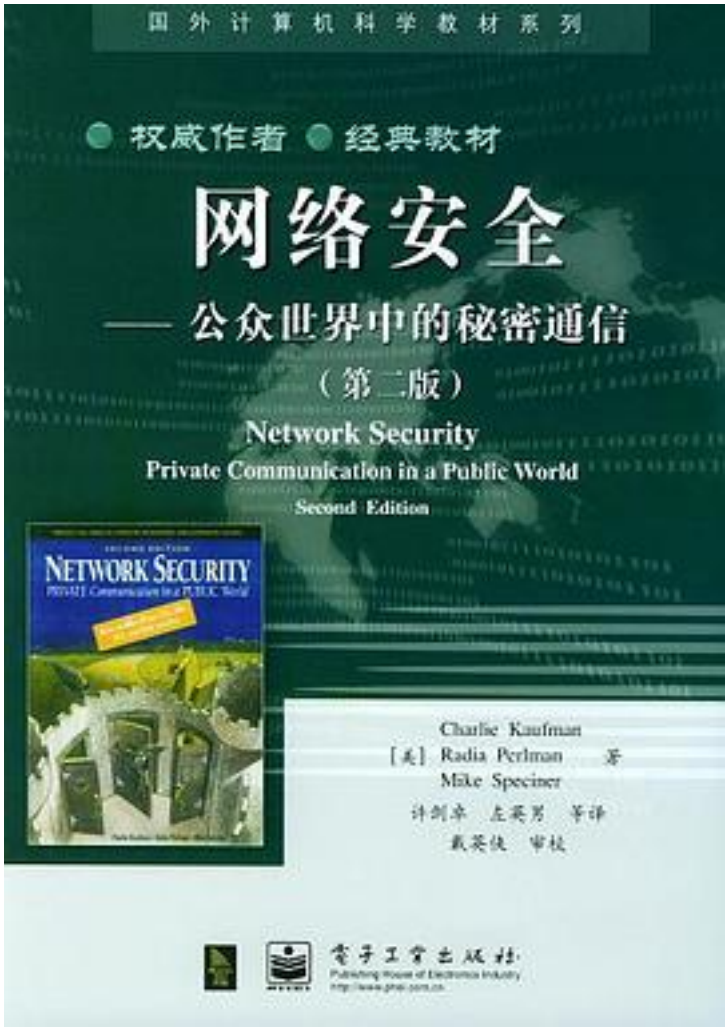
网络安全



网络安全_下载链接1_

著者:刘建伟

出版者:清华大学出版社

出版时间:2005-01-01

装帧:简装本

isbn:9787302105862

全书共分3篇15章。第1篇为网络安全基础,共3章,主要讨论了网络安全的基础知识,并从

网络协议安全性的角度出发,阐述了当今计算机网络中存在的安全威胁;第2篇为保密学基础,共5章,较祥细地讨论了网络安全中涉及的各种密码技术;第3篇为网络安全实践,共7章,主要介绍了网络安全实践中一些比较重要的产品及其技术应用。本书内容丰富,概念清楚,语言精练。在网络安全基本知识和保密学理论方面,力求深入浅出,通俗易懂;在网络安全产品方面,力求理论与实践相结合,具有很强的实用性。特别是每章的后面提供了很多习题,在书末也提供了大量的参考文献,便于有兴趣的读者继续深入地学习有关内容。

本书可作为高等院校信息安全、通信、计算机等专业的研究生和本科生教材,也可以作为网络安全工程师、网络管理员和计算机用户的参考用书,或作为网络安全培训教材。

作者介绍:

刘建伟,山东大学学士、硕士、西安电子科技大学博士,山东大学、中国海洋大学、北京航空航天大学兼职教授,中国电子学会高级会员。曾任海信集团技术中心副主任等职务,现任北京海信数码科技有限公司的总经理。长期从事通信、信息安全的教学和科研工作,获海信集团“科技标兵”称号。主持研制的海信防火墙获山东省科技进步二等奖,海信Netkey身份认证系统获山东省计算机应用新成果二等奖。在国内外学术刊物和会议上发表论文30篇,出版著作多部,合写著作曾获教育部全国普通高校优秀教材一等奖。

目录: 第1章 网络安全概论

15.3个人特征的身份证明技术
15.3.1手书签字验证
15.3.2指纹验证
15.3.3语音验证
15.3.4视网膜图样验证
15.3.5虹膜图样验证
15.3.6脸型验证
15.3.7身份证实系统的设计
15.4零知识证明的基本概念
15.4.1概述
15.4.2零知识证明的基本协议
15.4.3并行零知识证明
15.4.4使第三者相信的协议(零知识)
15.4.5非交互式零知识证明
15.4.6一般化理论结果
15.5零知识身份证明的密码体制
15.5.1FeigeFiatShamir体制
15.5.2GQ识别体制
15.5.3Schnorr识别体制
15.5.4FiatShamir，GQ和Schnorr体制的比较
15.5.5离散对数的零知识证明体制
15.5.6公钥密码体制破译的零知识证明
15.6身份认证协议实践
15.6.1安全壳远程登录协议
15.6.2Kerberos协议及其在Windows2000系统中的实现
15.6.3SSL和TLS
15.7智能卡技术及其应用
习题
参考文献
・・・・・・(收起)

网络安全_下载链接1_

标签

评论

网络安全_下载链接1_

书评

网络安全_下载链接1_