安全防御模型、信息安全法律法规、信息安全物理防御技术、网络攻防技术、密码技术、防火墙技术、入侵检测技术、操作系统安全技术和无线网安全技术等多方面的内容，不仅能够为初学信息安全技术的学生提供全面、实用的技术和理论基础，而且能有效培养学生信息安全的防御能力。

本书的编写融入了作者丰富的教学和企业实践经验，内容安排合理，每个章节都从“引导案例”开始，首先让学生知道通过本章学习能解决什么实际问题，做到有的放矢，激发学生的学习热情，使学生更有目标地学习相关理念和技术操作，最后针对“引导案例”中提到的问题给出解决方案，使学生真正体会到学有所用。整个章节围绕一个主题——案例，从问题提出（引导案例）到问题解决（案例实现），步步为营、由浅入深，结构严谨、浑然天成。此外，每章还配有习题和实训，不仅可以巩固理论知识，也为技能训练提供了基础。

本书可以作为高职高专计算机信息类专业的教材，也可以作为企事业单位网络信息系统管理人员的技术参考用书，同时也适合趋势科技 TCSP 认证证书培训使用。

图书在版编目（CIP）数据

信息安全技术与实施 / 武春岭主编. —2 版. —北京：电子工业出版社，2015.7
“十二五”职业教育国家规划教材

ISBN 978-7-121-26380-4

Ⅰ. ①信… Ⅱ. ①武… Ⅲ. ①信息系统—安全技术—高等职业教育—教材 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2015）第 137408 号

策划编辑：徐建军（xujj@phei.com.cn）
责任编辑：郝黎明
印　　刷：三河市双峰印刷装订有限公司
装　　订：三河市双峰印刷装订有限公司
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
开　　本：787×1 092　1/16　印张：18.25　字数：467.2 千字
版　　次：2010 年 10 月第 1 版
　　2015 年 7 月第 2 版
印　　次：2015 年 7 月第 1 次印刷
印　　数：3 000 册　　定价：38.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前言

随着科学技术的迅猛发展和信息技术的广泛应用，特别是我国国民经济和社会信息化进程的全面加快，网络与信息系统的基础性、全局性作用日益增强，信息安全已经成为国家安全的重要组成部分。近年来，在党中央、国务院的领导下，我国信息安全保障工作取得了明显成效，建设了一批信息安全基础设施，加强了互联网信息内容安全管理，为维护国家安全与社会稳定、保障和促进信息化健康发展发挥了重要作用。

但是，我国信息安全保障工作仍存在一些亟待解决的问题：网络与信息系统的防护水平不高，应急处理能力不强；信息安全管理和技术人才缺乏，关键技术整体上还比较落后，产业缺乏核心竞争力；信息安全法律法规和标准不完善；全社会的信息安全意识不强，信息安全管理薄弱等。与此同时，网上有害信息传播、病毒入侵和网络攻击日趋严重，网络泄密事件屡有发生，网络犯罪呈快速上升趋势，境内外敌对势力针对广播电视卫星、有线电视和地面网络的攻击破坏活动和利用信息网络进行的反动宣传活动日益猖獗，严重危害公众利益和国家安全，影响了我国信息化建设的健康发展。随着我国信息化进程的逐步推进，特别是互联网的广泛应用，信息安全还将面临更多新的挑战。

尤其是近几年来，随着网络发展的日趋庞大，网络环境也更加复杂。计算机网络安全威胁更加严重，病毒和蠕虫不断扩散、黑客活动频繁、垃圾邮件猛增都成为目前困扰网络信息安全的较大威胁。譬如，2009 年新的安全威胁 Conficker（飞客）的出现，打破了全球 500 万台计算机的感染记录，不仅对国家安全造成威胁，也直接影响广大计算机用户的正常工作和生活。

