Confessions of a Hacker

CLAYTON MCILRATH

I just doxed myself

In the last few years, we have seen a multitude of attacks against large corporations such as Target, Home Depot and Chase as well as government bodies like the Central Intelligence Agency, Federal Bureau of Investigations, and the United Nations. As technology becomes increasingly vital to institutions, so too does the importance of securing that tech. You are likely reading this as your own interest has been piqued, perhaps by one of the many well known data breaches that have occurred in recent years, or possibly because you work in the tech industry and are aware that security is a growing concern in the space. Whatever the case, by learning more about security, you are taking a step in the right direction in educating yourself. With a quick primer to the history of hacking and a correction of any misconceptions you may have about security, you will be better equipped to creating more secure applications and/or infrastructure.

The best place to start in better understanding security is to break the various impressions or preconceived notions that you may have acquired from the media about hacking. ***When you think of a hacker, what immediately comes to mind?*** Do you picture a character working on half a dozen monitors, typing rapidly and eventually arriving at some sort of “access granted” screen? Hollywood likes to portray hackers in a very specific light to make for better stories. In reality a hacker is no more than a tinkerer of technology.

Many programmers from mobile developers, hardware makers, and enterprise application developers are also hackers.

The term “hacker” is not even the best word to describe the nefarious technologists that appear in the news or media, though they are the ones to blame for liberally using the word hacker and inevitably changing the meaning. To most people in tech world, a “hacker” only denotes that an individual likes to push the boundaries of technology. A “cracker” is probably the word that reporters and writers should learn. Originally derived from the words “criminal hacker,” a cracker usually has a specific focus and mission in mind, often with malicious intent. Thus, you will see hacker used more often in the tech world (e.g.: “hackathon” events) to describe someone who likes to frequently work with different languages, tools and hardware. Cracker, on the other hand, is more often used by security experts to describe the malicious hackers.

Since ethics and morals are so hard to discern in the world of hacking, it is more important to embrace the myriad of intents and understand the basics of supporting solid security. Getting in the head of a hacker may be next to impossible without being a hacker yourself, but there are measures such as regular auditing and maintenance which can go along way towards making your network, hardware or applications more secure.

Before we dive into the history and facts, let’s make this a bit more personal. Allow me to do something that no hacker ever does: reveal to you my identity. In the hacker world, we call this “doxing” which generally comes with some very negative connotations. Identity is one of the most precious and valuable pieces of information one can own. Possessing intimate details about an individual is the first step towards accessing their finances, history, secrets, and possessions. Without further ado: ***my name is Clay Mcilrath, and I am a hacker***. There, I said it. Phew. I'm a little scared of what the world can do with that bit of information alone, but ultimately have to trust that my measures of securing myself will go a long way towards keeping my information safe. These days, I like to call myself a "security expert" as this is the more politically correct way of saying, "I am a hacker." As a mostly white hat hacker—ahem, I mean security expert—it is my personal goal to help others recover or prevent data breaches. I often do so by educating others so that they too, may think as I do. I hope this book helps you in your journey. Just by reading this, you are taking much greater strides towards protecting yourself and that is a great step in the right direction!

CHAPTER 1

Hacker lingo

Even though most technology terms are often very lame, hacker lingo is often amusing with origins in something a little more original and unique. In order to understand hackers, you must first understand the history, tools, and techniques which have paved the way for hackers.

Phreaking

Hacking was born in the early days of telecommunication. A hacker is considered a "phreak" if he or she manipulates or explores the software or hardware of telecommunication systems. From the fifties through to the new millennium, phreaking was not just a hobby, but a necessity for early hackers. The prices of long distance phone calls were steep, so phreaks would often manipulate the telecom companies to steal access codes and credits for more network time. These codes also served as a form of currency and may have been the inspiration for modern day crypto currencies such as Bitcoin.

Phreaking was the entry point to hacking as computers were first coming to the consumer market. Most hackers still hosted their conversations through telecom and used bulletin boards to post messages and share files. This allowed hackers to sharing secrets and connect with one another in person. Though modern telecom software is more secure today, phreaking still lives on through impersonation and manipulation of people within telecom companies. Most of the interest in modern day phreaking exists in only a "because I can" type of scenario.

Internet Relay Chat (IRC)

Entering the scene in the late eighties, and becoming very popular in the nineties, IRC quickly became the main form of communication between the early adopters of the internet. It is conceptually the same as modern day instant messaging or chat rooms, except the communication protocols and number of people involved in these chat rooms are much greater than you will find elsewhere. That statement is still true to this day, as IRC lives strong in the technical community, with popular channels still numbering in the thousands. IRC is mostly used by people in the technical industry, especially programmers and hackers.

Regular Expressions, Ciphers and Obfuscation

Programmers rely on regular expressions (regex) to identify and parse patterns in text or other data. A regular expression allows a developer to specify a pattern and then run that pattern search over a payload and identify any matches. A simple example of this would be to say in plain English: Find me all words containing the letters "r," "e," "d" in that order and case. This would then match the bold characters only in the following sentence:

Fred likes go to bed after eating his bread.
He also really loves the color red.

Through the development of more advanced matching formulas and algorithms, regex has evolved to become prevalent in many forms of programming, and subsequently hacking. With a more complex formula, newer information can be extracted and parsed, and machine learning algorithms can be created to start building intelligent systems that understand everything from human sentiment to hidden messages. Here is another example that matches the first letter of every word to show a hidden message:

Hello, I do drugs everyday now.
Maybe every Saturday, Sunday are good, eh?

Someone that happens across it without knowing the code might see just a weirdly formatted message perhaps dismissed as some internet troll, but shared between two people who understand the pattern, an entire subtext can be hidden. These simple ciphers are used by some of the more cryptic hackers to regularly obfuscate their communications, especially when talking through public channels. Likewise, security researches and government agencies try to create their own regex patterns to discover these “hidden in plain sight” ciphers and create smarter algorithms to decipher them.

I personally only use regex on a regular basis when it comes to scraping data from websites. Much of the data on the internet is available to digest in some way, but rarely is that data easily consumed or formatted nicely. My favorite project was for a media company that publishes daily arrest information and mugshots in a sleazy but amusing newspaper and website. This data is freely available on various county jail websites, but rarely as a database or flat files. Instead, I had to build out a scraping tool that relied heavily on regular expressions to parse different websites for the information, and then save that data to the server. Many times this involved parsing and reverse engineering many layers of obfuscation used by these government websites, as well as deciphering some of the authentication schemes and tokens used to verify that I was human.

Social Engineering

When it comes to modern hacking, understanding psychology is almost as relevant and important as understanding hardware or software. Many attacks on individuals are executed without a single line of code or software. I define social engineering as the process of leveraging personal information about an individual with a selfish or malicious intent. Social engineering can be used for everything from resetting passwords on bank accounts to manipulating people to do what you want. Hackers see the human brain as a logical, and vulnerable system, much like a complex computer program. This allows them to use logic, reasoning and emotion to discover the weak points of an individual.

Hackers use social engineering tactics on a regular basis to gain certain privileges and advantages in everyday life. I have witnessed many situations where a hacker was able to persuade a business to give them their product or provide a service for free.

I have to admit, I am guilty of using social engineering on a regular basis, sometimes without any conscious thought. Often times it is for something harmless in everyday life. For example, when I go to a bar or club that is charging a cover, I will analyze the setting and the bouncer to ascertain what type of conversation will allow me passage for free. Many times, I have simply said, "I left my credit card at the bar" or "I already paid, I just came outside to have a smoke" and been ushered in without a second look. Most people do not attempt such simple things either because they are bound morally or they do not think about manipulating people and situations in this way.

CHAPTER 2

Hackers are Everywhere

If you are like most people without exposure to security or a deep understanding of technology, then your views of a hacker may be skewed by the media. You have probably read or listened to the news reports about Edward Snowden, or think of hackers as the movies would portray them. It is almost a given that you have heard about the popular data breaches to Target and Home Depot in the last few years. While these events are incredibly well known, very rarely is there a name released and made popular like Snowden's. If hackers are real, then why are there so few names published in the media when a security breach is reported on? Many hackers spend a great deal of time and effort to protect their anonymity and hide behind many layers of software to remain hidden. Furthermore, hackers usually hide behind the name of an organization, often called a "sec," protecting their identity in numbers like a school of fish swimming together. Identity is so sacred to most hackers, that being discovered, or "doxed," is considered one of the worst possible outcomes.

The term "hacker" appears every day plastered across news headlines. The onslaught of news stories about hacks in the past few years means the general population knows that hacking happens outside of movies and books. Most of us think of hackers as menacing shadows lurking anonymously behind computer screens. We're certain that we don't want a hacker to gain access to our banking information, our social media accounts, or to any of the companies that may hold our personal data, but beyond that we have only murky ideas of what a hacker truly does and an unsettling but nebulous fear of the ramifications of modern day hacking.

Although hackers may seem to be elusive and mysterious, the truth is, they exist everywhere both online and off and many of them are just average people. Out of the rough estimate of 18 million developers in the world, it is likely that a majority of them could be considered a hacker. While that is a substantial amount of hackers, it is important to remember that hackers are generally only technologists that push the boundaries of hardware or software. Not all of them actively participate in black hat activities. Still, that is quite a large number, and if you regularly attend tech events you have likely shaken hands with a number of hackers already.

The early days of hacking

Cyber hacking was born before long before the internet as hackers exploited and probed telecommunication systems. A hacker is considered a "phreak" if he or she manipulates or explores the software or hardware of telecommunication systems. From the fifties through to the new millennium, phreaking was not just a hobby, but a necessity for early hackers. The prices of long distance phone calls were steep, so phreaks would often manipulate the telecom companies to steal access codes and credits for more network time. These codes also served as a form of currency and may have been the inspiration for modern day crypto currencies such as Bitcoin.

Phreaking was the entry point to hacking as computers were first coming to the consumer market. Most hackers still hosted their conversations through telecom and used bulletin boards to post messages and share files. This allowed hackers to sharing secrets and connect with one another in person. Though modern telecom software is more secure today, phreaking still lives on through impersonation and manipulation of people within telecom companies. Most of the interest in modern day phreaking exists in only a "because I can" type of scenario.

One of the most famous hackers in the days of phreaking was a hacker by the name of Kevin "Darkside" Mitnick. He was the most famous and publicized hacker in the 90's, notorious for his phreaking abilities. Mitnick played a cat and mouse game with the FBI for many years. He has penetrated many organizations including Novell, Sun Microsystems, and even went as far as spying on FBI phone calls. He had an addiction of sorts to hacking and for him the incentives were based entirely on the satisfaction of getting into a system or business through social engineering and software exploits. Often times his theft and impact was minimal, with childish antics of pranking individuals or calling celebrities. Still, the media loved to blame problems on Kevin and his hacks helped drive many legislative efforts towards regulating and criminalizing acts in cyber security. Kevin has a great book called Ghost in the Wires where he shares his personal experiences and journeys of phreaking.

