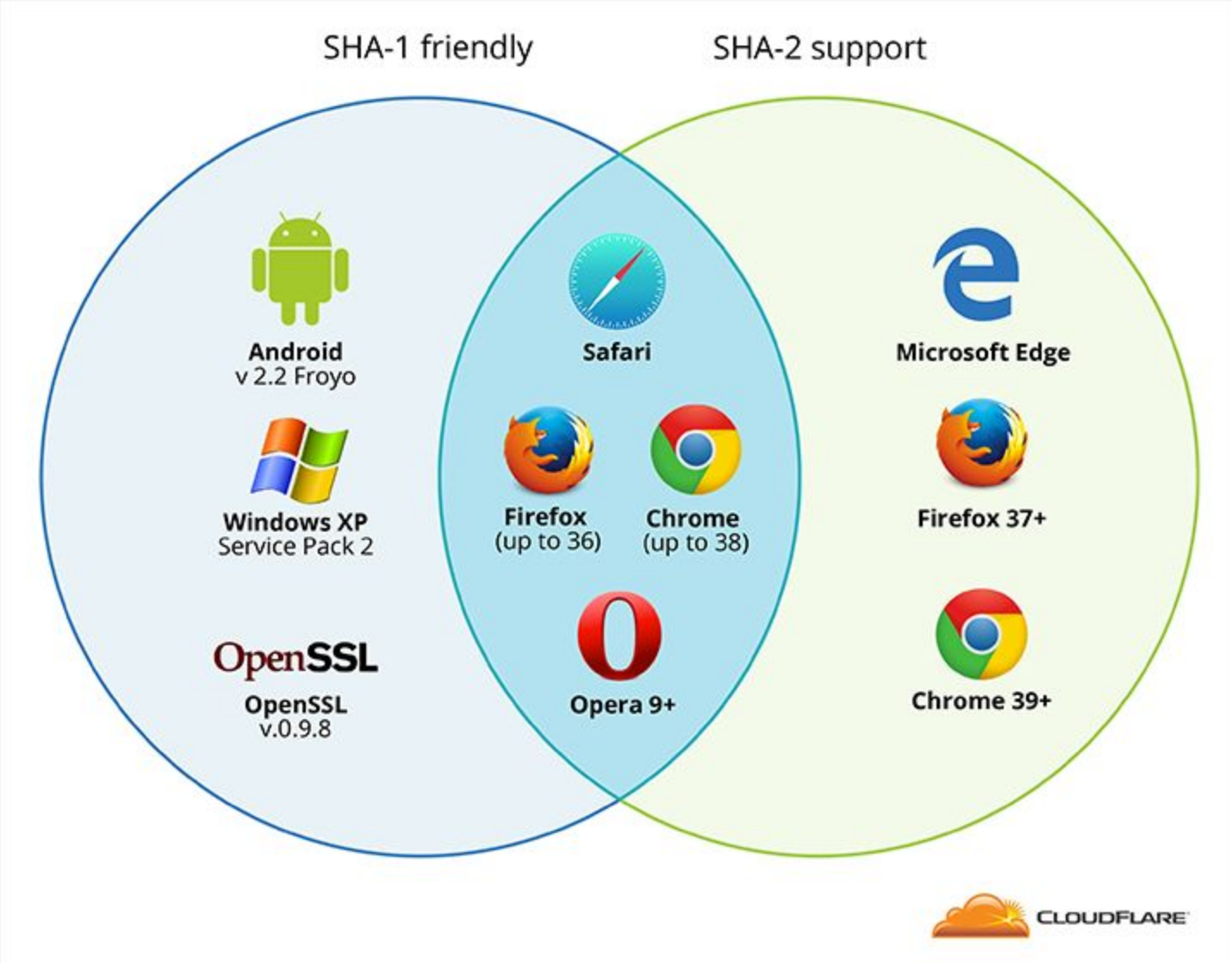
Security Now! #538 - 12-15-15

Q&A #225

This week on Security Now!

