Why Computer Security is hard to get right

Tennis Watkins

English 102 Class # 14612

James Palazzolo

10/4/2016

Tennis Watkins

English 102 Class # 14612

James Palazzolo

10/4/2016

Why Computer Security is hard to get right

As a society we now live in the information age. The computing power in our cell phones today far exceeds the computers of fifty years ago when a computer would occupy an entire room, but held very little information. Initially, computers required a person to operate them. This is no longer the case today. We live in an era with ubiquitous computing according to Dr. Michiu Kaku, a futurist and theoretical physicist holding the Henry Semat Chair and Professorship at the City College of New York (CUNY) who studies the frontiers of physics; computers are nearly everywhere (Kaku): in our phones, in our cars, and even in our kitchens to the extent that we could computer are ubiquitous. This raises a question about the effect "ubiquitous computing" is having on us (Perez).

> "IBM's 2015 Cyber Security Intelligence Index stated that 45 percent of all breaches were due to insiders and that 95 percent of those breaches were due to human error. In other words, 42.75 percent of the average companies' breaches were due mostly to inadequately or improperly trained personnel. That is a staggering statistic which should demonstrate why it is an imperative to educate the modern digital workforce on the importance of being safe 'digitally'." (Perez)

In addition to having the workforce trained to be safe “digitally, it is also important to have the the average home user trained to be safe ‘digitally’ as well; especially considering that more and more people complete financial transactions online.

From the inception of computer hardware and software, computer security has not been at the forefront of development, but it is starting to become a more pressing issue for developers and end-users. Computer software is difficult to engineer in a such manner that guarantees that only the predictable outcomes occur and the user doesn’t experience any unpredictable behaviors or issues. As Bruce Schneier said “A good attack is one that the engineers never thought of.” (Young Slide 4). For this reason, computer security is incredibly difficult to get right. Breaches of security seem to occur for a variety of reasons including financial gain and political gain, and entertainment value, thus there seems to be some basic flaws in computer systems or end-user practices that allow this to happen.

Since computers have become such an integral part of our lives, it seems that many users “trust” their computers without thinking about the risks they face when doing simple things like ordering an item from a website. Many end-users are not aware of security risks like coding flaws and phishing, a technique to trick users out of personal information by abusing their trust of digital interfaces with which they choose engage, so they do not use safe practices to minimize exposure to potential attacks and malware. In the words of Steve Gibson, host of computer security podcast Security Now!, users should “Trust No One”, or TNO, as much as possible. This is practice will help users avoid risks such as someone pretending to be a close friend or relative, when some other entity sent the attack instead. The idea of TNO is to not trust something digital unless you were expecting it or went searching for it and can verify the source.

Even cautious users are at risk for security breaches because it is very difficult to stay one step ahead of hackers. Software developers face a number of challenges including that of defending against attacks that they haven't yet imagined. As was observed by Ross Anderson, "where the party who is in a position to protect a system is not the party who would suffer the results of security failure, then problems may be expected." Both websites and software companies offer their services and do bear some risk but it is typically the user that suffers the most when there is a data breach or a flaw in their security. When a data breach occurs, or when a computer is infected by a virus or malware, there are costs incurred. For example, hackers recently broke into Yahoo's stealing 500 million users credentials that took two years to be detected after Yahoo had spent 10 million encryption technology because of previous intrusions (Perlroth and Goel). Another example, Maricopa County Community College District experienced a data breaches in 2011 and 2013. The costs for these incidents have exceeded $26 million (Faller). Ross Anderson in "Why Information Security is hard - an economic perspective" speaks to computer security from the point of view of economics. He discusses the motives behind securing computer systems and how, when an entity is economically responsible for information that must be secured, a more robust security can be found implemented at that location.

One of the challenges facing the computer security industry was and still is communication. It is difficult to discuss security without common language. Sandia National Laboratories, a 60 year old government-contracted research lab for science and technology, was commissioned to write the report "A Common Language for Computer Security Incidents" to provide common computer security terminology and vocabulary in order to facilitate

communication across the computer security sector, including journalists. While old by computer standards, this report set the stage for computer security and pushed it forward to a point where we have useful phrasing and can efficiently communicate issues (Howard & Longstaff). Many everyday users of computer systems do not understand what terms such as "phishing", "spoofing" and "botnets" mean so when consuming news stories that contain these terms they will not understand the risks being discussed and how to minimize exposure to those risks.

