1. Record Nr. UNINA9910482961603321

Titolo	Computer Security - ESORICS 2008 : 13th European Symposium on Research in Computer Security, Málaga, Spain, October 6-8, 2008. Proceedings / / edited by Sushil Jajodia
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2008
ISBN	3-540-88313-4
Edizione	[1st ed. 2008.]
Descrizione fisica	1 online resource (XIV, 602 p.)
Collana	Security and Cryptology ; ; 5283
Classificazione	54.30
Disciplina	005.8
Soggetti	Data encryption (Computer science) Seguridad informática Computer communication systems Computer software—Reusability E-commerce Management information systems Computer science Cryptology Theory of Computation Computer Communication Networks Performance and Reliability e-Commerce/e-business Management of Computing and Information Systems
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	Session 1: Intrusion Detection and Network Vulnerability Analysis -- Multiprimary Support for the Availability of Cluster-Based Stateful Firewalls Using FT-FW -- Identifying Critical Attack Assets in Dependency Attack Graphs -- Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory -- Session 2: Network Security -- Strongly-Resilient and Non-interactive Hierarchical Key-Agreement in MANETs -- Efficient Handling of Adversary Attacks in Aggregation Applications -- Symmetric Key Approaches to Securing BGP – A Little

Bit Trust Is Enough -- Session 3: Smart Cards and Identity Management -- Dismantling MIFARE Classic -- A Browser-Based Kerberos Authentication Scheme -- CROO: A Universal Infrastructure and Protocol to Detect Identity Fraud -- Session 4: Data and Applications Security -- Disclosure Analysis and Control in Statistical Databases -- TRACE: Zero-Down-Time Database Damage Tracking, Quarantine, and Cleansing with Negligible Run-Time Overhead -- Access Control Friendly Query Verification for Outsourced Data Publishing -- Session 5: Privacy Enhancing Technologies -- Sharemind: A Framework for Fast Privacy-Preserving Computations -- Modeling Privacy Insurance Contracts and Their Utilization in Risk Management for ICT Firms -- Remote Integrity Check with Dishonest Storage Server -- Session 6: Anonymity and RFID Privacy -- A Low-Variance Random-Walk Procedure to Provide Anonymity in Overlay Networks -- RFID Privacy Models Revisited -- A New Formal Proof Model for RFID Location Privacy -- Session 7: Access Control and Trust Negotiation -- Distributed Authorization by Multiparty Trust Negotiation -- Compositional Refinement of Policies in UML – Exemplified for Access Control -- On the Security of Delegation in Access Control Systems -- Session 8: Information Flow and Non-transferability -- Termination-Insensitive Noninterference Leaks More Than Just a Bit -- Security Provisioning in Pervasive Environments Using Multi-objective Optimization -- Improved Security Notions and Protocols for Non-transferable Identification -- Session 9: Secure Electronic Voting and Web Applications Security -- Human Readable Paper Verification of Prêt à Voter -- A Distributed Implementation of the Certified Information Access Service -- Exploring User Reactions to New Browser Cues for Extended Validation Certificates -- A Framework for the Analysis of Mix-Based Steganographic File Systems -- Session 10: VoIP Security, Malware, and DRM -- An Adaptive Policy-Based Approach to SPIT Management -- Structured Peer-to-Peer Overlay Networks: Ideal Botnets Command and Control Infrastructures? -- Eureka: A Framework for Enabling Static Malware Analysis -- New Considerations about the Correct Design of Turbo Fingerprinting Codes -- Session 11: Formal Models and Cryptographic Protocols -- Formally Bounding the Side-Channel Leakage in Unknown-Message Attacks -- Cryptographic Protocol Explication and End-Point Projection -- State Space Reduction in the Maude-NRL Protocol Analyzer -- Session 12: Language-Based and Hardware Security -- Code-Carrying Authorization -- CPU Bugs, CPU Backdoors and Consequences on Security.

Sommario/riassunto

This book constitutes the refereed proceedings of the 13th European Symposium on Research in Computer Security, ESORICS 2008, held in Torremolinos, Spain, in October 2008. The 37 revised full papers presented were carefully reviewed and selected from 168 submissions. The papers are organized in topical sections on Intrusion Detection and Network Vulnerability Analysis; Network Security; Smart Cards and Identity management; Data and Applications Security; Privacy Enhancing Technologies; Anonymity and RFID Privacy; Access Control and Trust Negotiation; Information Flow and Non-transferability; Secure Electronic Voting and Web Applications Security; VoIP Security, Malware, and DRM; Formal Models and Cryptographic Protocols; Language-based and Hardware Security.