

# Table of Contents

## Logging

Better Logging through Formality .....	1
<i>Chapman Flack and Mikhail J. Atallah</i>	
A Pattern Matching Based Filter for Audit Reduction and Fast Detection of Potential Intrusions .....	17
<i>Josué Kuri, Gonzalo Navarro, Ludovic Mé and Laurent Heye</i>	
Transaction-Based Pseudonyms in Audit Data for Privacy Respecting Intrusion Detection .....	28
<i>Joachim Biskup and Ulrich Flegel</i>	

## Data Mining

A Data Mining and CIDF Based Approach for Detecting Novel and Distributed Intrusions .....	49
<i>Wenke Lee, Rahul A. Nimbalkar, Kam K. Yee, Sunil B. Patil, Pragneshkumar H. Desai, Thuan T. Tran and Salvatore J. Stolfo</i>	
Using Finite Automata to Mine Execution Data for Intrusion Detection: A Preliminary Report .....	66
<i>Christoph Michael and Anup Ghosh</i>	

## Modeling Process Behavior

Adaptive, Model-Based Monitoring for Cyber Attack Detection .....	80
<i>Alfonso Valdes and Keith Skinner</i>	
A Real-Time Intrusion Detection System Based on Learning Program Behavior .....	93
<i>Anup K. Ghosh, Christoph Michael and Michael Schatz</i>	
Intrusion Detection Using Variable-Length Audit Trail Patterns .....	110
<i>Andreas Wespi, Marc Dacier and Hervé Debar</i>	
Flexible Intrusion Detection Using Variable-Length Behavior Modeling in Distributed Environment: Application to CORBA Objects .....	130
<i>Zakia Marrakchi, Ludovic Mé, Bernard Vivinis and Benjamin Morin</i>	

**IDS Evaluation**

The 1998 Lincoln Laboratory IDS Evaluation (A Critique) ..... 145  
*John McHugh*

Analysis and Results of the 1999 DARPA Off-Line Intrusion  
Detection Evaluation ..... 162  
*Richard Lippmann, Joshua W. Haines, David J. Fried,  
Jonathan Korba and Kumar Das*

Using Rule-Based Activity Descriptions  
to Evaluate Intrusion-Detection Systems ..... 183  
*Dominique Alessandri*

**Modeling**

LAMBDA : A Language to Model a Database for Detection of Attacks .... 197  
*Frédéric Cuppens and Rodolphe Ortalo*

Target Naming and Service Apoptosis ..... 217  
*James Riordan and Dominique Alessandri*

**Author Index** ..... 227



<http://www.springer.com/978-3-540-41085-0>

Recent Advances in Intrusion Detection  
Third International Workshop, RAID 2000 Toulouse,  
France, October 2-4, 2000 Proceedings  
Debar, H.; Me, L.; Wu, S.F. (Eds.)  
2000, X, 230 p., Softcover  
ISBN: 978-3-540-41085-0