本书作为信息安全知识普及与技术推广教材，涵盖信息安全概念、信息安全防御模型、信息安全法律法规、信息安全物理防御技术、网络攻防技术、密码技术、防火墙技术、入侵检测技术、操作系统安全技术和无线网安全技术等多方面的内容，不仅能够为初学信息安全技术的学生提供全面实用的技术和理论基础，而且精选案例力求实用新颖，能有效培养学生信息安全的防御能力。

重庆电子工程职业学院信息安全技术专业，是国家示范院校建设中唯一一个信息安全类国家级重点建设专业，该专业自 2003 年开办以来，就开设了“信息安全技术与实施”课程，目前该课程已经获得重庆市市级精品课称号。我们根据多年的实践教学经验，与信息安全服务公司合作，编写了该专业的核心技术教材，旨在更加有效地培养信息安全专业技术人才。

作为一本专注于信息安全技术的教材，本书详细介绍了信息安全领域常见的信息安全攻击技术和防御方法。本书共分 10 章：第 1 章信息安全概述；第 2 章物理实体安全与防护；第 3 章网络攻击与防范；第 4 章密码技术与应用；第 5 章数字身份认证；第 6 章防火墙技术与应用；第 7 章入侵检测技术与应用；第 8 章计算机病毒与防范；第 9 章操作系统安全防范；第

10 章无线网安全与防范。

本书的编写融入了作者丰富的教学和企业实践经验，内容安排合理，每个章节都先从“引导案例”开始，让学生知道通过本章学习能解决什么实际问题，激发学生的学习激情，引导学生渐入佳境，最后针对“引导案例”中的问题提出解决方案，使学生感受到学有所用的快乐。此外，每章还配有习题和实训，不仅可以巩固理论知识，而且也为技能训练提供了基础。本书第 1、2、6 和 10 章由武春岭编写；第 3 和 7 章由何欢编写；第 4 和 5 章由辽宁本溪机电工程学校宁蒙编写；第 8 章由李治国编写，第 9 章由胡凯编写。

在本书编写过程中，重庆电子工程职业学院廖雨萧同学和重庆金佩科技公司谌玺技术总监、张洋工程师也参与了部分内容的实践验证工作。本书还得到了电子工业出版社的大力支持与帮助。此外，本书部分内容来自互联网，在此一并致以衷心的感谢！

为了方便教师教学，本书配有电子教学课件，请有此需要的教师登录华信教育资源网（www.hxedu.com.cn）注册后免费进行下载，有问题时可在网站留言板留言或与电子工业出版社联系（E-mail:hxedu@phei.com.cn）。

由于编者水平有限，加上时间仓促，书中难免有不当之处，敬请各位同行批评指正，以便在今后的修订中不断改进。

编　者

目 录

第1章

信息安全概述

学习目标

- 了解信息安全的重要性及黑客文化。
- 掌握网络安全体系的结构组成。

引导案例

2009 年 1 月，法国海军内部计算机系统的一台计算机遭受病毒入侵，病毒迅速扩散到整个网络，导致网络一度不能启动，海军全部战斗机也因无法“下载飞行指令”而停飞两天。

仅仅是法国海军内部计算机系统的时钟停摆，法国的国家安全就出现了一个偌大的“黑洞”。设想，如果一个国家某一系统或领域的计算机网络系统出现问题或瘫痪，这种损失和危害将是不可想象的，而类似的事件不胜枚举。

目前，美国政府掌握着信息领域的核心技术，操作系统、数据库、网络交换机的核心技术基本掌握在美国企业的手中。微软操作系统、思科交换机的交换软件甚至打印机软件中嵌入美国中央情报局的后门软件已经不是秘密，美国在信息技术研发和信息产品的制造过程中就事先做好了日后对全球进行信息制裁的准备。

