Security Now! #656 - 03-27-18

TLS v1.3

This week on Security Now!

The mess with US voting machines, technology's inherent security vs convenience tradeoff, the evolving 2018 global threat landscape, welcome news on the bug bounty front from Netflix and Dropbox, we have the interesting results of Stack Overflow's 8th annual survey of 101,592 developers, worrisome news on the US government data overreach front, some useful and important new web browser features, messenger app troubles, a CRITICAL Drupal updated coming tomorrow, some welcome news for DNS security & privacy, a bit of miscellany and a look at the just-ratified TLS v1.3.

Our Picture of the Week

Security News

The US gets some election security coordination
https://www.cyberscoop.com/election-infrastructure-isac-dhs-cis/

The US Department of Homeand Security designated "Election Systems" as subsector of the country’s critical infrastructure early last year after the intelligence community broadly concluded that Russia had tried to interfere with the 2016 US presidential election.

"ISAC" is the abbreviation for "Information Sharing and Analysis Center" and a whole bunch of ISAC's already exist... and as of last week the US also has an "Elections Infrastructure ISAC."

https://www.nationalisacs.org/member-isacs

There are already many ISAC's. To give you a sense, the beginning of the list, which is in alphabetical order, reads: automotive, aviation, communications, defense industrial base, downstream natural gas, electricity, emergency management and response, financial services, healthcare, information technology... and that's just to the 'I's.

This feels like another level of bureaucracy whose effect will be very little change.

We've been discussing the problems with voting machines for years. We talked about how difficult it is turning out to be for the this summer's BlackHat and Defcon conferences to obtain secondhand machines. How their manufacturers are threatening resellers with legal action. This entire model -- of commercial manufacturers selling proprietary machines -- is all so broken and wrong.

Remote exploits, WiFi attacks, EvilMaid attacks...

How it should be...

The Intercept: "The NSA Worked to “Track Down” Bitcoin Users"
https://theintercept.com/2018/03/20/the-nsa-worked-to-track-down-bitcoin-users-snowden-documents-reveal/

NSA "XKeyScore" searching system / Projects "OAKSTAR" and "MONEYROCKET"

The use of an unnamed software utility whose purported purpose was to provide anonymity for Bitcoin transactions was actually subverted and used for surveillance.

No one should mistake the truth that the tradeoff for all of the many powerful conveniences of electronic communications and the Internet... is surveillance.

And this is not new. It has always been true. "Tapping someone's phone" or "Tracking their cellphone" have long been staples of fictional stories -- because they are very real.

You really cannot have it both ways. You can have convenience and "security opportunity"... but not an absolute security guarantee. If you want that meet naked, huddled under a thick blanket, in the middle of a football field, and whisper into the other person's hear. It's not as convenient as Skype... but the security assumptions are all completely transparent.

Symantec published their 2018 annual Internet Security Threat Report
https://www.symantec.com/security-center/threat-report

Symantec: "Cryptojacking Attacks Explode by 8,500 Percent"

(When the denominator is very small, even a modest numerator results in a large quotient.)

Stealthy miners steal resources and increase vulnerability.

As we know, the relatively sudden jump in the viability of crypto currency -- and in its real-world convertible valuation -- created a sudden demand for processing power. And as the difficulty of currency mining has climbed, to point where the electric power required to mine and cool typically exceeds the value of the mined coins, criminals have begun to steal other peoples' processing power.

To that end, Symantec logged 1.7 million cryptocurrency driven intrusions during the month of December 2017, alone.

1. End user browsers were the first target.
2. Higher-powered servers were next.
3. Symantec predicts that the next expected target-rich-environment will be the hundreds of millions of connected IoT devices...

At first blush this looks like the ultimate in distributed processing power. Individually they are low powered... but mining collectives mean that collectively, total IoT processing power can add up.

While this is true, the processing power in these devices is miniscule. Because cost is king for high volume consumer devices, these devices tend to have right-sized processors with little excess capacity. The argument has been made that they don't have the power to drive encrypted communications. While this may be an exaggeration, it remains to be proven that crypto mining can be profitably applied to lightbulbs, thermostats and door locks.

Even now, lower tech, targeted phishing remains the #1 way the majority of attacks begin.

And targeted attack groups are on the rise with the US being their biggest target.

Though lower tech, during 2017, 71% of attacks began with spear phishing.

So though the number of organizations subject to targeted attacks is low -- because they are aimed and not sprayed -- the risks posed to those attacked are quite high.

