

新编高等院校信息管理与信息系统专业核心教材

信息系统安全导论

Introduction to Information System Security

方勇 刘嘉勇 编著
戴宗坤 罗万伯 审校



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

<http://www.phei.com.cn>

新编高等院校信息管理与信息系统专业核心教材

信息系统安全导论

Introduction to Information System Security

方 勇 刘嘉勇 编著
戴宗坤 罗万伯 审校

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有,侵权必究。

图书在版编目(CIP)数据

信息系统安全导论/方勇,刘嘉勇编著. —北京:电子工业出版社,2003.3
新编高等院校信息管理与信息系统专业核心教材
ISBN 7-5053-8592-5

I. 信… II. ①方…②刘… III. 信息系统—安全技术—高等学校—教材 IV. TP309
中国版本图书馆 CIP 数据核字(2003)第 018335 号

责任编辑:韩同平

印刷:北京李史山胶印厂

出版发行:电子工业出版社 <http://www.phei.com.cn>

北京市海淀区万寿路 173 信箱 邮编 100036

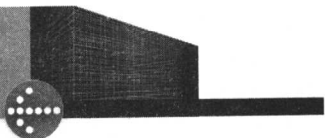
经销:各地新华书店

开本:787×980 1/16 印张:27.5 字数:567.6 千字

版次:2003 年 4 月第 1 版 2003 年 4 月第 1 次印刷

印数:5 000 册 定价:33.00 元

凡购买电子工业出版社的图书,如有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系。联系电话:(010)68279077



新 编 高 等 院 校
信 息 与 管 理
信 息 系 统
专 业 核 心 教 材

顾 问 (按姓氏笔画排序)

马费成 陈 禹 黄梯云

编委会 (按姓氏笔画排序)

马费成 王要武 叶继元
李一军 汪玉凯 陈京民
吴玲达 张维明 张基温
赵国俊 高 阳 戴宗坤

执行主编

张基温

总序

Z O N G X U

20 世纪 70 年代, 当强大的信息化巨潮还蕴藏在大洋深处, 我们的陆地还只有一阵微风吹来之时, 有识之士们就开始推动信息化专业人才的培养计划, 为迎接即将到来的信息化巨潮扩军备战。他们一方面推动着信息技术的普及; 一方面根据不同领域的需求, 从不同的角度创办了不同类型的信息化专业, 这就是管理信息系统专业、经济信息管理专业、科技信息管理专业、医学信息管理专业、林业信息管理专业、农业信息管理专业……实际上, 这些专业培养目标可以概括为: 为各行业、各部门培养以 CIO 为目标的信息化专门人才。从这一点上看, 这些专业的课程设置应当具有相当大的共同性。1996 年, 出于多种考虑, 教育部将这些专业合并为一个——信息管理与信息系统专业。

以 CIO 为目标的信息化专门人才是一类管理人才。但是他们所管理的主要对象是信息。这样的知识需求, 将信息管理与信息系统专业定位于管理学科, 与信息学、经济学、法学等学科交叉。这样的学科特点, 给课程建设和教材建设带来不少困难。近 30 年来, 尽管我们与许多的同行已经进行了不懈的努力, 把信息管理与信息系统专业的课程建设和教材建设向前推进了一大步, 但是仍然不尽人意, 许多课程和教材还没有体现信息管理专业的特色和需要。在多次有关的研讨会上, 大家一致呼吁编写一套真正体现信息管理与信息系统专业特色的教材。

新编和出版一套专业教材是要冒风险的。而编写和出版一套以瞬息万变的信息和信息技术为管理对象的专业教材就要冒更大的风险。国内信息业界著名的出版商——电子工业出版社, 以超人的胆略愿意同我们一道承担这一风险, 组织编写出版一套新的信息管理与信息系统专业核心教材。这套教材冠以“新编”二字, 是试图在其体系上能比已有教材更体现信息专业的特色, 同时在内容上要能反映最新信息技术的进步以及最新信息管理思想和方法。

目前, 国内开设信息管理与信息系统专业的高等院校已经超过 200 所。这样一个数字一方面表明信息化已经深入人心, 信息化队伍的规模正在急速扩大, 信息化队伍的素质正在不断提高; 另一方面, 也给我们添加了巨大的压力,

