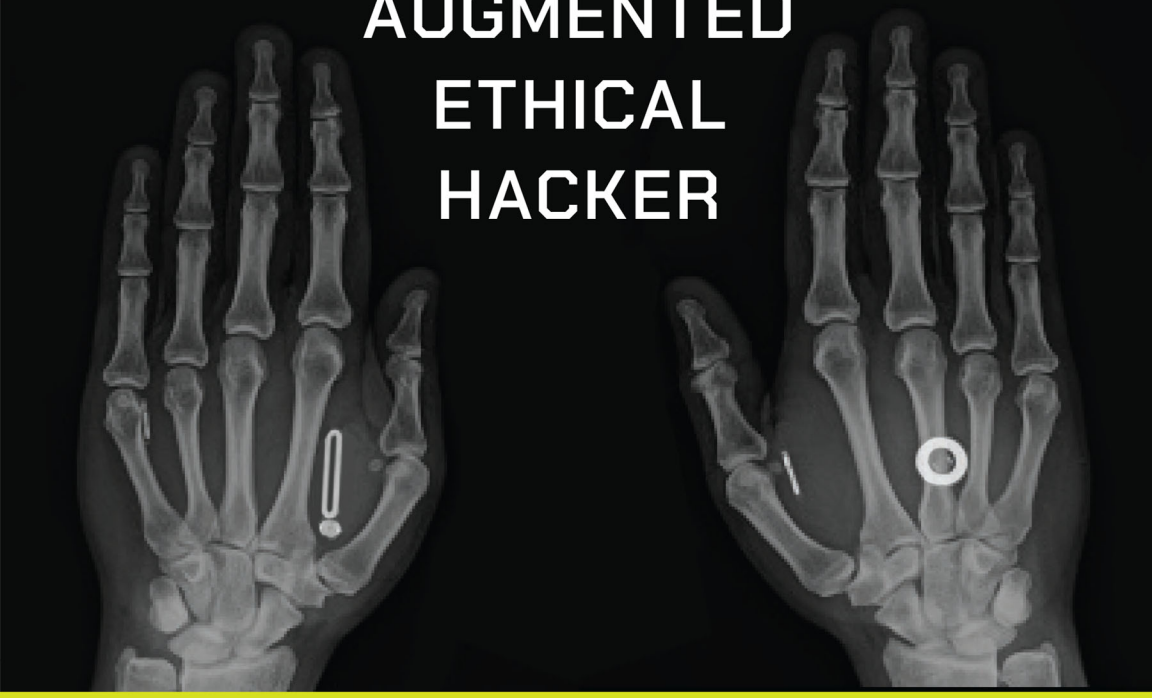
HUMAN HACKED

MY LIFE AND LESSONS AS THE WORLD'S FIRST AUGMENTED ETHICAL HACKER



LEN NOE
HaCkEr 213

Human Hacked

Human Hacked

My Life and Lessons as the World's First Augmented Ethical Hacker

LEN NOE

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada and the United Kingdom.

ISBNs: 9781394269167 (Paperback), 9781394269181 (ePDF), 9781394269174 (ePub)

Library of Congress Control Number: 2024945770

Cover image: Courtesy of Len Noe
Cover design: Wiley

This book is dedicated to my family. I didn't start out as something you could be proud of; I hope I have changed that.

To my wife, thank you for having the patience and understanding to see beyond the insanity that is me.

To my children, it took me a while, but I got it. I love you all.

To my grandchildren, Papa-Longbeard loves you more than life itself.

Contents at a Glance

Contents

Foreword

"Publicity, discussion, and agitation are necessary to accomplish any work of lasting benefit."

—Robert M. La Follette, Sr.'s speech in Evansville, Indiana (July 7, 1906), as quoted by Michael Wolraich in "Unreasonable Men: Theodore Roosevelt and the Republican Rebels Who Created Progressive Politics," July 22, 2014

