<<密码协议形式化分析>>

图书基本信息

书名：<<密码协议形式化分析>>

13位ISBN编号：9787111192299

10位ISBN编号：711119229X

出版时间：2006-7

出版时间：机械工业出版社

作者：王亚弟、束妮娜、韩继红、王娜

<<密码协议形式化分析>>

内容概要

本书对现在国内外最新的密码协议形成化分析方法与设计准则进行了比较详细的论述，建立了完整而系统密码协议研究理论，并介绍了当前最为流行的几个协议的实现方法。

全书共8章，分别介绍了密码协议所涉及的密码学基础知识，密码协议的概念、缺陷与可能受到的攻击类型，现有的一些密码协议形式化分析方法，密码协议的设计准则，密码协议分析的主要形式化语言和分析工具，Kerberos协议、IPSee协议、SSL协议、X.509以及SET协议这五个密码协议的实现方法和工作原理。

本书适合作为高等院校信息安全专业本科生、研究生使用，也可供从事信息安全研究的科技人员参考。

书的最后附有相关的参考文献，提供了与本书有关的资料，供有兴趣的读者参考。

<<密码协议形式化分析>>

书籍目录

出版说明序前言第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 1.5 PKI公钥基础设施 1.6 本章小结 1.7 习题第2章 密码协议概述 2.1 引言 2.2 密码协议基本概念 2.3 密码协议的缺陷及所受到的攻击实例 2.4 密码协议的设计与分析 2.5 密码协议形式化分析的研究与进展 2.6 本章小结 2.7 习题第3章 形式逻辑方法 3.1 BAN逻辑 3.2 扩展的BAN逻辑 3.3 BAN类逻辑现状 3.4 Kailar逻辑 3.5 本章小结 3.6 习题第4章 模型检测方法 4.1 引言 4.2 模型检测技术分析密码协议的方法和结果 4.3 CSP及FDR模型检测技术 ……第5章 定理证明方法第6章 密码协议的设计准则第7章 密码协议分析主要的形式化语言和分析工具 第8章 几个具体密码协议的实现方法和工作原理参考文献

<<密码协议形式化分析>>

版权说明