第一图书网, tushu007.com

<<网络安全新型技术研究及其应用>>

图书基本信息

书名：<<网络安全新型技术研究及其应用>>

13位ISBN编号：9787564707835

10位ISBN编号：7564707836

出版时间：2011-03-01

出版时间：电子科技大学出版社

作者：李洪伟

页数：219

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

内容概要

公钥密码系统面临的挑战不仅包括寻找和实现安全算法，还包括建立支持公钥认证的基础设施。
在传统的公钥基础设施PKI中，证书用来保证公钥和身份之间的联系，实现公钥的认证。
但是，PKI在实践中面临很多挑战，例如可扩展性和证书的管理。
为了解决PKI的这些问题，Shamir在1985年提出了基于身份的密码体制（IBC）。
在IBC中，公钥直接从用户唯一可标识的身份信息中获得，例如用户的姓名或者Email地址等，公钥的认证不再需要证书。
IBC是解决公钥认证的另外一种有效方法，和传统PKI相比，IBC在密钥管理上有很大的优势。
Shamir在提出IBC概念的同时构造了第一个基于身份的签名方案，但是在基于身份加密方面的研究工作一直都没有多大的进展。
直到2001年，Boneh与Franklin首次利用Weil对提出了一个实用安全的基于身份加密方案，使基于身份的公钥密码重新成为一个研究热点，许多基于身份的密码系统相继提出。
然而，在IBC中还存在一些有待解决的公开问题，如密钥托管、密钥撤销、密钥进化、安全模型等问题。
研究和解决这些问题对IBC无论在理论上还是实践中都具有重要的意义。
《网络安全新型技术研究及其应用》针对IBC中存在的问题进行了深入的研究，提出了一些有效的解决方案，取到了一些研究成果。

作者简介

李洪伟，电子科技大学计算机科学与工程学院，博士，讲师（享受副教授待遇），担任了国际会议“The 8th IEEE International Conferenceon Dependable Autonomicand Secure Computing”的程序委员和分会主席，国家留学基金委全额资助加拿大博士后，近年来在LNCS、Journalof Systems Engineeringand Electronics等国内外期刊或会议上发表学术论文10余篇，SCI、EI收录9篇，主持多项科研、教改项目，教学课程《计算机网络基础》被评为“四川省精品课程”。

书籍目录

第1章 网络安全风险分析1.1 TCP/JP协议缺陷1.2 路由协议实现缺陷1.3 软件缺陷1.4 操作系统安全问题1.5 网络安全风险1.6 本章小结第2章 网络安全体系结构2.1 信息安全总体框架2.2 0SI安全体系结构2.3 本章小结第3章 基于身份公钥密码概述3.1 基于身份公钥密码体制的研究背景和意义3.2 基于身份公钥密码的发展现状及其存在的问题3.3 本章小结第4章 基本概念和基础理论4.1 椭圆曲线4.2 双线性映射4.3 BDH及相关难题4.4 基于身份的公钥密码系统4.5 可证安全基础4.6 网格安全4.7 本章小结第5章 基于身份的认证协议研究5.1 -种基于身份的无线局域网认证协议5.2 本章小结第6章 基于身份的加密算法研究6.1 引言6.2 一种改进的基于身份的加密算法IIBE6.3 IIBE安全性的形式化证明6.4 仿真实验及分析6.5 本章小结第7章 基于身份的密钥进化算法研究7.1 引言7.2 一种基于身份的前向安全加密7.3 一种基于身份的抗入侵加密IBE-1R7.4 本章小结第8章 基于身份的密码算法在网格中的应用8.1 引言8.2 一种基于身份的网格体系结构8.3 一种基于身份的网格加密算法8.4 一种基于身份的网格签名算法8.5 一种基于身份的网格认证协议8.6 一种网格安全标准GSI的改进方案8.7 本章小结第9章 本书总结及其展望9.1 总结9.2 展望参考文献缩略词表

第一图书网, tushu007.com

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