Ken Patel
Literary Club Paper
February 14, 2022

Catch Me If You Can

Most of the following is true.

Kevin Mitnick faced a 460-year jail sentence and served over 4 years with 3 additional years of supervisory probation. Kevin did not kill anyone; he did not steal anything; he did not assault or otherwise harm or cause damage to anyone. He was convicted for playing a game of skill.

His father deserted his mother when Kevin was three years old. He was raised in the San Fernando Valley in southern California and moved around without garnering lasting friendships. His time was largely spent in solitude during the sixties and seventies. Riding the bus was relatively inexpensive and provided an outlet for the 12-year-old while his mother worked long hours in several low wage jobs. But while the initial bus fare was affordable, Kevin wanted to explore the entire Los Angeles region, which required money for bus transfers. If he could punch his own transfers, he could explore LA for free. Kevin had the gift of gab. He once sat near the bus driver and said, "I'm working on a school project and I need to punch interesting shapes on pieces of cardboard. The punch you use on the transfers would be great for me. Is there someplace I can buy one?" It sounded silly, but the bus driver did not envision a young kid manipulating him. So, he told Kevin where to buy the punch for $10. The very next day Kevin was in the store buying the ticket punch---but that was only step one. He still needed a book of blank transfers. Well, "Where did the buses get washed?" thought Kevin. He walked to the nearest bus depot and spotted a big dumpster in the area where the buses were cleaned. He pulled himself up and looked in---Jackpot! Kevin stuffed his pockets with partially used transfer books and he was off to explore all LA courtesy of indulging in his first bout of "dumpster diving." Did this twelve-year-old get into trouble? Nope. Did this set Mitnick off in the wrong direction? Perhaps.

In high school, Kevin met a friend who changed his life. Steve Shilita was arrogant and fancied himself an undercover cop. He would show off how he could have people call him without revealing his real phone number by using a phone company test circuit called a "loop around." The technique would loop two telephone numbers

together as if they were calling each other. Kevin learned to get the name and address assigned to any phone number by calling the phone company's Customer Name and Address (CNA) Bureau. With this knowledge and the basic tactic of "social engineering," Kevin was on his way. Social engineering requires reconnaissance to piece together information about a company, including how a particular department or business unit operates, what information the employees have, and their standard procedures. The technique works because people are very trusting of anyone who establishes credibility, typically by pretending to be an authorized employee. When he was ready to access nonpublished numbers, he would call a business office representative and say: "This is Jake Roberts, from the Non-Pub Bureau. I need to talk to a supervisor." When the supervisor came on the line, Kevin would say "Did you get our memo that we're changing our number?" She would check and come back on the line to say, "No, we didn't." Kevin would then say, "You should be using "213-687-9962" to which she would respond, "No, we dial 213-320-0055." Bingo, Kevin had the number! Kevin went on to say, "We'll be sending a memo but keep using your current number for now."

But when he called the Non-Pub Bureau, it turned out you needed your name on the list of authorized people with an internal callback number before they would release any customer information. Kevin's social engineering skills went into action by ad-libbing on the spot and saying, "My manager told me he was putting me on the list. I'll have to tell him you didn't get his memo yet." Kevin would have to provide a phone number internal to the phone company that he could receive calls on. After calling three different phone company business offices, he found a second-level person, whom he could impersonate. "This is Tom Hansen from the Non-Pub Bureau. We're updating our list of authorized employees. Do you still need to be on the list?" Of course, he said yes. "How do you spell your name and what's your phone number?"

The next call was to the Recent Change Memory Authorization Center, the phone company unit that handled adding or removing customer phone services, such as custom calling features. Kevin would pose as a manager from the business office, and it was easy for him to convince the clerk to add call forwarding to the manager's line, since

the number belonged to the telephone company. It worked like this: Kevin called a technician in the appropriate central office. Believing Kevin was a repair tech in the field, the technician clipped onto the manager's line using a lineman's handset and dialed the digits Kevin gave him, effectively call-forwarding the manager's phone to a "loop around" circuit. In those days, the loop around was Kevin's favorite tool. Phone company technicians used it for line testing, but for Kevin, it was a tool for setting up authorized callback when social engineering his targets.

