

# Mobile Malware Attacks and Defense

**The Only Book for Analyzing and Mitigating Mobile Malicious Code!**

- Understand the History and Threat Landscape of Rapidly Emerging Mobile Attacks
- Analyze Mobile Device/Platform Vulnerabilities and Exploits
- Mitigate Current and Future Mobile Malware Threats

**Ken Dunham, Technical Editor**

**Saeed Abu-Nimeh**

**Michael Becher**

**Seth Fogie**

**Brian Hernacki**

**Jose Andre Morales**

**Craig Wright**

# Mobile Malware Attacks and Defense

**Ken Dunham** Technical Editor

**Saeed Abu-Nimeh**

**Michael Becher**

**Seth Fogie**

**Brian Hernacki**

**Jose Andre Morales**

**Craig Wright**



E2009003583

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

#### Unique Passcode

28475016

PUBLISHED BY  
Syngress Publishing, Inc.  
Elsevier, Inc.  
30 Corporate Drive  
Burlington, MA 01803

#### Mobile Malware Attacks and Defense

Copyright © 2009 by Elsevier, Inc. All rights reserved. Printed in the United States of America. 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 the United States of America  
1 2 3 4 5 6 7 8 9 0

ISBN 13: 978-1-59749-298-0

Publisher: Laura Colantoni  
Acquisitions Editor: Brian Sawyer  
Technical Editor: Ken Dunham  
Developmental Editor: Gary Byrne  
Cover Designer: Michael Kavish

Page Layout and Art: SPI  
Copy Editor: Mike McGee  
Indexer: SPI  
Project Manager: Andre Cuello

For information on rights, translations, and bulk sales, contact Matt Pedersen, Commercial Sales Director and Rights, at Syngress Publishing; email [m.pedersen@elsevier.com](mailto:m.pedersen@elsevier.com).

#### Library of Congress Cataloging-in-Publication Data

Dunham, Ken.

Mobile malware attacks and defense / Ken Dunham  
p. cm.

ISBN 978-1-59749-298-0

1. Cellular telephone systems--Security measures. 2. Mobile communication systems--Security measures.  
3. Mobile computing--Security measures. 4. Computer crimes--Prevention. 5. Computer crimes--Case studies.  
6. Computer hackers. 7. Wireless Internet--Security measures. I. Title.

TK5102.85.D86 2008  
005.8--dc22

2008042884

# Visit us at

[www.syngress.com](http://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, please visit [www.syngress.com](http://www.syngress.com). Once registered, you can access your e-book with print, copy, and comment features enabled.

## **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 e-book format. These are available at [www.syngress.com](http://www.syngress.com).

## **SITE LICENSING**

Syngress has a well-established program for site licensing our e-books onto servers in corporations, educational institutions, and large organizations. Please contact our corporate sales department at [corporatesales@elsevier.com](mailto:corporatesales@elsevier.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. Please contact our corporate sales department at [corporatesales@elsevier.com](mailto:corporatesales@elsevier.com) for more information.



# Technical Editor

**Ken Dunham** (CISSP, GSEC, GREM, GCFA, GCIH Gold Honors) has more than a decade of experience on the frontlines of information security. As director of global response for iSIGHT Partners, he oversees all global cyber-threat response operations. He frequently briefs upper levels of federal and private-sector cyber security authorities on emerging threats, and he regularly interfaces with vulnerability and geopolitical experts to assemble comprehensive malicious code intelligence and to inform the media of significant cyber threats. A major media company identified Mr. Dunham as the top quoted global malicious code expert in 2006.

Mr. Dunham regularly discovers new malicious code, has written antivirus software for Macintosh, and has written about malicious code for About.com, SecurityPortal, AtomicTangerine, Ubizen, iDEFENSE, and VeriSign. He is one of the pioneers of Internet community antivirus support with Web sites rated as the best global resource by *Yahoo Internet Life*, *PC Week*, AOL, and many others. Mr. Dunham is a member of the High Technology Crime Investigation Association (HTCIA), Government Emergency Telecommunications and Wireless Priority Service, AVIEN, Virus Bulletin, InfraGard, an RCG Information Security Think Tank, CME, and many other private information-sharing channels. Mr. Dunham also participated in the CIA Silent Horizon (blue team) and DHS CyberStorm (observer) exercises.

Mr. Dunham is a certified reverse engineer and regularly analyzes emergent exploits and malicious code threats and actors targeting client networks. He also works as a Wildlist Reporter each month with the Wildlist organization. He is the author of several books and is a regular columnist for an information security magazine. Mr. Dunham is also the founder of the Boise Idaho Information Systems Security Association (ISSA) and Idaho InfraGard chapters.

