Enterprise Architecture

Research Product: ‘Security’ (August 2015)

There is probably a moment that doesn’t pass these days where a news story, a fiend or co-worker, or personal experience that hasn’t involved some aspect of information and computer security. You credit card or ATM card number was stolen, your computer gets infected with malware, you get spam emails from Nigerian Princes, your work network inexplicably goes out during the important part of the day, advertisements for “questionable” products and services at search engines, and multitudes of other cases of your “Spidey-sense” tingling that something may not be right in your digital world.[1]

In early August, computer and information security professional gathered for nearly two weeks in Las Vegas to participate in several conferences, traditionally known to be prime locations to announce major findings and research, hacks and exploits, and other clever work that researchers have been toiling away for weeks, months, or years in order to better understand the services and products we use every day.

Automobile Security

Within the weeks leading up to the Blackhat[2]/DefCon[3]/BSides[4] week, two major announcements from researchers regarding the security of automobile control systems was released. The first, announced by Charlie Miller and Chris Valasek, related to integrated control systems within Fiat-Chrysler brand automobiles, and was documented in an article in WIRED Magazine where the researchers proved their absolute control of a Jeep [5]with the article author in it on a highway. The second, released by Samy Kamkar a few days later centered on the OnStar system and the vulnerabilities in the mobile applications provided by Chrysler to consumers. This allowed an attacker to remotely unlock and control several other system components by intercepting, processing and spoofing a legitimate signal from an auto owner and replaying them via the captured data on an attacker’s device. Other carmakers have had vulnerabilities associated with flaws in keyless entry and immobilization systems exposed in months previous and have taken step to halt researchers’ disclosures of these flaws to the public[6]. That in itself is an

[1] http://lifehacker.com/another-day-another-hack-what-security-news-should-yo-1723127575

[2] https://www.blackhat.com/us-15/

[3] https://www.defcon.org

[4] https://www.bsideslv.org

[5] http://www.computerworld.com/article/2969233/security/blackberry-denies-its-os-was-to-blame-in-jeep-cherokee-hack.html

[6] http://www.theguardian.com/technology/2015/aug/18/security-flaw-100-car-models-exposed-scientists-volkswagen-suppressed-paper

interesting public policy and safety discussion that has yet to adequately be undertaken[7].

Overall, the release of these compromises has been met with mixed reaction. For Tesla, working with researchers, had a patch ready within days. However, the aspect of entry, through an unsecured Ethernet jack in the car itself indicates that it far from safe from any attack. Fiat-Chrysler worked through a blame game through their telematics system manufacturer, Harman[8], as well as provider of the operating system, Blackberry[9], who manages QNX development, which provides the base for the system. However, due to the delay of disclosure, which was nearly 18 months[10] from when they were aware, already had a $105m dollar fine issued against the carmaker for botched recalls. Fiat has issued USB tokens that can be used to provide the appropriate software upgrade to fix or mitigate discovered issues.

The last collection of hacks, actually two separate ones presented by Samy Kamkar, speak to an issue about selection a technology that can not be changed or upgraded due to a flaw in the core. The former, "OwnStar"[11] exploited a flaw in the cellphone application used to activate OnStar to remotely start and unlock equipped vehicles. This technology was not restricted to one carmaker, but rather several, and has led many to scramble to implement and push out a fix. The later, which involved building upon Kamkar's OpenSesame[12] project on fixed keyspace and rolling access codes, of which RollJam[13] takes it one step further by defeating rolling codes that are used by garage doors and automobile locking systems[14]. The code interception and replay exploits the vulnerability in the architecture and design of the system, something that cannot be field modified or easily upgraded[15]. The last victim of automobile "hacking" was a presentation on Tesla security, who had been at the previous years conference looking to hire security professionals, by independent researchers who took apart a version of the all-electric car to demonstrate how

[7] http://researchcenter.paloaltonetworks.com/2015/07/vehicle-hacks-and-the-age-of-iot-breach-prevention-is-the-only-way-forward/

[8] http://www.reuters.com/article/2015/08/04/us-fiat-chrysler-hacking-harman-intl-ind-idUSKCN0Q91TV20150804

[9] http://www.computerworld.com/article/2969233/security/blackberry-denies-its-os-was-to-blame-in-jeep-cherokee-hack.html

[10] http://www.cnet.com/news/fiat-chrysler-waited-18-months-to-tell-regulators-about-hacking-risk/

[11] http://www.engadget.com/2015/08/13/ownstar-hack/

[12] http://samy.pl/opensesame/

[13] http://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages/

[14] http://www.technewsworld.com/story/82362.html

[15] http://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/

difficult it was to actually obtain access into that platform[16]. However, upon gaining access to the platform, they discovered a lot of basic security flaws that took the "security through obscurity" (or in this case, "propriety") for granted, but as a result of these findings, Tesla proved to be a willing partner in fixing many of these issues and promptly released patches to address those discoveries.

