

1. Record Nr.	UNINA9910144348403321
Titolo	Recent Advances in Intrusion Detection : 7th International Symposium, RAID 2004, Sophia Antipolis, France, September 15-17, 2004, Proceedings / / edited by Erland Jonsson, Alfonso Valdes, Magnus Almgren
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2004
ISBN	3-540-30143-7
Edizione	[1st ed. 2004.]
Descrizione fisica	1 online resource (X, 322 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 3224
Disciplina	005.8
Soggetti	Management information systems Computer science Data encryption (Computer science) Computer security Computers and civilization Computer networks Operating systems (Computers) Management of Computing and Information Systems Cryptology Systems and Data Security Computers and Society Computer Communication Networks Operating Systems
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 at the end of each chapters and index.
Nota di contenuto	Modelling Process Behaviour -- Automatic Extraction of Accurate Application-Specific Sandboxing Policy -- Context Sensitive Anomaly Monitoring of Process Control Flow to Detect Mimicry Attacks and Impossible Paths -- Detecting Worms and Viruses -- HoneyStat: Local Worm Detection Using Honeypots -- Fast Detection of Scanning Worm Infections -- Detecting Unknown Massive Mailing Viruses Using

Proactive Methods -- Attack and Alert Analysis -- Using Adaptive Alert Classification to Reduce False Positives in Intrusion Detection -- Attack Analysis and Detection for Ad Hoc Routing Protocols -- On the Design and Use of Internet Sinks for Network Abuse Monitoring -- Practical Experience -- Monitoring IDS Background Noise Using EWMA Control Charts and Alert Information -- Symantec Deception Server Experience with a Commercial Deception System -- Anomaly Detection -- Anomalous Payload-Based Network Intrusion Detection -- Anomaly Detection Using Layered Networks Based on Eigen Co-occurrence Matrix -- Seurat: A Pointillist Approach to Anomaly Detection -- Formal Analysis for Intrusion Detection -- Detection of Interactive Stepping Stones: Algorithms and Confidence Bounds -- Formal Reasoning About Intrusion Detection Systems -- RheoStat: Real-Time Risk Management.

Sommario/riassunto

On behalf of the Program Committee, it is our pleasure to present to you the proceedings of the 7th Symposium on Recent Advances in Intrusion Detection (RAID 2004), which took place in Sophia-Antipolis, French Riviera, France, September 15–17, 2004. 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 - dressed issues that arise when studying intrusion detection, including information gathering and monitoring, from a wider perspective. Thus, we had sessions on detection of worms and viruses, attack analysis, and practical experience reports. The RAID 2004 Program Committee received 118 paper submissions from all over the world. All submissions were carefully reviewed by several members of the 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 meeting held May 24 in Paris, France. Fourteen papers and two practical experience reports were selected for presentation and publication in the conference proceedings. In addition, a number of papers describing work in progress were selected for presentation at the symposium. The keynote address was given by Bruce Schneier of Counterpane Systems. Hakan Kvarnstrom of TeliaSonera gave an invited talk on the topic "Fighting Fraud in Telecom Environments." A successful symposium is the result of the joint effort of many people.