The U.S. Department of Defence published a short list of tenets with the goal of informing the general public about risk exposure and good practices related to computing in the hopes of reducing system vulnerabilities (The Three Tenets of Cyber Security). Their tenets are: focus on what's critical (control access points to a computer system), move it "out of band" (make access points difficult to find and to breach), and Detect, React, Adapt (fight an "attack" as it is occurring). Following these tenets can help keep a computer system secure. Many businesses, educational institutions and other organizations use some or all of these tenets in their attempts to keep their systems and their data secure. Creating and maintaining secure systems places a hefty burden on developers with other projects, while potentially thousands of infiltrators can devote all their time into breaking into a system. "Even a very moderately resourced attacker can break anything that's at all large and complex. There is nothing that can be done to stop this, so long as there are enough different security vulnerabilities to do statistics: different testers find different bugs" (Ross Anderson).

Security is something that can not be done once, but rather a perpetual goal that requires constant monitoring and use of proper behaviors. For nearly the past decade, Adobe Flash has been constantly updating its source code to improve security; in a prime example of the notion

that: “The defender has to find and eliminate all exploitable vulnerabilities; the attacker only needs to find one!”(Bill Young). CVE, Common Vulnerabilities and Exposures, aims to provide common reference number for publicly known cyber security issues. CVE’s oldest recorded severe flaw with Adobe Flash dates back to 2008 (Vulnerability). Flash has proven year to year to be a problem for security, partly due to its large presence in marketing via Flash-based advertisements. This marks Flash as a valuable target for hackers to penetrate in order to gain access to user’s computers. As a result of persistent security issues with Flash, Amazon and Google are ending support for Flash-based ads in their advertising networks starting in 2017 (Cajucom et al. 6) An example of the necessity to continuously monitor the security of your software is the recent hacking of Apple iOS products. A government targeted a human rights activist with Trident, a chain of zero-day exploits (bugs that are discovered while already in use) designed to infect his iPhone, one of the most popular smartphones on the market. Because the activist followed best practices in not clicking on unknown links he was able to report the incident which led to the discovery of an chain of exploits, or flaws in the system, which could lead to the phone being compromised and turned into a device which could spy on the user. When made aware of the flaws Apple responded within 10 days to patch their software eliminating the flaws and pushed updates to their users (Marczak and Scott-Railton) . From these two examples, we can see that with more widespread usage also comes the attention of more hackers trying to find exploits in the software. Therefore, exploits are likely to be found due to the probability of being able to exfiltrate valuable user data.

Computer users need to be aware of the tradeoffs between security and convenience. For example, using the same password for multiple accounts is convenient but not secure because

once the password is cracked access is gained to all of those accounts. A firewall is a common tool used to secure a network of computers that provides filtering services on incoming network activity. There have been two methods for filtering: blacklisting and whitelisting,

> "...the very first deployments of firewalls were default open and blocking only specific things that were known not to want to be made public. And it took a while, but we finally reversed that model in firewalls where it's default block... although it's arguably more difficult, you're going to perhaps false block when you don't intend to. But that's better than having everything open by default and blocking only the things you know you want to prevent...for a long time we operated with a blacklist approach with firewalls, and then switched over to whitelisting and realized that's much more effective." (Steve Gibson)

Blacklist is more convenient because you supply a list of known programs/protocols/ports you wish to block, or deny access, leaving all other network activity free to pass. The problem with blacklisting is that it leaves you open to unknown threats. Whitelisting is less convenient because it only permits activity that has been explicitly authorized which could to some annoyance and additional effort required to grant access to new activities.

Even with the constant threats, there are some best practices that the average user can employ to improve their own cybersecurity.

- Never reuse a password; instead, use a password manager to create and maintain strong passwords. Gawker and rootkit.com, both forums for computer techs, report a password reuse rate of between 31% and 43%. These types of websites attract a more technically savvy crowd, which know the risks of password re-use and would cause their password reuse rates to be lower than typical users. This

would mean that the average user has password re-usage rate that is likely much greater than might be found on those forums. (Bonneau).

- Never click unknown links, especially if you didn't go looking for that information. Hackers will “spoof” a legitimate website, or create an imitation website in an effort to obtain usernames and passwords from unsuspecting users.
- Only install from the original source (never download pirated or cracked software), and always install updates. A user should not trust that other sources have not tampered with the original source code.
- Users should limit the use of the Administrator account because any process that might try to run on the computer will be able to automatically execute with prompting the user for access.
- Keep system and application software up-to-date so that any known holes in software security are patched. When a patch is released it draws attention to flaw in the software so hackers exploit this flaw on users who have not yet applied the patch.
- Ensure that a device firewall is active as it will try to prevent malicious software from gaining access to the device. Double check the settings within the system or security software occasionally to be sure the firewall is active.
- Do not click on or follow directions of popup windows that tell you that your computer is infected with a virus as these windows are malicious advertisements masquerading as antivirus software.

- Be careful with email attachments. Hackers will embed viruses or malware in files in the hopes that a user will download and open the file releasing the virus or malware into the system.

