Auerbach Publications
Taylor & Francis Group

WIRELESS CRIME AND FORENSIC INVESTIGATION

GREGORY KIPPER

WIRELESS CRIME AND FORENSIC INVESTIGATION

GREGORY KIPPER

Auerbach Publications
Taylor & Francis Group
Boca Raton New York

Auerbach Publications is an imprint of the
Taylor & Francis Group, an informa business

Auerbach Publications
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

No claim to original U.S. Government works
Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-10: 0-8493-3188-9 (Hardcover)
International Standard Book Number-13: 978-0-8493-3188-6 (Hardcover)

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the author and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the Auerbach Web site at
http://www.auerbach-publications.com

Dedication

For Grant

Author's Intent

Before the final idea of this book was fully visualized, I spent a lot of time thinking about what investigators and security professionals would need tomorrow, next year, and on, into the future; content that really needed attention but that was not widely covered. My thoughts kept coming back to conducting forensics in a wireless environment.

First, there is a need. I wanted to get some good material out to investigators on this particular type of forensics. Second, it is important. Mobile devices are changing the very dynamics of our society, and those changes will continue to evolve as people live and work, and as our children grow into adults. Crime will, of course, continue to be a factor, as well as the growth of new, inventive ways of carrying it out. My goal is that by the time you've finished this book, you will know a good deal more than you now do and that you'll be able to effectively apply this knowledge to your work.

Who Should Read This Book

For those of you who have read my first book, *Investigator's Guide to Steganography*, you will notice a similar style and organization in this book. I did my best to make this book readable for anyone, but it is, of course, tailored to the forensic investigator, the private investigator with technical skills, and the IT security professional. The flow of the book is designed to take you from basic to advanced understanding. It does not necessarily have to be read in order, but that is probably the best approach to take if you're a beginner or haven't looked at the technology in a while. I'm a big believer in keeping information in context: showing where technology came from and why it is being used, before approaching the subject of forensics. The book is crafted along those lines of thought.

Acknowledgments

First and foremost, I would like to thank Amber Schroader for her contributions to this book. Quite simply, without her support and that of the Paraben engineers and developers, this work would not have seen the light of day. I would also like to thank Ken Ammon, John Sleggs and NetSec, as well as Eoghan Casey from Knowledge Solutions, for contributing their insights and expertise. Their assistance and research added greatly to this endeavor. I'd also like to recognize all of my technical editors — Eric Cole, Amber Schroader, and Joe Tomasone — for their time, expertise, and personal contributions to this book. Additionally, I'd like to thank Dave and Lisa Stafford, Spike and Ruth, Cody McKinney, Rich O'Hanley, Kimberly Hackett, Rachael Panthier, and the Taylor & Francis crew. Additionally I'd like to acknowledge James Briggs for his great work on all the graphics that went into this book.

Greg Kipper

About the Author

Greg Kipper has been active in the field of IT security and information assurance for the past 12 years. Through his experiences in the intelligence community and IT security, he moved into the emerging field of digital forensics. The last six years of his career have been spent working on the future of technologies and their impact on the process of forensic evidence gathering. He is also the author of *Investigator's Guide to Steganography* and continues to contribute to the fields of security and digital forensics through participation in numerous conferences and organizations. Mr. Kipper is currently working in the greater District of Columbia area as a private consultant in the field.

Technical Editors

Amber Schroader

Amber Schroader has been involved in the field of computer forensics for the past 16 years. During this time, she has developed and taught numerous courses in the computer forensic arena, specializing in the field of wireless forensics as well as mobile technologies. She is the CEO of Paraben Corporation and continues to act as the driving force behind some of the most innovative forensic technologies. As a pioneer in the field, she has played a key role in developing new technology to help investigators with the extraction of digital evidence from hard drives, e-mail, and handheld and other mobile devices. Her extensive experience includes dealing with a wide array of forensic investigators, ranging from those at federal, state, and local levels to corporate. With an aggressive development schedule, she continues to bring new and exciting technology to the computer forensic community worldwide and is dedicated to supporting the investigator through the new technologies and training services that are being provided through the Paraben Corporation. Ms. Schroader is involved in many different computer investigation organizations including the Institute of Computer Forensic Professionals (ICFP), High Technology Crime Investigation Association (HTCIA), the Computer Forensic Tool Technology (CFTT) program, and Federal Law Enforcement Training Center (FLETC).

Eric Cole

Eric Cole is a renowned Thought Leader with over 15 years of experience in the network security consulting market space. Dr. Cole is currently chief scientist and director of cyber security for Lockheed Martin Information

Technology (LMIT). Cole continuously executes high-end consulting services with Fortune 500 companies, financial institutions, international organizations, and the federal government. As a recognized industry expert, he is a frequent keynote speaker at security events around the world, including the Systems Administration Network Security Institute, and has been interviewed by CBS News, *60 Minutes*, and CNN. Cole is a member of the HoneyNet project and the *Common Vulnerabilities and Exposures* (CVE) editorial board, and has authored several books, including *Hackers Beware, Hiding in Plain Sight, Network Security Bible,* and *Insider Threat*. Dr. Cole contributed to the development of several of the GIAC certifications.

