

Introduction to Cyberdeception

Neil C. Rowe • Julian Rrushi

Introduction to Cyberdeception

 Springer

Neil C. Rowe
US Naval Postgraduate School
Monterey, CA, USA

Julian Rrushi
Western Washington University
Bellingham, WA, USA

ISBN 978-3-319-41185-9 ISBN 978-3-319-41187-3 (eBook)
DOI 10.1007/978-3-319-41187-3

Library of Congress Control Number: 2016943730

© Springer International Publishing Switzerland 2016

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

*To Suzanne, who is only occasionally
deceptive.*

—NCR

*To the national hero of Albania, George
Castriot, aka Skanderbeg, whose skills in
deception helped protect his homeland and
the entire Europe from Ottoman conquest.*

—JR

Preface

We need new ideas in information security. This book offers a set of interrelated ideas about using deception as a framework for attack and defense of computer systems and networks, and mostly defense. Contrary to popular belief, deception is not always bad and can be a useful tool in cyberspace. Much activity is occurring in regard to cyberdeception, so we try to convey some understanding of what is going on.

This book is intended as an introduction to cyberdeception and can be used in a classroom or for independent study. The intended audience is people who deal with cybersystems in one way or another, especially programmers and people focusing on information security and information assurance. But it also includes managers and policymakers who need to understand the options.

We realize that this book may seem a little cynical. We prefer to think of it as realistic. Deception, like war, is ubiquitous in human society, and it is important to address the world as it is, not as we want it to be. Will this book encourage deception and thus lead to a deterioration of societies? We think not, since there are plenty of books on crime and war, and they have not generally caused higher levels of crime and war. Understanding crime, war, and deception enables doing something about them.

We have tried to provide plenty of references to a variety of work on cyberdeception and supporting topics, for readers who want to further pursue particular topics. (All Rowe's publications are available at <http://faculty.nps.edu/ncrowe>.) They range from nontechnical to technical. Cyberdeception is an active field of research and development today, so new developments occur frequently. Most of the book does not assume the reader knows much about cybersystems other than the basics of software and architectures. However, the later chapters are more technical for readers who want more details, and appendices are available online to provide examples of implementations.

James Bret Michael and Richard Riehle got us interested in studying cyberdeception. Especially helpful have been Barton Whaley, Dorothy Denning, Paul Thompson, and Glenn Fink. Partial funding for this work has been provided by the U.S. National Science Foundation under the Cyber Trust program.

Monterey, CA
Bellingham, WA

Neil C. Rowe
Julian Rrushi

Contents

1	Introduction.....	1
1.1	Deception as a Third Line of Defense	2
1.2	Terminology	3
1.3	Why Deceive in Cyberspace?	3
1.4	Goals of Cyberdeception.....	4
1.5	Deception Occurs Everywhere	5
1.6	Are You Overconfident About Being Fooled?	6
1.7	Is Deception Ethical?	6
1.8	Plan of the Book.....	7
	References.....	8
2	Psychology of Deception	9
2.1	Definitions of Deception	9
2.2	The Spectrum of Deception	10
2.3	The Sociology of Trust.....	11
2.4	Detecting Deception.....	12
2.5	Other Factors in Designing Good Deceptions	15
2.5.1	Providing Independent Evidence	15
2.5.2	Consistency.....	16
2.5.3	Deception by Commission Versus Deception by Omission	16
2.5.4	Confirmability of a Deception	17
2.5.5	Cognitive Limitations	17
2.5.6	Emotional Manipulation	18
2.5.7	Active Methods of Detecting Deception.....	18
2.5.8	Individual Differences in Susceptibility to Deception.....	18
2.5.9	Exploiting Self-Deception	20
2.5.10	Groupthink	20
2.6	Conclusions.....	20
2.7	Exercises	21
	References.....	22