Kevin dialed into the loop-around circuit and three-wayed in a number that would just ring and ring, so when Non-Pub called back to the authorized manager's line, the call would be forwarded to the loop-around and the caller would hear the ringing. Kevin let the person hear a few rings and then answered, "Pacific Telephone, Steve Kaplan." At that point, the person would give Kevin whatever Non-Pub information he was looking for. Then, he would call back the same technician and have the call-forwarding deactivated. The tougher the challenge, the greater the thrill. Kevin secured telephone numbers for celebrities, such as Roger Moore, Lucille Ball, James Garner and Bruce Springsteen. Sometimes Kevin would call a celebrity like Bruce and say, "Hey, Bruce, what's up?" No harm done, but it was exciting for young Kevin.

He used his telephone company hacking skills and expanded into the two-way radio world where there was already a cohort of nerds who befriended Kevin. He learned to modify a two-meter band radio so he could make his voice come out of the speaker in drive-thru restaurants, such as McDonald's. He and his friends would head to a McDonald's, park nearby where they could watch the action without being noticed and tune the handheld radio to the restaurant's frequency. A cop car would pull into the drive-through lane, and when it approached the speaker, Kevin would announce, "I am sorry. We don't serve cops here. You'll have to go to Jack in the Box." Once a woman pulled up and heard Kevin's voice over the speaker say, "Show me your boobies and your Big Mac is free!" She did not take it well. She parked her car, grabbed a baseball bat from her trunk and went running inside looking for the manager.

Once Kevin graduated high school with these seemingly sophomoric pranks behind him, he needed to find a way to land a job using these skills. General Telephone was actively recruiting high school graduates to their computer technical school---where one could be certified in 6 months for a programming job. Kevin had his plan. But while attending computer school, Kevin continued to hack using his deeper understanding of underlying machine language, which he had been using to hack before being formally trained.

His next target was Pacific Bell, with whom he had been playing cat and mouse games by getting into the company's telephone switches. Each time, a Pac-Bell security person would find Kevin in their system and block access. Kevin would remove the restrictions when they were not paying attention and he would be back in. It became work, but Kevin decided on a bigger challenge---hacking into the main control center for Pacific Bell. Meeting this challenge would allow Kevin to do anything an employee could do, ranging from creating new telephone numbers, tracing lines, disconnecting phone numbers, adding, and removing custom calling features and accessing phone logs at a time when this was novel and valuable. He would have the ultimate access and power of the main communication tool of the day, the telephone.

Kevin started his attack aimed at the Oakland control center in northern California. On his first call, he said that he was from the Electronic Systems Assistance Center providing support for all the control center software deployed throughout Pacific Bell. He did his research and used the name of a legitimate Pacific Bell employee in the assistance center and claimed that he needed to get into the control center because his data kit equipment was down for maintenance. Kevin asked the Oakland control center person for dial-up access. No sweat Kevin heard, and the person provided a dial-up number and a series of passwords while also staying on the line talking Kevin through each step. But oops, this system had "dial-back" security: you had to enter your phone number and wait for the computer to ring you back. "What now?" Kevin mused. Off the top of his head, Kevin said "Look, I'm off-site at a remote office and I won't be able to take a callback." He had magically hit on a reasonable sounding excuse. The Pacific Bell man said, "Sure, I can program it to by-pass the dial back when you log in with your

username." Kevin defeated the company's elaborate security once again with social engineering. He put an immense amount of time into this scheme through the 1980s, eventually gaining access to not only Pacific Bell, but the telephone companies in Utah, Nevada, New York City, Washington D.C., and the federal government telephone systems.

