

Contents

Aspects of Insider Threats	1
Christian W. Probst, Jeffrey Hunker, Dieter Gollmann, and Matt Bishop	
1 Introduction	1
2 Insiders and Insider Threats	2
2.1 Insider Threats	5
2.2 Taxonomies	6
3 Detection and Mitigation	7
4 Policies	9
5 Human Factors and Compliance	11
6 Conclusion	13
References	15
Combatting Insider Threats	17
Peter G. Neumann	
1 A Contextual View of Insiders and Insider Threats	17
2 Risks of Insider Misuse	20
2.1 Types of Insiders	20
2.2 Types of Insider Misuse	21
3 Threats, Vulnerabilities, and Risks	22
3.1 Relevant Knowledge and Experience	23
3.2 Exploitations of Vulnerabilities	24
3.3 Potential Risks Resulting from Exploitations	25
4 Countermeasures	25
4.1 Specification of Sound Policies for Data Gathering and Monitoring	27
4.2 Detection, Analysis, and Identification of Misuse	28
4.3 Desired Responses to Detected Anomalies and Misuses ..	29
5 Decomposition of Insider Misuse Problems	29
5.1 Stages of Development and Use	30
5.2 Extended Profiling Including Psychological and Other Factors	31

- 6 Requirements for Insider-Threat-Resistant High-Integrity Elections 33
- 7 Relevance of the Countermeasures to Elections 36
- 8 Research and Development Needs 39
- 9 Conclusions 40
- References 41
- Insider Threat and Information Security Management 45**
- Lizzie Coles-Kemp and Marianthi Theoharidou
- 1 Introduction 45
- 2 Definitions of Insider and the Relevance to Information Security Management 46
- 3 Risk and Insiderness 49
 - 3.1 The Importance of Organisational Culture and the Significance of Cultural Risks 51
 - 3.2 Fieldwork on Culture and the Insider Threat 51
- 4 The Structure of the ISMS and Traditional Information Security Management Responses to Insiderness 53
 - 4.1 Analysis - Turning an ISMS Inwards 54
 - 4.2 The Role of Operationalisation 55
- 5 Information Security Management Standards, Best Practice and the Insider Threat 56
 - 5.1 General Security Management Standards 56
 - 5.2 Guidelines Focused on the Management of the Insider Threat 57
 - 5.3 Analysis of the Contribution of Best Practice and Guidelines 60
- 6 Crime theories and insider threat 61
 - 6.1 Existing Connections between Crime Theories and Information Security Management 62
- 7 Implications of Crime Theories for ISMS Design 63
 - 7.1 Application of SCP to the ISO Control Domains 64
 - 7.2 Implications for ISMS Process Design 66
 - 7.3 Summary of Crime Theory Contribution 68
- 8 Conclusions 69
- References 70
- A State of the Art Survey of Fraud Detection Technology 73**
- Ulrich Flegel, Julien Vayssière, and Gunter Bitz
- 1 Introduction 73
 - 1.1 Data Analysis Methodology 74
- 2 Survey of Technology for Fraud Detection in Practice 76
 - 2.1 General Approaches for Intrusion and Fraud Detection .. 76
 - 2.2 State of the Art of Fraud Detection Tools and Techniques 78
- 3 Why Fraud Detection is not the Same as Intrusion Detection 80
- 4 Challenges for Fraud Detection in Information Systems 82
- 5 Summary 82

References 84

Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation 85
 Frank L. Greitzer and Deborah A. Frincke

- 1 Introduction 85
- 2 Background 88
- 3 Issues of Security and Privacy 91
- 4 Predictive Modeling Approach 94
- 5 Training Needs 106
- 6 Conclusions and Research Challenges 109
- 7 Acknowledgments 111
- References 111

A Risk Management Approach to the “Insider Threat” 115
 Matt Bishop, Sophie Engle, Deborah A. Frincke, Carrie Gates, Frank L. Greitzer, Sean Peisert, and Sean Whalen

- 1 Introduction 116
- 2 Insider Threat Assessment 117
 - 2.1 Example 120
 - 2.2 Summary 122
- 3 Access-Based Assessment 122
- 4 Psychological Indicator-Based Assessment 126
- 5 Application of Risk to System Countermeasures 130
 - 5.1 Example 133
 - 5.2 Summary 135
- 6 Conclusion 135
- References 135

