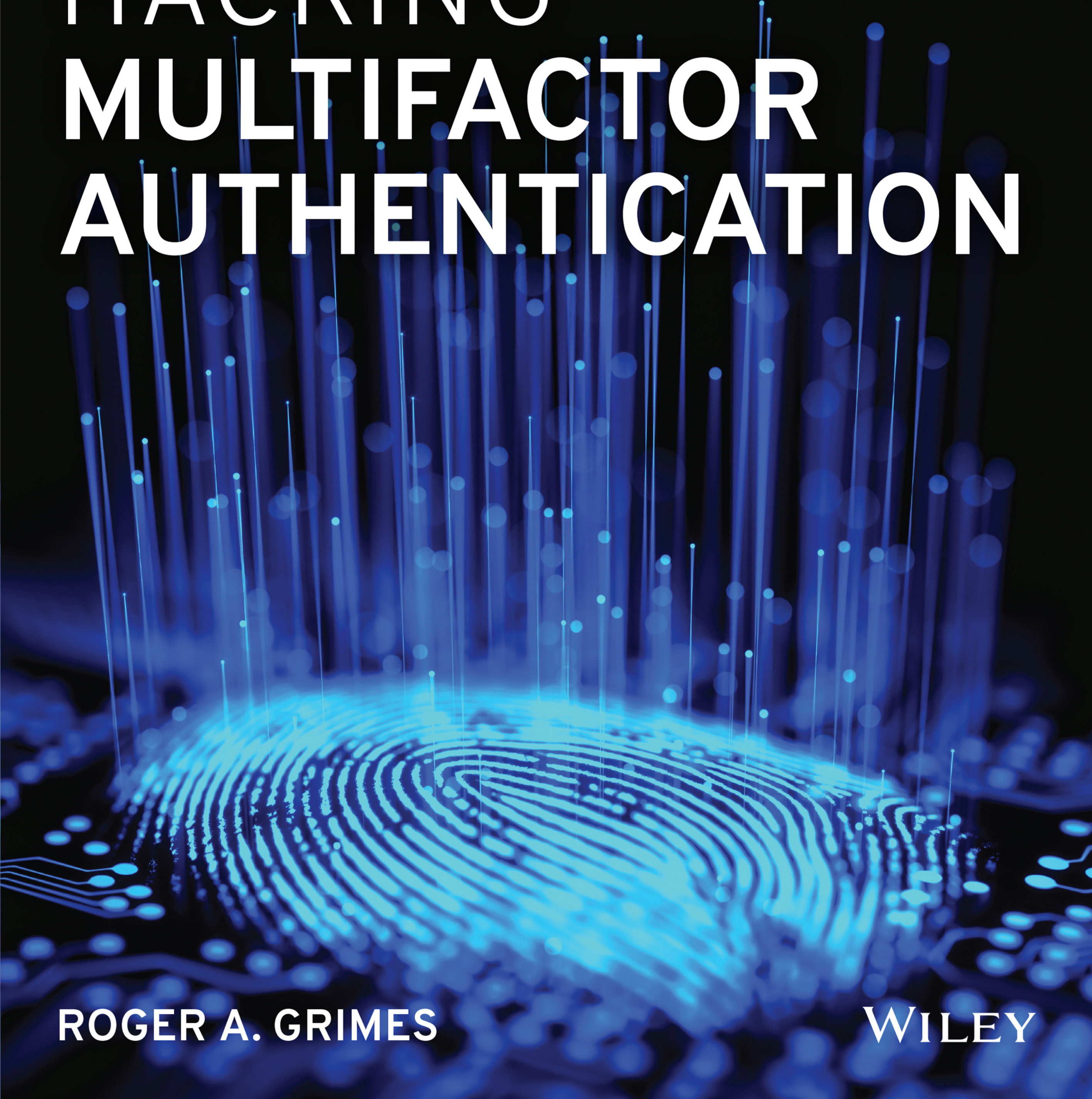
"A thoughtful demonstration that, like all security technologies, MFA is not a panacea."

—BRUCE SCHNEIER

HACKING MULTIFACTOR AUTHENTICATION



ROGER A. GRIMES

WILEY

Hacking Multifactor Authentication

Roger A. Grimes

WILEY

ISBN: 978-1-119-65079-9
ISBN: 978-1-119-67234-0 (ebk)
ISBN: 978-1-119-65080-5 (ebk)

Manufactured in the United States of America

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2020942316

I dedicate this book to my wife, Tricia. I’ve not had a bad day since the day I met her.

