Security Now! #658 - 04-10-18

Deprecating TLS 1.0 & 1.1

This week on Security Now!

This week we discuss Intel's big Spectre microcode announcement, Telegram is not long for Russia, the US law enforcement's continuing push for "lawful decryption", more state-level net neutrality news, Win10's replacement for "Disk Cleanup", a bug bounty policy update, some follow-up to last week's Quad-1 DNS conversation, why clocks had been running slow throughout Europe... then a look at the deprecation of earlier version of TLS and a big Cisco mistake.

Security News

Intel gives up on updating some chip microcode firmware for Spectre
The April 2nd, 2018 update of Intel's "Microcode Revision Guidance" states:

Intel's chart by CPUID has previously listed their various chips' status under the headings of Pre-Beta, Beta, Production Candidate and Production.

This latest update added the new "Stopped" status with the following explanation:

• Stopped – After a comprehensive investigation of the microarchitectures and microcode capabilities for these products, Intel has determined to not release microcode updates for these products for one or more reasons including, but not limited to the following:

- Micro-architectural characteristics that preclude a practical implementation of features mitigating Variant 2 (CVE-2017-5715)
- Limited Commercially Available System Software support
- Based on customer inputs, most of these products are implemented as “closed systems” and therefore are expected to have a lower likelihood of exposure to these vulnerabilities.

This is disappointing, but not a big surprise.

https://newsroom.intel.com/wp-content/uploads/sites/11/2018/04/microcode-update-guidance.pdf

InSpectre will be updated with this information to notify its users whether firmware has been made available for their CPU so there's hope... or whether it will never happen.

Russia takes the next step toward shuttering Telegram throughout Russia
Telegram inches further out of the Russian market
Four days ago, Russia's telecommunications watchdog filed today a lawsuit against Telegram (the very popular encrypted instant messaging app), asking a Moscow court to rule in favor of restricting access to the service inside Russia's borders.

Previously, the FSB, Russia's main intelligence service, had requested access to Telegram's encryption keys so it could access encrypted messages sent through the app.

Telegram, of course, refused to help. So the FSB filed a lawsuit to compel access to these encryption keys claiming their need for access for national security and the agency's fight against terrorism.

So far, every court ruling has been in favor of the Russian state, and the final decision came last month when Russia’s Supreme Court ruled that Telegram =must= hand over users' encryption keys to FSB agents without a court order, whenever agents came calling.

Also, of course, Telegram responded through its lawyers that it had no such plans. And, in a probably vain attempt to fight back, Telegram filed a lawsuit against the Russian government at the European Court of Human Rights (ECHR).

So the lawsuit filed four days ago is the next and final step necessary to have a communications service banned within Russia. If the Moscow court rules favorably for the communications watchdog -- as it surely will -- Telegram's Internet domains will be added to Russia's official national blocklist... which all Telcos and ISPs are required to abide, which will, in turn, shutdown Telegram throughout Russia.

Russia is thus expected to shortly be joining China is censoring the use of Telegram's encrypted and secure messaging product.

The Senate gets set to take another run at "Mandatory Lawful Decryption" of communications.
And speaking of state blowback against encryption...
Another effort in the US Congress is being pushed by a combination of the Justice Department and leaders of the Senate Judiciary Committee: Senate Judiciary Chairman Chuck Grassley and the ranking member Dianne Feinstein. At Justice, Deputy Attorney General Rod Rosenstein has become one of the leading voices regarding a legislative solution.

Recall that in the wake of the 2016 San Bernardino terrorist attack and Farook's work iPhone which could not be readily decrypted, Feinstein was pushing hard for encryption legislation with the "Compliance with Court Orders Act of 2016" which she had helped to draft along with Chairman Richard Burr. But that legislation was never put to a vote it was never introduced for a vote and the draft proposal was roundly criticized for seeking to mandate “backdoors” in popular consumer products.

The bottom line is that law enforcement and legislators are unlikely to ever give up on this issue. The fact that surveillance has never been more available and ubiquitous is lost on those who will not be satisfied to just have more. They clearly want to remove every barrier and for the US government to force full access to everything.

