1. Record Nr. UNISA996465788903316

Titolo	Trusted Systems [[electronic resource]] : First International Conference, INTRUST 2009, Beijing, China, December 17-19, 2009. Proceedings / / edited by Liqun Chen, Moti Yung
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010
ISBN	1-280-38811-0 9786613566034 3-642-14597-3
Edizione	[1st ed. 2010.]
Descrizione fisica	1 online resource (XIV, 263 p. 64 illus.)
Collana	Security and Cryptology ; ; 6163
Disciplina	005.8
Soggetti	Computer science Computer networks Cryptography Data encryption (Computer science) Electronic data processing—Management Algorithms Computers and civilization Theory of Computation Computer Communication Networks Cryptology IT Operations Computers and Society
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	Invited Talk -- On Design of a Trusted Software Base with Support of TPCM -- Secure Storage -- External Authenticated Non-volatile Memory with Lifecycle Management for State Protection in Trusted Computing -- A Method for Safekeeping Cryptographic Keys from Memory Disclosure Attacks -- Attestation -- Remote Attestation on Function Execution (Work-in-Progress) -- Scalable Remote Attestation with Privacy Protection -- Anonymous Credentials for Java Enabled

Platforms: A Performance Evaluation -- Trusted Network -- SocialClouds: Concept, Security Architecture and Some Mechanisms -- Privacy Enhanced Trusted Network Connect -- Research on Multistage Interconnection Architecture and Collision Detection Model -- Virtualization -- Trusted Virtual Domains – Design, Implementation and Lessons Learned -- Trusted Integrity Measurement and Reporting for Virtualized Platforms -- Applications -- A Feather-Weight Application Isolation Model -- Exploring Trust of Mobile Applications Based on User Behaviors -- Trusted Firmware Services Based on TPM -- Supporting Technology -- Improved Cryptanalysis of the FOX Block Cipher -- Bitwise Higher Order Differential Cryptanalysis.

Sommario/riassunto

This volume contains the 16 papers presented at the INTRUST 2009 conf- ence, held in Beijing, China in December 2009. INTRUST 2009 was the ?rst international conference on the theory, technologies and applications of trusted systems. It was devoted to all aspects of trusted computing systems, incl- ing trusted modules, platforms, networks, services and applications, from their fundamental features and functionalities to design principles, architecture and implementation technologies. The goal of the conference was to bring academic and industrial researchers, designers and implementers together with end-users of trusted systems, in order to foster the exchange of ideas in this challenging and fruitful area. The program consisted of 3 invited talks and 20 contributed papers. The - vited speakerswere Wenchang Shi (Renmin Universityof China), DavidWooten (Microsoft) and Scott Rotondo (Sun Microsystems). The ?rst speaker provided a paper, which is included in these proceedings. Special thanks are due to these speakers. The contributed talks were arranged with two main tracks, one devoted to academic aspects of trusted computing systems (addressed by these proce- ings), and the other devoted to industrial aspects. The contributed papers were selected out of 42 submissions from 13 countries. The refereeing process was rigorous, involving at least three (and mostly more) independent reports being prepared for each submission. We are very grateful to our hard-working and distinguished Program Committee for doing such an excellent job in a timely fashion.