The Mobile Application Hacker's Handbook

Dominic Chell
Tyrone Erasmus
Shaun Colley
Ollie Whitehouse

WILEY

The Mobile Application Hacker's Handbook

The Mobile Application Hacker's Handbook

Dominic Chell
Tyrone Erasmus
Shaun Colley
Ollie Whitehouse

WILEY

The Mobile Application Hacker's Handbook

Published by
John Wiley & Sons, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Published simultaneously in Canada

ISBN: 978-1-118-95850-6
ISBN: 978-1-118-95852-0 (ebk)
ISBN: 978-1-118-95851-3 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Library of Congress Control Number: 2014954689

I would like to dedicate this book to my wife Adele and thank her for her continued support not only whilst working on this book but throughout my career.

—Dominic

I would like to dedicate this book to Wendy, the love of my life. I cannot wait to spend my time with someone who understands me so well. You support me tirelessly in spite of me pursuing many time-consuming projects. You are owed many movie nights and a catch-up on time where I was absent while writing.

—Tyrone

I would like to dedicate this book to my parents, Jill and Andy, as well as my brother Dave, for all the support and encouragement they have given me over the years. My friends are also owed immensely for their support and friendship over the years.

—Shaun

I would like to dedicate this book to Ilma who for over a decade has kept the home fire burning whilst I've pursed my passion around the globe.

—Ollie

About the Authors

Dominic Chell is a cofounder of MDSec, where in addition to leading the mobile practice, he is responsible for delivering consultancy and training engagements for a variety of clients. Dominic's career has spanned over a decade and has been almost entirely focused on the technical aspects of application security. He has spoken at numerous conferences as well as releasing several publications on mobile security. Dominic is also listed as a subject matter expert for a secure iOS development exam.

Tyrone Erasmus has a degree in computer engineering and is currently the head of mobile security at MWR InfoSecurity South Africa. He enjoys delving into many different areas of penetration testing and security research, with a large portion of his research efforts in the past spent on Android. His interests lie predominantly in offensive security and the advancement of tools and new techniques in this sphere. He has spoken at various security conferences, and was part of the team that won the Android category at Mobile Pwn2Own in 2012. His work is acknowledged internationally in the Android hacking space, and he is known among peers as a well-rounded security professional.

Shaun Colley is a principal security consultant for IOActive where he focuses on mobile device security, native code review, and reverse engineering. During his career, he has been primarily focused on mobile security and reverse engineering. Shaun has also spoken several times at industry meets and conferences. He holds a BSc (Hons) in Chemistry from the University of Leeds, England.

Ollie Whitehouse is technical director for NCC Group, where he is responsible for Cyber Defence Operations, Managed Services, and its Exploit Development Group along technical innovation across the Technical Security Consulting practice. Ollie's career has spanned nearly two decades and included research, consultancy, and management positions at BlackBerry, Symantec, and @stake where he specialized in software, mobile, embedded, wireless, and telecommunications security.

About the Technical Editor

Rob Shimonski (`www.shimonski.com`) is a best-selling author and editor with over 15 years' experience developing, producing, and distributing print media in the form of books, magazines, and periodicals. To date, Rob has successfully created over 100 books that are currently in circulation. Rob has worked for countless companies to include CompTIA, Microsoft, Wiley, Cisco, the National Security Agency, and Digidesign.

Rob has over 20 years' experience working in IT, networking, systems, and security. He is a veteran of the US military and has been entrenched in security topics and assignments his entire professional career. In the military, Rob was assigned to a communications (radio) battalion supporting training efforts and exercises. Having worked with mobile phones since their inception, Rob is an expert in mobile phone development and security.

Credits

Executive Editor
Carol Long

Project Editor
Sydney Argenta

Technical Editor
Rob Shimonski

Production Editor
Rebecca Anderson

Copy Editor
Paula Lowell

Manager of Content Development and Assembly
Mary Beth Wakefield

Marketing Director
David Mayhew

Marketing Manager
Carrie Sherrill

Professional Technology and Strategy Director
Barry Pruett

Business Manager
Amy Knies

Associate Publisher
Jim Minatel

Project Coordinator, Cover
Patrick Redmond

Proofreader
Sarah Kaikini, Word One New York

Indexer
Johnna VanHoose Dinse

Cover Designer
Wiley

Cover Image
Clockwork gears © iStock.com/ Ryhor Bruyeu; App icon © iStock.com/ -cuba-

Acknowledgments

Firstly, Dominic would like to thank the other authors for their hard work in developing this book; without their contributions it would have been too big a mountain to climb! Dominic would also like to acknowledge the support of his colleagues from MDSec, in particular Marcus Pinto, Dan Brown, Ryan Chell, and Matthew Hickey who worked tirelessly to pick up the slack whilst he was writing this book. He would also like to highlight the great work that the wider security community has done in this field and which provided a foundation for him to expand his knowledge—where applicable, this work has been properly referenced in this book. Dominic is also indebted to the numerous individuals that he has had the pleasure of working with through the years and from who he learnt so much, including Dafydd Stuttard, John Heasman, Peter Winter-Smith, Adam Matthews, Sherief Hammad, and the rest of the team at the old NGS Software. Finally, Dominic would like to thank his parents for everything that they have done and continue to do; their support has been invaluable over the years.

Tyrone would like to acknowledge Daniel and the rest of the team at MWR for tinkering alongside him on Android and sharing their knowledge, as well as Riaan and Harry for supporting him through his career. He would also like to acknowledge his family and friends who keep an active interest in his life and reminded him that there is life beyond his computer screen. Finally, Tyrone would like to thank Dominic for contacting him out of the blue to be a part of the author team!

Shaun would like to thank all the authors of this book in helping to make it a reality; who knows where the idea for this book would be without them. Shaun would also like to thank his colleagues at IOActive for their support while writing this book. He would like to acknowledge all those with whom

he has shared in interesting conversations about computer security and other completely unrelated real-life topics, including Dominic Chell, Marcus Pinto, Matthew Hickey, John Heasman, Ilja van Sprundel, Peter Winter-Smith, Ben Harrison-Smith, Vincent Berg, and Shane Macaulay, among others. Finally, Shaun would like to thank his parents, Jill and Andy, his brother Dave, and the rest of his family for their continued support during his career; as well as his friends, just for being awesome mates.

Ollie would like to say thanks to all the security researchers who have published their security research relating to BlackBerry technologies, including Zach Lanier, Ben Nell, Ralf-Philipp Weinmann, Shivang Desa, Tim Brown, Alex Plaskett, Daniel Martin Gomez, and Andy Davis. Without the hard work and perseverance of these individuals, public understanding would not be where it is today. He would also like to thank the numerous individuals he's been lucky enough to work closely with over the years and from whom he learned so much, including Foob, Nathan Catlow, Bambam, Rob Wood, Aaron Adams, Pete Beck, Paul Collett, Paul Ashton, Jeremy Boone, Jon Lindsay, Graham Murphy, and Ian Robertson. Ollie's final thanks is to Twitter, for providing continual distractions, and Kismet (the cat) for keeping him company on weekends whilst he wrote his chapters.

Finally, as a team, we are grateful to the people at Wiley—in particular, to Carol Long, Sydney Argenta, and the rest of our editorial team. Their help in developing and polishing our manuscript was invaluable, and apologies again for testing our deadlines. In particular, a big apology from Shaun who loves nothing more than leaving everything till the last minute!

Contents at a Glance

Contents