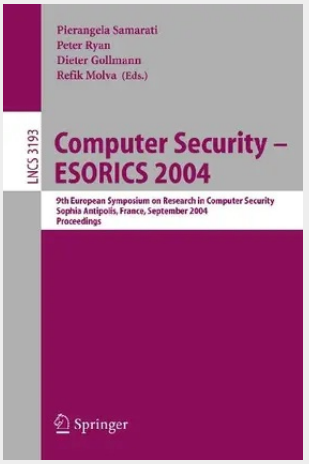
Samarati / Ryan / Gollmann

Computer Security - ESORICS 2004

9th European Symposium on Research Computer Security, Sophia Antipolis, France, September 13-15, 2004. Proceedings

ForewordfromtheProgramChairs These proceedings contain the papers selected for presentation at the 9th - ropean Symposium on Research in Computer Security (ESORICS), held during September 13–15, 2004 in Sophia Antipolis, France. In response to the call for papers 159 papers were submitted to the conference. These papers were evaluated on the basis of their signi?cance, novelty,and te- nicalquality. Eachpaper wasreviewedby at leastthree members of the program committee. The program committee meeting was held electronically; there was an intensive discussion over a period of two weeks. Of the papers submitted, 27 were selected for presentation at the conference, giving an acceptance rate lower than 17%. The conference program also included an invited talk. A workshop like this does not just happen; it depends on the volunteer e?orts of ahostofindividuals. Thereisalonglistofpeoplewhovolunteeredtheirtimeand energy to put together the workshopand who deserve special thanks. Thanks to all the members of the program committee, and the external reviewers, for all their hardwork in the paper evaluation. Due to the large number of submissions the program committee members were really required to work hard in a short time frame, and we are very thankful to them for the commitment they showed with their active participation in the electronic discussion.

Incorporating Dynamic Constraints in the Flexible Authorization Framework.- Access-Condition-Table-Driven Access Control for XML Databases.- An Algebra for Composing Enterprise Privacy Policies.- Deriving, Attacking and Defending the GDOI Protocol.- Better Privacy for Trusted Computing Platforms.- A Cryptographically Sound Dolev-Yao Style Security Proof of the Otway-Rees Protocol.- A Formalization of Anonymity and Onion Routing.- Breaking Cauchy Model-Based JPEG Steganography with First Order Statistics.- Comparison Between Two Practical Mix Designs.- Signature Bouquets: Immutability for Aggregated/Condensed Signatures.- Towards a Theory of Data Entanglement.- Portable and Flexible Document Access Control Mechanisms.- Possibilistic Information Flow Control in the Presence of Encrypted Communication.- Information Flow Control Revisited: Noninfluence = Noninterference + Nonleakage.- Security Property Based Administrative Controls.- A Vector Model of Trust for Developing Trustworthy Systems.- Parameterized Authentication.- Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks.- Hindering Eavesdropping via IPv6 Opportunistic Encryption.- On the Role of Key Schedules in Attacks on Iterated Ciphers.- A Public-Key Encryption Scheme with Pseudo-random Ciphertexts.- A Host Intrusion Prevention System for Windows Operating Systems.- Re-establishing Trust in Compromised Systems: Recovering from Rootkits That Trojan the System Call Table.- ARCHERR: Runtime Environment Driven Program Safety.- Sets, Bags, and Rock and Roll.- Redundancy and Diversity in Security.- Discovering Novel Attack Strategies from INFOSEC Alerts.



53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540229872
Medium: Buch
ISBN: 978-3-540-22987-2
Verlag: Springer
Erscheinungstermin: 06.09.2004
Sprache(n): Englisch
Auflage: 1. Auflage 2004
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 1450 g
Seiten: 457
Format (B x H): 155 x 235 mm

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