- Updates on governments and crypto
- Another chilling discovery thanks to the Shodan search engine
- The SHA-1 sunsetting dilemma and new proposed solution
- Google says bye bye to a Symantec root cert
- A new Wi-Fi router horror
- Do we known more about Satoshi Nakamoto?
- A masters thesis examines Telegram's homegrown crypto
- Some miscellany, a bit of health and Sci-Fi news
- **And... possibly the coolest question I've ever been asked for a Q&A!**



Security News:

Kazakhstan's New Encryption Law Could Be a Preview of US Policy
http://www.defenseone.com/technology/2015/12/kazakhstans-new-encryption-law-could-be-preview-us-policy/124286/

FBI Chief Asks Tech Companies to Stop Offering End-to-End Encryption
http://motherboard.vice.com/read/fbi-chief-asks-tech-companies-to-stop-offering-end-to-end-encryption
<Motherboard> After the recent attacks in Paris and San Bernardino, encryption has once again become a political target in Washington. Despite there still being no solid evidence the attackers benefited from or even used encryption (in at least one case, they coordinated via distinctly unencrypted text messages) law enforcement and national security hawks have used the tragedies to continue pressing tech companies to give the US government access to encrypted communications—even if that means rolling back security and changing the nature of their businesses.

At a Senate Judiciary Committee hearing on Wednesday, FBI director James Comey went so far as to suggest that companies providing users with end-to-end encryption might need to simply, well, stop doing that.

"It's not a technical issue, it's a business model question," said Comey, referring to companies like Apple and WhatsApp which encrypt data so that it can't be read by any third party, including the companies themselves. "Lots of good people have designed their systems and their devices so that judges' orders can not be complied with, for reasons that I understand, I'm not questioning their motivations."

"The question we have to ask is: should they change their business model?"

Moscow, Russia: All Russian citizen data MUST be stored ONLY in Russia... by January.

- http://www.theguardian.com/world/2015/dec/15/dear-facebook-dont-hand-our-data-to-kremlin-putin
- Russia has deployed a powerful "NSA-style" interception technology with monitoring & interception nodes in all Russian ISPs.
- In September Apple rented space in Russia to house the data of Russian citizens.
- Messaging app Viber, eBay, PayPal and Booking.com have decided to comply.
- But Twitter, Google & Facebook have remained silent... while allegedly sending high level representatives to private talks.

Data of Thirteen Million "MacKeeper" Users Exposed

- http://krebsonsecurity.com/2015/12/13-million-mackeeper-users-exposed/
- On recent evening, an IT help desk guy, Chris Vickery, was bored. So he queried the Shodan search engine for the IPs of any publicly-facing database servers listening for

incoming connections on port 27101.
- Port 27017 is commonly used by the MongoDB.
- He got four IPs belonging to Kromtech, publisher of MacKeeper.
- What Chris turned up was the MacKeeper user database server... containing 21 gigabytes of remotely accessible user data.
- Chris responsibly informed Kromtech, who quickly closed the public exposure and publicly stated that no one -- other than Chris -- had ever logged into their system.

Cloudflare, Facebook and others compromise on SHA-1 sunsetting:

- https://www.facebook.com/notes/alex-stamos/the-sha-1-sunset/10153782990367929
- <Alex Stamos> Blogging last Wednesday:
  Like many engineering fields, the practice of information security in the real world is all about finding an appropriate balance between two desirable goals. One of the most interesting areas of balance is between making systems secure against new attacks and providing security to the broadest population. This dynamic is readily apparent in the debate around the upcoming sunset of the SHA-1 hash algorithm, and my colleagues and I at Facebook believe that the current path forward should be reexamined.

  Our friends at CloudFlare have written an excellent post on the subject of SHA-1 certificates, and I would suggest you read their post for a good background on the issue.

  Facebook's data shows that 3-7% of browsers currently in use are not able to use the newer SHA-256 standard, meaning that tens of millions of people will not be able to securely use the Internet after December 31st. A disproportionate number of those people reside in developing countries, and the likely outcome in those counties will be a serious backslide in the deployment of HTTPS by governments, companies and NGOs that wish to reach their target populations.

  After discussing this issue with my colleagues at Facebook, we came together on the following points:

  1. The recent advancements in generating SHA-1 collisions do indicate that the industry should transition to SHA-256 certificates.
  2. We support the removal of SHA-1 support from the latest browser releases.

  Facebook has found success running a large TLS termination edge with certificate switching, where we intelligently choose which certificate a person sees based upon our guess as to the capabilities of their browser. This allows us to provide HTTPS to older browsers using SHA-1 while giving newer browsers the security benefits of SHA-256.

  We don't think it's right to cut tens of millions of people off from the benefits of the encrypted Internet, particularly because of the continued usage of devices that are known to be incompatible with SHA-256. Many of these older devices are being used in developing countries by people who are new to the Internet, as we learned recently when we rolled out TLS encryption to people using our Free Basics Platform. We should be investing in privacy and security solutions for these people, not making it harder for them to use the Internet safely.

