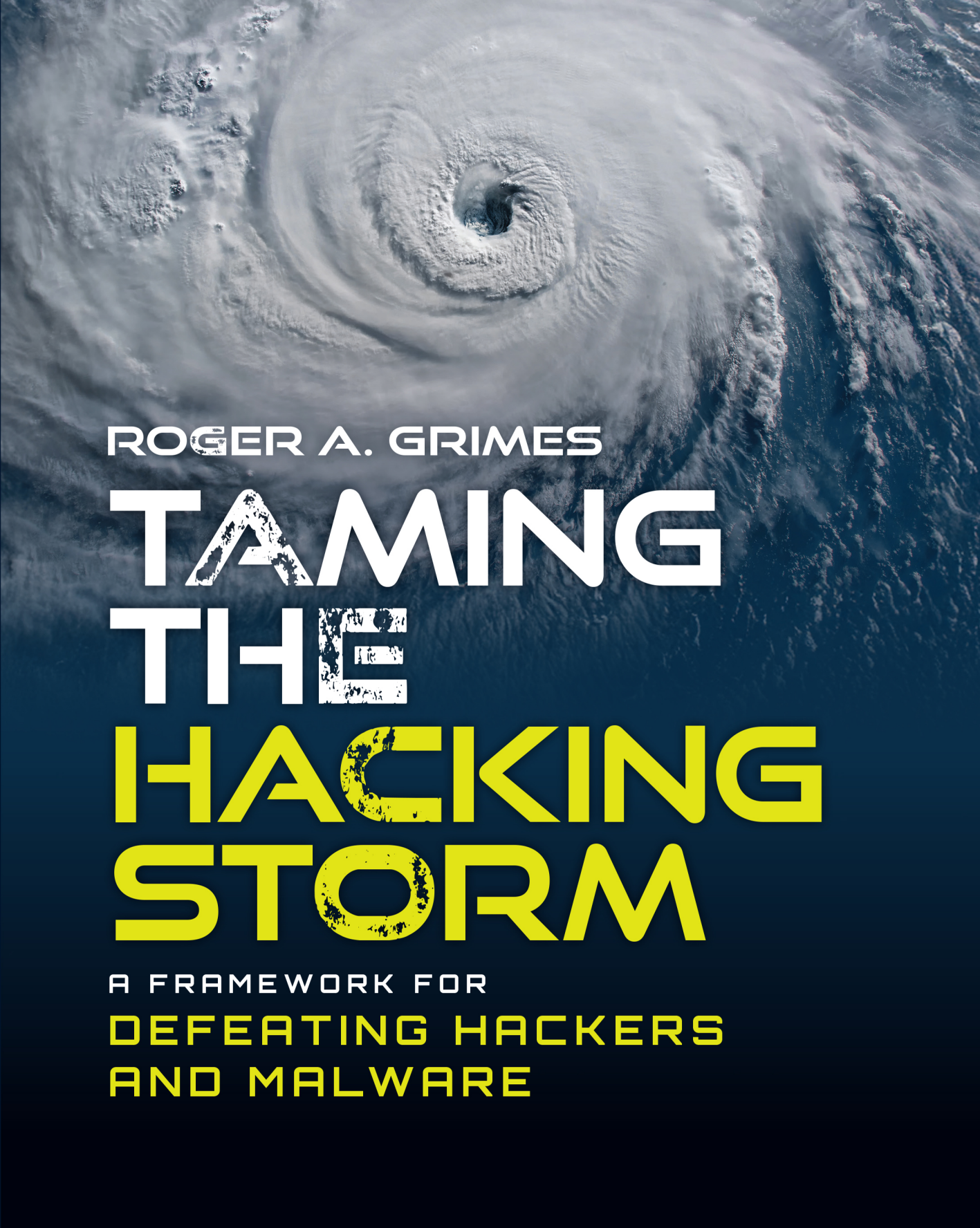
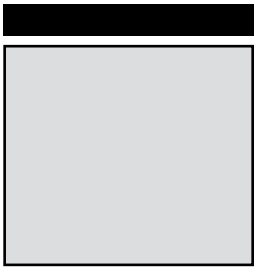


ROGER A. GRIMES

TAMING THE HACKING STORM

A FRAMEWORK FOR DEFEATING HACKERS AND MALWARE

Taming the Hacking Storm



Taming the Hacking Storm

A Framework for Defeating Hackers and Malware

Roger A. Grimes

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data Applied for:

Print ISBN: 9781394349586
ePDF ISBN: 9781394349609
epub ISBN: 9781394349593
OBook ISBN: 9781394352289

Cover Image: © elroce/Adobe Stock
Cover Design: Wiley

To all the Internet security practitioners who have dedicated their careers to fighting malicious hackers and their malware. Keep up the good fight!

