1. Record Nr. UNISA996465637603316

Titolo	Information Security [[electronic resource]] : 7th International Conference, ISC 2004, Palo Alto, CA, USA, September 27-29, 2004, Proceedings / / edited by Kan Zhang, Yuliang Zheng
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2004
ISBN	3-540-30144-5
Edizione	[1st ed. 2004.]
Descrizione fisica	1 online resource (XII, 442 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 3225
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer communication systems Operating systems (Computers) Algorithms Computers and civilization Management information systems Computer science Cryptology Computer Communication Networks Operating Systems Algorithm Analysis and Problem Complexity Computers and Society Management of Computing and Information Systems
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	Key Management -- Practical Authenticated Key Agreement Using Passwords -- Further Analysis of Password Authenticated Key Exchange Protocol Based on RSA for Imbalanced Wireless Networks -- Storage-Efficient Stateless Group Key Revocation -- Digital Signatures -- Low-Level Ideal Signatures and General Integrity Idealization -- Cryptanalysis of a Verifiably Committed Signature Scheme Based on GPS and RSA -- How to Break and Repair a Universally Composable Signature Functionality -- New Algorithms -- RSA Accumulator Based

Broadcast Encryption -- Chameleon Hashing Without Key Exposure -- Radix-r Non-Adjacent Form -- Cryptanalysis -- On Related-Key and Collision Attacks: The Case for the IBM 4758 Cryptoprocessor -- Security Analysis of Two Signcryption Schemes -- On The Security of Key Derivation Functions -- Intrusion Detection -- Evaluating the Impact of Intrusion Detection Deficiencies on the Cost-Effectiveness of Attack Recovery -- A Model for the Semantics of Attack Signatures in Misuse Detection Systems -- Detection of Sniffers in an Ethernet Network -- Using Greedy Hamiltonian Call Paths to Detect Stack Smashing Attacks -- Securing DBMS: Characterizing and Detecting Query Floods -- Access Control -- An XML-Based Approach to Document Flow Verification -- Model-Checking Access Control Policies -- A Distributed High Assurance Reference Monitor -- Using Mediated Identity-Based Cryptography to Support Role-Based Access Control -- Human Authentication -- Towards Human Interactive Proofs in the Text-Domain -- Image Recognition CAPTCHAs -- Certificate Management -- A Hierarchical Key-Insulated Signature Scheme in the CA Trust Model -- Certificate Recommendations to Improve the Robustness of Web of Trust -- Mobile and Ad Hoc Security -- Universally Composable Secure Mobile Agent Computation -- Re-thinking Security in IP Based Micro-Mobility -- Shared-Key Signature and Its Application to Anonymous Authentication in Ad Hoc Group -- Web Security -- Prevent Online Identity Theft – Using Network Smart Cards for Secure Online Transactions -- Provable Unlinkability Against Traffic Analysis Already After Steps! -- An Efficient Online Electronic Cash with Unlinkable Exact Payments -- Digital Rights Management -- Modifiable Digital Content Protection in P2P -- Survey on the Technological Aspects of Digital Rights Management -- Detecting Software Theft via Whole Program Path Birthmarks -- Software Security -- Effective Security Requirements Analysis: HAZOP and Use Cases -- The Obfuscation Executive.

Sommario/riassunto

The 2004 Information Security Conference was the seventh in a series that started with the Information Security Workshop in 1997. A distinct feature of this series is the wide coverage of topics with the aim of encouraging interaction between researchers in di?erent aspects of information security. This trend c- tinuedintheprogramofthisyear' sconference.Theprogramcommitteereceived 106 submissions, from which 36 were selected for presentation. Each submission was reviewed by at least three experts in the relevant research area. We would liketothankalltheauthorsfortakingtheirtimetopreparethesubmissions, and wehopethatthosewhosepapersweredeclinedwillbeableto? ndanalternative forum for their work. We were fortunate to have an energetic team of experts who took on the task of the program committee. Their names may be found overleaf, and we thank them warmly for their time and e?orts. This team was helped by an even larger number of external reviewers who reviewed papers in their particular areas of expertise. A list of these names is also provided, which we hope is complete. We would also like to thank the advisory committee for their advice and s- port. TheexcellentlocalarrangementswerehandledbyDirkBalfanzandJessica Staddon. We made use of the electronic submission and reviewing software s- plied by COSIC at the Katholieke Universiteit Leuven. Both the software and the ISC 2004 website were run on a server at UNC Charlotte, and were perfectly maintained by Seung-Hyun Im. We also appreciate assistance from Lawrence Teo in editing the proceedings.