

<<安全协议的建模与分析>>

图书基本信息

书名：<<安全协议的建模与分析>>

13位ISBN编号：9787111157212

10位ISBN编号：7111157214

出版时间：2005-1

出版时间：机械工业出版社

作者：[英] Peter Rya

页数：235

字数：381000

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>

<<安全协议的建模与分析>>

内容概要

本书主要介绍了安全协议的一种建模与分析方法：CSP（Communicating Sequential Processes，通信顺序进程）方法。

本书共有11章和3个附录，主要内容包括：安全协议概述、CSP方法介绍、安全协议的CSP建模方法、协议目标描述、FDR概述、Casper介绍、为FDR进行协议和入侵者编码、分析结果的定理证明、协议的简化转换、其他的安全协议分析方法以及安全协议分析所存在的问题与发展趋势。

附录包括：密码学背景知识、具体实例及第8章的详细证明过程。

本书可作为高等院校信息安全、计算机、通信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。

<<安全协议的建模与分析>>

书籍目录

译者序原书序第0章 绪论 0.1 安全协议 0.2 安全特性 0.3 密码学 0.4 分钥证书与基础设施 0.5 加密模式 0.6 密码学中的哈希函数 0.7 数字签名 0.8 安全协议的脆弱性 0.9 CSP方法 0.10 Casper:FDR的用户好界面 0.11 形式化分析的局限 0.12 小结第1章 CSP介绍 1.1 基本模块 1.2 并行运算符 1.3 隐藏与重命名 1.4 更多的运算符 1.5 过程行为 1.6 离散时间第2章 使用CSP对安全协议建模 2.1 可信赖的过程 2.2 协议模型的数据类型 2.3 入侵者建模 2.4 并归网络第3章 表达协议目的 3.1 Yahalom协议 3.2 保密性 3.3 认证 3.4 不可否认 3.5 匿名 3.6 小结第4章 FDR概述 4.1 比例过程 4.2 标准转换系统 4.3 开发成分结构 4.4 反例第5章 Casper 5.1 一个输入什么文件的例子 5.2 符号% 5.3 实例研究:大嘴青蛙协议 5.4 协议技术说明 5.5 哈希函数与Vernam加密 5.6 小结.....第6章 为FDR编码协议和入侵者第7章 定理证明第8章 简化转换第9章 其他方法第10章 发展趋势及更多的问题附录A 密码学背景知识附录B Yahalom协议的Casper表示附录C CyberCash阶函数分析参考文献符号列表专业词汇英语中对照表

<<安全协议的建模与分析>>

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>