

CONTENTS

	PREFACE	xi
1	PSYCHOLOGICAL SECURITY TRAPS <i>by Peiter “Mudge” Zatko</i>	1
	Learned Helplessness and Naïveté	2
	Confirmation Traps	10
	Functional Fixation	14
	Summary	20
2	WIRELESS NETWORKING: FERTILE GROUND FOR SOCIAL ENGINEERING <i>by Jim Stickley</i>	21
	Easy Money	22
	Wireless Gone Wild	28
	Still, Wireless Is the Future	31
3	BEAUTIFUL SECURITY METRICS <i>by Elizabeth A. Nichols</i>	33
	Security Metrics by Analogy: Health	34
	Security Metrics by Example	38
	Summary	60
4	THE UNDERGROUND ECONOMY OF SECURITY BREACHES <i>by Chenxi Wang</i>	63
	The Makeup and Infrastructure of the Cyber Underground	64
	The Payoff	66
	How Can We Combat This Growing Underground Economy?	71
	Summary	72
5	BEAUTIFUL TRADE: RETHINKING E-COMMERCE SECURITY <i>by Ed Bellis</i>	73
	Deconstructing Commerce	74
	Weak Amelioration Attempts	76
	E-Commerce Redone: A New Security Model	83
	The New Model	86
6	SECURING ONLINE ADVERTISING: RUSTLERS AND SHERIFFS IN THE NEW WILD WEST <i>by Benjamin Edelman</i>	89
	Attacks on Users	89
	Advertisers As Victims	98

	Creating Accountability in Online Advertising	105
7	THE EVOLUTION OF PGP'S WEB OF TRUST <i>by Phil Zimmermann and Jon Callas</i>	107
	PGP and OpenPGP	108
	Trust, Validity, and Authority	108
	PGP and Crypto History	116
	Enhancements to the Original Web of Trust Model	120
	Interesting Areas for Further Research	128
	References	129
8	OPEN SOURCE HONEYCLIENT: PROACTIVE DETECTION OF CLIENT-SIDE EXPLOITS <i>by Kathy Wang</i>	131
	Enter Honeyclients	133
	Introducing the World's First Open Source Honeyclient	133
	Second-Generation Honeyclients	135
	Honeyclient Operational Results	139
	Analysis of Exploits	141
	Limitations of the Current Honeyclient Implementation	143
	Related Work	144
	The Future of Honeyclients	146
9	TOMORROW'S SECURITY COGS AND LEVERS <i>by Mark Curphey</i>	147
	Cloud Computing and Web Services: The Single Machine Is Here	150
	Connecting People, Process, and Technology: The Potential for Business Process Management	154
	Social Networking: When People Start Communicating, Big Things Change	158
	Information Security Economics: Supercrunching and the New Rules of the Grid	162
	Platforms of the Long-Tail Variety: Why the Future Will Be Different for Us All	165
	Conclusion	168
	Acknowledgments	169
10	SECURITY BY DESIGN <i>by John McManus</i>	171
	Metrics with No Meaning	172
	Time to Market or Time to Quality?	174
	How a Disciplined System Development Lifecycle Can Help	178
	Conclusion: Beautiful Security Is an Attribute of Beautiful Systems	181
11	FORCING FIRMS TO FOCUS: IS SECURE SOFTWARE IN YOUR FUTURE? <i>by Jim Routh</i>	183
	Implicit Requirements Can Still Be Powerful	184
	How One Firm Came to Demand Secure Software	185
	Enforcing Security in Off-the-Shelf Software	190
	Analysis: How to Make the World's Software More Secure	193
12	OH NO, HERE COME THE INFOSECURITY LAWYERS! <i>by Randy V. Sabett</i>	199

	Culture	200
	Balance	202
	Communication	207
	Doing the Right Thing	211
13	BEAUTIFUL LOG HANDLING	213
	<i>by Anton Chuvakin</i>	
	Logs in Security Laws and Standards	213
	Focus on Logs	214
	When Logs Are Invaluable	215
	Challenges with Logs	216
	Case Study: Behind a Trashed Server	218
	Future Logging	221
	Conclusions	223
14	INCIDENT DETECTION: FINDING THE OTHER 68%	225
	<i>by Grant Geyer and Brian Dunphy</i>	
	A Common Starting Point	226
	Improving Detection with Context	228
	Improving Perspective with Host Logging	232
	Summary	237
15	DOING REAL WORK WITHOUT REAL DATA	239
	<i>by Peter Wayner</i>	
	How Data Translucency Works	240
	A Real-Life Example	243
	Personal Data Stored As a Convenience	244
	Trade-offs	244
	Going Deeper	245
	References	246
16	CASTING SPELLS: PC SECURITY THEATER	247
	<i>by Michael Wood and Fernando Francisco</i>	
	Growing Attacks, Defenses in Retreat	248
	The Illusion Revealed	252
	Better Practices for Desktop Security	257
	Conclusion	258
	CONTRIBUTORS	259
	INDEX	269