While most of these recent security vulnerabilities focus on the automobiles themselves, the infrastructure servicing them have proven to be just as vulnerable . Other research revealed during the Las Vegas conferences detailed access and control of Internet connected fuel tank monitoring systems[17]. These tanks and systems were at gas stations, truck stops and convenience stores, as detailed by Rapid 7 researchers earlier in the year, and the presentation in August 2015, demonstrated attacks through data captured from virtual honeypots called GasPot[18]. It showed that most attacks were politically motivated based on attributable sources and defacement tags[19]. This speaks to the fears of many that various portions of our critical infrastructure, particularly the energy and transportation sector, are vulnerable – either due to bad initial design or poor security practices.

Mobile

The biggest and loudest noise from the weeks leading up to the security conferences in Las Vegas surrounded several major vulnerabilities in the Android operating system found on millions of phones worldwide. The largest affected base, by sheer numbers alone, was subject to the "Stagefright" [20] vulnerability inherent in the multimedia playback framework. The initial exploit could be launched through a malicious MMS message to end-users and compromise their devices before the users even discovered it. The flaw dates back to Android 2.2, released back in 2010 and newer versions, and would include nearly a billion Android-based phones worldwide[21]. The issue becomes a larger concern given the fact that the fragmentation within the Android ecosystem prevents a patch from being quickly and uniformly applied to address issues such as this. However, the severity of this issue have pushed Google and Samsung to initiate plans to do monthly patch pushes to affected handsets from this point forward[22]. This however, does not solve those

[16] http://www.cnet.com/news/tesla-hackers-explain-how-they-did-it-at-def-con-23/

[17] http://www.wired.com/2015/08/internet-connected-gas-pumps-lure-hackers/

[18] http://www.theregister.co.uk/2015/08/07/gaspot_experiement_trend_micro/

[19] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_gaspot_experiment.pdf

[20] http://www.digitaltrends.com/mobile/android-stagefright-mms-hack-news/

[21] http://www.digitaltrends.com/mobile/why-a-billion-android-phones-will-never-be-safe/

[22] http://www.computerworld.com/article/2957364/cybercrime-hacking/google-and-samsung-to-push-monthly-security-updates-for-android.html

issues that still exist with carriers, such as Verizon and others, that control the OTA updates to customer handsets. As the month went on, other vulnerabilities we found in the MediaServer components[23] that Stagefright were based off of, leading to a very bad month for core Android security.

Then, on the heels of that vulnerability, one vendor specific issue was highlighted and details regarding another major flaw across the OS was released. HTC took a hard hit when it was noted that their fingerprint scans for authentication and identification were stored in easily accessible unencrypted files on the operating system and could easily be read[24][25][26]. Also, due to the flawed architecture constraints, malware could potentially bypass protections and read the fingerprint reader directly and use that data for other access in the system. This also tied into another manufacturer, Samsung, who along with HTC, are not using the TrustZone security features in the ARM chips in the handsets to isolate reader operations from the rest of the system. Each vector into the underlying systems has been proven by researchers to be rather trivial to exploit[27], leaving many more supposedly advanced phones at long term risk.

Adding to the flurry of Android vulnerabilities, and those affecting more modern handsets (in this case, those running Android 4.3 and newer, including Android M), also exists to compromise "system_server" process via OpenSSL X509 certificates in the core OS code[28] and result in privilege escalation. This is not a usual privilege escalation that results in one avenue of exploitation, but due to it exploiting a core process, provides access to many other processes and services on affected devices[29].

