1. Record Nr. UNISA996466170803316

| | |
|---|---|
| Titolo | Information Security Applications [[electronic resource] ] : 4th International Workshop, WISA 2003, Jeju Island, Korea, August 25-27, 2003, Revised Papers / / edited by Kijoon Chae, Moti Yung |
| Pubbl/distr/stampa | Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2004 |
| ISBN | 1-280-30671-8<br>9786610306718<br>3-540-24591-X |
| Edizione | [1st ed. 2004.] |
| Descrizione fisica | 1 online resource (XII, 512 p.) |
| Collana | Lecture Notes in Computer Science, , 1611-3349 ; ; 2908 |
| Disciplina | 005.8 |
| Soggetti | Cryptography<br>Data encryption (Computer science)<br>Computer networks<br>Computers, Special purpose<br>Operating systems (Computers)<br>Algorithms<br>Electronic data processing—Management<br>Cryptology<br>Computer Communication Networks<br>Special Purpose and Application-Based Systems<br>Operating Systems<br>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 at the end of each chapters and index. |
| Nota di contenuto | Network Security -- Model Checking of Security Protocols with Pre-configuration -- Remote Access VPN with Port Protection Function by Mobile Codes -- A Role of DEVS Simulation for Information Assurance -- Mobile Security -- Enhancing Grid Security Infrastructure to Support Mobile Computing Nodes -- Reliable Cascaded Delegation Scheme for Mobile Agent Environments -- Practical Solution for Location Privacy in |

Mobile IPv6 -- Intrusion Detection -- CTAR: Classification Based on Temporal Class-Association Rules for Intrusion Detection -- Viterbi Algorithm for Intrusion Type Identification in Anomaly Detection System -- Towards a Global Security Architecture for Intrusion Detection and Reaction Management -- Internet Security -- Intrusion-Tolerant System Design for Web Server Survivability -- PANA/IKEv2: An Internet Authentication Protocol for Heterogeneous Access -- An Automatic Security Evaluation System for IPv6 Network -- Secure Software, Hardware, and Systems I -- A Location Privacy Protection Mechanism for Smart Space -- Secure System Architecture Based on Dynamic Resource Reallocation -- Fair Exchange with Guardian Angels -- Secure Software, Hardware, and Systems II -- Sign-Based Differential Power Analysis -- Asymmetric Watermarking Scheme Using Permutation Braids -- Low-Power Design of a Functional Unit for Arithmetic in Finite Fields GF(p) and GF(2 m ) -- E-commerce Security -- Efficient Implementation of Relative Bid Privacy in Sealed-Bid Auction -- Multi-dimensional Hash Chain For Sealed-Bid Auction -- An Improved Forward Integrity Protocol for Mobile Agents -- Digital Rights Management -- Taming “Trusted Platforms” by Operating System Design -- A Software Fingerprinting Scheme for Java Using Classfiles Obfuscation -- Reducing Storage at Receivers in SD and LSD Broadcast Encryption Schemes -- Biometrics and Human Interfaces I -- 3D Face Recognition under Pose Varying Environments -- An Empirical Study of Multi-mode Biometric Systems Using Face and Fingerprint -- Fingerprint-Based Authentication for USB Token Systems -- Biometrics and Human Interfaces II -- Iris Recognition System Using Wavelet Packet and Support Vector Machines -- Biometrics Identification and Verification Using Projection-Based Face Recognition System -- Visualization of Dynamic Characteristics in Two-Dimensional Time Series Patterns: An Application to Online Signature Verification -- Public Key Cryptography / Key Management -- E-MHT. An Efficient Protocol for Certificate Status Checking -- A Comment on Group Independent Threshold Sharing -- Automation-Considered Logic of Authentication and Key Distribution -- Applied Cryptography -- The MESH Block Ciphers -- Fast Scalar Multiplication Method Using Change-of-Basis Matrix to Prevent Power Analysis Attacks on Koblitz Curves -- Constructing and Cryptanalysis of a 16 × 16 Binary Matrix as a Diffusion Layer.

Sommario/riassunto

The4thWorkshoponInformationSecurityApplications(WISA2003)wassp-sored by the following Korean organizations and government bodies: the Korea Institute of Information Security and Cryptology (KIISC), the Electronics and TelecommunicationsResearchInstitute(ETRI), andtheMinistryofInformation and Communication (MIC). The workshop was held in Jeju Island, Korea - ring August 25–27, 2003. This international workshop provided ample technical sessions covering a large spectrum of information security applications. Subjects covered included network/mobile security, electronic commerce security, digital rights management, intrusion detection, secure systems and applications, bio- trics and human interfaces, public key cryptography, and applied cryptography. The program committee received 200 papers from 23 countries (representing most geographic areas where security and applied cryptography research is c- ductedthroughouttheworld). Eachsubmittedpaperwaspeer-reviewedbythree program committee members. This year, we had two tracks: long and short p- sentation tracks. We selected 36 papers for the long presentation track and 34 papers for the short presentation tracks. This volume contains revised versions of papers accepted for the long presentation track. We would like to note that getting accepted to both tracks was an achievement to

be proud of, given the competitive nature of WISA this year. Papers in the short presentation track were only published in the WISA preproceedings as preliminary notes; ext-dedversionsofthesenotesmaybepublishedbyfutureconferencesorworkshops.