

4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP



Syngress Force

Emerging Threat Analysis

FROM MISCHIEF TO MALICIOUS

- An Elite Group of Security Researchers Identifies the Most Up-to-Date Threats for IT Professionals
- Cutting-Edge Advice on Phishing, Spam, Identity Theft, Insider Threat, Tools Not to Be Ignored, and More

David Maynor

Lance James

Spammer-X

Tony Bradley

Frank Thornton

Brad Haines

Brian Baskin

Anand Das

Hersh Bhargava

Jeremy Faircloth

Craig Edwards

Michael Gregg

Ron Bandes

VISIT US AT

www.syngress.com

Syngress is committed to publishing high-quality books for IT Professionals and delivering those books in media and formats that fit the demands of our customers. We are also committed to extending the utility of the book you purchase via additional materials available from our Web site.

SOLUTIONS WEB SITE

To register your book, visit www.syngress.com/solutions. Once registered, you can access our solutions@syngress.com Web pages. There you may find an assortment of value-added features such as free e-booklets related to the topic of this book, URLs of related Web site, FAQs from the book, corrections, and any updates from the author(s).

ULTIMATE CDs

Our Ultimate CD product line offers our readers budget-conscious compilations of some of our best-selling backlist titles in Adobe PDF form. These CDs are the perfect way to extend your reference library on key topics pertaining to your area of expertise, including Cisco Engineering, Microsoft Windows System Administration, CyberCrime Investigation, Open Source Security, and Firewall Configuration, to name a few.

DOWNLOADABLE E-BOOKS

For readers who can't wait for hard copy, we offer most of our titles in downloadable Adobe PDF form. These e-books are often available weeks before hard copies, and are priced affordably.

SYNGRESS OUTLET

Our outlet store at syngress.com features overstocked, out-of-print, or slightly hurt books at significant savings.

SITE LICENSING

Syngress has a well-established program for site licensing our e-books onto servers in corporations, educational institutions, and large organizations. Contact us at sales@syngress.com for more information.

CUSTOM PUBLISHING

Many organizations welcome the ability to combine parts of multiple Syngress books, as well as their own content, into a single volume for their own internal use. Contact us at sales@syngress.com for more information.

SYNGRESS®

Syngress Force

Emerging Threat Analysis

FROM MISCHIEF TO MALICIOUS

David Maynor
Lance James
Spammer-X
Tony Bradley
Frank Thornton
Brad Haines
Brian Baskin
Thomas Porter

Anand M. Das
Hersh Bhargava
Jeremy Faircloth
Craig Edwards
Michael Gregg
Ron Bandes
Paul Piccard

Syngress Publishing, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively “Makers”) of this book (“the Work”) do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

Syngress Media®, Syngress®, “Career Advancement Through Skill Enhancement®,” “Ask the Author UPDATE®,” and “Hack Proofing®,” are registered trademarks of Syngress Publishing, Inc. “Syngress: The Definition of a Serious Security Library”™, “Mission Critical™,” and “The Only Way to Stop a Hacker is to Think Like One™” are trademarks of Syngress Publishing, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

KEY SERIAL NUMBER

001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	893BYYYY789
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY

Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

Syngress Force Emerging Threat Analysis: From Mischief to Malicious

Copyright © 2006 by Syngress Publishing, Inc. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Printed in Canada.

1 2 3 4 5 6 7 8 9 0

ISBN: 1-59749-056-3

Publisher: Andrew Williams
Cover Designer: Michael Kavish

Page Layout and Art: Patricia Lupien
Indexer: Richard Carlson

Distributed by O’Reilly Media, Inc. in the United States and Canada.

For information on rights, translations, and bulk sales, contact Matt Pedersen, Director of Sales and Rights, at Syngress Publishing; email matt@syngress.com or fax to 781-681-3585.



Acknowledgments

Syngress would like to acknowledge the following people for their kindness and support in making this book possible.