Before the publicity of Kevin Mitnick, most of the public new very little about phreaking or hacking of any kind. Breaches to telecom companies were often kept quiet, as the businesses did not want a negative impact from the publicity. One such breach, that did not become well know for some time after, was initiated by the German hacker, Markus Hess in the 1980's. Hess was recruited by the KGB to spy for the Soviets and tasked with penetrating US military systems in order to obtain classified information. He was able to breach an estimated 400 computers in the United States, Germany and Japan including systems at MIT and the Pentagon. It was some time later that Hess' activity was detected and Hess was apprehended. This has since been publicized in a great book, The Cuckoo's Egg yet still has not become common knowledge.

As hackers came online

As technology and the internet became more accessible, many early phreaks started communicating with bulletin board systems and Internet Relay Chat (IRC) in order to share ideas, documents, and secrets with one another. As IRC quickly became a new standard form of communication between the early adopters of the internet, hackers started to find each other more easily to share knowledge and secrets with one another. IRC is conceptually pretty much the exact same as modern day instant messaging or chat rooms, except the communication protocols and number of people involved in these chat rooms are much greater than you will find elsewhere. That statement is still true to this day, as IRC lives strong in the technical community, with popular channels still numbering in the thousands. In general, IRC is only used by those in the technical industry, especially programmers and hackers.

Looking back on the hackers of old, many of them fall into a category that security experts today label as "elite." Labels are all a matter of perception, and an elite status is ranked the highest. Some elite hackers were introduced to hacking with analog systems such as phreaking or if they were on the digital front, they were writing most of their programs in machine code. These programmers know what "31337" means, and not because some young, wannabe-hackers made the term popular again in recent years. In the early days of the net, servers were expensive, so most IRC chats were hosted on public servers, and many people had to rely on them. For this reason, hackers that used these public servers needed a way to obfuscate their conversations from regex searching. One group had the bright idea of inventing 31337-speak which would represent letters in a way the human brain could interpret, but a machine would not be able to search. For example, with “31337” notice how a “3” looks similar to a backwards capital “E” and “1” looks like a lowercase “L” and finally “7” looks close enough to a capital “T.” This is where the term “elite” originates from, and is a great example of hacker culture.

Most programmers in the early 90’s were hackers or crackers in some way, because they were building low-level systems that ran large businesses. Programming languages were also more difficult to learn, so the barrier to entry was much higher. To be considered a good software creator you also needed to know how to break code. Many of these original programmers and hackers are among the most elite today. While there have been more layers added on over the last couple decades, much of the foundation is still the same: Assembly, C, Java, Cobol and Fortran are still at the core of almost all technology on the planet. This means that the elites in the hacker world understand the core of most technology more than the modern day software creators that are building on top of it.

Aside from just an understanding of technology, what really drives some of the best hackers is an understanding in psychology. Many attacks on individuals and businesses are executed without the use of complex technology or tools. The process of leveraging or extracting personal information with malicious or selfish intent, is often called social engineering. Social engineering can be used for everything from resetting passwords on bank accounts to manipulating people to do what you want. Hackers see the human brain as a logical, and vulnerable system, no different than a complex computer program. This allows them to use logic, reasoning and emotion in order to discover the weak points of an individual.

While most hackers escape with only minor traces of their organization left behind, there have been times when individuals have come forward or been captured. Most of these names never make the headlines, however, and thus tend to only be known within circles involved with security. Perhaps the most well-known hacker in the world, Edward Snowden, used his access and connections as a contractor for the CIA and NSA to release thousands of documents to the public. While this act alone is not exactly a form of hacking, his background is very much in security and systems, which qualifies him for both the title and reputation. Snowden is a great example of a morally motivated black hat, akin to the Anonymous hacker sec, and as such he has received both praise and criticism for his exploits.

Like Snowden, and often times working alongside him, Julian Assange has been a notorious hacktivist for quite some time. He is well known for his creation of WikiLeaks, a website that allows whistle-blowers and informants to anonymously share classified documents with the public. Many such documents are contributed by the black hat actions of hacktivist secs and individuals, in addition to inner operatives and employees within government institutions.

Present day hackers

Names like Mitnick, Snowden and Assange are recognized by most of the general public for their whistle-blower actions while many other hackers remain anonymous. As hackers became more famous and laws were created and defined to make exploits criminal, there arose a need for more secracy and anonymity. This has lead to the creation of hacker groups, or secs, which have replaced individual names and aliases in many contexts.

For years hacker secs have been relatively small and tight knit. Each hacker sec is built up by like-minded individuals and often shares a core theme, goal or agenda. Some are formed for a specific mission, and others exist as a hobbyist playground. The most famous of secs, in recent years, are: anonymous, lizard squad, lulzsec, syrian electronic army, chaos computer club, level seven, Tarh Andishan, TOA and Cicada 3301. Most have initiation rituals, similar to what you would see in a street gang or fraternity.

For a black hat or grey hat group, the reasons behind this are fairly obvious. Since the activities of a black hat group are almost always illegal, they need to be more selective about who they allow in. Often times this involves a hazing or initiation ritual in order to weed out the government spies and to quantify the initiate's talents and abilities. White hat hackers also tend to be quiet and selective about their activities and group involvement. This may seem counterintuitive, as they seemingly have nothing to hide, but there are subtleties that are still very sensitive. For example, let's say a collective of white hats are working on a popular open source program that powers banking software. If the software is discovered to have a large vulnerability, that information must be kept secret and safe until a patch can be released and distributed to the businesses. The differences between white, grey and black start to blur when looking at a collective of individuals. The mentality, knowledge, and operations of these secs tend to be very similar in many ways. Regardless of alignment they all tend to remain nameless, communicate in secret, and share their knowledge with only select individuals which they trust.

Anonymous is one of the newest and definitely the most known hacker group today. As a completely decentralized, anonymous, and open group, anon accepts any hacker or cracker that wants to be involved. Furthermore, the group proposes missions and calls to action that are opt-in only. With anon's adoption of democracy and open doors, they have positioned themselves as a group of vigilantes and most of the general public praises their activities. Anon's actions can rarely be labelled as anything but black hat, yet many people celebrate the group for executing attacks. The reasoning behind this is similar to the reasoning behind wars: one organization aims to defend or destroy another based upon validation of moral alignment. In the case of anonymous, they are generally well received because of their attacks against organizations that are deemed evil or corrupt such as ISIS, Westboro Baptist Church or even the US government.

Not many white hat secs get the same amount of press as the malicious ones, but Chaos Computer Club is a white hat sec that has managed to grab a few headlines over the years. This Germany based, hacker group has been around since 1981 and since that time has made many public demonstrations to educate and protect against security risks. Their most renowned demonstrations include robbing a bank, cloning an GSM cell phone card, and publishing the fingerprints of the German Minister of the Interior; each to educate the public on issues inherent in otherwise trusted technology.

Everyone has to start somewhere. Most hackers become so either because they are veteran programmers that start to pay more attention to security, or because they stem into from another tech-related interest such as gaming or web development. The tech world is so large and nebulous, that there is actually very little need to become a master at any one language or tool. Often times hackers today are identified as “script kiddies,” because they leverage existing tools or programming scripts to exploit software, without a deep understanding of how the exploit actually works. Script kiddies most often use existing penetration testing suites to quickly identify a vulnerability and then an exploit script that they have downloaded to actually exploit it. For example, there is a linux distro called Back Track which comes pre-installed with anonymity tools, pen testing applications, and automated programs for hacking things like wifi networks. With a minimal understanding, anyone with a basic background in tech can start to breach into websites, networks, and other systems.

Modern hardware has connected most of the planet together, with quick data transfers and standard interfaces. Software has bridged many gaps between languages and cultures. The internet has foster people to share knowledge liberally. With a wide variety of jobs, languages and tools, hacking has become not only a nuissance but also a necessity. With the evolution of technology comes a broader, yet more shallow relationship with the languages and hardware that powers them. White hats and black hats both have to leverage these new technologies and very actively maintain continued education in the tech space. Considering these facts, it is very easy to understand why hackers have become more popular in recent years and assume that their numbers will only continue to grow.

The future of hacking

As systems become more integrated via the Internet of Things and cross-compatibility of programs, hacking will probably only become more common. Integration makes for a more connected world, and like telecom to the world wide web, this makes for more vulnerabilities and easier dissemination of information. Gartner estimates that some 6.4 billion devices will be connected to the internet in 2016, making for an endless landscape for hackers.

Machine learning has become more popular over the last few years, which may make hackers behave entirely different than in the past. With the power of artificial intelligence at their disposal, we may see a world where hackers are little more than pre-built bots that are designed to test, infect and spread across the terrain of connected hardware. The incentives and motivations of such attacks will likely remain the same, with cyber attacks mostly being motivated by financial gain and smaller percentages motivated by hobby, hacktivism, or political interest. Likewise, white hat hackers are constantly improving automated software to test systems, update software and detect intrusions.

It is also fair to assume that hackers will often come from a younger and more tech aware demographic as secs like "lulzsec" has proven. With technology in the hands of millennials from an early age, programming and understand of software development is becoming more relevant in many education systems than writing or grammer. These groups will prove bothersome to larger and more archaic organizations as well, as lulzsec alone has claimed responsibility for very notable attacks against the US Senate, CIA and the Anti-Sec hacks alongside Anonymous. The most impressive thing about lulzsec is that the organization consisted of less than ten members, most of which were only teenagers or young adults. A small team of renegade black hats, Lizard Squad has also become well known for their powerful attacks against Xbox Live, Playstation Network and the Malaysia Airlines website. Lulzsec and Lizard Squad represents the most common form of a modern, and possibly future, collectives. The members are less likely to know each other on a personal level and keep their doors closed to new members. Their attacks have rarely seemed to have a purpose of financial gain, but rather for infamousy and pride. It is likely that the future of hacking will contain smaller and more privatized hacker secs like these, wherein they never dox themselves (reveal their personal identity) within an organization. Anonymitiy is becoming increasingly important to hackers, as the number of whistle-blowers and snitches in this world increase with pressure from government intelligence agencies.