What is most telling and in the most frank terms, is scary, is how long these flaws existed in the core components of the operating system of Android. In the agile-driven development strategies of many companies, it begs the question as to if security thinking (and thus everything that follows from having that mindset) is really effectively applied in these environments. The mantra of "fail fast, fail forward" championed from companies such as Google, owners of Android, are

[23] http://blog.trendmicro.com/trendlabs-security-intelligence/mediaserver-takes-another-hit-with-latest-android-vulnerability/

[24] http://www.extremetech.com/mobile/211985-htc-caught-storing-fingerprint-data-in-unencrypted-plain-text

[25] http://arstechnica.com/security/2015/08/severe-weaknesses-in-android-handsets-could-leak-user-fingerprints/

[26] http://techcrunch.com/2015/08/10/htc-is-now-essentially-worthless-and-insecure/

[27] http://arstechnica.com/security/2015/08/severe-weaknesses-in-android-handsets-could-leak-user-fingerprints/

[28] http://www.tomsguide.com/us/android-flaw-hijack-phones,news-21453.html

[29] http://www.theregister.co.uk/2015/08/10/another_android_flaw_hitting_55_percent_handsets/

learning from failures, and not just fixing things and writing it down to the process. In order for the "fail forward" to work, is to understand that if the underlying problem of being insecure is haunting a software project, that possibly that effort should be highlighted and have more focus on it during development, testing and QA. These are vulnerabilities that didn't crop up in minor point releases, but lasted through major revision changes and upgrades, indicating a lack of go od software engineering practices and appears to be more "winging it" to keep delivering on "features" and not realize that security should be one of them.

iOS

Like previous years, as much as there has been a recent focus on several blockbuster Android vulnerabilities, there still remain a number of iOS issues as well. In mo st cases within the past few months, vulnerabilities have been found in services that these devices leverage as well as how certain applications utilize development tools, in this case certain APIs and data protection methods. While present in iOS for several versions and required by Apple's own developer agreement, the sandbox capabilities have been proven spotty at best[30]. When combined with services, such as iCloud, which have had several high profile attacks regarding leaked information, the iOS platform appears no greater than a kitchen strainer when keeping user data safe from inquisitive parties[31]. Many mobile device management (MDM) products promise their customers that their solutions segregate private company data from regular user-space on the device, but due to these flaws in Apple's 3rd party app sandbox (aka "Quicksand" vulnerability), leave this data exposed and able to be accessed by other apps outside of these supposedly protected zones. As noted above, the other flaws in Apple services, such as keychain syncing, leave mobile and desktop computers at risk who use such services, without even needing direct physical access to the systems[32]. Even when best intentions and design guidelines are followed, core flaws (XARA[33]) still render even the more securely programmed apps greatly weakened. It is up to developers to not take APIs and other features for granted based upon promises by even the manufacturer, and should always remain as vigilant as possible and respond to flaws with appropriate and timely mitigating controls and protections.

Web and Application Vulnerabilities

Turn the page on your calendar, expect an announcement of a large-scale data breach. In most cases, these been through Internet-facing applications and websites.

[30] http://www.securityweek.com/attackers-can-exploit-ios-flaw-target-companies-using-mdm

[31] http://arstechnica.com/security/2015/06/serious-os-x-and-ios-flaws-let-hackers-steal-keychain-1password-contents/

[32]

[33] http://www.macrumors.com/2015/06/18/what-you-need-to-know-about-xara-exploits/

What were typically seen as research and development targets five year previously, the targets that have taken prominence in the news have centered on private information, whether it be from financial transactions, insurance and health care, or large caches of personal information from other service provider. There's no single attributor to the particular cause or vulnerability that was exploited, as many came about through an attacker's persistence on a given target's network or environment. However, in most cases, the typical responses from the breached included the standard boilerplate "credit monitoring" package, many, if not all, miss the potential impact of this data, when combined, or mosaic-ed together put potential other areas at risk, even potentially critical infrastructure.

For instance, a number of these breaches have had the resulting stolen data released to the Internet, as well as some events seeing it siphoned off to only those attacker's hands. Putting together the information collected in these (and possibly ones not reported) breaches, you can put together a mosaic of an individual if their information sits across multiple instances within those data dumps. If one of those people holds a sensitive position, or has controlled access to highly prized information in a organization not breached, that personal information can be used to gain access. This can be achieved by the use personal information often leveraged for verification purposes, or be perpetrated for outright blackmail against a selected target.