About the Author

Roger A. Grimes has been fighting malicious computer hackers and malware for more than three decades (since 1987). He's earned dozens of computer certifications (including CISSP, CISA, MCSE, CEH, and Security+). He even passed the very tough Certified Public Accountant (CPA) exam, although it has nothing to do with computer security and he is the (self-proclaimed) world's worst accountant. He's been a professional penetration tester breaking into companies and their websites and devices for over 20 years. Roger has been on nearly a dozen project teams tasked with hacking various multifactor authentication (MFA) solutions over his career.

He has created and updated dozens of computer security classes and taught thousands of students how to hack or defend. Roger is a frequent presenter at national computer security conferences, including RSA and Black Hat. He's previously written or cowritten 11 books on computer security and more than a thousand magazine articles. He was the weekly computer security columnist for *InfoWorld* and *CSO* magazines for nearly 15 years, and he's been working as a full-time computer security consultant for more than two decades. Roger is frequently interviewed by newspapers, including the Wall Street Journal, magazines, including *Newsweek*, and he has been a guest on radio shows, such as NPR's "All Things Considered." Roger currently advises companies, large and small, around the world on how to stop malicious hackers and malware quickest and most efficiently.

You can contact and read more from Roger at:

- Email: `roger@banneretcs.com`
- LinkedIn: `www.linkedin.com/in/rogeragrimes`
- Twitter: `@rogeragrimes`
- CSOOnline: `www.csoonline.com/author/Roger-A.-Grimes`

Acknowledgments

I would like to thank Wiley and Jim Minatel for greenlighting this book. I have been giving presentations on this topic for almost two years to enthusiastic crowds, and I'm glad they also saw the enthusiasm it generated. Wiley really is a great place to work with to write a book. Thanks to Kim Wimpsett for her project management. I think this is the third or fourth time Kim and I have worked together on a book. Thanks to Barath Kumar Rajasekaran for his editorial guidance, Pete Gaughan, copyeditor Elizabeth Welch, and proofreader Nancy Carrasco, in helping to prepare this book for publication.

Thanks to my employer, KnowBe4, Inc., and awesome CEO Stu Sjouwerman, Kathy Wattman, Kendra Irmie, and Mary Owens for letting me develop the original Hacking MFA presentation and go around the country presenting it. I truly love working for KnowBe4. It's been my favorite job of my career. Thanks to my friend and KnowBe4's Chief Hacking Officer, Kevin Mitnick, for showing me and the world many ways to hack what they thought was unhackable MFA solutions. Thanks to Erich Kron, my coworker, for the many discussions we had about MFA, for his MFA device demonstrations, and for many of the pictures in this book. I was lucky to have found and work elbow to elbow with a good friend and knowledgeable coworker. My wife, Tricia, frequently says she prefers Erich's presentation style over mine. . .so there's also that. Thanks to Corey Nachreiner and Alexandre Cagnoni of WatchGuard Technologies for agreeing to be this book's technical editors and for providing hours of discussion on the best MFA solutions and how to hack them. I think both of them have forgotten more than I know about MFA. My special thanks to Rolf Lindemann of Nok Nok for MitM classifications and FIDO defense information.

I want to thank all the MFA developers and vendors who have befriended me over the last two years and challenged me to see how secure their particular MFA solution was. It was only by looking at and reviewing well over a hundred solutions that I felt comfortable enough to write a book like this. Thanks to the hundreds of article writers and YouTube posters showing how they hacked various MFA solutions. Lastly, I have strived to be technically accurate at all times. If, however, I said something technically wrong, I apologize. I'm only human and I tried my best.

Contents at a Glance

Contents

Introduction

This book came about through an interesting happenstance. Arguably, the world's most infamous hacker, Kevin Mitnick, co-owner and Chief Hacking Officer at KnowBe4, Inc., did a public presentation that included showing how he could easily "hack around" two-factor authentication using a simple phishing email. Kevin is a lot more famous than I am, and his demonstration hack was viewed by thousands of people. And about that many wrote to him to get more details.

So many people wrote and requested interviews that the KnowBe4 (who I also work for) public relations team asked if I could help answer queries Kevin couldn't get to. I was glad to. I've got decades of experience in hacking different MFA solutions. Reporters accustomed to covering computer security topics frequently asked if we had yet reported the exploit Kevin used to the MITRE list of Common Vulnerabilities and Exposures (`cve.mitre.org`). The CVE is where most cybersecurity vulnerabilities, new or old, are listed and tracked. When a brand-new exploit is discovered, it's customary to report it to the CVE, along with relevant details. Most of us in the cybersecurity world follow it to check out what new exploits have been found and to see if we really need to be worried about them.