And then there was the National Security Agency, an itch that Kevin could not resist. NSA's telephone service was provided through a phone company in Laurel, Maryland, to which he had already gained access. Directory assistance listed the agency's public phone number. After randomly checking out several numbers with the same prefix, Kevin proceeded on the reasonable hunch that NSA was assigned the entire prefix. Using a test function for switch technicians called "Talk & Monitor," he was able to set up a circuit to listen to random calls in progress. He popped into one line and heard a man and woman talking—he could hardly believe that he was wiretapping the world's biggest wiretappers! Nervous and thrilled at the same time, Kevin had proved that he could do it. Time to get out. The likelihood of getting caught would be slim if he did it just once.

By this time, hackers were a known group largely focused on gaining wealth or knowledge for their advantage. Federal and state laws were passed by the late eighties and early nineties to prohibit such activity. Kevin, on the other hand, had an insatiable appetite for hacking into telecom companies and he continued to be best in class. He never hacked banks, credit card companies or any other company for financial gain. But the telecom companies were tiring of seeing hackers like Kevin in their systems, and they were constantly chasing and watching hacker activity. The Feds and LAPD were involved. Kevin was well-known as the master of hacking telecom companies, so his name was circulating. And he was addicted to the game spending most of his waking hours at it.

One day in the mid-nineties Kevin's cell phone rang, "Hey Kevin, it's Adam." It was his half-brother, the person in the world he was closest to who wasn't a hacker. In fact, Adam didn't even use a computer. After chatting for a bit, he told Kevin that an ex-

girlfriend of his knew a big super-hacker named Eric Heinz. She indicated that Eric knew some phone company stuff he might not know and wanted to speak with Kevin. And then Adam said, "Be careful Kevin. I don't think this girl is trustworthy." His first reaction was to blow the whole thing off and just not follow up. He had enough problems hacking with other guys he had known for years and could trust. But resisting temptation had never been one of Kevin's virtues---he called the number Adam had given. The phone was answered not by Eric but by a guy named Henry Spiegel, who was a colorful character with a reputation for being on the periphery of everything from bank robbery to porno to ownership of a hot new Hollywood nightclub, one of the written-about places where young actors and wannabes lined up outside every night. When Kevin asked to put Eric on the phone, Spiegel said, "I'll get him for you. I'll have to page him and then conference you in. He's really cautious." This sounded like over-kill or paranoia to Kevin, but he waited, even while thinking that talking to Eric was a bad idea. He had a gut feeling that someone was watching him. He thought that the Feds could be on to his hacking activities in his mind, but he had no real evidence to cause immediate concern and his appetite for hacking was overwhelming. So, he spoke with Eric anyway. Over the course of the next 6 months, Eric became a close friend and hacking confidant.

Kevin continued his life as a hacker spending an inordinate amount of time with Eric and a few others. He was not an unknown, USA Today's 1988 Money section had a huge picture of Kevin labeled "The Darth Vader of the Hacking World" and calling him the "Darkside Hacker." His time with Eric proved to be fruitful for his hacking obsession as Eric was knowledgeable about major telephone company systems. They hacked into Pacific Bell routinely. With the advent and popularity of cell phones, there was yet another complex system to hack. They also targeted government agencies, such as the Social Security Administration. No money was taken; no information was sold.

One curious aspect of Eric was that although he had told Kevin his phone number, Kevin had never visited his apartment. They always met at a coffee shop or at Kevin's place. When Kevin would call Eric, another man would always answer for which Eric always explained that it was his roommate. But the voices sounded different each

time he would call. Kevin hacked the telephone company records and discovered Eric's address and paid him a surprise visit. It was an apartment complex in one of a national string of rental properties owned by a conglomerate largely rented by companies putting employees up on temporary assignments. This sent shivers down Kevin's spine as he could not understand why Eric would live in such a place. He told Kevin that he was a native Californian and that his family was in the area. In short, there was nothing "temporary" about Eric. He hacked into the phone records for the apartment and discovered a twenty-page phone bill listing over a hundred calls. Many of them were to area code 202---Washington D.C.---and there also were lots of calls to the Los Angeles headquarters of the FBI.