Taking these ideas into account, I support CloudFlare's proposal for a different approach. Namely, the CA/Browser Forum should create a new type of Legacy Verified certificate that should only be issued to organizations that have demonstrated they are offering SHA-256 certificates to modern browsers. Such verification can be automated or manual, and appropriate measures can be put in place to reduce the risk of a collision attack. Those protections could include requiring LV applicants to have already passed OV or EV verification, as well as technical best practices such as serial number randomization. If this change cannot be implemented by December 31st, then we call on the CA/B Forum to delay the implementation of the SHA-1 rules for the period necessary to establish standards for Legacy certificates.

Facebook has already open sourced the code we use for certificate switching as part of our Proxygen HTTP library, and all are welcome to use it under the terms of our BSD-style license.

This is not an easy issue, and there are well-meaning people with good intentions who will disagree. We hope that we can find a way forward that promotes the strongest encryption technologies without leaving behind those who are unable to afford the latest and greatest devices.

- https://github.com/facebook/wangle/blob/master/wangle/ssl/SSLContextManager.cpp#L381
    - Examine the incoming ClientHello for support

- Guard against the possibility of downgrade attacks

- **Cloudflare: SHA-1 Deprecation: No Browser Left Behind**
    - https://blog.cloudflare.com/sha-1-deprecation-no-browser-left-behind/
    - <quote> The seemingly good news is that globally, SHA-2 is supported by at least 98.31% of browsers. Cutting 1.69% off the encrypted Internet may not seem like a lot, but it represents over 37 million people. That's the equivalent of the population of California not having access to encryption unless they upgrade their devices. As SHA-2 only sites proliferate, if these users on SHA-1-only browsers try and access an encrypted site, they'll see an error page that completely blocks their access.
    - China: 6% of user's today cannot do SHA-256.

Google to deprecate one of Symantec's Root Certificates

- https://googleonlinesecurity.blogspot.com/2015/12/proactive-measures-in-digital.html
- Posted by Ryan Sleevi, Software Engineer

Over the course of the coming weeks, Google will be moving to distrust the "Class 3 Public Primary CA" root certificate operated by Symantec Corporation, across Chrome, Android, and Google products. We are taking this action in response to a notification by Symantec Corporation that, as of December 1, 2015, Symantec has decided that this root will no longer comply with the CA/Browser Forum's Baseline Requirements. As these requirements reflect industry best practice and are the foundation for publicly trusted

certificates, the failure to comply with these represents an unacceptable risk to users of Google products.

Symantec has informed us they intend to use this root certificate for purposes other than publicly-trusted certificates. However, as this root certificate will no longer adhere to the CA/Browser Forum's Baseline Requirements, Google is no longer able to ensure that the root certificate, or certificates issued from this root certificate, will not be used to intercept, disrupt, or impersonate the secure communication of Google's products or users. As Symantec is unwilling to specify the new purposes for these certificates, and as they are aware of the risk to Google's users, they have requested that Google take preventative action by removing and distrusting this root certificate. This step is necessary because this root certificate is widely trusted on platforms such as Android, Windows, and versions of OS X prior to OS X 10.11, and thus certificates Symantec issues under this root certificate would otherwise be treated as trustworthy.

Symantec has indicated that they do not believe their customers, who are the operators of secure websites, will be affected by this removal. Further, Symantec has also indicated that, to the best of their knowledge, they do not believe customers who attempt to access sites secured with Symantec certificates will be affected by this. Users or site operators who encounter issues with this distrusting and removal should contact Symantec Technical Support.

Millions affected. Major exploit in Bell Canada's HomeHub 1000 & 2000 routers reveals WPA2-PSK in under one second.

- http://www.dslreports.com/forum/r30443059-Bell-Home-Hub-2000-Backdoor-Security-vulnerability
- With WPS disabled, Home Hub router access point's beacon states that WPS is not available.
- But, a request for WPSauthentication using the PIN 12345678 *will* succeed.
- The router promptly replies with the WPA2 passphrase.
- The attacker may then use this passphrase to connect.
- This all take less than a second. NO brute forcing required.
- This is NOT (one of the well known) problem with WPS.
- <quote> "Hello, I have just tested this on many BELLXXX routers. The PIN is actually 12345670, not 12345678.
    - (The last digit is a simple check-digit which must be '0' for the prefix '1234567')

WIRED thinks it has unmasked Satoshi Nakamoto... or maybe not

- http://www.wired.com/2015/12/bitcoins-creator-satoshi-nakamoto-is-probably-this-unknown-australian-genius/
- And then: Satoshi's PGP Keys Are Probably Backdated and Point to a Hoax
    - http://motherboard.vice.com/read/satoshis-pgp-keys-are-probably-backdated-and-point-to-a-hoax
- Leo???

