信息安全专业系列教材

信息安全导论

Xinxi Anquan Daolun

李 剑 编著

北京邮电大学出版社
www.buptpress.com

信息安全专业系列教材

信息安全导论

李　剑　编著

北京邮电大学出版社
·北京·

内 容 简 介

作为一本信息安全普及教材，本书介绍了信息安全领域最常用的知识。书中内容共 14 章。第 1 章是信息安全概述。第 2 章是黑客攻击技术。第 3 章是密码学基础。第 4 章是防火墙。第 5 章是入侵检测。第 6 章是 VPN 技术。第 7 章是信息安全协议。第 8 章是 Windows 操作系统安全。第 9 章是 Linux/Unix 操作系统安全。第 10 章是计算机病毒。第 11 章是 PKI 系统。第 12 章是信息系统安全管理。第 13 章是信息系统风险评估。第 14 章是信息系统应急响应。

本书适用于大学本科相关专业，可起到信息安全导向的作用。

图书在版编目(CIP)数据

信息安全导论/李剑编著. —北京：北京邮电大学出版社，2007

ISBN 978-7-5635-1473-1

Ⅰ. 信… Ⅱ. 李… Ⅲ. 信息系统—安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2007)第 141914 号

书　　名：信息安全导论

编　　著：李　剑

责任编辑：李欣一

出版发行：北京邮电大学出版社

社　　址：北京市海淀区西土城路 10 号(邮编：100876)

北方营销中心：电话：010-62282185　传真：010-62283578

南方营销中心：电话：010-62282902　传真：010-62282735

E-mail：publish@bupt.edu.cn

经　　销：各地新华书店

印　　刷：北京忠信诚胶印厂

开　　本：787 mm×960 mm　1/16

印　　张：16.5

字　　数：356 千字

印　　数：1—3 000 册

版　　次：2007 年 9 月第 1 版　2007 年 9 月第 1 次印刷

ISBN 978-7-5635-1473-1　　定　价：26.00 元

第 2 版总序

发展 21 世纪中国信息安全要靠教育，而搞好信息安全教育就需要好的教材。2004 年，北京邮电大学信息安全中心完成了第一套信息安全专业本科系列教材，该套教材被评为“北京市高等教育精品教材立项项目”，而后又被教育部列入“普通高等教育‘十五’国家级规划教材”。至今，三年多的时间过去了，这套教材在信息安全专业的教学中发挥了重要的作用，起到了较好的教学效果，受到教师和学生的好评。

在这三年中，我们始终致力于包括专业建设、课程建设、师资建设、教材建设、实训基地建设、实验室建设及校企就业（创业）平台建设等在内的信息安全本科专业的全面建设。2005 年，作为组长单位，我们完成了教育部“信息安全专业规范研究”和“信息安全学科专业发展战略研究”课题；召开了“全国高校本科‘信息安全专业规范与发展战略研究’成果发布与研讨会”；在国内第一次制定了信息安全专业规范，从知识领域、知识单元和知识点三个层次构建学科专业教学的知识体系；由通识教育内容、专业教育内容和综合教育内容三大部分构建课程参考体系；采用顶层设计的方法构建了带有实践性环节的教学体系；在国内第一次较全面地提出信息安全学科专业教学改革与创新研究的发展思路和政策建议，成果提交教育部教学指导委员会，对于引导高等学校信息安全学科专业教学改革与建设，指导信息安全学科专业评估，促进信息安全学科专业教学规范建设与管理，提高专业教育质量和水平有重要的作用。多所举办信息安全专业的高校都参照课题成果调整了自己的教学计划、课程体系和实验方案。

积极搭建信息安全专业校际交流平台。组织成立了“全国信息安全本科教材编写委员会”和“全国信息安全本科专业师资交流与培训互助组”。主持召开了“全国信息安全专业教学经验交流和师资培训研讨会”及“全国信息安全专业实验室建设和实验课程教学经验交流研讨会”。在四川绵阳建设了占地两万六千多平方米的全国信息安全专业本科生实习实训基地，接收了来自全国近 30 所高校的本科生进入该基地参加丰富多彩的实训。

努力建设精品课程。召开了“全国高校信息安全专业精品课程建设经验交流会议”，来自全国各地高校的专家齐聚北邮，介绍与交流了精品课程建设的经验。组织建设了全国第一批信息安全实验室，并且编写出版了信息安全实验指导教材，2007 年，我们的《现代密码学》课程申报了北京市精品课程，已经被专家评审通过，目前正在申报 2007 年度“国家精品课程”。