Could Eric be a FBI agent? Hold on, that wasn't the only possibility Kevin mused. Eric was part of a seedy group of hackers who frequented strip clubs and boasted about salacious escapades with strippers. A guy like this certainly would not pass the vetting for a FBI agent. Perhaps he was a person the Feds were targeting, or a hacker to whom the Feds gave immunity with the hope of luring more hackers for a larger sting operation. Kevin had sensed people were watching him. Kevin needed to conduct "traffic analysis," which is a process involving pulling call detail records of a person. Whom does the person call frequently? Who calls him? Who do those people call most often?

The analysis was clear. Eric was calling FBI agents frequently, and they in turn, were also calling FBI agents. One of the agents Eric was calling, was calling a number with the area code and exchange 213-894, which was the area code and exchange for the U.S. Attorney's Office for Los Angeles. The specific number was for a David Schindler, which was clear after Kevin called the number. Schindler was an Assistant U.S. Attorney who had a history of prosecuting hackers. So, the government already had a prosecutor assigned. Kevin crumbled; it would soon be over.

Kevin ran and fell into a comfortable routine as a new citizen of Denver. During the day, he would go to work at a law firm as a computer support tech, and head home every evening doing you know what. Hacking was still his entertainment and obsession—like playing a video game. But to play his game of choice, he had to always

stay alert. One lapse in attention or a sloppy mistake, and the Feds could show up at his door. Not the black wizards of Dungeons and Dragons, but the real, honest-to-God, lock-you-up-and-throw-away-the-key G-men. And, by this time, all hacking violations were federal crimes carrying harsher and longer sentences versus any state misdemeanors. And the Feds were anxious to show public examples of prosecutions. Hacking was a risky hobby.

Nonetheless, his friendship with fellow hacking expert, Eric Heinz, continued, even with Kevin's knowing the Feds were circling. Cell phone companies provided an insatiable lure and challenge. Knowing the cell numbers, text exchanges, locations, and associated habits of virtually anyone provided the hacking challenge of the century. They were successful. Nokia and Motorola were favorites and ubiquitous at the time. With Feds nearby, why not hack into the FBI's cell network and watch them watch him? So that's just what Kevin did, but without letting Eric know. The key to the FBI systems were entering via a FBI systems administrator---Kevin used social engineering to get their names. Cold calling and pretending to be another FBI system administrator with a problem provided the entryway. Many FBI system administrators used their social security numbers as their passwords, and a standard FBI email address with their names embedded. It was easy to obtain social security numbers once Kevin had their name because he had hacked into the Social Security Administration several years earlier. And now Kevin had his way into the FBI. Nowadays, two-step authentication prevents such easy hacking---the kind of entry that requires a code sent to your cell phone before the website allows you in. In the nineties, this did not exist.

Kevin discovered that the Feds indeed were monitoring him. He hacked more and he hacked a hacker, namely, his friend, Eric. And, yes, Eric indeed was a FBI agent. Kevin immediately moved to Seattle to hide once again. Several weeks passed. Once settled in a temporary apartment under an alias, he continued hacking the FBI only to discover a draft FBI press release being circulated internally:

"Washington D.C., 1995, January 26: Authorities are on the trail of a computer hacker named Kevin David Mitnick, age 31, originally from Los Angeles, California.

Mitnick is a ham radio enthusiast and is believed to use a scanner to keep track of police in the area where he is hiding. He is a known hacker and an expert at gaining control of computers to monitor or use communications systems and knows how to manufacture false identities using computers."

This hit Kevin like a ton of bricks. He was about to be the subject of a global manhunt. He suspected that the FBI was tracking his cell phone location. They were.

