

Table of Contents

Modeling Attacks

From Declarative Signatures to Misuse IDS	1
<i>Jean-Philippe Pouzol and Mireille Ducassé</i>	

Logging and IDS Integration

Application-Integrated Data Collection for Security Monitoring	22
<i>Magnus Almgren and Ulf Lindqvist</i>	

Interfacing Trusted Applications with Intrusion Detection Systems	37
<i>Marc Welz and Andrew Hutchison</i>	

IDS Cooperation

Probabilistic Alert Correlation	54
<i>Alfonso Valdes and Keith Skinner</i>	

Designing a Web of Highly-Configurable Intrusion Detection Sensors	69
<i>Giovanni Vigna, Richard A. Kemmerer, and Per Blix</i>	

Aggregation and Correlation of Intrusion-Detection Alerts	85
<i>Hervé Debar and Andreas Wespi</i>	

Anomaly Detection

Accurately Detecting Source Code of Attacks That Increase Privilege	104
<i>Robert K. Cunningham and Craig S. Stevenson</i>	

CDIS: Towards a Computer Immune System for Detecting Network Intrusions	117
<i>Paul D. Williams, Kevin P. Anchor, John L. Bebo, Gregg H. Gunsch, and Gary D. Lamont</i>	

Intrusion Tolerance

Autonomic Response to Distributed Denial of Service Attacks	134
<i>Dan Sterne, Kelly Djahandari, Brett Wilson, Bill Babson, Dan Schnackenberg, Harley Holliday, and Travis Reid</i>	

Legal Aspects

The Impact of Privacy and Data Protection Legislation on the Sharing of
Intrusion Detection Information 150
Steven R. Johnston

Specification-Based IDS

Experiences with Specification-Based Intrusion Detection 172
Prem Uppuluri and R. Sekar

System Health and Intrusion Monitoring Using a Hierarchy of
Constraints 190
Calvin Ko, Paul Brutch, Jeff Rowe, Guy Tsafnat, and Karl Levitt

Author Index 205