

<<信息安全原理与实践>>

图书基本信息

书名：<<信息安全原理与实践>>

13位ISBN编号：9787121042386

10位ISBN编号：712104238X

出版时间：2007-5

出版时间：电子工业

作者：Mark Stamp

页数：306

译者：杜瑞颖

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<信息安全原理与实践>>

内容概要

本书通过真实世界的实例来讲解信息安全的有关知识。作者在书中并没有给出大量的理论叙述，而是重点关注技术的发展，以及老师和学生们需要面对的安全与信息技术的挑战。

书中的内容主要包括以下四个方面： 密码：古典密码学，对称密钥密码系统，公钥密码系统，hash函数，随机数，信息隐藏，以及密码分析学。

访问控制：认证和授权，多级安全与多边安全，访问控制模型，隐蔽通道和推理控制，防火墙，以及入侵检测系统。

协议：简单认证协议，SSL，IPsec，Kerberos，以及GSM。

软件：缺陷和恶意软件，缓冲区溢出，病毒和蠕虫，软件逆向工程，数字版权管理，安全软件开发，以及操作系统安全。

<<信息安全原理与实践>>

作者简介

Mark Stamp博士：San Jose州立大学的计算机科学教授，他担任了本科生和研究生的信息安全课程的教学工作。

Stamp博士曾经在政府和工业界的信息安全领域供职过多年，并且有着在美国国家安全局（NSA）7年的工作经验。

<<信息安全原理与实践>>

书籍目录

第1章 引言11 人物角色12 Alice的网上银行13 关于本书14 人的问题15 原理和实践16 习题第一部分 密码第2章 密码学基础21 简介22 密码的含义23 古典密码24 现代密码发展历史25 密码编码学的分类26 密码分析学的分类27 小结28 习题第3章 对称密钥密码31 简介32 流密码33 分组密码34 完整性35 小结36 习题第4章 公钥密码41 简介42 背包密码43 RSA44 Diffie-Hellman算法45 椭圆曲线密码46 公钥密码符号47 公钥密码的应用48 公钥基础设施49 小结410 习题第5章 函数及其他密码51 什么是hash函数52 生日问题53 非密码学hash函数54 Tiger hash55 HMAC56 hash函数的使用57 其他密码相关话题58 小结59 习题第6章 高级密码分析61 简介62 线性分析和差分分析63 RSA的旁门攻击64 格约简与背包密码65 Hellman的时间-存储权衡攻击66 小结67 习题第二部分 访问控制第7章 认证71 简介72 认证方法73 口令74 生物统计学75 你所拥有的76 双因素认证77 单点登录和Web cookie78 小结79 习题第8章 授权81 简介82 访问控制矩阵83 多级安全模型84 多边安全85 隐蔽通道86 推理控制87 CAPTCHA88 防火墙89 入侵检测810 小结811 习题第三部分 协议第9章 简单认证协议91 简介92 简单安全协议93 认证协议94 认证和TCP95 零知识证明96 最好的认证协议是什么97 小结98 习题第10章 现实安全协议101 简介102 SSL103 IPSec104 Kerberos105 GSM106 小结107 习题第四部分 软件第11章 软件漏洞与恶意代码111 简介112 软件缺陷113 恶意软件114 基于软件的混合型攻击115 小结116 习题第12章 软件中的不安全因素121 简介122 软件逆向工程123 软件防篡改技术124 数字版权管理125 软件开发126 小结127 习题第13章 操作系统及安全131 简介132 操作系统安全功能133 可信操作系统134 下一代可信计算基135 小结136 习题附录参考文献索引

<<信息安全原理与实践>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>