3 Professional Deception	25
3.1 Military Deception	26
3.1.1 The Role of Deception in Military Activities	27
3.1.2 Principles of Military Deception	28
3.1.3 Counterintelligence	29
3.2 Stage Magic	30
3.2.1 Practices of Stage Magic	30
3.2.2 The Importance of a Narrative	32
3.2.3 Psychology for Magic	33
3.2.4 Minimization of Deception	33
3.3 Marketing	34
3.3.1 Types of Marketing and Their Deceptions	34
3.3.2 Deceptive Marketing in Cyberspace	35
3.3.3 Deception with Software Marketing	36
3.4 Conclusions	37
3.5 Exercises	37
References	38
4 Deception Methods for Defense	39
4.1 Classic Deception Taxonomies	40
4.2 Military Taxonomies	40
4.3 A Taxonomy from Linguistic Case Theory	42
4.3.1 Linguistic-Case Deception Categories	42
4.3.2 Examples of the Deception Cases	44
4.3.3 Rating the Case-Grammar Defensive Deception Methods for Defense	45
4.3.4 An Example Putting the Deceptions Together	48
4.4 Second-Order Deceptions	48
4.5 Resource Deception	49
4.6 Deception Presentation Tactics	50
4.7 Conclusions	51
4.8 Exercises	51
References	52
5 Deception Methods for Offense	55
5.1 Motivation for Offensive Deception	56
5.2 The Options in Offensive Deception	56
5.3 Applying the Deception Taxonomy to Offense	59
5.4 The Ethics of Offensive Deception	61
5.5 Conclusions	61
5.6 Exercises	61
References	62
6 Delays	63
6.1 Why Delay Defensively?	64
6.2 Delaying Tactics	65
6.3 How Much to Delay	66

6.4	Example: Delays in a Web Portal	68
6.5	Unpredictable Delays.....	70
6.6	Cascading Delays.....	70
6.7	The Spectrum of Delays.....	71
6.8	Other Forms of Time Manipulation	72
6.9	Conclusions.....	72
6.10	Exercises	72
	References.....	73
7	Fakes.....	75
7.1	Other Possible Cyber-Fakes.....	76
7.2	A Grammar for Random Error Messages	77
7.3	A Stochastic Grammar for Directories.....	78
7.4	Building a Stochastic Grammar.....	83
7.5	Detail-Changing Tactics.....	85
7.6	Fighting Spam and Phishing with Fakes.....	86
7.7	Fake Software	87
7.8	Fake File Systems	87
7.9	Distribution of Fake Documents.....	90
7.10	Other Useful Fakes	91
7.11	Dynamic Fakes with Packet Manipulation	93
7.12	Inducing Paranoia	93
7.13	Conclusions.....	94
7.14	Exercises	94
	References.....	95
8	Defensive Camouflage	97
8.1	Hiding a Honeypot.....	97
8.2	Disguising the Operating Systems and Networks.....	99
8.3	Concealing Patches	100
8.4	Covert Channels and Steganography	100
8.5	Other Anti-Forensics Techniques.....	101
8.6	Conclusions.....	102
8.7	Exercises	102
	References.....	104
9	False Excuses	105
9.1	The Philosophy of Excuses.....	106
9.2	Types of False Excuses	107
9.3	Ensuring Logically Consistent Excuses.....	109
9.3.1	A Consistency Example	109
9.3.2	Generalizing Consistency Analysis.....	110
9.3.3	Inferences of Resource Facets.....	111
9.3.4	Implementing Excuse Checking	114
9.4	Rating Excuses.....	114
9.4.1	Prior Rate of an Excuse.....	115
9.4.2	Relaxing Consistency Over Time.....	115

9.4.3	Consistency Between Sessions	117
9.4.4	Putting Together the Rating Factors.....	117
9.5	Conclusions.....	117
9.6	Exercises	117
	References.....	118
10	Defensive Social Engineering.....	121
10.1	Tactics and Plans for Social-Engineering Deceptions	122
10.2	Techniques to Increase Likelihood of Accepting the Scam	123
10.3	Bait.....	125
10.4	More About Spyware	126
10.5	Reputation Scams.....	127
10.6	Hoaxes.....	127
10.7	Bureaucratic Games	128
10.8	Strategic Deception.....	129
10.9	Conclusions.....	130
10.10	Exercises	130
	References.....	130
11	Measuring Deception	133
11.1	Misuse Detection	134
11.2	Anomaly Detection	136
11.2.1	Anomaly Detection of Insider Threats.....	138
11.3	Bayesian Inference.....	139
11.3.1	Naive Bayes Inference	140
11.3.2	Examples of Naïve Bayes Inference.....	141
11.3.3	Obtaining Necessary Probabilities.....	142
11.3.4	Weighted Bayesian Inference.....	143
11.4	Coordinated Detection of Attackers.....	144
11.5	More About Deception Detection	145
11.6	Active Deception Detection with Probing	146
11.7	The Asymmetry of Trust and Distrust.....	147
11.8	More About Building Good Honeypots.....	147
11.8.1	Experiments with Detection of Manipulated Data.....	148
11.8.2	Building a Convincing Honeypot	149
11.8.3	Metadata of Typical File Systems	149
11.9	Clues to Deception in a File System	154
11.10	Conclusions.....	155
11.11	Exercises	155
	References.....	158
12	Planning Cyberspace Deception	161
12.1	Cost-Benefit Analysis of Deception.....	161
12.1.1	Analysis of a Single Defensive Deception.....	162
12.1.2	Analysis of Two-Stage Offensive Deception.....	164
12.1.3	Analysis of Two-Stage Defensive Deception	166
12.1.4	Analysis of a Fake Honeypot.....	167

