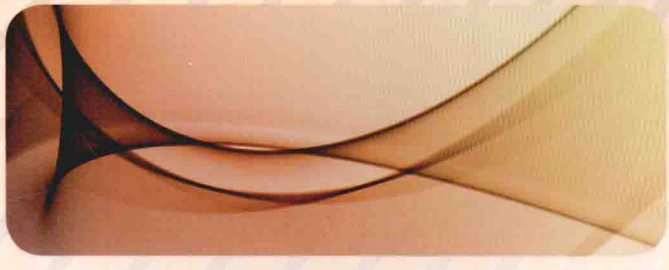
上海高校市级精品课程教材 | 上海市高等学校教育高地建设项目

网络安全技术与实践

Network Security Technologies and Practice

主编 贾铁军



高等教育出版社

上海高校
上海市高等学校教育高地建设项目

网络安全技术与实践

Wangluo Anquan Jishu yu Shijian

主　编　贾铁军
副主编　嵩　天　俞小怡　苏庆刚　沈学东
编　者　罗宜元　王　福　陈国秦　宋少婷

阜阳师范学院图书馆
藏书

高等教育出版社·北京

内容提要

本书是上海高校市级精品课程教材。全书共分12章，主要内容包括网络安全概述、网络安全技术基础、网络安全体系及管理、密码和加密技术、黑客攻防与检测防御、身份认证与访问控制、操作系统与站点安全、数据库与防护技术、计算机病毒及恶意软件防范、防火墙技术、电子商务及网站安全、网络安全新技术及解决方案。本书介绍了网络安全“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基本理论和实用技术。

本书可作为高等学校计算机与信息类、工程与管理类、电子商务类等专业相关课程的教材，也可作为培训教材或参考用书。

图书在版编目(CIP)数据

网络安全技术与实践/贾铁军主编. --北京：高等教育出版社，2014.8

ISBN 978-7-04-040624-5

Ⅰ. ①网… Ⅱ. ①贾… Ⅲ. ①计算机网络-安全技术-高等学校-教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2014)第151799号

策划编辑 时 阳	责任编辑 时 阳	封面设计 张雨微	版式设计 杜微言
插图绘制 邓 超	责任校对 李大鹏	责任印制 尤 静	

出版发行	高等教育出版社	咨询电话	400-810-0598
社 址	北京市西城区德外大街4号	网 址	http://www.hep.edu.cn
邮政编码	100120		http://www.hep.com.cn
印 刷	北京宏信印刷厂	网上订购	http://www.landraco.com
开 本	787mm×1092mm 1/16		http://www.landraco.com.cn
印 张	24	版 次	2014年8月第1版
字 数	600千字	印 次	2014年8月第1次印刷
购书热线	010-58581118	定 价	37.30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

版权所有 侵权必究

物 料 号 40624-00

前　言

目前，信息、物资、能源已经成为人类社会赖以生存与发展的三大支柱和重要保障。网络安全对于国家政治、经济、军事、科技和文化等方面的安全极为重要。世界各国都非常重视网络安全，不惜投入巨资和大量的人力物力，利用最先进的技术，力争构建最安全可靠的网络系统。网络安全决定了国家的信息主权。信息时代，强国推行信息强权和信息垄断，依仗信息优势控制弱国的信息技术。一旦缺乏自主创新的网络安全策略和手段，国家的信息主权就有可能葬送。正如美国未来学家托尔勒所说："谁掌握了信息，谁控制了网络，谁就将拥有整个世界。"网络安全主导国家信息安全。知识经济时代，竞争首先表现为科技竞争，其重点是对信息技术这一制高点的争夺。信息、资本、人才和商品的流向逐渐呈现出以信息为中心的竞争新格局。网络安全成为影响国家政治命脉、经济发展、军事强弱、社会稳定和民族与文化复兴等方面的关键因素。

在现代信息化社会，随着信息化建设和信息技术的快速发展，计算机网络技术的应用更加广泛和深入，网络安全问题不断出现，致使网络安全技术的重要性更加突出。网络安全已经成为世界各国关注的焦点，不仅关系到用户的信息和资产安全，也关系到国家安全和社会稳定，成为热门研究和人才需求的新领域。只有在法律、管理、技术、道德各方面采取切实可行的有效措施，才能确保网络安全建设又好又快地稳定发展。

