Chapter 6
Three Decades of Digital Security

Jeani Park

I've spent 30 long years as an exterminator- battling computer bugs, worms, and digital infestations of all types. Sure it's had its moments, but I've primarily played a comic game of whack-a-mole, fevered prayers, and after-action hedging.

Does this mean I preach doom and gloom, certain of cyber war sans relief, all end-of-day dystopian angst? Nah. I'm an optimist, always have been. And when it comes to the world of security, I have reason to be. There are three main reasons why:

- The remarkable advances in computing- particularly vis-a-vis data processing and manipulation of big data, "from everywhere" that "lives everywhere."
- The trend, by organizations of all sizes, to integrate and balance efficiency, automation, and protection.
- The flame of human ingenuity and innovation, with continues to foster unprecedented levels of healthy competition and choice.

Before I discuss how these three factors can and should drive the future of digital security, let's take a little walk down memory lane. I will discuss the advent of popular security products and services, starting just before the turn of the century. Each one came about in direct response to the day's "hottest" security breaches and concerns.

Computer Viruses

Way back in 1990, the first consumer antivirus product was released. But viruses were still fairly rare. It wasn't until 1995, when Windows 95 was released, that the number of Windows desktops consumer and business users exploded. Only a few

J. Park (✉)

D.A. Christofferson (ed.), *Women in Security*, Women in Engineering and Science, https://doi.org/10.1007/978-3-319-57795-1_6

years later, as a part of the Windows 1998 release, Internet Explorer was integrated into the operating system. This, in concert with the release of Outlook 1998, which introduced HTML mail, laid fertile ground for new types of fast spreading computer malware.

Indeed, who could forget the ILOVEYOU worm and the Anna Kournakova virus? The ILOVEYOU worm hit tens of millions of Windows computers in 2000. It spread via email containing a VBScript in an email attachment. Upon opening the attachment, which the user thought was a love letter, the user unknowingly unleashed a hidden VBScript that damaged files on his computer. Additionally, the ILOVEYOU worm sent a copy of itself to all contacts in the user's Windows Address Book.

Computer viruses had gone mainstream, gaining notoriety in popular press. Just a year later, the Anna Kournakova worm hit. This time the enticing email subject promised a photo of Anna Kournakova. Instead, once again, upon opening the email attachment, a VBScript executed that sent a worm to everyone in the victim's address book. But, unlike the ILOVEYOU virus, the Anna Kournakova virus didn't damage computers or their content.

Security Updates

In response to the burgeoning number of computer viruses, which now infected millions of systems, security companies, in conjunction with the operating system vendors, began to release more sophisticated and more frequent anti-virus updates and patches. "Update, patch, update, patch" became the new battle cry.

Companies hired waves of internal IT security staff. Computer users attended 'lunch and learns' about safe email practices. VPN (Virtual Private Network) connections became de rigueur for home-based corporate laptop use. And employees were forced to sit through long computer update sessions each time they joined their corporate networks.

'*Windows Update Services- 589 security updates in this critical patch. Might as well go out for a run, and maybe dinner. Save your work'*. And this was only the beginning.

Spam

Then came the spam. And more spam. And spam flooding email inboxes around the globe in 2001/2002/2003. Spam is unsolicited messages- in this case email that hogs bandwidth, drains productivity, and is just plain annoying. Do I look like I want to buy Rogaine; I have a veritable mane of hair for goodness sakes. Oh- and spam sometimes contains malware. In fact, as spam gangs began racking up profits, they employed malware to take over third party computers, turning them into spam bot slaves. This provided free computing power and added a layer of obfuscation around spam kingpins' identities.

Enter anti-spam services and products, a new challenge and source of revenue for antispam start-ups and the who's who of antivirus vendors. While the spam problem was exploding, I was gainfully employed at a large security company working on their business gateway email security offering. A competitor released a new digital anti-spam service that was one of the first purpose specific, business-focused security services. My company's counterpunch was the first on-premise, gateway anti-spam functionality, integrated into their gateway anti-virus and content scanning suite. The race was on.

Patching and Configuration

In addition to deploying the latest security products, IT staff quickly learned the importance of keeping all of their systems patched and properly configured.

Case in point, I was visiting a Fortune 100 East Coast manufacturer the day that SQL Slammer hit. The SQL Slammer worm attacked an unpatched buffer overflow vulnerably in the Microsoft SQL Server database product. Our client was running a small number of unpatched SQL Server instances in a regional parts and inventory warehouse. The worm crashed the servers, taking warehouse and shipping functions offline for several days. The worm generated so much network traffic that several routers crashed as well.

