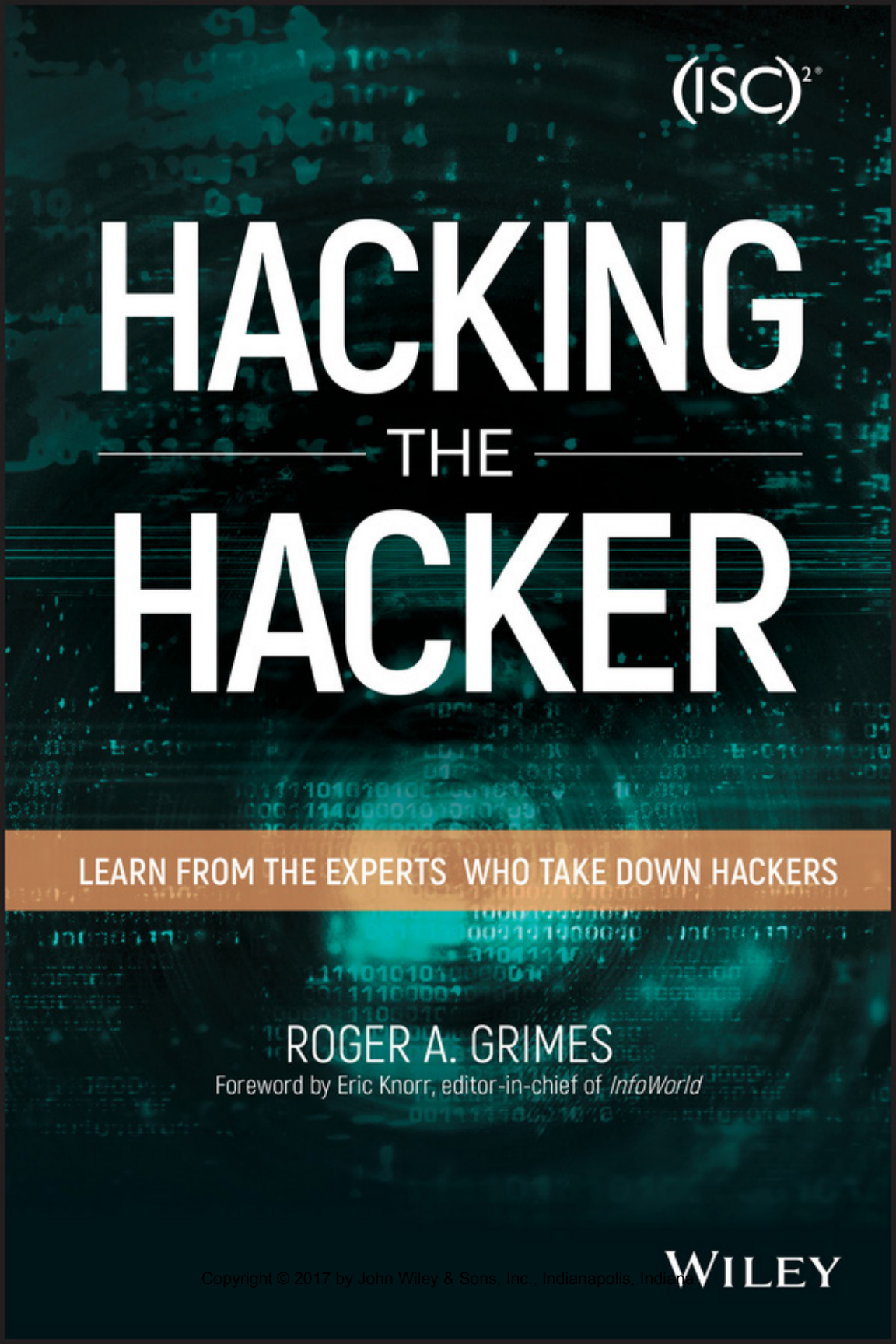

Copyright © 2017 by John Wiley & Sons, Inc., Indianapolis, Indiana

# Contents at a glance



Copyright © 2017 by John Wiley & Sons, Inc., Indianapolis, Indiana

Copyright © 2017 by John Wiley & Sons, Inc., Indianapolis, Indiana

Copyright © 2017 by John Wiley & Sons, Inc., Indianapolis, Indiana

# 1 What Type of Hacker Are You?

Many years ago, I moved into a house that had a wonderful attached garage. It was perfect for parking and protecting my boat and small RV. It was solidly constructed, without a single knot in any of the lumber. The electrical work was professional and the windows were high-quality and rated for 150 mph winds. Much of the inside was lined with aromatic red cedar wood, the kind that a carpenter would use to line a clothing chest or closet to make it smell good. Even though I can't hammer a nail straight, it was easy for me to see that the constructor knew what he was doing, cared about quality, and sweated the details.

A few weeks after I moved in, a city official came by and told me that the garage had been illegally constructed many years ago without a permit and I was going to have to tear it down or face stiff fines for each day of non-compliance. I called up the city to get a variance since it had been in existence for many years and was sold to me as part of my housing purchase. No dice. It had to be torn down immediately. A single day of fines was more than I could quickly make selling any of the scrap components if I took it down neatly. Financially speaking, the sooner I tore it down and had it hauled away, the better.

I got out a maul sledge hammer (essentially a thick iron ax built for demolition work) and in a matter of a few hours had destroyed the whole structure into a heap of wood and other construction debris. It wasn't lost on me in the moment that what had taken a quality craftsman probably weeks, if not months, to build, I had destroyed using my unskilled hands in far less time.

Contrary to popular belief, malicious hacking is more maul slinger than craftsman.

If you are lucky enough to consider a career as a computer hacker, you'll have to decide if you're going to aspire to safeguarding the common good or settle for pettier goals. Do you want to be a mischievous, criminal hacker or

Copyright © 2017 by John Wiley & Sons, Inc., Indianapolis, Indiana

a righteous, powerful defender? This book is proof that the best and most intelligent hackers work for the good side. They get to exercise their minds, grow intellectually, and not have to worry about being arrested. They get to work on the forefront of computer security, gain the admiration of their peers, further human advancement in the name of all that is good, and get well paid for it. This book is about the sometimes unsung heroes who make our incredible digital lives possible.