Syngress books are now distributed in the United States and Canada by O'Reilly Media, Inc. The enthusiasm and work ethic at O'Reilly are incredible, and we would like to thank everyone there for their time and efforts to bring Syngress books to market: Tim O'Reilly, Laura Baldwin, Mark Brokering, Mike Leonard, Donna Selenko, Bonnie Sheehan, Cindy Davis, Grant Kikkert, Opol Matsutaro, Steve Hazelwood, Mark Wilson, Rick Brown, Tim Hinton, Kyle Hart, Sara Winge, C. J. Rayhill, Peter Pardo, Leslie Crandell, Regina Aggio, Pascal Honscher, Preston Paull, Susan Thompson, Bruce Stewart, Laura Schmier, Sue Willing, Mark Jacobsen, Betsy Waliszewski, Kathryn Barrett, John Chodacki, Rob Bullington, Aileen Berg, and Wendy Patterson.

The incredibly hardworking team at Elsevier Science, including Jonathan Bunkell, Ian Seager, Duncan Enright, David Burton, Rosanna Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Beran, Emma Wyatt, Chris Hossack, Krista Leppiko, Marcel Koppes, Judy Chappell, Radek Janousek, and Chris Reinders for making certain that our vision remains worldwide in scope.

David Buckland, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, Pang Ai Hua, Joseph Chan, and Siti Zuraidah Ahmad of STP Distributors for the enthusiasm with which they receive our books.

David Scott, Tricia Wilden, Marilla Burgess, Annette Scott, Andrew Swaffer, Stephen O'Donoghue, Bec Lowe, Mark Langley, and Anyo Geddes of Woodslane for distributing our books throughout Australia, New Zealand, Papua New Guinea, Fiji, Tonga, Solomon Islands, and the Cook Islands.



Contributing Authors

David Maynor is a Senior Researcher with SecureWorks where his duties include vulnerability development, developing and evaluating new evasion techniques, and development of protection for customers. His previous roles include reverse engineering and researching new evasion techniques with the ISS Xforce R&D team, application development at the Georgia Institute of Technology, as well as security consulting, penetration testing and contracting with a wide range of organizations.

Lance James has been heavily involved with the information security community for the past 10 years. With over a decade of experience with programming, network security, reverse engineering, cryptography design & cryptanalysis, attacking protocols and a detailed expertise in information security, Lance provides consultation to numerous businesses ranging from small start-ups, governments, both national and international, as well as Fortune 500's and America's top financial institutions. He has spent the last three years devising techniques to prevent, track, and detect phishing and online fraud. He is a lead scientist with Dachb0den Laboratories, a well-known Southern California "hacker" think-tank, creator of InvisibleNet, a prominent member of the local 2600 chapter, and the Chief Scientist with Secure Science Corporation, a security software company that is busy tracking over 53 phishing groups. As a regular speaker at numerous security conferences and being a consistent source of information by various news organizations, Lance James is recognized as a major asset in the information security community.

Brad “RenderMan” Haines is one of the more visible and vocal members of the wardriving community, appearing in various media outlets and speaking at conferences several times a year. Render is usually near by on any wardriving and wireless security news, often causing it himself. His skills have been learned in the trenches working for various IT companies as well as his involvement through the years with the hacking community, sometimes to the attention of various Canadian and American intelligence agencies. A firm believer in the hacker ethos and promoting responsible hacking and sharing of ideas, he wrote the ‘Stumbler ethic’ for beginning wardrivers and greatly enjoys speaking at corporate conferences to dissuade the negative image of hackers and wardrivers. His work frequently borders on the absurd as his approach is usually one of ignoring conventional logic and just doing it. He can be found in Edmonton, Alberta, Canada, probably taking something apart.

Thomas Porter, Ph.D. (CISSP, IAM, CCNP, CCDA, CCNA, ACE, CCSA, CCSE, and MCSE) is the Lead Security Architect in Avaya’s Consulting & Systems Integration Practice. He also serves as Director of Network Security for the FIFA World Cup 2006.

Porter has spent over 10 years in the networking and security industry as a consultant, speaker, and developer of security tools. Porter’s current technical interests include VoIP security, development of embedded microcontroller and FPGA Ethernet tools, and H.323/SIP vulnerability test environments. He is a member of the IEEE and OASIS (Organization for the Advancement of Structured Information Standards). Porter recently published Foundation articles for SecurityFocus titled “H.323 Mediated Voice over IP: Protocols, Vulnerabilities, and Remediation”; and “Perils of Deep Packet Inspection.”