This book, like all my others, is also dedicated to my wife, Tricia. She has supported my vision to "fix the Internet" since the day we met over 27 years ago. On our honeymoon, she sat on the beach by herself for part of each day while I toiled up in our hotel suite, thinking and writing about how to better fight hackers and malware. I know neglecting your bride on your honeymoon is not the sign of a healthy work/life balance, but the fact that she supported my efforts toward this goal without a complaint even then speaks to the great life partner she is. I would not be who I am without her.

About the Author

Roger A. Grimes, data-driven evangelist at KnowBe4, Inc., has been a computer security consultant for 36 years, as well as an instructor, holder of dozens of computer certifications, and author of 15 books and more than 1,500 articles on computer security. He has spoken at many of the world's biggest computer security conferences (e.g., Black Hat, RSA, etc.); been featured in *Newsweek* magazine; appeared on television; been interviewed for NPR's *All Things Considered*, CNBC, the *Wall Street Journal;* and been a guest on dozens of radio shows and podcasts. He has worked at some of the world's largest computer security companies, including Foundstone, McAfee, and Microsoft. He has consulted for hundreds of companies, from the largest to the smallest, around the world. He specializes in social engineering, host and network security, ransomware, multifactor authentication, quantum security, identity management, anti-malware, hackers, honeypots, public key infrastructure, cloud security, cryptography, policy, and technical writing. His certifications have included CPA, CISSP, CISA, CISM, CEH, MSCE: Security, Security+, and yada-yada others, and he has been an instructor for many of them. His writings and presentations are often known for their real-world, contrarian views. He was the weekly security columnist for *InfoWorld* and *CSO* magazines between 2005 and 2019.

You can contact the author at:

Email: `roger@banneretcs.com`

LinkedIn: `https://www.linkedin.com/in/rogeragrimes`

Bluesky: `@rogeragrimes.bsky.social`

X/Twitter: `@rogeragrimes`

Mastodon: `https://infosec.exchange/@rogeragrimes`

Threads: `@rogeragrimes`

Contents

Preface
Taming the Internet

"It is not the critic who counts; not the man who points out how the strong man stumbles, or where the doer of deeds could have done them better. The credit belongs to the man who is actually in the arena, whose face is marred by dust and sweat and blood, who strives valiantly; who errs and comes short again and again; because there is not effort without error and shortcomings; but who does actually strive to do the deed; who knows the great enthusiasm, the great devotion, who spends himself in a worthy cause, who at the best knows in the end the triumph of high achievement and who at the worst, if he fails, at least he fails while daring greatly. So that his place shall never be with those cold and timid souls who know neither victory nor defeat."

– Theodore Roosevelt (1858–1919), "Man in the Arena" speech, given April 23, 1910

I'm out to fix all of Internet security, or at least as much as I can, before I depart Earth. I know from experience that mostly what I'm doing is inviting critics to pan my ideas and tell me how I'm not that smart. It's okay. I'm a man in the arena.

At nearly the same time that I started to develop an intense interest in personal computers, I also developed a strong interest in fighting malicious hackers and their malware programs. My interest was immediately intensely passionate, religious-like, and felt life-changing. And it turned out to be exactly that, as it changed the rest of my life and became my career. I don't know why because prior to that epiphany, I had never had an interest in becoming a cop or detective in real life, even though I have always greatly admired and appreciated them. But something clicked when I got into computers.

It wasn't like malicious hacking was rampant at the time. Back in 1987, there were only a few PC computer viruses, a few on Apple computers (e.g., Elk Cloner), and a few on IBM-compatible computers (e.g., Stoned, Pakistani Brain, etc.). They were so few and generally uncommon that popular and respected early *PC Magazine* columnist John Dvorak wrote a column declaring them a hoax.

