<<信息安全概论>>

图书基本信息

书名：<<信息安全概论>>

13位ISBN编号：9787810829984

10位ISBN编号：781082998X

出版时间：2007-6

出版时间：北京交大

作者：石志国

页数：271

<<信息安全概论>>

前言

信息安全学是一门新兴的学科，2004年成为一门正式的本科专业，目前已经成为很多科研机构和大专院校的一个重要研究领域。
信息安全概论需要全面阐述该学科目前的发展层次，研究内容和最新的发展方向。
本书对信息安全学科内容进行整体介绍，根据信息安全学目前最新发展重新规划学科的内容及各部分比重。
信息安全学是一门实践性很强的学科，本书除了对相关理论进行全面讲解外，还通过具体的实验、例子等更加具体形象地化解理论的枯燥和繁杂。
本书的整体定位是教材，书后提供大量习题，因此也可以同时作为相关考试的参考书。
为了方便使用，提高质量，本书提供完整的教学大纲及教案等辅助资料。
目前很多信息安全教程理论性很强，这样接受起来相对比较困难。
本书把理论知识和实验实践结合讲解，注重提高学习信息安全的趣味性与知识性，以及授课的生动性。
全书从信息安全研究层次角度分成4部分，共11章。
第一部分：信息安全基础第1章信息安全概述：介绍信息安全的学科内容、研究层次及安全威胁。研究信息安全的社会意义，相关道德标准及黑客行为学研究内容。
第二部分：密码学基础 第2章信息加密与密码分析：介绍密码学的基本概念、加密类型，混合加密方法以及消息一致性。
并介绍加密领域中两种主流加密技术：DES加密和RSA加密。
第3章认证与密钥管理技术：介绍哈希函数的分类与MD5的基本算法、常用的身份识别技术、电子ID身份识别和个人特征身份识别，以及密钥管理技术与管理系统。
第三部分：网络安全技术第4章PKI公钥基础设施原理：介绍PKI／CA模型的构成、RSA算法在PKI／CA中的应用、PKI策略、PKI的规划和建设，以及CA的应用。
第5章防火墙与入侵检测技术：介绍防火墙的基本概念、分类、实现模型，以及如何利用软件实现防火墙的规则集；介绍入侵检测系统的概念、原理，以及如何利用程序实现简单的入侵系统。
第6章IP安全与Web安全：介绍IPSec：的必要性，IPSec中的AH协议和ESP协议、密钥交换协议IKE以及VPN的解决方案等。
第7章典型攻击技术简介：介绍常用的网络入侵技术，包括社会工程学攻击、物理攻击、暴力攻击、漏洞攻击及缓冲区溢出攻击等。

<<信息安全概论>>

内容概要

本书系统介绍了信息安全学科的内容。
本书与同类书籍相比，大大提高了实践部分的比例，全书理论与实践的比例约为6：4，并引用大量的经典例子，注重提高学习信息安全的趣味性与知识性及授课的生动性。
全书从信息安全研究层次角度分成4部分，共11章。
第一部分：信息安全基础，介绍信息安全学的基本概念及安全的评价标准。
第二部分：密码学基础，介绍信息加密与密码分析、认证及密钥管理技术。
第三部分：网络安全技术，介绍PKI公钥基础设施原理、防火墙与入侵检测技术、IP安全与web 安全，以及简单介绍了典型攻击技术。
第四部分：系统与应用安全技术，介绍安全操作系统理论、恶意代码与病毒机制、可信计算的基本概念及信息安全法律与法规。
本书可作为高等学校和各类培训机构相关课程的教材或参考书。

<<信息安全概论>>

书籍目录

章节摘录

插图：但美国联邦PKI体系和加拿大政府PKI体系并不完全一致，他们都有各自的特点。
在体系结构上，美国联邦PKI体系结构比较复杂，它包含各种信任域结构，即树状结构，网状结构和信任列表等，因此，联邦桥认证机构仅是一个桥梁；而加拿大政府PKI体系结构比较简单，它是一个树状结构，从结构上看，中央认证机构仿佛是一个根认证机构。
在信任关系的建立上，美国联邦：PKI体系结构中的联邦桥认证机构是各信任域建立信任关系的桥梁，但它并不强调在建立信任关系时必须遵循交叉认证证书中所确定的担保等级之间的一一映射关系；在加拿大政府PKI体系中，各信任域之间建立信任关系必须经过中央认证机构。
在采用的技术上，美国联邦PKI体系中的成员采用多种不同的PKI产品和技术，如VeriSign，Baltimore和Entrust等公司的技术；而加拿大政府PKI体系中强调使用Entrust公司的技术。
在组成成员上，美国联邦PKI体系中除了各级政府和不同的政府机构外，还可包括与政府或政府机构有商业往来的合作伙伴；而加拿大政府PKI体系中的成员都是联邦的各级政府或政府机构。
4.3.4 我国的PKl发展规划由于PKI作为国家信息安全基础设施的重要战略地位及核心技术（密码技术）的特殊敏感性，中国PKI体系的建立与发展既不能简单地照搬国外的技术与架构，也不能盲目地完全走自由市场的道路。
国家PKI体系应在国家控制和主导下，制定统一的发展战略和管理模式，在走向市场化道路的同时，应由国家负责统一协调、管理和监控，以打破一些行业内部的变相垄断，加强各行业之间的合作，避免重复建设，促进平等竞争，建设一个有利于发展我国网络经济的体系。
我国的PKI体系结构如图4-10所示。

<<信息安全概论>>

编辑推荐

《信息安全概论》为清华大学出版社，北京交通大学出版社出版发行。
原理与技术的完美结合，教学与科研的最新成果，语言精炼，实例丰富，可操作性强，实用性突出。

版权说明