

- | | |
|-------------------------|------------------------------|
| 1. Record Nr. | UNIORUON00407818 |
| Autore | ISPE |
| Titolo | Azioni programmatiche / Ispe |
| Pubbl/distr/stampa | [s.l.] , : [s.n.] , 1971 |
| Descrizione fisica | 145 p. ; 29 cm. |
| Soggetti | PROGRAMMAZIONE ECONOMICA |
| Lingua di pubblicazione | Italiano |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
-
- | | |
|------------------------|--|
| 2. Record Nr. | UNINA9910484226403321 |
| Titolo | Recent Advances in Intrusion Detection : 13th International Symposium, RAID 2010, Ottawa, Ontario, Canada, September 15-17, 2010, Proceedings / / edited by Somesh Jha, Robin Sommer, Christian Kreibich |
| Pubbl/distr/stampa | Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010 |
| ISBN | 1-280-38871-4
9786613566638
3-642-15512-X |
| Edizione | [1st ed. 2010.] |
| Descrizione fisica | 1 online resource (524 p. 160 illus.) |
| Collana | Security and Cryptology, , 2946-1863 ; ; 6307 |
| Altri autori (Persone) | JhaSomesh
SommerRobin
KreibichChristian |
| Disciplina | 004.6 |
| Soggetti | Computer networks
Computer programming
Cryptography
Data encryption (Computer science)
Computers and civilization
Algorithms
Data structures (Computer science)
Information theory
Computer Communication Networks
Programming Techniques |

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 Protection -- What Is the Impact of P2P Traffic on Anomaly Detection? -- A Centralized Monitoring Infrastructure for Improving DNS Security -- Behavior-Based Worm Detectors Compared -- High Performance -- Improving NFA-Based Signature Matching Using Ordered Binary Decision Diagrams -- GrAVity: A Massively Parallel Antivirus Engine -- Malware Detection and Defence -- Automatic Discovery of Parasitic Malware -- BotSwindler: Tamper Resistant Injection of Believable Decoys in VM-Based Hosts for Crimeware Detection -- CANVuS: Context-Aware Network Vulnerability Scanning -- HyperCheck: A Hardware-Assisted Integrity Monitor -- Kernel Malware Analysis with Un-tampered and Temporal Views of Dynamic Kernel Memory -- Bait Your Hook: A Novel Detection Technique for Keyloggers -- Evaluation -- Generating Client Workloads and High-Fidelity Network Traffic for Controllable, Repeatable Experiments in Computer Security -- On Challenges in Evaluating Malware Clustering -- Why Did My Detector Do That?! -- Forensics -- NetStore: An Efficient Storage Infrastructure for Network Forensics and Monitoring -- Live and Trustworthy Forensic Analysis of Commodity Production Systems -- Hybrid Analysis and Control of Malware -- Anomaly Detection -- Anomaly Detection and Mitigation for Disaster Area Networks -- Community Epidemic Detection Using Time-Related Anomalies -- A Data-Centric Approach to Insider Attack Detection in Database Systems -- Privilege States Based Access Control for Fine-Grained Intrusion Response -- Web Security -- Abusing Social Networks for Automated User Profiling -- An Analysis of Rogue AV Campaigns -- Fast-Flux Bot Detection in Real Time -- Posters -- A Client-Based and Server-Enhanced Defense Mechanism for Cross-Site Request Forgery -- A Distributed HoneyNet at KFUPM: A Case Study -- Aspect-Based Attack Detection in Large-Scale Networks -- Detecting Network Anomalies in Backbone Networks -- Detecting the Onset of Infection for Secure Hosts -- Eliminating Human Specification in Static Analysis -- Evaluation of the Common Dataset Used in Anti-Malware Engineering Workshop 2009 -- Inferring Protocol State Machine from Real-World Trace -- MEDUSA: Mining Events to Detect Undesirable uSer Actions in SCADA -- On Estimating Cyber Adversaries' Capabilities: A Bayesian Model Approach -- Security System for Encrypted Environments (S2E2) -- Towards Automatic Deduction and Event Reconstruction Using Forensic Lucid and Probabilities to Encode the IDS Evidence -- Toward Specification-Based Intrusion Detection for Web Applications -- Toward Whole-System Dynamic Analysis for ARM-Based Mobile Devices -- Using IRP for Malware Detection.
Sommario/riassunto	On behalf of the Program Committee, it is our pleasure to present the proceedings of the 13th International Symposium on Recent Advances in Intrusion Detection Systems (RAID 2010), which took place in

Ottawa, Ontario, Canada, during September 15-17, 2010. As in the past, the symposium brought together leading researchers and practitioners from academia, government, and industry to discuss intrusion detection research and practice. There were eight technical sessions presenting full research papers on network protection, high performance, malware detection and defense (2 sessions), evaluation, forensics, anomaly detection and access protection, and Web security. Furthermore, there was a poster session presenting emerging research areas and case studies. The RAID 2010 Program Committee received 102 full-paper submissions from all over the world. All submissions were carefully reviewed by independent reviewers on the basis of technical quality, topic, space, and overall balance. The final decision took place at a Program Committee meeting held during May 19-20 in Oakland, California, where 24 papers were eventually selected for presentation at the conference and publication in the proceedings. As a continued feature, the symposium later also accepted 15 poster presentations reporting early-stage research, demonstration of applications, or case studies. The authors of accepted posters were also offered the opportunity to have an extended abstract of their work included in the proceedings.
