<<安全协议>>

图书基本信息

书名：<<安全协议>>

13位ISBN编号：9787302099666

10位ISBN编号：7302099669

出版时间：2005-12

出版时间：清华大学

作者：卿斯汉 编著

页数：362

字数：494000

<<安全协议>>

内容概要

本书是中国第一部关于安全协议的专门教材。
全书共分12章，全面介绍了安全协议的基本理论与关键技术。
主要内容包括引论；安全协议的密码学基础；认证协议；非否认协议；安全电子商务协议；其他类型的安全协议；BAN类逻辑；Kailar逻辑；Rubin逻辑；串空间模型；CSP方法；实用协议SSL及其安全性分析；安全协议攻击；安全协议设计；安全协议的公开问题；安全协议的发展与展望等。
本书精心选材、内容翔实、重点突出、特点鲜明，理论结合实际，既包括安全协议研究的最新进展，也包括作者在此研究领域的科研成果。
本书可以作为信息安全、计算机、通信等专业的本科高年级学生和研究生的教材，也可供从事相关专业的教学、科研和工程技术人员参考。

作者简介

卿斯汉，研究员，博士生导师，中科院软件所首席研究员，中科院信息安全技术工程研究中心主任。国内外著名信息安全专家，国家保密局技术顾问，中国信息安全标准化技术委员会委员，世界可信计算组织TCG专家，中国可信计算工作组组长，国家金财工程专家委员会委员，国家汽车计算

<<安全协议>>

书籍目录

第1章 引言 1.1 信息系统与信息系统安全 1.2 信息系统的攻击与防御 1.2.1 被动窃听与主动攻击 1.2.2 信息对抗的历史回顾 1.2.3 攻击目标与攻击分类 1.2.4 入侵检测技术 1.3 数学基础 1.3.1 数论基础 1.3.2 代数基础 1.3.3 计算复杂性理论基础 1.4 本书的取材、组织与安排第2章 安全协议的密码学基础 2.1 密码学的基本概念 2.2 古典密码学 2.2.1 换位密码 2.2.2 代替密码 2.2.3 转轮密码机 2.3 分组密码 2.3.1 分组乘积密码 2.3.2 数据加密标准 2.3.3 IDEA密码体制 2.3.4 先进加密标准和Rijndael密码算法 2.3.5 分组密码的工作模式 2.4 公开密钥密码 2.4.1 公开密钥密码的基本概念 2.4.2 MH背包体制 2.4.3 RSA体制 2.4.4 Rabin体制 2.5 数字签名 2.5.1 数字签名的基本概念 2.5.2 RSA数字签名 2.5.3 数字签名标准 2.6 散列函数 2.6.1 散列函数的基本概念 2.6.2 安全散列标准 2.7 总结 习题第3章 认证协议 3.1 经典认证协议 3.1.1 NSSK协议 3.1.2 NSPK协议 3.1.3 Otway?Rees协议 3.1.4 Yahalom协议 3.1.5 Andrew安全RPC协议 3.1.6 “大嘴青蛙”协议 3.2 关于认证协议攻击的讨论 3.2.1 Dolev?Yao模型 3.2.2 攻击者的知识和能力 3.2.3 重放攻击 3.3 针对经典认证协议的攻击 3.3.1 针对NSSK协议的攻击 3.3.2 针对NSPK协议的攻击 3.3.3 针对Otway?Rees协议的“类型缺陷”型攻击 3.3.4 针对Yahalom协议的攻击 3.3.5 针对Andrew安全RPC协议的攻击 3.3.6 针对“大嘴青蛙”协议的攻击 3.4 其他重要的认证协议 3.4.1 Kerberos协议 3.4.2 Helsinki协议 3.4.3 Woo?Lam单向认证协议 3.5 认证协议攻击的其他实例 3.5.1 攻击A(0)协议的3种新方法 3.5.2 攻击NSSK协议的一种新方法 3.5.3 攻击Otway?Rees协议的两种新方法 3.6 有关认证协议的进一步讨论 3.6.1 认证协议设计与分析的困难性 3.6.2 认证协议的分类 3.6.3 认证协议的设计原则 3.7 总结 习题第4章 BAN类逻辑 4.1 BAN逻辑 4.1.1 BAN逻辑构件的语法和语义 4.1.2 BAN逻辑的推理规则 4.1.3 BAN逻辑的推理步骤 4.2 应用BAN逻辑分析NSSK协议 4.2.1 应用BAN逻辑分析原始NSSK协议 4.2.2 应用BAN逻辑分析改进的NSSK协议 4.3 应用BAN逻辑分析Otway?Rees协议 4.4 应用BAN逻辑分析Yahalom协议 4.5 BAN类逻辑 4.5.1 Nessett对BAN逻辑的批评 4.5.2 BAN类逻辑 4.6 SVO逻辑 4.6.1 SVO逻辑的特点 4.6.2 SVO逻辑的语法 4.6.3 SVO逻辑的语义 4.6.4 应用SVO逻辑分析A(0)协议 4.6.5 应用SVO逻辑分析改进的A(0)协议 4.7 关于认证协议和BAN类逻辑的讨论 4.8 总结 习题第5章 非否认协议与安全电子商务协议第6章 安全电子商务协议的形式化分析第7章 其他类型的安全协议第8章 Rubin逻辑第9章 典型的实用协议——SSL协议第10章 SSL协议的安全性分析第11章 串空间模型第12章 安全协议的新进展参考文献

<<安全协议>>

版权说明