使我们深感责任重大。好在国内本领域的三位知名学者——黄梯云、陈禹、马费成以及其他一批有名专家和后起之秀愿意与我们共担风险，鼓舞了我们挑起这副重担的勇气。同时，我们也把这套教材的不断精化寄希望于广大的同仁，愿我们把这套教材越改越好，永改永新。

新编高等院校信息管理与信息系统

专业核心教材编委会

2002年5月

本书针对高等院校信息管理与信息系统、计算机、通信、信息安全等专业的本科生和硕士研究生的教学特点，更加强调理论和工程技术应用相结合而编写的教材。

本书的重点在于给出信息系统安全的基础理论背景知识、信息系统安全体系结构、开放系统互连安全框架及其机制性技术、系统安全技术和基本知识。在系统安全技术方面，对信息系统的入侵与攻击技术、防火墙技术、入侵检测与监控技术、物理隔离技术及防病毒技术的主要内容进行了介绍，并给出了一部分具体的运用方案。本书特别通过对信息系统安全的五大安全服务和多种实现机制的较为完整而系统的介绍，使读者能系统地了解并掌握信息系统安全体系的构建方法、信息系统安全框架及其实现机制的主要内容。

本书由两部分构成。第一部分包括第1章，从信息系统和信息系统安全的层次结构引出与信息系统安全有关的问题，并从信息系统风险控制点及其对抗措施梗概和安全工程方法论方面为第二部分进行了必要的准备和铺垫。第二部分包括第2~6章，从信息系统安全体系的构建方法出发，对安全框架、安全服务和安全机制进行了较为详细的介绍，比较完整和系统地给出了信息系统安全体系的架构及支持技术。重点讨论了防火墙技术、入侵检测与漏洞扫描技术、物理隔离技术，同时对恶意程序与病毒对计算机及网络系统的威胁及其对策，以及技术实现方法进行了讲解，并对PKI做了较为详细的介绍。全书涉及的内容十分广泛，本科生或研究生在学习时，可根据学时数在内容、重点和深度方面进行选择。

本书由四川大学信息安全研究所组织编写，戴宗坤教授做了全书的结构设计和统筹，并由戴宗坤和罗万伯教授对全书进行了审校。方勇编写第1，4，6章及第5章的5.3节，其余部分由刘嘉勇编写。

四川大学信息安全研究所全体同志为本书的编写提供了优越的工作环境和多方面的帮助。本书的编写还从其他同行的著作（包括网站）中得到了帮助。作者在此一并表示衷心的感谢。

由于作者水平有限，且本书涉及较多新概念、新内容和研究课题，再加上技术发展很快，因此，本书中难免存在缺点和错误，诚望读者批评赐教，为推动我国信息系统安全工程高级技术人才的培养共同出力。

作 者

于四川大学信息安全研究所

Introduction to

新编高等院校信息管理与信息系统
专业核心教材顾问

(按姓氏笔画排序)

马费成 陈禹 黄梯云

新编高等院校信息管理与信息系统
专业核心教材编委会

(按姓氏笔画排序)