So, in addition to reimaging the servers and patching them properly, the IT staff also had to tend to corrupted routers and routing tables. At this location alone, the attack cost millions of dollars.

Updates to Network Devices

Speaking of networking, in the typical IT department the network computing staff has traditionally been separate from the information systems staff. This means that network hardware passwords and patches may not be updated per corporate information systems policies or schedules. And integration testing may or may not occur.

The result: many an organization has been compromised by malware entering through a forgotten fax machine, printer, or an unauthorized end user hot spot. Such breaches are particularly relevant in universities, private companies, and unregulated industries, where end users both demand and have more digital freedom.

Glut of Security Attacks

The sheer glut of security attack targets is now a factor too, particularly for consumers. For example, my mother has an iMac and eagerly logs on daily for her book club chain email and political joke fix. In an attempt to keep these top secret communications private, she uses a consumer antivirus product and regularly updates her system with patches. Finally, she joined Lifelock and even password protected her computer. Sounds impressive, eh?

Well, she forgot about her router and her wireless network. By default her wireless network was enabled and not password protected (even though she exclusively uses a wired Ethernet connection). To boot, she'd never changed her router password from the vendor's default password. Heavens to mergetroid. The neighbors must have her book club's reading list by now! Seriously, remember that *everything* connected to the network needs to be password protected and patched.

The Bad Guys Always Adapt

Increasingly, the protectors hardened email, the perimeter, and the network. So, much like biologic viruses, digital viruses needed novel tricks to thwart these new defenses. Rising to the challenge, the bad guys adapted. Enter the era of keyloggers, Remote Access Trojans, and back doors. These new threats changed the game and upped the ante. Remote Access Trojans slipped pass firewalls by opening ports and communicating out of the network, in what was considered "the reverse direction".

Clever kernel level and memory viruses evaded signature-based protections. And no longer were the virus writers motivations so benign, chasing curiosity, mischief, or bragging rights. Nope. The new wave of hackers included criminals- organized and well funded. Ransom-ware was born. Hackers sabotaged or 'coopted' digital assets until blackmail demands were met. Criminal organizations turned to cybercrime. And ironically, what made the Internet such a powerful, positive tool: the breakdown of geographic and socioeconomic barriers, democratization of knowledge and opportunity, and amplification of ideas and data sharing, made it all the more dangerous.

New devices and attack targets provided novel opportunities for increasingly sophisticated hackers. Wireless networks were everywhere. A hacker could now duck into Starbucks for a juicy midday hack along with his latte. Different operating systems, browsers, and databases were on the rise. MacOS, previously a smidge of endpoint OS (Operating Systems) market share, became popular.

Dizzying Array of Technology and System Updates

New web applications were written for Internet Explorer, Firefox, Chrome and Safari browsers. Portable USB (Universal Serial Bus) storage sticks and hard drives proliferated. New identity directories and authorization schemes were deployed. Users had more choices- resulting in new functionality and reduced costs. But, at a heavy burden to IT and security professionals. This would be analogous to someone breaking into the Post Office and mixing up all of the residents names and addresses. Luckily, though an critical vulnerability existed, Dan Kaminsky found it and brought the key vendors together to patch it before it was exploited in the wild.

IT staff and developers alike now had to account for a dizzying array of security update systems, patches, and configurations. IT staff implemented new processes to package and schedule updates, which required testing in a lab environment before being pushed to production.

While working for a small software firm, I received a frantic call from a security professional at a Fortune 50 company. He was in a full blown panic because one of my software patches was in conflict with another vendor's patch. Our customer urgently needed to push out the combined update package, which contained several new features and functions. So, my small resource constrained company had to coordinate and trouble shoot with another vendor to make our patch simpatico with theirs. And note, a change to our patch meant that we had to go back and run through the testing cycle again across our entire matrix of platforms and devices.

Suddenly, security patching and maintenance was much more serious, complex and costly. Ironically, the very systems that became mission critical to security, in this case update and patching systems, in turn became juicy targets for attackers. A *Who's protecting the protectors* type of thing.

A recent example- the security defenders who reverse engineered the Stuxnet malware at first thought that the virus writers had compromised the Microsoft Windows Update Service. This would have been an epic hack with massive fallout. Luckily, this was not the case. Instead, the Stuxnet creators had spoofed the system.

