1. Record Nr. UNINA9910484221703321

Titolo	Information and Communications Security : 12th International Conference, ICICS 2010, Barcelona, Spain, December 15-17, 2010 Proceedings / / edited by Miguel Soriano, Sihan Qing, Javier López
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010
ISBN	1-280-39076-X 9786613568687 3-642-17650-X
Edizione	[1st ed. 2010.]
Descrizione fisica	1 online resource (XIV, 474 p. 120 illus.)
Collana	Security and Cryptology, , 2946-1863 ; ; 6476
Altri autori (Persone)	SorianoMiguel QingSihan LopezJavier
Disciplina	005.8
Soggetti	Data protection Cryptography Data encryption (Computer science) Data structures (Computer science) Information theory Coding theory Algorithms Computer networks Data and Information Security Cryptology Data Structures and Information Theory Coding and Information Theory Computer Communication Networks
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	Cryptographic Hash Functions: Theory and Practice -- Cryptographic Hash Functions: Theory and Practice -- Session 1A. Access Control -- Rewriting of SPARQL/Update Queries for Securing Data Access -- Fine-

Grained Disclosure of Access Policies -- Session 1B. Public Key Cryptography and Cryptanalysis -- Manger's Attack Revisited -- Horizontal Correlation Analysis on Exponentiation -- Threshold Public-Key Encryption with Adaptive Security and Short Ciphertexts -- Session 1C. Security in Distributed and Mobile Systems -- A Trust-Based Robust and Efficient Searching Scheme for Peer-to-Peer Networks -- CUDACS: Securing the Cloud with CUDA-Enabled Secure Virtualization -- SEIP: Simple and Efficient Integrity Protection for Open Mobile Platforms -- Securing Mobile Access in Ubiquitous Networking via Non-roaming Agreement Protocol -- Compromise-Resilient Anti-jamming for Wireless Sensor Networks -- Session 1D. Cryptanalysis -- On Practical Second-Order Power Analysis Attacks for Block Ciphers -- Consecutive S-box Lookups: A Timing Attack on SNOW 3G -- Session 2A. Authentication -- Efficient Authentication for Mobile and Pervasive Computing -- Security Enhancement and Modular Treatment towards Authenticated Key Exchange -- Federated Secret Handshakes with Support for Revocation -- Session 2B. Fair Exchange Protocols -- An Agent-Mediated Fair Exchange Protocol -- A New Method for Formalizing Optimistic Fair Exchange Protocols -- Unconditionally Secure First-Price Auction Protocols Using a Multicomponent Commitment Scheme -- Session 2C. Anonymity and Privacy -- Proving Coercion-Resistance of Scantegrity II -- Anonymity and Verifiability in Voting: Understanding (Un)Linkability -- A Secure and Practical Approach for Providing Anonymity Protection for Trusted Platforms -- Time Warp: How Time Affects Privacy in LBSs -- Session 2D. Software Security -- Return-Oriented Rootkit without Returns (on the x86) -- Experimental Threat Model Reuse with Misuse Case Diagrams -- Automatically Generating Patch in Binary ProgramsUsing Attribute-Based Taint Analysis -- Session 3A. Proxy Cryptosystems -- Identity-Based Proxy Cryptosystems with Revocability and Hierarchical Confidentialities -- Ciphertext Policy Attribute-Based Proxy Re-encryption -- Session 3B. Intrusion Detection Systems -- Hybrid Detection of Application Layer Attacks Using Markov Models for Normality and Attacks -- A Trust-Based IDS for the AODV Protocol -- IDS Alert Visualization and Monitoring through Heuristic Host Selection -- A Two-Tier System for Web Attack Detection Using Linear Discriminant Method.

Sommario/riassunto

Information and communication security must provide technological solutions to the tension between the accelerating growth of social, economical and g- ernmental demand for digitalization of information on the one hand, and on the other, the legal and ethical obligation to protect the individuals and organi- tions involved. These proceedings contain the papers accepted at the 2010 International Conference on Information and Communications Security (ICICS 2010), held in Barcelona, Spain, during December 15-17, and hosted by the Information Security Group of the Universitat Polit` ecnica de Catalunya, UPC. ICICS2010wasthe12theventintheICICSconferenceseries, startedin1997, which brought together leading researchers and engineers involved in multiple disciplines of information and communications security, to foster the exchange of ideas in aspects including, but not limited to, authentication and authori- tion, distributed and mobile systems security, e-commerce, fraud control, int- lectual property protection, operating system security, anonymity and privacy, and trusted computing. Inresponsetothecallforpapers, 135submissionswerereceivedforthisyear's installment of the conference series. Each paper received at least three pe- reviews on the basis of its signi'cance, novelty, technical quality and relevance to this event.The highly competitive selectionprocessresultedinonly31 papers being

accepted, subject to a ?nal revision before publication. ICICS 2010 was held under the sponsorshipof the Spanish governmentand a number of private companies, particularly Scytl, which we would like to thank.