

CONTENTS IN DETAIL

ACKNOWLEDGMENTS	xv
------------------------	-----------

INTRODUCTION	xvii
---------------------	-------------

1		
AN OVERVIEW OF INFORMATION VISUALIZATION		1

Why Information Visualization?	2
Preattentive Processing	4
Data Types	4
Categorical, Ordinal, and Interval Data Types	6
Hierarchical Data	7
Graph (Network) Data	9
Graphical Layout Techniques	9
Using Starplots to Visualize Multivariate Data	10
Small Multiples	11
Focus + Context	12
Interaction Techniques	12
The Visual Information–Seeking Mantra	14
Interacting with Objects and Controls	16
Conclusions	20

2		
THE BEAUTY OF BINARY FILE VISUALIZATION		21

Identifying Data Files and Executable Files	21
Seeing the Structure of a Text File	22
Using Color to Enhance the Picture	24
Using Carriage Returns and Line Feeds to See the Semantic Structure	25
Comparing Human and Machine Processing	25
Creating Smart Books	26
Dissecting the Security Behavior of a Microsoft Word Document	29
Using Multiple Columns to Display Large Documents	32
Conclusions	34

3		
PORT SCAN VISUALIZATION		35

Networking Overview	36
Internet Protocol Hierarchy	36
Visualizing Port Scans	44
Mapping Packet Data to Visualizations	44
Viewing Packet Header Data Using a Parallel Coordinate Plot Visualization	44

Visualizing a Port Scan	45
Overcoming Occlusion Through Zooming.....	46
Quickly Assessing Header Fields	51
Comparing the Visual Fingerprints of Nmap and Unicornscan	55
Visualization of Network Scanning Output	56
Conclusions.....	58

4 VULNERABILITY ASSESSMENT AND EXPLOITATION 59

Nessus.....	60
Dissecting a Nessus Vulnerability Assessment.....	61
Using a Packet Length Visualization	62
Finding and Removing the Port Scan.....	63
Animating Packets	65
Exploring the Remaining Activity	66
Identifying the Specific Ports	68
Metasploit.....	72
Choosing an Exploit	73
Choosing a Payload	74
Executing the Attack	75
Determining the Source and Destination Sockets.....	76
Analyzing the Initial Exploitation and Follow-up Activity	78
Stepping Through the Attack	79
Conclusions.....	81

5 ONE NIGHT ON MY ISP 83

Analyzing the ISP Dataset	84
Big-Picture Analysis.....	84
Analyzing and Removing Slices of Traffic	92
Conclusions.....	104

6 A SURVEY OF SECURITY VISUALIZATION 105

Visualizing the Global Spread of the Sony Rootkit.....	106
Analyzing Antivirus Effectiveness.....	108
Monitoring Widespread Network Attacks Using Distributed Sensors	111
Analyzing Process-to-Process Communication.....	112
Analyzing Sanitized Data Using Visualization	113
Exploring Packet Byte Structure	114
Using 3D Visualization to Map Attacks to Physical Location and Organizational Mission	117
Using Multiple Views of Security Data to Gain Insight	119
Using Extended Timelines to Observe Honeynet Trends.....	120
Detecting Intrusion and Misuse on Large-Scale Networks.....	122
Monitoring Intrusion Detection Alerts on an Enterprise Network	124
Conclusions.....	124

7	FIREWALL LOG VISUALIZATION	127
Link Graphs.....		128
The Link Graph Generation Process.....		132
1. Define Objective		132
2. Identify Data Fields.....		133
3. Map Data to Graph Nodes.....		133
4. Define Color Mappings.....		137
5. Iteratively Filter.....		138
6. Iteratively Aggregate		139
Outbound Traffic Analysis with Firewall Logs.....		140
Analyzing Firewall Logs.....		140
Interpreting Firewall Graphs		142
Wrapping Up.....		145
Hypothesis-based Firewall Log Analysis		145
Conclusions.....		148
8	INTRUSION DETECTION LOG VISUALIZATION	149
Intrusion Detection Signature Tuning with TreeMaps.....		150
Constructing TreeMaps of IDS Data.....		152
Analyzing TreeMaps.....		153
Signature Tuning Process.....		154
Source-based Analysis		156
Destination-centric Analysis.....		157
Alert Threshold Analysis.....		158
Conclusions.....		159
9	ATTACKING AND DEFENDING VISUALIZATION SYSTEMS	161
Study Failure in Order to Succeed.....		163
Attacking a Security Visualization System.....		163
Labeling Attacks.....		164
Occlusion Attacks.....		166
Windshield Wiper Attacks.....		167
Autoscale Attacks.....		169
Round-Off Attacks.....		170
Other Graphical Attacks.....		173
Attacking Data.....		174
Attack Constraints.....		175
Defending Your System.....		175
Provide Diverse Visualization Windows.....		175
Protect Your Data		176
Design Your System with Security in Mind.....		176
Train Users to Be Alert for Attack.....		177
Apply Secure Coding Practices		177
Provide Powerful Filtering Mechanisms.....		177
Conclusions.....		181

10 **CREATING A SECURITY VISUALIZATION SYSTEM** **183**

Analyze Your Users and Their Tasks	184
Review All Datastreams.....	185
Assess Available Technology	187
Design Dataflow, Visualizations, and Interaction	188
Dataflow Design	189
Visualization Design	190
Interaction Design.....	191
Build the System.....	193
Test and Evaluate the System	194
Generate Documentation	195
Conclusions.....	195

11 **UNEXPLORED TERRITORY** **197**

New Challenges	197
Security Visualization in the IPv6 Era	198
Keeping Up with the Data	198
Malicious Visualization	199
New Areas to Explore	200
Visual Cryptanalysis	200
Reverse Engineering of Software	202
Security Visualization in the Classroom	204
The Network Operations Center of the Future	204
Visualization for Offensive Tools.....	204
Metadata Analysis.....	205
Wireless Security Visualization.....	205
VoIP Security.....	205
Spam Analysis	205
Database Security	206
Webserver Security	206
(lm)mobile Device Security.....	206
Game Platform Security.....	206
Memory Visualization and Analysis	207
Application Layer Visualization Support	207
Outbound Data Flow Monitoring.....	207
Visualization for End Users	208
New Solutions to Try	208
Bridge to Machine Processing	208
Build a Security Visualization Community	210
Conduct Formal Evaluation	212
Generate Graphical Reports	212
Unify Security Datastreams	214
Improve Filtering	214
Passively Identify Attackers	214
Try Crossing Disciplinary Boundaries	215

12		
TEACHING YOURSELF		217
General Information Visualization	218	
Classic Information Visualization Books	218	
Classic Information Visualization Research Papers	219	
Security Visualization	220	
Open Source Security Visualization Applications.....	221	
Security Visualization Coverage in Books	225	
Human-Computer Interaction	225	
Computer Security	226	
Hacker Conferences	227	
Security Tools and Datasets	227	
CONCLUSION		229
INDEX		231