<<   /Information and communications security>>

13   ISBN   9783540494966

10   ISBN   3540494960

          2006-12

          Springer-Verlag New York Inc

     Ning, Peng (EDT) / Qing, Sihan (EDT) / Li, Ninghui (EDT)

     558

                    PDF

          http://www.tushu007.com

This book constitutes the refereed proceedings of the 8th International Conference on Information and Communications Security, ICICS 2006, held in Raleigh, NC, USA in December 2006.   The 22 revised full papers and 17 revised short papers presented were carefully reviewed and selected from 119 submissions. The papers are organized in topical sections on security protocols, applied cryptography, access control and systems security, privacy and malicious code, network security, systems security, cryptanalysis, applied cryptography and network security, as well as security implementations.

Security Protocols Strong and Robust RFID Authentication Enabling Perfect Ownership Transfer A Robust and Secure RFID-Based Pedigree System (Short Paper) A Topological Condition for Solving Fair Exchange in Byzantine Environments A Security Analysis of the Precise Time Protocol (Short Paper) Applied Crytography An Identity-Based Proxy Signature Scheme from Pairings Finding Compact Reliable Broadcast in Unknown Fixed-Identity Networks (Short Paper) Formal Analysis and Systematic Construction of Two-Factor Authentication Scheme (Short Paper) Hierarchical Key Assignment for Black-Box Tracing with Efficient Ciphertext Size Trace-Driven Cache Attacks on AES (Short Paper) Access Control and Systems Security A Construction for General and Efficient Oblivious Commitment Based Envelope Protocols Defining and Measuring Policy Coverage in Testing Access Control Policies Distributed Credential Chain Discovery in Trust Management with Parameterized Roles and Constraints (Short Paper) An Operating System Design for the Security Architecture for MicroprocessorsPrivacy and Malicious Code Point-Based Trust: Define How Much Privacy Is Worth Efficient Protocols for Privacy Preserving Matching Against Distributed Datasets Quantifying Information Leakage in Tree-Based Hash Protocols (Short Paper) An Anonymous Authentication Scheme for Identification Card A Wireless Covert Channel on Smart Cards (Short Paper) Network Security From Proxy Encryption Primitives to a Deployable Secure-Mailing-List Solution Mathematical Foundations for the Design of a Low-Rate DoS Attack to Iterative Servers (Short Paper) An Independent Function-Parallel Firewall Architecture for High-Speed Networks (Short Paper) ……Systems SecurityCryptanalysisApplied Cryptography and Network SecuritySecutrity ImplementationsAuthor Index

PDF

:http://www.tushu007.com