

Contents

Approaches in Anomaly-based Network Intrusion Detection Systems	1
Damiano Bolzoni and Sandro Etalle	
1	Introduction 1
2	Anomaly-Based Intrusion Detection Systems 2
2.1	Payload-based vs header-based approaches 4
3	Setting up an ABS 6
3.1	Building the Model 7
3.2	Setting the threshold 8
4	PAYL and POSEIDON 8
4.1	PAYL 8
4.2	POSEIDON 9
5	Conclusions 12
6	Appendix 13
6.1	PAYL algorithm 13
6.2	SOM algorithm 14
	References 15
Formal Specification for Fast Automatic Profiling of Program Behavior . .	17
Roberto Di Pietro, Antonio Durante, and Luigi.V. Mancini	
1	Introduction 17
2	Related works 19
3	Methodology 21
4	Case Study 22
4.1	POP3 commands 22
4.2	The FSM (step 1) 23
4.3	VSP specification for ipop3d (step 2) 24
4.4	Compiling VSP (step 3) 27
4.5	Visiting the FSM1 (step 4) 28
4.6	Executing Traces (step 5) 28
5	Using the Methodology to Configure REMUS 29
5.1	Results 30

6	Concluding remarks	31
7	Appendix	32
7.1	The critical system calls	32
7.2	Postgres VSP Specification	32
	References	32
Learning Behavior Profiles from Noisy Sequences		39
Ugo Galassi		
1	Introduction	39
2	Learning by Abstraction	41
3	Regular Expressions	42
4	String Alignment and Flexible Matching	43
5	The Learning Algorithm	45
5.1	ω_S Operator	46
5.2	ω_I Operator	47
5.3	Basic learning cycle	48
5.4	Refinement cycle	50
6	Evaluation on Artificial Traces	51
6.1	Motif reconstruction in presence of noise	52
6.2	Assessing the influence of alphabet size and motif length	53
6.3	Discovering graph structured patterns	57
7	User Profiling	59
7.1	Key Phrase Typing Model	59
7.2	Text Typing Model	60
8	Conclusion	62
	References	62
Correlation Analysis of Intrusion Alerts		65
Dingbang Xu and Peng Ning		
1	Introduction	66
2	Approaches Based on Similarity between Alert Attributes	67
2.1	Probabilistic Alert Correlation	68
2.2	Statistical Anomaly Analysis to Detect Stealthy Portscans	69
2.3	Root Cause Analysis	70
2.4	Statistical Causality Analysis Based Approach	71
2.5	Alert Clustering and Merging in MIRADOR Project	72
3	Approaches Based on Predefined Attack Scenarios	74
3.1	Aggregation and Correlation in IBM/Tivoli Systems	74
3.2	Chronicles Based Approach	75
4	Approaches Based on Prerequisites and Consequences of Attacks	76
4.1	Pre-condition/Post-condition Based Approach in MIRADOR Project	77
4.2	A Prerequisite and Consequence Based Approach	78
4.3	Attack Hypothesizing and Reasoning Techniques	79
5	Approaches Based on Multiple Information Sources	82
5.1	Mission-Impact-Based Approach	83

- 5.2 A Data Model M2D2 for Alert Correlation 84
- 5.3 Triggering Events and Common Resources Based Approach 85
- 6 Privacy Issues in Alert Correlation 86
 - 6.1 An Approach on Alert Sharing and Correlation 87
 - 6.2 Generalization and Perturbation Based Approaches 88
- 7 Summary 90
- References 90

An Approach to Preventing, Correlating, and Predicting Multi-Step Network Attacks 93

Lingyu Wang and Sushil Jajodia

- 1 Introduction 93
- 2 Related Work 95
- 3 Preliminaries 97
 - 3.1 Attack Graph 97
 - 3.2 Intrusion Alert and Correlation 99
- 4 Hardening Network To Prevent Multi-Step Intrusions 100
 - 4.1 A Motivating Example 100
 - 4.2 A Graph-Based Algorithm for Hardening A Network . . . 102
 - 4.3 Minimum-Cost Solutions 106
- 5 Correlating and Predicting Multi-Step Attacks 108
 - 5.1 Motivation 108
 - 5.2 Queue Graph-Based Alert Correlation 109
 - 5.3 Hypothesizing Missing Alerts and Predicting Future Alerts 114
 - 5.4 Compressing Result Graphs 117
 - 5.5 Empirical Results 119
 - 5.6 Effectiveness 120
 - 5.7 Performance 122
- 6 Conclusion 124
- References 126

Response: bridging the link between intrusion detection alerts and security policies 129

Hervé Debar, Yohann Thomas, Frédéric Cuppens, and Nora Cuppens-Boulahia

- 1 Introduction 129
- 2 Problem statement 130
 - 2.1 Domain terminology 130
 - 2.2 Intrusion Prevention and Response 132
 - 2.3 Comprehensive Approach to Response 133
- 3 Security Policy Formalism 133
 - 3.1 Choice of a Security Policy Formalism 133
 - 3.2 The Or-BAC Formalism 134
 - 3.3 Or-BAC Contexts 136

- 3.4 Presentation of a use case 137
- 3.5 Modelling of the use case 139
- 4 Applying Or-BAC for threat response 144
 - 4.1 Examples of threat contexts 144
 - 4.2 Atomic contexts 148
 - 4.3 Composed contexts 149
 - 4.4 Context activation 151
 - 4.5 Context deactivation 154
 - 4.6 Influence of Mapping on the Response Strategy 154
- 5 The Threat Response System 155
 - 5.1 System Architecture 155
 - 5.2 Alert Correlation Engine (ACE) 155
 - 5.3 Policy Instantiation Engine (PIE) 157
 - 5.4 Policy Decision Point (PDP) 157
 - 5.5 Policy Enforcement Point (PEP) 158
- 6 From alerts to new policies 158
 - 6.1 Syntactic mapping 158
 - 6.2 Enrichment 159
 - 6.3 Strategy application 160
- 7 Case Study: e-mail Server 160
 - 7.1 Threats related to the use case 161
 - 7.2 Threat analysis 163
 - 7.3 Revised description of the Policy Components 164
 - 7.4 Definition of the Security Policy 165
 - 7.5 The Mapping Predicates 167
- 8 Issues with the Approach 167
- 9 Conclusion 168
- References 169

Intrusion Detection and Reaction: an Integrated Approach to Network Security 171

M. Esposito, C. Mazzariello, F. Oliviero, L. Peluso, S. P. Romano, and C. Sansone

- 1 Introduction 172
- 2 Related Work 173
 - 2.1 Intrusion Detection Systems 173
 - 2.2 Traceback 176
- 3 The Proposed Framework 177
- 4 An Architecture for Intrusion Detection 178
 - 4.1 An Approach to Intrusion Detection 179
 - 4.2 Performance evaluation 188
 - 4.3 A Distributed Intrusion Detection System 191
 - 4.4 Privacy Issues in Intrusion Detection 193
- 5 Intrusion Reaction: a System for Attack Source Detection 195
 - 5.1 The ASSYST Architecture 195

5.2 Attack Sessions 196

5.3 The ASP Protocol 197

5.4 ASSYST: case studies 197

5.5 Intrusion detection subsystem 201

5.6 Traffic classification and intrusion reaction 202

5.7 ASSYST implementation details 203

5.8 ASP protocol implementation details 204

5.9 Testing the Approach 205

6 Conclusions and Future Work 205

References 207

Glossary of Terms Used in Security and Intrusion Detection 211

Index 247