Security Leftovers

By *Roy Schestowitz*
Created *17/06/2019 - 4:36pm*
Submitted by Roy Schestowitz on Monday 17th of June 2019 04:36:25 PM Filed under Security [1]

- **Microsoft Warns about Worm Attacking Exim Servers on Azure [2] [Ed: Microsoft should also warn "customers" of Windows back doors for the NSA, but it does not (this one was patched ages ago; the Microsoft back doors aren't). Shouldn't Microsoft ask its proxies and partners, as usual, to come up with buzzwords and logos and Web sites for bugs in FOSS, then talk about how FOSS is the end of the world?]**

- **The Highly Dangerous 'Triton' [Attackers] Have Probed the US Grid [3] [Ed: It's Windows [4]]**

  > Over the past several months, security analysts at the Electric Information Sharing and Analysis Center (E-ISAC) and the critical-infrastructure security firm Dragos have been tracking a group of sophisticated [attackers] carrying out broad scans of dozens of US power grid targets, apparently looking for entry points into their networks. Scanning alone hardly represents a serious threat. But these [attackers], known as Xenotime?or sometimes as the Triton actor, after their signature malware?have a particularly dark history. The Triton malware was designed to disable the so-called safety-instrument systems at Saudi Arabian oil refinery Petro Rabigh in a 2017 cyberattack, with the apparent aim of crippling equipment that monitors for leaks, explosions, or other catastrophic physical events. Dragos has called Xenotime "easily the most dangerous threat activity publicly known."

- **A Researcher Found a Bunch of Voting Machine Passwords Online [5]**

  > A little more than a week ago, the Department of Homeland Security confirmed that it was going to forensically analyze computer equipment associated with part of the 2016 elections in North Carolina in association with questions about Russian hacking. The news prompted an

information security researcher to announce that he?d found evidence of other election security issues in North Carolina last fall, which he?d kept quiet until now.

Chris Vickery, the director of cyber-risk research at UpGuard, a cybersecurity services firm, tweeted June 7 that he had found an unlocked online repository that contained what he said were passwords for touchscreen voting machines. The repository, he said, also contained other information, including serial numbers for machines that had modems, which theoretically could have allowed them to connect to the internet.

Vickery said that after he found the open repository in September 2018, he immediately told state officials, who locked the file. State officials have told Mother Jones that the passwords were nearly 10 years old and encrypted?a claim disputed by Vickery and a Democratic technology consultant in North Carolina?but admitted that the file shouldn?t have been publicly available online.

- **TPM now stands for Tiny Platform Module: TCG shrinks crypto chip to secure all the Things [6] [Ed: Misusing the word "trust" to obliterate computer freedom [7] and general-purpose computing]**

  The Trusted Computing Group (TCG), a nonprofit developing hardware-based cybersecurity tools, has started work on the "world's tiniest" Trusted Platform Module (TPM).

  TPMs are silicon gizmos designed to protect devices by verifying the integrity of essential software ? like firmware and BIOS ? and making sure no dodgy code has been injected into the system prior to boot.

  These are widely used to protect servers. Now TCG wants to adopt the technology for devices that are so small that the inclusion of a full TPM chip might be impractical due to cost, space and power considerations.

  The first tiny TPM prototype, codenamed Radicle, was demonstrated last week at a TCG members' meeting in Warsaw, Poland.

  [...]

  We have to mention that for years, TCG and its TPMs were criticised by the open-source software community, which suspected the tech could be used for vendor lock-in ? GNU father Richard Stallman called trusted computing "treacherous computing", but it looks like his worst fears have not come to pass.

  That doesn't mean TPMs haven't seen their share of dark days: back in 2017, it emerged that security chips made by Infineon contained a serious flaw, with experts estimating that 25 to 30 per cent of all TPMs used globally were open to attack.

- **What Is a Buffer Overflow [8]**

A buffer overflow vulnerability occurs when you give a program too much data. The excess data corrupts nearby space in memory and may alter other data. As a result, the program might report an error or behave differently. Such vulnerabilities are also called buffer overrun.

Some programming languages are more susceptible to buffer overflow issues, such as C and C++. This is because these are low-level languages that rely on the developer to allocate memory. Most common languages used on the web such as PHP, Java, JavaScript or Python, are much less prone to buffer overflow exploits because they manage memory allocation on behalf of the developer. However, they are not completely safe: some of them allow direct memory manipulation and they often use core functions that are written in C/C++.

- **Any iPhone can be hacked [9]**

Apple?s so called secure iPhones can be turned over by US coppers using a service promoted by an Israeli security contractor.

Cellebrite publicly announced a new version of its product known as a Universal Forensic Extraction Device or UFED, one that it's calling UFED Premium. In marketing that update, it says that the tool can now unlock any iOS device cops can lay their hands on, including those running iOS 12.3.

Cellebrite claims UFED Premium can extract files from many recent Android phones as well, including the Samsung Galaxy S9 but no-one ever called them secure and safe.

What is unusual is that Cellebrite is making broad claims about turning over Apple gear. This is not a cat-and-mouse claim where they exploit a tiny flaw which one day might be fixed. It would appear that Cellebrite has its paw on a real howler.

- **Cellebrite Claims It Can Unlock ?Any? iPhone And iPad, 1.4 Billion Apple Devices Hackable [10]**

Israel-based Cellebrite has announced a new version of its system Universal Forensic Extraction Device (UFED) ? UFED Premium ? which is capable of unlocking any iPhone, high-end Android device, or an iPad.

The forensics company has suggested that UFED Premium is meant to help the police in unlocking iPhones and Android smartphones and getting data from locked smartphones.

