1. Record Nr. UNINA9910483262903321

Titolo	Information Security Practice and Experience : Second International Conference, ISPEC 2006, Hangzhou, China, April 11-14, 2006, Proceedings / / edited by Kefei Chen, Robert Deng, Xuejia Lai, Jianying Zhou
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-33058-5
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XIV, 392 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 3903
Altri autori (Persone)	ChenKefei <1959->
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Computer networks Operating systems (Computers) Computers and civilization Electronic data processing - Management Information storage and retrieval systems Cryptology Computer Communication Networks Operating Systems Computers and Society IT Operations Information Storage and Retrieval
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	Cryptoanalysis -- DPA-Resistant Finite Field Multipliers and Secure AES Design -- Signed MSB-Set Comb Method for Elliptic Curve Point Multiplication -- Diophantine Approximation Attack on a Fast Public Key Cryptosystem -- Further Security Analysis of XTR -- Network Security I -- A Counting-Based Method for Massive Spam Mail Classification -- Model and Estimation of Worm Propagation Under Network Partition -- Tackling Worm Detection Speed and False Alarm in

Virus Throttling -- Network Security II -- Using Data Field to Analyze Network Intrusions -- Adversarial Organization Modeling for Network Attack/Defense -- A Novel Dynamic Immunization Strategy for Computer Network Epidemics -- Preventing Web-Spoofing with Automatic Detecting Security Indicator -- Security Protocol -- Security Protocol Analysis with Improved Authentication Tests -- A Protocol of Member-Join in a Secret Sharing Scheme -- More on Shared-Scalar-Product Protocols -- Communication Security -- Efficient Public Key Broadcast Encryption Using Identifier of Receivers -- A Practical Clumped-Tree Multicast Encryption Scheme -- Trojan Horse Attack Strategy on Quantum Private Communication -- Signature and Key Agreement -- Linkable Democratic Group Signatures -- Identity-Based Key Agreement with Unilateral Identity Privacy Using Pairings -- Short (Identity-Based) Strong Designated Verifier Signature Schemes -- Identity Based Key Insulated Signature -- Application I -- Design and Implementation of an Extended Reference Monitor for Trusted Operating Systems -- A Design and Implementation of Profile Based Web Application Securing Proxy -- An Efficient and Practical Fingerprint-Based Remote User Authentication Scheme with Smart Cards -- Application II -- Domain-Based Mobile Agent Fault-Tolerance Scheme for Home Network Environments -- Using?-Calculus to Formalize Domain Administration of RBAC -- An Efficient Way to Build Secure Disk -- Practical Forensic Analysis in Advanced Access Content System -- Cryptographic Techniques -- Security Analysis of a Server-Aided RSA Key Generation Protocol -- Integrating Grid with Cryptographic Computing -- Three-Round Secret Handshakes Based on ElGamal and DSA -- System Security -- Securing C Programs by Dynamic Type Checking -- A Chaos-Based Robust Software Watermarking -- Privately Retrieve Data from Large Databases -- An Empirical Study of Quality and Cost Based Security Engineering.

Sommario/riassunto

This volume contains the Research Track proceedings of the Second Information Security Practice and Experience Conference 2006 (ISPEC 2006), which took place in Hangzhou, China, April 11–14, 2006. The inaugural ISPEC 2005 was held exactly one year earlier in Singapore. As applications of information security technologies become pervasive, issues pertaining to their deployment and operations are becoming increasingly imp- tant. ISPEC is an annual conference that brings together researchers and pr- titioners to provide a con?uence of new information security technologies, their applications and their integration with IT systems in various vertical sectors. ISPEC 2006 received 307 submissions. This is probably the highest number of paper submissions in any information security-related technical conferences. Due to this exceptionally large number of submissions and the high quality of the submitted papers, not all the papers that contained innovative ideas could be accepted. Each paper was sent to at least three Program Committee m- bers for comments. Based on the reviewers' comments and discussion by the Program Committee, of the 307 submissions, 35 were selected for inclusion in these proceedings as research track papers and another 21 papers were selected as industrial track papers and are published in the Journal of Shanghai Jiaotong University (Science).