The last staple in the future of hacking will likely be politically motivated cyber wars. The Syrian Electronic Army, for example, was created to retaliate against businesses that were promoting Anti-Syrian media. This group of roughly 20 members attacked news sites such as The Onion, New York Times, and many smaller media outlets. Many of their victims suffered irreversible damage and data loss to their websites. Most notably, was their hijacking of the twitter account belonging to the Associated Press. Once on the account, they published a tweet stating that the White House had been attacked and Obama was injured, which resulted in a $136 billion dollar drop in the S & P 500 financial index! We are nearing a day when wars will be waged entirely online. Evidence of this exists with groups like Tarh Andishan. After a worm, named Stuxnet, wreaked havoc on Iran's network, the government responded by creating this hacker group of an estimated 20 elite crackers. Since their formation, the group has targeted government and business entities alike to wage war under "Operation Cleaver." So far the damages have been highly destructive and successful with notable damages being done to the United States Navy and Saudi Aramco. Of course the United States National Security Organization (NSA) has their own internal hacking group as well. State sponsored groups and government intelligence organizations exist in most first world countries. The Tailored Access Operation (TAO) group has some of the greatest talent and abilities in the world, often times recruiting from the US military or even offering bailouts for highly skilled hackers that have been caught and arrested. To date, they are known to have captured incredible amounts of data, create powerful worms, and have even leveraged federal national security laws to force tech giants like Google and Apple to allow them backdoor access to consumer devices. Among other things, TAO represents George Orwell's Big Brother like no other organization on the planet, with capabilities of turning on and tapping into mobile devices to access the microphone and geolocation. They have even been rumored to have invented and injected secret decryption techniques for some of the most common encryption software and programs around the world.

Famous Hacker Secs

For years hacker secs have been relatively small and tight knit. Most have initiation rituals, similar to what you would see in a street gang or fraternity. For a black hat or grey hat group, the reasons behind this are fairly obvious. Since the activities of a black hat group are seldom legal, they need to be more selective about who they allow in. Often times this involves a hazing or initiation ritual to weed out the government spies and to quantify the initiate's talents and abilities.

White hat hackers also tend to be quiet and selective about their activities and group involvement. This may seem counterintuitive, as they seemingly have nothing to hide, but there are subtleties that are still very sensitive. For example, let's say a collective of white hats are working on a popular open source program that powers banking software. If the software is discovered to have a large vulnerability, that information must be kept secret and safe until a patch can be released and distributed to the businesses.

The differences between white, grey and black start to blur when looking at a collective of individuals. The mentality, knowledge, and operations of these secs tend to be very similar in many ways. Regardless of alignment they all tend to remain nameless, communicate in secret, and share their knowledge with only select individuals which they trust.

Each hacker sec is built up by like-minded individuals and often shares a core theme, goal or agenda. Some are formed for a specific mission, and others exist as a hobbyist playground. The most famous of secs, in recent years, are: anonymous, lizard squad, lulzsec, Syrian electronic army, chaos computer club, level seven, Tarh Andishan, TOA and Cicada 3301.

Anonymous

Anonymous is one of the newest and definitely the most known hacker group today. As a completely decentralized, anonymous, and open group, anon accepts any hacker or cracker that wants to be involved. Furthermore, the group proposes missions and calls to action that are opt-in only. With anon's adoption of democracy and open doors, they have positioned themselves as a group of vigilantes and most of the general public praises their activities. Anon's actions can rarely be labelled as anything but black hat, yet many people celebrate the group for executing attacks. The reasoning behind this is similar to the reasoning behind wars: one organization aims to defend or destroy another based upon validation of moral alignment. In the case of anonymous, they are generally well received because of their attacks against organizations that are deemed evil or corrupt such as ISIS, Westboro Baptist Church or even the US government.

Lizard Squad

A small team of renegade black hats, Lizard Squad has become well known for their attacks against Xbox Live, Playstation Network and the Malaysia Airlines website. This sec represents the most common form of collective, as the members are likely to know each other on a personal level and keep their doors closed to new members. Their attacks have rarely seemed to have a purpose of financial gain, but rather for fame and pride.

lulzsec

Similar to Lizard Squad, the lulzsec commits their attacks mostly for public recognition, or as they say, "for the lulz." This group has claimed responsibility for very notable attacks against the US Senate, CIA and the AntiSec hacks alongside Anonymous. The most impressive thing about lulzsec is that the organization consisted of less than ten members, most of which were only teenagers or young adults.

Syrian Electronic Army

The SEA was created to retaliate against businesses that were promoting Anti-Syrian media. This group of roughly 20 members attacked news sites such as The Onion, New York Times, and many smaller media outlets. Many of their victims suffered irreversible damage and data loss to their websites. Most notably, was their hijacking of the twitter account belonging to the Associated Press. Once on the account, they published a tweet stating that the

White House had been attacked and Obama was injured, which resulted in a $136 billion dollar drop in the S & P 500 financial index!

Chaos Computer Club

Not many white hat secs get the same amount of press as the malicious ones, but CCC has managed to grab a few headlines and make the world a better place with their actions. This Germany based, hacker group has been around since 1981 and since that time has made many public demonstrations to educate and protect against security risks. Their most renowned demonstrations include robbing a bank, cloning an GSM cell phone card, and publishing the fingerprints of the German Minister of the Interior; each to educate the public on issues inherent in otherwise trusted technology.

Level Seven

With a reputation for malicious attacks against banks, hotels and even NASA, L7 was a formidable group for about a year in the late 90's. Unlike more private secs such as Lizard Squad or lulzsec, Level Seven had an open door policy for allowing new hackers into the group. Ultimately, this open door policy is what likely lead to their downfall. The group was busted very quickly by the FBI in early 2000.

Tarh Andishan

We are nearing a day when wars will be waged entirely online. Evidence of this exists with groups like Tarh Andishan. After a worm, named Stuxnet, wreaked havoc on Iran's network, the government responded by creating this hacker group of approximately 20 elite crackers. Since their formation, the group has targeted government and business entities alike to wage war under "Operation Cleaver." So far the damages have been highly destructive and successful with notable damages being done to the United States Navy and Saudi Aramco.

Tailored Access Operations

Of course the United States National Security Organization (NSA) would have their own internal hacking group. State sponsored groups and government intelligence organizations exist in most first world countries. TAO has some of the greatest talent and abilities in the world, often times recruiting from the US military or even offering bailouts for highly skilled hackers that have been caught and arrested. To date, they are known to have captured incredible amounts of data, create powerful worms, and have even leveraged federal national security laws to force tech giants like Google and Apple to allow them backdoor access to consumer devices. Among other things, TAO represents George Orwell's Big Brother like no other organization on the planet, with capabilities of turning on and tapping into mobile devices to access the microphone and geolocation. They have even been rumored to have invented and injected secret decryption techniques for some of the most common encryption software and programs around the world.

Cicada 3301

Perhaps one of the most mysterious and interesting of all hacker groups is Cicada 3301. This group is only known due to the cryptic puzzles they release to the public to recruit highly talented individuals. The puzzles involve an incredibly deep understanding of cryptography, research, operating systems and programming and clues have been published in mediums across the globe from print to bootable USB drives. Many speculate that Cicada is backed by the NSA, CIA, Darpa and many other national security organizations. Regardless of the speculation, not a single person has been able to confirm the acceptance of the recruits or the organization's true purpose.

Famous Individuals

While most hackers escape with only minor traces of their organization left behind, there have been times when individuals have come forward or been captured. Most of these names never make the headlines, however, and thus tend to only be known within circles involved with security. Names like Snowden and Assange are recognized by most of the general public for their whistle-blower actions while other significant individuals like Mitnick, Iceman, Poulsen or McKinnon may go unnoticed.

Edward Snowden

Perhaps the most well known hacker in the world, Snowden used his access and connections as a contractor for the CIA and NSA to release thousands of documents to the public. While this act alone is not exactly a form of hacking, his background is very much in security and systems, which qualifies him for both the title and reputation. Snowden is a great example of a morally motivated black hat, akin to the Anonymous hacker sec, and as such he has received both praise and criticism for his exploits.

Julian Assange

Like Snowden, and often times working alongside him, Julian Assange has been a notorious hacktivist for quite some time. He is well known for his creation of WikiLeaks, a website that allows whistle-blowers and informants to anonymously share classified documents with the public. Many such documents are contributed by the black hat actions of hacktivist secs and individuals, in addition to inner operatives and employees within government institutions.

Kevin Mitnick

One of the most famous hackers in the days of phreaking was a hacker by the name of Kevin "Darkside" Mitnick. He was the most famous and publicized hacker in the 90's, notorious for his phreaking abilities. Mitnick played a cat and mouse game with the FBI for many years. He has penetrated many organizations including Novell, Sun Microsystems, and even went as far as spying on FBI phone calls. He had an addiction of sorts to hacking and for him the incentives were based entirely on the satisfaction of getting into a system or business through social engineering and software exploits. Often times his theft and impact was minimal, with childish antics of pranking individuals or calling celebrities. Still, the media loved to blame problems on Kevin and his hacks helped drive many legislative efforts towards regulating and criminalizing acts in cyber security. Kevin has a great book called Ghost in the Wires where he shares his personal experiences and journeys of phreaking.

Max Ray "Iceman" Butler

Whether Ray “Iceman” Butler started out in as white hat or black, after running a security consulting company for a few years he was discovered to be one of the world’s biggest hackers. Butler was discovered to have stolen over 2 million credit cards numbers and racking up $86 million in fraudulent charges. To handle the volume of cards which he possessed, he created “Carders Market,” where hackers could buy and sell stolen credit card information with each other. He was arrested in 2007 and given a 13 year sentence.

Kevin Poulsen

Also known as Dark Dante to some, Poulsen was a master of telecommunication hacking. Shortly after hacking a radio station to win a prize Porsche, the FBI forcing Poulsen to go underground for over a year. He was then featured on an episode of television show, “Unsolved Mysteries,” which gave viewers a 1-800 number for information. Shortly after airing, the phone lines mysteriously crashed. When he was finally apprehended, he was sentenced to five years in a federal prison. In addition to the prison sentence, he was given a three year ban on computer and internet use set to begin after his release; making him the first American hacker to serve such a ban.

Gary McKinnon

With a cocky attitude and a lot of skill, Gary McKinnon breached nearly 100 US military networks and left taunting notes on their machines mocking their security. He also wiped a few critical systems, causing over 2,000 computers of the US Army to crash for a full 24 hours or more. Supposedly on a mission to uncover UFO secrets and other securities, McKinnon was caught but never successfully extradited to the United States from the UK's asylum.

What motivates a hacker?

The news is quick to report a data breach, but often times it is unclear what the motivation for the attack was to begin with, or what is done with stolen assets following an attack. In order to increase your own security, you may be wondering what information or systems you actually need to secure. Before you can begin to adopt more secure practices and programs, you must first be able to get inside the head of a hacker. Knowing their motivation, habits, skills, and psychology may be the first ways towards creating a more secure environment.

Stolen credit cards, identities and digital assets are obvious motivations for an individual to become a criminal hacker. However, the organized attacks of larger groups or the penetration tests performed by white hat hackers can be harder to understand. Some hackers are motivated solely by personal passions such as political movements, fame, power or trying to protect the greater good which can be hard to distinguish from the intent of monetary gain.