These practices are just a few of the many that will help users stay safe while computing.

We live in a time unprecedented in history. We have access to information 24 hours a day, seven days a week using our phones, a laptop computer, or a tablet computer. Because we are so digitally connected we are vulnerable to threats which can do us harm. Whether that be stealing usernames and passwords, or stealing our identity. With this increased level of connectedness the security of our data and our digital devices becomes extremely important. Unfortunately, securing the data and devices is a difficult thing to do. Users need to become more proactive and aware of the best practices so that they to do not become the next victim in a digital battle between the forces of good and evil.

Works Cited

Anderson, Ross. "Why information security is hard-an economic perspective." Computer security applications conference, 2001. acsac 2001. www.acsac.org/2001/papers/110.pdf. 30 Aug. 2016.

"Best Practices for Keeping Your Home Network Secure" The Information Assurance Mission at NSA Apr. 2011 http://www.24af.af.mil/Portals/11/documents/AFD-110722-051.pdf?ver=2016-04-26-150055-163 25 Sept. 2016.

Bonneau, Joseph. "Measuring password re-use empirically." Light Blue Touchpaper. 2 Sept. 2011. https://www.lightbluetouchpaper.org/2011/02/09/measuring-password-re-use-empirically/ 25 Sept. 2016.

Cajucom, E., Dacuno P., Aquino K., Aquilino B., Hilyati A., Jamaludin S., . . . Michael M. "Threat Report 2015" F-Secure Corporation. 11 Apr. 2016. https://www.f-secure.com/documents/996508/1030743/Threat_Report_2015.pdf 25 Sept. 2016.

Davis, Michelle R. "Schools Learn Lessons From Security Breaches." Education Week. Web. 21 Oct. 2015.www.edweek.org/ew/articles/2015/10/21/lessons-learned-from-security-breaches.html. 30 Aug. 2016.

Faller, M. B. "Maricopa County colleges computer hack cost tops $26M" The Arizona Republic. 17 Dec. 2014. http://www.azcentral.com/story/news/local/phoenix/2014/12/17/costs-repair-massive-mccd-computer-hack-top-million/20539491/ 25 Sept. 2016.

Gibson, Steve. "Security Now! Episode 370: Mark Russinovich." Gibson Research Corporation. 19 Sept. 2012. https://www.grc.com/sn/sn-370.htm. 25 Sept. 2016.

Gibson, Steve. "Security Now! Episode 573: Memory and Micro Kernels." Gibson Research Corporation. 16 Aug. 2016. www.grc.com/sn/sn-573.pdf. 30 Aug. 2016.

Howard, John D., and Thomas A. Longstaff. "A Common Language for Computer Security Incidents." (1998). PDF file. Accessed from http://prod.sandia.gov/techlib/access-control.cgi/1998/988667.pdf. 30 Aug. 2016.

Hess, Ken. "10 security best practice guidelines for consumers" ZDNet. 5 Mar. 2013 http://www.zdnet.com/article/10-security-best-practice-guidelines-for-consumers/ 25 Sept. 2016

Kaku, Michio. "About : Explorations in Science :: Official Website of Dr. Michio Kaku" Michio Kaku. http://mkaku.org/home/about/ 25 Sept. 2016.

Marczak, B., & Scott-Railton, J. "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender" The Citizen Lab. 25 Aug. 2016. https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/ 25 Sept. 2016.

Perez, Roi. "Cyber-security Awareness a Battle Between the Rational and Impulsive Brains" SC Magazine. 5 July 2016. http://www.scmagazineuk.com/cyber-security-awareness-a-battle-between-the-rational-and-impulsive-brains/article/504960/ 25 Sept. 2016.

Perlroth N., & Goel V. "Yahoo, reluctant to disturb users, set them up for huge data breach" The Seattle Times Company. 1 Oct. 2016.

http://www.seattletimes.com/business/technology/yahoo-reluctant-to-disturb-users-set-them-up-for-huge-data-breach/ 25 Sept. 2016.

"The Three Tenets of Cyber Security". U.S. Air Force Software Protection Initiative. 2001. www.spi.dod.mil/tenets.htm. 30 Aug. 2016.

“Vulnerability Details : CVE-2007-0071” MITRE Corporation. 9 Apr. 2008. https://www.cvedetails.com/cve/CVE-2007-0071/ 25 Sept. 2016.

Young, Bill. "Foundations of Computer Security Lecture 2: Why Security is Hard." www.cs.utexas.edu/~byoung/cs361/lecture2.pdf. 30 Aug. 2016.

Zlatanov, Nikola. "Computer Security and Mobile Security Challenges." Research Gate. , Dec. 2015. www.researchgate.net/publication/298807979_Computer_Security_and_Mobile_Security_Challenges. 30 Aug. 2016.