For the first decade or so after that period, even as hackers and their malware programs began to really flourish, most hackers and malware programs really didn't go out of their way to permanently harm someone or something. Back then, hacking and writing computer virus programs was more of a way for someone (usually men aged 12 to 24) to brag about their programming and hacking machismo to similarly minded online social communities. There were only a few exceptions (e.g., PC Cyborg ransomware trojan, Michelangelo virus, etc.) where a hacker program intentionally tried to harm something. But almost none stole money. And most, if they did do something harmful, really didn't intend to.

I followed an early online newsletter called *The Dirty Dozen*, so-called because it described all the currently-existing-at-time dozen malware programs to be aware of. Originally created by Tom Neff and later updated by Eric Newhouse, it quickly grew over the next few years to include many "dozens." Here's an example from 1988: `https://totse.totseans.com/viruses/virus _ information/dd.html`.

I had read a 1987 book called *FluShot Plus* by Ross Greenberg, which described early malware and how to fight it. Greenberg covered how he created what he thought was a totally secure sandboxed environment and invited hackers to hack it: which they successfully did many times in a continuing cat-and-mouse game that portended today's back-and-forth antivirus battles.

The *FluShot Plus* book is such an early book on computer malware that I can't even find a mention or reference to it on the Internet. Imagine something that really existed in the real world that the Internet has no record of! Part of that reason is that the Internet wasn't really even the "everywhere Internet" as we know it now. We had a patchwork of globally connected messaging systems, but it wasn't called the Internet. The official Internet was something only privileged universities and colleges had and could afford at the time. I owned a physical copy of the *FluShot Plus* book for decades. If I had to point to a single thing that piqued my interest in fighting malicious hackers and malware the most, it was that book.

Greenberg also made an early companion antivirus program called FluShot Plus, and he eventually wrote one of the first antivirus scanning programs that could scan for multiple malware programs at the same time called Virex PC. Before then, if you thought you had a malware program on your computer, you had to hope that someone had made a dedicated "detector" program and run that specific program that looked for that one malware program. And if you learned from the detector program that you did indeed have that malware program, you had to execute and run another companion program, if you were lucky and it even existed, to remove the malware program as you crossed your fingers.

The now infamous and late John McAfee made the "virus scanner" program explode in popularity around 1988–1989 and, with it, a new mega swarm of virus writers. Before John created his VirusScan program, there were probably less than a dozen computer viruses. However, one of the weird side effects of writing a popular computer virus-eradication program was that it attracted new people who wanted to code a brand new computer virus and get their 15 minutes of fame.

I first met John in 1987 or 1988 on a computer virus fighting online group called Virus L (I think that was what it was called) on FIDONet, an early precursor of today's Internet. From that meeting, John encouraged me to learn Assembly language to disassemble viruses, and for the next few years I was disassembling and documenting DOS computer viruses for him. At first, he would send me one or two new computer viruses a month to look at, but within less than two years he was sending me dozens a day. I could not keep up. My real full-time job as an accountant was suffering. John eventually started McAfee Associates and had teams of full-time virus disassemblers. He did not need me.

But I was fully hooked into fighting malicious hackers and their malware programs by then, spending every spare hour I could on it…even neglecting my new wife and young babies more than I should have in pursuit of my new passion. I was, even back then, doing consulting services to companies hit by computer viruses. I remember dressing up in my finest brown corduroy suit and walking into the board rooms of Fortune 100 banks in distress and being paid big money to advise the U.S. Navy when they got hit by computer viruses.

It was all headed stuff, and if they knew just how scared I was inside my own young head, they would probably chased me out. But I did help them. I was even in *Newsweek* magazine in March 1992 along with John in an article about the Michelangelo boot virus that was erasing hard drives (actually only the master partition tables) around the world.

My passion was expanded past just computer malware when I read Clifford Stoll's 1989 *The Cuckoo's Egg* (`https://www.amazon.com/Cuckoos-Egg-Tracking-Computer-Espionage/dp/1668048167`) about tracking and trapping a foreign hacker using a honeypot. Not coincidentally, I later wrote a book on honeypots in 2005 called *Honeypots for Windows* (`https://www.amazon.com/Honeypots-Windows-Experts-Voice-Grimes/dp/1590593359`). I started to learn about hackers, hacking, and how to stop them.

