1.	Record Nr.	UNISA996465682303316
	Titolo	Trusted Systems [[electronic resource]] : Second International Conference, INTRUST 2010, Beijing, China, December 13-15, 2010, Revised Selected Papers / / edited by Liqun Chen, Moti Yung
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2011
	ISBN	3-642-25283-4
	Edizione	[1st ed. 2011.]
	Descrizione fisica	1 online resource (XIV, 362 p. 73 illus.)
	Collana	Security and Cryptology ; ; 6802
	Disciplina	004
	Soggetti	Computer networks Cryptography Data encryption (Computer science) Electronic data processing—Management Algorithms Computers and civilization Data protection Computer Communication Networks Cryptology IT Operations Computers and Society Data and Information Security
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Includes index.
	Nota di contenuto	Intro -- Title -- Preface -- Table of Contents -- Implementation Technology -- Seamless Integration of Trusted Computing into Standard Cryptographic Frameworks -- Introduction -- Related Work -- Our Contribution and Background -- Architecture Overview -- Comparison to Classic TCG Trusted Software Stacks -- Connection and Context Setup -- Using the doTSS Client API -- System Implementation -- Server Architecture -- Client Architecture -- Client/Server Communication Protocol -- doTSS on Embedded Systems -- Conclusion and Future Work -- References -- Design and

Implementation of Document Access Control Model Based on Role and Security Policy -- Introduction -- Background and Motivation -- Previous Works -- Challenging Issues -- Our Contributions -- XACML-RBAC Framework -- Document Access Control Model -- Security Requirements of Model -- Security Policy of the Model -- Static Security Rules -- Dynamic Security Rules -- Information Flow Analysis -- Document Access Control System -- Implementation -- Evaluation -- Conclusion and Future Work -- References -- Towards High-Performance IPsec on Cavium OCTEON Platform -- Introduction -- Background -- Cavium OCTEON -- Run-to-Completion vs Pipeline -- IPsec -- Encrypting Algorithms -- IPsec Implementation -- OUTBOUND Design -- INBOUND Design -- Performance Evaluation -- Development Platform and Test Environments -- Experiment on Different Encryption Algorithms and Packet Length -- Experiment on Different Core Numbers -- Experiment on Pipeline and Run-to-Completion Mechanism -- Conclusion -- References -- Security Analysis -- An Abstract Model of a Trusted Platform -- Introduction -- Trusted Computing -- Trusted Platforms -- The Need for Reasoning about Platform Properties -- A CSP Primer -- Why CSP -- An Abstract Model -- Runtime System -- Resources -- Applications -- Platform Configurations.

Platform Instantiation and Property Verification -- Initial Memory Contents -- Component Location Configuration -- Application Logic -- Property Specification and Verification -- Case Study: Cooper's Trusted Grid Platform -- Property Specification -- Common Setup -- Instantiating a Malicious Platform -- Instantiating a Non-malicious Platform -- Property Verification, Results and Discussion -- Performance Results -- Observations -- Application Specification -- Extending Configurations -- State Space Reduction -- Performance and Scalability of the Model -- Related Work -- Conclusion and Future Work -- References -- Modeling TCG-Based Secure Systems with Colored Petri Nets -- Introduction -- Preliminaries -- Trusted Computing -- Colored Petri Nets -- Modeling TCG-Based Secure Systems with CPN -- Basic Model -- Process Management -- Synchronous I/O -- Data Management -- Late Launch -- Case Studies -- Memory Protection in TrustVisor -- Remote Attestation Based on Dynamic Root of Trust -- Related Work -- Secure Systems Based on Trusted Computing -- CPN Based Formal Studies -- Formal Verification on Trusted Computing -- Conclusion -- References -- Information Flow Graph: An Approach to Identifying Covert Storage Channels -- Introduction -- The Information Flow Graph Approach -- Graph Notation and Semantics -- Constructing An Information Flow Graph -- Pruning the Information Flow Graph -- Searching for Information Flow Paths -- Analyzing Operation Sequences -- Example Analyses Using Information Flow Graph -- A Brief Description of the File System Example -- Example Information Flow Graph and Scenario List for File System Example -- Comparison of IFG, CFT and SRM Analyses for the File System Example -- Comparison among SRM, CFT and IFG -- Conclusion and Future Work -- References -- Trusted Subjects Configuration Based on TE Model in MLS Systems.

Introduction -- Related Works -- Trusted Subjects Configuration -- Notation for Trusted Subject -- Information Flow Graph -- MLS Policy Information Flow Graph -- Type Enforcement Policy and Entity Information Flow Graph -- Determine the Trusted Subjects -- Security Label Range of Trusted Subjects -- Risk Information Flow Graph -- Risk of Trusted Subjects -- Risk Security -- The Assurance Requirements of Trusted Subjects -- Conclusions -- References -- Cryptographic Aspects (I) -- Key Exchange with Anonymous Authentication Using

Registration -- Login -- Password Change -- Implementation -- Security Considerations -- Related Work -- Conclusion and Future Work -- References -- A Game Theory-Based Surveillance Mechanism against Suspicious Insiders in MANETs -- Introduction -- Background and Motivation -- Related Works -- Challenging Issues -- Our Contributions -- Threat Analysis -- Reputation Mechanism -- Misbehavior Prediction -- Surveillance Game -- Multilevel Surveillance -- Reward and Punishment Scheme -- Surveillance Game Model -- Game Solutions -- Decision Making -- Case Study -- Conclusion -- References -- Hardware Security -- Hardware Trojans for Inducing or Amplifying Side-Channel Leakage of Cryptographic Software -- Introduction -- Preliminaries and Related Work -- Bug Attacks -- Micro-Architectural Side-Channels -- Fault Attacks -- Activation Mechanisms -- Method 1: Snooping the Data Bus -- Method 2: Snooping Operands of Instructions -- Effects of the Trojan -- Fault Induction -- Timing Variation -- Variation of Power Consumption -- Case Studies -- Attacking AES -- Attacking RSA -- Conclusions -- References -- An Emerging Threat: Eve Meets a Robot -- Introduction -- What is a Robot? -- Security of Robotics -- A Simple Active Attack and a Countermeasure -- Active Attacks on Robots.
Information Leakage Attacks on Robots.

Sommario/riassunto

This book constitutes the thoroughly refereed post-conference proceedings of the International Conference on Trusted Systems, INTRUST 2010, held in Beijing, China, in December 2010. The 23 revised full papers were carefully reviewd and selected from 66 submissions for inclusion in the book. The papers are organized in seven topical sections on implementation technology, security analysis, cryptographic aspects, mobile trusted systems, hardware security, attestation, and software protection.

2.	Record Nr.	UNICAMPANIAVAN0068346
	Titolo	Le radici della bioetica 2 / a cura di Elio Sgreccia, Vincenza Mele, Dario Sacchini
	Pubbl/distr/stampa	Milano, : Vita e pensiero, 1998
	ISBN	88-343-8270-6
	Descrizione fisica	xi, 384 p. ; 22 cm.
	Lingua di pubblicazione	Italiano
	Formato	Materiale a stampa
	Livello bibliografico	Monografia