1. Record Nr. UNINA9910483214003321

Titolo	Information and Communications Security : 11th International Conference, ICICS 2009 / / edited by Sihan Qing, Chris J. Mitchell, Guilin Wang
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
ISBN	1-280-38340-2 9786613561329 3-642-11145-9
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XIV, 504 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 5927
Classificazione	DAT 461f DAT 465f SS 4800
Altri autori (Persone)	QingSihan MitchellChris WangGuilin, Dr.
Disciplina	004n/a
Soggetti	Cryptography Data encryption (Computer science) Computer networks Computer programming Data structures (Computer science) Information theory Coding theory Data protection Cryptology Computer Communication Networks Programming Techniques Data Structures and Information Theory Coding and Information Theory Data and Information Security
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 Talks -- How to Steal a Botnet and What Can Happen When You Do -- A User-Mode-Kernel-Mode Co-operative Architecture for Trustable Computing -- Cryptanalysis -- Security Evaluation of a DPA-Resistant S-Box Based on the Fourier Transform -- Security Analysis of the GF-NLFSR Structure and Four-Cell Block Cipher -- Algorithms and Implementations -- The rakaposhi Stream Cipher -- Design of Reliable and Secure Multipliers by Multilinear Arithmetic Codes -- Hardware/Software Co-design of Public-Key Cryptography for SSL Protocol Execution in Embedded Systems -- Public Key Cryptography -- Online/Offline Ring Signature Scheme -- Policy-Controlled Signatures -- Public Key Encryption without Random Oracle Made Truly Practical -- A Public-Key Traitor Tracing Scheme with an Optimal Transmission Rate -- Security Applications -- Computationally Secure Hierarchical Self-healing Key Distribution for Heterogeneous Wireless Sensor Networks -- Enabling Secure Secret Updating for Unidirectional Key Distribution in RFID-Enabled Supply Chains -- Biometric-Based Non-transferable Anonymous Credentials -- Software Security -- Secure Remote Execution of Sequential Computations -- Architecture- and OS-Independent Binary-Level Dynamic Test Generation -- System Security -- Measuring Information Flow in Reactive Processes -- Trusted Isolation Environment: An Attestation Architecture with Usage Control Model -- Denial-of-Service Attacks on Host-Based Generic Unpackers -- Network Security -- Predictive Pattern Matching for Scalable Network Intrusion Detection -- Deterministic Finite Automata Characterization for Memory-Based Pattern Matching -- A LoSS Based On-line Detection of Abnormal Traffic Using Dynamic Detection Threshold -- User-Assisted Host-Based Detection of Outbound Malware Traffic -- Assessing Security Risk to a Network Using a Statistical Model of Attacker Community Competence -- Short Papers I -- Using the (Open) Solaris Service Management Facility as a Building Block for System Security -- IntFinder: Automatically Detecting Integer Bugs in x86 Binary Program -- A Comparative Study of Privacy Mechanisms and a Novel Privacy Mechanism [Short Paper] -- Database Security -- Collusion-Resistant Protocol for Privacy-Preserving Distributed Association Rules Mining -- GUC-Secure Join Operator in Distributed Relational Database -- Trust Management -- TSM-Trust: A Time-Cognition Based Computational Model for Trust Dynamics -- Bring Efficient Connotation Expressible Policies to Trust Management -- A User Trust-Based Collaborative Filtering Recommendation Algorithm -- Applied Cryptography -- Fingerprinting Attack on the Tor Anonymity System -- Proactive Verifiable Linear Integer Secret Sharing Scheme -- A Multi-stage Secret Sharing Scheme Using All-or-Nothing Transform Approach -- Digital Audio Watermarking Technique Using Pseudo-Zernike Moments -- Short Papers II -- An Image Sanitizing Scheme Using Digital Watermarking -- Adaptive and Composable Oblivious Transfer Protocols (Short Paper) -- Discrete-Log-Based Additively Homomorphic Encryption and Secure WSN Data Aggregation.

Sommario/riassunto

This book constitutes the refereed proceedings of the 11th International Conference on Information and Communications Security, ICICS 2009, held in Beijing, China, in December 2009. The 37 revised full papers presented together with one invited paper were carefully reviewed and selected from 162 submissions. The papers are organized in topical sections on cryptanalysis, algorithms and implemantations, public key cryptography, security applications, software security, system security, network security, database security, trust management, and applied cryptography.