三年多的时间过去了，信息安全的教育和产业都取得了丰硕的成果，随着信息安全向更高层次的发展，其趋势已经从基础的网络层建设开始向内容层建设过渡。为适应信息安全教育的发展需要，积极探索培养创新型高素质人才，我们按照制定的学科发展战略和专业规范的精神，结合近几年的教学实践，对原信息安全专业本科系列教材进行了全面修订。这次修订不仅对原来的系列教材在第1版的基础上进行修改和完善，还补充了信息安全最新的研究成果，使教材的内容更加翔实和新颖。同时，在原有体系的基础上又增加了一些新的课程教材。在新修订的系列教材中，目前有《信息安全概论(第2版)》、《现代密码学及其应用》、《网络安全(第2版)》、《信息安全管理》、《计算机病毒原理与防治(第2版)》、《数字版权管理》、《计算机系统安全》、《网络安全实验教程》、《信息安全专业科技英语》、《防火墙、入侵检测与VPN》、《对称密码学及其应用》、《信息安全导论》等12本教材。随着信息安全专业教学的需要，今后还将不断有新的教材补充进来。希望通过对内容的精心组织和设计能促进信息安全课程的建设，同时涌现出更多的信息安全精品课程。

在这次修订中，我们组织了强大的师资队伍，将多次讲授相关课程的教师充实到本次修订队伍中。经过反复研讨，本着理论与实际相结合的原则，对原来的系列教材进行了较大的修改和扩充，我们希望这套新修订的系列教材能够满足国内各类高校信息安全本科专业以及相关方向的不同需求。

虽然我们在这次修订中投入了很大精力，但是由于水平有限，时间仓促，且信息安全专业的发展速度非常快，不足之处和错误在所难免，我们衷心期望使用和关心该系列教材的师生，继续对新的系列教材提出宝贵意见和建议。

本系列教材也是国家重点基础研究发展计划(973)(课题编号：2007CB310704和2007CB311203)资助的成果，并在积极申报“普通高等教育‘十一五’国家级规划教材”。

在本系列教材的修订过程中，得到了北京邮电大学出版社的大力支持，同时也得到了北京邮电大学信息安全中心成员的支持与配合，在此一并表示感谢。

教授、博士生导师、全国政协委员

杨义先

前　言

北京邮电大学信息工程学院较早在全国开设了信息安全本科专业。为了引导大学本科生对信息安全这一专业所涉及的专业知识有一个全面的了解，作者编写了《信息安全导论》这本书。本教材比较全面地介绍了目前信息安全领域常用的攻击技术和防护技术，以及信息安全管理的知识，但是所讲述的内容都不深，只是起到导向的作用。本教材适合于大学本科相关专业的学生。

在讲解时，教师可以根据所要教的学生对象来选择要教的内容以及内容的深度。本书共分为14章内容。

第1章是信息安全概述，主要包括信息安全的概念、信息安全发展过程、信息安全的基本要素以及信息安全的需求和实现等。第2章是黑客攻击技术，包括黑客的概述、黑客攻击的概念、信息系统的安全威胁、攻击的一般流程、攻击的技术与方法、恶意软件的防治等。第3章是密码学基础，包括密码学的历史、密码学的发展、密码体制的分类、密码学与信息安全的关系、古典密码学、对称密码学、非对称密码学、Hash算法、密码学的新方向等。第4章是防火墙，包括防火墙的概念、防火墙的分类、防火墙的作用、防火墙技术、防火墙体系结构、防火墙的硬件实现技术、防火墙的发展等。第5章是入侵检测，包括入侵检测的概念、入侵检测的历史、入侵检测的作用、入侵检测的分类、入侵检测技术、入侵检测的标准化、入侵检测的发展等。第6章是VPN技术，包括VPN的概念、VPN的分类、VPN的特点、VPN技术、VPN的发展趋势等。第7章是信息安全协议，包括Kerberos协议、SSL协议、SET协议、IPSec协议等。第8章是Windows操作系统安全，包括Windows操作系统安全基本配置、Windows操作系统安装注意事项等。第9章是Linux/Unix操作系统安全，包括Linux/Unix操作系统安全概述、Linux/Unix操作系统安全技术等。第10章是计算机病毒，包括计算机病毒的分类、计算机病毒的特征、计算机病毒的清除、计算机病毒的工作原理、典型计算机病毒的介绍、计算机病毒的发展等。第11章是PKI系统，包括PKI系统的来历、PKI系统的概述、PKI系统的组成、PKI系统的体系结构、数字证书、PKI系统的应用与发展等。第12章是信息系统安全管理，包括信息安全管理模式、建立信息安全管理的意义、信息安全相关法律法规等。第13章是信息系统风险评估，包括风险评估的概念、风险评估的意义、风险评估的方法、国际主流风险评估标准等。第14章是信息系统应急响应，包括应急响应的概念、应急响应的目标和任务、应

