

## <<安全协议理论与方法>>

### 图书基本信息

书名：<<安全协议理论与方法>>

13位ISBN编号：9787030122773

10位ISBN编号：7030122771

出版时间：2003-1

出版时间：科学出版社

作者：范红,范红 编,冯登国

页数：421

字数：532000

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>

## <<安全协议理论与方法>>

### 内容概要

本书是《信息安全国家重点实验室信息安全丛书》之一。

书中系统地介绍了当前计算机网络安全协议的理论和方法，主要内容包括安全协议的基本概念、缺陷以及可能受到的攻击类型，基于推理结构性方法，基于攻击结构性方法，基于证明结构性方法，安全协议分析的形式化接口，安全协议设计的形式化方法，Kerberos协议，IPSec协议，SSL协议，X·509以及SET协议。

本书可作为高等院校计算机、通信、信息安全等专业的教学参考书，也可供从事相关专业的教学、科研和工程技术人员参考。

## &lt;&lt;安全协议理论与方法&gt;&gt;

## 书籍目录

第1章 引论 1.1 密码体制 1.2 数字签名 1.3 Hash函数 1.4 密钥管理与分配 1.5 PKI公钥基础设施第2章 安全协议 2.1 安全协议概述 2.2 安全协议的缺陷 2.3 安全协议及其受到的攻击实例 2.4 安全协议的形式化分析 小结第3章 基于推理结构性方法 3.1 BAN逻辑 3.2 GNY逻辑 3.3 AT逻辑 3.4 SVO逻辑 3.5 Kailar逻辑 3.6 CS逻辑 3.7 KG逻辑 3.8 Nonmonotomic逻辑 小结第4章 基于攻击结构性方法 4.1 一般目的的验证语言 4.2 单一代数理论模型 4.3 特别目的的专家系统 小结第5章 基于证明结构性方法 5.1 human-readable证明法 5.2 Paulson归纳法 5.3 Schneider秩函数 5.4 strand space 5.5 Attacks限定法 5.6 Rewriting逼近法 5.7 Maude分析法 5.8 invariant技术 小结第6章 安全协议分析的形式化语言 6.1 安全协议分析预言：CPAL 6.2 安全协议简单接口说明语言——ISL&AAPA 6.3 安全协议通用说明语言——CAPSL 6.4 安全协议分析编译器Casper 5.5 安全协议的积分——spi积分 小结第7章 安全协议设计的形式化方法 7.1 Heintze&Tygar：模型及其构成 7.2 Gong&Synersion：fail-stop协议 7.3 Buttyan&Staaman简单逻辑 7.4 Rudolph抽象模型 小结第8章 Kerberos 8.1 Kerberos协议概况 8.2 票据标志使用与请求 8.3 消息交换 8.4 ULTRIX操作系统上Kerberos的实现第9章 IPsec协议 9.1 IPsec体系结构 9.2 安全联盟 9.3 IPsec的安全协议 9.4 IPsec的应用第10章 SSL V3.0 10.1 SSL V3.0概况 10.2 SSL V3.0中的状态 10.3 记录层协议 10.4 Change Cipher Spec协议 10.5 Alert协议 10.6 握手协议层第11章 X.509 11.1 X.509 v3证书概述 11.2 证书及其扩展 11.3 CRL及其扩展 11.4 证明路径的检验 11.5 算法支持第12章 SET协议 12.1 背景及商业要求 12.2 系统设计 12.3 证书管理结构 12.4 证书请求协议 12.5 证书撤消 12.6 SET私有扩展参考文献

<<安全协议理论与方法>>

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>