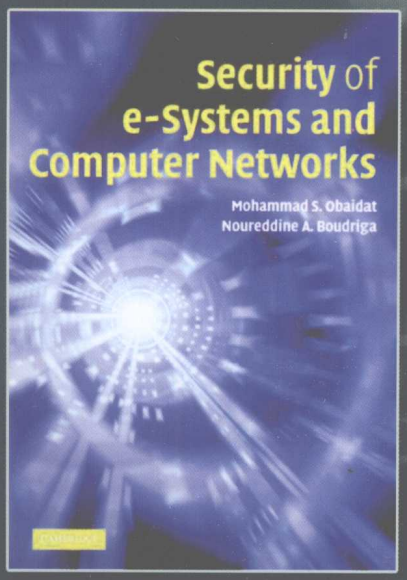
国外计算机科学教材系列

CAMBRIDGE

计算机网络安全导论

Security of e-Systems and Computer Networks



[美] Mohammad S. Obaidat
[突尼斯] Noureddine A. Boudriga 著
毕红军 张 凯 译

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

国外计算机科学教材系列

计算机网络安全导论

Security of e-Systems and Computer Networks

［美］ Mohammad S. Obaidat

［突尼斯］ Noureddine A. Boudriga

著

毕红军 张 凯 译

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

本书系统地介绍了计算机网络安全各个核心领域，自底向上，逐层剖析，从安全服务基础、公钥密码体制和数字签名技术入手，描述了 PKI、生物测量和电子信任等各种安全工具与技术框架，讨论了电子服务、电子政务、电子商务和 WLAN 安全等应用，并且重点研究了包括 IDS、VPN、恶软防护和风险管理在内的企业级防护手段与技术。本书有三个突出特点：一是内容全面，全面梳理了整个网络安全领域的研究现状，内容广博、视野开阔，提供了该领域的全景视图；二是观点新颖，体现了近年来网络安全领域的最新成果；三是贴近实际，以企业级安全防护为着眼点，统合学界成果和业界实践。

本书对计算机、电信、信息学、系统与软件工程等专业的科研人员和网络安全从业人员来说，是一本不可多得的参考书，并且也十分适用于用做研究生或高年级本科生的网络安全、信息系统安全、通信系统安全、电子系统安全等课程的教科书。

版权贸易合同登记号　图字：01-2009-0632

图书在版编目(CIP)数据

计算机网络安全导论/(美)奥巴代特(Obaidat,M.S.)，(突尼斯)布德里卡(Boudriga,N.A.)著；毕红军，张凯译. —北京：电子工业出版社，2009.5
(国外计算机科学教材系列)
书名原文: Security of e-Systems and Computer Networks
ISBN 978-7-121-08703-5

Ⅰ. 计… Ⅱ. ①奥…②布…③毕…④张… Ⅲ. 计算机网络－安全技术－教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2009)第 062691 号

策划编辑：冯小贝
责任编辑：余　义
印　　刷：北京京师印务有限公司
装　　订：
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：787×1092　1/16　印张：17.5　字数：448 千字
印　　次：2009 年 5 月第 1 次印刷
定　　价：33.00 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。

出 版 说 明

21世纪初的5至10年是我国国民经济和社会发展的重要时期，也是信息产业快速发展的关键时期。在我国加入WTO后的今天，培养一支适应国际化竞争的一流IT人才队伍是我国高等教育的重要任务之一。信息科学和技术方面人才的优劣与多寡，是我国面对国际竞争时成败的关键因素。

当前，正值我国高等教育特别是信息科学领域的教育调整、变革的重大时期，为使我国教育体制与国际化接轨，有条件的高等院校正在为某些信息学科和技术课程使用国外优秀教材和优秀原版教材，以使我国在计算机教学上尽快赶上国际先进水平。

电子工业出版社秉承多年来引进国外优秀图书的经验，翻译出版了“国外计算机科学教材系列”丛书，这套教材覆盖学科范围广、领域宽、层次多，既有本科专业课程教材，也有研究生课程教材，以适应不同院系、不同专业、不同层次的师生对教材的需求，广大师生可自由选择和自由组合使用。这些教材涉及的学科方向包括网络与通信、操作系统、计算机组织与结构、算法与数据结构、数据库与信息处理、编程语言、图形图像与多媒体、软件工程等。同时，我们也适当引进了一些优秀英文原版教材，本着翻译版本和英文原版并重的原则，对重点图书既提供英文原版又提供相应的翻译版本。

