

Contents

Part I Overview of Cyber Situational Awareness

1	Cyber SA: Situational Awareness for Cyber Defense	3
	P. Barford, M. Dacier, T. G. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, S. Jha, J. Li, P. Liu, P. Ning, X. Ou, D. Song, L. Strater, V. Swarup, G. Tadda, C. Wang, and J. Yen	
1.1	Scope of the Cyber SA Problem	3
1.2	Background	5
1.3	Research Goals	6
1.4	Research Agenda	7
1.4.1	Principles and Rationales	7
1.4.2	A Collection of Viewpoints on the Research Agenda	7
1.5	Conclusion	13
	References	14
2	Overview of Cyber Situation Awareness	15
	George P. Tadda and John S. Salerno	
2.1	What is Situation Awareness (SA)?	15
2.2	Situation Awareness Reference and Process Models	18
2.2.1	Situation Awareness Reference Model	18
2.2.2	Situation Awareness Process Model	24
2.3	Visualization	26
2.4	Application to the Cyber Domain	27
2.5	Measures of Performance and Effectiveness	28
2.5.1	Confidence	29
2.5.2	Purity	31
2.5.3	Cost Utility	32
2.5.4	Timeliness	33
2.5.5	Measures of Effectiveness	33
2.6	Conclusion	34
	References	34

Part II The Reasoning and Decision Making Aspects

3	RPD-based Hypothesis Reasoning for Cyber Situation Awareness . . .	39
	John Yen, Michael McNeese, Tracy Mullen, David Hall, Xiaocong Fan, and Peng Liu	
3.1	Introduction	39
3.2	Naturalistic Decision Making as a Holistic Model for Cyber SA . .	41
3.2.1	Decision and Hypotheses	41
3.2.2	The Recognition-Primed Decision (RPD) Model	41
3.3	RPD-based Hypothesis Generation and Reasoning for Cyber SA . .	42
3.3.1	Recognition-based Hypothesis Generation	43
3.3.2	Hypothesis-driven Story Building	43
3.3.3	Collaborative RPD-based Hypothesis Generation and Reasoning	44
3.4	Hypergraph-based Hypothesis Reasoning	45
3.4.1	Modeling Events as Network Entities	46
3.4.2	Hypergraph-based Network Analysis Techniques	46
3.5	Market-based Evidence Gathering	47
3.6	Summary	48
	References	49
4	Uncertainty and Risk Management in Cyber Situational Awareness	51
	Jason Li, Xinming Ou, and Raj Rajagopalan	
4.1	Reasoning about Uncertainty is a Necessity	51
4.2	Two Approaches to Handling Dynamic Uncertainty	52
4.2.1	The logical approach	52
4.2.2	The statistical approach	53
4.3	From Attack Graphs to Bayesian Networks	53
4.3.1	A case study	54
4.3.2	Desired properties of Bayesian Networks in Intrusion Analysis	55
4.3.3	Building BN's from attack graphs	56
4.4	An Empirical Approach to Developing a Logic for Uncertainty in Situation Awareness	57
4.4.1	A case study	57
4.4.2	Encoding the case study in logic	58
4.4.3	Comparison with previous approaches	62
4.5	Static Uncertainty and Risk Management	63
4.5.1	CVSS metrics	63
4.5.2	Combining CVSS and Attack Graphs	65
4.6	Conclusion	65
	References	65

Part III Macroscopic Cyber Situational Awareness

5	Employing Honeynets For Network Situational Awareness	71
	P. Barford, Y. Chen, A. Goyal, Z. Li, V. Paxson, and V. Yegneswaran	
5.1	Introduction	72
5.2	Background	73
5.3	Classifying Honeynet Activity	74
5.4	Experiences With Activity Classification	76
5.5	Situational Awareness In-depth	77
	5.5.1 Source Arrivals	79
	5.5.2 Destination/Source Net Coverage	80
	5.5.3 Source Macro-analysis	81
5.6	Towards Automated Classification	84
5.7	Assessing Botnet Scanning Patterns	85
	5.7.1 Monotonic Trend Checking	85
	5.7.2 Checking for Liveness-Aware Scanning	86
	5.7.3 Uniformity Checking	87
	5.7.4 Dependency Checking	87
5.8	Extrapolating Global Properties	87
	5.8.1 Assumptions and Requirements	88
	5.8.2 Estimating Global Population	89
	5.8.3 Exploiting IPID/Port Continuity	90
	5.8.4 Extrapolating from Interarrival Times	92
5.9	Evaluation of Automated Classification	92
	5.9.1 Basic Characteristics of Botnet Events	94
	5.9.2 Event Correlation	95
	5.9.3 Property-Checking Results	95
	5.9.4 Extrapolation Evaluation & Validation	98
5.10	Summary	101
	References	101
6	Assessing Cybercrime Through the Eyes of the WOMBAT	103
	Marc Dacier, Corrado Leita, Olivier Thonnard, Van-Hau Pham, and Engin Kirda	
6.1	Foreword	103
6.2	Introduction	104
6.3	Leurre.com v1.0 Honeyd	104
	6.3.1 Historical background	104
	6.3.2 Some technical aspects	105
	6.3.3 Generic picture	107
	6.3.4 Some illustrative examples	108
6.4	Leurre.com v2.0: SGNET	112
	6.4.1 Increasing the level of interaction	112
	6.4.2 ScriptGen	112
	6.4.3 SGNET: a ScriptGen-based honeypot deployment	113