*Ken wrote Chapters 1, 2, 3 and 6 (the introduction, visual payloads, timeline threats, and vishing).*



# Contributing Authors

**Saeed Abu-Nimeh** is a Ph.D. candidate at Southern Methodist University. His research focuses on network and e-mail security. He is interested in studying phishing and pharming attacks and spends his time developing solutions to thwart electronic identity theft and protect mobile users against various types of attacks. He is a member of IEEE, the Anti-Phishing Working Group (APWG), and SMU High Assurance Computing and Networking (HACNet) Lab.

*Saeed wrote Chapter 6 (Phishing, Smishing, and Vishing).*

**Michael Becher** received his master's degree in computer science in the year 2006 from RWTH Aachen University of Technology, Germany. He is currently a Ph.D. candidate at the University of Mannheim, Germany, researching on the security of mobile devices like smartphones, sponsored by mobile network operator T-Mobile. One of Michael's main research topics is dynamic analysis of mobile malware and software in general.

Michael worked on several topics in the security area previously, where he authored an article about direct memory access in FireWire and a book about Web application firewalls.

*Michael wrote Chapter 8 (Analyzing Mobile Malicious Code).*

**Seth Fogie** is the VP of Dallas-based Aircanner Corporation, where he oversees the development of security software for the Windows Mobile (Pocket PC) platform. He has coauthored numerous technical books on information security, including the best-selling *Maximum Wireless Security* and *Windows Internet Security: Protecting Your Critical Data* from Sams Publishing, *Security Warrior* from O'Reilly, and *Cross Site Scripting Attacks: XSS Exploits and Defense* from Syngress. Seth frequently speaks at IT and security conferences/seminars, including Black Hat, Defcon, CSI, and Dallascon. In addition, Seth has coauthored the HIPAA medical education course

for the Texas Medical Associate and is acting site host for security for InformIT.com, where he writes articles and reviews/manages weekly information security-related books and articles.

*Seth wrote Chapter 7 (Operating System and Device Vulnerabilities) and Chapter 10 (Debugging and Disassembly of MM).*

**Brian Hernacki** is an architect in Symantec Research Labs, where he works with a dedicated team to develop future technologies. Hernacki has more than 10 years of experience with computer security and enterprise software development. He has conducted research and commercial product development in a number of security areas, including intrusion detection and analysis techniques, honeypots, and wireless and mobile technologies. Hernacki earned a bachelor's degree in computer engineering, with honors, from the University of Michigan.

*Brian wrote Chapter 11 (Mobile Malicious Code Mitigation Measures).*

**Jose Andre Morales** is a Ph.D. graduate in computer science from Florida International University in the research area of computer virus detection based on identifying self-replication. He focuses on detecting viruses in mobile devices and develops antivirus solutions. He is a member of Sigma Xi, Upsilon Phi Epsilon, ACM and IEEE. He is also the cofounder of the Computing Hispanic Ph.D. Mailing List.

*Jose wrote Chapters 3 (Timeline of Mobile Malicious Code, Hoaxes, and Threats), 4 (Overview of Malicious Mobile Code Families), and 5 (Taxonomy of Mobile Malicious Code).*

**Craig Wright** is associate director, risk advisory services at BDO Kendalls (NSW-VIC) Pty. Ltd. He has authored numerous IT security-related articles and books. He also has designed the architecture for the world's first online casino (Lasseter's Online) in the Northern Territory. He designed and managed the implementation of many of the systems that protect the Australian Stock Exchange as well as the security policies and procedural practices within Mahindra and Mahindra, India's largest

vehicle manufacturer. The Mahindra group employs over 50,000 people in total and has numerous business interests from car to tractor manufacturing to IT outsourcing. Craig is one of the few people with a GSE certification and the first in the compliance stream. He has 27 GIAC certifications and is working on his eighth GIAC Gold paper.

*Craig wrote Chapter 9 (Forensic Analysis of Mobile Malicious Code).*





# Acknowledgments/Contributors

The authors of this book want to thank multiple individuals, lists, and private sources within the computer security industry for their ongoing support and development of mobile malicious code products and services. The following individuals significantly contributed to content within this book as noted for each:

**Collin Mulliner** is a programmer, hacker, and a full-time security researcher. Collin's main area of research is the security of mobile devices and networks with a special emphasis on mobile and smartphones. In recent years Collin was doing a lot of research and development on Bluetooth. He created the first Bluetooth port scanner. Since 1997, Collin has done projects for most of the existing mobile device platforms. In 2006, Collin received a master's in computer science degree from the University of California, Santa Barbara.