Two cases such as this were very public for 2015, the Federal Government's breach of the Office of Personnel Management's (OPM) databases and the leak of a proclaimed "affair" enabling website, Ashley Madison. In the former, one of the databases for the SF-86, the system used to gather security clearance information from background checks, was completely stolen. The risk here, is that as part of the requirement of filling this out, even if the Federal employee is denied a clearance, they have detailed much more personal information (criminal, health, mental, financial, travel) than typically seen in a database for, example, a health insurer. This system also includes required lists of contacts with foreign nationals by those employees, and the type of work and information they have handled and currently handle – essentially a "little black book" for Federal employees with access to extremely sensitive information. In the latter case, with the Ashley Madison breach, the site marketed itself as a facilitator for extramarital affairs and fantasy encounters. With multiple data "dumps" made of information exfiltrated from the site, researchers are pouring over it for interesting items – and for those with non-publicly disclosed data sources, such as those from OPM and those from health insurers – can assist in the development of profiles that can be used for exploitation and/or blackmail. However, upon review of how these occurred, it appears that in most cases, basic security polices and protections were neither followed nor implemented.

A lot of what backs these websites and services are large databases, and one of the larger suppliers of this technology, Oracle, had its CSO fire off a very terse blog post[34] to customers and researchers that asked them to not violate their licensing agreements and to not attempt to find vulnerabilities in their software or systems. Oracle has had a speckled past with the information security community, and this latest incident was the equivalent of putting chum in the water to attract sharks, as the security community took Oracle to task over a flawed view on how vulnerability research and disclosure is performed. Assuredly, when a software developer ignores the reality of the environment in which their software is deployed, they will end up putting their customers at greater risk, asking them ignore threats and challenges to their operations. If other companies who develop similarly critical software and services also followed this practice, the current state of computing on and off the Internet would be a bigger morass than it currently finds itself in.

Contrary to the view from Oracle, other software developers have been rather proactive in taking a stance against poor security or high-risk activities. In a move that will force a number of websites to find alternative means to develop and deliver their content, both Google with their Chrome browser, and Firefox will be disabling Adobe Flash by default as a way to protect users from exploits through the popular web plug-in[35]. This was already on the heels of the much publicized eschewing of native Flash support by the popular, yet a minority player, Apple OS X and Safari for HTML 5 and its media extensions. However, HTML 5 is not without its own problems due to the "fast and loose" architecture that was built into the standard for extensibility and flexibility[36], as well as the new WebAssembly[37], which is a lower-level web language that comes with a potential to be even more dangerous than JavaScript under the guise of being more portable and faster than its predecessor. However dealing with bytecode and powerful instructions[38] have proven difficult in the past, such as Java, and there's been no guarantee that those issues have been addressed and lessons learned[39] in the development and use of this new language[40]. For every step forward that's made to try to make the Internet safe, a potential slide backward tends to occur for the sake of speed or portability, without, often consideration that one size may not fit all, and optimization does have its practical limits.

Major Platforms

[34] http://www.theregister.co.uk/2015/08/18/row_over_disavowed_figures_oracle_cso_anti_security_rant/

[35] http://thenextweb.com/insider/2015/07/14/firefox-rings-the-death-knell-for-flash/

[36] https://www.owasp.org/index.php/HTML5_Security_Cheat_Sheet

[37] https://medium.com/javascript-scene/what-is-webassembly-the-dawn-of-a-new-era-61256ec5a8f6

[38] http://www.2ality.com/2015/06/web-assembly.html

[39] https://github.com/WebAssembly/design/issues/205

[40] http://arstechnica.com/information-technology/2015/06/the-web-is-getting-its-bytecode-webassembly/

Apple

Apple was, again, a favorite target of security researchers, if not for their marketplace hubris, but also for the fact more and more novice users are flocking to the platform in the shape of MacBook laptops and iMacs. Like iOS and the mobile devices, the combination of near ubiquitous hardware and OS X combination has identified a number of new exploits since this time last year, most substantial being "Thunderstike 2"[41]. The Thunderstrike vulnerability affects the Thunderbolt connectors on most modern Mac desktops and laptops and targets the firmware on connected devices[42], very similar to an older IEEE1394 Firewire vulnerability that affected Apple products a number of years ago. Due to this affecting the firmware of the affected system, most anti-virus and rootkit detection products available can not detect issues at that level due to their own access restrictions and are extremely difficult to remove[43].