Around midnight, he heard a loud knock on the door, "Who is it?" Another knock. Kevin called out, "Who are you looking for?" "Kevin Mitnick. Are you Kevin Mitnick?" "No, go check the mailboxes." It became quiet. Kevin had put his name on an empty apartment's mailbox as a decoy. At this point, his mind was racing. He looked for an escape route. He went on the balcony of his apartment and looked around---nobody was around. Bed sheets? Could he tie them together and drop down from his third-floor apartment? Probably not given the Feds were close and would soon figure out his mailbox decoy. Regardless, what if the Feds tried to shoot him while trying to escape? He was a computer hacker without a gun. He called his mom and told her that he loved her and to pass the same along to his grandmother. Although Kevin was using an alias and had taken great care to put everything in his new name, there was always chance that he missed something.

More knocking. Kevin yelled, "Go away and come back tomorrow when I'm awake!" Eventually, he cracked the door to find a well-suited, middle-aged FBI agent sticking his foot in the door to block him from slamming the door. "Are you Kevin Mitnick?" Kevin responded that he was not. Then, another agent started in on him to which Kevin asked for a search warrant. They had one, but it did not have his address shown. Kevin put his best lawyer face on and exclaimed, "It's not valid, no address!" The agents started searching his apartment anyway. More shouts to stop and get out of his apartment to no avail. One of the agents shoved Kevin against the wall and put Kevin's "Most Wanted" photo in his face and said, "Doesn't this look like you?" He smiled to himself as he had never seen a wanted poster of himself, but it was an old one---a heavier, grubby-looking photo before he started working out and had better grooming

habits. Kevin asserted that the photo was not him and that they were mistaken. The Feds continued searching for two more hours. Another agent arrived with another search warrant, this time with the correct address.

One of the agents paraded through his closet, item by item, inspecting every clothing article and every pocket. After a while, he found a wallet and held it up. "Well, well, whadda we have here?!" he said in a distinctly Southern drawl. He started pulling out driver's licenses in several earlier names Kevin used to disappear. But Kevin thought that there was still nothing in the wallet that would pin him to Kevin Mitnick. The Feds caucused and contemplated taking him downtown to fingerprint him to which Kevin asked, "That's a good idea. What time do you want me at your office in the morning?" They ignored him and kept searching. So far, his luck was holding out.

And then it happened—the agent inspecting his clothes found an old ski jacket and pulled out a piece of paper from a zippered inner pocket. "A pay stub," he announced. "Made out to Kevin Mitnick." The agent glared and said, "Mitnick, the jig is up! You are under arrest!" As they cuffed him, he realized that he was not leaving for just a short period of time.

The next morning, still in sweats after going to the gym 12 hours before, Kevin had his first court appearance. The hearing lasted a few minutes with the Magistrate ordering him to be held without bail. As Kevin exited the courthouse in chains, he heard shouts of "Hey Kevin!" and noticed hundreds of paparazzi clicking away at him. What he had not seen was an article published by the New York Times on the front-page with FBI quotes asserting that Mitnick was the most wanted computer hacker in the world, had access to trade secrets worth billions, and was a huge threat to society. The article had been picked up by Dateline, Good Morning America, and other major shows all with the theme of "America's Most Wanted Hacker Has Been Arrested," cementing the public's image of Kevin as "Osama bin Mitnick."

He faced twenty-three counts of access device fraud. His worst case was 460 years. And for what? These "evil" crimes? Even the New York Times article confirmed that he never sought financial gain, nor had he sold valuable trade secret information. In

fact, Kevin had a court-appointed attorney---had he stole credit card numbers or sold secret information, he could have afforded his own attorney.

The plea deals over the course of the next 18 months were outrageous---all non-binding meaning the judge could impose a stiffer sentence. All involved more than eight years of prison plus several million dollars in restitution payments. But Kevin was essentially an indigent prisoner with a court-appointed attorney. So, he remained incarcerated without bail. While in prison, Kevin befriended a Russian man named Yuri, who had heard about him and was a fellow hacker enthusiast. Yuri had 6 months left on his sentence and was anxious to get out. He was a Russian immigrant and longed for the days of freedom. His animosity for his former home, Russia, was always front and center along with hacking schemes to bring down the country. He also had animosity for what he liked to call the "Cowboy Americans" who reveled in gas-guzzling pick-up trucks and copious amounts of steak. He posited that bringing down America was as easy as stopping the flow of gas and beef to the populace.