12.2	Analysis of Propagation of Deceptions.....	169
12.3	Quantifying Tactics from the Deception Taxonomies	170
12.4	Counterplanning Against Attacks with Deception.....	171
12.4.1	Attack Plans	172
12.4.2	Tracking Attack Plans	176
12.4.3	Ploys for Counterplans.....	177
12.4.4	Greedy Counterplanning	179
12.4.5	Planning Multiple Deceptions.....	180
12.4.6	Ploy Presentation	181
12.4.7	Entropy Measurement of Deceptions.....	182
12.5	Conclusions.....	183
12.6	Exercises	183
	References.....	186
13	Software Engineering of Deceptive Software and Systems.....	189
13.1	Experimental deception	190
13.2	Deception architectures.....	190
13.3	Defensive Deceptive Firewalls	192
13.4	Low-Interaction Honeypots	194
13.4.1	Overview	194
13.4.2	Case Study: The Honeyd Honeypot.....	195
13.4.3	Case Study: A Deceptive Web Server with Honeyd	198
13.4.4	Case Study: A Deceptive Web Server with Glastopf	199
13.5	Implementing Simple Deceptions in Full-Interaction Honeypots	202
13.6	Server and Spam Honeypots.....	205
13.7	Honeypots Attacking Other Machines	205
13.8	Strategies for Deception Implementation	206
13.8.1	Hand-Coded Deceptions	206
13.8.2	Software Instrumentation with Wrappers	206
13.8.3	Deception Control Policies	208
13.8.4	Virtualization and Redirection	209
13.8.5	Deceptions in Hardware.....	210
13.9	Conclusions.....	211
13.10	Exercises	211
	References.....	212
14	Decoy I/O Devices	215
14.1	Motivation.....	216
14.2	Design Issues for Fake I/O Devices.....	216
14.2.1	Design details.....	217
14.2.2	Tactics for Decoy Devices	220
14.2.3	Hardware Support for Decoy Devices	221
14.2.4	Tracking Down Malicious Activity.....	222
14.3	Case Study: Decoy Network Interface Controller	223
14.3.1	Anti-Malware Testing.....	223
14.3.2	Results of Testing	224

14.3.3	More About Coexistence with Real NICs	226
14.4	Conclusions.....	228
14.5	Exercises	228
	References.....	229
15	Deception for the Electrical Power Industry	231
15.1	Simulating Electrical Power Plants.....	232
15.2	Building a Power-Plant Simulator	232
15.3	Mirage Architecture	233
15.4	Defense of Electrical Substations	235
15.4.1	Defensive Deception for Electrical Substations.....	235
15.5	Deception Engineering for a Real Example of Malware.....	236
15.5.1	Operation of Havex	236
15.5.2	Experiments with Havex	237
15.6	Conclusions.....	238
15.7	Exercises	238
	References.....	239
16	Law and Ethics for Software Deception	241
16.1	Applying Ethics to Cyberspace.....	241
16.1.1	Ethical-Climate Issues.....	243
16.1.2	Escalation of Distrust	243
16.1.3	Ensuring Minimal Harms	244
16.1.4	Privacy.....	244
16.1.5	Entrapment	245
16.1.6	Trespassing.....	245
16.1.7	Strategic Deception	245
16.2	Legal Issues in Deception	245
16.2.1	Fraud.....	246
16.2.2	Entrapment	246
16.2.3	Retaliation	247
16.2.4	International Law on Cyberattacks.....	247
16.3	Conclusions.....	248
16.4	Exercises	248
	References.....	249
	Chapter Photographs.....	251
	Appendix A: Fake Directory Generator	253
	Appendix B: Stochastic String Generator	267
	Appendix C: Resource-Deception Consistency Checker.....	273
	Appendix D: Rootkit Attack Planner	283
	Appendix E: Counterplanner for Attacks	319