

1. Record Nr.	UNINA9910485051903321
Titolo	Proceedings of the IFIP TC 11 23rd International Information Security Conference : IFIP 20th World Computer Congress, IFIP SEC'08, September 7-10, 2008, Milano, Italy / / Sushil Jajodia; Pierangela Samarati; Stelvio Cimato
Pubbl/distr/stampa	New York, New York : , : Springer, , [2008] ©2008
ISBN	0-387-09699-X
Edizione	[1st ed. 2008.]
Descrizione fisica	1 online resource (722 p.)
Collana	IFIP Advances in Information and Communication Technology, , 1868-4238 ; ; 278
Disciplina	616.994
Soggetti	Preleukemia
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Articles that correspond to the papers and the edited discussions presented at an international symposium held at Innsbruck in 1978.
Nota di bibliografia	Includes bibliographies and index.
Nota di contenuto	Hiding in Groups: On the Expressiveness of Privacy Distributions -- Practical Privacy-Preserving Benchmarking -- Enhancing Privacy in Remote Data Classification -- Minimizing SSO Effort in Verifying SSL Anti-phishing Indicators -- Robbing Banks with Their Own Software— an Exploit Against Norwegian Online Banks -- Collaborative architecture for malware detection and analysis -- Realizing Stateful Public Key Encryption in Wireless Sensor Network -- Establishing secure links in low-rate wireless personal area networks -- An Asynchronous Node Replication Attack in Wireless Sensor Networks -- A B Formal Framework for Security Developments in the Domain of Smart Card Applications -- An Implementation of a Privacy Enforcement Scheme based on the Java Security Framework using XACML Policies -- Negotiation of Prohibition: An Approach Based on Policy Rewriting -- An Integrity Lock Architecture for Supporting Distributed Authorizations in Database Federations -- Role Signatures for Access Control in Open Distributed Systems -- Policies and Security Aspects For Distributed Scientific Laboratories -- A Fuzzy Model for the Composition of Intrusion Detectors -- Investigating the problem of IDS false alarms: An experimental study using Snort -- User Session

Modeling for Effective Application Intrusion Detection -- A Product Machine Model for Anomaly Detection of Interposition Attacks on Cyber-Physical Systems -- Anomaly Detection with Diagnosis in Diversified Systems using Information Flow Graphs -- Behavioral Intrusion Detection Indicators -- Leveraging Lattices to Improve Role Mining -- A Parallelization Framework for Exact Knowledge Hiding in Transactional Databases -- Efficient Coalition Detection in Traitor Tracing -- SPIT Identification Criteria Implementation: Effectiveness and Lessons Learned -- Detecting More SIP Attacks on VoIP Services by Combining Rule Matching and State Transition Models -- A Decentralized Bayesian Attack Detection Algorithm for Network Security -- An Operation-Based Metric for CPA Resistance -- YASIR: A Low-Latency, High-Integrity Security Retrofit for Legacy SCADA Systems -- Adversary Modeling and Simulation in Cyber Warfare -- Interactive Selection of ISO 27001 Controls under Multiple Objectives -- Feasibility of Automated Information Security Compliance Auditing -- Software Licence Protection and Management for Organisations -- A Vulnerability Prioritization System Using A Fuzzy Risk Analysis Approach -- ASTRA : A Security Analysis Method Based on Asset Tracking -- A Knowledge-Based Bayesian Model for Analyzing a System after an Insider Attack -- Portable User-Centric Identity Management -- Ubiquitous Privacy-Preserving Identity Management -- Facilitating Privacy Related Decisions in Different Privacy Contexts on the Internet by Evaluating Trust in Recipients of Private Data -- Using Virtualization to Create and Deploy Computer Security Lab Exercises -- DigForNet: Digital Forensic in Networking -- A Live Digital Forensic system for Windows networks -- HoneyID : Unveiling Hidden Spywares by Generating Bogus Events -- A Security Protocol for Self-Organizing Data Storage -- Protecting Financial Institutions from Brute-Force Attacks -- Agency Theory: Can it be Used to Strengthen IT Governance? -- A new Accounting Mechanism for Modern and Future AAA Services -- A user survey on the sense of security, Anshin -- Multi-Layer Encryption for Multi-Level Access Control in Wireless Sensor Networks -- A Comparative Study of Anomaly Detection Techniques in Web Site Defacement Detection -- Managing the lifecycle of XACML delegation policies in federated environments -- Assessing the Likelihood of Privacy Policy Compliance -- Classification features for detecting Server-side and Client-side Web attacks.

---

## Sommario/riassunto

International Federation for Information Processing The IFIP series publishes state-of-the-art results in the sciences and technologies of information and communication. The scope of the series includes: foundations of computer science; software theory and practice; education; computer applications in technology; communication systems; systems modeling and optimization; information systems; computers and society; computer systems technology; security and protection in information processing systems; artificial intelligence; and human-computer interaction. Proceedings and post-proceedings of refereed international conferences in computer science and interdisciplinary fields are featured. These results often precede journal publication and represent the most current research. The principal aim of the IFIP series is to encourage education and the dissemination and exchange of information about all aspects of computing. For more information about the 300 other books in the IFIP series, please visit [www.springer.com](http://www.springer.com). For more information about IFIP, please visit [www.ifip.org](http://www.ifip.org).

---