

<<电子商务网络协议的形式化分析理论与>>

图书基本信息

书名：<<电子商务网络协议的形式化分析理论与应用>>

13位ISBN编号：9787030200327

10位ISBN编号：7030200322

出版时间：2008-1

出版时间：科学出版社

作者：谢晓尧

页数：146

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>

<<电子商务网络协议的形式化分析理论与>>

内容概要

本书叙述了与信息安全有密切联系的基于网络电子商务协议的形式化分析理论方法与实际应用。具体内容包括：电子商务协议的形式化逻辑分析方法、通用形式化Petri网模型分析方法、有穷自动机模型检测分析方法、安全认证和交易的基本协议，以及协议的有色Petri网模型及分析的软件工具CPN Tools等。

同时，本书应用这些分析方法和工具具体分析了相关的认证和支付等协议。

本书适合于高等院校计算机专业、电子商务专业高年级本科生和研究生阅读，也可供科研人员参考。

书籍目录

序前言第1章 概论 1.1 信息安全的基本定义 1.2 网络的安全问题 1.3 网络安全体系结构第2章 电子商务协议的形式化分析理论基础 2.1 电子商务的定义 2.2 电子商务协议的安全性 2.2.1 电子商务协议的安全性 2.2.2 电子商务协议的设计原则 2.2.3 电子商务协议的安全分析 2.2.4 电子商务协议形式化分析方法分类第3章 电子商务协议的形式化逻辑分析方法 3.1 BAN逻辑 3.1.1 BAN逻辑公式 3.1.2 BAN逻辑的推理规则 3.1.3 BAN逻辑的评价 3.2 Kailar逻辑 3.2.1 Kailar逻辑公式 3.2.2 Kailar逻辑的推理规则 3.3 NDL逻辑 3.3.1 NDL逻辑的语法 3.3.2 NDL逻辑的推理规则 3.4 卿周逻辑 3.4.1 卿周逻辑的语法 3.4.2 卿周逻辑的推理规则第4章 电子商务协议的通用形式化Petri网模型分析方法 4.1 Petri网概述 4.2 Petri网的定义 4.3 Petri网的应用实例 4.4 Petri网的特性 4.4.1 保守网 4.4.2 有界网 4.4.3 活动性 4.4.4 并发与冲突 4.5 Petri网的扩充 4.5.1 输入函数和输出函数的扩充 4.5.2 触发条件的扩充 4.5.3 旗标和库所的扩充(着色Petri网) 4.6 Petri网的替换与合成 4.7 常用的Petri网模型 4.7.1 库所/变迁网(P/T网)的形式化定义 4.7.2 有色网的形式化定义 4.7.3 常量弧有色网的形式化定义 4.8 Petri网的分析 4.8.1 常量弧网 4.8.2 库所/变迁网(P/T网) 4.8.3 有色网 第5章 电子商务协议的形式化有穷自动机模型检测分析方法 5.1 有穷自动机的定义 5.2 传输通道类别 5.3 通道DFA 5.4 协议实体DFA 5.5 DFA的简化 5.6 DFA的合成第6章 基于电子商务安全认证和交易的基本协议 6.1 安全认证的基本协议 6.1.1 Needham—Schroeder认证协议 6.1.2 Kerberos认证协议 6.1.3 Otway—Rees认证协议 6.2 电子交易的基本协议 6.2.1 网上交易协议遵循的原则 6.2.2 IBS支付协议 6.2.3 CMP1及CMP2非否认协议第7章 基于公钥基础设施PKI的安全认证协议第8章 基于工商管理的安全认证协议第9章 安全认证协议的Petri网模型第10章 支付协议的有穷自动机模型第11章 协议的有色Petri网模型及分析参考文献

编辑推荐

《电子商务网络协议的形式化分析理论与应用》由科学出版社出版。

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>