**NOTE** Although the terms "hacker" or "hacking" can refer to someone or an activity with either good or bad intentions, the popular use is almost always with a negative connotation. I realize that hackers can be good or bad, but I may use the terms without further qualification in this book to imply either a negative or a positive connotation just to save space. Use the whole meaning of my sentences to judge the intent of the terms.

## Most Hackers Aren't Geniuses

Unfortunately, nearly everyone who writes about criminal computer hackers without actual experience romanticizes them all as these uber-smart, god-like, mythical figures. They can guess any password in under a minute (especially if under threat of a gun, if you believe Hollywood), break into any system, and crack any encryption secret. They work mostly at night and drink copious amounts of energy drinks while littering their workspaces with remnants of potato chips and cupcakes. A school kid uses the teacher's stolen password to change some grades, and the media is fawning on him like he's the next Bill Gates or Mark Zuckerberg.

Hackers don't have to be brilliant. I'm living proof of that. Even though I've broken into every single place where I've ever been hired to do so, I've never completely understood quantum physics or Einstein's Theory of Relativity. I failed high school English twice, I never got higher than a C in math, and my grade point average of my first semester of college was 0.62. That was composed of five Fs and one A. The lone A was in a water safety class because I had already been an oceanfront lifeguard for five years. My bad grades were not only because I wasn't trying. I just wasn't that smart and I wasn't trying. I later learned that studying and working hard is often more valuable than

Copyright © 2017 by John Wiley & Sons, Inc., Indianapolis, Indiana

being born innately intelligent. I ended up finishing my university degree and excelling in the computer security world.

Still, even when writers aren't calling bad-guy hackers super-smart, readers often assume they are because they appear to be practicing some advanced black magic that the rest of the world does not know. In the collective psyche of the world, it's as if "malicious hacker" and "super intelligence" have to go together. It's simply not true. A few are smart, most are average, and some aren't very bright at all, just like the rest of the world. Hackers simply know some facts and processes that other people don't, just like a carpenter, plumber, or electrician.