I laughed. The hack Kevin demonstrated (which is called *session cookie hijacking* and is covered in Chapter 6, "Access Control Token Tricks" of this book) has been around for decades. It's not new at all. In fact, it's one of the most common forms of network hacking. Dozens of free hacking tools are available that help hackers to do it, and it's likely been used to take over millions of user accounts over three decades. It's been used to take over thousands of accounts protected by two-factor authentication, at least since the late 1990s. It's the opposite of new.

I was surprised that when I talked to the beat reporters and computer security people I knew, most thought it was a new attack. So, not only did everyone's mom and dad and regular people not know that it wasn't new, but knowledgeable, experienced computer security people—who you would *expect* to know—didn't know that. It was surprising to me.

I was also surprised that many of the people I spoke to thought the attack was due to a vulnerability in LinkedIn, the website Kevin used in his demonstration. It wasn't. What Kevin showed could be used against hundreds to thousands of popular sites, and LinkedIn, in particular, didn't have a flaw that they were going to have to close. It was an attack against a very common form of multifactor authentication and how it worked in general. No patch was coming to fix some flaw. And you could update the multifactor authentication solution that was used with it to prevent the particular type of attack Kevin demonstrated, but it could be attacked at least another five different ways, as can any multifactor authentication method.

To many of the people I talked with, I shared that I knew of at least 10 ways (as I quickly counted) to hack different forms of multifactor authentication. They were all shocked. As a result, I decided to write a column about it in CSOOnline (www.csoonline.com), where I was a writer at the time. By the time I finished the column (www.csoonline.com/article/3272425/authentication/11-ways-to-hack-2fa.html) in May 2018 I had come up with 11 ways.

I was sharing the news of my column with the CEO of KnowBe4, Stu Sjouwerman, the next morning when he wisely suggested I create a presentation on the topic and start giving it. Within a few days, I had created a new presentation called 12 Ways to Defeat Multi-Factor Authentication (info.knowbe4.com/webinar-12-ways-to-defeat-mfa). As I did more research and thinking, I quickly came up with new ways to hack MFA nearly every week.

I'm up to over 50 ways now, all of which I share in this book. The presentation turned into a long whitepaper. At KnowBe4, the average whitepaper is three to five pages long; mine was 20 pages. It was the longest whitepaper in the history of KnowBe4, and it quickly became a running joke around the office and one that still follows me around. I shared that I had originally created a rough draft double that size and that the 20 pages was my trimmed-down version after their chiding. That then led it into becoming a short e-book (www.knowbe4.com/how-to-hack-multi-factor-authentication) at 40 pages.

I began to give my presentation around the country and world, including at the biggest computer security conferences, RSA and Black Hat. In both places I had standing room–only crowds and long lines of attendees trying to get in to see some of the hack discussions. My original 12 Ways to Defeat Multi-Factor Authentication presentation grew to be so long that I now have to choose which fifth of the hacks I'm going to share with audiences, although Kevin's original MFA hacking demo is still clearly a crowd favorite (and I provide the URL for it in this book).

Jim Minatel, my longtime friend and acquisitions editor at Wiley, came to see me give the presentation at RSA and saw the enthusiastic crowds. I was sick as a dog when I gave the presentation. In fact, I was hospitalized for a week the day after the presentation with an acute, life-threatening illness. I felt like I had done a terrible job at presenting the material. I certainly would love a future do-over. But Jim saw the crowds and the energy the material generated and asked if I would write a book on the subject. I said yes over lunch, and this is that book. The best part is that now I've given hundreds and hundreds of pages to share everything I know on the subject. Even then I'm sure several more books of the same size could be written on the subject. Multifactor authentication and its weaknesses are many. In truth, even this book is just scratching the surface. It's 500-plus pages of summary material. But I hope all readers will better understand the strengths and weaknesses of multifactor authentication and that MFA developers will create better, more secure, solutions.

The ultimate objective of this book is to appropriately frame the security and weaknesses of all MFA solutions. If you know only the benefits and none of the risks, you're more likely to implement an MFA solution without the appropriate policies, controls, and education. This book is a push-back against the overzealous marketing messages broadcast by some MFA vendors. MFA solutions can significantly reduce many forms of cybersecurity risk, but they aren't a perfect panacea and it doesn't mean we can throw away all the previous computer security lessons learned. If you come away with a suitable understanding of what MFA can and can't do, and change your practices and controls appropriately, then I've done my job.

