

<<信息与计算机安全进展>>

图书基本信息

书名：<<信息与计算机安全进展>>

13位ISBN编号：9783540476993

10位ISBN编号：3540476997

出版时间：2006-12

出版时间：湖南文艺出版社

作者：Rannenberg, Kai 编

页数：438

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>

<<信息与计算机安全进展>>

内容概要

This book constitutes the refereed proceedings of the First International Workshop on Security, IWSEC 2006, held in Kyoto, Japan in October 2006. The 30 revised full papers presented were carefully reviewed and selected from 147 submissions. The papers are organized in topical sections on signatures, security evaluation, authentication, encryption and key exchange, network security, security for multimedia, cryptanalysis and implementation, as well as access control.

<<信息与计算机安全进展>>

书籍目录

Signatures (1) ID-Based Ring Signature Scheme Secure in the Standard Model A Short Verifier-Local Revocation Group Signature Scheme with Backward Unlinkability Sound Computational Interpretation of Symbolic Hashes in the Standard Model Security Evaluation A Requirement Centric Framework for Information Security Evaluation A Model-Based Method for Security Configuration Verification Personal Computer Privacy: Analysis for Korean PC Users Signatures (2) Short Traceable Signatures Based on Bilinear Pairings Ring Signature with Designated Linkability Ad Hoc Group Signatures Rateless Codes for the Multicast Stream Authentication Problem Authentication Crossing Borders: Security and Privacy Issues of the European e-Passport A New Approach to Hide Policy for Automated Trust Negotiation Towards Remote Policy Enforcement for Runtime Protection of Mobile Code Using Trusted Computing IP Address Authorization for Secure Address Proxying Using Multi-key CGAs and Ring Signatures Security for Multimedia A Study of Detection Method of Printed Image Alteration Using Digital Watermark Real-Time Watermark Embedding for High Resolution Video Watermarking Inhibiting Card Sharing Attacks Network Security A Flooding-Based DoS/DDoS Detecting Algorithm Based on Traffic Measurement and Prediction Hardware Stack Design: Towards an Effective Defence Against Frame Pointer Overwrite Attacks Modeling of Network Intrusions Based on the Multiple Transition Probability Encryption and Key Exchange Cryptanalysis and Implementation Access Control Author Index

<<信息与计算机安全进展>>

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>