Another similar close call, and this one was real, occurred in 2008 when Dan Kaminsky found a fundamental flaw in the DNS protocol. The Domain Name Services system is the addressing and routing system for the Internet. Upon exploit, bad actors could poison DNS caches allowing then to redirect network clients to their choice of DNS servers.

Common Attack Vectors

Back to the most common attack vectors. Though email remains both a common malware ingress point and spreading mechanism, the first five years of the new century saw the rise of a new entrant to this infamy: the web. In addition to browser attacks on the user side, those traveling the virtual highway encountered a variety of new threats. When one surfs the web, there is software and data on both sides of the interaction. And most of the time, the website server resides remotely, outside of the firewall and outside of local security staff control.

This opens Internet users up to the possibility of spoofed web requests, web traffic redirection, interception of the traffic, and milieus websites and web data itself.

Fake Sites

In addition web-oriented malware, websites are rich fodder for fake content. Fraudsters have been known to set up ersatz banking web sites that look nearly identical to the real bank web sites. The fraudsters then trick users to “log in” to their false sites and thus share their login credentials with the bad guys. Some fraudsters have even created websites for fake medical offices as a part of Medicaid and Medicare reimbursement scams.

The relative ease of creating fake content and spoofing website identity has driven a spate of trust services and companies that validate the identity of website owners, the safety of websites, and the risk of associated content and downloadable assets. Also, secure transmission protocols such as https have standard for secure browsing. And finally, biometrics and double factor authentication are more common than not for hardening identity checks.

Last but not least, certificate authorities sit at the apex of the digital trust chain.

Digital Certificate Authorities

Certificate authorities make it their job to validate and assure the identity of certificate owners. Digital certificates are issued for things like web browsers, web sites, and software programs. The certificate authority system is hierarchical, with a few well known root authorities anchor the system. A breach of the certificate authorities would be even more cataclysmic than a breach of the major update and patch systems. It would fracture the underlying trust of the Internet.

There have been a few breaches of smaller, peripheral certificate authorities, but fortunately the system has remained for the most part uncompromised.

As discussed, during the first decade of the twenty-first century, business servers, network attached devices and websites were typical attack targets, along with consumer laptops.

Mobile Computing

But as 2010 approached, the next digital trend caught fire- the move to truly portable computing. Large brick-like laptops fell by the wayside and notebooks, tablets, and full-featured smart phones exploded in number. What did this mean? There were a whole slew of new attack targets and attack surfaces. But, given the commensurate differences in hardware, operating systems, and applications, there was a notable lag in the associated inception of malware. Moreover, the iOS operating system had become wildly popular, and as a proprietary, closed system it was significantly more secure.

Hackers Parry, Reinvent and Adapt

Did the flood of new devices, protocols, applications, and operating systems discourage the bad actors? Not a chance. A decade into the new century, the hackers continued to do what they do best- parry, re-invent, and adapt. Case in point, the iOS XcodeGhost exploit and iCloud's celebrity photo theft. iOS, once considered immune, was no longer. And hackers became even more inventive, infamously attacking Target via their Point of Sale and HVAC (Heating, Ventilation and Air Conditioning) systems and devices. And then came the programmable logic controller (PLC) attacks. PLCs control and automate the electromechanical operation of industrial machinery.

Stuxnet was the first widely known PLC breach. Stuxnet was a sophisticated worm that infected software running centrifuges purifying plutonium for nuclear weapons. This attack is considered the first widely known act of a national-state engaging in cyberwar.

We Can Do Better

Wow. Malware writers and those intent on digital mischief seem to have the run of the landscape. Well, not necessarily.

I stated at the beginning of this article that I wasn't all doom and gloom when it came to security in the twenty-first century. How can this be given what I've told you. Given the huge increase in targets, the wide variety of targets and attack surfaces, and the sophistication and connectedness of malware writers and the hacker community at large. Computer antivirus software wasn't enough. Protecting the perimeter wasn't enough. Protecting the network hasn't saved the day. And more people, machines, and data are spoofed, sabotaged and stolen than ever. What can we do?

Rest assured, we can do better. First of all, we need to have realistic expectations. Anything connected to any network is at some risk. Absolute security is unattainable. Given that baseline understanding, consumers and corporate security defenders must critically assess digital assets, data, and behaviors, creating a value to risk matrix. Obviously, assets and information with the highest value and highest risk warrant the most focus and the most security spend.

Next, three key factors I mentioned earlier come into play: advanced computation and analysis of disparate pools of data; elevated awareness as security becomes increasingly strategic; and the continued acceleration of innovation.

First of all, let's examine the astounding advances in data analysis and computation. Let's examine these three factors in order.