Tom lives in Chapel Hill, North Carolina with his wife, Kinga – an Asst. Professor of Internal Medicine at the University of North Carolina – and two Chesapeake Bay Retrievers.

Brian Baskin [MCP, CTT+] is a researcher and developer for Computer Sciences Corporation, on contract to the Defense Cyber Crime Center's (DC3) Computer Investigations Training Program (DCITP). Here, he researches, develops, and instructs computer forensic courses for members of the military and law enforcement. Brian currently specializes in Linux/Solaris intrusion investigations, as well as investigations of various network applications. He has designed and implemented networks to be used in scenarios, and has also exercised penetration testing procedures.

Brian has been instructing courses for six years, including presentations at the annual DoD Cyber Crime Conference. He is an avid amateur programmer in many languages, beginning when his father purchased QuickC for him when he was 11, and has geared much of his life around the implementations of technology. He has also been an avid Linux user since 1994, and enjoys a relaxing terminal screen whenever he can. He has worked in networking environment for over 10 years from small Novell networks to large, mission-critical, Windows-based networks

Brian lives in the Baltimore, MD area with his lovely wife and son. He is also the founder, and president, of the Lightning Owners of Maryland car club. Brian is a motor sports enthusiast and spends much of his time building and racing his vehicles. He attributes a great deal of his success to his parents, who relinquished their household 80286 PC to him at a young age, and allowed him the freedom to explore technology.

Tony Bradley (CISSP-ISSAP) is the Guide for the Internet/Network Security site on About.com, a part of The New York Times Company. He has written for a variety of other Web sites and publications, including *PC World*, SearchSecurity.com, WindowsNetworking.com, *Smart Computing* magazine, and *Information Security* magazine. Currently a security architect and consultant for a Fortune 100 company, Tony has driven security policies and technologies for antivirus and incident response for Fortune

500 companies, and he has been network administrator and technical support for smaller companies.

Tony is a CISSP (Certified Information Systems Security Professional) and ISSAP (Information Systems Security Architecture Professional). He is Microsoft Certified as an MCSE (Microsoft Certified Systems Engineer) and MCSA (Microsoft Certified Systems Administrator) in Windows 2000 and an MCP (Microsoft Certified Professional) in Windows NT. Tony is recognized by Microsoft as an MVP (Most Valuable Professional) in Windows security.

On his About.com site, Tony has on average over 600,000 page views per month and 25,000 subscribers to his weekly newsletter. He created a 10-part Computer Security 101 Class that has had thousands of participants since its creation and continues to gain popularity through word of mouth. Aside from his Web site and magazine contributions, Tony is also coauthor of *Hacker's Challenge 3* (ISBN: 0072263040) and a contributing author to *Winternals: Defragmentation, Recovery, and Administration Field Guide* (ISBN: 1597490792) and *Combating Spyware in the Enterprise* (ISBN: 1597490644).

Jeremy Faircloth (Security+, CCNA, MCSE, MCP+I, A+, etc.) is an IT Manager for EchoStar Satellite L.L.C., where he and his team architect and maintain enterprisewide client/server and Web-based technologies. He also acts as a technical resource for other IT professionals, using his expertise to help others expand their knowledge. As a systems engineer with over 13 years of real-world IT experience, he has become an expert in many areas, including Web development, database administration, enterprise security, network design, and project management. Jeremy has contributed to several Syngress books, including *Microsoft Log Parser Toolkit* (Syngress, ISBN: 1932266526), *Managing and Securing a Cisco SWAN* (ISBN: 1-932266-91-7), *C# for Java Programmers* (ISBN: 1-931836-54-X), *Snort 2.0 Intrusion Detection* (ISBN: 1-931836-74-4), and *Security+ Study Guide & DVD Training System* (ISBN: 1-931836-72-8).

Paul Piccard serves as Director of Threat Research for Webroot, where he focuses on research and development, and provides early identification, warning, and response services to Webroot customers. Prior to joining Webroot, Piccard was manager of Internet Security Systems' Global Threat Operations Center. This state-of-the-art detection and analysis facility maintains a constant global view of Internet threats and is responsible for tracking and analyzing hackers, malicious Internet activity, and global Internet security threats on four continents.