And while we're on the topic of legislation… **The State of Oregon has joined Washington State in passing its own Net Neutrality legislation.**
Yesterday, Oregon's governor Kate Brown today signed their own net neutrality bill into law, making Oregon the second state to pass a net neutrality law since the Federal Communications Commission voted to repeal nationwide rules.

The new law was written carefully and narrowly in an attempt to survive lawsuits from ISPs. As such, rather than imposing prohibitions on Internet providers, the law simply forbids state agencies from purchasing fixed or mobile Internet service from ISPs that violate the core net neutrality principles as were laid out in the soon-to-be-repealed FCC rules.

ISPs that sell Internet service to Oregon state agencies will be required to publicly disclose whether they in any way filter, block or throttle otherwise lawful Internet traffic or engage in any form of paid prioritization, notwithstanding reasonable non-commercial biased network management/

Washington state was first to pass a net neutrality law, and Washington's went further than Oregon's by imposing the rules upon ISPs, regardless of whether they sell Internet service to state agencies.

And, as we have noted here previously, beyond Washington and Oregon, the governors of five other states -- Vermont, Hawaii, Montana, New Jersey, and New York -- have all issued executive orders to impose net neutrality rules upon ISPs that provide Internet service to state government agencies.

Oregon's new law, which takes effect on January 1st, 2019, <quote> "mandates that public bodies in Oregon only contract with Internet service providers that operate under net neutrality, which requires Internet service providers to enable equal access for all Web traffic, regardless of the source." The legislation will apply to new broadband service contracts or renewals entered into on or after that date.

However, I was disappointed to see one glaring caveat in the law: The legislation acknowledges the possibility that even state agencies might be forced to choose an ISP that violates net neutrality when and if here are no other options. In other words, the purchasing requirements will =not= apply when an ISP is <quote> "the sole provider of fixed broadband Internet access service to the geographic location subject to the contract."

<<grumble>>

Still... whereas it feels as though we are destined to lose the "absolute encryption" battle with the federal government, the feeling is different with Net Neutrality. This one I think we're destined to win.

Windows 10's "Free Up Space Now" Ushers In a New Era for Disk Cleanup

BleepingComputer's founder Larry Abrams posted a mention of a forthcoming feature of the so-called Windows 10 Spring Creator's Update which he expects will cause him to stop recommending Windows "Disk Cleanup" in favor of the new "Free up space now" (not quite as catchy but I suppose it's more descriptive). Since I was recently recommending "Disk Cleanup" I wanted to pass along Larry's observation...

https://www.bleepingcomputer.com/news/microsoft/windows-10-s-free-up-space-now-ushers-in-a-new-era-for-disk-cleanup/

Apparently "Disk Cleanup" will not be going away, but "Free up space now" -- which Windows 10 users will be able to find by searching for "storage" -- will do everything Disk Cleanup now does, but more easily, more completely, and more thoroughly.

Bug Bounties may create a market distortion (But *I* have a bigger worry.)
https://www.cyberscoop.com/bug-bounty-marketplace-katie-moussouris-microsoft/

The "Cyberscoop" site had an interesting perspective on the bug bounty market which tempers my own recent bullishness about it, so I wanted to share it for some perspective. Last Wednesday's article title was "The bug bounty market has some flaws of its own" and it gets its inspiration and position from Katie Moussouris (Moo-sir-is) who founded Microsoft's bug bounty program, was then the Chief Policy Officer at HackerOne, and is now the founder of Luta Security.

Today is the first day of the 3-day CyberUK 2018 conference hosted by the UK's national Cyber Security Centre which is a part of GCHQ... and Katie is there presenting and tweeting up a storm.

Katie's website homepage banner says announces "#1 Solutions Architects for Vulnerability Disclosure or Bug Bounty Programs" and her homepage currently announces: "The UK government announced at the CyberUK Conference that its new National Cyber Security Centre (NCSC) is partnering with Luta Security, Inc. to invite a select group of security practitioners in the community to participate in the historic first UK government pilot for vulnerability coordination."

And the bottom of the homepage reads: "Bounty Smarter, Not Harder."