Whereas it's remarkable that those who penetrate security for cryptojacking or DDoSing typically never look into the networks they have managed to occupy, targeted attackers do nothing BUT look inside. These attackers are skilled, well-resourced, and capable of stealing valuable information or causing serious disruption over long periods of time.

Such efforts target an organization's critical infrastructure and often dwell inside for years.

Researchers who eventually discover their presence are often shocked to see how far back the evidence trail goes.

The motive for most is intelligence and information gathering, as they patiently scour networks while avoiding detection.

Another growing segment within the threat space are malware attacks within the software supply chain.

The possibility that the "software update supply chain" could be attacked to implant malware into an otherwise legitimate software package has always been a worry.

As we know, it's no longer the realm of worry and theory. During 2017 the number of incidents have doubled over previous years and malicious software updates have infiltrated even the most well-guarded networks.

The Ukrainian outbreak of "Petya" is a perfect example... where the compromise of legitimate accounting software was the malware's point of entry, allowing Petya to then spread laterally across corporate networks across the globe.

Symantec's statistics for the continuing surge in mobile malware is daunting with new mobile malware variants showing a 54% increase during 2017... and -- get this! -- Symantec's protection systems blocking an average of 24,000 malicious mobile applications EACH DAY last year.

(Note that these are not 24,000 unique pieces of malware, but 24,000 appearances.

As we know, keeping our constantly changing devices updated, and actively avoiding sketchy software and other offerings, is the best we can individually do. But in the case of Android, where the supply chain ecosystem is, by design, much less tightly controlled than iOS, only 20 percent -- 1 in 5 -- devices are running the latest major release of Android, and only 2.3 percent are up to date with the latest minor release.

Synamtec's analysis of the evolution of the ransomware world is interesting.

Their report states that during 2016 the profitability of ransomware led to a crowded market. But that during 2017 the market made a correction, reducing the average ransom to $522 and

signaling the commoditization of ransomware.
It's not gone by any means, and when it hits few things are less disruptive. But ransomware often suffered from trying to get too much money from those who didn't have it to give and/or could recover from attacks either by wiping and starting over or restoring their systems from backups.

Netflix launches a public bug bounty program
https://www.cyberscoop.com/netflix-bug-bounty-program/
https://threatpost.com/netflix-opens-public-bug-bounty-program-with-15k-payout-cap/130630/

Last week we were talking about the big (and time limited) Microsoft and Intel bug bounties for side-channel attack discoveries.

Last Wednesday Netflix announced that it would be expanding its own bug bounty program, opening it to any white hat hacker and increasing the top reward to $15,000.

Netflix's bug bounty program, which is managed by Bugcrowd, allows any registered hackers to scour Netflix mobile, cloud and software platform for minor and critical bugs valued between $100 to $15,000. The program includes the Netflix.com website as well as its Android and iOS mobile apps... in use by over 117 million Netflix users.

According to Bugcrowd, the typical Netflix bounty payout hs been $1,086.

And "Bugcrowd" will be worth keeping an eye on.
They describe themselves as "A Radical Cybersecurity Advantage: Managed Bug Bounties for the Enterprise."

In February, Bugcrowd took in a $26 million round of funding after expanding into offices in London and Sydney.

More than anything, the whole idea of Bug Bounties is worth thinking about. What does it mean?

And Dropbox:
And also, last Wednesday, Dropbox updated its vulnerability disclosure policy to clarify its relationship with cybersecurity researchers and also to offer a standard for the rest of the tech industry to hopefully follow.

Among other things, DropBox has pledged that they would not bring a DMCA claim against good faith participants in the bug bounty program.

- A clear statement that external security research is welcomed.

- A pledge to not initiate legal action for security research conducted pursuant to the policy, including good faith, accidental violations.

- A clear statement that we consider actions consistent with the policy as constituting "authorized" conduct under the Computer Fraud and Abuse Act (CFAA).

- A pledge that we won't bring a Digital Millennium Copyright Act (DCMA) action against a researcher for research consistent with the policy.

- A pledge that if a third party initiates legal action, Dropbox will make it clear when a researcher was acting in compliance with the policy (and therefore authorized by us).

- A specific note that we don't negotiate bounties under duress. (If you find something, tell us immediately with no conditions attached.)

- Specific instructions on what a researcher should do if they inadvertently encounter data not belonging to themselves.

- A request to give us reasonable time to fix an issue before making it public. We do not, and should not, reserve the right to take forever to fix a security issue.

101,592 Stack Overflow users participated in their 2018 "Developer Survey."
https://insights.stackoverflow.com/survey/2018/
What did they learn?

