

Table of Contents

Network Infrastructure

- Mitigating Distributed Denial of Service Attacks
Using a Proportional-Integral-Derivative Controller 1
M. Tylutki and K. Levitt
- Topology-Based Detection of Anomalous BGP Messages 17
C. Kruegel, D. Mutz, W. Robertson, and F. Valeur

Anomaly Detection I

- Detecting Anomalous Network Traffic with Self-organizing Maps 36
M. Ramadas, S. Ostermann, and B. Tjaden
- An Approach for Detecting Self-propagating Email
Using Anomaly Detection 55
A. Gupta and R. Sekar

Correlation

- Statistical Causality Analysis of INFOSEC Alert Data 73
X. Qin and W. Lee
- Correlation of Intrusion Symptoms: An Application of Chronicles 94
B. Morin and H. Debar

Modeling and Specification

- Modeling Computer Attacks: An Ontology for Intrusion Detection 113
J. Undercoffer, A. Joshi, and J. Pinkston
- Using Specification-Based Intrusion Detection for Automated Response . . . 136
I. Balepin, S. Maltsev, J. Rowe, and K. Levitt

IDS Sensors

- Characterizing the Performance of Network Intrusion Detection Sensors . . . 155
L. Schaelicke, T. Slabach, B. Moore, and C. Freeland
- Using Decision Trees to Improve Signature-Based Intrusion Detection 173
C. Kruegel and T. Toth
- Ambiguity Resolution via Passive OS Fingerprinting 192
G. Taleck

Anomaly Detection II

Two Sophisticated Techniques to Improve HMM-Based Intrusion Detection Systems	207
<i>S.-B. Cho, S.-J. Han</i>	
An Analysis of the 1999 DARPA/Lincoln Laboratory Evaluation Data for Network Anomaly Detection	220
<i>M.V. Mahoney and P.K. Chan</i>	
Author Index	239



<http://www.springer.com/978-3-540-40878-9>

Recent Advances in Intrusion Detection
6th International Symposium, RAID 2003, Pittsburgh,
PA, USA, September 8-10, 2003, Proceedings
Vigna, G.; Jonsson, E.; Kruegel, C. (Eds.)
2003, X, 242 p., Softcover
ISBN: 978-3-540-40878-9