This morning, during the #CYERUK18 conference, Katie tweeted:

Watching Gav Thomas who leads Microsoft Security Response in the UK speak about vulnerability discovery & mitigations at @CYBERUKevents #CYBERUK18

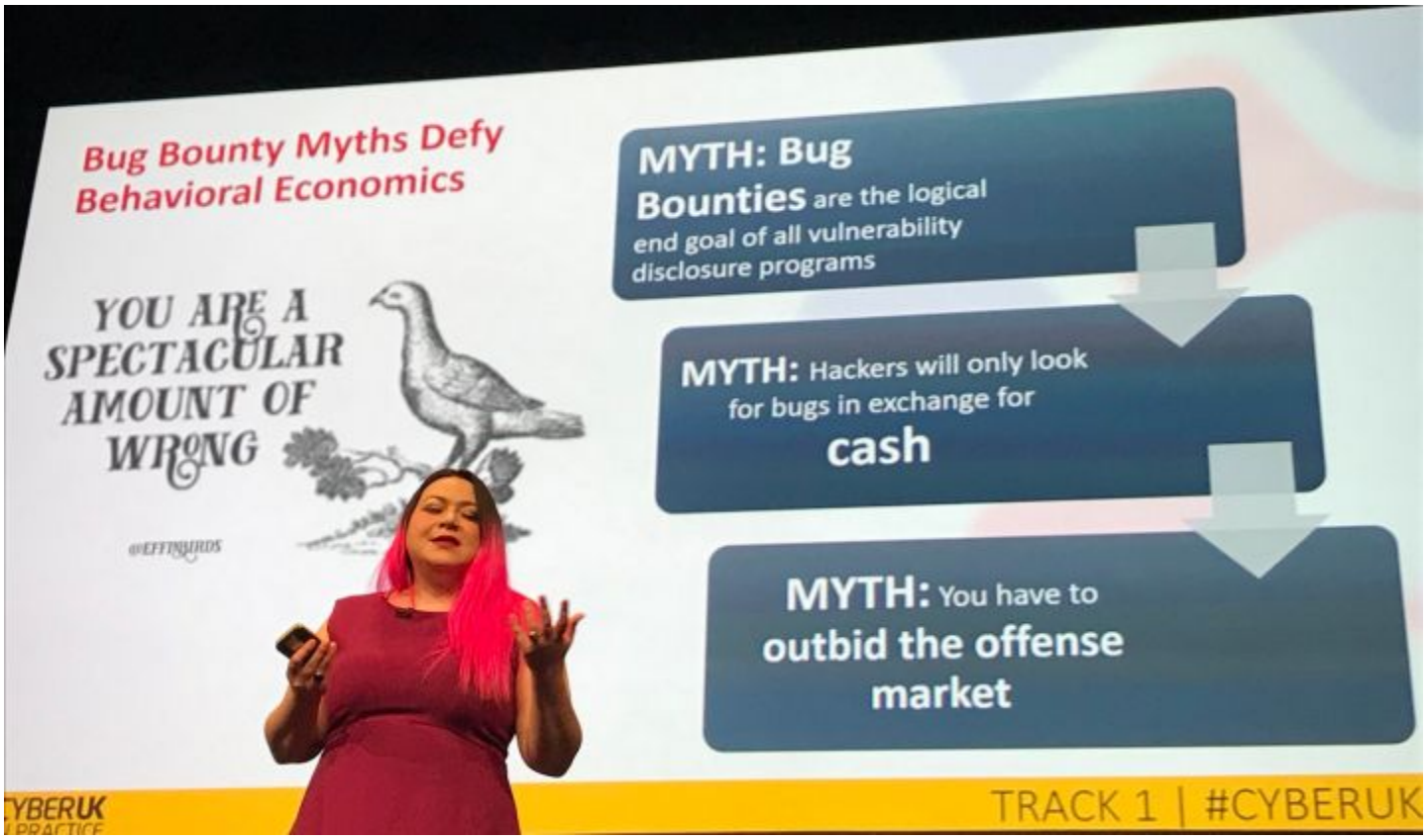
Evolution of the Microsoft bug bounties! Can you believe that a decade ago, Microsoft said they'd never pay for vulnerability research? Launching the first Microsoft bug bounties nearly 5 years ago, it's been interesting to watch the evolution in MS & the ecosystem. #CYBERUK18

Deep root cause analysis leads to the elimination of classes of vulnerabilities, mitigations added make exploitation harder, even when number of cases goes up. #maturity #CYBERUK18

Also this morning, Facebook's Sheryl Sandberg posted:
“Mark is in D.C. to testify before the U.S. Congress today and tomorrow. [And, yes… he did, indeed, dress up in a coat and tie.] This is an important opportunity to speak with policy makers about the steps we’re taking to protect people who use our services.”