His career includes management positions at VistaScape Security Systems, Lehman Brothers, and Coopers & Lybrand. Piccard was researcher and author of the quarterly Internet Risk Impact Summary (IRIS) report. He holds a Bachelor of Arts from Fordham University in New York.

Frank Thornton runs his own technology consulting firm, Blackthorn Systems, which specializes in wireless networks. His specialties include wireless network architecture, design, and implementation, as well as network troubleshooting and optimization. An interest in amateur radio helped him bridge the gap between computers and wireless networks. Having learned at a young age which end of the soldering iron was hot, he has even been known to repair hardware on occasion. In addition to his computer and wireless interests, Frank was a law enforcement officer for many years. As a detective and forensics expert he has investigated approximately one hundred homicides and thousands of other crime scenes.

Combining both professional interests, he was a member of the workgroup that established ANSI Standard "ANSI/NIST-CSL 1-1993 Data Format for the Interchange of Fingerprint Information." He co-authored *WarDriving: Drive, Detect, and Defend: A Guide to Wireless Security* (Syngress Publishing, ISBN: 1-93183-60-3), as well as contributed to *IT Ethics Handbook: Right and Wrong for IT Professionals* (Syngress, ISBN: 1-931836-14-0) and *Game Console Hacking: Xbox, PlayStation, Nintendo, Atari, & Gamepark 32* (ISBN: 1-931836-31-0). He resides in Vermont with his wife.

Anand Das has seventeen plus years of experience creating and implementing business enterprise architecture for the Department of Defense (DOD) and the commercial sector. He is founder and CTO of Commerce Events, an enterprise software corporation that pioneered the creation of RFID middleware in 2001. Anand is a founding member of EPCglobal and INCITS T20 RTLS committee for global RFID and wireless standards development. He formulated the product strategy for AdaptLink™, the pioneer RFID middleware product, and led successful enterprise wide deployments including a multi-site rollout in the Air Force supply chain. Previously he was Vice President with SAIC where he led the RFID practice across several industry verticals and completed global rollouts of RFID infrastructure across America, Asia, Europe and South Africa. He served as the corporate contact for VeriSign and played a key role in shaping the EPCglobal Network for federal and commercial corporations. Earlier, he was chief architect at BEA systems responsible for conceptualizing and building the Weblogic Integration suite of products. He has been a significant contributor to ebXML and RosettaNet standard committees and was the driving force behind the early adoption of service-oriented architecture. Anand has held senior management positions at Vitria, Tibco, Adept, Autodesk and Intergraph.

Anand has Bachelor of Technology (Honors) from IIT Kharagpur and Master of Science from Columbia University with specialization in computer integrated manufacturing. He served as the past chairman of NVTC's ebusiness committee and is a charter member of TIE Washington, DC. Anand and his wife, Annapurna, and their two children live in Mclean, VA.

Michael Gregg is the President of Superior Solutions, Inc. and has more than 20 years' experience in the IT field. He holds two associate's degrees, a bachelor's degree, and a master's degree and is certified as CISSP, MCSE, MCT, CTT+, A+, N+, Security+, CNA, CCNA, CIW Security Analyst, CCE, CEH, CHFI, CEI, DCNP, ES Dragon IDS, ES Advanced Dragon IDS, and TICSA.

Michael's primary duties are to serve as project lead for security assessments helping businesses and state agencies secure their IT resources and assets. Michael has authored four books, including: *Inside Network Security Assessment*, *CISSP Prep Questions*, *CISSP Exam Cram2*, and *Certified Ethical Hacker Exam Prep2*. He has developed four high-level security classes, including Global Knowledge's Advanced Security Boot Camp, Intense School's Professional Hacking Lab Guide, ASPE's Network Security Essentials, and Assessing Network Vulnerabilities. He has created over 50 articles featured in magazines and Web sites, including *Certification Magazine*, GoCertify, *The El Paso Times*, and SearchSecurity.