The discussion of cybercriminals attacking various devices is a daily headline in print and online. Criminals seem to craft new and innovative ways to attack and exploit an ever-improving and robust defensive posture offered by cybersecurity "experts" around the globe. These experts will not hesitate to exclaim the threat loudly so they can sell you every solution you *need* 24 hours a day, seven days a week. Cybercriminals steal data and money, and cybersecurity companies demand data and money. Who wins? Not the people. They are too busy getting services or getting served; they are in the middle and completely lost in an increasingly more complex dance of ever-changing threats, vulnerabilities, and solutions. What is needed is a reference, a guide to what is happening and what will soon happen on a broad scale and certainly in the near future, information with principles that transcend time and something where those principles apply universally to all devices. It must include information about the expanding threat surface, the broader range of vulnerable available devices, and even things we do not consider part of our digitally connected world. . .yet. These concepts and ideas are not offered in the general discourse. There is a good reason for that: it would clarify the risks and threats so people could select the mitigation options and solutions they need in an informed manner. In short, they would spend less money. For our own sake, we need to see the future, understand it, identify the threats and vulnerabilities, assess the risks, and apply the most cost-effective solutions to mitigate our risk. We need this book.

This is the story of an unlikely hero told in his own words—his first-hand account of the human and transhuman experience—by a man who has chosen to be the solution, not just part of the solution, but the whole thing. Let me explain: in cybersecurity, we set up demonstration labs to test hardware and software for vulnerabilities and anything a malicious actor could inflict on us. We look for solutions so that when those components are put into a production unit, they will deliver the desired result or complete the desired action—no more and no less. In this story, that demonstration lab is a man, a man who has dedicated his life to the service of others, a man who sees the

future and knows we must be active now to ensure adequate security, which allows us to continue to enjoy the freedom in our lives.

I can faintly remember the events in 1969 when I was not quite five years old. My mother pointed to our 13-inch black-and-white TV set, the kind with the antenna on top. When you smacked it just right, the reception was crystal clear. We were in our apartment in North White Plains just north of New York City and watched Neil Armstrong change the course of human events. First, a jump, then one small step at a time into history. There was already so much history in and around the town where I grew up. Just a few miles from where we lived, lay the fields of Battle Hill, where General Washington defended the city of White Plains, and the Miller House, which was his local headquarters where he planned the city's defense. We were around the corner from the colossal Kensico Dam, built from the granite of a local quarry with a history all its own, an impact that changed the face of Westchester County forever and became a significant part of the New York City aqueduct system. In 1908, the Briarcliff Trophy Race was held. It was the first American International Road Race, and it encircled the county and ran cars by the names of Isotta, Fiat, Stearns, and Apperson among the finishers. As a kid growing up there, we learned and knew all these events were important, but none was more significant than that of Armstrong. When I was four years old, I understood it just as well as my six-year-old brother and my mother, who appeared to us to be frozen in time. Her face revealed the hidden depths of her feelings as she stood there, mouth slightly ajar, her expression utterly neutral. Now, 50 years later. . .

There are times when we have an epiphany of a significant change in the direction of our lives; then there is that once-in-a-lifetime awakening that signals a change in the future of the human race. To say that Armstrong's walk on the moon changed the course of human events is something of an understatement; most can say they know it happened, and some of us *lived* it. I believed deep in my heart for nearly five decades that I had experienced the seminal moment in human history in my lifetime. It was the pinnacle of achievement that unlocked the greatest adventure humans could experience. We knew the implications of that one act were immense, but we had no idea the breadth and scope of that impact. I acknowledge now that I believe I was wrong. I have worked hard over the years to highlight and inform audiences what I saw as the "Wild West" re-created in the medical IT space. I hoped to bring the message of human-machine interfaces, cooperation, and impending cyborgs with the importance of INFOSEC in DNA and at the submolecular level to the cybersecurity and medical worlds. My results were measured as success at best. I knew there was more, and I believed there was a story to tell, but the audience's appetite was lacking. People were suffering from malnutrition of information and ideas, but like a centenarian whose tender life and existence slipped away on their deathbed, they either refused food and drink or were too weak to engage.

My mind was changed on a hot and humid afternoon in Paris; it was June 29, 2022, to be precise. I had flown in for work because I was scheduled to speak at a conference, Hack in Paris. I planned to arrive with my wife (as I always do), but her father's passing had sidetracked our plans—she would have to join me later as our three children went with her to the services. I stayed at the hotel contracted by the company sponsoring the conference and made my way downstairs to the lobby area for a café. Near the restaurant was the bar, three stools in all, but on the farthest one sat a person who *had* to be a hacker. I could make out the outline through the opaque glass with a classical floral arrangement etched into it, birds and flowers. But I could not directly see the person. The words, the phrases, it could be only one thing—a unicorn! It had to be an American hacker. Now, most hackers are introverts while most Americans are extroverts, but for the next few minutes, the bar was to stage a performance of epic proportions; yes, this was a spectacle I did not want to miss. I had come to Paris to find an American enigma wrapped in a paradox; I was intrigued. I dared not turn away as I jockeyed myself to the most expensive seats in the orchestra section in the bar. I was in the front row.

