<<安全协议>>

图书基本信息

书名：<<安全协议>>

13位ISBN编号：9787563520497

10位ISBN编号：756352049X

出版时间：2009-8

出版时间：北京邮电大学出版社

作者：曹天杰，张永平，汪楚娇　编著

页数：241

<<安全协议>>

前言

密码学的用途是解决各种难题。
当我们考虑现实世界中的应用时，常常遇到以下安全需求：机密性、完整性、认证性、匿名性、公平性等，密码学解决的各种难题围绕这些安全需求。
安全协议是使用密码学完成某项特定的任务并满足安全需求的协议，又称密码协议，它在网络和分布式系统中有着大量的应用。
安全协议使用分组密码、公开密钥密码、散列函数、消息认证码、数字签名等密码原语构造，这些密码原语好比是砖头，安全协议就是利用砖头建筑的具有不同功能的大楼，比如写字楼、游泳馆、住宅等。
我们知道即使砖头是结实的，如果设计得不好，大楼也是容易倒塌的，也是不安全的。
本教材将讲解如何利用密码原语这些砖头构建一座座既要提供各种不同功能，又要安全牢固的“大楼”。
安全协议经过几十年的研究，已经取得了丰硕的成果，近些年的发展更是十分迅猛。
遗憾的是，已有教材不能全面地反映安全协议的整个研究领域，不能让学生把握安全协议的全貌，达不到领会基本概念、掌握基础知识的目标。
作为密码学的后续课程，国内60多所高校的信息安全专业大多设置了安全协议课程。
因此，对安全协议进行系统的总结，出版一部安全协议的教材是十分必要的。
本书内容全面、选材新颖、前后连贯。
讲述了安全协议的基本理论、安全协议的主要类型及安全协议的分析方法。
（1）内容全面。
较全面地介绍了满足各种应用需要的安全协议，包括经典协议（即使有缺陷）、标准化的协议、现实中广泛应用的协议。
（2）选材新颖。
作者一直从事安全协议方面的研究，能够把握这一领域发展的主流方向，因此在取材上能够把最新的研究成果引入教材。
如认证密钥交换协议包括可否认的认证密钥交换协议、通信匿名的认证密钥交换协议、用户匿名的认证密钥交换协议，这些新概念进入教材能够开阔学生的视野，把学生引入到前沿课题中。
教材编写中，有些例题、习题选自己出版的学术论文。

<<安全协议>>

内容概要

本书全面和系统地讲述了安全协议的基本理论、安全协议的主要类型及安全协议的分析方法。围绕机密性、完整性、认证性、匿名性、公平性等实际需求，较全面地介绍满足各种应用需要的安全协议。

本书主要内容包括：安全协议概述、安全协议的密码学基础、基本的安全协议、认证与密钥建立协议、零知识证明、选择性泄露协议、数字签名变种、非否认协议、公平交换协议、安全电子商务协议、安全多方计算、安全协议的形式化分析。

