

Table of Contents

- The Insider Attack Problem Nature and Scope..... 1**
 - 1 Introduction 1
 - 2 Types of Attack 1
 - 2.1 Misuse of Access 1
 - 2.2 Defense Bypass 2
 - 2.3 Access Control Failure 2
 - 3 Defend or Detect 3
 - 4 The Role of Process 4
 - 5 Conclusion 4
- Reflections on the Insider Threat..... 5**
 - 1 Introduction 5
 - 2 Who Is an Insider? 6
 - 2.1 Motive 6
 - 2.2 Effect 7
 - 2.3 Defining the Insider Threat..... 8
 - 2.4 Context 8
 - 3 Insider Threat Issues 9
 - 3.1 Data 9
 - 3.2 Psychology 10
 - 3.3 Monitoring and Privacy 12
 - 3.4 Detecting Insider Attacks 13
 - 3.5 Technology 13
 - 4 Conclusions 14
 - Acknowledgments 15
- The “Big Picture” of Insider IT Sabotage Across U.S. Critical Infrastructures..... 17**
 - 1 Introduction 19
 - 2 General Observations About Insider IT Sabotage 20
 - 3 Model of the Insider IT Sabotage Problem 24
 - 3.1 Insider Expectation Escalation 25
 - 3.2 Escalation of Disgruntlement 26
 - 3.3 Attack Setup and Concealment..... 27
 - 3.4 The Trust Trap 28
 - 4 Possible Leverage Points for Addressing the Problem 29
 - 4.1 Early Mitigation Through Expectation Setting..... 29
 - 4.2 Handling Disgruntlement Through Positive Intervention..... 30
 - 4.3 Targeted Monitoring..... 31
 - 4.4 Eliminating Unknown Access Paths..... 32
 - 4.5 Measures Upon Demotion or Termination 34
 - 5 A Workshop on Insider IT Sabotage 35

5.1	The Instructional Case	36
6	Conclusion	39
6.1	Value of Modeling for Insight	40
6.2	Related CERT Research	41
	Acknowledgments	43
	Appendix A: System Dynamics Background	45
	Appendix B: The Insider IT Sabotage Training Case	48
1	Introduction.....	48
1.1	Background.....	48
1.2	The Final Weeks	50
	Appendix C: Model of the Insider IT Sabotage Problem.....	52
	Appendix D: Insider Sabotage Mitigating Measures	52
	Data Theft: A Prototypical Insider Threat.....	53
1	Introduction.....	53
1.1	Data Theft.....	53
1.2	Data Leakage	54
1.3	Risk.....	54
1.4	Recommendations	55
2	Status Quo.....	55
2.1	History	55
2.2	Risks & Controls	55
3	Recommendations.....	61
3.1	Technical Controls.....	61
3.2	Administrative Controls.....	64
3.3	Areas for Further Research.....	66
4	Conclusions.....	67
	Acknowledgments	67
	A Survey of Insider Attack Detection Research	69
1	Introduction.....	69
2	Insider Attacks.....	72
3	Detecting Insider Attacks.....	73
3.1	Host-based User Profiling.....	73
3.2	Network-Based Sensors.....	81
3.3	Integrated Approaches.....	82
3.4	Summary.....	83
4	Future Research Directions.....	85
5	Conclusion	87
	Naive Bayes as a Masquerade Detector: Addressing a Chronic Failure	91
1	Introduction.....	91
2	Related Work	92
3	Background on Naive Bayes.....	94
4	Objective and Approach	94

