

Table of Contents

Network Infrastructure

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

Anomaly Detection I

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

Correlation

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

Modeling and Specification

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

IDS Sensors

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

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

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