本书内容全面、选材新颖、前后连贯，是江苏省高等学校精品教材建设立项项目。

本书不仅可以作为信息安全专业本科生、研究生教材，也可以作为信息安全领域科研人员的参考书。

<<安全协议>>

书籍目录

第1章 安全协议概述 1.1 安全协议的概念 1.1.1 协议、算法与安全协议 1.1.2 协议运行环境中的角色 1.2 常用的安全协议 1.3 安全协议的安全性质 1.4 对安全协议的攻击 1.4.1 窃听 1.4.2 篡改 1.4.3 重放 1.4.4 预重放 1.4.5 反射 1.4.6 拒绝服务 1.4.7 类型攻击 1.4.8 密码分析 1.4.9 证书操纵 1.4.10 协议交互 1.5 安全协议的缺陷 1.6 安全协议的三大理论分析方法 1.6.1 安全多方计算 1.6.2 安全协议的形式化分析方法 1.6.3 安全协议的可证明安全性理论 习题1第2章 安全协议的密码学基础 2.1 密码学的基本概念 2.2 数论中的一些难题 2.3 随机数 2.4 分组密码 2.5 公开密钥密码 2.5.1 公开密钥密码的基本概念 2.5.2 ：RSA体制 2.5.3 Rabin体制 2.6 散列函数 2.7 消息认证 2.8 数字签名 2.8.1 数字签名的基本概念 2.8.2 RSA签名 2.8.3 ：RSA签名标准PSS 2.8.4 数字签名标准DSS 2.8.5 一般的离散对数签名体制 2.8.6 ElGamal数字签名 2.8.7 Schnorr签名体制 2.8.8 Okamoto签名体制 2.8.9 基于椭圆曲线的数字签名算法ECDSA 2.9 基于身份的公钥密码学 2.9.1 基于身份的密码系统与基于PKI的密码系统的比较 2.9.2 基于身份的加密方案 2.9.3 基于身份的签名方案 习题2第3章 基本的安全协议 3.1 秘密分割 3.2 秘密共享 3.3 阈下信道 3.3.1 阈下信道的概念 3.3.2 基于ElGareal数字签名的阈下信道方案 3.3.3 基于RSA数字签名的阈下信道方案 3.4 比特承诺 3.4.1 使用对称密码算法的比特承诺 3.4.2 使用单向函数的比特承诺 3.4.3 使用伪随机序列发生器的比特承诺 3.5 公平的硬币抛掷 3.5.1 单向函数抛币协议 3.5.2 公开密钥密码抛币协议 3.6 智力扑克 3.6.1 基本的智力扑克游戏 3.6.2 三方智力扑克 3.7 不经意传输 习题3第4章 认证与密钥建立协议第5章 零知识证明第6章 选择性泄露协议第7章 数字签名变种第8章 非否认协议第9章 公平交换协议第10章 安全电子商务协议第11章 安全多方计算第12章 安全协议的形式化分析参考文献

章节摘录

插图：1．参与者协议执行过程中的双方或多方，也就是人们常说的发送方和接收方。
协议的参与者可能是完全信任的人，也可能是攻击者和完全不信任的人。
比如认证协议中的发起者和响应者，零知识证明中的证明人和验证者，电子商务中的商家、银行和客户等。
2．攻击者攻击者（敌手）就是协议过程中企图破坏协议安全性和正确性的人。
人们把不影响协议执行的攻击者称为被动攻击者，他们仅仅观察协议并试图获取信息。
还有一类攻击者叫做主动攻击者，他们改变协议，在协议中引入新消息、修改消息或者删除消息等，达到欺骗、获取敏感信息、破坏协议等目的。
攻击者可能是协议的合法参与者，或是外部实体，或是两者的组合体，也可能是单个实体，或是合谋的多个实体。
攻击者可能是协议参与者，他可能在协议期间撒谎，或者根本不遵守协议，这类攻击者叫做骗子，由于是系统的合法用户，因此也称为内部攻击者。
攻击者也可能是外部的实体，他可能仅仅窃听以获取可用信息，也可能引入假冒的消息，这类攻击者称为外部攻击者。
3．可信第三方可信第三方（Trusted Third Party，TTP）是指在完成协议的过程中，值得信任的第三方，能帮助互不信任的双方完成协议。
仲裁者是一类特殊的可信第三方，用于解决协议执行中出现的纠纷。
仲裁者是在完成协议的过程中，值得信任的公正的第三方，“公正”意味着仲裁者在协议中没有既得利益，对参与协议的任何人也没有特别的利害关系。
“值得信任”表示协议中的所有人都接受仲裁的结果，即仲裁者说的都是真实的，他做的仲裁是正确的，并且他将完成协议中涉及他的部分。
其他可信第三方如密钥分发中心、认证中心等。

编辑推荐

<<安全协议>>

版权说明