## Defenders Are Hackers Plus

If we do an intellectual comparison alone, the defenders on average are smarter than the attackers. A defender has to know everything a malicious hacker does plus how to stop the attack. And that defense won't work unless it has almost no end-user involvement, works silently behind the scenes, and works perfectly (or almost perfectly) all the time. Show me a malicious hacker with a particular technique, and I'll show you more defenders that are smarter and better. It's just that the attacker usually gets more press. This book is an argument for equal time.

## Hackers Are Special

Even though I don't classify all hackers as super-smart, good, or bad, they all share a few common traits. One trait they have in common is a broad intellectual curiosity and willingness to try things outside the given interface or boundary. They aren't afraid to make their own way. Computer hackers are usually life hackers, hacking all sorts of things beyond computers. They are the type of people that when confronted with airport security are silently contemplating how they could sneak a weapon past the detectors even if they have no intention of actually doing so. They are figuring out whether the expensive printed concert tickets could be easily forged, even if they have no intention of attending for free. When they buy a television, they are wondering if they can access its operating system to gain some advantage. Show me a hacker, and I'll show you someone that is questioning status quo and exploring at all times.

Copyright © 2017 by John Wiley & Sons, Inc., Indianapolis, Indiana

**NOTE** At one point, my own hypothetical scheme for getting weapons past airport security involved using look-alike wheelchairs with weapons or explosives hidden inside the metal parts. The wheelchairs are often pushed past airport security without undergoing strong scrutiny.

## Hackers Are Persistent

After curiosity, a hacker's most useful trait is persistence. Every hacker, good or bad, knows the agony of long hours trying and trying again to get something to work. Malicious hackers look for defensive weaknesses. One mistake by the defender essentially renders the whole defense worthless. A defender must be perfect. Every computer and software program must be patched, every configuration appropriately secure, and every end-user perfectly trained. Or at least that is the goal. The defender knows that applied defenses may not always work or be applied as instructed, so they create "defense-in-depth" layers. Both malicious hackers and defenders are looking for weaknesses, just from opposite sides of the system. Both sides are participating in an ongoing war with many battles, wins, and losses. The most persistent side will win the war.

## Hacker Hats

I've been a hacker my whole life. I've gotten paid to break into places (which I had the legal authority to do). I've cracked passwords, broken into networks, and written malware. Never once did I break the law or cross an ethical boundary. This is not to say that I haven't had people try to tempt me to do so. Over the years, I've had friends who asked me to break into their suspected cheating spouse's cellphone, bosses who asked me to retrieve their boss's email, or people who asked to break into an evil hacker's server (without a warrant) to try to stop them from committing further hacking. Early on you have to decide who you are and what your ethics are. I decided that I would be a good hacker (a "whitehat" hacker), and whitehat hackers don't do illegal or unethical things.

Hackers who readily participate in illegal and unethical activities are called "blackhats." Hackers who make a living as a whitehat but secretly dabble in blackhat activities are known as "grayhats." My moral code is binary on this issue. Grayhats are blackhats. You either do illegal stuff or you don't. Rob a bank and I'll call you a bank robber no matter what you do with the money.

Copyright © 2017 by John Wiley & Sons, Inc., Indianapolis, Indiana

This is not to say that blackhats can't become whitehats. That happens all the time. The question for some of them is whether they will become a whitehat before having to spend a substantial amount of time in prison. Kevin Mitnick (https://en.wikipedia.org/wiki/Kevin_Mitnick), one of the most celebrated arrested hackers in history (and profiled in Chapter 5), has now lived a long life as a defender helping the common good. Robert T. Morris, the first guy to write and release a computer worm that took down the Internet (https://en.wikipedia.org/wiki/Morris_worm), eventually became an Association for Computing Machinery Fellow (http://awards.acm.org/award_winners/morris_4169967.cfm) "for contributions to computer networking, distributed systems, and operating systems."