At the time, I didn't realize cybersecurity would become my life's passion and a multidecade career. In my full-time professional life, I have worked my way from PC repair technician to network technician, to network supervisor, to regional director of networks and technology for a large healthcare organization, and finally to vice president of information services of a midsize hospitality company. But during all of that, my real passion was fighting hackers and malware. I was reading everything I could on it. I was frequently making money consulting on it. I was, for sure, neglecting my full-time job to really work on computer security. My bosses thought I was working on budgets or something

like that, and really, I was researching and fighting hackers. My full-time jobs were funding my even fuller-time professional hobby. I'm not sure how I didn't get fired because I wasn't a great boss or manager.

By April 2003, I realized I had enough of doing anything that wasn't computer security related. I remember calling my wife one day out of the blue and telling her I was quitting my very well-paying job as a VP and going to start doing computer security full-time. She already knew of my passion but wasn't as gleeful as I was since we had four kids to support and a large mortgage.

She cautioned me to do general computer consulting instead and do computer security when I could until I could make it into a full-time business. And I could understand her concern. There wasn't a field called cybersecurity. There were not even a ton of malicious hackers. John's antivirus program seemed to be getting more and more accurate, and there was a real possibility that the problem of computer malware might be solved. A lot more hackers were getting arrested and put in jail…finally…including infamous early hacker, Kevin Mitnick, who decades later became my employer, friend, and supporter. It seemed like there was a real chance that the world was going to get a handle on hackers and their malware programs.

Yes, it's very funny to think about that now.

I remember thinking, "Well, we are starting to arrest the hackers and get a handle on malware programs…but there's going to be a lot more computers in the future, so even if there will be fewer of them as a percentage overall to fight, they will likely still be a big problem." With that, I went full-time to computer security in 2003 and never looked back. Fairly soon, I had a better-paying job teaching hacking to students and doing penetration testing for a cool company called Foundstone (ironically, later bought by McAfee Associates).

I mention all this because there was a time when we had computers and the Internet, and it wasn't all that clear that hackers and malware would get as bad as they are today. Hacking and malware were present, but they were not everywhere. Most people and companies didn't get hit by them. The people who got "hit" by malicious hackers and malware were just "unlucky," we thought. Most people and companies didn't suffer real damage if they were hit by hackers or malware. And we thought it was bad back then.

Boy, were we wrong!

How Bad Is It Now?

If there is one thing I'm surprised about today from being in cybersecurity for more than 36 years now, it's how bad Internet crime is today, and no one is really trying anything substantially different to fix it. I could never have imagined that we would have malware (i.e., ransomware) that is taking down thousands of companies a year, even huge conglomerates, entire cities, law enforcement,

and so on…stealing billions of dollars a year…literally killing people (i.e., death rates go up when ransomware hits hospitals), info-stealing malware accessing millions of passwords and logon "cookies" a day, taking over millions of user accounts a day, exploiting hundreds of thousands of devices a day, and stealing hundreds of millions of dollars a day from people and businesses.

People's credit card information is stolen so routinely that most people don't even mind that much. It's considered just part of how life works now. Victims just wait for their new cards in the mail and then update their Amazon and other online payment accounts. My personal credit card got stolen five times in 6 months this year, and I'm still using it (well, the updated version of it with new numbers). All our personal and confidential information has been stolen so many times that any time a new hacker breaches a billion new records about our lives, it barely makes the news. And most of us, when we read about the latest breach involving our information, just give a collective sigh. I mean, everyone's personal information has been stolen so many times already; what does one more theft of it really add to our personal risk?

Even if you don't see it in your personal email inbox, most emails on the Internet are malicious (e.g., spam, phishing attacks, etc.). Most of the bad emails are filtered out before they get to your inbox, but they are there, taking up bandwidth on the Internet. A large percentage of the messages sent to our phones are malicious. Social media sites are full of scam artists and romance scammers. It's difficult to sell or buy something on the Internet without getting scammed. A kid can send a ginormous distributed denial of service (DDoS) attack and take down almost any website or service for $5 or free.

Now add to all that already existing mess, artificial intelligence-enabled deepfakes. It takes me longer to create a new account on any of the thousands of free AI-enabled deepfake services than it does to create a deepfake audio or video of you or anyone else fraudulently saying or doing anything. All I need is a picture of the victim and six seconds of their voice to create a realistic-looking and sounding fake audio or video clip that would likely fool their mother.

Out of everything I could think of about the Internet and cybercrime in the early days, I could never have imagined how bad cyberattacks would get and that the world collectively really doesn't do much to stop them.