急响应的阶段、应急响应的方法、计算机犯罪取证等。

感谢杨义先教授、罗群副教授，他们对本书的出版提出了宝贵的意见和建议。参与本书审阅编写等工作的还有景博等，这里一并谢过！

最后作者对本书用到的参考文献的作者和一些资料的作者表示衷心的感谢。

由于水平有限，本书疏漏与错误之处在所难免，恳请广大同行和读者指正，我将在下一版中改正。我的电子邮箱是 lijian@bupt.edu.cn。

李　剑

目　　录

第1章

信息安全概述

随着互联网的飞速发展，信息作为一种无形的资源，被广泛应用于政治、军事、经济、科研等各行各业，其重要性与日俱增。然而，随之所带来的安全性问题也越来越多。

在计算机问世之初，计算机的数量还相当少，懂得计算机技术的人也不多，那时的计算机应用的安全性问题不十分突出。20世纪80年代以后，分布式网络日益普及，跨国的计算机网络逐渐建立起来，最明显的例子是因特网在全球的迅速普及和发展。根据美国国家科学基金会(U. S. National Science Foundation)的统计，1995—2003年，因特网的用户数从3 000万增加到了10亿以上，为今天的计算机犯罪的产生和发展提供了温床。据统计，1998—2003年，信息安全事件增长了23倍(1998年为3 734次，2003年为127 529次)。以下是几个计算机犯罪的例子。

1988年11月2日，美国康奈尔大学的学生罗伯特·莫里斯释放多个蠕虫病毒，造成因特网上近6 000台主机瘫痪，据称损失高达几千万美元。

1989年3月2日凌晨，3名德国黑客因涉嫌向前苏联出售机密情报被捕，他们在两年多的时间内，闯入了许多北约国家和美国的计算机系统，窃取了许多高度机密的信息。

1996年9月，美国中央情报局的主页被一群远在瑞典的少年黑客改为中央笨蛋局(Central Stupidity Agency)。

2000年10月，黑客人侵微软公司并获取微软新开发产品的机密源代码事件披露，震动了微软公司高层，其中包括比尔·盖茨本人。有的媒体冠以“黑客太黑，微软太软”的大标题，以讽刺连微软这样的著名公司都无法挡住黑客凶猛的攻击。

上述事实说明，在信息时代，信息系统的安全性已经成为非常重要的研究课题。利用计算机进行信息犯罪已经侵入到政府机关、军事部门、商业、企业等单位，如果不加以遏制，轻则干扰人们的日常生活，重则造成巨大的经济损失，甚至威胁到国家的安全，所以信息安全已经引起许多国家，尤其是发达国家的高度重视，它们不惜在此领域投入大量的人力、物力和财力，以达到提高计算机信息系统安全的目的。

1.1 信息的概念

ISO/IEC 的 IT 安全管理指南(GMITS,即 ISO/IEC TR 13335)对信息(Information)的解释是:信息是通过在数据上施加某些约定而赋予这些数据的特殊含义。

一般意义上的信息是指事物运动的状态和方式,是事物的一种属性,在引入必要的约束条件后可以形成特定的概念体系。通常情况下,可以把信息理解为消息、信号、数据、情报和知识。信息本身是无形的,借助于信息媒体以多种形式存在或传播,它可以存储在计算机、磁带、纸张等介质中,也可以记忆在人的大脑里,还可以通过网络等方式进行传播。

对现代企业来说,信息是一种资产,包括计算机和网络中的数据,还包括专利、标准、商业机密、文件、图纸、管理规章、关键人员等,就像其他重要的商业资产那样,信息资产具有重要的价值,因而需要进行妥善保护。