为满足高校计算机与信息类、工程与管理类、电子商务类等本科生、研究生等高级人才培养的需要，我们编写了这本教材。多年来，本书编者在高校从事计算机网络与安全等领域的教学、科研及学科专业建设与管理工作，积累了大量宝贵的实践经验，谨以此书奉献给广大师生。

本书共分12章，内容包括网络安全概述、网络安全技术基础、网络安全体系及管理、密码和加密技术、黑客攻防与检测防御、身份认证与访问控制、操作系统与站点安全、数据库与防护技术、计算机病毒及恶意软件防范、防火墙技术、电子商务及网站安全、网络安全新技术及解决方案。本书中包含了很多经过编者多年实践总结出来的案例及研究成果，便于实际应用。书中带"*"的部分为选学内容。

本书旨在介绍最新的网络安全技术、成果、方法和实际应用，主要有以下特点。

1. 内容先进，结构新颖。本书吸收了国内外大量的新知识、新技术、新方法和国际通用准则，注重科学性、先进性、操作性，图文并茂，学以致用。

2. 注重实用性。坚持"实用、特色、规范"的原则，突出实用及素质能力培养，列出了大量案例和同步实验，将理论知识与实际应用有机结合。

3. 提供丰富的配套资源。为方便师生，本书配有多媒体课件，并提供课程资源网站、实验与习题解答等资源。上海市精品课程资源网站网址为 http://jiatj.sdju.edu.cn/webanq。

本书由主持上海市精品课程建设项目的贾铁军教授任主编并编写第1、6、8、9、12章，嵩天（北京理工大学）任副主编并编写第2章，俞小怡（大连理工大学）任副主编并编写第11章，苏庆刚（上海电机学院）任副主编并编写第10章，沈学东（上海电机学院）任副主编并编写第7章，罗宜元（上海电机学院）编写第4章，王福（公安部第三研究所）编写第3章，陈国秦（腾讯控股有限

公司)编写第5章,宋少婷(大连信源网络科技有限公司)编写部分实验、习题并制作部分课件等,于淼等参加本书编写大纲的讨论、审校等工作。邹佳芹多次对全书的文字、图表进行校对、编排,查阅了大量资料并制作了部分课件。

非常感谢在本书编写过程中给予大力支持和帮助的各界同人。本书在编写过程中参阅了大量重要的文献资料,难以完全准确注明,在此对相关作者深表诚挚谢意!

由于网络安全技术涉及的内容比较庞杂,网络安全技术发展速度快、知识更新迅速,而且作者水平及时间有限,书中难免存在不妥之处,敬请读者海涵。欢迎提出宝贵意见和建议,主编邮箱:jiatj@163.com。

编 者

2014年3月于上海

试读结束:需要全本请在线购买: www.ertongbook.com

目　录

第1章　网络安全概述

21世纪已经进入信息化时代，随着信息技术的快速发展和广泛应用，计算机网络在给人们带来信息资源共享等极大便利的同时，也出现了许多网络安全问题，并成为信息安全的重要研究内容和社会需求量极大的研究方向，不仅关系到企事业机构的信息化建设与发展、网络系统的正常使用以及用户资产和信息资源的安全，也关系到国家安全和社会稳定，不仅成为各国关注的焦点，也成为热门研究和人才需求的新领域。

教学目标

- 掌握网络安全的概念、目标和内容
- 理解网络安全面临的威胁及脆弱性
- 掌握网络安全技术的相关概念、种类和模型
- 理解网络安全研究的现状与趋势
- 了解物理（实体）安全与隔离技术
- 了解构建虚拟局域网的方法

1.1　网络安全概念及内容

【案例1-1】全球重大数据泄露事件频发，针对性攻击持续增多。根据赛门铁克公司2013年10月发布的安全分析报告，全球近几年最严重的一起重大数据泄露事件已造成1.5亿用户的个人资料被泄露。到目前为止所知的数据泄露事件中，被泄露最多的信息为用户的真实姓名、证件账号（如社会保险卡卡号）和出生日期等重要信息，而且各种有针对性的攻击也持续增多。