- At 69.8%, JavaScript has remained the most popular programming/scripting/markup language for the sixth year in a row.
- At 38.8% vs 34.4%, Python has surpassed C#, after surpassing PHP last year.
- And Python is the fastest growing language.

- At 49.6%, Node.js has remained the most popular framework.
- At 27.8% vs 27.2%, React has surpassed .NET Core to enter the top 3 frameworks.

- At 58.7%, MySQL remained the most popular database technology, a spot it has occupied since the first survey.
- At 19.7%, SQLite dropping from #3 to #5.

- At 78.9%, Rust ranked as the most loved programming language with "Kotlin" taking second place at 75.1% and Python in third with 68%.

- At 89.9%, Visual Basic 6 was voted as the most dreaded language... for its third year with that dubious honor.
- (Note... that places VB6 above COBOL in "dread" ranking.)

- For the second year in a row, developers chose Python as the language they most wanted to learn.

- Visual Studio Code and Visual Studio ranked 1st and 2nd as the most popular IDEs, though looking over the category, most are editors more than IDEs. (Notepad++, Sublime Text and Vim are 3rd, 4th, and 5th.)

- Android Studio was the most popular IDE among mobile developers, while Vim was the most popular among sysadmins and devops.

- As with years past, Windows remained the developers' primary operating system (followed by MacOS and Linux) and more than half of all developers use two monitors.

- And at 16%, the #1 ranking focus is Web development.

Bleeping Computer provided a great breakdown:
https://www.bleepingcomputer.com/news/technology/massive-stack-overflow-100k-user-survey-reveals-todays-hottest-technologies/

US Congress Passes CLOUD Act Hidden in Budget Spending Bill
Late last Thursday night the US congress passed a $1.3 trillion dollar spending bill to keep the US government funded through September.

The photo of the printed legislation is "impressive". I think I recall seeing that it was 2200 pages. It was about an 18 inch high stack sitting on a table next to our president as he announced the bill's successful passage.

However, arguably buried in that Omnibus legislation was the so-called "CLOUD act" where CLOUD stands for Clarifying Lawful Overseas Use of Data. Given that this new legislation was proposed six weeks earlier as a means for dealing with Microsoft's refusal five years ago to turn over US citizen's data residing in Ireland... you can guess what that "clarification" amount to... even if you didn't know that the EFF was glowing a gasket over then-the proposed legislation... which is now the law of the land.

As BleepingComputer put it:
The unaltered and now official CLOUD Act effectively eliminates the need for search warrants and probable cause for obtaining a US citizen's data stored online. US law enforcement only need to point to some account and tech companies must abide and provide all the needed details, regardless if the data is stored in the US or overseas.

Further, the bill recognizes foreign law enforcement and allows the US President to sign data-sharing agreements with other countries without congressional oversight. The CLOUD Act will then allow foreign law enforcement to require data on their own citizens stored in the US, also without obtaining a warrant or proving probable cause.

The EFF notes that: "Since there is no more need for a foreign law enforcement agency to obtain US warrants or prove probable cause, this opens the door wide open to political abuses."

The EFF's page makes their feelings clear. It's titled: "A New Backdoor Around the Fourth Amendment: The CLOUD Act" where they explain how this is a backdoor circumvention of the US Constitution's protection against illegal search and seizure.

So... we now have official, warrantless, cross-border data sharing.
Many years ago we coined the term TNO for "Trust No One" ...

https://www.bleepingcomputer.com/news/government/us-congress-passes-cloud-act-hidden-in-budget-spending-bill/
https://www.eff.org/deeplinks/2018/03/new-backdoor-around-fourth-amendment-cloud-act
https://threatpost.com/senate-gives-nod-to-controversial-cross-border-data-access-bill/130757/

Firefox to join Chrome and Opera with a built-in Ad Filtering System
https://www.bleepingcomputer.com/news/security/firefox-to-get-an-ad-filtering-system/
https://wiki.mozilla.org/Firefox/Roadmap

Slated for the 3rd quarter of 2018, Firefox's Roadmap Wiki has announced that an "abusive ad blocker" will be appearing and, as with Chrome, plans are that it will be enabled by default.

Those of us using uBlock Origin already have a lot of this protection, and I'm always amazed and chagrinned when I use any browser that has zero content filtering. So it will be nice to have Firefox keeping pace.

And for Firefox enthusiasts, allow me to recommend a peek at the Mozilla Roadmap.