在图书选题上，我们大都选择国外著名出版公司出版的高校教材，如Pearson Education培生教育出版集团、麦格劳－希尔教育出版集团、麻省理工学院出版社、剑桥大学出版社等。撰写教材的许多作者都是蜚声世界的教授、学者，如道格拉斯·科默（Douglas E. Comer）、威廉·斯托林斯（William Stallings）、哈维·戴特尔（Harvey M. Deitel）、尤利斯·布莱克（Uyless Black）等。

为确保教材的选题质量和翻译质量，我们约请了清华大学、北京大学、北京航空航天大学、复旦大学、上海交通大学、南京大学、浙江大学、哈尔滨工业大学、华中科技大学、西安交通大学、国防科学技术大学、解放军理工大学等著名高校的教授和骨干教师参与了本系列教材的选题、翻译和审校工作。他们中既有讲授同类教材的骨干教师、博士，也有积累了几十年教学经验的老教授和博士生导师。

在该系列教材的选题、翻译和编辑加工过程中，为提高教材质量，我们做了大量细致的工作，包括对所选教材进行全面论证；选择编辑时力求达到专业对口；对排版、印制质量进行严格把关。对于英文教材中出现的错误，我们通过与作者联络和网上下载勘误表等方式，逐一进行了修订。

此外，我们还将与国外著名出版公司合作，提供一些教材的教学支持资料，希望能为授课老师提供帮助。今后，我们将继续加强与各高校教师的密切联系，为广大师生引进更多的国外优秀教材和参考书，为我国计算机科学教学体系与国际教学体系的接轨做出努力。

电子工业出版社

教材出版委员会

译 者 序

计算机网络安全无疑算得上是当今计算机学界的“显学”，一时研究者云集，成果迭出，各高校也都纷纷开出网络安全的课程或专业。然而，由于计算机网络安全涉及领域太广，初学者往往不知从何下手，即便是本领域的从业者，也时有“只缘身在此山中”的茫然。究其原因，主要是目前的网络安全教材和图书中，专注于某一问题、某一技术、某一产品的比较多，而具备全局视点，能够综合梳理整个领域，进而拼接出网络安全的全景视图的则少得多。

本书正是这样一种努力的成果，试图从原理到技术、从框架到应用、从软硬件系统到管理规程制度，自底向上，逐层剖析，以求尽可能全面地介绍电子系统与计算机网络安全的各个核心领域。可以说，本书最显著的特点之一，就是内容全面，这体现在如下几个方面：一是介绍的面比较广，举凡公钥密码体制、数字签名技术、PKI、生物测量技术、电子信任管理、电子服务、电子商务、电子政务、WLAN、IDS、VPN、恶意软件防护、风险管理等无所不包，而且详略得当，重点突出；二是对于重要的问题，不仅仅满足于泛泛介绍，而且阐明其理论基础，并往往给出示例，便于理解；三是对于各类安全技术，不仅介绍其原理和功能，而且也专门讨论其面临的挑战与问题，例如，关于 RSA 算法，除了介绍其概念、原理和示例，还专门用一节的篇幅介绍针对 RSA 的攻击技术的发展。

本书的第二个显著特点，就是观点新颖。这体现在：一方面，本书介绍了许多新技术和近年来的热点问题，例如生物测量技术、SOA、移动商务、移动政务、WLAN 安全等；另一方面，书中引入的大量参考资料，大多数是近年来比较有权威性的著作，其所引用的统计图表和产品列表，都是比较晚近的数据，例如，第 1 章引用的调查报告，是最近两三年的数据，而第 13 章讨论的各种防护软件，大部分现在还在销售；此外，书中还提出了作者自己的新的研究成果，例如生物测量中的击键节奏测量技术、风险分析中的 NetRAM 框架等。

本书的第三个显著特点，就是贴近实际。本书不仅介绍了近年来学界的研究成果，而且总结了业界的实践经验，甚至还分析了当前市场上的相关产品。众所周知，网络安全绝不仅仅是个技术问题，而是“三分技术、七分管理”，为此，本书用了不少篇幅从企业安全经理(或 CSO)的角度出发，分析了网络安全所涉及的项目规划、风险分析、文档准备、制度制定等管理要素，寓理论于实践，对网络安全从业人员有着较强的指导作用。