I always try to blend in when in Paris; I mean, my French is pretty good (so say my French friends as they snicker in my face). I can quietly order food and get and give directions; I can even quietly ask for a bathroom. I want you to realize I can do all that loudly, too. I am from New York, and when appropriate, I do. This situation was different; it was the quintessential French bar in a quiet, posh hotel, but this guy was louder than all the other collective souls in the bar all by himself. He was not rude or arrogant; he was a jovial and pleasant guy with a friendly voice. His comments were nothing but pleasantries, and then I looked up and saw him—I was stunned. He was polite and respectful of everyone he engaged. Len was just happy and loved having a moment with the people there. But his body told a story of many lives and many miles. He was a fresh spirit who had found his freedom through the years of tough mileage. This is Len Noe; he loves life.

These past couple of years, I have gotten to know Len, and I can characterize him as a fun-loving yet serious individual who saw the future yesterday and plans today for people to be comfortable and safe with their tomorrows. Some are gifted with insight, few can engage with critical problem-solving skills and logic, and even fewer are gifted with the motivation for action—a chance to be part of the future and, simultaneously, part of history. Len has all these: he sees the future, he analyzes the pros and the cons and the multitude of variables that will impact who we are and where we are going, and, most significantly, he puts himself directly in the middle of an amazing human experiment looking to offer insight and solutions to us mere mortals.

That seminal moment of which I spoke was not in 1969; no, it is now, or more precisely, it was when I met Len Noe. I was astonished! He knew what I knew: that the intersection of people and technology is that moment; it took me meeting another like-minded individual to make that infant concept

blossom into a moment of actualization. This is not the extension of humans and technology; no, this is the integration of technology and people. Len lives at the threshold of the path of eternal opportunity and is leading us all forward. This book shows those traditional boundaries blending and disappearing; you will see the possibilities of technology and the trajectory of abilities and understand what that means for all of us. Cybersecurity and device security are not new concepts but rather imperfect ones. It all began a short time ago in a place not far from most of us. . .

Medical devices were first, and they taught us that we could use a computer in vivo, or inside the body, to make our lives more functional and to make us freer from the restrictions of a crippling medical condition. It took a brave soul at the FOCUS 11 at a Las Vegas conference to show us that we cannot be quick to put these devices in vivo without a thorough security check. Barnaby Jack, a New Zealand–born hacker, got access to an insulin pump using a high-gain antenna, and then in 2012, he demonstrated how to kill someone with a pacemaker. The security gauntlet had been thrown down.

Jack is not the first to point out critical devices' complete and inadequate security. From their inception, SCADA boxes (supervisory control and data acquisition boxes) have been widely used to manage critical infrastructure. Initial SCADA systems relied on large minicomputers for computing tasks and operated as independent systems without connectivity to other systems. Communication protocols used were proprietary and lacked standardization, meaning one could not talk to another outside their company or function.

With advancements, SCADA systems evolved to distributed architectures, where processing was distributed across multiple stations connected by a local area network (LAN), reducing costs compared to the first generation. However, security was still overlooked due to proprietary protocols and limited understanding beyond developers.

Today, SCADA systems leverage web technologies, enabling users to access data and control processes remotely via web browsers like Brave, Google Chrome, and Mozilla Firefox. This shift to web SCADA systems enhances accessibility across various platforms, including servers, personal computers, tablets, and mobile phones. Most important, they are drenched in security processes and protocols. That is a good thing because who can conceive a person being used as a SCADA device, and what could that do to critical infrastructure? In the historical context, it seems the lesson was learned, so what about medical and public health issues?

The threats a hacker poses with in vivo offensive devices designed to hack other in vivo devices, such as the insulin pump or a handheld device like a cell phone or tablet, are significant and concerning. With the advancement of technology and the integration of human-embeddable devices, such as Radio Frequency Identification (RFID) chips and pacemakers, into the human body, the potential for malicious exploitation and cyberattacks increases. The threat

surface keeps growing, which means there are more and more ways for a criminal to manipulate your phone or pacemaker.