Well, billions are spent to stop malicious hackers and malware. Every year, more money is spent trying to stop cyberattacks than in the previous year. And every year, cyberattacks just get worse. And strangely, and befuddling to me, even though how we are defending is clearly not working, we aren't really doing anything different year-to-year to change things. We literally see how bad cybercrime is, predict it's likely to be worse next year, and then don't do anything significantly different to make better defenses.

Almost nothing anyone proposes works to significantly reduce cybercrime, or if it actually could, it never ends up getting widely deployed. Well, some rare things (like DMARC, SPF, and DKIM) do work and get broadly accepted but,

unfortunately, are so limited in what they impact that it's like plugging your finger in a dike that is already bursting around you. But there are a few examples of greatness and what could be.

Most Internet security fixes are temporary, whack-a-mole fixes to partially fix a very narrow, specific problem. Hackers can move around the new defenses in a day, and it then takes the Internet defense industry months to years to respond adequately. Defenders close one hole and the attackers open up a new one. It's an ever-changing game of hide and seek, and the hackers are always one step ahead and winning.

Most malicious hackers are able to steal millions of dollars and cause broad-spectrum harm without almost any fear of reprisal. To actually catch a hacker, present evidence, and have them charged, arrested, tried, and sentenced is far rarer than a lightning strike.

Imagine how good you would get if your job was to rob banks and you could never get caught, arrested, and stopped. Imagine that the worst penalty for robbing a bank was that you were stopped from robbing that particular bank, but you could drive to the next one and successfully rob it? And there was zero chance of getting arrested?

You would likely get very good at robbing banks. You would likely get very rich robbing banks. And unless you screwed up and accidentally made the wrong person mad, didn't pay the right bribe, or just got too insanely greedy, no one was ever going to stop you.

That is the story of today's Internet. It's full of crime, and nothing seems likely to change that soon.

There Is a Solution

Here's the surprising secret. There are ways to make the Internet and everyone on it significantly more resilient to malicious hacking attacks. It isn't impossible. In fact, it's far from impossible. It's do-able. And we could implement and achieve near-perfect Internet security with a modicum of change and expense in less than a year. Most people wouldn't even notice significant changes. They would just be along for the ride as we went from a very insecure Internet to a fairly secure Internet.

I've been thinking about how to make the Internet far more secure for my entire career. It's something I wake up and go to sleep thinking about. There hasn't been a day since 1987 that fixing the Internet hasn't been the majority of what I've been thinking about. It has become my life's passion.

If one day, I had been successful in helping to make the Internet a far safer place for people to compute, then my career would have been worth it. And if not, my career, as great as it has been for me and others I have helped in little ways, will have been an overall waste for humanity. I'm not here to fix the temporary little problems that fix only part of the problem. I want to fix it all.

That's the way I think about it. I feel a daily frustration because there are ways to fix the Internet and we just aren't doing them.

This book is a result of a solution I've been thinking about, refining, and promoting for more than 20 years to anyone who would listen or read.

My Early Writings on the Subject

Early on, when I first started to think about ways to solve the woes of the Internet, I was just envisioning better antivirus solutions, "next-generation" this and that, like nearly every computer security vendor was selling. But then I started to notice that all of that, version after version, the next big thing, was also failing. Nothing traditional seemed to be working. Even the new, supposedly better stuff was not working. And the reality was that each new year was worse than the last. It hasn't gotten better in more than 36 years. It just gets worse.

I started to ponder the larger underlying issues that were really causing all the other problems that I could see and experience. "Why was the Internet so full of crime?" Why aren't today's solutions working?" What would it take to make the Internet a far safer place to compute?"

About a year later, I had the beginnings of what would become my "Fix the Internet" solution. For a few years, I just posted my solution on various computer security blogs and Internet channels to anyone who would listen. Those postings are likely lost to time.

In 2005, I was made the weekly security columnist at *InfoWorld* magazine, a role I kept until 2019. I actively sought the job to broadcast my ideas about how to make the Internet a far safer place. The previous *InfoWorld* security columnists were promoting vendor ideas that were for sure not going to work. So, I claimed to be a better expert and asked for the job.

It was there that I began writing in earnest about the biggest underlying problem of why malicious hacking is so prevalent on the Internet, including this column on June 16, 2006: `https://www.infoworld.com/article/2189099/hackers-keep-hacking-because-they-can.html`. This was me finally figuring out why malicious hacking and crime were so rampant on the Internet. I finally had my answer to the first part of the problem.