*Collin wrote sections on MMS, Palm, and J2ME in Chapter 7.*

**Ralf Hund** is a master's candidate in mathematics and computer science at the University of Mannheim, Germany. As a student helper at the Laboratory for Dependable Distributed Systems, he has completed work that includes the development of a sandbox for the Windows Mobile platform. He has a special interest in practical aspects of IT security (e.g., software security, static malware analysis, and dynamic malware analysis).

Ralf has more than 10 years of experience in reverse engineering and programming on Windows and Linux operating systems, with a special focus on low-level details.

*Ralf wrote the technical sections of Chapter 8 on behavioral analysis of MMC.*

Additional individuals we would like to thank for helping in technical review include Mikko H. Hypponen, Fred Doyle, Joep Gommers, and Josh Murray.

# Contents

- Chapter 1 Introduction to Mobile Malware . . . . . 1**
- Introduction . . . . . 2
- Understanding Why Mobile Malware Matters Today . . . . . 3
- An Introduction to MM Threats . . . . . 6
- An Introduction to Mobile Security Terminology . . . . . 9
- Vectors for Spreading MM . . . . . 9
- Bluetooth . . . . . 10
- MMC . . . . . 10
- Multimedia Messaging Service (MMS) . . . . . 10
- HTTP . . . . . 10
- SMS . . . . . 10
- Attack Types . . . . . 11
- Hacking Defaults . . . . . 11
- Denial-of-Service (DoS) . . . . . 11
- Exploit . . . . . 11
- Bloover/II . . . . . 11
- Bluebug . . . . . 11
- BlueBump . . . . . 11
- BlueChop . . . . . 11
- BlueDump . . . . . 12
- Bluejacking . . . . . 12
- Blueprinting . . . . . 12
- BlueSmack . . . . . 12
- Bluesnarf/++ . . . . . 12
- BlueSniff . . . . . 12
- Bluetooone . . . . . 12
- Car Whispherer . . . . . 12
- HeloMoto . . . . . 13
- RedFang . . . . . 13
- Snarf . . . . . 13
- Warnibbling . . . . . 13
- MM Terms . . . . . 13
- Ad/Spyware . . . . . 13
- Mobile Malware . . . . . 13

Payload . . . . .	14
Rogue Software . . . . .	14
Trojan . . . . .	14
Virus . . . . .	14
Worm . . . . .	14
Summary . . . . .	15
Solutions Fast Track . . . . .	15
Frequently Asked Questions . . . . .	17
<b>Chapter 2 Visual Payloads . . . . .</b>	<b>19</b>
Introduction . . . . .	20
F-Secure RF Lab . . . . .	20
Identifying Visual Payloads of MM . . . . .	23
Cabir . . . . .	23
Skulls . . . . .	25
CommonWarrior . . . . .	29
BlankFont . . . . .	32
Summary . . . . .	33
Solutions Fast Track . . . . .	33
Frequently Asked Questions . . . . .	34
<b>Chapter 3 Timeline of Mobile Malware, Hoaxes, and Threats . . . . .</b>	<b>35</b>
Introduction . . . . .	36
Qualifying Fear, Uncertainty, and Doubt (FUD) in the Mobile Market . . . . .	36
Global Demand for Mobile Devices . . . . .	37
An Historical Timeline of MM . . . . .	38
Genesis (2004) . . . . .	55
Telefonica . . . . .	55
Epoc.Fake.A . . . . .	55
Hacktool.SMSDOS . . . . .	56
Worm.SymbOS.Cabir.A. . . . .	56
Virus.WinCE.Duts. . . . .	57
Backdoor.WinCE.Brador . . . . .	57
Trojan.Skulls.A . . . . .	57
Middle Ages (2005) . . . . .	58
Trojan.SymbOS.Cardtrap . . . . .	58
Trojan.SymbOS.PbStealer. . . . .	59
Industrial Era (2006–2007) . . . . .	59
Trojan.SMS.J2ME.RedBrowser . . . . .	59

Worm.MSIL.Cxover . . . . .	60
Trojan-Spy.SymbOS.Flexispy . . . . .	61
Worm.SymbOS.Mobler.A . . . . .	61
SymbOS.Viver.A . . . . .	62
Modern Times and Beyond (2008 – ) . . . . .	62
Trojan.iPhone.A . . . . .	62
WinCE.InfoJack.A . . . . .	63
Trojan.POC.MM.Gotcha.A . . . . .	63
Worm.POC.MM.Stranger.A . . . . .	64
Future Threats . . . . .	64
Summary . . . . .	67
Solutions Fast Track . . . . .	67
Frequently Asked Questions . . . . .	69
Notes . . . . .	70