If all of this sounds deathly frightening, think of the problems caused if a malicious actor used an in vivo offensive device to launch an attack that loads inaccurate data into your pacemaker, so much so that your doctor decides to change your medication or treatment. That same malicious actor could also insert content into the cell phone of a high-level diplomat who is closing a deal to provide humanitarian relief to a country or a region recently hit by a natural disaster. How would the other diplomats take it if that attack loaded images created by deepfake technology to send underage child porn from one of the other diplomats' phones to all the other diplomats? Would the deal still go through, or would it potentially lead to war? Now let's say it goes to the BBC for the whole world to see, for the world to judge. . .it is the only story to talk about for the next week until the news cycle is updated.

What else could a malicious actor do? Plenty, and it could range from mildly inconvenient to debilitating or even deadly. Most would come in the form of standard attacks that include remote control, manipulation, data breach, malware injection, or exploitation of vulnerabilities in other ways. None of this sounds pleasant to the average person, and what's worse is that the average citizen has no defense against them.

To say this is a doom-and-gloom book is not accurate. So we will get to the key message of this book, and that is the plethora of usable information it provides. It is all about understanding threats from malicious actors and criminals using in vivo implanted cyber tools to attack those same people in plain language, a guide for average citizens and security experts alike.

Len explicitly breaks down complex subjects into language that anyone can understand. He is the experiment; he is giving us information that he has collected and solutions that we can understand. He addresses security concerns that most security experts have never considered a threat. Len is a visionary who has taken action to face those threats by boldly engaging and leading by example.

Is this a work of lasting benefit? I say yes, and I know you will, too. The public discourse and awareness around in vivo hacking techniques and appropriate security and mitigation techniques will impact everyone and will be a focus of discussion in the future, but that conversation must start now.

Len, keep agitating! People are listening.

And it begins. . .

Introduction

Sufficiently advanced technology is indistinguishable from magic.

—Arthur C. Clark

For hackers, it's all about the challenge. To us, every system is a puzzle waiting to be solved, a chance to prove our skills. With laptops as our tools, we're not just tech enthusiasts, we're digital assassins, thriving on the adrenaline of outsmarting the most complex codes and anyone with the arrogance to claim their networks and systems are secure.

Sometimes it's almost too easy. Everyone wants to be a hero, and nobody likes a scene. It's all mine for the taking; I just have to see who today's lucky victim is. It's a public place—people everywhere walking and carrying on without a care in the world. Stores entice shoppers with sales and gimmicks everywhere—to me it's like taking candy from a baby. I don't know them, and it's nothing personal; everyone is fair game. If you haven't figured it out by now, I am a hacker. Today there is something special I need, something very specific. In this case, it's a link in a much larger attack. I like keeping things random, that way I'm less likely to be discovered. I'm not even worried about being caught with the tools I use. I promise you won't see them. I have the payload set for Android; now it's time to destroy someone's life.

I see *you* standing there looking like a zombie, head in your phone. I wonder what may have you so enthralled that the rest of the world has ceased to exist. But in reality, who cares? I'll look for myself soon enough. The overhead music is drowning out the muffled chatter of multiple conversations on the move. You're my target today because you meet the criteria I'm looking for. I would love to build your ego and say it's because you look like someone whose career choice or wardrobe would make you a target, but in this case it's not that sophisticated. The fact that you haven't looked up from your Android phone in the last five minutes and are completely oblivious to the world around you may be the perfect combination for what I'm looking for.

I know you are not paying attention as I close the distance between us, your head still in the phone, just as I expected. You haven't looked up in a while now; I hope whatever you are doing was worth it. The people around me seem to fade into the background. There is nobody else in the world for the next few minutes; it's just you and me. I have set the stage, all the pieces are in place, I will know whatever I want about you before the end of the day, and that's just the beginning. What's worse is I will use *your* device for that upcoming larger attack that will lead the authorities right to *you*. Imagine trying to explain that *you* had no idea that *your* phone was involved in a

cyberattack against a large corporation with expensive lawyers. You have no idea what's about to happen, and even worse is when it's over, you still won't.

I'm shrieking at the top of my lungs, "Oh God, please help me! Please someone help me!" I think I have your attention. Now everyone is looking, anticipating what's going to come next. All they see is an older man in what appears to be in extreme distress screaming for help. Social engineering is only one of the tools in my arsenal; I have been doing things like this for a long time. "Please, *you*, I was just on a call with my daughter, and there has been an emergency with my infant grandchild. My battery just died. She was on the way to the hospital in an ambulance. I don't know where they are going"—insert crying and sounds of agony—"Please, *you*, can I use your phone to call my daughter back to find where I need to go? Please! *Oh God*!" Buckle up, let's go for a ride together.

