1. Record Nr. UNISA996465899803316

Titolo	Advances in Information and Computer Security [[electronic resource]] : First International Workshop on Security, IWSEC 2006, Kyoto, Japan, October 23-24, 2006, Proceedings / / edited by Hiroshi Yoshiura, Kouichi Sakurai, Kai Rannenberg, Yuko Murayama
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-47700-4
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XIII, 438 p.)
Collana	Security and Cryptology ; ; 4266
Disciplina	005.8
Soggetti	Data encryption (Computer science) Operating systems (Computers) Management information systems Computer science Computers and civilization Computer communication systems Algorithms Cryptology Operating Systems Management of Computing and Information Systems Computers and Society Computer Communication Networks Algorithm Analysis and Problem Complexity
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	Signatures (1) -- ID-Based Ring Signature Scheme Secure in the Standard Model -- A Short Verifier-Local Revocation Group Signature Scheme with Backward Unlinkability -- Sound Computational Interpretation of Symbolic Hashes in the Standard Model -- Security Evaluation -- A Requirement Centric Framework for Information Security Evaluation -- A Model-Based Method for Security Configuration Verification -- Personal Computer Privacy: Analysis for

Korean PC Users -- Signatures (2) -- Short Traceable Signatures Based on Bilinear Pairings -- Ring Signature with Designated Linkability -- Ad Hoc Group Signatures -- Rateless Codes for the Multicast Stream Authentication Problem -- Authentication -- Crossing Borders: Security and Privacy Issues of the European e-Passport -- A New Approach to Hide Policy for Automated Trust Negotiation -- Towards Remote Policy Enforcement for Runtime Protection of Mobile Code Using Trusted Computing -- IP Address Authorization for Secure Address Proxying Using Multi-key CGAs and Ring Signatures -- Security for Multimedia -- A Study of Detection Method of Printed Image Alteration Using Digital Watermark -- Real-Time Watermark Embedding for High Resolution Video Watermarking -- Inhibiting Card Sharing Attacks -- Network Security -- A Flooding-Based DoS/DDoS Detecting Algorithm Based on Traffic Measurement and Prediction -- Hardware Stack Design: Towards an Effective Defence Against Frame Pointer Overwrite Attacks -- Modeling of Network Intrusions Based on the Multiple Transition Probability -- Encryption and Key Exchange -- Chosen Ciphertext Security from Identity-Based Encryption Without Strong Condition -- Ciphertext-Auditable Public Key Encryption -- Provably-Secure Two-Round Password-Authenticated Group Key Exchange in the Standard Model -- Cryptanalysis and Implementation -- On the Effectiveness of TMTO and Exhaustive Search Attacks -- Low Power AES Hardware Architecture for Radio Frequency Identification -- The High-Speed Packet Cipher System Suitable for Small Sized Data -- Access Control -- A Tool for Managing Security Policies in Organisations -- Information Flow Query and Verification for Security Policy of Security-Enhanced Linux -- The Complexity of Discretionary Access Control -- Traceroute Based IP Channel for Sending Hidden Short Messages.

Sommario/riassunto

ItwasourpleasuretoholdtheInternationalWorkshoponSecurity2006(IWSEC 2006) this year in Kyoto and to publish the proceedings as a volume of the Lecture Notes in Computer Science series. The workshop was our ? rst trial in that two major academic society groups on security in Japan, viz. ISEC and CSEC, jointly organized it; ISEC is a te- nical group on information security of the Institute of Electronics, Information and Communication Engineers (IEICE), and CSEC is a special interest group on computer security of the Information Processing Society of Japan (IPSJ). It was Ryoichi Sasaki, the former head of CSEC, who proposed holding such an international workshop in Japan for the ?rst time, two years ago. The two groups supported his idea and started organizing the workshop. CSEC has its annual domestic symposium, the Computer Security Symposium (CSS), in - tober for three days, and we decided to organize the workshop prior to CSS this year. The initial aim of the workshop was primarily to provide young researchers with the opportunity to present their work in English. However, due to more submissions than we had anticipated, the quality of the accepted papers became far better than we had expected. Theconferencereceived147submissions, outofwhichtheprogramcommittee selected 30 for presentation. These proceedings contain the ?nal versions of the accepted papers, which the authors ?nalized on the basis of comments from the reviewers. Since these revisions were not subject to editorial review, the authors bear full responsibility for the contents of their papers.