对于有志于从事网络安全研究的年轻学子来说，本书是一本入门必读书，用以构筑个人整个网络安全研究生涯的“绪论”部分，而只有对整个领域的研究现状有了大体了解，才能够更好地做好本方向、本专业的细致研究。对于在政府或企业 IT 部门从事网络管理工作的从业者来说，本书是一本启迪思路的参考书。和许多行业一样，目前国内的网络安全工作中，存在着某种急功近利的倾向，恨不得只依靠买一批设备、上一批系统，就能够把安全问题一劳永逸地解决掉。如何科学规划，如何扎扎实实地提高网络安全防护水平，把网络安全工作带入有序推进、良性发展的轨道，本书尝试着给出了答案。

在全书的翻译过程中，我们感觉到原书作者思维严谨、行文流畅、术语精当、用词多样。为保持原书风貌，翻译时我们力求做到“信、达”，对于容易产生歧义的术语，都注明原文，对于难以理解的部分，都尽量添加注解，对于原书中公式推导、示例计算，都一一进行了推演和订正。翻译工作中，前7章主要由毕红军负责，后7章主要由张凯负责，张凯还承担了全书的审校工作。

计算机网络安全领域的发展一日千里，新技术、新概念、新词语层出不穷，而译者学业不精、水平有限，再加上工作繁忙、时间仓促，很多地方难免存在误译和疏漏，还望读者不吝斧正。如有赐教，请电邮联系，地址：ihavenodream@sina.com。

本书中文版的翻译出版，首先归功于原书作者Obaidat教授和Boudriga教授，没有他们艰苦细致的开创性工作，一切都无从谈起。其次，要感谢电子工业出版社的冯小贝编辑和余义编辑，以及其他相关工作人员，正因为他们的不懈努力，本书才能够有机会和中国读者见面。最后，感谢我们的家人，他们默默的支持，是我们工作的前提和动力。

译　者

2009年4月于重庆林园

前　言

近年来，随着各个单位越来越依赖于电子系统和计算机网络，这些系统的安全日益成为一个重要的问题。对电子商务系统、电子政务系统或网站的访问可能带来多种风险，从侵犯隐私、损失金钱到泄露国家安全情报，乃至引起大灾难，不一而足。电子安全方案旨在提供5种重要服务，即用户鉴别、系统完整性、通信保密性、业务服务可用性和交易(Transaction)抗抵赖性。本书中提供的大多数电子安全方案都使用了两种主要的密码技术，即公钥加密体系和数字签名。当然，有效的解决方案还必须符合国家相关法律的规范。

投入在计算机网络和电子系统上的资金数以十亿计，因此，确保这些系统的安全不仅对系统的正常运行极其重要，而且对公司、单位的未来，乃至国家安全都事关重大。由于确保各种电子系统平台的安全存在种种困难，而人们对安全性更好、性价比更高的系统的需求日渐增长，电子系统和网络安全领域就成为了进行研究、开发和投资的沃土。电子系统安全涵盖了许多方面，包括技术、应用、趋势和挑战等。

本书是第一本完全专注于讨论电子系统和网络安全的书籍，包含4个部分，共14章。

第1章阐述了系统安全的重要性，并提出了网络安全和用户防护方面的相关概念。本章还介绍了全书中用于定义服务、信息、计算机安全和网络安全的一些基本术语。此外，本章还涉及了安全开销、服务、威胁和漏洞等相关主题。

第2章讨论了加密及其实际应用，主要关注公钥密码体制中使用的几种技术。本章也详细介绍了密码的不同种类，及其在提供基础电子服务方案中的应用。本章向读者提供了一些简单的例子，以解释那些主要概念和手段是如何行之有效的。本章还讨论了对称加密手段、公钥密码体制、RSA 和 ElGamel 算法、公钥管理、生存周期、密钥分发和对公钥密码体制的攻击等相关主题。

第3章主要讨论用户与消息鉴别，具体介绍了数字签名方案及其应用，阐释了哈希函数和密钥生成的概念。这些概念构成了所有采用公钥体系的防护手段的技术支撑，因此显得十分重要。本章还讨论了强鉴别方案和弱鉴别方案、针对数字签名鉴别的攻击、哈希函数和鉴别应用等主题。

第4章详细介绍了公钥基础设施(PKI)系统，涉及PKI体系结构模型、管理功能、公钥证书、信任层次模型、验证路径处理和 PKI 部署等方面。本章特别强调了关于证书生成、证书验证和证书撤销的定义。此外，本章还讨论了交叉验证、PKI操作、PKI评估和PKI防护等相关问题。