1.1.1　网络安全的概念及目标

1. 信息安全与网络安全的概念

信息安全的定义目前尚未统一。国际标准化组织（ISO）对信息安全（Information Security）的定义是：为数据处理系统建立和采取的技术与管理等安全保护措施，保护计算机硬件、软件、数据不因偶然及恶意的原因而遭到破坏、更改和泄露。

《中华人民共和国计算机信息系统安全保护条例》将信息安全定义为：计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。信息安全主要是为了防止信息被非授权泄露、更改、破坏或使信息被非法的系统辨识与控制，确保

试读结束：需要全本请在线购买：　www.ertongbook.com

信息的完整性、保密性、可用性和可控性，主要涉及物理（实体）安全、运行（系统）安全与数据（信息）安全三个层面，如图1-1所示。

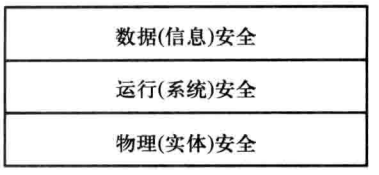


图1-1　一种信息安全的层次模型

拓展阅读：从信息安全的作用层面看，计算机与网络的设备安全称为物理安全或实体安全；计算机与网络设备运行过程中的系统安全，也就是信息系统稳定运行的状态，称为运行安全；对于信息自身的安全，涉及狭义的“信息安全”问题，包括在信息系统中处理、存储数据和在网络中传输数据以及审查过程的安全问题，称为数据安全。信息安全的作用层面也可以称为信息安全的层次模型，这也是国内专家学者广泛认同的关于信息安全的定义方式。

信息安全的发展经历了通信保密、信息安全（以保密性、完整性和可用性为目标）和信息保障三个阶段。进入21世纪，随着信息技术的快速发展与广泛应用，信息安全的内涵也在不断更新和延伸，从最初的信息保密性发展到信息的完整性、可用性、可控性和可审查性，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论、技术和方法。信息安全本身涵盖的范围很广，从防范企业商业机密和用户信息泄露与篡改，防范对不良信息的浏览，到国家军事、政治等机密信息的安全。本书主要侧重网络信息安全。信息安全是一个综合性交叉学科领域，综合利用了数学、信息学、通信和计算机等诸多学科长期积累和最新发展的成果。

信息安全按照范围和处理方式可划分为3个级别：计算机安全、网络安全和信息系统安全。计算机安全是信息安全的基础，网络安全是信息安全的核心。

网络环境下的信息安全称为网络信息安全，其体系是保证信息安全的关键，包括计算机及其网络系统安全、安全协议、安全机制（数字签名、信息认证、数据加密等）、操作系统和数据库系统安全等，其中任何一个漏洞或隐患都可能威胁整个系统的安全。网络信息安全服务包括支持网络信息安全服务的基本理论、技术支持、管理与策略、机制和方法，以及基于新一代网络体系结构的网络安全服务体系结构等。

计算机网络安全（Computer Network Security）简称网络安全，是指利用计算机网络技术、管理、控制和措施，保证网络系统及数据（信息）的保密性、完整性，网络服务的可用性、可控性和可审查性，即保证网络系统的硬件、软件及系统中的数据资源得以完整、准确、连续运行，服务不受干扰、破坏和非授权使用。狭义上，网络安全是指计算机及其网络系统资源和数据资源不受有害因素的威胁和危害。广义上，凡是涉及计算机网络信息安全属性特征（保密性、完整性、可用性、可控性、可审查性）的相关理论、技术和方法等，都是网络安全的研究领域。

网络安全是一门涉及计算机科学、网络技术、信息安全技术、通信技术、计算数学、密码技术和信息论等多个学科的综合性交叉学科，是计算机与信息科学的重要组成部分，为近20年发展起来的新兴学科，集成了信息安全、网络技术与管理、分布式计算、人工智能等多个领域的知识和研究成果，其概念、理论和技术仍在不断发展和完善之中。