Data Analysis and Computation

Why is this so important? Simple- the volume and variety of security information. Remember, security products, services, and platforms receive endpoint data, network data, website data, mobile data, application data, wireless data, and hardware data. And, it's coming from everywhere, all the time. Early products called security information managers attempted to collect and normalize a wide array of security information and send back actionable changes and directives. But they were hampered by processing requirements, the elementary nature of algorithms, and the difficulty in normalizing disparate data.

The march of innovation, on all fronts, is addressing early problems. We continue to enjoy mind-boggling leaps in computer processing. Hardware and software advances, along with next-generation ASICs (Application-Specific Integrated Circuits) and even bleeding-edge disruptors such as quantum computers, have enabled organizations around the world to analyze their internal, external, and supply chain data through different lenses, more completely and deeply than ever before. With the staggering volume of continuous security-oriented flows, experts have made strides in data modeling, abstraction, and transformation.

All of these improvements allow different data: such as geospacial, audio, industrial control, and even complex video data to be consumed and processed right along with text, image, and meta data. Imagine the possibilities. New high-speed cameras are able to capture biochemical and physical reactions at the atomic level. Improvements in artificial vision can resolve images better than the human eye. The latest satellites can detect dynamic events in space and on earth with exponential precision. Hence, new algorithms will assess such video feeds against audio recordings and other event captures and knowledge, improving deductive and predictive accuracy at unprecedented levels.

As service providers, governments, corporations and consumer collect and track cleaner and more insightful security data, actions, and closed loop feedback, the information stores increase in value. New ways of sharing such information, while protecting confidentiality, foster novel collective insights and knowledge. Through advances in deep learning and artificial intelligence, these insights and knowledge will only improve.

Deep Learning and Artificial Intelligence

Deep learning and artificial intelligence are prime beneficiaries of increased computing power because deep learning requires huge quantities of data and the ability to run thousands of simultaneous calculations and simulations to ferret out results that often run counter to intuition and common sense. Security professionals will increasingly rely on deep learning and artificial intelligence given the flood of security data, incidents, and complex workflows that have become the status quo. For instance, through deep learning, a security professional might discover that contractors hired via a specific vendor, who created patches for mobile networking codebases for the company's Hong Kong geography, left back doors in the code that were exploited to steal intellectual property. Discovering this causal link could be nearly impossible via manual human inspection, particularly given the number of systems, databases, and touch points the causal chain crossed.

Deep learning and artificial intelligence insights will allow security teams to 'find the needles in the haystack', to be sure. But they will also empower security teams to apply contextually relevant automation and remediation, real-time, while highlighting well-described critical issues. In addition, security professionals will be able to deploy just-in-time alerts, warnings and prompts that can tease out malicious acts from the unintended and accidental. For example, a warning might tell users that they are attempting to access top secret materials during off hours from a VPN ingress point- and request acknowledgment of this fact. Thus, users who didn't mean to take such actions can stop before they either break rules or take undue risks. Finally, deep learning and artificial intelligence will enable analysis of security sensor data, events and incidents against real-time financial information, production data, updates in laws and regulations, market and competitor news, and even brand equity measures-permitting more informed cross disciplinary executive decision making. It will be easier for business leaders to weigh metrics-driven risk against innovation and increased revenue, both cross-functionally and by product, market, geography, or buyer profile. Over time, automation, remediation, and "just in time" user behavior modification will be built into products from the ground up. This will harken the age of "security as a service", innately. Security will be cheaper, stronger, and integral. Thus, deep learning and artificial intelligence, appropriately applied, should be embraced.

Summary

In summary, the wild west of security has curled many security and business leaders toes for the past thirty years or so. We braved the advent of security attacks by user profile and characteristic, access point and method, device and asset type, operating system, language and currency format, social engineering, identity and verification method, etc. And then the attacks became multi-pronged and multi-layered. And the number of devices with programmable logic chips and Internet access exploded. Finally, the number of digital users blossomed, growing ever savvy and connected.

Eek. But, as I claimed, three key forces will help turn the tide, elucidating the digital security landscape and helping tame it. First, security awareness and quality education will become more pervasive. Social engineering and cooperative online efforts are already speeding this along. Concomitantly, vast improvements in computing power, memory, connectedness, flexible architectures, and smart sensors will foster deep learning and artificial intelligence solutions that will help tip the security balance towards the defenders. We will realize fewer costly breaches along with smarter overall business decision making. Viva Les Information Technology and Security Superheroes!