“Today we’re announcing another important step - a bounty program that gives people money for information that helps us take action against bad actors. We’re looking for cases where people or groups have collected data using an app connected to Facebook and then sold or transferred that data to another company where it can potentially be abused. This type of behavior is unacceptable and violates our policies. Because it’s a new program, it will change as people use it and give us feedback. You can learn more about it here: https://facebook.com/data-abuse”

Sheryl's posting was picked up and tweeted by Facebook Security at 7:13am this morning, and Katie retweeted that tweet, adding… Following the abuse of data, enforcing terms of service for third party apps, creating a bounty for whistleblowers who have firsthand knowledge of data abuse are all a positive evolution in the social media privacy space. Bounties are incentives for both information & behavior.



The gist of Katie's position is that companies can be acting foolishly by simply throwing massive bounties at the problem and that offering to pay for bugs risks and should not be used as a substitute for putting well-managed systems in place to prevent those bugs from ever shipping in the first place.

Katie has previously tweeted: “If you can make considerably more money hunting bugs, there will be nobody left to fix them. Those who do the hard work of code maintenance in corporations, dealing with [office] politics for a salary that’s ~1 bounty are 1 bad meeting away from rage-quitting to hunt bugs full time.”

In an interview with CyberScoop Katie said: [Bug bounty seeking] “Motivations vary among hackers … but most are driven by some combination of three factors: Financial compensation, peer recognition and “the pursuit of intellectual happiness — loving what you do.”

In the book "New Solutions for Cybersecurity" recently published by MIT Press, to which Katie contributed, an analysis of the trade in software flaws revealed that the defensive bug bounty market is highly stratified, with a small number of extremely skilled individuals bringing home the lion’s share of rewards. In the datasets they analyzed, the authors found “a small number of key sellers are finding the overwhelming majority of all bugs.”

In one dataset provided by bounty program managers HackerOne, for example, just 5 percent of hunters found 23 percent of flaws — and there were similar numbers in datasets from bounty programs run by Facebook and others.

Okay... so perhaps don't give up your day job. It's going to take hours of pouring through disassembled code or writing your own custom fuzzing pentesting code to find and track down flaws. But if you have the time and enjoy the work, it COULD pay off.

But... while thinking about the market dynamics created by such incentives a *very* worrisome possibility occurred to me:

We have the givens that:

- It is extremely difficult to create flawless code.
- It is extremely difficult to find flaws by inspection. They are inherently difficult to see.

And "backdoors" is the term we use for deliberately inserted loopholes in a system's security. But as we have previously seen, not all backdoors take the form of a retrospectively obvious hard-coded password in the firmware. There can also be very cleverly disguised "Greydoors" occupying a grey area -- as we saw with, for example the DualEC DRBG which =may= have been a deliberate design flaw designed and implanted into it by the NSA, who then paid RSA a large sum to make that slowest source of entropy their library's default.

The suspicion is that the NSA may have had a state-sponsor-level interest in the injection of a carefully weakened algorithm into the mainstream.

But, offering an award of a quarter of a million dollars to the discoverer of a critical flaw in a mainstream commercial system... can also create a POWERFUL incentive for such a flaw to first be deliberately implanted by a confederate accomplice who has code-writing access.

It is so extremely difficult to create flawless code that no one expects it any longer. This tends to remove suspicion... which, in turn, means that it is absolutely possible for a very subtle yet still critical flaw to be DELIBERATELY added to existing code in such a fashion that it cannot be seen by inspection, cannot be found casually, and for which a compelling subsequent "discovery miracle story" can subsequently be fabricated... with a substantial award at the other end.

In the past we have posited the possibility that intelligence agencies might have planted agents deep into software organizations for just this purpose. And while that's always a possibility, the pressure to run cryptojacking "malmining" shows that cash remains king... and $250,000 is a lot of incentive to dangle, especially when no one expects perfect code any longer.