近年，美国“棱镜”事件愈演愈烈。据美国国家安全局承包商前雇员爱德华·斯诺登透露，过去 6 年间，美国国家安全局和联邦调查局通过微软、谷歌、苹果、雅虎等 9 大网络巨头的服务器监控美国及全球其他国家的电子邮件、聊天记录、视频和照片等，引发全球舆论关注。与此同时，美国国家安全局和联邦调查局还对中国华为公司和中国前领导人胡锦涛等进行监控，中国的信息安全形势相当严峻。2014 年 2 月 27 日，中央网络安全和信息化领导小组宣告成立，并在北京召开了第一次会议。中共中央总书记、国家主席、中央军委主席习近平亲自担任组长，李克强、刘云山任副组长，再次体现了中国最高层全面深化改革、加强顶层设计的意志，显示出在保障网络安全、维护国家利益、推动信息化发展的决心。

金融、商贸、交通、通信、军事……随着计算机网络逐渐渗入人类社会的各个领域，越来越多的机构不得不重新布局以便与技术的发展保持一致，国家的整个民用和军用基础设施都越来越依赖于网络，网络也因此成为一国赖以正常运转的“神经系统”。一旦出现漏洞，事关国计民生的许多重要系统都将陷入瘫痪的状态，国家安全也岌岌可危……

1.1 信息安全介绍

随着全球互联网的迅猛发展，越来越多的人亲身体会到了信息化给人们生活带来的实实在在的便利与实惠。信息化带动了工业化，并由此带动全球经济以前所未有的惊人速度向前发展。然而任何事情都有两面性，信息化也是如此，它在给经济带来新高、给人们带来实惠的同时，也由此产生了新的威胁。目前“信息战”已是现代战争克敌制胜的法宝，科索沃战争、海湾战争就是“信息战”应用成功的范例。尤其是美国“9·11 事件”给世界各国的信息安全问题再次敲响了警钟，因为恐怖组织摧毁的不仅仅是世贸大厦，随之消失的还有众多公司的数据。

自 2003 年元月以来，蠕虫病毒“冲击波”对全球范围内的互联网发起了不同程度的攻击，制造了一场规模空前的互联网“网瘫”灾难事件。迄今为止，许多组织、单位和实体仍然没有完全走出“冲击波”和“震荡波”的阴影，而 2007 年的“熊猫烧香”又给互联网用户留下了深刻的印象。据权威机构调查显示，计算机攻击事件正在以每年 64%的速度增加。另据统计，全球约 20 秒就有一次计算机入侵事件发生，Internet 上的网络防火墙约 1/4 被突破，约有 70%以上的网络信息主管人员报告因机密信息泄露而受到了损失。

信息安全涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科。由于目前信息的网络化，信息安全主要表现在网络安全上，所以目前许多人将网络安全与信息安全等同起来。实际上，叫信息安全比较全面、科学，本书中也不加严格区分。

信息安全是一个关系国家安全和主权、社会的稳定、民族文化的继承和发扬的重要问题。信息安全问题已引起了各国政府的高度重视，政府为此建立了专门的机构，并出台了相关标准与法规。

1.1.1 信息安全的概念

信息安全的概念是随着计算机化、网络化、信息化的逐步发展提出来的。当前对信息安全的说法较多，计算机安全、计算机信息系统安全、网络安全、信息安全的叫法同时并存。事实上，它们是有区别的，应该说它们是计算机化、网络化、信息化发展到一定阶段的产物，各自的侧重点不同。

国际标准化组织（ISO）对计算机系统安全的定义是：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄漏。由此可以将计算机网络的安全理解为：通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。因此，采用网络安全保护措施的目的是确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄漏等。

针对信息安全，目前尚没有公认的权威定义。美国国家安全电信和信息系统安全委员会（NSTISSC）对信息安全做如下定义：信息安全是对信息、系统及使用、存储和传输信息的硬件的保护。一般认为，信息安全主要包括物理安全、网络安全和操作系统安全，网络安全是目前信息安全的核心，本书不对网络安全和信息安全加以严格区分。