5	Experiment With Synthetic Data	95
5.1	Variable Selection	95
5.2	Synthetic Data	97
5.3	Experiment Control	99
5.4	Procedure.....	99
5.5	Results and Analysis.....	100
6	Naive Bayes Mathematical Formulation	101
6.1	Calculating the Anomaly Score.....	101
6.2	Manipulating the Anomaly Score.....	103
6.3	Effect of NBSCs	105
7	Exploiting NBSCs to Cloak Attacks.....	106
8	Naive Bayes Fortification	107
8.1	The Fortified Detector	107
8.2	Evaluation Methodology	108
8.3	Evaluation Results and Analysis	109
9	Discussion.....	110
10	Conclusion.....	111
 Towards a Virtualization-enabled Framework for Information		
Traceability (VFIT).....		113
1.	Introduction	114
2.	Threat Model and Requirements.....	114
3.	Background.....	116
3.1.	Models of Policy Enforcement.....	116
3.2.	Hardware Virtualization	117
4.	System Architecture.....	117
4.1.	Platform Architecture	118
4.2.	Network Architecture	119
5.	Implementation.....	120
5.1.	Virtualization-enabled Information Tracing.....	121
6.	Analysis	124
6.1.	Performance Discussion	125
6.2.	Threat Mitigation.....	126
7.	Related Work.....	126
8.	Conclusion	129
Acknowledgments		129
 Reconfigurable Tamper-resistant Hardware Support Against Insider		
Threats: The Trusted ILLIAC Approach.....		133
1	Introduction	133
2	Software-based Transparent Runtime Randomization	135
3	Tamper-resistant Key-store Support for Threshold Cryptography	137
3.1	Crypto-engine Architecture	138
3.2	Security Analysis.....	139
4	Information Flow Signature Checking for Data Integrity.....	140

4.1	Threat Model	141
4.2	Approach	141
4.3	Implementation	143
5	System Architecture Including the Trusted Computing Engine	144
5.1	Protecting Against Insider Attack With User-level Privileges: Runtime Guarantees	146
5.2	Protecting Against Insider Attack with Administrative Privileges: Initialization and Runtime Guarantees	147
6	Conclusions and Future Directions	149
Surviving Insider Attacks: A Call for System Experiments		153
1	Introduction.....	153
2	Principles for Survivability	155
2.1	Avoidance of a Single Point of Failure.....	156
2.2	Independence of Failure Modes and Attack Vulnerabilities	157
2.3	Fast Recovery from Failure and Attack	158
2.4	Attack Deterrence	159
2.5	Least Privilege Authorization	160
3	Cost Factors	161
4	Conclusion: A Call for Research and Development Experiments	161
Preventative Directions For Insider Threat Mitigation Via Access Control		165
1	Introduction.....	165
2	Definitions and Threat Model	168
2.1	The Insider	168
2.2	Types of Insiders	169
2.3	Damage of Insider Attacks	169
2.4	Threat Model	170
3	Background and Primitives.....	171
3.1	Authentication and Authorization.....	171
3.2	Access Control Principles.....	172
3.3	MAC, DAC, and Intermediate Schemes.....	172
3.4	Users and Groups.....	173
3.5	Roles and Role Engineering	174
3.6	Public Key Cryptography	174
4	Requirements	175
4.1	Functionality	175
4.2	Usability and Cost	176
4.3	Scale and Complexity	178
4.4	Domain Considerations	179
5	Tools	181
5.1	Passwords: Knowledge-Based Authentication	181
5.2	Biometrics: Physiology-Based Authentication	182
5.3	Tokens: Possession-Based Authentication	183
5.4	PKI: Authentication via Digital Certificates.....	184

5.5	Distributed Authentication and Identity Management.....	185
5.6	Distributed Authorization.....	186
6	Ongoing Challenges.....	188
6.1	A Snapshot of a Motion Picture	189
6.2	Privilege Issuance and Review	189
6.3	Auditing and Visualization.....	190
6.4	Role Drift and Escalation	190
6.5	Expressiveness and Need to Know.....	191
6.6	Incentives.....	191
7	Conclusions	191
	Acknowledgments	192
Taking Stock and Looking Forward – An Outsider’s Perspective on the Insider Threat.....		195
1	Introduction	196
2	What Is An “Insider Threat”?	198
3	How Does The Research Community Get Better Data?	201
3.1	Changing the Incentives that Organizations Face.....	205
3.2	Integrating Technical Solutions with Social Science Perspectives.....	209
3.3	Creating a Response and Recovery System for Insider Threats ..	211
4	Conclusion	213
Research Challenges for Fighting Insider Threat in the Financial Services Industry.....		215
1	Introduction	215
2	Employee Screening And Selection	216
3	Access Controls	217
4	Monitoring And Detection.....	218
Hard Problems and Research Challenges Concluding Remarks.....		219
Index		223

<http://www.springer.com/978-0-387-77321-6>

Insider Attack and Cyber Security

Beyond the Hacker

Stolfo, S.J.; Bellovin, S.M.; Hershkop, S.; Keromytis, A.D.;

Sinclair, S.; Smith, S. (Eds.)

2008, XII, 223 p. 20 illus., Hardcover

ISBN: 978-0-387-77321-6