Besides the firmware issues, Apple also managed to have a pair of root-level exploitable flaws within their dynamic library infrastructure that were only introduced in the recent revision of its operating system, OS X. The first of which, when pasted in the terminal window (shell) of any Mac running the affected version of the OS, a set of commands would leverage this exploit to acquire root privileges[44]. So simple and short was this exploit, that it took up less space than required for a typical Tweet[45]. Weeks later another root-level exploit was released[46], this time taking aim at issues with IOKit[47] and its handling of NULL page exceptions[48] and exist within the new OS X 10.11 (El Capitan) codebase as well according to the primary researcher[49].

Microsoft

Recently Microsoft released their long awaited flagship operating system, Windows 10, to the consumer market. It was seen as a departure from previous efforts, and a major attempt to "right some wrongs" that had irked developers and users alike. However, as the covers were pulled off of the OS, troubling issues and concerns

[41] http://www.wired.com/2015/08/researchers-create-first-firmware-worm-attacks-macs/

[42] https://www.schneier.com/blog/archives/2009/10/evil_maid_attac.html

[43] http://arstechnica.com/apple/2015/08/thunderstrike-2-rootkit-uses-thunderbolt-accessories-to-infect-mac-firmware/

[44] http://arstechnica.com/security/2015/08/0-day-bug-in-fully-patched-os-x-comes-under-active-exploit-to-hijack-macs/

[45] http://www.theregister.co.uk/2015/07/22/os_x_root_hole/

[46] http://www.macrumors.com/2015/08/17/os-x-10-10-5-tpwn-vulnerability/

[47] http://www.tomsguide.com/us/os-x-zero-day-flaws,news-21476.html

[48] https://www.suidguard.com/stories/index.html

[49] https://github.com/kpwn/tpwn

began to be raised. First out of the gate was the WiFi password-sharing feature (WiFi Sense) that attempts to use social network capabilities to allow "friends" to easily attach to each others networks. However, besides potentially being a major privacy breach waiting to happen, the potential for exploitation is merely a simple social engineering attempt and lackadaisical configuration management away[50]. While it's not the actual password that's getting shared, but rather an encrypted, tokenized version, it's still susceptible for abuse, especially for the careless or novice users out there[51].

Other privacy concerns have cropped up in the month post release, particularly regarding what you agree to upon even installing the software. In an egregious attempt to prevent pirated software from being installed on the platform among other "features", Microsoft leverages the language in their privacy policy to justify their ability to look at your data and determine it being "good or bad":

"We will access, disclose and preserve personal data, including your content (such as the content of your emails, other private communications or files in private folders), when we have a good faith belief that doing so is necessary to protect our customers or enforce the terms governing the use of the services."[52]

As well as this section when detailing how Windows may arbitrarily deal with, what it determines, as unauthorized software.

"We may automatically check your version of the software, which is necessary to provide the Services and download software updates or configuration changes, without charging you, to update, enhance and further develop the Services, including those that prevent you from accessing the Services, playing counterfeit games or using unauthorized hardware peripheral devices."[53]

This is an overly broad statement that allows a lot for interpretation and has gotten consumer rights specialists and technologists up in arms about how it may be used and what it really means[54]. Some analysts walk back the uproar over statements like the one above, however, understanding that many users will not take the time to read every detail of a EULA nor really spend time tweaking group, let alone individual settings, doesn't realize the truth in technology adoption currently[55].

[50] http://krebsonsecurity.com/2015/07/windows-10-shares-your-wi-fi-with-contacts/
[51] http://www.rockpapershotgun.com/2015/07/28/windows-10-wifi-sharing/
[52] https://www.microsoft.com/en-us/privacystatement/default.aspx
[53] http://www.csoonline.com/article/2975005/operating-system-security/is-windows-10-the-end-of-privacy-as-we-know-it.html
[54] http://www.techrepublic.com/article/windows-10-violates-your-privacy-by-default-heres-how-you-can-protect-yourself/
[55] http://www.techrepublic.com/article/windows-10-violates-your-privacy-by-default-heres-how-you-can-protect-yourself/

Often, much of this can be traced back to the choice of defaults by Microsoft themselves, who already finds it at their advantage to enable, rath er than disable, features that lock in uses of certain services and features that the company can leverage for various purposes, even if the user does see some tangible benefit[56]. Most enterprise customers won't be directly affected by these particular issu es, mainly by the nature of how they are often installed and managed, but with the push towards cloud services and their integration with the desktop, more and more, data rights and privacy between entities will been scrutinized[57].