1.1.2 信息安全的内容

信息安全涉及个人权益、企业生存、金融风险防范、社会稳定和国家的安全，它是物理安全、网络安全、数据安全、信息内容安全、信息基础设施安全、国家信息安全的总和。

1．物理安全

物理安全是指用来保护计算机网络中的传输介质、网络设备和机房设施安全的各种装置与

管理手段。物理安全包括防盗、防火、防静电、防雷击和防电磁泄漏等方面的内容。

物理上的安全威胁主要涉及对计算机或人员的访问。可用于增强物理安全的策略有很多，如将计算机系统和关键设备布置在一个安全的环境中，销毁不再使用的敏感文档，保持密码和身份认证部件的安全性，锁住便携式设备等。物理安全的实施更多的是依赖于行政的干预手段并结合相关技术。如果没有基础的物理保护，如带锁的开关柜、数据中心等，物理安全是不可能实现的。

2．网络安全

计算机网络的逻辑安全主要通过用户身份认证、访问控制、加密、安全管理等方法来实现。

（1）用户身份认证。身份证明是所有安全系统不可或缺的一个组件。它是区别授权用户和入侵者的唯一方法。为了实现对信息资源的保护，并知道何人试图获取网络资源的访问权，任何网络资源拥有者都必须对用户进行身份认证。当使用某些更尖端的通信方式时，身份认证特别重要。

（2）访问控制。访问控制是制约用户连接特定网络、计算机与应用程序，获取特定类型数据流量的能力。访问控制系统一般针对网络资源进行安全控制区域划分，实施区域防御的策略。在区域的物理边界或逻辑边界使用一个许可或拒绝访问的集中控制点。

（3）加密。即使访问控制和身份验证系统完全有效，在数据信息通过网络传送时，企业仍可能面临被窃听的风险。事实上，低成本和连接的简便性已使 Internet 成为企业内和企业间通信的一个极为诱人的媒介。同时，无线网络的广泛使用也在进一步加大网络数据被窃听的风险。加密技术用于针对窃听提供保护。它通过使信息只能被具有解密数据所需密钥的人员读取来提供信息的安全保护。它与第三方是否通过 Internet 截取数据包无关，因为数据即使在网络上被第三方截取，它也无法获取信息的本义。这种方法可在整个企业网络中使用，包括在企业内部（内部网）、企业之间（外部网）或通过公共 Internet 在虚拟专用网络（VPN）中传送私人数据。加密技术主要包括对称式和非对称式两种，这两种方式都有许多不同的密钥算法来实现，在此不一一详述。

（4）安全管理。安全系统应当允许由授权人进行监视和控制。使用验证的任何系统都需要某种集中授权来验证这些身份，而无论它是 UNIX 主机、Windows NT 域控制器还是 Novell Directory Services（NDS）服务器上的/etc/passwd 文件。由于能够查看历史记录，如突破防火墙的多次失败尝试，安全系统可以为那些负责保护信息资源的人员提供宝贵的信息。一些更新的安全规范，如 IPSec，需要包含策略规则数据库。要使系统正确运行，就必须管理所有这些要素。但是，管理控制台本身也是安全系统的另一个潜在故障点。因此，必须确保这些系统在物理上得到安全保护，并确保对管理控制台的任何登录进行验证。

3．操作系统安全

计算机操作系统担负着自身庞大的资源管理，频繁的输入输出控制，以及不可间断的用户与操作系统之间的通信任务。由于操作系统具有“一权独大”的特点，所有针对计算机和网络的入侵及非法访问都是以攫取操作系统的最高权限作为入侵的目的。因此，操作系统安全的内容就是采用各种技术手段和采取合理的安全策略，降低系统的脆弱性。

与过去相比，如今的操作系统性能更先进、功能更丰富，因而对使用者来说更便利，但同时也增加了安全漏洞。要减少操作系统的安全漏洞，需要对操作系统予以合理配置、管理和监控。做到这点的秘诀在于集中、自动管理机构（企业）内部的操作系统安全，而不是分散、人工管理每台计算机。