Black Market Money

With a combined loss of almost 100 million credit cards and customer information, Target and Home Depot suffered a significant amount of damages in an attack that only copied information. The motivation for the hackers was simple: selling valid credit cards and identities on the black market is highly lucrative. Many of these records sold from $25–130 dollars each, which is much higher volume and easier to disperse than for the group that executed the attack to try and charge each card themselves. Furthermore, the anonymity of these hackers remains in tact, and they will likely walk away giving them the opportunity to attack another business in the future.

How do you protect against an attack, which even a large corporation did not defend against? The answer is simple: you should research and understand the vulnerabilities which were exploited in these types of attacks.

In the case of Home Depot, their point-of-sale systems were infected with malware and remained compromised for five months. The breach occurred from an exploit of a zero day vulnerability, which is essentially to say that the initial programmers of the POS software did not test and secure their program thoroughly enough. With more time invested into testing and auditing of the code, the vulnerability may never have been released. If the penetration point was more obscure and difficult to prevent entirely, the breach could have still been discovered quicker with more frequent auditing and white hat penetration testing.

Target's breach is even more difficult to defend. While Home Depot was blindsided a bit more (which still is not a great excuse), Target's newly purchased malware detection program actually caught the attack early on. The hackers leverage access to target's system through an HVAC contractor, but still needed to deploy their infected code across their network. Target's highly sophisticated security system, called FireEye, would have protected Target from any information lost with it's honeypot techniques. The software, which is used at many high end agencies such as the CIA, makes a virtual clone of the network and monitors activity. When an attacker breaches the network, they are actually trapped in the fake one, and lead to believe that they are making changes to real thing. This allows security teams to respond to abnormal activity before allowing any data to be exchanged with the real machines. Rather than responding to FireEye's warnings, Target's security team disabled the feature and ignored the warnings. To make matters worse, their Symantec Endpoint Protection antivirus program also managed to detect the malware and escalate alerts to the security team, who then passed along the warnings higher up the chain, only for the alerts to be ignored.

Political Agenda

Everyone has to earn a living, and some hackers make a great living by working for governments. The United States and Israeli intelligence agencies are often funded to create offensive measures by employing some of the best and brightest hackers. One of the most incredible and scary attacks executed by these governments was the creation of Stuxnet. The Stuxnet program was a virus designed to infect Microsoft Windows based Seimen controllers. This dangerous virus was deployed at uranium enrichment facilities in Iran with a function to spin the centrifuges in the nuclear power plants at uneven speeds while hiding the data from operators. Given the control and secret nature of the program, it could have been used to create much more disastrous results, especially if deployed with more malicious purposes.

Another suspected government attack comes from China. They have been unofficially blamed for many cyber attacks against the United States government in recent years, as the cyber wars begin to escalate. The US Pentagon has released reports implying that Chinese black hats have executed a few successful attacks, breaching networks and retrieved schematics for many critical systems, including the missile defense systems.

Unless you are the Chief Executive Officer for utility company or the head of security for your nation, you may not be too worried about these types of attacks. Nonetheless, it is important to recognize the implications and the fact that governments will sanction such attacks. Preventative measures against these organizations are difficult as you have to outsmart some very sharp hackers. The best measure of defense in this case, is to better understand and consider abstract possibilities like a hacker does.

Passion

Emotions can be highly motivating to some. Crackers in particular, tend to be highly egotistical and proud, leading them to respond with extremes. One example of this is the DDOS attack that was executed against Spamhaus in 2013. Spamhaus is one of the world's largest anti-spam services, protecting millions of users from malicious material and annoying content. When they blacklisted emails coming from an internet service provider, called Cyberbunker, they probably did not expect a retaliation which would not only cripple their own network but also much of Europe. The attack hit Spamhaus with traffic rates of up to 300 GB per second, making it one of the largest attacks in history.

The positive outcome of the Spamhaus attack is that many of the world's largest internet tech companies have rallied together to create tools and systems which aim to help businesses protect themselves. Google, CloudFront and others have now created and opened services which help businesses mitigate risks against their servers or websites, often for a very affordable fee. With businesses small and large now having the ability to leverage powerful services, there is little room for excuse these days, in being crippled by a DDOS attack.

Fame and Power

Many small hacker secs love to get public recognition and stroke their egos. Impressive attacks can also be proving grounds which gain them access to more powerful organized crime units. When lizard squad decided to set their sites on PlayStation Network and Xbox Live, they likely had one of these goals in mind. Usually these attacks are executed by smart, but amateur script kiddies and black hat hackers. Other times, they are an ego boost by a single hacker who wants to be recognized for his skills. Whatever the case, these attacks tend to be fairly common and the most annoying to most organizations.

Protecting against these attacks is actually fairly easy. DDOS attacks can be mitigated by leveraging cloud services, points of failure can be identified by security consultants, and application code audits can be performed by software development companies. The most secure systems and businesses are the ones who regularly consult experts and audit and update their software.

Types of Hackers

Borrowed either from Western movies or Dungeons and Dragons —where dark characters wore black hats and good characters wore white—hackers are labelled as either black hat, gray hat, or white hat. A black hat hacker is typically your evil-doer, committing crimes as a part of a larger organization with the intent to profit from their actions. A white hat hacker tends to be the security professionals that test, audit, and contribute to software that aim to protect systems and applications. Finally, a gray hat is someone who falls somewhere in the middle, often times operating alone without permission, finding and exploiting vulnerabilities, and asking for compensation to fix the weakness.

Most hackers are part of a given group, and fall into the black hat, white hat, or gray hat categories. Often times this involves a hazing or initiation ritual in order to weed out the government spies and to quantify the initiate's talents and abilities. White hat hackers also tend to be quiet and selective about their activities and group involvement. This may seem counterintuitive, since they seemingly have nothing to hide, but there are subtleties that are still very sensitive. For example, let's say a collective of white hats are working on a popular open source program that powers banking software. If the software is discovered to have a large vulnerability, that information must be kept secret and safe until a patch can be released and distributed to the businesses. The gray hat hackers have hacking characteristics that are considered both black hat and white hat hackers, but they work independently.

Black Hat

As mentioned earlier, the black hat hacker is an evil-doer. They commit crimes with the intent to profit from their actions, with a complete disregard for whether or not they harm organizations or individuals. Anonymous is one of the newest and definitely the most known black hat hacker groups today. As a completely decentralized, anonymous, and open group, anon accepts any hacker that wants to be involved. Furthermore, the group proposes missions and calls to action that are opt-in only. With Anon's adoption of democracy and open doors, they have positioned themselves as a group of vigilantes and most of the general public praises their activities. This is probably due to their attacks against organizations that are deemed evil or corrupt such as ISIS, Westboro Baptist Church or even the US government.

Like Snowden, and often times working alongside him, Julian Assange has been a notorious hacktivist for quite some time. He is well known for his creation of WikiLeaks, a website that allows whistle-blowers and informants to anonymously share classified documents with the public. Many such documents are contributed by the black hat actions of hacktivist secs and individuals, in addition to inner operatives and employees within government institutions.

White Hat

Not many white hat secs get the same amount of press as the malicious ones. Good news just never seems to have the impact that bad news has. But Chaos Computer Club is a white hat sec that has managed to grab a few headlines over the years. This Germanybased hacker group has been around since 1981, and since that time has made many public demonstrations to educate and protect against security risks. Their most renowned demonstrations include robbing a bank, cloning an GSM cell phone card, and publishing the fingerprints of the German Minister of the Interior; each to educate the public on issues inherent in otherwise trusted technology.

Gray Hat

Some hackers become so either because they are veteran programmers that start to pay more attention to security, or because they stem into from another tech-related interest such as gaming or web development. The tech world is so large and nebulous, that there is actually very little need to become a master at any one language or tool. Often times hackers today are using existing penetration testing suites and tools in order to find and exploit vulnerabilities in a system. For example, there is a Linux distro called Back Track that comes pre-installed with anonymity tools, pen testing applications, and automated programs for hacking things like WIFI networks. With a minimal understanding, a gray hat hacker individual with a basic background in tech can start to breach into websites, networks, and other systems.

CHAPTER 3

I’m not a snitch

In order to teach you principles and disciplines of security, I must first fix any false preconceived notions you may have about what a hacker is. The general public has major flaws in how they perceive hackers and security. Stop and try to picture a hacker in your head for a moment. Did you picture a scene from a movie? Hollywood likes to portray us as some lonely, nerdy guy, typing really fast, looking at six different monitors and wearing all black. In reality, hackers come in all types of varieties; some of us even dress sharply and have normal social lives. Rather than talking about hackers conceptually, I want to tell you about a few hackers that I know. For the record, I am not a snitch. These guys are all people that have given me explicit permission to publish their information, or I have left out enough details to preserve their anonymity.

Ben, the “31337” Elite Hacker

Labels are all a matter of perception. I like to call someone elite if they’ve been programming and hacking since before I was born (1987 for the record). Many of them were introduced to hacking with analog systems by phreaking (hacking phone lines) or if they were on the digital front, they were writing most of their programs in machine code. These programmers know what 31337 means, and not because some young, wannabe-hackers made the term popular again in recent years. In the early days of the net, servers were expensive, so most IRC chats were hosted on public servers, and many people had to rely on them. For this reason, hackers that used these public servers needed a way to obfuscate their conversations from regex searching. One group had the bright idea of inventing 31337-speak which would represent letters in a way the human brain could interpret, but a machine would not be able to search. For example, with "31337" notice how a "3" looks similar to a backwards capital "E" and "1" looks like a lowercase "L" and finally "7" looks close enough to a capital "T." This is where the term "elite" originates from, and is a great example of hacker culture.

Before dropping off the face of the Earth, likely swallowed up by the NSA, I knew a very elite hacker by the name of Ben. He was a white-collar kind of guy at a paper supply company. I like to think of him as Dwight Schrute from The Office. By day he built software, creating some of the first order management and fulfillment software that ever existed. At all hours of the night, however, you could find him online trying to break anything and everything. I first met Ben in a hacker group called Cult of the Dead Cow. I was just learning how to program at the time, and was all-too excited about the latest and greatest scripts that would make me feel like a rebel hacker. It was there, after I was ranked as best defense in a game Capture the Flag (CTF) that I realized I was a hacker. In CTF, a group would spend a weekend trying to capture each other's flags, which was represented by a uniquely signed file located in a standard location on the hard disk. The rules were simple:

- The game runs for 72 hours
- You are disqualified if your computer is offline for more than 5 minutes
- Your hard disk must be read-only

- Points are counted by flags stolen minus number taken

Somehow I came out in third place in a group of 30 elite hackers, with a score of zero. Ben messaged me immediately after the game ended, to find out how I had managed to save my flag from being taken. The solution, to me, was simple. I knew that I was not on the same playing field as the other members, so instead of focusing on offense, I created the most simple and easy defense I could think of: whenever my hard disk was read, I would simply shut down the computer. I literally soldered the ribbon that communicates with the hard disk to a power supply switch, so that no software effort could counteract the measure. All I had to worry about was making sure it would reboot and be back online within five minutes. Ben thought this was genius and asked me to be his Padawan. Yes, Padawan, like an apprentice Jedi in Star Wars; I guess Hollywood did nail us with the whole nerd label.