Who This Book Is For

This book is primarily aimed at anyone who is in charge of or managing their organization's computer security and, in particular, logon authentication. It is for anyone who is considering reviewing, buying, or using multifactor authentication for the first or the tenth time. It's for developers and vendors who make multifactor authentication solutions. Prior to this book there has not been a single place where anyone, customer or vendor, could go to learn about all the common ways multifactor authentication can be hacked. Now there is that source, although I'm sure I haven't covered every hacking method, defense, and caveat. But I tried.

It's mostly for all the people who have heard the great security promises that multifactor authentication will give and somehow equate those vendor promises with a larger falsehood, that using MFA means "I can't get hacked!" Nothing could be further from the truth. This book is your counterargument any time someone tries to convince you that using MFA means you don't have to worry about hacking anymore. That isn't true and will never be true.

It also dispels the naive notion that we really want a 100 percent secure solution. We don't. Society wants a security solution that impacts them the least and provides "just OK" protection. This is a hard reality that both administrators and developers learn in the marketplace of computer security products. Some of the best, really secure computer products never get purchased by more than a few companies, and they end up on the tall heap of unused products.

In that respect, this book reminds me of the famous quote delivered by Jack Nicholson's character, Colonel Nathan Jessup, in the 1992 movie *A Few Good Men*: "You can't handle the truth!" You may not like to hear that we don't want the best security, but ignore what the user wants at your own peril. So, the purpose of this book is not only about developers and customers learning all the ways to hack MFA, but also about when layered security is just *too much* security.

What Is Covered in This Book?

Hacking Multifactor Authentication contains 25 chapters separated into three parts:

Part I: Introduction Part I discusses authentication basics and the problems that MFA is trying to solve. It includes the background facts you'll need to know to understand why MFA is a favored authentication solution and how it is hacked.

Chapter 1: Logon Problems Chapter 1 covers the central problems that MFA is trying to solve. MFA didn't come out of the blue. Password and single-factor solutions failed so often that better and improved authentication solutions were invented. Learn about the problems MFA is trying to solve.

Chapter 2: Authentication Basics Authentication isn't one process—it's a series of connected processes with a multitude of different components. Any of the steps and components can be hacked. To understand how MFA can be hacked, you first have to understand how authentication works with or without MFA involved. Chapter 2 provides that foundation.

Chapter 3: Types of Authentication Chapter 3 covers dozens of types of authentication, describes how they differ from one another, and examines the inherent strengths and weaknesses of each type of solution.

Chapter 4: Usability vs. Security Security is always a trade-off between user-friendliness and security. MFA is no exception. The most secure options will often not be tolerated by end users. Chapter 4 covers the fundamental challenges of good security and when good security actually becomes so onerous that it becomes bad security. The best security options are good trade-offs between usability and security. Find out when that line is crossed.

Part II: Hacking MFA This part of the book covers the various ways to hack and attack various MFA solutions. Mitigations and defenses for each of the attacks are detailed in each chapter.

Chapter 5: Hacking MFA in General Chapter 5 begins by explaining the very high-level ways that MFA can be hacked, with a summary of the various techniques. Every MFA solution is susceptible to multiple hacking attacks and are covered in the rest of the chapters of this section.

Chapter 6: Access Control Token Tricks Chapter 6 starts off by discussing, in detail, one of the most popular, decades-long, MFA hacking methods: that of compromising the resulting access control token. Chapter 6 shows multiple ways in which access control tokens can be compromised.

Chapter 7: Endpoint Attacks A compromised device or computer can be attacked in hundreds of different ways, including bypassing or hijacking MFA solutions. A compromised endpoint cannot be trusted. Chapter 7 discusses several popular endpoint attacks.

Chapter 8: SMS Attacks Chapter 8 covers multiple Short Message Service (SMS) attacks, including subscriber identity module (SIM) hacks. For years now, the U.S. government has said that SMS should not be used for strong authentication and yet the most common MFA solutions on the Internet involve SMS. Learn why that shouldn't be the case.

Chapter 9: One-Time Password Attacks One-time password (OTP) solutions are among the most popular MFA solutions, and they are good but not unhackable. Chapter 9 covers the various types of OTP solutions and how to hack them.

Chapter 10: Subject Hjack Attacks Unlike most of the other MFA attacks described in this book, subject hijack attacks are not very popular. In fact, they have not been knowingly accomplished in a single public attack. Still, they can be done, and simply knowing about them and how they can be accomplished is an important lesson. Chapter 10 covers one specific type of subject hijack attack on the world's most popular corporate authentication platform, in enough detail, that you will likely be worried about them forever.