

1. Record Nr.	UNISA996466167903316
Titolo	Recent Advances in Intrusion Detection [[electronic resource] ] : 8th International Symposium, RAID 2005, Seattle, WA, USA, September 7-9, 2005, Revised Papers / / edited by Alfonso Valdes, Diego Zamboni
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-31779-1
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (X, 351 p.)
Collana	Security and Cryptology ; ; 3858
Disciplina	005.8
Soggetti	Management information systems Computer science Computer communication systems Operating systems (Computers) Data encryption (Computer science) Computers and civilization Management of Computing and Information Systems Computer Communication Networks Operating Systems Cryptology Computers and Society
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	Worm Detection and Containment (I) -- Virtual Playgrounds for Worm Behavior Investigation -- Empirical Analysis of Rate Limiting Mechanisms -- Anomaly Detection -- COTS Diversity Based Intrusion Detection and Application to Web Servers -- Behavioral Distance for Intrusion Detection -- Intrusion Prevention and Response -- FLIPS: Hybrid Adaptive Intrusion Prevention -- Towards Software-Based Signature Detection for Intrusion Prevention on the Network Card -- Defending Against Injection Attacks Through Context-Sensitive String Evaluation -- System Call-Based Intrusion Detection -- Improving Host-Based IDS with Argument Abstraction to Prevent Mimicry Attacks -- On Random-Inspection-Based Intrusion Detection -- Environment-

Sensitive Intrusion Detection -- Worm Detection and Containment (II)  
-- Polymorphic Worm Detection Using Structural Information of Executables -- Anomalous Payload-Based Worm Detection and Signature Generation -- Network-Based Intrusion Detection -- On Interactive Internet Traffic Replay -- Interactive Visualization for Network and Port Scan Detection -- A Fast Static Analysis Approach to Detect Exploit Code Inside Network Flows -- Mobile and Wireless Networks -- Sequence Number-Based MAC Address Spoof Detection -- A Specification-Based Intrusion Detection Model for OLSR.

---

## Sommario/riassunto

On behalf of the Program Committee, it is our pleasure to present the proceedings of the 8th Symposium on Recent Advances in Intrusion Detection (RAID 2005), which took place in Seattle, Washington, USA, September 7-9, 2005. The symposium brought together leading researchers and practitioners from academia, government and industry to discuss intrusion detection from research as well as commercial perspectives. We also encouraged discussions that addressed issues that arise when studying intrusion detection, including monitoring, performance and validation, from a wider perspective. We had sessions on the detection and containment of Internet worm attacks, anomaly detection, automated response to intrusions, host-based intrusion detection using system calls, network intrusion detection, and intrusion detection, in mobile wireless networks. The RAID 2005 Program Committee received 83 paper submissions from all over the world. All submissions were carefully reviewed by several members of Program Committee and selection was made on the basis of scientific novelty, importance to the field, and technical quality. Final selection took place at a Program Committee meeting held on May 11 and 12 in Oakland, California. Fifteen papers and two practical experience reports were selected for presentation and publication in the conference proceedings. The keynote address was given by Phil Attfield of the Northwest Security Institute.

---