With the actual problem at hand, I was able to come up with solutions. In June 2007, I wrote two *InfoWorld* columns about how to solve the problem of rampant Internet crime (`https://www.infoworld.com/article/2205234/the-security-solution-revolution.html` and `https://www.infoworld.com/article/2208906/the-security-solution-revolution-continued.html`). I wrote another on September 14, 2007 (`https://www.infoworld.com/article/2330189/trust-key-to-internet-security.html`). Six months later, in January 2008, I wrote another (`https://www.infoworld.com/article/2319151/internet-security-what-will-work.html`). The following is the headline and a bit of the article from that posting.

by Roger Grimes
Columnist

Internet security: What will work

Analysis
Jan 18, 2008 • 5 mins

Here's a radical plan for making the Internet safe for every legitimate user

That doesn't mean there aren't solutions. Last year, in several columns, I detailed one of the ways that a more secure Internet might be forged in the future. It's my vision. And the more I think about it, it's the only way I can see the Internet becoming significantly more secure. All other plans that I've come across break down under scrutiny or seem to rely on us becoming accustomed to a significant amount of computer crime. The other plans might reduce computer crime, but only temporarily and by a small amount.

I remember my editor-in-chief and friend, Eric Knorr, telling me to lay off writing so much about my plan to fix the Internet for a little while because I was repeating it over and over too much, perhaps boring the readers. Eric was probably right, but it didn't stop me from repeatedly re-stating an improved version of my solution several times a year for the rest of my career.

I eventually created a whitepaper and then resolved to write about and update that whitepaper every year or two. Here's a version from 2021: `https://www.linkedin.com/pulse/wanna-fix-internet-roger-grimes`. I sent it to industry luminaries and national cybersecurity leaders, like Bruce Schneier and Jen Easterly, director (until January 20, 2025) of the Cybersecurity and Infrastructure Security Agency (CISA). But I'm tired of writing and updating whitepapers and wanted to go a bit more formal. This book is the most recent and detailed look at my solution of how to make the Internet a far safer place for people to compute.

My solution today is far more mature and incorporates technologies that did not exist back in the early days of my articles and whitepapers, but when I look back at my original ideas from nearly two decades ago, I'm surprised that much of what they said is still the same basis of the stronger solution I promote today. Internet attacks have changed over time (not as much as you would think), but even with those changes, I didn't need to significantly update my solution. I think it's a sign of a good solution when changes in technologies and attacker methods don't mean you have to update your solution.

I've shown my "Fix the Internet" idea to thousands of people over the last 15 years. I've defended its ideas online to knowledgeable friends and industry luminaries, had its ideas covered by other publications, and even defended it in formal academic debates. All along, I've had critics poke holes and point out weaknesses. Along with debating to defend my ideas, I've always asked my

critics one central question: "OK, you don't like my proposal. That's OK. What can you think of to better secure the Internet that is better than my idea?"

I always hear crickets.

I get it. Solving the problem of significantly securing the Internet is not an easy task. It took me 20 years to come up with a good solution, and I'm constantly re-evaluating it. If you can come up with a better solution, I welcome it. I don't care whose solution wins as long as we do something different that works to significantly reduce cybercrime. But I do think that my solution is pretty good and will work.

Why Hasn't Your Solution Happened Yet?

Many readers might be asking why, if my solution is so good, hasn't it already taken over the Internet and made it more secure? That's a great question and if I knew the answer, I would be a billionaire. How to influence enough people so that we get a far more secure Internet is the remaining big challenge of my life and career. I either do it or fail. This book is part of that fight.

Fixing Internet security will take major company support (like from Google, Microsoft, etc.), and a sizable percentage of cybersecurity-minded companies, people, and governments from all walks of life and cultures, to support it. It's hard to get the people sitting at your dinner table to agree on something, much less the entire world. People and governments are very different in different parts of the world. People very much differ on what securing the Internet really means. I'll cover how I solved that problem in Part II of the book.