2. 网络安全的目标及特征

网络安全问题包括两方面的内容：一是网络的系统安全，二是网络的数据安全，而网络安全

的最终目标和关键是保护网络的数据安全。

网络安全的目标是指计算机网络在信息的采集、存储、处理与传输的整个过程中，根据安全需求，具备相应物理及逻辑上的安全防护、监控、恢复和对抗的能力。网络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保密性、完整性、可用性、可控性和可审查性。其中，保密性、完整性、可用性是网络安全的基本要求。网络信息安全的5大要素反映了网络安全的特征及目标要求，如图1-2所示。

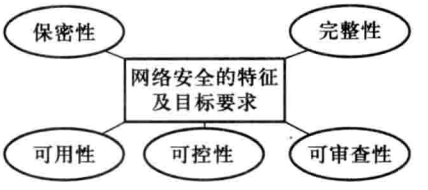


图1-2 网络安全的特征及目标要求

(1) 保密性

保密性(Confidentiality)也称机密性，指保证信息不泄露或不提供给非授权用户、实体和过程。它强调网络中的信息只能被授权用户使用的特征。提供保密性安全服务的因素包括保护数据的位置、数据类型、数据的数量、数据的价值等。

(2) 完整性

完整性(Integrity)是指网络信息未经授权不可改变的特性，即信息在存储或传输过程中保持不被修改及破坏或丢失的特性。完整性也是网络安全最基本的安全特征。

影响信息完整性的因素包括人为和非人为两种。人为因素又分为有意和无意两种，前者是指不法分子对合法用户的系统或数据进行侵扰或破坏，如计算机病毒、网络攻击等；后者是指使用不当或操作失误。非人为因素是指通信过程中的干扰噪声、系统软硬件的差错等。

(3) 可用性

可用性(Availability)也称有效性，是指网络信息系统和信息资源可以被授权用户按照规定要求正常使用或在非正常情况下可恢复使用的特性。可用性是衡量网络信息系统和信息资源面向用户服务的一种安全特性，即在系统运行时可以正确存取所需信息，当系统一旦出现意外或遭受攻击和破坏时，可以快速恢复并可正常使用的能力。网络信息系统只有稳定、持续和正常运行，授权用户才可及时地根据需求获取系统所提供的服务。

(4) 可控性

可控性(Controllability)是指对信息内容和信息传播过程的管理控制能力，对网络系统及信息在一定传输范围和存储空间内的可控程度，用户应能控制授权范围内信息的流向及行为方式。如采用常规传播站点和监控形式，利用加密等策略，严格执行可控规程。可控性也包括网络系统的可靠性(Reliability)，是指网络信息系统可以在规定的条件与时间内，提供特定功能和服务的特性。可控性是所有网络信息系统正常运行的基本前提和保障。

(5) 可审查性

可审查性又称不可否认性(No-repudiation)、抗抵赖性或拒绝否认性，指网络通信双方在信息传输和交互过程中，能够确认发送方的身份和所提供信息的真实同一性，即所有参与者不可能否认或抵赖本人的真实身份，以及所提供信息的原样性和完成的操作与承诺。

网络安全目标俗称要求达到“五不”，即进不来、看不了、改不成、拿不走、跑不掉。

实际上，计算机网络安全的目标需要均衡考虑安全性和网络系统性能的发挥。通常，企事业单位的安全措施包括三个主要目标：对数据的存取控制，保证网络系统及数据的完整性，并在系统发生故障时可进行系统恢复和数据备份。

网络安全实际上是一个相对的概念，世界上的任何事物都没有绝对的安全。通常，只要根据实际需求，在有限的时间内保证系统和数据安全，或让非授权行为在一定的时间和成本范围内难以实现，即可认为系统是安全的。不可过分追求安全性，否则可能降低网络传输速度，同时浪费更多的资源、服务和成本。

拓展阅读：网络安全需求的定义包括三个方面，即网络安全硬件、网络安全软件和网络安全服务。其中，用于保护计算机信息系统安全的专用硬件和软件属于计算机信息系统安全专用产品。由于网络安全与国家安全密切相关，所以各国网络安全产品的关键技术并不公开。发达国家对出口的密码产品会进行各种限制，有些国家甚至会在一些出口的网络安全系统中设置后门，以获取和控制他国的信息或技术。为此，各国既不能引进难以监控的信息网络安全技术和产品，也不能照抄国外的网络安全技术，必须把发展网络安全立足于本国网络安全专业人才的培养和自主创新上。