Michael is also a faculty member of Villanova University and creator of Villanova's college-level security classes, including Essentials of IS Security, Mastering IS Security, and Advanced Security Management. He also serves as a site expert for four TechTarget sites, including SearchNetworking, SearchSecurity, SearchMobileNetworking, and SearchSmallBiz. He is a member of the TechTarget Editorial Board.

Hersh Bhargava is the founder and CTO of RafCore Systems, a company that provides RFID Application Development and Analytics platform. He is the visionary behind RafCore's mission of making enterprises respond in real-time using automatic data collection techniques that RFID provides. Prior to RafCore Systems, he founded AlbumNet Technologies specializing in online photo sharing and printing. With 15 years of experience in building enterprise strength application, he has worked in senior technical positions for Fortune 500 companies. He earned a Bachelor of Technology in Computer Science and Engineering from IIT - BHU.

Craig Edwards is the administrator for the ChatSpike IRC network and creator of the IRC security software IRC Defender (www.ircdefender.org). IRC Defender is a security service that

keeps malicious users and programs out of IRC networks and is actively maintained to deal with current threats. Craig is also the creator of the WinBot IRC bot (www.winbot.co.uk), an automated IRC client which is designed to keep control of IRC channels, and has been instrumental in its design, maintenance, and support and web site for over five years. During this time it has been published on magazine cover CDs in the United Kingdom.

Ronald T. Bandes (CISSP, CCNA, MCSE, Security+) is an independent security consultant. Before becoming an independent consultant, he performed security duties for Fortune 100 companies such as JP Morgan, Dun and Bradstreet, and EDS. Ron holds a B.A. in Computer Science.

Contents

Foreword	xxix
Part I VoIP	1
Chapter 1 Threats to VoIP Communications Systems . . .	3
Introduction	4
Denial-of-Service or VoIP Service Disruption	4
Call Hijacking and Interception	12
ARP Spoofing	15
H.323-Specific Attacks	20
SIP-Specific Attacks	21
Summary	22
Solutions Fast Track	23
Frequently Asked Questions	25
Chapter 2 Validate Existing Security Infrastructure for VoIP	27
Introduction	28
Security Policies and Processes	29
Physical Security	41
Perimeter Protection	43
Closed-Circuit Video Cameras	43
Token System	44
Wire Closets	45
Server Hardening	45
Eliminate Unnecessary Services	46
Logging	47
Permission Tightening	48
Additional Linux Security Tweaks	51
Activation of Internal Security Controls	53
Security Patching and Service Packs	57
Supporting Services	58
DNS and DHCP Servers	58
LDAP and RADIUS Servers	60

NTP	.61
SNMP	.61
SSH and Telnet	.62
Unified Network Management	.63
Sample VoIP Security Policy	.64
Purpose	.64
Policy	.65
Physical Security	.65
VLANs	.65
Softphones	.65
Encryption	.65
Layer 2 Access Controls	.66
Summary	.67
Solutions Fast Track	.68
Frequently Asked Questions	.70
Chapter 3 Recommendations for VoIP Security	.73
Introduction	.74
Reuse Existing Security Infrastructure Wisely	.75
Security Policies and Processes	.75
Physical Security	.76
Server Hardening	.77
Supporting Services	.78
Combine Network Management Tools and Operations	.78
Confirm User Identity	.79
802.1x and 802.11i	.81
Public Key Infrastructure	.81
Active Security Monitoring	.82
NIDS and HIDS	.82
Logging	.83
Penetration and Vulnerability Testing	.83
Logically Segregate VoIP from Data Traffic	.84
VLANs	.84
QoS and Traffic Shaping	.86
Firewalls	.86
NAT and IP Addressing	.88
Access Control Lists	.88

