<<认证理论及应用>>

图书基本信息

书名：<<认证理论及应用>>

13位ISBN编号：9787302208273

10位ISBN编号：7302208271

出版时间：2009-11

出版时间：清华大学出版社

作者：李晓航，王宏霞，张文芳　编著

页数：222

前言

21世纪是信息的时代。
随着国家信息化的不断推进和电子商务、电子政务的大力建设，信息已经成为最能代表综合国力的战略资源，信息化正在对国家和社会的各方面产生巨大影响。
然而，伴随信息化而来的信息安全问题也随之突显，能否有效地保护信息资源，保护信息化进程健康、有序、可持续发展，已经成为关乎国家和社会发展的头等大事。
保障信息安全主要依靠密码学理论及其相关应用。
密码学的最初目的是“保密”，即保证机密信息只能被系统中授权的各方所获得。
然而随着攻击手段的不断发展，主动攻击逐渐成为信息系统安全的主要威胁，如何防止敌手对信息系统进行主动攻击变得越来越重要。
“认证”（Authentication）是现代密码学中对抗主动攻击的重要手段，它对于开放网络环境中各种信息系统的安全有着重要作用，其主要目的是提供信息的真实性、完整性和不可抵赖性，以对抗伪造、篡改和重放等攻击。
可以说，在某些情况下“认证”比“保密”更为重要。
为了更好地突出认证理论在现代密码学中的重要作用，建立信息安全专业良好的课程体系结构，作者所在高校开设了“认证理论及应用”这门课，作为信息安全专业的主要专业课。
但在授课中发现，经典的密码学教材大都以“保密”为主，以“认证”为辅。
为此，作者在参考国内外经典教材的基础上，编写了《认证理论及应用》讲义，用于课堂教学，并在此基础上，结合教学实践和科研工作编著了本书。

<<认证理论及应用>>

内容概要

本书是一本集中介绍信息安全领域中认证技术的教材。
全书共分为8章，主要内容包括认证理论的基础、Hash函数和报文鉴别、数字签名、实体认证和密钥交换协议、身份认证协议、智能卡技术及其在认证系统中的应用、基于数字水印技术的多媒体认证、典型的实用网络认证协议等。
本书在编排时主要围绕密码学中为对抗主动攻击而引入的认证理论及相关内容，突出了应用性，并结合作者在相关领域的科研成果引入了新的认证技术，如基于数字水印的多媒体认证技术。
本书可作为信息安全、计算机应用等专业的研究生和高年级本科生以及相关领域技术人员的教材，为他们在认证理论及应用方面的学习和工作提供必要的参考。

作者简介

李晓航，西南交通大学信息科学与技术学院教师。
长期主讲“ 认证理论及应用 ”和“ 信息系统安全技术 ”等课程。
作为主要研发人员参加国防科技重点实验室基金试点项目1项和铁道部科技司开发项目2项，并主持多项软件开发项目，发表学术论文数篇，研究兴趣与专长：信息安全技术

<<认证理论及应用>>

书籍目录

章节摘录

插图：第1章 认证理论基础随着信息的多元化及数字化的迅猛发展，信息安全技术显得越来越重要，而且信息安全技术应用水平的高低直接影响了信息高速公路建设的进一步发展。
近20年来，由于计算机硬件处理能力的极大提高和密码学的迅速发展，信息安全理论与技术也在逐步完善和丰富。
认证技术是信息安全理论与技术的一个重要方面，主要包括用户认证和信息认证两个方面。
前者用于鉴别用户身份，后者用于保证通信双方的不可抵赖性和信息的完整性。
根据认证信息的性质可以将用户认证分为秘密知识证明，物理介质证明和实体特征证明。
秘密知识证明主要通过通信双方共享的口令、个人识别码和密钥等进行身份认证。
在物理介质证明中，证明方必须提供令牌卡、信用卡和密钥卡等物理介质验证自己的身份。
实体特征证明包括实体的物理特征和生物特征，物理特征主要包括计算机通信设备的网卡（如地址、硬盘序列号等），生物特征包括指纹、笔迹、脸形、虹膜、视网膜、脉搏、耳廓和声音等。
在某些情况下，信息认证显得比信息保密更为重要。
例如，在金融网络中发生的业务或交易，可能交易的具体内容并不需要保密，但是交易双方应当能够确认是对方发送（接收）了这些信息，同时接收方还能确认接收的信息是完整的，即在通信过程中没有被修改或替换。
另一个例子是网络中的信息广播（通知），此时接收方主要关心的是信息的真实性和信息来源的可靠性。
因此，在这些情况下，信息认证将处于首要的地位。
从用户角度来看，非法用户常采用以下手段对网络系统进行攻击。

<<认证理论及应用>>

版权说明