However, even with the privacy snafu, many changes within Windows 10, built on painful lessons from previous OS releases, have led to it potentially being the most secure version ever. The integration of multi-factor authentication is a big step in making the OS more modern, and less reliant on "shims" into the older authentication systems seen on XP, Vista and Windows 7. Add to that more enterprise relevant features such as device lockdown, a newer and less "bloaty" web browser (Edge) to replace Internet Explorer, and near continuous updates and patches, essentially shortening (at least for consumers) the time from flaw discovery to fix[58].

Other Platforms and Devices

If there was a buzzword that the tech community has begun to over use in the past 18 months, it has been IoT, or "The Internet of Things". Much like how 3D, VR, cloud, and mobile became the darlings for a time and either withered or just be came commonplace, the next up for the hype would definitely be IoT. However, much like cloud technologies, which were borne by the proliferation of virtualization technologies, IoT has its roots in just the idea of connecting single, or specialized systems to a network and having them perform a task and send that data to another location as a collection or command and control point[59]. Initially it began with academics and researchers connecting simple devices up to the web, such as a coffeepot or soda machine, in order to demonstrate the status or inventory of that device, but that merely mirrored industrial control systems (ICS) that have been in use but never openly connected to the Interne[60]t. Now, with the advancement of processing power, rise of IPv6, and near ubiquitous access to some kind of network (wired or wireless), the idea of linking everything and anything together has taken

[56] http://www.slate.com/articles/technology/bitwise/2015/08/windows_10_privacy_problems_here_s_how_bad_they_are_and_how_to_plug_them.html

[57] http://www.wired.com/2015/08/windows-10-security-settings-need-know/

[58] http://www.cio.com/article/2954912/windows/how-to-get-the-most-out-of-windows-10-enterprise-security-features.html

[59] http://www.darkreading.com/attacks-breaches/iot-flaw-discoveries-not-impactful--yet/d/d-id/1321199

[60] http://www.infoworld.com/article/2972161/network-security/akamai-the-internets-aging-protocols-make-juicy-targets.html

off. Understandably, some of the first technologies were geared towards home automation and security, such as lightbulbs, weather stations, and security cameras[61]. The second wave, taking hints from old promotional videos from General Electric and Microsoft, are smart appliances and surfaces that pull in data from what they do (such as refrigerate) or their environment, and provide data to the owner or automate simple tasks based upon that data, in the form of triggers. At any point along that path, many of these devices and solutions contain vulnerabilities that can and have been exploited, or use those control systems to take control of the larger environment, such as a home. The Federal Trade Commission (FTC) has attempted to get ahead of this wave, and issued warnings to developers that security should not take a backseat when these products are sold to consumers to install[62].

While not traditionally considered IoT devices, many medical devices find themselves network enabled, whether it be in a medical facility or wired to a home network for remote reporting and control, or just a personal-are-network (PAN) used to short distance tuning. There has been plenty written about the issues with Zigbee-enabled wireless devices[63] being susceptible to attack due to being susceptible to injection attacks and spoofing[64], however non-wireless devices are also a target. All medical devices have to adhere to FDA standards[65], however, often those standards may contain gaps due to the speed and diversity of certain technologies. The most trumpeted of recent medical device flaws is the Symbiq infusion pump[66], which demonstrated poor system design through weak authentication and stored or easily guessed system passwords, and unsecure communication channels (Telnet and FTP) that enabled complete control of the device by attackers. The company, in advisory issued along with a DHS CERT note[67], didn't mention a recall, but a discontinuation of the use of the devices and those newer devices should be used instead. This potentially leaves devices in the hands of individuals and organizations that can not easily acquire replacement hardware, such as those in the developing world or other areas, as well as those who acquired the products through secondary or refurbished markets in which ownership trails are spotty at best.

