<<安全协议原理与验证>>

图书基本信息

书名：<<安全协议原理与验证>>

13位ISBN编号：9787563526727

10位ISBN编号：7563526722

出版时间：2011-8

出版时间：北京邮电大学出版社

作者：王聪　等编著

页数：303

<<安全协议原理与验证>>

内容概要

本书介绍安全协议及其验证方法，主要内容包括三个部分：1.基础知识，包括安全协议基本原理介绍、安全性分析以及密码学基础；2.安全协议原理，包括安全协议概述、经典的密码交换及认证协议、电子商务协议以及应用中的安全协议；3.安全协议的分析与验证方法，包括BAN逻辑、BAN类逻辑、Kailar逻辑、CS逻辑、串空间理论及CSP方法等。

本书较为全面、深入地介绍了信息安全体系中的安全协议原理及安全协议的分析验证方法。内容安排由浅入深，重点突出，涵盖了当前安全协议研究领域的主要成果。

本书可作为高等院校信息安全、计算机、通信等专业高年级本科生和研究生教材，也可供从事相关专业的教学、科研和工程技术人员参考。

<<安全协议原理与验证>>

书籍目录

第一部分 基础知识
　第1章 引言
　第2章 密码学基础
第二部分 安全协议原理
　第3章 安全协议概述
　第4章 认证与密钥交换协议
　第5章 电子商务协议
　第6章 实际使用中的的安全协议
第三部分 安全协议的分析、验证方法
　第7章 BAN逻辑
　第8章 BAN类逻辑
　第9章 Kailar逻辑
　第10章 时间相关安全协议分析
　第11章 串空间模型理论及协议分析方法
　第12章 安全协议的CSP分析方法
　第13章 其他安全协议分析验证方法
参考文献

章节摘录

版权页：插图：任何安全协议都是为了完成一定的安全目标，即要达到一定的安全属性。
简单地说，安全协议的目标就是保证某些安全属性在协议执行完毕时能够得以实现。
换句话说，评估一个安全协议是否安全就是检查其所要达到的安全属性是否受到入侵者的破坏。
下面介绍安全协议中的一些安全属性。
1.2.1秘密性在网络中运行的任何有效协议都包含一些不能被合法参与者之外的人知道的秘密信息，协议参与者正是基于这些秘密信息完成必要的操作，达到安全目的。
秘密性是安全协议的基本属性。
保证协议的秘密性即是要保证这些秘密信息不会被攻击者获取。
1.2.2认证性安全协议的另外一个基本属性则是认证性。
认证可以分为两类：实体认证和数据认证。
前者对通信方的身份进行认证，并强调实时性。
后者对通信数据进行认证，确保传输中没有被篡改，保证传输的数据最初来自于某个合法用户。
无论是实体认证还是数据认证，都是利用一个不可冒充的秘密信息来证明一个主体或数据来源的身份，即协议中是由数据的秘密性来获得实体和数据的认证性。
1.2.3完整性完整性是指协议的特定数据不被非法篡改、删除。
但需要说明的是，在网络环境中，任何数据都可能被篡改，完整性只是提供发现篡改的机制。
1.2.4不可否认性不可否认性是指协议参与者必须对自己的合法行为负责，发送者不能对自己发出了某消息这一事实进行抵赖，同时接收者也不能对自己接收了某消息这一事实进行否认。
不可否认性是电子商务协议的一个重要性质，是保证交易正常进行的必要条件。
保证不可否认性最常用的技术是数字签名。

编辑推荐

《安全协议原理与验证》为普通高校信息安全系列教材之一。

<<安全协议原理与验证>>

版权说明