And note, also, that if nefarious purchasers are also in the game, unscrupulous developers might be induced to plant such flaws into code for eventual sale to someone other than their employer.

Follow-up: Secure DNS, Cloudflare, Quad9, GoogleDNS...
GRC's DNS Benchmark =was= updated to add 1.1.1.1, 1.0.0.1, 9.9.9.9.

Most people confirmed that 1.1.1.1 was fast, but my experience with 1.0.0.1 being a lot slower was =not= generally found by others... and in several cases it beat out 1.1.1.1.

A bunch of people jumped up and down, annoyed that I had barely mentioned the Quad 9 (9.9.9.9) service that I had previously been excited about. But what can I say? I'm fickle!

Cloudflare, Google, Quad9 all support DNS over TLS on port 853 and are compliant with RFC7858.

The "wire format" of DNS over TLS is identical to DNS over TCP which was defined in RFC1035 way back in November of 1987.

DNS over HTTPS is different since it uses the HTTP web semantics of GET and POST.
Cloudflare supports DNS over TLS on 1.1.1.1 and 1.0.0.1 on port 853.
The certificate presented is for cloudflare-dns.com.
Cloudflare has open source DoH clients for Linux, macOS and Windows 32 and 64 bit.
https://developers.cloudflare.com/1.1.1.1/dns-over-https/cloudflared-proxy/
This establishes a virtual DNS server on the local system's localhost port.

It is this DoH variant that the next release of Mozilla will be experimentally supporting in Firefox 60. Firefox 60 is the current Nightly version of Firefox, and will ship on May 8, 2018.

DNS over TLS with pfSense
https://www.netgate.com/blog/dns-over-tls-with-pfsense.html
Last Tuesday / April 03, 2018 / by Ivor Kreso

Cloudflare's new DNS service has a lot of industry attention, so we wanted to offer a quick guide that covers setting up your DNS servers in pfSense, including configuring DNS over TLS. In addition to Cloudflare DNS servers, the following guide also applies to Quad9 DNS service.

Thanks to Unbound, the built-in DNS resolver, which has been enabled by default since pfSense version 2.3, makes configuring DNS over TLS a very simple task with pfSense.

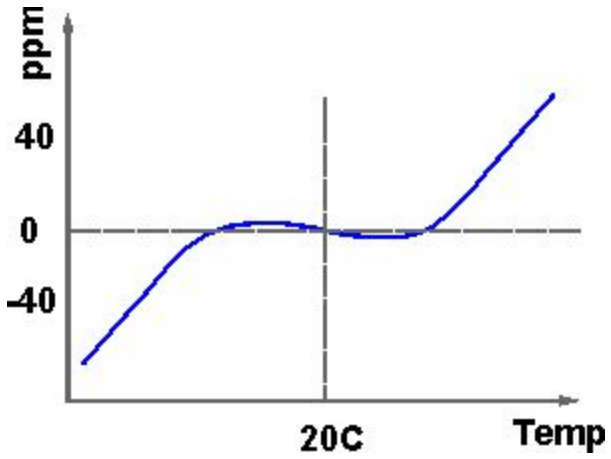
Miscellany

The European power grid is back on time...
https://arstechnica.com/tech-policy/2018/04/european-grid-dispute-resolved-lost-6-minutes-returned-to-oven-clocks/

This week, Europe's electric transmission lobby announced that oven, microwave, and alarm clocks across the continent were no longer six minutes behind. WHAT??!!??!!

How did they get back the lost time? By resolving a grid dispute between Serbia and Kosovo and running the continental grid at a slightly higher frequency than normal.

- Quartz crystal's, temperature compensation.
- AC, unlike DC, by its very nature provides a time reference. Zero crossings.
- 60hz, 50hz.



Between mid-January and early March of this year, a grid dispute between Serbia and Kosovo resulted in 113 Gigawatt Hours of unmet demand from Kosovo. Since Kosovo is part of the Continental Europe Power System, the unmet demand on the 25-country system pulled more power than was available, resulting in a grid-wide slow down of the spinning generators which were unable to keep up with the demand.

This, in turn, led to a system-wide decline in frequency to an average frequency of 49.996Hz.