Joe Tomasone

Joe Tomasone is the senior network security engineer for Fortress Technologies. With more than 15 years in the IT industry, he has extensive practical experience in networking and security, and has briefed local, state, and federal agencies such as the Pentagon, the White House Communications Agency, the National Security Agency, the U.S. Air Force, U.S. Navy, and U.S. Army, plus numerous Fortune 1000 companies on wireless and wired security. In his current role, he is responsible for educating potential customers and partners on wireless security matters as well as the features and benefits of the company's Air Fortress family of products. He is a frequent speaker on these topics at conferences and to industry groups such as ISSA and Infragard.

Introduction

My in-laws just came to visit, and when they walked in the door, they were amazed at how much my five-month-old child had grown. They had not seen her in about two months and were astounded at how much she had changed. My first reaction was, "You really think she has changed that much?" As I see her every day, I do not notice the changes because I adapt and grow as she grows, which introduces an interesting problem. Although my daughter has been growing rapidly, because I am constantly around her, the day-by-day or hour-by-hour changes are so subtle that I fail to realize how significant the change has been until I look back at a picture when she was born, compare it to how she looks now, and realize that miraculous growth has occurred.

Similarly, we can all relate to this phenomenon with our children, but the same metamorphosis has been occurring with technology. Those who work with technology on a daily basis may be less aware of the dramatic growth. We do not always recognize or understand the change until a significant time period has elapsed or until others have pointed it out to us. Probably the one area in which this phenomenon has been most pronounced is wireless technology.

Wireless impacts everything we do and has become an integral part of our lives. Although I could fill pages talking about wireless, the focus here is on wireless data transfer in regard to computers. I am using the term *computers* in the liberal sense, indicating any device that has some processing and storage capability. For many people, one of their last activities before they go to sleep at night — and one of the first things they do in the morning — is utilize a wireless device. Whether it is a home computer or a BlackBerry to check on the status of a company and make sure no last-minute e-mails have arrived, wireless is all around us. And if you think they are everywhere now, you have not seen anything yet. Many of those who actively utilize wireless capabilities may think there is no scope left for practical development; the current technical boundaries often limit our perspective on creative ideas for the future. A perfect example is that many people five years ago thought cell phones were pretty sophisticated, but since then that technology has been taken to an entirely new level. Similar advancements will continue to occur.

As we move into the future most, if not all, critical data at some point between source and destination is going to go over a wireless link — if not several. As homes and offices, towns, cities, states, and countries continue to increase their bandwidth and connectivity, a natural solution to the problem is wireless. It is easy to install and does not require significant changes to operate. Let us start with the smallest example, a house. As technology advances, houses are going to have an increased need for bandwidth for home control systems. If you decide to install all new wiring to support a home control system you, in essence, will need to replace all Sheetrock® and walls in your house to support the number of wires that would be needed. Or in very strategic locations, you could install a few wireless access points, and have the same connectivity and benefit at a fraction of the cost and for a fraction of the time it would take to set up the network. Now take this example and scale it up to a town, city, or country. The problem with wires only gets worse, and the tremendous benefit provided by wireless only increases.

Therefore, in the next several years we can almost guarantee that critical data is going to be routed over wireless links. The efficiencies are too great to be ignored, and the functionality benefit will only continue to rise. As new, complex solutions of data transfer continue to occur, wireless, in most cases, is going to be the only reasonable solution to this problem.

Although wireless solves many problems, it creates a huge number of issues. The biggest problems with wireless is control, which leads to security problems. Wired connections are controlled, and if you cannot get access to the wires to either tap them midstream or at the demarc points, you are not able to intercept the signal. However, with wireless, anyone within a certain area is able to intercept the signal. Whether they can actually process or interrupt the signal is a completely different problem, but they can at least see the signal, which makes the attacker's problem much easier than if it was a wired situation. Many of you might think I am stating the obvious; however, obvious or not, this is a concept that many people either forget about or ignore in implementing solutions.

Now for the really bad news. The problem of controlling and securing wireless is not a linear problem; it is an exponential problem in terms of complexity. This means the longer we allow functionality to increase, the problem of securing those wireless networks increases at a much steeper pace.

As most organizations traditionally do after they implement a solution, they assume it is secure, and after it is compromised or they see the potential for compromise from other organizations, they slowly address the problem. We have readily observed with viruses, worms, and other problems that this reactive measure does not work and does not scale. With a problem space as big and as complex as wireless, proactive measures must be put in place, and they must be put in place immediately. Organizations can either pay now, or they can pay later. However, one problem is that wireless is like a high interest rate credit card. If you pay off the debt now, you no longer have any debt to worry about, but if you pay later by paying the minimal each month, you will probably never be able to pay it off because of the compound growth of the problem. Even if you do manage to pay it off, you will end up paying much more than you needed to.

General security is also a concern with any new technology, and when we think security we typically think of stopping an attacker from breaking in or gaining access. However, based on the broad reach of wireless, stopping someone from passively listening in is just as critical. Therefore, all current disciplines need to be applied to the wireless arena. Intrusion detection systems, firewalls, and forensics are just a few of the key areas that one must understand and apply to proactively solve the wireless problem.

Dr. Eric Cole

Contents