- **Web-based DNA sequencers getting compromised through old, unpatched flaw [11]**

DnaLIMS is developed by Colorado-based dnaTools. It provides software tools for processing and managing DNA sequencing requests.

These tools use browsers to access a UNIX-based web server on the local network, which is responsible for managing all aspects of DNA sequencing.

A simple Google search shows that dnaLIMS is used by a number of scientific, academic and medical institutions.

- **Generrate Cryptographically Secure RANDOM PASSWORD [12]**

- **DMARC, mailing list, yahoo and gmail [13]**

  Gmail was blocking one person?s email via our list (he sent that using Yahoo and from his iPhone client), and caused more than 1700 gmail users in our list in the nomail block unless they check for the mailman?s email and click to reenable their membership.

  I panicked for a couple of minutes and then started manually clicking on the mailman2 UI for each user to unblock them. However, that was too many clicks. Suddenly I remembered the suggestion from Saptak about using JavaScript to do this kind of work. Even though I tried to learn JavaScript 4 times and failed happily, I thought a bit searching on Duckduckgo and search/replace within example code can help me out.

- **Tired of #$%& passwords? Single Sign-on could be savior [14]**

  So how is single sign-on more secure, if Facebook is in charge? It's not, say security experts. "They?ve shown they can?t be trusted with our information," says Rudis.

- **Are SSO Buttons Like ?Sign-in With Apple? Better Than Passwords? [15]**

  Apple recently announced a new product that could prevent users from giving away their email ID to every other site on the internet. It?s expected to launch sometime later in 2019.

  Called ?Sign-in with Apple,? it is similar to other Single Sign-on services provided by Google and Facebook. The button lets you login to websites without creating a new user account every time.

- **App Makers Are Mixed on ?Sign In With Apple? [16]**

But other app makers have mixed feelings on what Apple has proposed. I spoke to a variety of developers who make apps for iOS and Android, one of whom asked to remain anonymous because they aren?t authorized to speak on behalf of their employer. Some are skeptical that Sign In with Apple will offer a solution dramatically different from what?s already available through Facebook or Google. Apple?s infamous opacity around new products means the app makers don?t have many answers yet as to how Apple?s sign in mechanism is going to impact their apps. And one app maker went as far as referring to Apple?s demand that its sign-in system be offered if any other sign-in systems are shown as ?petty.?

- **Chinese Cyberattack Hits Telegram, App Used by Hong Kong Protesters [17]**

  ?This case was not an exception,? he wrote.

  The Hong Kong police made their own move to limit digital communications. On Tuesday night, as demonstrators gathered near Hong Kong?s legislative building, the authorities arrested the administrator of a Telegram chat group with 20,000 members, even though he was at his home miles from the protest site.

- **Security News This Week: Telegram Says China Is Behind DDoS [18]**

  As protests erupted in the streets of Hong Kong this week, over a proposed law that would allow criminal suspects to be extradited to mainland China, the secure messaging app Telegram was hit with a massive DDoS attack. The company tweeted on Wednesday that it was under attack. Then the app?s founder and CEO Pavel Durov followed up and suggested the culprits were Chinese state actors. He tweeted that the IP addresses for the attackers were coming from China. ?Historically, all state actor-sized DDoS (200-400 Gb/s of junk) we experienced coincided in time with protests in Hong Kong (coordinated on @telegram). This case was not an exception,? he added. As Reuters notes, Telegram was DDoSed during protests in China in 2015, as well. Hong Kong does not face the strict [Internet] censorship that exists in mainland China, although activists have expressed concern about increased pressure from Beijing on the region.

- **Nextcloud signs public letter, opposing German plan to force decryption of chat [19]**

Security

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59

[2] https://www.bleepingcomputer.com/news/microsoft/microsoft-warns-about-worm-attacking-exim-servers-on-azure/
[3] https://www.wired.com/story/triton-hackers-scan-us-power-grid/
[4] https://www.cyberark.com/threat-research-blog/anatomy-triton-malware-attack/
[5] https://www.motherjones.com/politics/2019/06/a-researcher-found-a-bunch-of-north-carolina-voting-machine-passwords-online/
[6] https://www.theregister.co.uk/2019/06/17/worlds_tiniest_tpm_hopes_to_secure_all_the_things/
[7] https://www.youtube.com/watch?v=s7WDbnHlc1E
[8] https://www.acunetix.com/blog/web-security-zone/what-is-buffer-overflow/
[9] https://www.fudzilla.com/news/mobile/48887-any-iphone-can-be-hacked
[10] https://fossbytes.com/cellebrite-claims-it-can-unlock-any-iphone-and-ipad-1-4-billion-apple-devices-hackable/
[11] https://www.helpnetsecurity.com/2019/06/17/dnalims-vulnerability-exploitation/
[12] https://www.commandlinefu.com/commands/view/24555/generrate-cryptographically-secure-random-password
[13] https://kushaldas.in/posts/dmarc-mailing-list-yahoo-and-gmail.html
[14] https://eu.usatoday.com/story/tech/talkingtech/2019/06/15/google-says-tough-passwords-dont-matter-instant-sign-solution/1461379001/
[15] https://fossbytes.com/are-sso-buttons-like-sign-in-with-apple-better-than-passwords/
[16] https://www.wired.com/story/sign-in-with-apple-mixed-reactions/
[17] https://www.nytimes.com/2019/06/13/world/asia/hong-kong-telegram-protests.html
[18] https://www.wired.com/story/telegram-says-china-behind-ddos/
[19] https://nextcloud.com/blog/a-bad-idea-nextcloud-signs-public-letter-opposing-german-plan-to-force-decryption-of-chat/