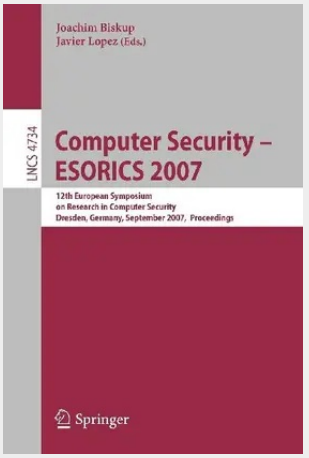
Biskup

Computer Security - ESORICS 2007

12th European Symposium On Research In Computer Security, Dresden, Germany, September 24 - 26, 2007, Proceedings



This book constitutes the refereed proceedings of the 12th European Symposium on Research in Computer Security, ESORICS 2007, held in Dresden, Germany in September 2007. It features 39 revised full papers. ESORICS is confirmed as the European research event in computer security. It presents original research contributions, case studies and implementation experiences that address any aspect of computer security, in theory, mechanisms, applications, or practical experience.

Invited Lecture.- Trustworthy Services and the Biological Analogy.- Security Architecture and Secure Components I.- Security of Multithreaded Programs by Compilation.- Efficient Proving for Practical Distributed Access-Control Systems.- Maintaining High Performance Communication Under Least Privilege Using Dynamic Perimeter Control.- Access Control I.- Pragmatic XML Access Control Using Off-the-Shelf RDBMS.- Conditional Privacy-Aware Role Based Access Control.- Satisfiability and Resiliency in Workflow Systems.- Applied Cryptography I.- Completeness of the Authentication Tests.- SilentKnock: Practical, Provably Undetectable Authentication.- Generalized Key Delegation for Hierarchical Identity-Based Encryption.- Change-Impact Analysis of Firewall Policies.- Fragmentation and Encryption to Enforce Privacy in Data Storage.- Information Confinement, Privacy, and Security in RFID Systems.- Formal Methods in Security I.- A Logic for State-Modifying Authorization Policies.- Inductive Proofs of Computational Secrecy.- What, Indeed, Is Intransitive Noninterference?.- Traceability and Integrity of Execution in Distributed Workflow Management Systems.- Dynamic Information Flow Control Architecture for Web Applications.- Cloak: A Ten-Fold Way for Reliable Covert Communications.- Applied Cryptography II.- Efficient Password-Based Authenticated Key Exchange Without Public Information.- Improved Anonymous Timed-Release Encryption.- Encryption Techniques for Secure Database Outsourcing.- Access Control II.- Click Passwords Under Investigation.- Graphical Password Authentication Using Cued Click Points.- Obligations and Their Interaction with Programs.- Applied Cryptography III.- On the Privacy of Concealed Data Aggregation.- Synthesizing Secure Protocols.- A Cryptographic Model for Branching Time Security Properties - The Case of Contract Signing Protocols.- Security Architecture and Secure Components II.- Security Evaluation of Scenarios Based on the TCG's TPM Specification.- Analyzing Side Channel Leakage of Masked Implementations with Stochastic Methods.- Insider Attacks Enabling Data Broadcasting on Crypto-Enforced Unicast Links.- Towards Modeling Trust Based Decisions: A Game Theoretic Approach.- Extending the Common Services of eduGAIN with a Credential Conversion Service.- Incorporating Temporal Capabilities in Existing Key Management Schemes.- A Policy Language for Distributed Usage Control.- Countering Statistical Disclosure with Receiver-Bound Cover Traffic.- Renewable Traitor Tracing: A Trace-Revoke-Trace System For Anonymous Attack.- Formal Methods in Security III.- Modular Access Control Via Strategic Rewriting.- On the Automated Correction of Security Protocols Susceptible to a Replay Attack.- Adaptive Soundness of Static Equivalence.

106,99 €
99,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540748342
Medium: Buch
ISBN: 978-3-540-74834-2
Verlag: Springer
Erscheinungstermin: 12.09.2007
Sprache(n): Englisch
Auflage: Erscheinungsjahr 2007
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 961 g
Seiten: 628
Format (B x H): 155 x 235 mm

fachmedien.de
WISSEN. EINFACH. FINDEN.

27.11.2026 | 11:30 Uhr

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)