Encryption	89
Regulations	89
Summary	91
Of Layers, Compartments, and Bulkheads	91
Specific Recommendations	91
Solutions Fast Track	94
Frequently Asked Questions	100
Chapter 4 Skype Security.	103
Introduction	104
Skype Architecture	105
Features and Security Information	107
Instant Messaging	107
Encryption	108
Chat History	109
Skype Calls(Voice Chat)	109
Group Chat	110
File Transfer	112
Malicious Code	113
Client Security	114
Summary	117
Solutions Fast Track	118
Frequently Asked Questions	120
Part II Malware.	123
Chapter 5 The Transformation of Spyware	125
Introduction	126
The Humble Beginnings	126
Targeted Marketing	126
Hitting the Internet Target	128
Selling Software	128
Adware Evolves	129
Making a Name for Itself	131
All Roads Lead to Microsoft	131
The Making of a Buzzword	131
The Early Effects of Spyware	131
Early Means of Prevention	132

Spyware in the Twenty-First Century	134
How Spyware Has Evolved	134
Increased Use of Spyware in the Commission of Criminal Acts	135
Antispyware Legislation	136
The Future of Spyware	138
Summary	139
Solutions Fast Track	139
Frequently Asked Questions	141
Chapter 6 Spyware and the Enterprise Network	143
Introduction	144
Keystroke Loggers	145
How Keystroke Loggers Work	146
Known Keystroke Loggers	149
KeyGhost	149
KEYKatcher/KEYPhantom	150
Invisible KeyLogger Stealth	151
Spector	151
Boss EveryWhere	152
Known Exploits	153
Trojan Encapsulation	155
How Spyware Works with Trojan Horses	155
Known Spyware/Trojan Software	157
D1Der	157
Sony Digital Rights Management	157
Kazanon	158
Spyware and Backdoors	159
How Spyware Creates Backdoors	159
Known Spyware/Backdoor Combinations	160
A Wolf in Sheep's Clothing: Fake Removal Tools	162
Summary	164
Solutions Fast Track	164
Frequently Asked Questions	165
Chapter 7 Global IRC Security	167
Introduction	168
DDoS Botnets Turned Bot-Armies	168

Methods of Botnet Control	169
Reprisals	172
The ipbote Botnet: A Real World Example	173
Information Leakage	175
Copyright Infringement	176
Other Forms of Infringement	176
Transfer of Malicious Files	179
How to Protect Against Malicious File Transfers	181
What to Do if a Malicious File Infects Your Network	182
Prevention of Malicious File Sends in the Client	182
DCC Exploits	182
Firewall/IDS Information	183
Port Scans	183
IDS	183
Summary	185
Solutions Fast Track	185
Frequently Asked Questions	187

Chapter 8 Forensic Detection and Removal of Spyware 189

Introduction	190
Manual Detection Techniques	190
Working with the Registry	190
Registry Basics	191
Start-Up Applications	193
File Association Hijacking	195
Detecting Unknown Processes	196
Researching Unknown Processes	199
Detecting Spyware Remnants	202
Temporary File Caches	202
Windows System Restore	203
Windows File Protection	205
Windows Hosts File	205
Internet Explorer Settings	207
Detection and Removal Tools	208
HijackThis	208
Reviewing HijackThis Results	210

Reviewing a HijackThis Sample Log	213
Removing Detected Items	218
HijackThis Miscellaneous Tools	219
a ² HiJackFree	220
InstallWatch Pro	223
Performing a Scan with the InstallWatch Pro Wizard	225
Performing a Scan without the InstallWatch Pro Wizard	228
Reviewing InstallWatch Pro Results	228
Unlocker	230
VMware	232
Snapshots	235
Enterprise Removal Tools	235
BigFix Enterprise Suite	235
FaceTime	238
Websense Web Security Suite	238
Summary	240
Solutions Fast Track	242
Frequently Asked Questions	243
Part III Phishing and Spam.	245
Chapter 9 Go Phish!.	247
Introduction	248
The Impersonation Attack	250
The Mirror	250
Setting Up the Phishing Server	254
Setting Up the Blind Drop	259
Preparing the Phishing E-Mail	262
Preparing the Con	266
Results	270
The Forwarding Attack	270
E-Mail Preparation	271
The Phishing Server and the Blind Drop	273
Preparing the Con	274
Results	276