## Chapter 4 Overview of Mobile Malware

<b>Families . . . . .</b>	<b>71</b>
Introduction . . . . .	72
Cabir . . . . .	72
Skuller . . . . .	78
Doomboot . . . . .	83
Cardtrap . . . . .	87
Summary . . . . .	90
Solutions Fast Track . . . . .	91
Frequently Asked Questions . . . . .	92

## Chapter 5 Taxonomy of Mobile Malware . . . . . 93

Introduction . . . . .	94
Infection Strategy . . . . .	95
Wireless Communication . . . . .	95
MMS . . . . .	95
Bluetooth . . . . .	99
E-mail . . . . .	102
Wired Communication . . . . .	103
Removable Storage . . . . .	103
Device-to-PC (D2P) Synchronization . . . . .	105
Other Infection Strategies . . . . .	106
SMS . . . . .	106
Wi-Fi . . . . .	107
OS Vulnerabilities . . . . .	107

Distribution . . . . .	108
Wireless Communication . . . . .	109
SMS . . . . .	109
Bluetooth . . . . .	112
Wired Communication . . . . .	113
Removable Storage . . . . .	113
Payload . . . . .	114
Communications Component . . . . .	114
Sending SMS Messages: Nuisance . . . . .	115
File System . . . . .	115
Infesting Files: Nuisance . . . . .	115
Overwriting Files: Nuisance . . . . .	115
Multimedia Components . . . . .	116
Taking Photos: Devious . . . . .	116
Recording Voices: Devious . . . . .	116
Clandestine Video Recorder: Devious . . . . .	116
Playback: Devious . . . . .	117
Telephone Component . . . . .	117
Dialing Other Phone: Nuisance . . . . .	117
Dialing Your Own Phone: Nuisance . . . . .	117
Using the Phone to Cover Your Tracks: Devious . . . . .	118
Data Farming . . . . .	118
Stealing Contacts: Devious . . . . .	118
Summary . . . . .	121
Solutions Fast Track . . . . .	121
Frequently Asked Questions . . . . .	123
<b>Chapter 6 Phishing, SMishing, and Vishing . . . . .</b>	<b>125</b>
Introduction to Phishing and Vishing . . . . .	126
Introduction to Phishing . . . . .	127
Phishing Mobile Devices . . . . .	130
Bluetooth Phishing . . . . .	131
SMS Phishing . . . . .	132
Voice over IP Phishing . . . . .	134
Breaking Phishing Filters via Pharming . . . . .	136
Introduction to Pharming . . . . .	137
Attack Details . . . . .	140
Attack Setup . . . . .	141
Hiding the Attack . . . . .	142
pf Firewall Rules . . . . .	143

Web Server vhost File . . . . .	143
The hosts.allow File. . . . .	143
Packet Capture Analysis . . . . .	144
The EarthLink Toolbar . . . . .	144
The Netcraft Toolbar . . . . .	146
SpoofGuard . . . . .	148
The Google Toolbar . . . . .	150
Internet Explorer. . . . .	152
Firefox . . . . .	153
The Opera Browser. . . . .	154
SpoofStick . . . . .	156
Attack Prevention. . . . .	157
IP Verification . . . . .	158
OpenDNS. . . . .	158
SSL and HTTPS . . . . .	158
Virtual Private Networks . . . . .	158
Web Proxies . . . . .	158
Applying Machine Learning for Phishing Detection . . . . .	159
Bayesian Additive Regression Trees . . . . .	160
Classification and Regression Trees . . . . .	161
Logistic Regression. . . . .	162
Neural Networks . . . . .	162
Random Forests . . . . .	163
Support Vector Machines . . . . .	163
Detecting Mobile Phishing Using a Distributed Framework. . . . .	164
Learning Phishing E-mails . . . . .	166
Data Standardization, Cleansing, and Transformation . . . . .	167
Textual Analysis . . . . .	170
Structural Analysis . . . . .	171
Experimental Studies . . . . .	174
Evaluation Metrics. . . . .	174
Experimental Setup . . . . .	175
Experimental Results . . . . .	176
Discussion . . . . .	179
An Introduction to Vishing. . . . .	180
How Can I Spot a Vishing Attack? . . . . .	181
Understanding Vishers' Tools and Techniques . . . . .	182
VoIP Server . . . . .	183
VoIP Phone Management Software. . . . .	184
Interactive Voice Management (IVM) Software . . . . .	184