Protecting against the growing use of Punycode Homograph (Unicode) Attacks
https://www.bleepingcomputer.com/news/security/chrome-extension-detects-url-homograph-unicode-attacks/

Bleeping Computer picked up on a highly useful extension for Chrome that really should, like abusive ad blockers, become built into every one of our browsers: A "Homograph Domain" name detector. It stops users in their tracks with a big red warning window.

Edge displays the simple ASCII-based representation of UNICODE, known as Punycode.

Chrome displays the ASCII in the titlebar but the UNICODE in the URL address bar.

Firefox DOES show dangerous unicode by default but it can be tweaked using about:config.
IDN_show_punycode (search for 'puny') Make it TRUE (dark)

"Phish.AI IDN Protect" -- Chrome store and Github
https://chrome.google.com/webstore/detail/phishai-idn-protect/mikecfgnmakjomepfcghpbhfamjbjhid
https://github.com/phishai/idn-protect-chrome

Facebook Collected Your Android Call History and SMS Data For Years
https://thehackernews.com/2018/03/facebook-android-data.html

Without permission, Facebook's Messenger App was surreptitiously collecting and uploading not only all of its users' contact information, but also a complete call and text message history.

Earlier versions of Android allowed this to occur, and Facebook took advantage of that undisclosed capability.

Facebook claims that it never did this without permission, but many users whose data was collected are very security and privacy aware and are quite certain they were careful to never provide such permission.

Facebook claims that they never sell such data... bud regardless of that controversy, we know that they can be subpoenaed for whatever they have. So if they have more than they should, everyone loses.

Meanwhile: Telegram Ordered to Hand Over Encryption Keys to Russian Authorities
https://threatpost.com/telegram-ordered-to-hand-over-encryption-keys-to-russian-authorities/130581/

Last Tuesday, one week ago, the top court in Russia ruled that the Telegram -- who is currently providing encrypted messaging services to 9.5 million active Russian users -- has 15 days to hand over the app's encryption keys to Russian authorities so that those authorities may decrypt Telegram users' messages.

Turning over the keys would put Telegram in compliance with an anti-terrorism rule, signed into a 2018 law, that requires messaging services to provide authorities a means to decrypt a user's correspondence.

In reply, Pavel Durov, Telegram's founder, told Bloomberg news that his company plans to appeal the ruling, which could drag the process out deep into the summer months.

On the day of the ruling, Pavel tweeted: "Threats to block Telegram unless it gives up private data of its users won't bear fruit. Telegram will stand for freedom and privacy." — Pavel Durov (@durov) March 20, 2018

Russia's Federal Security Service (FSB) argues that possessing the encryption keys is not a violation of a user's privacy. It's only under court order that those keys can be used to access encrypted content.

If Telegram doesn't comply, the app could eventually be blocked in Russia just as China blocked Telegram in 2015.

Mediascope estimates that Telegram has 9.5 million users located in Russia and 100 million users globally.

Drupal provides one week notice of a ‘Highly Critical’ Bug to be patched TOMORROW
Drupal 7 and 8 core highly critical release on March 28th, 2018 PSA-2018-001
https://www.drupal.org/psa-2018-001

Description

There will be a security release of Drupal 7.x, 8.3.x, 8.4.x, and 8.5.x on March 28th 2018 between 18:00 - 19:30 UTC, one week from the publication of this document, that will fix a highly critical security vulnerability. The Drupal Security Team urges you to reserve time for core updates at that time because exploits might be developed within hours or days. Security release announcements will appear on the Drupal.org security advisory page.

While Drupal 8.3.x and 8.4.x are no longer supported and we don't normally provide security releases for unsupported minor releases, given the potential severity of this issue, we are providing 8.3.x and 8.4.x releases that include the fix for sites which have not yet had a chance to update to 8.5.0. The Drupal security team strongly recommends the following:

- Sites on 8.3.x should immediately update to the 8.3.x release that will be provided in the advisory, and then plan to update to the latest 8.5.x security release in the next month.

- Sites on 8.4.x should immediately update to the 8.4.x release that will be provided in the advisory, and then plan to update to the latest 8.5.x security release in the next month.

- Sites on 7.x or 8.5.x can immediately update when the advisory is released using the normal procedure.

The security advisory will list the appropriate version numbers for all three Drupal 8 branches. Your site's update report page will recommend the 8.5.x release even if you are on 8.3.x or 8.4.x, but temporarily updating to the provided backport for your site's current version will ensure you can update quickly without the possible side effects of a minor version update.

This will not require a database update

The Security Team or any other party is not able to release any more information about this vulnerability until the announcement is made. The announcement will be made public at https://www.drupal.org/security, over Twitter, and in email for those who have subscribed to our email list.

