<<密码学与网络安全>>

图书基本信息

书名：<<密码学与网络安全>>

13位ISBN编号：9787302193395

10位ISBN编号：7302193398

出版时间：2009-3

出版时间：清华大学出版社

作者：卡哈特

页数：427

字数：689000

译者：金名

前言

随着计算机技术，尤其是网络技术的飞速发展，各行各业都离不开计算机，离不开网络。
网络技术的出现和发展，在极大地方便了我们的工作和学习的同时，也带来了很多安全方面的难题。
因安全漏洞和黑客入侵而造成巨大损失的案例日益增多。
网络安全问题日益重要和迫切。
要实现网络安全，就离不开加密技术。
本书以清晰的脉络、简洁的语言，介绍了各种加密技术、网络安全协议与实现技术等内容，并给出了具体的案例实现分析，是一本关于密码学与网络安全的理论结合实践的优秀教材。
本书自第1版出版以来，期间出现了多种新技术，已有的技术与协议又开发出了新版本，我们应当在本书中能看到这些新技术。
本书对第1版所做的主要修改如下：·更详细地阐述了现代算法，如AES、SHA－256及其变体TLS等。
·给出了更多的数学基础（只要有需要）。
·扩展了已有的内容（只要有需要）。
·介绍了一些在上一版中没有包含但在课程上将会讲授的内容。
本书在上一版的基础上，对一些翻译欠妥的地方进行了修改，在此表示感谢。
本书由金名、张长富等主译，李晓春、王春桥、龚亚萍、韦笑、何雄、周云、袁科萍、王雷、贺军、贺民、陈安南、霍丽娜、史广飞、侯鹏、张红军、董武、陈河南、王峰、沈宏、郑晓蕊、李伟、白晓平、李月、汤效平、李东锋、邵世磊、张新苗、刘大为、薛飞、邹晓东、陈占军、夏绪虎、刘占坤、冯苗、裘蕾、任世华、金颖、吴霞、韩毅、马以辉、樊庆红等人也参与了部分翻译工作。
欢迎广大读者指正。

<<密码学与网络安全>>

内容概要

本书以清晰的脉络、简洁的语言，介绍了各种加密技术、网络安全协议与实现技术等内容，包括各种对称密钥算法与AES，非对称密钥算法、数字签名与RSA，数字证书与公钥基础设施，Internet安全协议，用户认证与Kerberos，Java、．NET和操作系统的加密实现，网络安全、防火墙与VPN，并给出了具体的加密与安全的案例实现分析，是一本关于密码学与网络安全的理论结合实践的优秀教材。

本书特点　　本书语言表达流畅、简洁，使本书的阅读不再枯燥。

全书多达425幅插图，极大地方便了读者的学习和理解。

全书提供了丰富的多项选择题、练习题、设计与编程题，有利于加深读者对所学知识的理解和掌握。

作者简介

Atul Kahate在印度和世界IT业中已经有12年的工作经验，他取得了统计学学士学位和计算机系统专业的MBA学位。
他与他人为Tata McGraw-Hill出版公司合著了多部著作，不少书被用作教材或全世界的大学/学院/IT公司用作参考书。
Atul Kahate还在印度和国外获得过多个奖项，过去曾就职于Syntel、L&T Infotech American Express和德国银行，现就职于i-flex solution有限公司。

<<密码学与网络安全>>

书籍目录

第1章　计算机攻击与计算机安全　1.1　简介　　1.2　安全需求　　1.3　安全方法　　1.4　安全性原则　　1.5　攻击类型　　1.6　本章小结　　1.7　实践练习　第2章　加密的概念与技术　　2.1　简介　　2.2　明文与密文　　2.3　替换方法　　2.4　变换加密技术　　2.5　加密与解密　　2.6　对称与非对称密钥加密　　2.7　夹带加密法　　2.8　密钥范围与密钥长度　　2.9　攻击类型　　2.10　本章小结　2.11　实践练习　第3章　对称密钥算法与AES　3.1　简介　　3.2　算法类型与模式　3.3　对称密钥加密法概述　3.4　数据加密标准　……第4章　非对称密钥算法、数字签名与RSA第5章　数字证书与公钥基础设施第6章　Internet安全协议第7章　用户认证与Kerberos第8章　Java、NET和操作系统的加密实现第9章　网络安全、防火墙与VPN第10章　加密与安全案例分析附录A　数学背景知识附录B　数字系统附录C　信息理论　附录D　实际工具附录E　Web资源附录F　ASN、BER、DER简介　参考文献术语表

章节摘录

插图：1.5.7 特定攻击窃听与伪装Internet上的计算机用所谓分组的小块数据（分组）交换消息。
分组就像把实际数据放在信封中，加上地址信息。
攻击者的目标是这些分组，因为它们要在Internet上从源计算机发往目标计算机。
这些攻击有两大类：分组窃听（Packet sni：fling或snooping）和分组伪装（Packet spoofing）。
由于这个通信使用的协议是Internet协议（IP），因此这些攻击又称为IP窃听（IP snifling）和IP伪装（IP spoofing），其意思是相同的。
下面介绍这两种攻击。
（a）分组窃听：分组窃听是对正在进行的会话的被动攻击。
攻击者不干扰会话，只是监视传递的分组（即窃听）。
显然，为了防止分组窃听，就要以某种方式保护传递的信息。
这可以在两个层次进行：以某种方式编码传递的信息；编码传输链路。
要读取分组，攻击者就要访问这些分组，最简单的方法是控制通信量经过的计算机，通常是路由器。
但是，路由器是高度保护的资源，因此攻击者很难攻击，它们会转而攻击同一路径中保护较差的计算机。
（b）分组伪装：分组伪装就是用不正确的源地址发送分组。
这时，接收方（接收包含伪源地址的分组）会向这个伪装地址（spoofed address）发送答复，而不是答复攻击者，可能造成三种情况：（i）攻击者截获答复——如果攻击者在目的地和伪装地址之间，则可以看到答复，用这个信息进行劫持（hijacking）攻击。
（ii）攻击者不用看到答复——如果攻击者的意图是拒绝服务攻击，则攻击者不用看到答复。
（iii）攻击者不想看到答复——攻击者可能只是对主机有仇恨，把它的地址作为伪装地址，向目的地发送分组。
攻击者不想看到分组，只是让伪装地址收到分组和感到迷惑。

<<密码学与网络安全>>

编辑推荐

《密码学与网络安全(第2版)》语言表达流畅、简洁，使《密码学与网络安全(第2版)》的阅读不再枯燥。
《密码学与网络安全(第2版)》多达425幅插图，极大地方便了读者的学习和理解。
《密码学与网络安全(第2版)》提供了丰富的多项选择题、练习题、设计与编程题，有利于加深读者对所学知识的理解和掌握。

版权说明