[61] https://securityledger.com/2015/04/research-iot-hubs-expose-connected-homes-to-hackers/

[62] https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices

[63] http://www.tomsguide.com/us/medical-devices-blackhat,news-19294.html

[64] http://www.willhackforsushi.com/presentations/toorcon11-wright.pdf

[65] http://www.nuvation.com/blog/electronic-design-services/iot-medical-device-design-meeting-fda-guidelines

[66] http://www.hospira.com/en/about_hospira/newsroom/cybersecurity/cybersecurity_vulnerabilities

[67] https://ics-cert.us-cert.gov/advisories/ICSA-15-161-01

Payment systems and devices have been a prime target beyond the data breaches at retailers, due to the near ubiquity of personal card readers such as Square and PayPal, but also NFC-enabled payment in everything from smartphones to card consolidators such as Coin. To combat recent shortcomings with traditional magnetic stripe readers, the payment card industry has mandated that newly issued cards shall contain a "chip and PIN" component. Recently a flaw had been discovered in the popular Square reader, allowing researchers to turn the swipe reader into a skimmer device[68]. While not an issue with the device itself, the ability to turn free hardware into such a product, quickly and cheaply, continues to expose the issues with relying on old technology to perform financial transactions. The US credit card processing terminals around the US are supposed to be switched to the chip and pin capability by this October, but the roll-out is still piecemeal at best. However, the NFC "touchless" systems currently in use[69] and the chip-and-pin wireless terminals have been found to contain vulnerabilities[70] in their design over the past few years that prevent them from being a perfect alternative. Sadly this only covers preventing potential fraud through point-of-sale (POS) instances, but with the prevalence of Internet-based transactions, the use of such a system is useless in these cases (often recorded as a "card not present" transaction)[71].

Laws and Regulations

On the non-technical side, there have also been a number of developments worth noting, some regarding laws and policy, but also how some issues and vulnerabilities exist in our public services currently in action. First is the application of the results from a decades-old arms control agreement, called The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, or Wassenaar for short that threatens the "freedom" of security researchers, not only in the US, but also worldwide. Due to the language in this agreement, Category 5, Part 2, many researchers will run afoul of the international agreement and could place them in the same category as military arms dealers by simply researching vulnerabilities in systems, applications and hardware, essentially criminalizing their work and potentially putting many at risk due to an overly broad definition[72]. While it attempts to block or prohibit tools that are or can be classified as offensive in nature, defenders that check for vulnerabilities and problems in the systems they are set to protect also use those same tools. This is a very dangerous precedent to be setting and doesn't reflect the actual reality of the

[68] http://mashable.com/2015/08/04/square-reader-card-skimmer/

[69] http://www.wired.com/2014/11/chip-n-pin-foreign-currency-vulnerability/

[70] https://www.lightbluetouchpaper.org/2014/05/19/the-pre-play-vulnerability-in-chip-and-pin/

[71] http://sec.cs.ucl.ac.uk/users/smurdoch/papers/oakland14chipandskim.pdf

[72] https://community.rapid7.com/community/infosec/blog/2015/06/12/wassenaar-arrangement--frequently-asked-questions

profession and need within the space for such access, putting practitioners at a risk for being charged with an international-level crime.

As noted earlier, the Federal Trade Commission (FTC) has taken a larger role in addressing who regulates much of the digital world apart from the communication channels (of which the Federal Communications Commission [FCC] handles). With a ruling from the 7th Circuit[73], signals that consumers do have a standing with complaints that companies may not protect their data as they should (*Remijas v. Neiman Marcus*), and can result in penalties if consumer data is mishandled or lost during a compromise or breach. This is on the heels of the FTC stepping up its enforcement[74] on how companies are required to handle consumer data in relation to privacy laws for online transactions, but also how personal data is being treated in the new landscape of IoT[75].

One of the two, more interesting than most, presentations at this year's DefCon was how to exploit, what the researcher Chris Rock termed, as an "end-of-life vulnerability", which involved spoofed credentials and access to the systems that manage birth and death records[76]. While sadly, this is more often seen on television or in the movies, used by spies or those who wish to "go off the grid", Mr. Rock's description of how poorly the system manages authentication and verification of its users and actions within the system as well as how easily that information, or order to forge the activity, is available to the general public. This is equivalent to input validation and SQL injection if it were merely a vulnerability on a website, but the Rock had determined that most of this takes place between scraping databases and filling out standard forms that require no multiple verification components. The lack of these verification "gates" can lead to multiple types of fraud, typically those often leveraged with identity theft, and Mr. Rock had urged that multi-factor authentication be used, if even a phone call, in these, now openly vulnerable cases[77]. Sadly, as it's seen as a parallel to technical exploits, it is up to regulatory and law making bodies to address these issues and enforce them, but it does provide a good example of how blended threats can result in rather catastrophic consequences.

