1. Record Nr. UNINA9910484642903321

Titolo	Information and Communications Security : 8th International Conference, ICICS 2006, Raleigh, NC, USA, December 4-7, 2006, Proceedings / / edited by Peng Ning, Ninghui Li
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-49497-9
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XIV, 562 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 4307
Altri autori (Persone)	NingPeng QingSihan LiNinghui
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Data protection Electronic data processing - Management Computers and civilization Computer networks Algorithms Cryptology Data and Information Security IT Operations Computers and Society Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	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 Microprocessors -- Privacy 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) -- Estimating Accuracy of Mobile-Masquerader Detection Using Worst-Case and Best-Case Scenario -- An Enhanced N-Way Exchange-Based Incentive Scheme for P2P File Sharing (Short Paper) -- Systems Security -- Provably Correct Runtime Enforcement of Non-interference Properties -- An Attack on SMC-Based Software Protection -- Modular Behavior Profiles in Systems with Shared Libraries (Short Paper) -- Efficient Protection Against Heap-Based Buffer Overflows Without Resorting to Magic -- Cryptanalysis -- Cryptanalysis of Timestamp-Based Password Authentication Schemes Using Smart Cards -- Cryptanalysis of ID-Based Authenticated Key Agreement Protocols from Bilinear Pairings (Short Paper) -- Seifert's RSA Fault Attack: Simplified Analysis and Generalizations -- The Fairness of Perfect Concurrent Signatures -- Applied Cryptography and Network Security -- Secure Set Membership Using 3Sat -- Left-to-Right Signed-Bit ?-Adic Representations of n Integers (Short Paper) -- Universal Designated Verifier Signature Without Delegatability -- Tracing HTTP Activity Through Non-cooperating HTTP Proxies (Short Paper) -- Security Implementations -- A Fast RSA Implementation on Itanium 2 Processor -- Efficient Implementation of Public Key Cryptosystems on Mote Sensors (ShortPaper) -- Threshold Implementations Against Side-Channel Attacks and Glitches -- Hardware-and-Software-Based Security Architecture for Broadband Router (Short Paper).

Sommario/riassunto

It is our great pleasure to welcome you to the Eighth International Conference on Information and Communications Security (ICICS 2006), held in Raleigh, North Carolina, USA, December 4–7, 2006. The ICICS conference series is an established forum that brings together researchersand scholars involved in m- tiple disciplines of Information and Communications Security in order to foster exchangeof ideas. The past sevenICICS conferences wereheld in Beijing, China (ICICS 1997); Sydney, Australia (ICICS 1999); Xi'an China (ICICS 2001); S- gapore (ICICS 2002); Hohhot City, China (ICICS 2003); Malaga, Spain (ICICS 2004); and Beijing, China (ICICS 2005). The conference proceedings of the past seven events have been published by Springer in the Lecture Notes in Computer Science series, in LNCS1334,LNCS1726,LNCS2229, LNCS 2513,LNCS 2836, LNCS 3269, and LNCS 3783, respectively. This year we received a total of 119 submissions on various aspects of - hoc and sensor network security. The Program Committee selected 22 regular papers and 17 short papers that cover a variety of topics,

including security protocols, applied cryptography and cryptanalysis, access control in distributed systems, privacy, malicious code, network and systems security, and security implementations. Putting together ICICS 2006 was a team e?ort. First of all, we would like to thank the authors of every paper, whether accepted or not, for submitting their papers to ICICS 2006. We would like to express our gratitude to the Program Committee members and the external reviewers, who worked very hard in - viewing the papers and providing suggestions for their improvements.