Suspected hit-and-run driver caught in Florida... after /HER/ car called the cops

- http://www.foxnews.com/us/2015/12/07/suspected-hit-and-run-driver-caught-in-florida-after-her-car-called-cops/
- (From our mailbag: Troy Frericks)
- Police caught a driver linked to an alleged hit-and-run in Florida after her own vehicle called the cops, local media reported.

  Investigators received an automated call from the Ford's emergency response system, offering to let them speak with the driver if they pressed zero, according to WPBF.

  So a dispatcher talked to the driver, Cathy Bernstein of Port St. Lucie. She denied there had been a crash and said she hadn't been drinking, police reported.

  But cops say they saw significant front-end damage to the vehicle when they went to her home. Bernstein then claimed she had hit a tree, according to police.

  Eventually she admitted to the hit-and-run, police said, adding that she was actually trying to escape from an earlier crash. Bernstein was arrested, WPBF reported.

Telegram Cryptanalysis

- http://cs.au.dk/~jakjak/master-thesis.pdf
- Jakob Jakobsen - Computer Science Masters Thesis
- (Aarhus University, Denmark - Founded in 1928, Denmark's second oldest university and the largest, with a total of 43,600 enrolled students.)
- Abstract: The number one rule for cryptography is never create your own crypto. Instant messaging application Telegram has disregarded this rule and decided to create an original message encryption protocol. In this work we have done a thorough cryptanalysis of the encryption protocol and its implementation. We look at the underlying cryptographic primitives and how they are combined to construct the protocol, and what vulnerabilities this has. We have found that Telegram does not check integrity of the padding applied prior to encryption, which lead us to come up with two novel attacks on Telegram. The first of these exploits the unchecked length of the padding, and the second exploits the unchecked padding contents. Both of these attacks break the basic notions of security, and are confirmed to work in practice. Lastly, a brief analysis of the similar application TextSecure is done, showing that by using well known primitives and a proper construction provable security is obtained. We conclude that Telegram should have opted for a more standard approach.
- Table of Contents:
  - Random Padding Vulnerability
  - Reply and mirroring attacks in older versions
  - Timing attacks
  - Known attacks on primitives
  - Experimental Validations:
  - Attack #1 - Padding length extension
  - Attack #2 - Padding plaintext collision
  - Malicious server attack

- Conclusion: TextSecure is based on strong primitives that have withstood cryptanalysis from the crypto community for years, and these are combined in a way that provenly provides authenticated encryption.
  Telegram on the other hand has crafted its own encryption scheme and deployed it in an unproven state, and prior to any scrutiny from other cryptographers.
  We have seen this done time and time again, and rarely with good results. Take for example the smart grid meters that were shown to use terrible crypto back in April this year.
  Furthermore, the DH Ratchet is a very nice way of providing forward secrecy on a per-message basis with little overhead, which is an improvement over Telegram's one key per 100 messages approach.

Miscellany:

"Steve the physicist?"

- IcyvRan TocVuc @IcyvRan
- I was listening to episode 537, and you said referring to yourself: "being a physicist". WHAT?!!!!

Chris Wronski @theemptyset

- @SGgrc RE: AOL ['s Desktop "FDO" scripting language] no-authentication, remember that this comes from the days of point-to-point modem connections.

Ultimate Outsider @OutsiderSupreme

- Thanks @SGgrc and @leolaporte for mentioning my GWX Control Panel on Security Now! Feel free to contact me w/any future questions/concerns.

An anonymous listener asks...

- Hi Steve,
  You mentioned that PDF you put together about your SciFi book recommendations.
  But when was the last time you updated that PDF?
  - (The Expanse series... petered out during the 4th book and never finished it.)
  - Lost Fleet /Jack Campbell
  - Michael McCollum
  - Peter Hamilton

SyFy Sci-Fi:

- Childhood's End
- The Expanse

Health Corner:

Magnesium:

"Carl Engelbrecht"
Steve, which magnesium supplement would you recommend? THX
Hi Carl!

