

Table of Contents

Stepping Stone Detection

Detecting Long Connection Chains of Interactive Terminal Sessions	1
<i>Kwong H. Yung</i>	
Multiscale Stepping-Stone Detection: Detecting Pairs of Jittered Interactive Streams by Exploiting Maximum Tolerable Delay	17
<i>David L. Donoho, Ana Georgina Flesia, Umesh Shankar, Vern Paxson, Jason Coit, Stuart Staniford</i>	
Detecting Malicious Software by Monitoring Anomalous Windows Registry Accesses	36
<i>Frank Apap, Andrew Honig, Shlomo Hershkop, Eleazar Eskin, Sal Stolfo</i>	

Anomaly Detection

Undermining an Anomaly-Based Intrusion Detection System Using Common Exploits	54
<i>Kymie M.C. Tan, Kevin S. Killourhy, Roy A. Maxion</i>	

Correlation

Analyzing Intensive Intrusion Alerts via Correlation	74
<i>Peng Ning, Yun Cui, Douglas S. Reeves</i>	
A Mission-Impact-Based Approach to INFOSEC Alarm Correlation	95
<i>Phillip A. Porras, Martin W. Fong, Alfonso Valdes</i>	
M2D2: A Formal Data Model for IDS Alert Correlation	115
<i>Benjamin Morin, Ludovic Mé, Hervé Debar, Mireille Ducassé</i>	

Legal Aspects / Intrusion Tolerance

Development of a Legal Framework for Intrusion Detection	138
<i>Steven R. Johnston</i>	
Learning Unknown Attacks – A Start	158
<i>James E. Just, James C. Reynolds, Larry A. Clough, Melissa Danforth, Karl N. Levitt, Ryan Maglich, Jeff Rowe</i>	

Assessment of Intrusion Detection Systems

Evaluation of the Diagnostic Capabilities of Commercial Intrusion Detection Systems	177
<i>Hervé Debar, Benjamin Morin</i>	
A Stochastic Model for Intrusions	199
<i>Robert P. Goldman</i>	
Attacks against Computer Network: Formal Grammar-Based Framework and Simulation Tool	219
<i>Vladimir Gorodetski, Igor Kotenko</i>	
Capacity Verification for High Speed Network Intrusion Detection Systems	239
<i>Mike Hall, Kevin Wiley</i>	

Adaptive Intrusion Detection Systems

Performance Adaptation in Real-Time Intrusion Detection Systems	252
<i>Wenke Lee, João B.D. Cabrerá, Ashley Thomas, Niranjan Balwalli, Sunmeet Saluja, Yi Zhang</i>	

Intrusion Detection Analysis

Accurate Buffer Overflow Detection via Abstract Payload Execution	274
<i>Thomas Toth, Christopher Kruegel</i>	
Introducing Reference Flow Control for Detecting Intrusion Symptoms at the OS Level	292
<i>Jacob Zimmermann, Ludovic Mé, Christophe Bidan</i>	
The Effect of Identifying Vulnerabilities and Patching Software on the Utility of Network Intrusion Detection	307
<i>Richard Lippmann, Seth Webster, Douglas Stetson</i>	

Author Index	327
-------------------------------	------------