Legally Sustainable Solutions for Privacy Issues in Collaborative Fraud Detection 139
 Ulrich Flegel, Florian Kerschbaum, Philip Miseldine, Ganna Monakova, Richard Wacker, and Frank Leymann

- 1 Introduction 139
- 2 Monitoring Modern Distributed Systems 140
 - 2.1 Evidence Model 142
- 3 Observing Fraudulent Service Behaviours 145
 - 3.1 Architectural Support 148
- 4 Introduction to the Legal Perspective 149
- 5 Basic Principles of Data Privacy Law 150
 - 5.1 A Set of Six Basic Rules 151
- 6 General Legal Requirements of Fraud Detection Systems 153
 - 6.1 Privacy Relevance of Fraud Detection Systems 154
 - 6.2 Necessary Data for Fraud Detection 154
 - 6.3 Transparency in the Fraud Detection Context 155
 - 6.4 Purpose Specification and Binding in Fraud Detection 155

- 6.5 Permissibility of Fraud Detection 155
- 6.6 Quality of Event Data 156
- 6.7 Security of Event Data 156
- 7 Technical Solutions for Privacy-respecting Fraud Detection 156
 - 7.1 Technical Requirements 157
 - 7.2 Lossless Information Reduction with Covered Data 161
 - 7.3 Lossy Information Reductions for Timestamps 161
- 8 Legal Improvements by Pseudonymizing Event Data 165
 - 8.1 Technical Description 165
 - 8.2 Privacy Relevance of Pseudonymized Event Data 166
 - 8.3 Strengthening the Data Privacy Official 167
 - 8.4 Disclosure With Legal Permission 167
 - 8.5 Data and System Security 168
- 9 Conclusion 168
- References 169

Towards an Access-Control Framework for Countering Insider Threats . 173

Jason Crampton and Michael Huth

- 1 Introduction 173
- 2 Motivation and related work 177
 - 2.1 Illustrative scenarios 177
 - 2.2 Definitions of insiders 179
 - 2.3 Access control 180
 - 2.4 The insider problem and access control 181
- 3 Trust, trustworthiness, and the insider problem 182
 - 3.1 Insiderness 183
 - 3.2 Trust management and risk assessment 183
 - 3.3 Pragmatics of identifying suspicious events 184
- 4 Toward a context- and insider-aware policy language 185
 - 4.1 Context and request predicates 186
 - 4.2 Requirements 186
 - 4.3 Policy transformations via declarative programming 187
 - 4.4 Discussion of requirements 188
 - 4.5 Policy transformations 189
 - 4.6 Risk- and trustworthiness-aware policy composition 190
- 5 Access-control architectures and the insider problem 191
- 6 Concluding remarks 192
- References 194

Monitoring Technologies for Mitigating Insider Threats 197

Brian M. Bowen, Malek Ben Salem, Angelos D. Keromytis, and Salvatore J. Stolfo

- 1 Introduction 197
- 2 Related Research 200
- 3 Threat Model - Level of Sophistication of the Attacker 201
- 4 Decoy Properties 202

- 5 Architecture 207
 - 5.1 Decoy Document Distributor 207
 - 5.2 SONAR 208
 - 5.3 Decoys and Network Monitoring 208
 - 5.4 Host-based Sensors 211
- 6 Concluding Remarks and Future Work 215
- References 217
- Insider Threat Specification as a Threat Mitigation Technique 219**
- George Magklaras and Steven Furnell
- 1 Introduction 219
 - 1.1 The Insider Threat Problem 220
- 2 Background 221
 - 2.1 The Common Intrusion Specification Language 221
 - 2.2 Panoptis 225
- 3 Insider Misuse Taxonomies and Threat Models 226
- 4 The Scope of the Insider Threat Prediction Specification Language 237
 - 4.1 The Domain Specific Language Programming Paradigm . 240
- 5 Conclusion..... 242
- References 242



<http://www.springer.com/978-1-4419-7132-6>

Insider Threats in Cyber Security

Probst, C.W.; Hunker, J.; Bishop, M.; Gollmann, D. (Eds.)

2010, XII, 244 p., Hardcover

ISBN: 978-1-4419-7132-6