Most programmers in the early 90's were hackers or crackers in some way, because they were building low-level systems that ran large businesses. Programming languages were also more difficult to learn, so the barrier to entry was much higher. To be considered a good software creator you also needed to know how to break code. Many of these original programmers and hackers are among the most elite today. While there have been more layers added on over the last couple decades, much of the foundation is still the same: Assembly, C, Java, Cobol and Fortran are still at the core of almost all technology on the planet. This means that the elites in the hacker world understand the core of most technology more than the modern day software creators that are building on top of it. Despite being elite and having some of the most amazing knowledge and abilities of anyone that calls themselves a hacker, most of the elites remain on the ethical side but still fall under gray hat in most of the cases I have seen.

Jon, the "Script Kiddie" Hacker

Everyone has to start somewhere. Most hackers become so either because they are veteran programmers that start to pay more attention to security, or because they stem into from another tech-related interest such as gaming or web development.

As a 20-something programmer, my friend Jon is a good example of where a hacker begins his journey. His age and curiosity align with a majority of entry-level hackers. I first started working with Jon many years ago when I hired him as a front-end web developer. I ran a small dev shop at the time and Jon stood apart from the developers I had trained before him because he was especially young and hungry to learn. As we became friends, I noticed his growing inquisition towards darknet. While many developers attempt to explore darknet at least once, most fail to find it, or are so scared that they quickly leave when they do. Jon was intrigued by the hidden world and conspiracies that lay hidden off the grid of public domains. He quickly learned the basics of protecting his identity, using browser such as Tor and a linux distro called Tails; both of which take measures to separate identifiable information about the user from the servers he/she may be communicating with.

The tech world is so large and nebulous, that there is actually very little need to become a master at any one language or tool. Often times hackers in this genre are using penetration testing suites and tools in order to find and exploit vulnerabilities in a system. For example, there is a linux distro called Back Track which comes pre-installed with anonymity tools, pen testing applications, and automated programs for hacking things like wifi networks. With a minimal understanding, anyone with a basic background in tech can start to breach into websites, networks, and other systems.

Jon is a master of leveraging and learning these new tools. His methodologies and skills are shallow but broad, and earn him the script kiddie label. A script kiddie is often described as someone who can program enough to run and modify an existing hacking program, but does not have a deep understanding of what the program is actually exploiting. That is not to say that script kiddies are not true hackers or that they are less of a threat. In fact, I would say that script kiddies comprise the majority of the hacker community and can unknowingly and even unwillingly pose a great threat to the average individual or company. Equally, they are capable of becoming strong white hats as they have a better understanding of existing exploits and tools. I have seen many script kiddies become unofficial security experts and auditors, standing apart from the average developer who may not think twice about vulnerabilities.

Aside from exploring the inner world of darknet, and harmlessly tinkering on his own hardware and networks, Jon has remained very innocent and ethical when it comes to hacking. What he may not know, however, is that he already possesses the skills needed to perform very malicious attacks if he chose to do so. With strong front-end web development, and light programming, Jon could easily build a phishing site, run a bashing script on a login, or hack into a neighbor's wifi with relative ease. Thankfully, the multitude of script kiddies on the web are more like Jon and only hack to satisfy their curiosities with technology or integrate different systems together very quickly. The biggest threat to the average consumer is when script kiddies are either guided to the dark side by Sith Lords or they let their curiosity chip away at their moral fiber.

Daemon, the Sith Lord

If an elite hacker is bad, I like to call them Sith Lords. Black hat, grey hat, and white hat may be great labels in a general sense, but do not clearly communicate one's abilities or intent. Being black hat for example does not specify that the hacker steals credit cards or identities or whether they are a novice or elite.

I have only ever met a few Sith Lords. True to the name, they keep their identities hidden extremely well. One such individual may be one of the most ruthless of all. I cannot reveal his real name, as I fear what the repercussions would be, but I well refer to him as Daemon. A product of the Russian Mafia, Daemon has always been surrounded by brilliant minds with malicious intent and funding to boot. As if I have not already divulged enough personal information in this book already, I must tell you an embarrassing story so that you may understand how and why I managed to meet Daemon.

Once upon a time, I fell victim to a Craigslist scam. For the record, we are talking very early days of Craigslist before anyone knew or talked about scams. The con was simple: a girl from the states was selling her laptop to recoop some of her costs of living abroad. She wanted me to wire the money to her after she set up an escrow service through a shipping company. I get a very convincing shipping confirmation email, from a beautifully crafted, but fake, shipping company website. Down I stroll to Western Union to transfer the $600 I had promised (a good deal, but not a steal for the item I was purchasing) and day later, it hit me: this was a scam. Crap! Rather than sitting back and doing nothing, I decided to email the scammer and say congratulations for fooling me. I used traceroute to track down the writer's location, and discovered the location to be somewhere in Nigeria. Surprisingly, the scammer replied to me. I will spare you the details of the dialogue, and instead cut to the poor fool's demise. He was willing to get on AIM (AOL Instant Messenger) and chat. Within minutes, I was able to penetrate his machine and identify him. I thought this was my chance to turn the tables and get my money back. Instead, it put me on the radar of a high crime organization and I failed to recover my losses. A short time after hacking the Nigerian, I wake up one morning to find a message on my computer. Let's summarize a bit and get to the part where Daemon blackmails me into doing a job with them. We were going to perform a DDOS attack to breach into an MSN server. I was supposed to go in and start pulling whatever databases or files I could get my hands on, along with four others. Later I would find out my true purpose: to be the fall guy. This is important, because stealing and leveraging another hacker's identity is, for many hackers, valued above all else. By owning my identity and leaving me and my information at the scene of a cybercrime, I became incredibly valuable to an otherwise risky attack for Daemon.

I am going to fast forward a little bit more and just say that, yes, I got in trouble but nothing serious. We will leave it at that. I would also like to share a word of caution for anyone entering the hacker space: you look the part, act the part, and fit the part to be framed for a crime! Above all else, protect your identity as you learn!

Since that MSN attack, I have learned quite a bit more about Daemon. In a way, he became my nemesis for how he had used me. As I learned more about him, however, I realized that I was up against a much more than just an individual, but rather a very powerful group. I do not pretend to know the inner workings of the Russian Mafia, but the little I have learned taught me not to mess with them. I am under the impression that a good majority of Nigerian scams, ATM hacks, major network breaches, etc have come from this single organization. Daemon and others like him are amongst their top people. A modern day Godfather looks like a computer geek. I wonder if they still wear fedoras?

Matt, the Master Jedi

My good friend, Matt, started off with low-level programming languages. The guy could probably rewrite ebay in Assembly if you paid him enough. Since day one, he has possessed strong moral fiber, which lead his skills to be focused on white hat hacking. Matt has always focused on hacking in order to protect and educate via penetration testing and audits. Now to be fair, all of us have to tinker with black hat, at least a little, in order to understand how someone will think and attempt to penetrate a system. Still, Matt has always done so with permission of his clients or using his own machines.

Matt is not what you would expect a hacker to look or act like in real life. Unless you were to meet under the specific guise of tech, you probably would not even know he was a programmer and master of IT. Out of all the hackers I know in real life, Matt is probably the most personable, friendly and outgoing. He is very quick to make others laugh and can hold a conversation with anyone about anything. When he is not doing tech, you will find Matt spending time with his kids and family or playing video games.

Also starting out on a Commodore 64, Matt spent many years building and breaking software and networks. By becoming a Certified Ethical Hacker (CEH), but also having a solid understanding of black hat principles, Matt found himself working with some of the most reputable institutions in the world. He has many incredible, funny, and terrifying stories. My favorite story of his sounds like it came straight from a Bond movie, complete with mounted guns, armed guards, a hidden hillside entrance, elevators with no buttons, and more. Hollywood has not butchered every facet of hacker culture, as you will find in real life that the security measures with Swiss banks or government agencies are very much like the movies or greater. Unfortunately, they are not my stories to tell! What I can and will say about Matt's tales, is that they represents the shift of modern hacking. Most of the best modern hackers spend their time consulting clients or contributing to Open Source Software. Many of these hackers are very morally good, and discover some of the most notable flaws in popular software packages. On the programming front, I have also noticed a loosened grip on old languages and tools, in favor of more modern ones such as Go. Just like the early days of the elite, programming in Go requires a more intimate understanding, separating the novice and elite. I am, personally, under the impression that many Go developers are commonly also hackers.

Adam, the Acolyte

Most black hats start out as hobbyists. Few make a career from it. To them bashing passwords or breaking into hardware for freebies is rewarding enough. Most black hats, in general, are lazy and will only invest their time into things that reward quickly and easily. A great example of this type of hacker is my good friend Adam. He started hacking around 12 years old, using codes to change the prices on vending machines or stealing credit cards to pull a little money whenever he was in a pinch. He started out as a script kiddie, and slowly worked his way up the ranks to become both a strong programmer and cracker. His cracking days are long behind him, but he carries the hacker mentality to this day and turns his own thoughts of exploits towards creating more secure software.

Like most hackers, Adam had a mentor who aimed to teach him better practices and essential skills around programming, penetration testing, and social engineering. To be considered a good hacker, you still have to meet the first and oldest of criteria: be a really proficient and powerful programmer. Adam started programming very young, and his knowledge of code allowed him to invent and explore vulnerabilities in his everyday life. A thorough understanding of hardware, networking and memory management are a must to penetrate secure systems. Modern programming languages and operating systems abstract even the best of developers away from many of these foundational tools, so Adam is a rare breed compared to other programmers around him.

If I were to guess, based upon the ecosystem and climate of hackers today, I would say that only 10% of self-proclaimed hackers are at Adam's skill level or above. Regardless of my arbitrary estimates, there are still a significant number of hackers in the world, and many of them are only interested in using their knowledge and abilities for their own gain.

