1. Record Nr. UNINA9910484701903321

Titolo	Autonomic and Trusted Computing : 4th International Conference, ATC 2007, Hong Kong, China, July 11-13, 2007, Proceedings / / edited by Bin Xiao, Laurence T. Yang, Christian Muller-Schloer, Yu Hua
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2007
ISBN	3-540-73547-X
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (XVIII, 574 p.)
Collana	Programming and Software Engineering, , 2945-9168 ; ; 4610
Disciplina	005.8
Soggetti	Computer science Data protection Software engineering Computer networks Cryptography Data encryption (Computer science) Application software Theory of Computation Data and Information Security Software Engineering Computer Communication Networks Cryptology Computer and Information Systems Applications
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	International conference proceedings.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Keynote Speech -- An Intelligent Home System as a Development and Test Platform for Ubiquitous Computing -- Remarks on Self-organization and Trust in Organic Computing Systems -- Cryptography and Signatures -- ZigBee Security Using Identity-Based Cryptography -- Efficient Identity-Based Signcryption Scheme for Multiple Receivers -- Identity-Based Proxy Signature from Pairings -- Cryptanalysis of BGW Broadcast Encryption Schemes for DVD Content Protection -- A Digital Signature Mechanism and Authentication Scheme for Group

Communication in Grid -- Cryptanalysis of Server-Aided RSA Key Generation Protocols at MADNES 2005 -- Autonomic Computing and Services -- Service-Context Knowledge-Based Solution for Autonomic Adaptation -- Middleware Based Context Management for the Component-Based Pervasive Computing -- Building Autonomic and Secure Service Oriented Architectures with MAWeS -- Biology as Inspiration Towards a Novel Service Life-Cycle -- Design of Service–Based Systems with Adaptive Tradeoff Between Security and Service Delay -- Secure and Trusted Computing -- Provably Secure Identity-Based Threshold Unsigncryption Scheme -- Final Fantasy – Securing On-Line Gaming with Trusted Computing -- An Efficient and Secure Rights Sharing Method for DRM System Against Replay Attack -- Establishing Trust Between Mail Servers to Improve Spam Filtering -- Autonomic Models and Architectures -- An Architecture for Self-healing Autonomous Object Groups -- A Generic and Modular System Architecture for Trustworthy, Autonomous Applications -- Cooperative Component Testing Architecture in Collaborating Network Environment -- An Approach to a Trustworthy System Architecture Using Virtualization -- Trusted Models and Systems -- CuboidTrust: A Global Reputation-Based Trust Model in Peer-to-Peer Networks -- A TrustEvolution Model for P2P Networks -- An Adaptive Trust Control Model for a Trustworthy Component Software Platform -- Towards Trustworthy Resource Selection: A Fuzzy Reputation Aggregation Approach -- Intrusion Detection -- An Adaptive Spreading Activation Approach to Combating the Front-Peer Attack in Trust and Reputation System -- Research on Cost-Sensitive Learning in One-Class Anomaly Detection Algorithms -- Improved and Trustworthy Detection Scheme with Low Complexity in VBLAST System -- Stepping-Stone Detection Via Request-Response Traffic Analysis -- SPA Countermeasure Based on Unsigned Left-to-Right Recodings -- Access Control -- A New One-Way Isolation File-Access Method at the Granularity of a Disk-Block -- Novel Remote User Authentication Scheme Using Bilinear Pairings -- On the Homonymous Role in Role-Based Discretionary Access Control -- Ontology Based Hybrid Access Control for Automatic Interoperation -- Recoverable Tamper Proofing Technique for Image Authentication Using Irregular Sampling Coding -- Trusted Computing and Communications -- A Decomposition Strategy Based Trusted Computing Method for Cooperative Control Problem Faced with Communication Constraints -- Formal Analysis of Secure Bootstrap in Trusted Computing -- Calculating Trust Using Aggregation Rules in Social Networks -- Enhancing Grid Security Using Trusted Virtualization -- A Wearable System for Outdoor Running Workout State Recognition and Course Provision -- Key Management -- Malicious Participants in Group Key Exchange: Key Control and Contributiveness in the Shadow of Trust -- Efficient Implementation of the Keyed-Hash Message Authentication Code Based on SHA-1 Algorithm for Mobile Trusted Computing -- A Secure DRM Framework for User's Domain and Key Management -- A Secret-Key Exponential Key AgreementProtocol with Smart Cards -- Key Establishment Scheme for Sensor Networks with Low Communication Cost -- Worm Detection and Data Security -- A Worm Containment Model Based on Neighbor-Alarm -- A Distributed Self-healing Data Store -- Malicious Codes Detection Based on Ensemble Learning -- Generating Simplified Regular Expression Signatures for Polymorphic Worms -- Secured Services and Applications -- AAA for Spontaneous Roaming Agreements in Heterogeneous Wireless Networks -- A Prediction-Based Fair Replication Algorithm in Structured P2P Systems -- TransCom: A Virtual Disk Based Self-management System -- Defending Against Jamming Attacks in Wireless

	Local Area Networks -- Fault-Tolerant Systems -- Schedulability Analysis of the Fault-Tolerant Hard Real-Time Tasks with Limited Priority Levels -- A Property-Based Technique for Tolerating Faults in Bloom Filters for Deep Packet Inspection -- A Fuzzy Logic Approach for Secure and Fault Tolerant Grid Job Scheduling -- An Enhanced DGIDE Platform for Intrusion Detection.
Sommario/riassunto	No fewer than 55 revised full papers are presented in this volume, all given at the 4th International Conference on Autonomic and Trusted Computing, held in Hong Kong, China in July 2007. The papers, presented together with one keynote lecture, were carefully reviewed and selected from 223 submissions. The papers are organized in topical sections on, among others, cryptography and signatures, autonomic computing and services, and secure and trusted computing.