马费成 王要武 叶继元
李一军 汪玉凯 陈京民
吴玲达 张维明 张基温
赵国俊 高阳 戴宗坤

执行主编：张基温

111111

新编高等院校信息管理与信息系统
专业核心教材

书 目

信息网络技术原理

计算机系统原理

数据仓库与数据挖掘技术

信息系统安全导论

管理信息系统

信息检索导论

信息系统工程

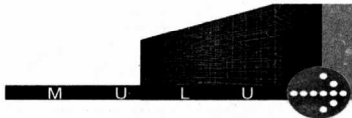
多媒体技术

信息资源开发与管理

数据库技术与应用

电子政务

电子商务原理



第 1 章 绪论	(1)
1.1 信息系统概述	(2)
1.1.1 信息系统的定义	(2)
1.1.2 信息系统的发展过程	(2)
1.2 信息系统安全	(3)
1.2.1 基本概念	(3)
1.2.2 信息保密与信息系统安全	(5)
1.3 影响信息系统安全的因素	(6)
1.3.1 信息系统自身的安全脆弱性	(6)
1.3.2 对信息系统安全的威胁	(10)
1.4 信息系统安全的防御策略	(14)
1.4.1 防御策略的基本原则	(14)
1.4.2 信息系统安全的工程原则	(17)
1.4.3 典型信息系统的安全需求分析	(18)
1.5 信息系统安全要素	(22)
1.5.1 信息系统的安全目标	(22)
1.5.2 信息系统安全的构成要素	(22)
1.6 信息系统安全保护等级划分准则	(29)
1.6.1 第一级 用户自主保护级	(30)
1.6.2 第二级 系统审计保护级	(30)
1.6.3 第三级 安全标记保护级	(31)
1.6.4 第四级 结构化保护级	(32)
1.6.5 第五级 访问验证保护级	(32)
本章小结	(33)
思考题	(34)
第 2 章 信息系统安全体系	(35)
2.1 ISO 开放系统互连安全体系结构	(36)
2.1.1 安全体系的安全服务	(37)

2.1.2	安全体系的安全机制	(43)
2.2	TCP/IP 安全体系	(48)
2.2.1	Internet 网络体系结构	(49)
2.2.2	Internet 安全体系结构	(51)
2.2.3	网络层安全协议 IPsec	(55)
2.2.4	传输层安全协议 TLS	(72)
2.3	开放系统互连的安全管理	(80)
2.3.1	安全管理的概念	(80)
2.3.2	安全管理的主要内容	(80)
	本章小结	(83)
	思考题	(84)
第 3 章	安全服务及功能配置	(85)
3.1	概述	(86)
3.2	机密性保护	(86)
3.2.1	基本概念	(86)
3.2.2	机密性服务及面临的威胁	(89)
3.2.3	机密性策略的表达方法	(91)
3.2.4	机密性服务信息和设施	(92)
3.3	访问控制服务	(93)
3.3.1	访问控制服务功能	(93)
3.3.2	访问控制组件的分布及威胁	(99)
3.3.3	访问控制策略与实现	(100)
3.3.4	访问控制信息 (ACI)	(106)
3.3.5	访问控制服务设施	(108)
3.4	鉴别服务	(110)
3.4.1	基本概念	(111)
3.4.2	鉴别信息	(113)
3.4.3	人类用户鉴别	(116)
3.4.4	鉴别的阶段	(118)
3.4.5	可信第三方的参与	(119)
3.4.6	鉴别服务设施	(122)
3.4.7	针对鉴别的攻击及对抗措施	(125)
3.5	抗抵赖服务	(129)
3.5.1	基本概念	(129)

3.5.2	原发抗抵赖及递交抗抵赖服务	(129)
3.5.3	可信第三方的角色	(130)
3.5.4	抗抵赖服务的五个阶段	(132)
3.5.5	抗抵赖策略	(134)
3.5.6	抗抵赖服务信息和设施	(135)
3.6	完整性保护	(137)
3.6.1	基本概念	(137)
3.6.2	对完整性的威胁和攻击	(139)
3.6.3	完整性策略与策略表达	(139)
3.6.4	完整性服务信息和设施	(140)
3.7	安全审计和报警	(141)
3.7.1	基本概念	(142)
3.7.2	安全审计和报警的策略及其他	(149)
3.7.3	安全审计和报警服务信息及设施	(150)
	本章小结	(153)
	思考题	(154)
第 4 章	信息安全技术原理	(157)
4.1	密码技术	(158)
4.1.1	概述	(158)
4.1.2	密码技术原理	(159)
4.1.3	密码算法	(160)
4.1.4	密钥及密钥管理框架	(166)
4.1.5	密钥管理实现方案	(168)
4.2	访问控制技术	(174)
4.2.1	概述	(174)
4.2.2	访问控制技术原理	(175)
4.2.3	与其他安全服务和安全技术的交互	(183)
4.2.4	网络访问控制组件的分布	(185)
4.2.5	访问控制信息的管理	(188)
4.2.6	通信访问控制和路由控制	(189)
4.3	机密性保护技术	(190)
4.3.1	概述	(190)
4.3.2	机密性保护技术	(191)
4.3.3	密钥管理	(194)