And THIS, in turn, caused AC time-based clocks which were dutifully counting the zero crossings and dividing by 50 to get "seconds" were counting those passing seconds too slowly... as a consequence, over the span of three months, clocks throughout all of Continental Europe lost six minutes!

So... last month, the European Network of Transmission System Operators (ENTSO-E) publicly admonished Serbia and Kosovo for not properly balancing their grids according to previous agreements. The group wrote: "This average frequency deviation, that has never happened in

any similar way in the CE [Continental Europe] Power system, must cease. ENTSO-E is urging European and national governments and policymakers to take swift action."

Two days later, on March 8, the Transmission System Operators (TSOs) from Serbia and Kosovo confirmed that they were back to balancing their grids appropriately.

And finally, last week, ENTSO-E announced that it had restored the lost six minutes to clocks around the continent by maintaining a slightly higher than normal average frequency of 50.01Hz for a month. The missing energy was put back into the system with the collective help of the 25 member countries, which "carried out a compensation programme to restore the situation to normal."

"One of the effects is notably that the digital clocks geared by electric frequency are now back on time," ENTSO-E wrote. That is, as long as you oven-clock owners within the Continental Europe Power System didn't change your slow clocks to the correct time a month ago. If you did, now you could be six minutes fast. But at least you're less likely to be late now.

Thanks to ArsTechnica for their reporting of this wonderfully whacky story.

SpinRite

J.D. Green (@Cybts1) / 4/9/18, 10:07 AM

@SGgrc Hi Steve, love hearing you on @SecurityNow each week. On last show you spoke about an email about spin-rite, I was wondering if spin-rite works on thumb drives. I have one that seems to be corrupted and I would like to recover it's contents. Thanks for all you work.

Deprecating TLS 1.0 & 1.1

https://www.digicert.com/blog/depreciating-tls-1-0-and-1-1/

I loved this line from DigiCert's blog: "... But on the internet there’s a big difference between nearly dead and dead."

As we know, we now finally have TLS v1.3 and TLS v1.2 support is now quite solid. Yet, of the 150,000 HTTPS-enabled sites monitored by SSL Pulse, 88% support TLS 1.0 and 85% support TLS 1.1.

https://www.ssllabs.com/ssl-pulse/

Most of the internet is using TLS 1.2 which is now the only version of the protocol recommended by cryptographers and considered to be “modern.”

But a small portion of users may not be ready for the switch due to outdated software. Despite being released in 2008, TLS 1.2 support was absent from some major platforms and browsers

for some time. Internet Explorer did not support TLS 1.2 until five years later with 2013's release of version 11; and Android versions prior to 5.0 (released 2014) only supported TLS 1.0, which represents nearly 18% of Android devices still in use today.

Cloudflare, which, as one of the world's largest CDNs, has good visibility into things happening at internet-scale. They recently shared about 11% of traffic on their network uses TLS 1.0 (with only a tiny portion (0.38%) using TLS 1.1) -- and the reset presumably already having jumped to v1.2.

But still... 11% being TLS v1.0? But most of that might be older appliances and NOT humans clicking links in web browsers.

A major change that is finally spurring the deprecation of TLS 1.0 is an upcoming deadline in the PCI (Payment Card Industry) standards. These standards cover security practices related to handling credit cards and apply to many businesses. Starting June 30, 2018, websites will need to stop supporting TLS 1.0 to remain PCI compliant.

The most websites already support TLS 1.2 and only antique web browsers don't, Internet user won't notice any effect from this.

This deprecation will primarily affect non-browser software, APIs, and other internet infrastructure.

Older versions of development tools which don't support TLS 1.2, such as curl, are still widely in use—either directly by developers or as dependencies bundled into other software. Github was one of the first major services to turn off TLS 1.0 and 1.1. They made the change in February, which revealed a number of breakages in developer tools.

Many major websites and services have announced that they are also ending support later this year:

- DigiCert disabled support for TLS 1.0 and 1.1 for all of their services, including their website and API, on April 1st.
- KeyCDN will end support for TLS 1.0 and 1.1 on March 30th, as will Cloud.gov.
- Fastly will stop supporting TLS 1.0 and 1.1 on May 8th.
- Cloudflare will disable TLS 1.0 and 1.1 support for their API on June 4th.
- Microsoft's Office 365 will support only TLS 1.2 starting October 31st.

~30~