Magnesium is absolutely required for more than 300 chemical reactions.

- ~80% of Westerners are not getting sufficient magnesium.
- Soil is becoming increasingly mineral poor.
- NPK fertilizer: Nitrogen (N), Phosphorus (P), Potassium (K)
- Since magnesium is taken up into cells only 1% is in serum, so there's no reliable testing for it.
- RDA for women is 310 to 320 milligrams (mg) and 400 to 420 for men.
- Paleolithic diets had about 1-to-1 ration of calcium to magnesium. Current Western diets have a ration more like 3.5-to-1.
- Magnesium is generally relaxing.
- My own symptomology:
    - PVCs (arrythmias -- ectopic beats) "skip a beat"
    - Kidney stone - Mg helps to prevent solids from precipitating out of solution.
    - Blood pressure was drifting upwards.
- "The Magnesium Miracle" by Carolyn Dean, 1st edition 2007, updated 2014

> Steve, which magnesium suppliment would you recomend? THX

The trick with Magnesium is absorption. The traditional simple salts of magnesium such as magnesium oxide, carbonate, citrate, malate, taurate, etc. are dissociated (dissolved) by our stomach acid, freeing the magnesium. But free magnesium has very low intestinal absorption. This leaves much of it unabsorbed and, if taken in what would be a sufficient dosage to be useful, induces diarrhea by osmotically drawing water into our intestines.

That's not in itself dangerous. By which I mean that's the way our intestinal tracts are deliberately cleaned out in preparation for a colonoscopy. We're given an empty jug with some powder in the bottom -- that's magnesium oxide, the least well absorbed and least expensive magnesium available. We add water and drink it all down over the first half of the day. With the result that we are completely and gently washed out by the effect of the magnesium. Of course, it would be very unhealthy to do this other than in preparation for medical tests.

So, how to get magnesium absorbed?

One company -- Albion Minerals -- figured out how to do this. They turn magnesium molecules into what our body treats as food by chemically binding atoms of magnesium to pairs of small and simple amino acids to create dipeptides... essentially small and simple proteins. They favor the use of the smallest possible amino acid, glycine, and they may use a pair of glycine molecules to create magnesium bisglycinate, or they may use one glycine and one lysine to create a magnesium glycinate/lysinate chelate.

Albion has patents and trademarks, so what you want to look for is "Albion Minerals" and/or a round seal with TRAACS. Anyone's magnesium that has that will be among the best and most absorbable available.

I like the Doctor's Best brand, so I purchase theirs:
http://www.amazon.com/dp/B000BD0RT0/
Thanks for your note and question!

SpinRite:

Juddson in Pennsylvania
Subject: SpinRite on SCSI RAID drives
:
We recently had a major drive failure on a RAID storage array at my place of work. Not sure of the configuration, but I don't think it matters much for my question. Apparently one of the drives had failed some time ago, and no one had noticed. So when the second drive failed, people of course noticed immediately. It contained critical financial data and company records, so there was a bit of panic going around.

I am not on the sys admin team, I'm just a developer on the software team, so I was not directly involved. However, I was aware of the issue (as were we all, since this was a corporate server), and that one of the options on the table was to send the entire array back to the drive manufacturer for recovery, with a price tag upwards of $10,000.

I own a copy of SpinRite, and pictured myself swooping in to save the day. (With the assumption that my company would be more than happy to pay for a SpinRite site license having saving $10,000). Upon recommending the solution to our lead system administrator, I was essentially chastised for having even mentioned SpinRite. The drives were SCSI drives, and it seems as though SpinRite in the eyes of professional data recovery firms is akin to a homeowner trying to fix their own septic system failure. You're just going to make it worse, leave it to the professionals.

Is there any way that SpinRite could have helped in this situation? I was imagining that we could pull the failed drive out of the array, mount it individually, run SpinRite on it and return it to the array. Is there any way to do this easily with a SCSI drive?

How do you respond to the notion that SpinRite will just make your problem worse, I assume by performing heaving read/write operations on the disc and thereby worsening the drive wear? I know that is not your position, otherwise, you wouldn't provide this product. I'm mainly curious as to how to respond in future situations when I experience SpinRite skepticism.

As far as the array in question, we apparently were able to recover from a backup, which we initially thought had been lost as well. I still wish we would have tried SpinRite, just to see what it could have done, if anything.
Thanks!