1.1.2 网络安全涉及的内容及侧重点

可以从不同方面讨论网络安全涉及的主要内容、保护范畴及侧重点。

1. 网络安全涉及的主要内容

通常，从网络安全技术及应用的角度讲，网络安全涉及的内容包括操作系统安全、数据库安全、网络站点安全、病毒与防护、访问控制、加密与鉴别七个方面，具体内容将在后续章节详细介绍。从层次结构上来讲，也可以将网络安全涉及的内容概括为物理安全、运行安全、系统安全、应用安全和管理安全五个方面。

（1）物理安全

物理安全（Physical Security）也称实体安全，指保护硬件系统和软件系统，即计算机网络设备、设施及其他媒介免遭水灾、火灾、盗窃、雷击、地震、有害物质、静电和其他环境事故破坏的措施及过程，包括环境安全、设备安全和媒体安全三个方面。物理安全是信息系统安全的基础，包括机房安全、场地安全、机房环境（温度、湿度、电磁、噪声、防尘性、静电及振动等）、建筑安全（防火、防雷、围墙及门禁安全）、设施安全、设备可靠性、通信线路安全、辐射控制与防泄露、动力、电源/空调、灾难预防与恢复等。

（2）运行安全

运行安全（Operation Security）主要是指为了网络系统正常运行和服务所采取的各种安全措施，包括计算机网络及系统运行安全和网络访问控制的安全，如设置防火墙实现内外网的隔离，实施网络访问控制，意外时进行系统应急备份及系统恢复。运行安全包括内外网的隔离机制、系统升级与加固、网络系统安全性监测、网络安全产品运行监测、应急处置机制与配套服务、灾难恢复机制与预防、定期检查与评估、跟踪最新安全漏洞、安全审计、系统升级改造、网络安全咨询等。

（3）系统安全

系统安全（System Security）主要是指为了确保整个系统的安全所采取的各种安全举措，主要包括操作系统安全、数据库系统安全和网络系统安全。根据网络系统的特点、实际条件和管理要求，通过有针对性地为系统提供安全策略、保障措施、应急修复方法、安全建议和安全管理规范等，确保整个网络系统的安全运行。

(4) 应用安全

应用安全(Application Security)主要是指确保各种用户实际应用和服务安全的措施。应用安全由应用软件开发平台的安全和应用系统的数据安全两部分组成,主要包括数据资源访问控制验证测试、用户身份鉴别检测、业务应用软件安全性测试分析、业务数据安全检测与审计、数据唯一性/一致性/防冲突检测、数据保密性测试、业务现场的备份与恢复机制检查、系统可靠性测试和系统可用性测试等。

(5) 管理安全

管理安全(Management Security)也称为安全管理,主要是指对相关人员及网络系统进行安全管理的各项内容,包括法律法规、政策策略、规范标准、人员管理、应用系统使用管理、软件管理、设备管理、文档管理、数据管理、操作管理、运营管理、机房管理、安全教育与培训等。

图 1-3 网络安全的层次结构

从层次结构上讲,网络安全所涉及的主要内容及其关系如图 1-3 所示。具体来说,就是在网络信息安全法律法规的基础上,以管理安全和运行安全为保障,贯穿整个实体安全、操作系统安全、网络安全和应用安全的全过程,确保网络正常运行与服务的安全、平稳、有序。