第5章介绍了用于系统安全的生物测量(Biometric)方案，对各种生物测量技术做了详细介绍和评论，对各种生物测量方案的准确度做了分析和比较。我们还指明了生物测量系统面临的问题和挑战。

第6章讨论了通信网络中的信任管理，涉及到“信任”相对于“安全”的概念定义，以及包括活动凭证和SPKI在内的数字凭证(Digital Credential)。本章还介绍了授权与访问控制系统、信任策略，以及诸如门诊信息系统、电子支付系统、分布式防火墙之类的信任管理应用。

第 7 章验证了电子服务范式，讨论了其所描述的技术特征，研究了其所带来的安全挑战。本章还介绍了良构的电子服务，展示了其组成和分发方式。此外，本章还讨论了 UDDI/SOAP/WSDL 与 ebXML 计划、消息保护机制、注册表安全等主题。

第 8 章介绍了通过可信途径提供电子政务服务的主要方法，奠定了确保电子政务服务的安全基础，使得电子政务能够真正改变个人、企业与政府打交道的方式。本章涉及的主题包括：电子政务的概念与实践、电子政务中的鉴别与隐私问题、电子投票安全、电子政务安全工程、电子政务安全监控，以及响应支持系统等。

第 9 章讨论了电子商务的需求，介绍了用以保护电子商务的主要技术，特别强调了 SSL、TLS 和 SET 协议。同时，本章还涉及了电子支付、移动商务(M-Commerce)、SET 与交易安全等主题。

第 10 章评论和检验了无线局域网(WLAN)的安全性，介绍了各种主流技术的优缺点，讨论了 WLAN 安全中的主要问题。此外，本章还涉及了 WLAN 攻击、安全服务、有线等效保密协议(WEP)及其优缺点、Wi-Fi 安全访问协议(WPA)及其优点、移动 IP，以及虚拟专用网(VPN)等主题。

第 11 章从全局角度对入侵进行了分类，介绍了检测恶意流量和异常行为的主要方法，包括模式匹配、特征(Signature)分析、流量异常分析、启发式分析、协议异常分析等。本章提出了一个模型，以描述事件、告警和关联，它定义了当前企业中最常用的入侵检测方法的基本原理。本章还对该模型中的主要概念进行了调查。此外，本章还讨论了关联函数的定义与作用、检测技术和关于入侵检测系统的其他问题。

第 12 章介绍了虚拟专用网(VPN)的基本知识和技术。还对 VPN 服务做了评论，这些服务包括内部网(Intranet)VPN、外部网(Extranet)VPN 和远程访问 VPN。本章具体讨论了在使用了 VPN 技术的共享网络上传输数据时应考虑的安全问题，以及 PPTP、L2TP 等 VPN 使用的协议。此外，本章还评论了 VPN 中提供的服务质量(QoS)。

第 13 章讨论了恶意软件(Malware)的定义与分类，介绍了病毒、蠕虫和木马等主流的恶意软件的制作和传播方法。本章还介绍了企业应当采取的防护措施，并给出了一些用以加强防护的指导方针。此外，本章还涉及了基于防火墙的防护、入侵防御系统、防护方针和多态性(Polymorphism)挑战等主题。

第 14 章调查了风险管理框架所应当具有的特征，讨论了现有的常见风险管理方法，提出了基于漏洞分析、威胁分析、风险分析和实施控制等一系列重要概念的结构化方法。本章还强调了这些方法的用法与限制，以及风险分析和风险评估技术的作用。此外，本章还涉及了风险库的管理、风险评估、系统状态监控方案(如基于模式的监控和基于行为的监控)等主题。

本书对网络与信息安全领域的研究者和从业者来说是一本不可多得的参考书。本书还可以用做研究生或高年级本科生的信息安全、电子安全、网络安全、信息系统安全、电子商务安全和电子政务安全等课程的教科书。

感谢原书写作计划的评阅人，他们提出了非常具有建设性的建议。也感谢我们的学生，在课堂上试用此书稿时，他们提出了一些反馈意见。十分感谢剑桥出版社的编辑与助理编辑们的通力合作和出色工作。

目　录

第1部分　电 子 安 全

第 3 部分 电子安全应用

第 4 部分 企 业 防 护