Early on the boundary between legal and illegal hacking wasn't as clearly drawn as it is today. In fact, most early illegal hackers were given superhero cult status. Even I can't help but be personally drawn to some of them. John Draper (a.k.a. "Captain Crunch") used a toy whistle from a box of Cap'n Crunch cereal to generate a tone (2600 Hz) that could be used to steal free long-distance phone service. Many hackers who released private information for "the public good" have often been celebrated. But with a few exceptions, I've never taken the overly idealized view of malicious hackers. I've had a pretty clear vision that people doing unauthorized things to other people's computers and data are committing criminal acts.

Years ago, when I was first getting interested in computers, I read a book called *Hackers: Heroes of the Computer Revolution* by Steven Levy. In the dawning age of personal computers, Levy wrote an entertaining tale of hackers, good and mischievous, embodying the hacker ethos. Most of the book is dedicated to people who improved the world through the use of computers, but it also covered the type of hackers that would be arrested for their activities today. Some of these hackers believed the ends justified the means and followed a loose set of morals embodied by something Levy called "hacker ethics." Chief among these beliefs were the philosophies that any computer could be accessed for any legitimate reason, that all information should be free, and to distrust authority. It was a romanticized view of hacking and hackers, although it didn't hide the questionable ethical and legal issues. In fact, it centered around the newly pushed boundaries.

Steven Levy was the first author I ever sent a copy of his own book to and asked him to autograph my copy and send it back (something others have done to me a few times now that I'm the author of eight previous books). Levy has gone on to write or become the technical editor for several major

Copyright © 2017 by John Wiley & Sons, Inc., Indianapolis, Indiana

magazines, including *Newsweek*, *Wired*, and *Rolling Stone*, and he has written six other books on computer security issues. Levy continues to be a relevant technology writer to this day. His book, *Hackers*, introduced me to the wonderful world of hacking in general.

Later on, other books, like Ross Greenberg's *Flu-Shot* (long out of print) and John McAfee's *Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System* (`https://www.amazon.com/Computer-viruses-diddlers-programs-threats/dp/031202889X`) introduced me to fighting malicious hackers. I read these books and got excited enough to make a lifelong career out of combating the same threats.

Along the way, I've learned that the defenders are the smartest hackers. I don't want to paint all malicious hackers with the same brush of mediocrity. Each year, a few rogue hackers discover something new. There are a few very smart hackers. But the vast majority of malevolent hackers are fairly average and are just repeating something that has worked for twenty years. To be blunt, the average malicious hacker doesn't have enough programming talent to write a simple notepad application, much less discover on their own how to break into some place, crack encryption, or directly successfully guess at passwords—not without a lot of help from other hackers who previously did the real brain work years before.

The irony is that the uber-smart people I know about in the computer world aren't the malicious hackers, but the defenders. They have to know everything the hacker does, guess at what they might do in the future, and build a user-friendly, low-effort defense against it all. The defender world is full of PhDs, master's degree students, and successful entrepreneurs. Hackers rarely impress me. Defenders do all the time.

It is common for defenders to discover a new way of hacking something, only to remain publicly silent. It's the job of defenders to defend, and giving malicious hackers new ways to hack something before the defenses are in place won't make anyone else's life easier. It's a way of life for defenders to figure out a new hack and to help with closing the hole before it gets discovered by the outside world. That happens many more times than the other way around (such as the outside hacker discovering a new hole).

I've even seen defenders figure out a new hack, but for cost efficiency or timing reasons, the hole didn't get immediately fixed, and later on, some outside hacker gets credit as the "discoverer." Unfortunately, defenders don't always get immediate glory and gratification when they are doing their day jobs.

Copyright © 2017 by John Wiley & Sons, Inc., Indianapolis, Indiana

After watching both malicious hackers and defenders for nearly three decades, it's clear to me that the defenders are the more impressive of the two. It's not even close. If you want to show everyone how good you are with computers, don't show them a new hack. Show them a new, better defense. It doesn't require intelligence to find a new way of hacking. It mostly just takes persistence. But it does take a special and smart person to build something that can withstand constant hacking over a long period of time.

If you want to impress the world, don't tear down the garage. Instead, build code that can withstand the hacker's mauling axe.

Copyright © 2017 by John Wiley & Sons, Inc., Indianapolis, Indiana