Unlike Kevin, Yuri had hacked for financial fortune, credit cards, social security numbers and bank account information. Yuri and Kevin spent hours discussing the intricacies of hacking. Yuri had a group of Russian friends in the U.S. and back in Russia, who were working on a scheme in which they could plant lock-up codes in any computer system with a unique decryption code only they would possess. Yuri told Kevin the application was endless and that it had never been done before. Yuri was criminally minded and dangerous. Kevin was not. He posited that one could put the lock-up code in the system by simply having an authorized user click on a phishing link, and boom, the code was planted. Only the decryption key code could unlock it. Yuri told Kevin that he could ask for money in exchange for the key code---a ransom. And once he targeted companies, he could bring them down and stop their operations costing them millions or billions. Why stop there? Yuri could sell the names of target companies to stock traders for a fee, so they could short the stock knowing about their impending ransomware attack. And he could get into company systems in ways that would jeopardize the safety of employees, customers, and the public. It would ensure a large

and easy pay-off. Kevin had the sense that he had been touched by evil. Yuri would be out in 6 months.

The publicity of Kevin's incarceration was global. He had been held in a pretrial facility for hacking with no proof of "financial losses" to companies as required by law. Fellow hackers and supporters launched a "Free Kevin" campaign filled with public protests, shirts, and pins galore. After over 4 years, a "binding" plea deal was finally offered. Kevin accepted it and was ultimately released in January of 2000.

A reversal of fortune. Two months after release, Kevin received a letter from then Senator Fred Thompson asking if he would testify to a Senate subcommittee on "Cyberattack: Is the Government Safe?" This was flattering and Kevin seized the opportunity. In the aftermath, it was as if a magic door had opened. He became a media celebrity speaking on television and news shows and was asked to host any and every show related to the internet. He wrote articles for the Harvard Business Review and countless computer-related magazines. Kevin appeared on 60 Minutes and Good Morning America. And all this as a convicted felon.

Today, has Kevin kicked the hacking habit? No, he is still staying up into the wee hours of the morning hacking, but in a different way---for Mitnick Security Consulting. Kevin does "ethical hacking" using his skills to test companies' security defenses by identifying weaknesses in their controls. And what about Yuri and his distaste for "Cowboy Americans?" After the rise of ransomware attacks and last year's $11 Million payment by the meat company, JBS, and Colonial Pipeline's $4 Million payment to keep its gas flowing, Kevin is haunted by his conversations with Yuri while in prison and is hot on his trail.

Kevin Mitnick had transformed himself from the World's Most Wanted Hacker to the Most Wanted Security Expert---just like magic.

Epilogue

As a lawyer for the soap and diaper enterprise on Fifth street, I cover cybersecurity law among other areas. Today, cyber-defense actions are a must and include running tabletops or war games involving ransomware stopping sales and manufacturing. Imagine sales orders stopping for 2 weeks while computer inventory systems are locked by ransomware---that's $3 billion in sales for a $80 billion company like P&G. Every aspect of modern-day manufacturing involves software ripe for attack. Imagine every safety feature and its back-up locking up during a ransomware attack while operations continue with dire safety risks. Ransomware defense tactics are elusive and ever-changing. Companies employ "red teams" simulating attacks on their systems and "blue teams" creating architecture to defend against such attacks. And some like P&G even employ "purple teams" combining red and blue teams to harden systems to attack. Despite these efforts, ransomware attacks happen and often. While we don't employ Kevin Mitnick, we rely on people like him to help fight cybercriminals.

Source: *Ghost in the Wires*, Kevin Mitnick, 2011.