需要注意的是,要从安全保护的角度去考察信息资产,不能只停留在静态的一个点或者一个层面上。信息是有生命周期的,从其创建或诞生,到被使用或操作,到存储,再到被传递,直至其生命期结束而被销毁或丢弃,各个环节各个阶段都应该被考虑到,安全保护应该兼顾信息存在的各种状态,不能遗漏。

1.2 信息安全的概念

“安全”一词的基本含义为:“远离危险的状态或特性”,或“主观上不存在威胁,主观上不存在恐惧”。在各个领域都存在着安全问题,安全问题是普遍存在的。随着计算机网络的迅速发展,人们对信息的存储、处理和传递过程中涉及的安全问题越来越关注,信息领域的安全问题变得非常突出。

信息安全是一个广泛而抽象的概念,不同领域、不同方面对其概念的阐述都会有所不同。建立在网络基础之上的现代信息系统,其安全定义较为明确,那就是:保护信息系统的硬件、软件及相关数据,使之不因为偶然或者恶意侵犯而遭受破坏、更改及泄露,保证信息系统能够连续、可靠、正常地运行。在商业和经济领域,信息安全主要强调的是削减并控制风险,保持业务操作的连续性,并将风险造成的损失和影响降低到最低程度。

信息安全就是关注信息本身的安全,而不管是否应用了计算机作为信息处理的手段。信息安全的任务是保护信息资源,以防止偶然的或未授权者对信息的恶意泄露、修改和破坏,从而导致信息的不可靠或无法处理等。这样可以在人们最大限度地利用信息的同时使得损失最小。

信息技术的应用，引起了人们生产方式、生活方式和思想观念的巨大变化，极大地推动了人类社会的发展和人类文明的进步，把人类带入了崭新的时代——信息时代。在这个时代里，信息已经成为社会发展的重要资源。然而，人们在享受信息资源所带来的巨大利益的同时，也面临着信息安全的严峻考验。信息安全已经成为世界性问题。

信息安全之所以引起人们的普遍关注，是由于信息安全问题目前已经涉及人们日常生活的各个方面。以网上交易为例，传统的商务动作模式经历了漫长的社会实践，在社会的意识、道德、素质、政策、法规和技术等各个方面，都已经完善，然而对于电子商务来说，这一切却处于刚刚起步阶段，其发展和完善将是一个漫长的过程。所谓的电子商务是指利用各种电子工具和电子技术从事各种商务和贸易活动的过程，是整个商务和贸易活动的自动化和电子化。假设作为电子商务活动中的交易人，无论从事何种形式的电子商务都必须清楚以下事实：交易方是谁？信息在传输过程中是否会被篡改（即信息的完整性）？信息在传送途中是否会被外人看到（即信息的保密性）？网上支付后，对方是否会不认账（即不可抵赖性）？等等。因此，无论是商家、银行还是个人，对电子交易安全的担忧是必然的，电子商务的安全问题已经成为阻碍电子商务发展的瓶颈，如何改进电子商务的现状，让用户不必为安全担心，是推动安全技术不断发展的动力。

信息作为一种资产，是企业或组织进行正常商务运作和管理不可或缺的资源。从最高层次来讲，信息安全关系到国家的安全；对组织机构来说，信息安全关系到正常运作和持续发展；就个人而言，信息安全是保护个人隐私和财产的必然要求。无论是个人、组织还是国家，保持关键的信息资产的安全性都是非常重要的。信息安全的任务，就是要采取措施（技术手段及有效管理）让这些信息资产免遭威胁，或者将威胁带来的后果降到最低程度，以此维护组织的正常运作。

总的来说，凡是涉及保密性、完整性、可用性、可追溯性、真实性和可靠性保护等方面的技术和理论，都是信息安全所要研究的范畴，也是信息安全所要实现的目标。

1.3 信息安全的威胁

信息安全的威胁是指某个人、物、事件或概念对信息资源的保密性、完整性、可用性或合法使用所造成的危险。攻击就是对安全威胁的具体体现。

目前还没有统一的方法来对各种威胁进行分类，也没有统一的方法来对各种威胁加以区别。信息安全所面临的威胁与环境密切相关，不同威胁的存在及重要性是随环境的变化而变化的。下面给出一些常见的安全威胁。

（1）服务干扰：以非法手段窃得对信息的使用权，恶意添加、修改、插入、删除或重复某些无关信息，不断对网络信息服务系统进行干扰，使系统响应减慢甚至瘫痪，影响用户的正常使用，如一些不法分子在国外干扰我国正常卫星通信等。