All eyes are on you now, it may be just you and me in this little game, but we have quite the audience here watching my little spectacle. I selected this place for that exact reason: I need all these onlookers for my plan to work. At this point, how can you say no? Remember, in this day and age if there is anything exciting, someone is recording it on their phone. Do *you* wanna go viral? Do you *really* want to take the chance that this video could get out? Do you want to be the hero or the next meme about a heartless person? I am playing you; I just put you into a situation you can't get out of. How many bystanders are staring at us? I am sure you are feeling the pressure at this point, but I'm not—this is all by my design, and it's all playing out exactly like I want it to.

So, of course, you agree. What real choice did I leave you with? By this point, you may have even started to feel good about helping me. Who would want to be in my shoes if the circumstances were reversed? Nobody seems to notice the smile that comes to the corners of my lips as your arm extends to hand me the phone. The cold feeling of the case as it slides in my hand—the hard part is over. Now for the next act.

I start moving my arms around and start talking to myself out loud; I have to make this believable. "What's my daughter's phone number? Who remembers phone numbers anymore? They are all programmed into my phone!" During all my ministrations of my arms and keeping the focus on me, I look at the screen. Nothing, guess this one is going to be the full show. "Her area code is 313, 313. . .722? Oh God, my grandbaby!" Turning in circles in apparent shock and anguish, I swipe down from the top and quickly enable Near Field Communications (NFC)—thank you Android for standardization. Swiping back up with my thumb, I see what I have been waiting to see. I know it's psychosomatic, but I can't help but almost *feel* it. . .there's the pop-up on the screen.

URL redirection requesting a download. "313-722-6. . ." Accept download. "What hospitals are close to here?" Accept Install from unknown source, done. "I can't believe I can't remember her number"—insert more crying and

acting ashamed—"I can't remember. You have been so kind. Thank you so much, but I have to go plug my phone in to get the number." Nobody understands how hard it is to fight smiling now. It's time to go. Handing you back your phone, I thank you profusely as I slowly fade back into the crowd. Your phone is already connected to my command-and-control server. I have already compromised your phone, and you are still watching me walk away—possibly wondering what just happened, possibly saying a prayer for my injured granddaughter. Whatever the case, you will go back to your day, your life. The fact that I'm going with you *inside* the device that holds more data than your wallet or purse will stay my little secret. . .for now.

What was the purpose of this deception, you ask? To hack your phone right in front of your eyes—and *you* have no idea it even happened. I did it not just with *you* watching me; I did it with the *whole crowd* watching me and possibly live streaming the entire event. This is a testament to how blatant I can be and still not get caught.

You never saw me possibly enable NFC—you were put on the spot and were essentially just acting out the part that I had selected for you to play in this drama. How many normal end users know what NFC is used for? Would you even notice later it was on and think "I need to run anti-virus, anti-malware, scan my phone?" Of course not, because "phones don't get attacked like that; they are not computers."

Surprise: They do, and I can do it better than most. If you noticed at all, would you think that maybe you hit that NFC button by accident and turn it back off? If so, you'd missed the only clue I left—good luck with any investigation later. Would you even connect our little interaction as an attack, or would it be relegated to the back of your mind as a strange social event? Honestly, most devices have NFC enabled for the purposes of Apple Pay and Android Wallet. Can't have that convenience without opening a vulnerability for me.

I played you. I used misdirection to keep your eyes focused on me. You were looking at a man breaking down, not the fact that my thumb was accepting the download and installing my payload on your device. Before I explain how I pulled this off, let me ask you a question: if you did see the request for download pop up, what caused it to happen in the first place? How would *you* explain the fact that *your* device just magically decided to download my specific payload the minute it was in *my* hand?

You never saw the bulge in the top of my hand hiding a microchip as it energized from your mobile device; you never noticed that, while I had your attention, my fingers were doing something completely different, something destructive and invasive. You would know if someone was attacking your technology right in front of you. . .*wouldn't you*?

You see through the eyes of the old, expecting to see hackers sitting in a dark basement with a hoodies on, staring at a computer terminals with lines of green code in an endless loop of scrolling characters. But that's not the case anymore—I did hack you and your mobile device, and I used bleeding-edge