6.5	Analysis of Attack Events	117
6.5.1	Identification of Attack Events	117
6.5.2	Armies of Zombies	119
6.5.3	Impact of Observation View Point.....	122
6.6	Multi-Dimensional Analysis of Attack Events	123
6.6.1	Methodology	123
6.6.2	Clique-based Clustering	124
6.6.3	Combining Cliques of Attackers	127
6.7	Beyond Events Correlation: Exploring the epsilon-gamma-pi-mu space.....	129
6.7.1	Degrees of freedom	130
6.7.2	Interesting cases	131
6.8	Conclusions	133
	References	134

Part IV Enterprise Cyber Situational Awareness

7	Topological Vulnerability Analysis	139
	Sushil Jajodia and Steven Noel	
7.1	Introduction	139
7.2	System Architecture	140
7.3	Illustrative Example	142
7.4	Network Attack Modeling	145
7.5	Analysis and Visualization.....	147
7.6	Scalability	149
7.7	Related Work.....	152
7.8	Summary	152
	References	153
8	Cross-Layer Damage Assessment for Cyber Situational Awareness ..	155
	Peng Liu, Xiaoqi Jia, Shengzhi Zhang, Xi Xiong, Yoon-Chan Jhi, Kun Bai, and Jason Li	
8.1	INTRODUCTION	155
8.1.1	A Multi-Level Damage Assessment Framework	156
8.1.2	Existing Damage Assessment Techniques	159
8.1.3	Focus of This Work: Damage Assessment Cross Instruction Level and OS Level	160
8.2	PEDA: An Architecture For Fine-Grained Damage Assessment In A Production Environment	161
8.3	VM-Based Cross-Layer Damage Assessment: An Overview	163
8.3.1	System Model	163
8.3.2	Problem Statement	164
8.3.3	Overview of Our Approach	165
8.4	Design And Implementation	165
8.4.1	Cross-Layer Damage Assessment when the Guest Kernel is Not Compromised.....	166

8.4.2	Cross-Layer Damage Assessment when the Guest Kernel is Compromised	168
8.4.3	“What-if” Damage Assessment	169
8.5	Preliminary Evaluation	171
8.5.1	Compromised Process Damage Assessment Experiment	171
8.5.2	Malicious Kernel Module Experiment	172
8.6	RELATED WORK	173
8.7	LIMITATIONS	174
8.8	Conclusion	174
	References	174

Part V Microscopic Cyber Situational Awareness

9	A Declarative Framework for Intrusion Analysis	179
	Matt Fredrikson, Mihai Christodorescu, Jonathon Giffin, and Somesh Jha	
9.1	Introduction	179
9.2	A Survey of Related Work	180
9.2.1	Forensic Analysis of Intrusions	180
9.2.2	Recovery From and Remediation of Intrusions	182
9.2.3	Intrusion Detection	182
9.2.4	Security Analysis	183
9.2.5	Event Collection and Processing Infrastructure	184
9.2.6	Common Characteristics of Existing Techniques	186
9.3	Overview and Case Study	187
9.3.1	Intrusion Scenario	188
9.3.2	System Auditing	188
9.4	Intrusion Analysis Framework	189
9.4.1	Information Extraction and Normalization	190
9.4.2	Event Correlation and Dependence Analysis	191
9.4.3	Simplification and Refinement	192
9.5	The SLog Declarative Programming Language	192
9.5.1	Language Constructs and Syntax	192
9.5.2	Semantics	194
9.6	Functional Evaluation	195
9.6.1	Collected Data	195
9.6.2	Usage and Results	195
9.7	Conclusion	196
	References	197
10	Automated Software Vulnerability Analysis	201
	Emre C. Sezer, Chongkyung Kil, and Peng Ning	
10.1	Introduction	201
10.2	Common Ground	203
10.3	MemSherlock: An Automated Debugger for Unknown Memory Corruption Vulnerabilities	203

- 10.3.1 Generating Write Sets 204
 - 10.3.2 Debugging Vulnerabilities 207
 - 10.3.3 Automated Debugging Using MemSherlock 209
- 10.4 CBones: Security Debugging Using Program Structural Constraints 211
 - 10.4.1 Program Structural Constraints 212
 - 10.4.2 Security Debugging through Constraints Verification ... 214
 - 10.4.3 Extracting Constraints 216
 - 10.4.4 Runtime Monitoring 216
 - 10.4.5 Security Debugging Using CBones 217
- 10.5 Comparison 218
- 10.6 Conclusion 219
- References 219

Part VI The Machine Learning Aspect

- 11 Machine Learning Methods for High Level Cyber Situation Awareness** 227
 - Thomas G. Dietterich, Xinlong Bao, Victoria Keiser, and Jianqiang Shen
 - 11.1 Introduction 227
 - 11.2 The TaskTracer System 228
 - 11.2.1 Tracking the User’s Current Project 228
 - 11.2.2 Assisting the User 229
 - 11.2.3 Instrumentation 232
 - 11.3 Machine Learning for Project Associations 232
 - 11.3.1 The Email Tagger 232
 - 11.3.2 Project Switch Detector 234
 - 11.3.3 The Folder Predictor 238
 - 11.4 Discovering User Workflows 240
 - 11.4.1 Building the Information Flow Graph 242
 - 11.4.2 Mining the Information Flow Graph 242
 - 11.4.3 Recognizing Workflows 243
 - 11.4.4 Experimental Evaluation 243
 - 11.5 Discussion 245
 - 11.6 Concluding Remarks 246
 - References 246
- Author Index** 249

Cyber Situational Awareness

Issues and Research

Jajodia, S.; Liu, P.; Cohan, V.; Wang, C. (Eds.)

2010, XII, 252 p. 20 illus., Hardcover

ISBN: 978-1-4419-0139-2