从体系结构方面讲,网络信息安全的主要内容及其相互关系如图 1-4 所示。

从网络安全攻防体系方面讲,可以将网络安全研究的主要内容概括为两个体系:攻击技术和防御技术,如图 1-5 所示。

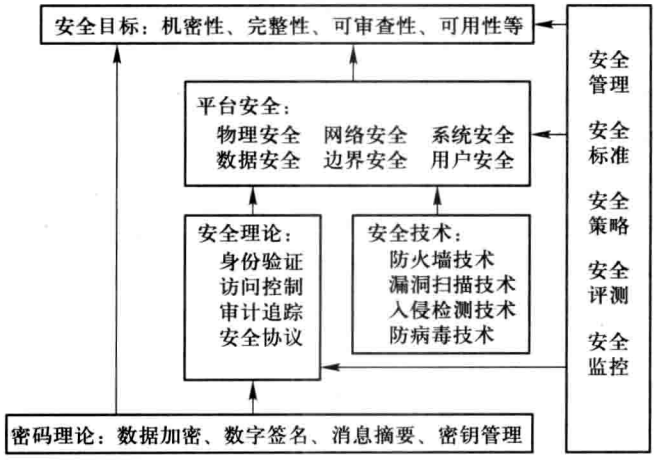


图 1-4 网络信息安全的内容及其相互关系

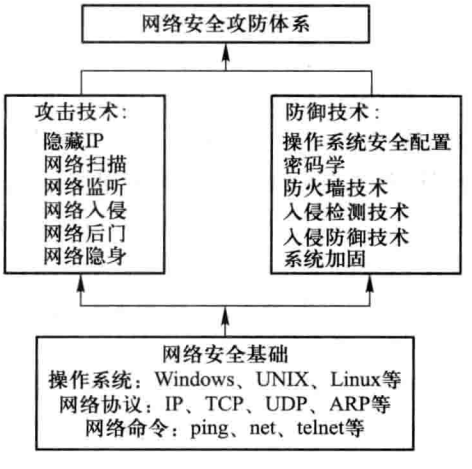


图 1-5 网络安全攻防体系

拓展阅读:国外面向属性的网络信息安全框架将网络信息安全确定为 3 个层次的结构:机密性、完整性和可用性。国内面向应用的网络信息安全框架将网络信息安全结构从上至下分为内容安全、数据安全、运行安全和实体安全。国内也有一些专家或学者从不同的内涵和外延将网络信息安全分为 3 个层次:法律保障、安全管理和安全技术,或 4 个层次:实体安全、逻辑安全、操作系统安全和联网安全。

2. 网络安全的保护范畴及侧重点

通常,狭义上的网络安全与计算机系统安全、数据安全和密码安全密切相关,但涉及的保护范畴不同。计算机系统安全的保护范畴是系统硬件、软件和相关文件等,通过系统运行环境访问控制与限制,或利用专用软件或操作系统的安全功能进行安全保护;数据安全的保护范畴包括所有数据资源在采集、存储、处理、传输等过程中的安全;密码安全是数据安全、网络安全和计算机系统安全的基础与核心,也是身份认证、访问控制、审查和防止信息泄露的最有效手段。

网络安全涉及技术和管理等多个方面,需要相互补充、综合防范。网络安全技术主要侧重于利用技术手段防范外部攻击和病毒等,网络安全管理则侧重于内部人为因素的管理。如何更有效地保护重要数据,提高网络系统的安全性,已经成为必须解决的重要问题。

实际上,网络安全涉及的内容对于不同人员或部门,侧重点也有所不同。

(1) 网络安全研究人员

通常,网络安全研究人员对于具体的网络安全问题,关注从理论上采用数学等方法精确描述安全问题的特征,之后通过建立安全模型等手段具体解决。

(2) 网络安全工程师

网络安全工程师或研发工程师主要侧重于采用网络安全工程技术和方法,从实际应用角度出发,开发更成熟的网络安全解决方案和新型网络安全产品,注重网络安全工程建设开发与管理、安全防范工具、操作系统防护技术和安全应急处理措施等。

(3) 网络安全评估人员

网络安全评估人员一般关注的是网络安全评价标准与准则、安全等级划分、网络安全风险评估、安全产品测评方法与工具、网络问题的评价、网络信息采集与分析等。

(4) 网络安全管理员

网络安全管理员主要关注与网络安全管理有关的策略、机制、身份认证、访问控制、入侵检测、系统加固与防御措施、网络安全审计、网络安全应急响应和计算机病毒防治等安全管理技术和举措,主要职责是进行与网络安全管理相关的制度建设、安全策略与机制优化、规划与计划管理、总结与反馈、配置与维护等,保障授权用户快捷、方便地访问网络资源。同时,协助网络安全技术人员防范非法访问、黑客攻击、病毒侵扰、服务中断和垃圾邮件等各种威胁,并做好安全审计,系统一旦遭到破坏,能够采取相应的应急响应和恢复等措施。