I've come to the ultimate conclusion that it will likely take a tipping point event, like a digital equivalent of the 9/11 attack, to happen to the Internet, where it goes down for a day or a week or even just a sizable portion of it, like all of banking or the stock market. Without a big enough wake-up event threatening the established order, I don't think we'll see much movement toward significant progress. After all, Internet crime is pretty bad right now, and no one is really doing anything other than small, incremental fixes that will not work to significantly improve the security of the Internet anytime soon.

Pain and tipping point events make things happen. 9/11 significantly improved the aircraft passenger industry and the entire mass travel industry beyond it. We knew that hijackers could get into cockpits and fly planes into buildings or that terrorists could sneak bombs onto planes in water bottles, toothpaste tubes, and underwear long before 9/11. Our travel security experts knew all of that was a possibility prior to what happened that day.

But it took 9/11 happening so that the needed defenses and interruption to our regular lives would not only happen without people yelling and being mad, but even begged for. Now, we all pour out our liquids, make sure our

toothpaste tube is only 3 ounces in size or less, throw away our sharp objects, and go through body scanners that can see our every contour. Before 9/11 happened, society simply wouldn't have tolerated it.

It took the pain happening for the needed defenses to be implemented. We, humans, are all taught to be proactive in school, but the reality is that we are mostly only reactive at scale, only implementing defenses after it's already too late, only after way more blood is on the ground than there needs to be.

Perhaps we will fix the Internet before something big happens, but I've been waiting for it for more than two decades. So, I'm not holding my breath. But I'm trying every day.

About This Book

The book is broken down with four major parts over 18 chapters. The first part defines what the problem is, part of which I've begun hinting to here in the preface. It will cover the major underlying problem that underlies all other problems. You can't solve the problem if you can't adequately define the problem. After understanding what the real Internet security problem is, Part II states the solution(s). It will do so in summary form and in more detail over individual chapters.

In Part III, I do threat modeling to find potential weaknesses and answer common questions. I'm not only open to someone finding fault with my ideas but invite it. If my ideas are good, they will withstand evaluation from smart people. Part IV covers other issues and challenges that need to be resolved in order for the Internet to be all it can be. Issues include minimizing vulnerabilities, better patching, and getting better international cooperation.

Acknowledgments

First, I want to thank KnowBe4 CEO Stu Sjouwerman and my team leader, Kathy Wattman, for their unflinching support of my goal to make the Internet a far better and safer place. They let me write, rant, and teach about it every day as my full-time job.

Special thanks to Dr. Loren Kohnfelder. If I can call anyone a mentor, it's Loren. Loren invented digital certificates in 1978 and is considered by many to be the "Father of PKI." He has never stopped trying to fix all the hardest problems in computer security. In our weekly talks, we regularly discuss how to fight hackers and improve Internet security. Loren was my sounding board for much of this project, he was my biggest constructive critic, and he always pushed me to better threat model everything I proposed.

Forever thanks to Bruce Schneier. His writings and books have impacted my thinking on how to better secure the Internet more than anyone else. He gets it better than anyone else.

I want to give special thanks to Tim Draegen, founder of Dmarcian and co-creator of DMARC. As one of the only people I know who has actually created and implemented a widespread recent Internet security standard, he has spent hours counseling me on how to be more effective and persuasive in trying to get my own solutions implemented.

Thanks to Zeke Hill, senior anti-cheat analyst at Riot Games, for educating me about how to best mitigate fake device IDs.

I want to thank Jim Minatel and Wiley for greenlighting this book. This is our sixth book together. Thanks to the rest of the Wiley team, including Ashirvad Moses and Annie Melnick.

Lastly, I strive to be as technically accurate and honest as possible. If you see a mistake in the book, it is solely mine.

Chapter Summaries

Here I summarize what is covered in each chapter.

Part I. Identifying the Problem

Part I discusses how bad Internet security is and the main underlying problem.

Chapter 1: How Bad Is Internet Security

Chapter 1 discusses how bad Internet cybercrime is, using reported statistics and figures. It shouldn't shock anyone that cybercrime involves many billions of dollars each year with millions and millions of victims. Any solution(s) to significantly improve Internet security, if successful, should significantly decrease these figures over time.

Chapter 2: How We Are Attacked and Why

This chapter covers how all Internet malicious hacking and malware exploitation happens. It focuses on the initial root access causes of hacking and the motivations of the involved cybercriminals. This chapter is a comprehensive, albeit brief, look at the cybercrime ecosystem that a good Internet security solution would mitigate.