The Popup Attack	276
Setting Up the Phishing Server	278
E-Mail Preparation	281
Preparing the Con	282
Results	285
Summary	286
Solutions Fast Track	286
Frequently Asked Questions	288
Chapter 10 E-Mail: The Weapon of Mass Delivery . . .	289
Introduction	290
E-Mail Basics	290
E-Mail Headers	290
Mail Delivery Process	294
Anonymous E-Mail	299
Forging Our Headers	302
Open Relays and Proxy Servers	303
Proxy Chaining, Onion Routing, and Mixnets	306
E-mail Address Harvesting	310
Harvesting Tools, Targets, and Techniques	311
Hackers and Insiders	320
Sending Spam	320
The Tools of the Trade	321
The Anti-Antispam	323
Summary	329
Solutions Fast Track	330
Frequently Asked Questions	332
Chapter 11 How Spam Works	335
Who Am I?	336
The Business of Spam	336
Spam in the Works: A Real-World Step-by-Step Example	338
Setting the Stage	340
The E-mail Body	342
Chapter 12 Sending Spam	349
The Required Mindset to Send Spam	350
Methods of Sending Spam	351
Proxy Servers	351

Simple Mail Transfer Protocol Relays	355
Spam-Sending Companies	357
Botnets	358
Internet Messenger Spam	364
Messenger Spam	366
Common Gateway Interface Hijacking	368
Wireless Spam	375
BGP Hijacking and Stealing IP blocks	377
Chapter 13 Your E-mail: Digital Gold	383
What Does Your E-mail Address Mean to a Spammer?	384
Hackers and Spammers: Their United Partnership	386
Harvesting the Crumbs of the Internet	389
Network News Transfer Protocol	390
Internet Relay Chat Harvesting	392
whois Database	393
Purchasing a Bulk Mailing List	395
Mass Verification	397
Inside Information	402
Chapter 14 Creating the Spam Message and Getting It Read	405
Jake Calderon? Who Are You?	406
How to Sell a Product	407
Formats and Encoding	411
Plaintext Encoding	411
Rich Text	413
HTML	413
Collecting Hidden Data	416
Unsubscribe and Opt-out Links	417
Random Data	420
Hosting Content	422
HTML Injection and Hijacking	424
Part IV RFID	431
Chapter 15 RFID Attacks: Tag Encoding Attacks	433
Introduction	434
Case Study: John Hopkins vs. SpeedPass	434

The SpeedPass	434
Breaking the SpeedPass	438
The Johns Hopkins Attack	441
Lessons to Learn	443
Summary	445
Chapter 16 RFID Attacks: Tag Application Attacks . . .	447
MIM	448
Chip Clones—Fraud and Theft	448
Tracking: Passports/Clothing	453
Passports	455
Chip Cloning > Fraud	457
Disruption	459
Summary	460
Chapter 17 RFID Attacks: Securing	
Communications Using RFID Middleware	461
RFID Middleware Introduction	462
Electronic Product Code System Network Architecture	462
EPC Network Software Architecture Components . . .	462
Readers	463
RFID Middleware	463
EPC Information Service	464
Object Name Service	464
ONS Local Cache	464
EPC Network Data Standards	464
EPC	465
PML	465
RFID Middleware Overview	465
Reader Layer—Operational Overview	467
Smoothing and Event Generation Stage	470
Event Filter Stage	471
Report Buffer Stage	471
Interactions with Wireless LANs	471
802.11 WLAN	472
Attacking Middleware with the Air Interface	473

- [download online Unbalanced: A View from the Vestibule Schizophrenia and Hyperattention](#)
- [download Theories in Second Language Acquisition: An Introduction \(2nd Edition\) here](#)
- [download Morito pdf, azw \(kindle\), epub, doc, mobi](#)
- [The Real Jerk: New Caribbean Cuisine pdf, azw \(kindle\), epub](#)

- <http://jaythebody.com/freebooks/Warriors--Extraordinary-Tales-from-the-Battlefield.pdf>
- <http://patrickvincitore.com/?ebooks/Agricola--Germany--and-Dialogue-on-Orators.pdf>
- <http://wind-in-herleshausen.de/?freebooks/Writing-Reviews-for-Readers--Advisory.pdf>
- <http://www.1973vision.com/?library/Adventures-in-Solitude--What-Not-to-Wear-to-a-Nude-Potluck-and-Other-Stories-from-Desolation-Sound.pdf>