Text-To-Speech (TTS) and Interactive Voice Recording (IVR) . . . . .	186
Outbound Calling . . . . .	187
Vishing Packs . . . . .	187
Mitigating Vishing Attacks . . . . .	188
Consumer Education . . . . .	188
Notifications . . . . .	189
Summary . . . . .	190
Solutions Fast Track . . . . .	190
Frequently Asked Questions . . . . .	194
Notes . . . . .	196

## Chapter 7 Operating System and Device

<b>Vulnerabilities . . . . .</b>	<b>197</b>
Introduction . . . . .	198
Windows Mobile . . . . .	198
WM Details . . . . .	199
File System . . . . .	199
Xip. . . . .	199
Encryption . . . . .	199
Code Signing . . . . .	200
Operating System . . . . .	200
Kernel Mode vs. User Mode . . . . .	200
Drivers . . . . .	201
Memory/Process Limitation . . . . .	201
Vulnerability Details . . . . .	202
Core Operating System . . . . .	202
KDataStruct . . . . .	202
Pocket IE . . . . .	203
Active Sync. . . . .	204
Bluetooth . . . . .	205
PocketPC MMS-Based Vulnerabilities . . . . .	205
The MMS Client . . . . .	205
PocketPC MMS Composer . . . . .	206
Code Execution via SMIL . . . . .	206
Shellcode Walkthrough . . . . .	207
Denial-of-Service via WAP Push and Wi-Fi . . . . .	208
Attack Details . . . . .	209
Bypassing Code-Signing Protections . . . . .	210
Installing Your Own Certificate . . . . .	210

Registry Hack . . . . .	211
Buffer Overflow vs. Code Signing . . . . .	211
Exploiting WM . . . . .	212
The Tools . . . . .	212
IDA Pro . . . . .	212
Visual Studio 2005 . . . . .	213
WM Applications . . . . .	213
The Process . . . . .	213
An Example - FlexWallet . . . . .	214
Setup . . . . .	214
Initial Analysis and Target Selection . . . . .	215
Probe Target . . . . .	216
Analyze Crash . . . . .	217
Building the Exploit . . . . .	219
iPhone . . . . .	222
iPhone System Details . . . . .	222
Operating System . . . . .	222
Applications . . . . .	223
Open Source Tool Chain . . . . .	225
Exploiting the iPhone . . . . .	225
iPhone Hacking . . . . .	225
The Jailbreak Process . . . . .	225
Exploit Details . . . . .	227
A Flawed Shell Model . . . . .	228
Root Account . . . . .	228
Static Addressing . . . . .	228
Static Systems . . . . .	228
Reuse of Old Code . . . . .	228
Metasploit . . . . .	229
An iPhone Exploit in Action . . . . .	229
Metasploit vs. libtiff . . . . .	231
Tool Tip - Iphonedbg . . . . .	234
Symbian . . . . .	234
Symbian Details . . . . .	234
File System . . . . .	235
Operating System . . . . .	235
Security . . . . .	235
Platform Security . . . . .	235
Code Signing . . . . .	236



Vulnerability Landscape for Symbian . . . . .	237
Warezed Installers. . . . .	237
Social Engineering. . . . .	239
BlackBerry . . . . .	240
BlackBerry Details . . . . .	241
BlackBerry Vulnerabilities . . . . .	241
General Security Issues. . . . .	242
BlackBerry Enterprise Server Issues . . . . .	242
BBProxy . . . . .	242
J2ME – Java 2 Micro Edition . . . . .	245
MIDlets – J2ME Applications . . . . .	245
J2ME Security . . . . .	245
MIDlet Permissions and Signing. . . . .	246
Past Vulnerabilities. . . . .	246
Siemens S55 Permission Request Race Condition . . . . .	247
KVM Buffer Overflow Vulnerability . . . . .	247
Current Vulnerabilities . . . . .	247
The Nokia 6131 NFC Silent MIDlet Installation Vulnerability. . . . .	247
PushRegistry Abuse on the Nokia 6131 NFC. . . . .	248
Other Notable Platforms . . . . .	248
Palm OS . . . . .	248
Palm OS Security . . . . .	249
The Palm OS Password Issue . . . . .	249
Palm OS Security Lock ByPass Vulnerabilities . . . . .	249
Palm OS Malware . . . . .	249
The LibertyCrack Trojan . . . . .	250
The Phage Virus . . . . .	250
The Vapor Trojan. . . . .	250
Linux. . . . .	250
Android . . . . .	250
Exploit Prevention . . . . .	252
WM Defense . . . . .	252
iPhone Defense . . . . .	252
J2ME Defense . . . . .	252
Symbian Defense . . . . .	253
Handheld Exploitation . . . . .	253
Wireless Attacks. . . . .	253
802.11 Wardriving . . . . .	253
802.11 Jamming . . . . .	256