1. Record Nr. UNISA996465663603316

Titolo	Computer Security -- ESORICS 2009 [[electronic resource]] : 14th European Symposium on Research in Computer Security, Saint-Malo, France, September 21-23, 2009, Proceedings / / edited by Michael Backes, Peng Ning
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
ISBN	3-642-04444-1
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XVI, 706 p.)
Collana	Security and Cryptology ; ; 5789
Disciplina	005.822gerDNB
Soggetti	Computer security Data encryption (Computer science) Coding theory Information theory Data structures (Computer science) Computer science—Mathematics E-commerce Systems and Data Security Cryptology Coding and Information Theory Data Structures and Information Theory Discrete Mathematics in Computer Science 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 bibliografia	Includes bibliographical references and index.
Nota di contenuto	Network Security I -- Learning More about the Underground Economy: A Case-Study of Keyloggers and Dropzones -- User-Centric Handling of Identity Agent Compromise -- The Coremelt Attack -- Type-Based Analysis of PIN Processing APIs -- Declassification with Explicit Reference Points -- Tracking Information Flow in Dynamic Tree Structures -- Network Security II -- Lightweight Opportunistic Tunneling (LOT) -- Hide and Seek in Time — Robust Covert Timing

Channels -- Authentic Time-Stamps for Archival Storage -- Towards a Theory of Accountability and Audit -- Reliable Evidence: Auditability by Typing -- PCAL: Language Support for Proof-Carrying Authorization Systems -- Network Security III -- ReFormat: Automatic Reverse Engineering of Encrypted Messages -- Protocol Normalization Using Attribute Grammars -- Automatically Generating Models for Botnet Detection -- Dynamic Enforcement of Abstract Separation of Duty Constraints -- Usable Access Control in Collaborative Environments: Authorization Based on People-Tagging -- Requirements and Protocols for Inference-Proof Interactions in Information Systems -- A Privacy Preservation Model for Facebook-Style Social Network Systems -- New Privacy Results on Synchronized RFID Authentication Protocols against Tag Tracing -- Secure Pseudonymous Channels -- Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing -- Content Delivery Networks: Protection or Threat? -- Model-Checking DoS Amplification for VoIP Session Initiation -- The Wisdom of Crowds: Attacks and Optimal Constructions -- Secure Evaluation of Private Linear Branching Programs with Medical Applications -- Keep a Few: Outsourcing Data While Maintaining Confidentiality -- Data Structures with Unpredictable Timing -- WORM-SEAL: Trustworthy Data Retention and Verification for Regulatory Compliance -- Corruption-Localizing Hashing -- Isolating JavaScript with Filters, Rewriting, and Wrappers -- An Effective Method for Combating Malicious Scripts Clickbots -- Client-Side Detection of XSS Worms by Monitoring Payload Propagation -- Formal Indistinguishability Extended to the Random Oracle Model -- Computationally Sound Analysis of a Probabilistic Contract Signing Protocol -- Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption -- A Generic Security API for Symmetric Key Management on Cryptographic Devices -- ID-Based Secure Distance Bounding and Localization -- Secure Ownership and Ownership Transfer in RFID Systems -- Cumulative Attestation Kernels for Embedded Systems -- Super-Efficient Aggregating History-Independent Persistent Authenticated Dictionaries -- Set Covering Problems in Role-Based Access Control.

Sommario/riassunto

This book constitutes the proceedings of the 14th European Symposium on Research in Computer Security, ESORICS 2009, held in Saint-Malo, France, in September 2009. The 42 papers included in the book were carefully reviewed and selected from 220 papers. The topics covered are network security, information flow, language based security, access control, privacy, distributed systems security, security primitives, web security, cryptography, protocols, and systems security and forensics.