<<安全协议>>

图书基本信息

书名：<<安全协议>>

13位ISBN编号：9787302232902

10位ISBN编号：7302232903

出版时间：2011-1

出版时间：清华大学出版社

作者：冯登国

页数：520

<<安全协议>>

前言

随着全球信息化程度的日益提高，网络已经成为人类获取信息、沟通交流以及社会生产和生活活动的一种不可或缺的重要载体和手段，信息安全的重要性和紧迫性日益突显。
随着金融、能源、交通、电信等重要基础设施对网络的依赖性逐渐增大，信息安全对于社会和经济的影响也越来越大。
信息安全问题已经由个人、团体的隐私与机密性问题上升为国家的战略性问题，而安全协议是解决网络安全问题最直接、最有效的手段之一，它可以有效地解决源认证和目标认证、消息的完整性、匿名通信、抗拒绝服务、抗抵赖、授权等一系列重要安全问题。
安全协议是建立在密码算法基础上的一种高互通协议，它运行在计算机网络或分布式系统中，为安全需求的各方提供一系列步骤，借助于密码算法来达到密钥分发、身份认证以及安全地实现网络通信或电子交易等目的。
我领导的安全协议研究团队，从1995年便开始安全协议的研究工作，分两个方面展开研究。
重点采用理论与实践相结合的技术路线：一方面是理论与技术研究，主要采用以讨论班为主的自由研究模式；另一方面是应用与实践研究，主要采用以工作组为主的集中研究模式。
曾得到中国科学院“百人计划”项目、国家自然科学杰出青年基金项目、国家自然科学基金项目和国家973计划项目课题的支持，取得了一批高水平的研究成果，培养了一批核心骨干人才，发表了一批高质量学术论文，也在已出版的部分著作中反映了我们的一些研究成果。
我一直想把我们在安全协议方面的研究成果和对安全协议的理解写成一本专著与同行分享，以便更多的学者受益。
从1999年开始动手写作，转眼就是10年，在这期间，易稿数次，举办过多次安全协议研讨会，与数名专家进行过交流，调研过包括研究、应用和实践等在内的各种安全需求。
理论与技术在不断发展，应用和实践范围在不断扩大和深人，人类对安全协议的认识水平也在不断提高，在这种背景下，要写一本“好”书非常困难，但我还是下决心推出了这本书，试图系统全面地覆盖安全协议的核心内容，并反映我所领导的团队在这一领域的部分前沿成果。
因此，本书是作者及其团队长期从事安全协议研究和实践工作的方法和经验的总结，同时也吸收了国内、外现有相关成果中的许多精华。

<<安全协议>>

内容概要

本书共分4篇16章。
系统地介绍安全协议的基本理论、关键技术以及典型应用和实践。
主要内容包括密码算法基础知识，可证明安全性、形式化分析、零知识证明、安全多方计算等基础理论与方法，秘密共享、数字签名、身份识别、密钥交换、健忘传输、公平交换等基本安全协议，以及kerberos协议、x．509协议、ipsec协议、tls／ssl协议、入侵容忍ca协议、基于身份的pki协议、可信计算平台远程证明协议等。
　本书可供从事信息安全、密码学、计算机、通信、数学等专业的科技人员、硕士和博士研究生参考，也可供高等院校相关专业的师生参考。

<<安全协议>>

书籍目录

章节摘录

插图：在一个大的分布式环境中运行安全协议所面临的最大问题是，其所处的网络通信环境是不安全的。
如果将协议及其所处的环境视为一个系统，那么在这个系统中，一般而言包括发送和接收消息的诚实主体和一个攻击者，以及用于管理消息发送和接收的规则。
协议的合法消息可被攻击者截取、修改、重放、删除和插入。
攻击者将所有已知的消息放入其知识集合KS（Knowledge Set）中。
诚实主体之间交换的任何消息都将被加入到攻击者的KS中，并且攻击者可对KS中的消息进行操作，将所得消息也加入到KS中。
攻击者可进行的操作至少包括级联、分离、加密和解密。
图2.1是安全协议系统模型的示意图。
一个被动攻击者可在线窃听敏感信息。
而一个主动攻击者则可截获数据包并对其进行任意的修改，甚至可以伪装成通信主体欺骗诚实主体与其进行非法通信。
加密运算可以有效地阻止主动入侵，因为在不知道密钥的前提下，对密文消息的丝毫改动都将导致解密运算的失败，此时攻击者能做的仅仅是阻止消息送达或准时送达其目的地。
归纳起来，攻击者的行为表现为以下几种形式。

<<安全协议>>

编辑推荐

《安全协议:理论与实践》：信息安全理论与技术系列丛书

<<安全协议>>

版权说明