1. Record Nr. UNISA996466306003316

Titolo	Network and System Security [[electronic resource]] : 7th International Conference, NSS 2013, Madrid, Spain, June 3-4, 2013, Proceedings / / edited by Javier Lopez, Xinyi Huang, Ravi Sandhu
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
ISBN	3-642-38631-8
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (XX, 793 p. 207 illus.)
Collana	Security and Cryptology ; ; 7873
Disciplina	005.8
Soggetti	Computer security Computer communication systems Data encryption (Computer science) Management information systems Computer science E-commerce Systems and Data Security Computer Communication Networks Cryptology Management of Computing and Information Systems e-Commerce/e-business
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Stochastic Traffic Identification for Security Management: eDonkey Protocol as a Case Study -- A Technology Independent Security Gateway for Real-Time Multimedia Communication -- Efficient Attribute Based Access Control Mechanism for Vehicular Ad Hoc Network -- Evaluation of Detecting Malicious Nodes Using Bayesian Model in Wireless Intrusion Detection -- Model the Influence of Sybil Nodes in P2P Botnets -- Network Security: Security Protocols and Practice A Novel Security Protocol for Resolving Addresses in the Location/ID Split Architecture -- The OffPAD: Requirements and Usage -- Information-Oriented Trustworthiness Evaluation in Vehicular Ad-hoc Networks -- Using Trusted Platform Modules for Location

Assurance in Cloud Networking -- Network Security: Network Attacks and Defense Tracing Sources of Anonymous Slow Suspicious Activities -- Static Analysis for Regular Expression Denial-of-Service Attacks -- Next-Generation DoS at the Higher Layers: A Study of SMTP Flooding -- Towards Hybrid Honeynets via Virtual Machine Introspection and Cloning -- System Security: Malware and Intrusions MADS: Malicious Android Applications Detection through String Analysis -- X-TIER: Kernel Module Injection -- Leveraging String Kernels for Malware Detection -- Insiders Trapped in the Mirror Reveal Themselves in Social Media -- System Security: Applications Security On Business Logic Vulnerabilities Hunting: The APP LogGIC Framework -- Using the Smart Card Web Server in Secure Branchless Banking -- Liability for Data Breaches: A Proposal for a Revenue-Based Sanctioning Approach -- Efficient and Private Three-Party Publish/Subscribe -- System Security: Security Algorithms and Systems Marlin: A Fine Grained Randomization Approach to Defend against ROP Attacks -- Mobile Trusted Agent (MTA): Build User-Based Trust for General-Purpose Computer Platform -- Anomaly Detection for Ephemeral Cloud IaaS Virtual Machines -- JShadObf: A JavaScript Obfuscator Based on Multi-Objective Optimization Algorithms -- Forward Secure Certificateless Proxy Signature Scheme -- Leakage-Resilient Zero-Knowledge Proofs of Knowledge for NP -- On the Security of an Efficient Attribute-Based Signature -- Factoring RSA Modulus with Known Bits from Both p and q: A Lattice Method -- Performance Prediction Model for Block Ciphers on GPU Architectures -- Threshold-Oriented Optimistic Fair Exchange -- Secure Storage and Fuzzy Query over Encrypted Databases -- A Highly Efficient RFID Distance Bounding Protocol without Real-Time PRF Evaluation -- Privacy Preserving Context Aware Publish Subscribe Systems -- A New Unpredictability-Based RFID Privacy Model -- Privacy-Preserving Multi-party Reconciliation Using Fully Homomorphic Encryption -- Privacy-Preserving Password-Based Authenticated Key Exchange in the Three-Party Setting -- Key Agreement and Distribution Light Weight Network Coding Based Key Distribution Scheme for MANETs -- Identity-Based Dynamic Authenticated Group Key Agreement Protocol for Space Information Network -- Authentication and Key Agreement Based on Hyper-sphere Using Smart Cards -- An Efficient Constant Round ID-Based Group Key Agreement Protocol for Ad Hoc Networks -- Human Identification with Electroencephalogram (EEG) for the Future Network Security -- Building Better Unsupervised Anomaly Detector with S-Transform -- Fault-Tolerant Topology Control Based on Artificial Immune in WMNs -- Virtually Reconfigurable Secure Wireless Networks Using Broadcast Tokens -- On the Use of Key Assignment Schemes in Authentication Protocols -- On the Interactions between Privacy-Preserving, Incentive, and Inference Mechanisms in Participatory Sensing Systems -- Security Authentication of AODV Protocols in MANETs -- Architecture for Trapping Toll Fraud Attacks Using a VoIP Honeynet Approach -- Towards a Privacy-Preserving Solution for OSNs -- Measuring and Comparing the Protection Quality in Different Operating Systems -- Collusion-Resistant Domain-Specific Pseudonymous Signatures -- On the Applicability of Time-Driven Cache Attacks on Mobile Devices -- Ancestor Excludable Hierarchical ID-Based Encryption Revisited -- Think Twice before You Share: Analyzing Privacy Leakage under Privacy Control in Online Social Networks -- A Dynamic and Multi-layer Reputation Computation Model for Multi-hop Wireless Networks -- Distributed and Anonymous Publish-Subscribe -- Enhancing Passive Side-Channel Attack Resilience through Schedulability Analysis of Data-Dependency Graphs -- Combining Dynamic Passive Analysis and Active Fingerprinting for

Effective Bot Malware Detection in Virtualized Environments -- Filtering Trolling Comments through Collective Classification -- Security Analysis of Touch Inputted Passwords: A Preliminary Study Based on the Resistance against Brute Force Attacks -- A Pairing-Free Identity Based Authentication Framework for Cloud Computing -- Formal Modeling and Automatic Security Analysis of Two-Factor and Two-Channel Authentication Protocols -- Towards a More Secure Apache Hadoop HDFS Infrastructure: Anatomy of a Targeted Advanced Persistent Threat against HDFS and Analysis of Trusted Computing Based Countermeasures -- A Formally Verified Initial Authentication and Key Agreement Protocol in Heterogeneous Environments Using Casper/FDR -- A Comprehensive Access Control System for Scientific Applications -- Partial Fingerprint Reconstruction with Improved Smooth Extension -- Modeling and Analysis for Thwarting Worm Propagation in Email Networks -- On Secure and Power-Efficient RFID-Based Wireless Body Area Network -- Towards Authenticated Objects -- A Finger-Vein Based Cancellable Bio-cryptosystem.

Sommario/riassunto

This book constitutes the proceedings of the 7th International Conference on Network and System Security, NSS 2013, held in Madrid, Spain, in June 2013. The 41 full papers presented were carefully reviewed and selected from 176 submissions. The volume also includes 7 short papers and 13 industrial track papers. The paper are organized in topical sections on network security (including: modeling and evaluation; security protocols and practice; network attacks and defense) and system security (including: malware and intrusions; applications security; security algorithms and systems; cryptographic algorithms; privacy; key agreement and distribution).