Mozilla & Cloudflare team up to test a trusted DNS solution
Trusted Recursive Resolver via DNS over HTTPS: "DoH"

The proposal is moving through the IETF draft process and is expected for a ratification vote later this year.

DNS is considered to be one of the least secure and private remain aspects of the Internet and we were just talking last week about how even some VPNs fail to tunnel the system's local DNS queries... thus leaking them to the user's local network, provider and ISP.

Matthew Prince, the co-founder and CEO of Cloudflare in an interview with Threatpost said: "DNS is a 45-year-old protocol. It was never built to have encryption in it or be secure. Yet, DNS acts as the internet’s vital directory and is vulnerable to many different types of abuses. This is a privacy nightmare. This is a security nightmare. And, this is a performance nightmare, and yet it’s the foundation on the internet.

Another way to look at this is that we have just about managed to pervasively wrap our web browser traffic in HTTPS authentication and encryption to shield it from prying eyes... but NOTHING has yet been done to similarly protect most system's VERY REVEALING domain name to IP lookups. Nothing.

"DoH" establishes a static and persistent tunnel to a high-speed provider with a geographically nearby point of presence, through which DNS queries and replies are exchanged without any intermediary being able to see any of that traffic. It's very much like an entirely transparent VPN for DNS.

Cloudflare maintains that using a DNS resolver via an HTTPS request is more efficient then traditional DNS over UDP and can shave up to 15 milliseconds from the time it takes to make DNS queries to render a webpage. And Matthew Prince suggested that even more time can be shaved when Cloudflare acts as the authoritative DNS hosting service. That makes sense since then Cloudflare would not need to ask anyone else.

Google is also working in this direction. They already support DNS-over-HTTPS with an API offered by their Google Public DNS service.

Firefox's initial DoH functionality will appear in FF v60. Firefox uses the term "Trusted Recursive Resolver (TRR)", so using "about:config" and searching "trr" will pull up the configuration settings.

Ghacks page has thorough documentation of the settings:
https://www.ghacks.net/2018/03/20/firefox-dns-over-https-and-a-worrying-shield-study/

Miscellany

Sci-Fi --> Star Trek: Discovery on CBS All Access (which really means "paid access")
(But 7-day week free trial.) And this is NOT Jean Luc's Prime-Directive-Driven universe. It is set ten years before the universe of Kirk and Spock and the captain is a bit of a "just get the job done" renegade.

"Disk Cleanup" / "Clean up system files"
DO NOT DO THIS if you'll need your computer soon

TLS v1.3

Technical Summary

This document specifies version 1.3 of the Transport Layer Security (TLS) protocol. TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery.

Document Quality

There are over 10 interoperable implementations of the protocol from different sources written in different languages. The major web browser vendors and TLS libraries vendors have draft implementations or have indicated they will support the protocol in the future. In addition to having extensive review in the TLS working group, the protocol has received unprecedented security review by the academic community. Several TRON (TLS Ready or Not) conferences were held with academic community to give them a chance to present their findings for TLS. This has resulted in improvements to the protocol. There was also much consideration and discussion around any contentious points, resolved through polls and working group last calls.

Please note that ID-nits complains about the obsoleted/updated RFCs not being listed in the abstract. This is intentional because the abstract is now a concise and comprehensive overview and is free form citations, as per RFC7322.

TLS 1.3 bring us improved cryptography:

TLS 1.3 completely drops support for earlier and formally obsolete hashing algorithms (such as MD5) and adds support for newer and much stronger alternatives such as ChaCha20, Poly1305, Ed25519, x25519, and x448.

TLS 1.3 supports quicker initial handshake connection negotiation between the client and the server... so HTTPS over TLS v1.3 will no longer be slower than HTTP for that reason.

TLS 1.3 supports new features to reduce the time needed to establish encryption handshakes with hosts to which the client has recently connected.

TLS 1.3 brings strong protection against downgrade attacks which, if not prevented, could allow an attacker to trick a server into using an older and less secure version of the protocol.

And despite the efforts by the financial business sector to make TLS v1.3's Perfect Forward Secrecy feature optional, it was adopted and approved as-is, without any weakening, unanimously by all the IETF members.

Browsers like Chrome, Edge, Firefox, and Pale Moon have already rolled out support for earlier versions of the TLS 1.3 draft, and will be updating their support to the final and now official standard.

SSL 2.0	1995	
SSL 3.0	1996	(+1)
TLS 1.0	1999	(+3)
TLS 1.1	2006	(+7)
TLS 1.2	2008	(+2)
TLS 1.3	2018	(+10)

~30~