1. Record Nr. UNISA996465741603316

Titolo	Advances in information and computer security : Second International Workshop on Security, IWSEC 2007, Nara, Japan, October 29-31, 2007, proceedings / / Atsuko Miyaji, Hiroaki Kikuchi, Kai Rannenberg (editors)
Pubbl/distr/stampa	Berlin ; ; Heidelberg : , : Springer, , [2007] ©2007
ISBN	3-540-75651-5
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (XIV, 462 p.)
Collana	Lecture notes in computer science ; ; 4752
Disciplina	005.8
Soggetti	Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Software and Multimedia Security -- A Note on the (Im)possibility of Using Obfuscators to Transform Private-Key Encryption into Public-Key Encryption -- Design Issues of an Isolated Sandbox Used to Analyze Malwares -- Collusion-Resistant Fingerprinting Scheme Based on the CDMA-Technique -- Public-Key Cryptography (1) -- Reduction Optimal Trinomials for Efficient Software Implementation of the ? T Pairing -- Experiments on the Linear Algebra Step in the Number Field Sieve -- Batch Pairing Delegation -- Botnet Traffic Detection Techniques by C&C Session Classification Using SVM -- A Global Authentication Scheme for Mobile Ad-Hoc Networks -- An Efficient Pre-authentication Scheme for IEEE 802.11-Based Vehicular Networks -- Intrusion Detection and Identification System Using Data Mining and Forensic Techniques -- Run-Time Randomization to Mitigate Tampering -- Privacy-Preserving Eigentaste-Based Collaborative Filtering -- Secure and Private Incentive-Based Advertisement Dissemination in Mobile Ad Hoc Networks -- Verifiable Internet Voting Solving Secure Platform Problem -- Enforcement of Integrated Security Policy in Trusted Operating Systems -- Salvia: A Privacy-Aware Operating System for Prevention of Data Leakage -- InfoCage: A Development and Evaluation of Confidential File Lifetime Monitoring Technology by Analyzing Events from File Systems and GUIs -- Public-Key Cryptography (2) -- Accredited Symmetrically Private Information Retrieval -- Generic

Certificateless Encryption in the Standard Model -- On Security Models and Compilers for Group Key Exchange Protocols -- Processing Multi-parameter Attacktrees with Estimated Parameter Values -- Practical Security Analysis of E-Voting Systems -- Fine-Grained Sticky Provenance Architecture for Office Documents -- Secure Anonymous Communications with Practical Anonymity Revocation Scheme -- GAS: Overloading a File Sharing Network as an Anonymizing System -- A Composite Privacy Protection Model -- Nominative Signature from Ring Signature -- Anonymous Authentication Protocols with Credit-Based Chargeability and Fair Privacy for Mobile Communications -- How to Find Many Collisions of 3-Pass HAVAL -- A Secure Threshold Anonymous Password-Authenticated Key Exchange Protocol.

Sommario/riassunto

The International Workshop on Security (IWSEC 2007) was the second in the annualseriesthat startedin 2006.IWSEC 2007washeld at the New Public Hall in Nara, Japan, during October 29–31, 2007. This year there were 112 paper submissions, and from these 30 papers were accepted. Accepted papers came from 27 di?erent countries, with the largest proportion coming from Japan (12). Estonia, China, Korea, Spain, Taiwan and the USA contributed 2 papers each and Canada, Germany, Greece, Poland, Turkeyand Vietnam contributed 1 paper each. We would liketo thank all of the authors who submitted papers to IWSEC 2007. The contributed papers were supplemented by one invited talk from the - inent researcher Prof. Doug Tygar (UC Berkeley) in information security. We were fortunate to have an energetic team of experts who formed the Program Committee. Their names may be found overleaf, and we are sincerely grateful for all their great e?orts. This team was supported by an even larger number of individuals who reviewedpapers in their particulararеasof expertise. A list of these names is also provided; we hope it is complete.