(5) 安全保密监察人员

安全保密监察人员必须掌握网络信息泄露、窃听、检测和过滤等各种技术手段,确保涉及国家政治、军事、经济等重要机密信息的安全;检测和过滤威胁国家安全的不良信息,以免给国家安全和稳定带来不利影响。对于公共安全机构,应当熟悉国家和行业部门颁布的常用网络安全监察法律法规,了解网络安全取证、网络安全审计、知识产权保护、社会文化安全等规定和措施,对于窃取或破坏商业机密信息、电子出版物侵权、软件盗版、色情与暴力信息传播等各种违法犯罪行为,能够进行有效的网络监察、取证和处置。

(6) 军事国防相关人员

军事国防相关人员更注重信息对抗、信息加密、安全通信协议、无线网络安全、入侵攻击与防范、应急处理和网络病毒传播等网络安全的新技术和新方法,设法取得网络信息优势,扰乱敌方指挥系统,摧毁敌方网络基础设施,以打赢未来信息战争。

除相关专业人员和机构外，所有网络用户都应关心实际应用中的网络安全问题，注意保护个人隐私和商业信息安全。

讨论与思考：

(1) 什么是信息安全和网络安全？网络安全的目标是什么？
(2) 网络安全所研究的主要内容是什么？
(3) 网络安全与信息安全的相关内容及其关系如何？

1.2 网络安全的威胁及隐患

明确网络安全威胁的现状及发展态势，有利于更好地学习和理解网络安全的重要性、必要性和重要现实意义，有助于深入探究和强化网络安全。

1.2.1 国内外网络安全的现状

【案例 1-2】我国网络遭受攻击近况。据国家互联网应急中心(CNCERT)和国家信息安全漏洞共享平台(CNVD)发布的数据，2014 年 2 月 10 日至 16 日的一周内，中国境内被篡改的网站数量为 8 965 个，较前一周增长了 79.7%；被植入后门的网站数量为 1 168 个；被仿冒的网站页面数量为 181 个。其中，政府网站被篡改 418 个，植入后门 35 个。感染网络病毒的主机数量约为 69 万个，新增信息安全漏洞 280 个。

另据 CNCERT 的数据显示，中国遭受境外网络攻击的情况日趋严重。CNCERT 抽样监测发现，2013 年 1 月 1 日至 2 月 28 日，境外 6 747 台木马或僵尸网络控制服务器控制了中国境内 190 万余台主机，其中位于美国的 2 194 台控制服务器控制了中国境内 128.7 万台主机。无论是按照控制服务器数量还是按照控制中国主机数量排名，美国都名列第一。

国内外网络安全威胁现状主要包括以下 5 个方面。

(1) 法律法规和管理不完善

随着信息技术的快速发展和广泛应用，国内外的法律法规和管理政策等在解决信息资源保密性、完整性、可用性、可控性、可审查性等方面出现了一些问题，显得相对滞后且不够健全与完善。一些企事业机构或个人用户的法制观念淡薄，对网络风险和隐患不甚了解，网络安全意识不强，自身管理措施和方法不完善，甚至出现了内部监守自盗的案件。重技术、轻管理以及网络安全知识不够普及已经成为一个重要问题。

(2) 企业和政府的侧重点不一致

政府注重信息及网络安全的可管性和可控性，企业则注重其可用性、效益和可靠性。由国际标准化组织 ISO 制定的 OSI 协议及美国政府组织研发的 KRS 系统等，由于不受企业欢迎而难以实施和推广。一些欠发达国家或地区对网络安全技术重视不够，经费投入无法满足实际需要，或时常被挤占及挪用。

(3) 网络安全规范和标准不统一

网络安全是一个系统工程，只有统一技术的规范和标准，才能更好地实施。美国的计算机网

试读结束：需要全本请在线购买： www.ertongbook.com