Chapter 3: The Problem

Behind most cybercrime lies one main underlying problem that allows all the others to flourish. This chapter discusses a similar real-world crime issue and what it took to solve it. It covers the main Internet security problem we need to solve ahead of all others.

Chapter 4: Challenges

Internet security hasn't been great for decades. Everyone knows cybercrime is rampant. So why haven't better solutions been deployed for the decades the Internet has been in existence? Chapter 4 covers the big reasons why we don't yet have better Internet security. It covers these challenges that would impact any proposed solution from a strategic and tactical perspective.

Part II. The Technology Solution

Part II covers the theory and details of how to provide the solution to fix Internet security, including all its component parts and technologies.

Chapter 5: The Solution

Chapter 5 reveals the general theory of my proposed solution to better secure the Internet. It summarizes the solution and introduces the new paradigms and services, which are then covered in more detail in the following chapters. It includes a quick threat model of the general theory of the solution and how well it might work against today's Internet threats.

Chapter 6: Technology Solution Summary

Chapter 6 covers how the solution's general theory can be accomplished. It will introduce all the needed components and technologies. Then, Chapters 7–12 discuss each component in more detail.

Chapter 7: Trusted Identity

One of the central tenets of a more secure Internet is the ability for anyone to be able to trust the identity of those who are trying to connect to them. Today's Internet is the opposite of that, with pervasive anonymity and poor identity services far more common than not. Out of every part of the solution, this is

the most important part. If we do it right, we have a chance to better secure the Internet. If we fail at this one thing, there is no chance.

Chapter 8: Safe and Trusted Devices

You can't have a trusted user identity without ensuring that the user comes from a trusted location and device. If an attacker can compromise a user's device, nothing else that happens on it, including identity and authentication, can be trusted. Chapter 8 covers the technologies needed to give us safe and trusted devices, including safe hardware booting and reliable device identities.

Chapter 9: Trusted OSs and Apps

The operating systems and applications users use to compute, communicate, and connect to others must have strong integrity and trustworthiness. Chapter 9 covers how trusted operating systems and applications work. We are fairly close to having trusted operating systems and applications already; we just need them to be more pervasive.

Chapter 10: Trusted Networks

Once we have trusted devices, OS, applications, and identity, we need a trusted network path to ensure that all that goodness gets from point A to Z. Chapter 10 covers trusted networks, how we create them, and how we ensure that others can trust them.

Chapter 11: Trust Assurance Service

No matter how great your trust system is end-to-end, there will always be trusted nodes that get compromised and exploited. Badness will come from trusted places. Chapter 11 covers a DNS-like service with both client and global Internet components that any participating node can use to determine a particular communicating node's trustworthiness and see if it is or isn't reported as currently compromised. This service will likely have to be supported by substantial funding.

Chapter 12: Internet Security Global Alliance

Chapter 12 covers a new needed group of security matter experts dedicated to fixing and managing the Internet's security. Today's most popular Internet standards groups aren't dedicated to security and have not proven to be able

to deliver good security solutions in a timely manner. A different approach is needed; Chapter 12 discusses what that new approach should be.

Part III. Challenging the Solution

Every security defense product needs to be threat modeled. Part III covers a second threat model of the solution and answers common questions.

Chapter 13: Threat Modeling

Every cybersecurity solution should be publicly threat-modeled. Chapter 13 threat models the various types of attacks that can be attempted against the solution and technologies that were presented in Part II.

Chapter 14: Common Questions

Upon learning about my solution, which relies on verified identity, many people who believe in stronger privacy, if not absolutely anonymity, have legitimate privacy concerns about it. I've heard these questions and many others many times over the decades. Chapter 14 was written to discuss common questions and my answers.

Part IV. Other Needed Solutions

Internet security involves many big problems, not all of which are directly addressed with the solution proposed in this book. Part IV is a quick look at those other issues with other recommended solutions.

Chapter 15: Secure Coding

About one-third of all successful data breaches involve programmed software or firmware vulnerabilities and it has been this way since the beginning of computers. Chapter 15 covers the problem of insecure coding and suggests better fixes.

Chapter 16: Better Patching

Less than 2% of vulnerabilities in any given year are ever exploited by a real-world hacker against a real-world company. Still, unpatched vulnerabilities exist across the globe and large quantities, accounting for a third of all data breaches. Chapter 16 covers the problems with current patch management and recommends robust fixes.