1. Record Nr. UNINA9910483259103321

Titolo	Computer Security – ESORICS 2006 : 11th European Symposium on Research in Computer Security, Hamburg, Germany, September 18-20, 2006, Proceedings / / edited by Eugene Asarin, Dieter Gollmann, Jan Meier, Andrei Sabelfeld
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-44605-2
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XII, 550 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 4189
Altri autori (Persone)	GollmannDieter MeierJan <1977-> SabelfeldAndrei
Disciplina	005.8
Soggetti	Computer science Cryptography Data encryption (Computer science) Operating systems (Computers) Computer networks Database management Electronic data processing - Management Theory of Computation Cryptology Operating Systems Computer Communication Networks Database Management IT Operations
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	Finding Peer-to-Peer File-Sharing Using Coarse Network Behaviors -- Timing Analysis in Low-Latency Mix Networks: Attacks and Defenses -- TrustedPals: Secure Multiparty Computation Implemented with Smart Cards -- Private Information Retrieval Using Trusted Hardware -- Bridging the Gap Between Inter-communication Boundary and Internal

Trusted Components -- License Transfer in OMA-DRM -- Enhanced Security Architecture for Music Distribution on Mobile -- A Formal Model of Access Control for Mobile Interactive Devices -- Discretionary Capability Confinement -- Minimal Threshold Closure -- Reducing the Dependence of SPKI/SDSI on PKI -- Delegation in Role-Based Access Control -- Applying a Security Requirements Engineering Process -- Modeling and Evaluating the Survivability of an Intrusion Tolerant Database System -- A Formal Framework for Confidentiality-Preserving Refinement -- Timing-Sensitive Information Flow Analysis for Synchronous Systems -- HBAC: A Model for History-Based Access Control and Its Model Checking -- From Coupling Relations to Mated Invariants for Checking Information Flow -- A Linear Logic of Authorization and Knowledge -- Prêt à Voter with Re-encryption Mixes -- Secure Key-Updating for Lazy Revocation -- Key Derivation Algorithms for Monotone Access Structures in Cryptographic File Systems -- Cryptographically Sound Security Proofs for Basic and Public-Key Kerberos -- Deriving Secrecy in Key Establishment Protocols -- Limits of the BRSIM/UC Soundness of Dolev-Yao Models with Hashes -- Conditional Reactive Simulatability -- SessionSafe: Implementing XSS Immune Session Handling -- Policy-Driven Memory Protection for Reconfigurable Hardware -- Privacy-Preserving Queries on Encrypted Data -- Analysis of Policy Anomalies on Distributed Network Security Setups -- Assessment of a Vulnerability in Iterative Servers Enabling Low-Rate DoS Attacks -- Towards an Information-Theoretic Framework for Analyzing Intrusion Detection Systems.

Sommario/riassunto

This book constitutes the refereed proceedings of the 11th European Symposium on Research in Computer Security, ESORICS 2006. The 32 revised full papers presented were carefully reviewed and selected from 160 submissions. ESORICS is confirmed as the European research event in computer security; it presents original research contributions, case studies and implementation experiences addressing any aspect of computer security - in theory, mechanisms, applications, or practical experience.