The second of the two more novel presentations revolve around locks and the keys used within them. For those that find locksport (the activity of picking locks to learn or for fun, but not as an offensive skill) an interesting pastime, mastering the light touch of a pick, rake and tension wrench – technology has stepped in to the game slightly to make it just a little less interesting. Typically to pick locks requires a light

[73] http://www.wired.com/2015/07/new-hope-victims-data-breaches/

[74] https://www.ftc.gov/news-events/press-releases/2015/03/ftc-seeks-technologists-new-research-investigations-office

[75] https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices

[76] http://www.engadget.com/2015/08/10/kill-virtual-people/

[77] http://www.computerworld.com/article/2966130/cybercrime-hacking/def-con-how-to-virtually-kill-someone-or-cash-in-on-fake-babies.html

touch, a feel and good ears to hear the pins catch and bind and the cylinder turn ever so slightly. However, thought he use of some slick computer programing, a picture of the key or keyway, and a reasonably good resolution 3D printer, you can print your way into a locked area. A project called Keysforge[78] leverages several technologies to develop a solid model, useful in CAD programs and 3D printers to generate a model of a key for a keyway[79]. One of the upsides, for those who have restrictions on obtaining key copies (such as those marked "Do Not Duplicate"), this may, with refinement, offer such an opportunity to obtain such copies. While this project was not developed in a offensive manner, but as a way to demonstrate to the lock design industry that inexpensive attacks are viable, even when there's a policy framework in place attempting to prevent an activity.

In the wake of the Office of Personnel Management breaches earlier in the year, a number of other high profile sites and organizations have had their data spill across the Internet, the Cybersecurity Information Sharing Act (CISA)[80] has been once again, stalled in Congress. This is not without reason, as previous versions of the legislation had glaring issues regarding privacy, indemnification, and general logic flaws in how information is shared between the government and private industry, that another delay was not surprising[81]. However, there has been some resistance to this legislation from the public, indicating that they are concerned about potential large violations of privacy that, given the current broad language, could occur if the sharing agencies and organizations do not adopt comprehensive data standards. Unlike information sharing between agencies and groups within the public sector, specifically intelligence related data; there is a higher bar for sharing such detailed information down to the private sector. This has a greater impact on individual citizens and even companies if personally identifiable information (PII) or other sensitive data is shared with a group, due to this legislation, that ends up in the wrong hands, is mishandled, lost, or is stolen[82]. However, after the OPM breach, the trust within the government, and from outside, that even the most sensitive of data, such as personnel records and background investigation data can be handled properly, will probably keep the passing of this legislation from happening in the near future, even though this has been a priority pushed from both the White House and Congress.

Conclusion

[78] http://www.wired.com/2015/08/this-app-lets-anyone-3-d-print-do-not-duplicate-keys/

[79] https://keysforge.com

[80] https://www.congress.gov/bill/114th-congress/senate-bill/754/text

[81] http://www.pcworld.com/article/2958677/senate-delays-vote-on-cisa-cyberthreat-info-sharing-bill.html

[82] http://www.washingtonpost.com/news/powerpost/wp/2015/08/05/cybersecurity-faces-key-senate-vote/

Overall, if you choose any common technology to use, inevitably, there's a flaw, and with that, a potential vulnerability. Vigilance during its operation and awareness of where and when it's used will me everybody's first line of defense. As demonstrated above, our collective trust that a service provider or manufacturer has security as their top priority is generally misplaced, and requires us to think a few steps down the road for our own safety. However, this doesn't require us to be paranoid, just skeptical and take claims with a "grain of salt" and pressure those groups from which we purchase a good or service from to think about us, and what their responsibility is after that initial interaction or transaction. For those that do go the extra mile, that provides a level of transparency, but are also welcoming feedback and critique is to be open and provide such to them in order to demonstrate that we care about our own well being and others. This isn't strictly self-interest, but the basic need for self-preservation in this digitally oriented world. As a trustee of many of our guests, patrons and customers' data and experiences – we too, should use that same measure to ensure that the work we do and our interactions go to build and uphold the trust they've put in to us, knowing that as we help make memories, we are also securing them.