4.4	完整性保护技术	(196)
4.4.1	概述	(196)
4.4.2	完整性机制的分类描述	(196)
4.4.3	与其他安全服务和安全技术的交互	(201)
4.4.4	通信协议需求	(201)
4.4.5	完整性在体系结构中的位置	(203)
4.5	鉴别技术	(204)
4.5.1	概述	(204)
4.5.2	鉴别技术原理	(206)
4.5.3	与其他安全服务和安全技术的交互	(215)
4.5.4	非密码鉴别机制	(216)
4.5.5	基于密码的鉴别机制	(222)
4.5.6	数据原发鉴别	(225)
4.5.7	设计鉴别协议时应注意的问题	(226)
4.5.8	通信协议需求和鉴别在体系结构中的位置	(229)
4.6	数字签名技术	(231)
4.6.1	概述	(231)
4.6.2	带附录的签名技术	(231)
4.6.3	带消息恢复的数字签名技术	(256)
4.7	抗抵赖技术	(259)
4.7.1	概述	(259)
4.7.2	抗抵赖技术原理	(260)
4.7.3	抗抵赖技术面临的威胁	(266)
4.7.4	与其他安全组件和安全技术的交互	(269)
4.7.5	通信协议需求	(269)
4.8	安全审计和报警机制	(270)
4.8.1	一般概念	(270)
4.8.2	安全报警报告功能	(271)
4.8.3	安全审计跟踪功能	(272)
4.8.4	与其他安全组件和安全技术的交互	(273)
4.9	公证技术	(274)
4.10	普遍安全技术	(274)
	本章小结	(276)
	思考题	(278)

第 5 章 信息安全实用技术	(281)
5.1 概述	(282)
5.2 防火墙技术	(285)
5.2.1 基本概念	(285)
5.2.2 防火墙的基本类型	(287)
5.2.3 防火墙的体系结构及其配置形式	(292)
5.2.4 防火墙的局限性	(296)
5.2.5 防火墙的应用示例	(298)
5.3 入侵检测及预警技术	(306)
5.3.1 基本概念	(306)
5.3.2 针对 TCP/IP 协议安全缺陷的网络攻击	(307)
5.3.3 网络入侵攻击的典型过程	(314)
5.3.4 入侵检测系统的基本原理	(318)
5.3.5 入侵检测的基本方法	(325)
5.3.6 入侵检测系统的结构	(326)
5.3.7 入侵检测实现时若干问题的考虑	(331)
5.4 漏洞检测技术	(333)
5.4.1 入侵攻击可利用的系统漏洞的类型	(334)
5.4.2 漏洞检测技术分类	(335)
5.4.3 漏洞检测的特点	(336)
5.4.4 漏洞检测系统的设计实例	(337)
5.5 网络隔离技术	(340)
5.5.1 概述	(340)
5.5.2 网络隔离的基本技术	(343)
5.5.3 实现网络隔离的典型方案	(348)
5.6 计算机病毒防范	(350)
5.6.1 恶意程序	(351)
5.6.2 病毒的特点	(356)
5.6.3 病毒的类型	(363)
5.6.4 病毒的传染方式	(366)
5.6.5 反病毒技术概述	(371)
5.6.6 计算机病毒技术的新动向	(381)
本章小结	(386)
思考题	(388)

第 6 章 公开密钥基础设施	(389)
6.1 概述	(390)
6.1.1 PKI 的定义	(391)
6.1.2 X.509 证书和证书撤销列表	(394)
6.2 PKI 提供的服务	(396)
6.3 PKI 的构成	(398)
6.4 PKI 标准	(401)
6.4.1 与 PKI 定义相关的标准	(401)
6.4.2 与 PKI 应用相关的标准	(402)
6.5 PKI 的信任模型	(402)
6.5.1 CA 的严格层次结构	(403)
6.5.2 CA 的分布式信任结构	(404)
6.5.3 CA 的 Web 模型	(406)
6.5.4 CA 的以用户为中心的信任模式	(407)
6.5.5 交叉认证	(408)
6.6 PKI 的运行模型	(410)
6.7 国外 PKI 体系发展状况	(411)
6.7.1 美国联邦 PKI 体系结构	(412)
6.7.2 加拿大政府 PKI 体系结构	(415)
6.7.3 两种体系的比较	(416)
本章小结	(417)
思考题	(418)
英文缩略词英汉对照表	(421)
参考文献	(425)



第

绪 论

章

- 本章基于信息系统的基本概念，描述了信息系统安全的内涵和方法论，指出了信息系统存在的风险和系统的安全需求、信息系统常见的威胁和防御策略，阐述了信息系统的安全要素。