Clay, the Padawan

If an acolyte is a black hat hacker in training, then it only makes sense for a padawan to be a white hat in training. While my past has been a blend of wearing all three hats, I am currently focused on learning more about ethical hacking and using my expertise for a greater good. I am honestly not sure what drives most hackers to want to become white hat. Often times I only meet ethical hackers in large corporations or specialized firms that do penetration testing and security auditing. For myself, I have been more motivated by the desire to educate and inform programmers about security so that the maker movement can move forward more aggressively. Currently, the Internet of Things (IoT) is hindered by a lack of standards and security protocols. All too often I see novice hackers piecing together technology in a way that would be all too easy to crack and exploit if they were produced commercially. Most programmers today seem to have a huge lack of understanding of security or writing automated tests for their own software. I have made it my mission to try and create the tools and information resources that will help make security more enjoyable and digestible than the stale white papers that have been an industry standard.

I started hacking at an early age. My father and I were tinkerers in all things tech related, so often times we would get the hardware and software hand-me-downs or broken items from family and friends. This gave us a regular supply of things to take apart, put together and hack on to create something useful. Furthermore, he and I were always studying to one up a spy vs anti-spy relationship. Since receiving my first desktop around 12 years old, and first laptop at 15, I have constantly been obsessed with learning. My father's use of spyware to monitor my activities inspired me to try and branch out from the typical windows environment into Gentoo and Ubuntu from a very early age. By 16 years old, I was regularly in IRC chat rooms asking questions and trying to understand the underlying systems that powered an operating system. This lead to me eventually being a core contributor to the Ubuntu team in the very early days of their formation. Once I had a solid understanding of the OS, I started venturing into networking. I played MUD's (text based games over telnet) on a regular basis and expanding the programs to include new features. One day a friend asked me to break into his girlfriend's computer because he wanted to see her chat history. Being young, with very emotion-lead morals, I was eager to help him and found that I could break into not only her account, but then was also able to social engineer my way into her email which then gave me password resets to every other website she was a member of. This day stood out to me, as it was the first time I realized that I was a hacker. I of course was very soon after discovered, and had to deal with the repercussions, but my self-perspective was forever changed.

Fast forward to now, into my late 20's. I have been a hacker and programmer for over decade. I have spent many years as a gray or black hat, and now I feel a drive to use my skills for causes I believe to be morally right. This has lead me into hacktivism via the anonymous group, consulting clients on security, and building open source tools for developers.

CHAPTER 4

How does a hacker work?

Hackers use many a myriad of different tools and techniques. The resources for a hacker are so numerous, that it is entirely possible that no two hackers have the same tools or approaches for how they operate. For this reason, hacking is highly expressive and serves as identification of self for some. With a choice of over a thousand programming languages, dozens of operating systems, and hundreds of different communication protocols, hackers have so many options to explore and test for vulnerabilities. While it would be impossible to describe every tool and technique, it is easy enough to talk address the most common form of attacks and how to protect against them.

Man in the Middle (MiTM)

Hardware is always communicating, and at each layer where one system talks to another, a hacker can potentially sit and listen to the data sent back and forth. MiTM attacks most often occur over network connections, usually between a client machine and a server. Generally, the victims of these types of attacks are only a small group at a time, but with the use of malware or with lacking security protocols on either the client or server, they can be powerful on a much larger scale.

The simplest form of MiTM attacks may involve a hacker sitting at a coffee shop. The attacker can exploit vulnerabilities in a wireless router's by exploiting weak or default passwords. Their attacks can be simple, such as capturing form data like user login credentials or credit cards entered on a shopping cart. Most of the time these attacks go unnoticed, even when a browser and server have secure communication connections. The attacker can easily serve as a relay for the information and satisfy the security protocols that are implemented between the client and server and copy any and every interaction between the two.

Man in the middle attacks can also be carried out through DNS spoofing, port stealing, traffic tunneling, route mangling, and many other phrases that you may not care to memorize. The point is simply that these attacks are common and sometimes the hardest to recognize. All systems should be sending only secured data back and forth by using SSL certificates on website, obfuscating routes and creating custom encryption schemes.

Injections

Sometimes a hacker does not have to sit back and hijack data from the network. Instead they can go straight to the source and extract all the information at once. Many websites use a relational database on their back-end server, which is often built on and powered by SQL. These databases can be exploited by injecting database query logic into forms and url's to extract extra information from the database. Whenever a website is built on an off the shelf-solution, such as wordpress, it comes riddled with vulnerabilities which hackers can easily look for. Proprietary software on the other hand, can be even more insecure. If a developer is hired to build a website, and does not know about best practices or security standards, then they may unknowingly be creating an extremely vulnerable application. Not only do SQL injections pose a threat for the back-end, but hackers can also introduce scripts on the front-end using cross-site scripting (XSS) techniques in order to modify the website or steal information.

Protecting from injections should be done on the application level by hiring a strong and competent development company to either audit, patch or build the initial application. Modern frameworks, such as Ruby on Rails, comes with many security measures implemented at the core and out of the box provide a certain level of security. Schemaless databases such as MongoDB also help protect against injections, as the database itself does not have a query language.

Brute Forcing

Brute forcing is the act of attempting multiple username and password logins on a system by using a program to automate and test various combinations repeatedly. In the example of the MiTM hacker sitting at a cafe, a brute forcing attack was buried subtly in the details. Often times, a cafe may secure their router by changing the password on initial setup, but still leave either a default username. In addition, low end routers do not have any sort of brute force detection or lockout. This combination makes it incredibly easy for a hacker to get in. For example, if the hacker knows that the router username is “admin” he can create a program that will run through an algorithm or database of password combinations, often called rainbow tables, in order to find the correct password.

Protecting from brute forcing is actually pretty simple. It is important to first of all purchase commercially hardware such as a mid or high level router when offering up a public connection. For software applications, brute forcing can be protected against with fraud detection software and lockouts written into proprietary application code.

Do hackers make money?

The short answer is: yes. Whether operating as a white hat hacker that audits and pen tests systems, or capturing data to sell on the black market, most hackers can easily earn a six figure income or more. As we have already explored, sometimes the data in a raw format is worth more money on the black market than individual transactions. Extortion, scamming and social engineering also allows a hacker to more manually extract money from their victims, often with a much higher rate of return.

Selling Stolen Data

With a combined loss of almost 100 million credit cards and customer information, Target and Home Depot suffered a significant amount of damages in an attack that only copied information. The motivation for the hackers was simple: selling valid credit cards and identities on the black market is highly lucrative. Many of these records sold from $25-130 dollars each. Selling this information on the black market gave the hackers a higher volume and made it easier for them to disperse than if they would have charge each card themselves. Furthermore, the anonymity of these hackers remains intact. They will likely walk away, giving them the opportunity to attack another business in the future.

In the case of Home Depot, their point-of-sale systems were infected with malware and remained compromised for five months. The breach occurred from an exploit of a zero day vulnerability, which is essentially to say that the initial programmers of the POS software did not test and secure their program thoroughly enough. With more time invested into testing and auditing of the code, the vulnerability may never have been released. If the penetration point was more obscure and difficult to prevent entirely, the breach could have still been discovered with more frequent auditing and white hat penetration testing.

Stolen credit cards or user identity are one of the most common goods sold. Most hackers have no interest in executing further attacks on the victims, instead, they sell this data to others who may have a specific agenda or operation established. Some buyers seek out user authentication databases in order to test the same email address and password on other services. Others may be interested in using stolen data for extortion. Surprisingly, there are even a large amount of legitimate businesses that purchase data on the black market to send spam emails to in order to try and sell a product or service.

Using Data for other Attacks

Darknet is the underbelly of the publicly accessible internet. Akin to the tip of an iceberg, public domains and networks only account for a small percentage of the entire internet. Most servers, networks, and machines live unlisted and anonymous. A portion of this network is mapped out with private addresses and comprises what many call the "dark web" or "darknet." It is here that the hackers, gangsters and black market traders roam freely under a cloak of anonymity. Many people come here to share secrets, buy and sell on the black market, hire hackers or assassins, and many other dark things. Stolen credit cards or user identity are one of the most common goods sold. Most crackers have no interest in executing further attacks on the victims, instead, they sell this data to others who may have a specific agenda or operation established. Some buyers seek out user authentication databases to test the same email address and password on other services. Others may be interested in using stolen data for extortion. Surprisingly, there are even a large amount of legitimate businesses that purchase data on the black market to send spam emails to try and sell a product or service.

Just like any other petty thief, many hackers operate quietly and independently to make a less ambitious living off of smaller targets. Whether it's to breach a well known company or deface websites to boast their name, these small time hackers like to stay off the grid and make a living off the pocket books of fewer people. By focusing on a more specific type of victim, these thieves can leverage their knowledge to draw from bank accounts or extort just one or two independently wealthy people. They may also purchase credit cards on Darknet and set up a legitimate looking monthly transaction. To the victim, these transactions look like a utility bill, but they transfer the money to the hacker's bank account. There are many ways a petty thief can operate, and because their crimes are smaller, they may do so for years without any real threat of pursuit or prosecution.

Hacker for Hire

Keep in mind, the word "hacker" is not always representing the criminal. Many hackers are for hire as security exports or certified ethical hackers. There are quite a few companies, such as Tekkis, that help businesses by performing security audits, risk assessment, penetration testing, HIPAA/PCI/Meaningful Use compliance, and many other services. These hackers for hire are on your side, and the best ones know how to think like a black hat.

Of course, black hats are often for hire as well. Some of the more novice black hats advertise their services in various places around darknet. The more advanced hackers tend to take some time to track down, and can often only be found by getting in touch with their group. Malicious hackers are often hired to for personal vendettas to deface websites or by businesses or government agencies looking to infiltrate and steal secrets.

Passion Projects Pay Too

Emotions can be highly motivating. Hackers in particular tend to be highly egotistical and proud, leading them to respond with extremes. One example of this is the DDOS attack that was executed against Spamhaus in 2013. Spamhaus is one of the world's largest anti-spam services, protecting millions of users from malicious material and annoying content. When they blacklisted emails coming from an Internet Service Provider, called Cyberbunker, they probably did not expect a retaliation that would not only cripple their own network, but also much of Europe. The attack hit Spamhaus with traffic rates of up to 300 GB per second, making it one of the largest attacks in history.

Many small hacker secs love to get public recognition and stroke their egos. Impressive attacks can also be proving grounds, which gain them access to more powerful organized crime units. When lizard squad, a black hat hacking group known for distributed denial-of-service (DDoS) attacks to disrupt gaming related services, decided to set their sites on the PlayStation Network and Xbox Live, they likely had one of these goals in mind. Usually these attacks are executed by smart, but amateur script kiddies and black hat hackers. Other times, they are an ego boost by a single hacker who wants to be recognized for his skills. Whatever the case, these attacks tend to be fairly common and the most annoying to most organizations.

Aren't hackers geniuses?

Most hackers are hobbyists, tinkerers or they are employed in technology fields. Fictional tales have created the modern day image for what a hacker looks like. In such movies as The Girl With the Dragon Tattoo and Ex Machina hackers are portrayed as possessing a rare combination of genius and skill. If you replace these characters with a humble family technician working for Google, you lose the mysterious edge to the tale. The truth is hackers can be average doers and dreamers with an above average interest in technology.