实际上，如果不集中管理操作系统安全，相应的成本和风险就会非常高。目前所知道的安

全入侵事件，一半以上缘于操作系统根本没有合理配置，或者没有经常核查及监控。操作系统都是以默认安全设置来配置的，因而极容易受到攻击。

那些人工更改了服务器安全配置的用户，把技术支持部门的资源过多地消耗于帮助用户处理口令查询上，而不是处理更重要的网络问题。考虑到这些弊端，难怪许多管理员任由服务器操作系统以默认状态运行。这样一来，服务器可以马上投入运行，但这却大大增加了安全风险。

现有技术可以减轻管理负担。要加强机构（企业）网络内操作系统的安全，需要做到以下三方面。

首先，对网络上的服务器进行配置应该在一个地方进行，大多数用户大概需要数十种不同的配置。然后，这些配置文件的一个镜像或一组镜像在软件的帮助下可以通过网络下载。软件能够自动管理下载过程，不需要为每台服务器手工下载。此外，即使有某些重要的配置文件，也不应该让本地管理员对每台服务器分别配置，这样做是很危险的，最好的办法就是一次性全部设定。一旦网络配置完毕，管理员就要核实安全策略的执行情况，定义用户访问权限，确保所有配置正确无误。管理员可以在网络上运行（或远程运行）代理程序，不断监控每台服务器。代理程序不会干扰正常操作。

其次，账户需要加以集中管理，以控制对网络的访问，并且确保用户拥有合理访问机构（企业）资源的权限。策略、规则和决策应在一个地方进行，而不是在每台计算机上进行，然后为用户系统配置合理的身份和许可权。身份生命周期管理程序可以自动管理这一过程，减少手工过程带来的麻烦。

最后，操作系统应该配置成能够轻松、高效地监控网络活动，可以显示谁在进行连接，谁断开了连接，以及发现来自操作系统的潜在安全事件。

1.1.3 信息安全策略

安全策略是针对网络和系统的安全需要，做出允许什么、禁止什么的规定，通常可以使用数学方式来表达策略，将其表示为允许（安全的）或不允许（不安全的）的状态列表。为达到这个目的，可假设任何给定的策略能对安全状态和非安全状态做出公理化描述。实践中，策略极少会如此精确，往往使用文本语言描述什么是用户或系统允许做的事情。这种描述的内在歧义性导致某些状态既不能归于“允许”一类，也不能归于“不允许”一类，因此制定安全策略时，需要注意此类问题。

1．物理安全策略

物理安全策略的目的是保护计算机系统、网络服务器、打印机等硬件实体和通信链路免受自然灾害、人为破坏和搭线攻击，验证用户的身份和使用权限，防止用户越权操作；确保计算机系统有一个良好的电磁兼容工作环境；建立完备的安全管理制度，防止非法进入计算机控制室和各种偷窃、破坏活动的发生。抑制和防止电磁泄漏，即 Tempest 技术，是物理安全策略的一个主要问题。目前主要防护措施有两类：一类是传导发射的保护，主要采取对电源线和信号线加装性能良好的滤波器，减小传输阻抗和导线间的交叉耦合；另一类是对辐射的防护。

2．访问控制策略

访问控制是网络安全防范和保护的主要策略，其主要任务是保证网络资源不被非法使用和非法访问。它是维护网络系统安全、保护网络资源的重要手段。各种安全策略必须相互配合才能真正起到保护作用，可以说访问控制是保证网络安全的核心策略之一。下面分别叙述几种访问控制策略。

（1）入网访问控制。入网访问控制为网络访问提供了第一层访问控制。它是用来控制哪些用户能够登录到服务器并获取网络资源，控制准许用户入网的时间和准许在哪个工作站入网。