

1. Record Nr.	UNINA9910484064203321
Titolo	Information Security : 8th International Conference, ISC 2005, Singapore, September 20-23, 2005, Proceedings // edited by Jianying Zhou, Robert H. Deng, Feng Bao
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (XII, 520 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 3650
Altri autori (Persone)	ZhouJianying LopezJavier DengRobert
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Computer networks Operating systems (Computers) Algorithms Computers and civilization Electronic data processing - Management Cryptology Computer Communication Networks Operating Systems Computers and Society IT Operations
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	Network Security I -- A Dynamic Mechanism for Recovering from Buffer Overflow Attacks -- SVision: A Network Host-Centered Anomaly Visualization Technique -- Trust & Privacy -- Time-Based Release of Confidential Information in Hierarchical Settings -- "Trust Engineering:" From Requirements to System Design and Maintenance -- A Working National Lottery System Experience -- A Privacy Preserving Rental System -- Key Management & Protocols -- Constant Round Dynamic

Group Key Agreement -- A Key Pre-distribution Scheme for
 Wireless Sensor Networks: Merging Blocks in Combinatorial Design --
 ID-based Multi-party Authenticated Key Agreement Protocols from
 Multilinear Forms -- On the Notion of Statistical Security in
 Simulatability Definitions -- Public Key Encryption & Signature --
 Certificateless Public Key Encryption Without Pairing -- Tracing-by-
 Linking Group Signatures -- Chaum's Designated Confirmer Signature
 Revisited -- Network Security II -- Routing-Assisted Defense
 Against DDoS Attacks -- IPSec Support in NAT-PT Scenario for IPv6
 Transition -- Signcryption -- Hybrid Signcryption Schemes with
 Outsider Security -- Analysis and Improvement of a Signcryption
 Scheme with Key Privacy -- Efficient and Proactive Threshold
 Signcryption -- Crypto Algorithm & Analysis -- Error Oracle Attacks on
 CBC Mode: Is There a Future for CBC Mode Encryption? -- Hardware
 Architecture and Cost Estimates for Breaking SHA-1 -- On the Security
 of Tweakable Modes of Operation: TBC and TAE -- A Non-redundant
 and Efficient Architecture for Karatsuba-Ofman Algorithm --
 Cryptography -- Compatible Ideal Contrast Visual Cryptography
 Schemes with Reversing -- An Oblivious Transfer Protocol with Log-
 Squared Communication -- Applications -- Electronic Voting: Starting
 Over? -- Timed-Release Encryption with Pre-open Capability and Its
 Application to Certified E-mail System -- Universally Composable
 Time-Stamping Schemes with Audit -- A Multiplicative Homomorphic
 Sealed-Bid Auction Based on Goldwasser-Micali Encryption -- Software
 Security -- Building a Cryptovirus Using Microsoft's Cryptographic API
 -- On the Security of the WinRAR Encryption Method -- Towards Better
 Software Tamper Resistance -- Authorization & Access Control --
 Device-Enabled Authorization in the Grey System -- Evaluating Access
 Control Policies Through Model Checking -- A Cryptographic Solution
 for General Access Control -- Student Papers -- Integrity
 Improvements to an RFID Privacy Protection Protocol for Anti-
 counterfeiting -- A Formal Definition for Trust in Distributed Systems
 -- A Practical Voting Scheme with Receipts -- New Constructive
 Approach to Covert Channel Modeling and Channel Capacity Estimation
 -- Efficient Modeling of Discrete Events for Anomaly Detection Using
 Hidden Markov Models.

Sommario/riassunto

This volume contains the proceedings of the 8th International Information Security Conference (ISC 2005), which took place in Singapore, from 20th to 23rd September 2005. ISC 2005 brought together individuals from academia and industry involved in many research disciplines of information security to foster the exchange of ideas. During recent years this conference has tried to place special emphasis on the practical aspects of information security, and since it passed from being an international workshop to being an international conference in 2001, it has become one of the most relevant forums at which researchers meet and discuss emerging security challenges and solutions. Advised by the ISC Steering Committee, and in order to provide students with more opportunities for publication, ISC 2005 accepted extra student papers - besides the regular papers. The initiative was very well accepted by the young sector of the scientific community, and we hope that the success of this idea will remain for next ISC events. Another important factor for the success of ISC 2005 was that selected papers in the proceedings will be invited for submission to a special issue of the International Journal of Information Security. The result was an incredible response to the call for papers; we received 271 submissions, the highest since ISC events started. It goes without saying that the paper selection process was more competitive and difficult than ever before — only 33 regular papers were accepted, plus 5

student papers for a special student session.