Some hackers are absolutely geniuses, and many technologists are by default a very smart group, however, the skills and intelligence are often exaggerated by the media. Up and coming hackers have an immediate advantage of starting out with technology young and becoming familiar with it at an early age. Would you describe yourself as a genius because you know how to drive a car? Perhaps 100 years ago, your driving ability and comfort would seem incredible to most. This is often the analogy that relates best to modern hackers. Most are hobbyists, tinkerers or employed in technology simply because it aligns with their interests and they have readily had the opportunity to learn and grow with the tools.

Fictional tales have created the modern day image for what a hacker looks like. The Girl With the Dragon Tattoo or movies like Swordfish, portray hackers in a way that makes them seem like they posses a rare combination of skill and ethics. If you replace Lisbeth Sanders (Dragon Tattoo) with a middle aged college professor or Stanley Jobson (Swordfish) with a humble family man working for Microsoft, then you lose the mysterious edge to the tale. The truth is hackers really are, in most cases, just average doers and dreamers with an above average interest in technology.

Furthering the exaggerated image of hackers, news outlets are often romanticizing hacker stories. Dramatic news reports are released describing hacker attacks as "elaborate" or sophisticated when in reality, most attacks occur when one hacker buys another hacker's malware and finds a new target to deploy it on. Most hackers do not even really know complex tools, principles or systems well enough to be considered elite hackers. Instead they lazily poke around look for common vulnerabilities and make a very weak attempt at exploiting it.

CHAPTER 5

Is anyone safe?

With so many businesses doing things wrong, surely some are doing things right. Generally, the individuals and businesses that remain secure have a mindset that things are never secure enough. Regular attention to software and hardware maintenance, monitoring, testing and upgrades tend to make for the best security. From application code to infrastructure, prioritizing security really has a large impact for a business, even if those results are not immediately recognized or quantifiable. Security is often measured in losses, as the gains and prevented breaches are not as easily measured.

Many security consultants will tell you that your twitter account is more secure than your bank account. So many people seem to think that businesses with high profile data, such as banks, government or healthcare, must also have top of the line security. The sad reality is that even though these industries are regulated for certain security measures, most of the technologies used to protect and assess are quite dated and contain many vulnerabilities. Tech companies like Facebook or Twitter on the other hand are bleeding edge technology companies, which rely entirely on the stability and security of their technology to exist as a business. Whether bank or financial institution is hacked is not incredibly important to the businesses breached, in the grand scheme of things. Often times, insurance companies, consumers and other providers take on the brunt of the damage without seeing compensation or recovery. If an organization was under the impression that a single data breach could bankrupt their business, many would be incredibly secure like many of the tech giants are. These tech giants often do security right, as they understand the importance of automated testing, regular updates, penetration testing and other best technology practices.

Hackers want to come after you

This is not a scare tactic, it is simply true: you are a target for hackers. Often times, hackers are after anyone and everyone. Maybe your business has yet to be discovered or catch the interest of the right hacker, but that does not mean you will not be discovered at a future time. Everyone from the biggest corporations to the tiniest mom and pop shop are targets for hackers. The only thing protecting you by default is that hackers are lazy. Most hackers will not spend any serious amount of time seeking out and trying various ways of penetrating a business. Often times they will run a bot that goes out and crawls various websites and networks until a website that meets a certain set of criteria is found. By now, you should understand that hackers have a wide variety of motivators, so it's only safe to assume that a number of those may apply to you. Additionally, you should also be considering the various interests a hacker may have to penetrate you. From the simplest form of bragging rights to extracting data from your database, file system, or simply wanting control of your machines, hackers have many reasons for targeting both individuals and businesses, large and small.

You may think that your company isn't large enough to be an attractive target for a hacker, but that is a myth. This is not a scare tactic, it is simply a true statement: ***you are a target for hackers***. Hackers are opportunists. Maybe your business hasn't been discovered or hasn't caught the interest of the right hacker, but that does not mean you will not be discovered. It is a common misconception that hackers are only interested in large organizations, governments, or financial institutions. In reality, everyone from the biggest corporations to the tiniest mom and pop shops qualify as targets for hackers.

From the simplest form of bragging rights, to extracting data from your database, file system, or simply wanting control of your machines, hackers have many reasons for targeting anyone. According to Verizon's Data Breach Reports, more than 70% of data breaches targeted organizations with less than 100 employees.

The assumption that you are small enough to fly under the radar can have devastating consequences. Hackers tend to follow a simple formula when assessing a target: reward divided by effort equates to the level of interest. If you have a company that favors the hacker's gain versus effort and are under 100 employees, consider these chilling statistics for a moment:

- Your employees are your greatest threat
- The cost of being hacked averages $36,000
- There's a 100% chance that one in ten people will click a malicious link.
- On average, it costs north of $50,000 per 1,000 records lost

Emails are probably the first tier of interesting data. Even if you collect nothing more than these emails, your database is of value to someone on the black market, because they can easily launch phishing attacks against your customers pretending to be you. Protect even the seemingly unimportant data such as newsletter lists. At the very least, your company can be held accountable for leaked emails and the backlash for receiving spam from a leaked database can go viral. So, be proactive and avoid being a hacker target.

The next level up is user authentication data, such as usernames and passwords. Sad as it may be, most people use the same login credentials across multiple applications. By breaching your database of credentials, a hacker can easily create a script to try those credentials across multiple other applications such as bank websites, social networks, and email providers. When storing this type of data, it's best to use encrypted passwords (or better yet, token based authentication) and secure connections between your clients and your application.

Credit cards, Social Security numbers, and other financial data are obviously the most valuable. This data is among the most coveted by hackers and is often still collected by many applications via very insecure connections or stored in plain text in databases by many businesses. Many products and services exist, which take much of this responsibility off of your shoulders and also meet many of the compliance standards you may otherwise need to implement.

Acknowledge the fact that hackers may have an interest in you, and you will then be able to start thinking about ways to enhance your security, taking into account the specifics described here. Note that beefing up security does not always imply higher cost either. You can start to increase security with minimal effort or cost by simply staying informed, educating your employees, and keeping software up to date.

Governments and Banks are still weak

It's a common misconception that big banks, government, and healthcare companies are secure from hackers. Conventional wisdom would say that people who have the most sensitive information should be the ones that have the best security, but the issue is that good security comes from good technology practices. In other words, really secure organizations pay regular attention to software and hardware maintenance, monitoring, testing and upgrades.

Security implementations are based on a sliding scale. On one end you have top level security, which creates a huge inconvenience for an organization and its members. On the other end you have very little or no security, which results in almost no inconvenience. Security is never absolute, and any organization must decide where they fit best on the scale so that the level of security and convenience or inconvenience mesh with the risk they are willing to take.

Even though large companies are spending big bucks on protecting their data, the 2015 Verizon Breach Investigations Report shows that over 50% of breaches take beyond just a few days to discover. Fewer than 6% of these attacks are ever revealed and discovered by the companies themselves, and instead are reported on by outside security specialists, often in some quarterly evaluation. Clearly, spending money alone is not a true solution to correct the problem. In some of the most famous and significant attacks in the last few years, the breaches went unnoticed for many months:

- Goodwill: 18 months
- Michaels: 8 months
- Home Depot: 5 months
- Neiman Marcus: 5 months
- JP Morgan: 2 months

At the very least, the money that is being spent on security should be in setting up more frequent audits. In addition, if these businesses focused on a proactive security strategy, rather than reactive, they would have much better results. Many companies only suffer one major security breach and then finally prioritize standards to prevent future breaches. However, if they have valued high security standards from the beginning, many major breaches may be avoided.

The businesses that do seem to get it right, are businesses that are on the bleeding edge of technology such as Facebook, Twitter and Google. Even relatively small businesses that are heavily invested in technology understand the importance of security and prioritize it as such. Tech businesses rely, almost entirely, on the stability and security of their underlying software. If all organizations were under the impression that a single data breach could bankrupt their business, many would be incredibly secure and breaches would occur far less often.

Security products only do so much

As counterintuitive as it may seem to the average Joe, more security software often brings more vulnerabilities. Security software engineers are often focused on testing and breaking other software with tight integration points and thorough penetration tests. These engineers, however, are not often practiced or conscious towards securing their own software. Even something as basic and widely adopted as OpenSSL, which is an open source library used by millions of products, was recently discovered to have a huge security issue called Heartbleed. This vulnerability may have been known by hackers for the years since it slipped into the source code of OpenSSL on New Year's Eve of 2011, since it was not discovered and patched until April of 2014.

Even the most basic of encryption protocols can have holes like this, so it only makes sense that large antivirus programs and complex intrusion detection software may have similar or even more grand bugs in them. Less is more when it comes to security, and proprietary versus open source each comes with tradeoffs when it comes to vulnerabilities.

As if the insecurities in software weren't enough, many businesses add to the problem when they invest in software or hardware tools that are then never properly installed. By only partially integrating a system, such as antivirus software, but neglecting to set up automatic updates and patches, the tools become vulnerable to simple zero-day exploits. Same goes for hardware boxes and firewalls, which are often purchased but then never installed because the business does not want to be inconvenienced with the downtime that may be required for installation.

There are many industry problems that need to be addressed, such as transparency in vulnerabilities and exploits introduced to software. Companies that make security software and hardware don't want to receive the bad press that comes with a patch that fixes a hole with their product, but this silence makes for a lack of recognition of importance. If more businesses cared about security systems and created a demand for better software and hardware, it is likely we would see a shift of providers trying to create more integrated and hassle-free products over time.

Compliance is just the starting point

Many businesses make the mistake of thinking of security and compliance as synonymous terms. While compliance does increase security through a rigid set of requirements and audits, it is more of a reporting tool and minimum set of standards set regulated by organizations such as PCI, HIPAA, or the Sarbanes-Oxley Act. Proper security measures should aim to protect you from threats by controlling how information is shared between your technology and others. Compliance on the other hand is more of a regularly scheduled demonstration to the regulatory organizations, that you are meeting a specific set of security standards that they have defined. Compliancy tests and regulations can be cumbersome to make you feel jaded towards security as a whole, but it is absolutely crucial to invest in both.

Unlike security standards, which can often be numerous and more loosely defined on a case by case basis, compliancy focuses on a set of regulations which allow for a business to execute certain actions or practices. Compliancy certificates are often awarded for passing these regulated tests, and can then give the company legal ability to process credit cards, share medical information, or go public. These standards have helped tremendously over the years, but businesses often do not audit their systems beyond these checklists or worse yet, do not follow the rules and regulations properly. To get a better feel for what you should focus on, first try and understand the following standards and practices that are currently regulated or recommended based upon industry.

All Applications

Whether your product is web, mobile, private or public; to protect yourself legally, you should protect all personally identifiable information with encryption. Even email addresses and names should be encrypted when transmitted from a client to a server. As a most basic example, all websites should be using https, and sensitive data such as passwords should be one-way encrypted when stored in a database. While these standards may not be regularly enforced, they are an industry standard and as such are expected and are actually punishable for violations in many regions.

Health Applications

The Health Insurance Portability and Accountability Act (HIPAA) defines many rules and regulations for how medical companies must carry out and enforce many aspects from administrations, to technical and physical security measures. HIPAA enforces quite an extensive list and can be very aggressive against violators, so compliancy is incredibly important. Even though HIPAA is elaborate and strict, the compliancy alone does not protect businesses from vulnerabilities, nor does it ensure that a breach will not result in violation or penalties.

E-Commerce

All applications that accept credit cards, even in cases where the information is not stored, are subject to the Payment Card Industry Data Security Standard (PCI-DSS) regulations. Unlike HIPAA, which defines a single core set of standards, PCI compliance comes with various levels of certifications depending on certain statistics like volume of transactions. Many businesses are not even aware that they need to be PCI compliant until a breach occurs and they are surprised with a lawsuit or fine that is charged against them for violating compliance standards.

Government

Many local and federal government agencies in various countries have their own set of compliance regulations. In the US a minimum set of standards are required under the National Institute of Standards and Technology (NIST) regulation. Some of these agencies are required to comply with the Federal Information Security Management Act (FISMA) while others, such as defense agencies, have additional standards such the Defense Information Assurance Certification and Accreditation Process (DIACAP). All agencies are then held accountable and are regularly monitored, audited and assessed by the Federal Risk and Authorization Management Program (FedRAMP).

More money does not mean more secure

While investing in better security from a monetary standpoint is certainly not a bad thing, some of the most effective security is free. Educating employees on best practices, potential threats and maintenance is a great place to start. Most businesses leave security to the IT team and think that the responsibility ends there. In reality, everyone from the shareholders to CEO and custodial staff should care about security.

Consider the fact that custodial staff has physical access to your offices for example. What types of security do you need to protect against a physical attack? If a janitor forgets to lock an external door, or worse yet, has personal intent to steal from your business, where are you points of failure? Perhaps individual offices, servers and switches should have separate lock and key access. Systems could be powered down during hours the office is closed, with any type of activity triggering an alarm. Rather than physical office keys, maybe digital ones are used instead so when an employee is let go, the business can remain confident in who has access. These are just a few things that may or may not have a cost associated with, but the first step is absolutely free: thought and consideration to points of entry.

Play through another hypothetical, this time with a contracted software engineer. While laws, contracts and intent should be ample protection from the contractor themselves, consider the fact that they, for a period of time, might have full access to your tech infrastructure. What are your processes and procedures following the contract to ensure that they have wiped any intellectual property or access? Do you have a process for changing security credentials and keys on all the critical layers after they are finished with the work? Where are you storing these credentials? Once again, the questions you can ask yourself and the processes you can implement for your company on this front, can have little to no cost.

Physical and credential security are only the beginning. Education and understanding may be the most important first step towards creating a more secure system and business. While compliance may feel like having your teeth pulled out, reading through and understanding industry reports, such as the white papers by Verizon and Veracode are both informative and quite enjoyable. Passing along this information amongst your employees and partners will kick off many internal discussions about assessing and protecting the company from the ground up.

While it may seem like throwing more cash and software at the problem would make things better, the reality is, it can make them much worse. While security software can be incredibly valuable, the programs and tools themselves, can contain vulnerabilities. When building security software, most companies are focused on how to break other software rather than how to build their own. The mindsets are very different, and while each has a place and value, they should work in tandem for the most effective results. Thus, many security consultants will tell you "less is more" when it comes to protecting systems. Physical security, hardware, and proprietary tests can be incredibly effective, especially when compared to off the shelf antivirus software or intrusion technology.

Even when it comes to hardware devices and internal tools, many businesses fall short in following through with the integration of these devices or tools. Furthermore, many of these are very generic intrusion detection tools, and the like, which do not cater to the unique networks and operations of an individual business. Hiring software engineers as contractors or consultants is often a much more effective way at securing your business, as they will lead you towards building custom tools that fit your specific needs and vulnerabilities.

Nobody is impenetrable

Hackers use a myriad of different tools and techniques. The resources for a hacker are so numerous, that it is entirely possible that no two hackers have the same tools or approaches for how they operate. For this reason, it is virtually impossible to make any system completely impenetrable. Instead, the question asked should be: how do I protect myself better than my competitors?

In the early days of hosting, many companies would brag about 99% uptime. With the growing popularity of uptime monitors, it was discovered that systems go down all the time. With a large enough DDOS attack, it is pretty much impossible to guarantee that your systems can always remain online, no matter how stable they are. Instead, the focus should be on recovery time, the security of the systems when they come back up, and the order in which those systems or services become available. For example, if your website was the target of an attack and you were forced to reboot in the event of a crash (an automated process for many hosts and applications) the operating system may spin up the database services before the web server. This can potentially expose a protocol or service to outside attack if the web server intercepts request or provide sanitization to these services. The same is true for many other layers of protection, such as firewalls. It may be best to load test your application. Plan the order at which services will reboot and audit the services, ports and protocols that are initiated when securing yourself. After that, you should have a plan of defense:

- What uptime or attack monitoring product will you use?
- How will you respond to notifications of downtime?
- Who will handle the response to unusual activity?

Answering these questions will not only give you peace of mind, but you will start the process of becoming both proactive and having faster reaction times. Let's face it, you cannot prepare for every type of event, but you can recognize and respond to the common symptoms of an attack in a faster and more efficient manner

CHAPTER 6

How do I protect myself?

You are not helpless in preventing attacks. Assuming there is some elite hacker out there who you are helpless to protect yourself against is to buy into the Hollywood lie. Remember that crackers are incredibly lazy with their efforts. With no capital investment, you can protect yourself significantly just by educating yourself and anyone connected with your business. You can, and should, instead invest your capital towards hiring security consultants and outside penetration testers. You also do not need to overhaul and protect every facet of your system overnight. Rather than trying to outrun the bear, which is the hacker, focus instead on being the next fastest person, by continually enhancing your security. Here are a few simple principles and practices to get you started on your journey of being more secure:

Lower the value of your data

If you are storing credit cards for an e-commerce website, perhaps a product, such as Stripe, could be a better option for you. Rather than storing information about a user, consider using Single Sign On authentication schemes and instead relating meta data to a user identification number. Encrypt passwords that are stored in a database with one way encryption schemes; you can validate whether the user has entered the correct password by comparing the resulting hash instead. Many times, hackers will look for these types of integrations. If your product uses a dedicated and secure 3rd party for many aspects, they usually will move along without even attempting to hack in. You should also consider a public privacy and data policy telling your customers and hackers alike what type of information you do or do not store. This can strong way to promote a sense of security as well as deter malicious types from poking around.

Test everything

In application code, some developers follow a practice of Test-Driven Development (TDD). There are few frameworks or languages that promote this heavily, but testing is incredibly important. Application code with strong tests can quickly alert you if something is broken. This is one of the best ways to ensure zero day exploits and more secure proprietary code.

In addition, hiring security companies to perform penetration testing is incredibly valuable. They will generate reports and recommendations for you, and by working with different companies and performing various tests, you will continually harden your system. Some services or areas you should consider testing may include (some of these are borrowed from Tekkis.com): load testing, compliance auditing, risk assessment, penetration testing, breach assessment, HIPAA/Meaningful Use/PCI, wireless security testing, network testing, VOIP testing, backend database hacking, reverse engineering, advanced exploitation, mobile and BYOD, web application testing, active directory, social engineering, malware detection, and operating systems.

Hire or create excellent teams

The best security professionals are independent and very hard to hire. Even Chief Security Officers at large corporations are rarely qualified to implement any of the processes or tests that are needed for their company. Independent security experts and consulting firms are in high demand, as they are vital to creating some of the best security. When hiring internally, you may want to bring on a security expert by your 10th technical hire. After that, it is typical to have a ratio of a single security expert per 100 engineers, give or take depending on the industry. Senior security experts tend to be expensive as well, so do not be surprised if the salary demands or contract rates are higher than you expect. Remember that as hackers, there are many ways to make money, both legally and illegally, so the white hats need to make a living and be incentivized too.

Some caveats of hiring a hacker internally range from egos to poor management. Hackers tend to think a lot differently than most business types, and usually the more abrasive or weird they are, the more talent they possess. It is crucial to remember that hackers are best at breaking things, and not necessarily building or patching vulnerabilities. Pairing them tightly with operations or development leaders makes for a diverse and competent security team. Often times, it is best to also abstract away business decisions and budgets from hackers, and instead pair them with operations for better budget planning, tech procurement, legal and management. Finally, make sure that there is top-down support and buy in for the security team. Without priority and support, security teams not only tend to make less progress, but they can become bothersome towards the company because of their restlessness or demands.

Update, educate, and maintain

Operating systems release security updates, firmware upgrades become available for hardware, and all the time software patches and updates are released. Staying on top of these updates regularly is absolutely critical for security. We have already established how lazy hackers are, and one of the easiest and lazy ways for them to pen test various businesses is to keep an eye on security announcements and look for a bug to exploit. For example, the heartbleed vulnerability found and reported about the OpenSSL library lead to many hackers creating a script to start probing different websites and checking to see if they were currently vulnerable. They could then create a database of these websites and decide to target one of them based upon the value of the website and data contained therein. Do not let excuses of cost, ease of management, or deprecation stop you from updating your systems!

Wrapping Up

Security is not a "set it and forget it" problem. Security is not an engineering problem either, where a peak optimization is cause for slowing or stopping progress. What security really entails is a cat and mouse game of protecting your systems against very active and real adversaries that will constantly require your attention. If you are not attacking security issues at frequent and regular intervals, then you are falling behind and dropping your guard.

Nobody can help you but yourself. In the event of a breach, very few law enforcement agencies have the ability to help in any meaningful way. You are accountable to your customers, and protecting their data falls on your shoulders alone. Build great security teams, and be transparent with your user base in order to ensure that you are considerate of both internal and external perception and issues.

By working with the right people, from outside consultants to internal employees, you should be able to keep up with defending yourself from a good majority of the hacker community. Education is crucial, and nobody should be ignored when it comes to teaching about security standards and practices within your company.

I hope you have reading this book as much as I enjoyed creating it. I am an application and systems consultant and developer by trade and available for hire through my company, Unicorn. Within our network, we are connected to hundreds of the best and brightest people to help build, secure and test applications, networks and systems. Good luck on your journey, and stay secure!