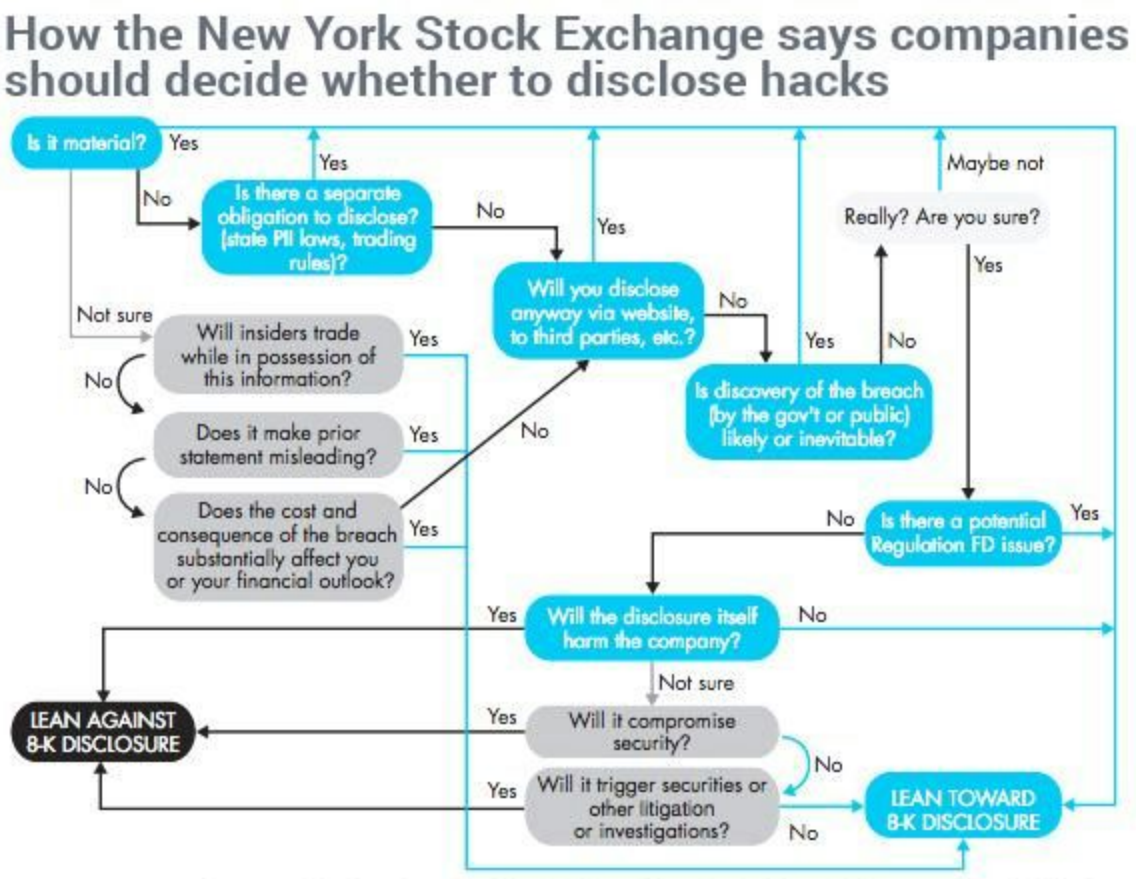
Security Now! #531 - 10-27-15

Q&A #221

This week on Security Now!

- 1Password metadata, revisited
- Bad Western Digital HD Encryption
- How the NSA is seeing into encrypted data
- An update on the "Let's Encrypt" project
- The future of the beleaguered SHA-1 hash
- Miscellany
- 10 questions, thoughts and observations from our terrific listeners!



Source: Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers Provides Actionable Advice and Best Practices

Security News:

1Password metadata, revisited

- 1Password (@1Password)
  - @briemens @TWiT @SGgrc It's encrypted by Dropbox password. More info here:
- https://blog.agilebits.com/2015/10/19/when-a-leak-isnt-a-leak/
  - "When a Leak Isn't a Leak" referred to Dale's post, but did not link to it.
  - Basically says nothing.
- Apple Insider:
  - http://appleinsider.com/articles/15/10/20/1password-to-change-file-formats-after-key-file-found-to-contain-unencrypted-data
- The actual problem was an early fundamental design decision which didn't scale:
  - An individual, single, separate small file per vault entry.
- Paul Moore:
  - Paul Moore (@Paul_Reviews)
    I wonder if @SGgrc will take the opportunity to correct himself on #LastPass leaking metadata during #SecurityNow tonight? / cc @leolaporte
  - https://paul.reviews/privacy-password-managers-a-reality-check/
  - Rants for a while, then attempts to equate LastPass HTTPS secured retrieval of website Favicons (though he apparently doesn't know what a Favicon is) with 1Password's non-encryption of all user data at rest.
- LastPast had two choices:
  - Have clients directly query sites for favicons, which may have been over HTTP and reveal their IP (and site cookie) to every website queried.
  - Or... have LastPass function as a secure proxy, communicating over HTTPS with lastpass.com to securely and anonymously obtain the favicon from remote sites without divulging the site's cookie to LastPass nor the client's IP to the site.

WD HDD Crypto...

- http://eprint.iacr.org/2015/1002.pdf
- On the (in)security of a Self-Encrypting Drive series
- Abstract:
  - Self encrypting devices (SEDs) doing full disk encryption are gettingmore and more widespread. Hardware implemented AES encryption provides fast and transparent encryption of all user data on the storage medium, at all times. In this paper we will look into some models in a self encryption external hard drive series; theWestern Digital My Passport series. We will describe the security model of these devices and show several security weaknesses like RAM leakage, weak key attacks and even backdoors on some of these devices… resulting in decrypted user data without the knowledge of any user credentials.

DH weakened?

- "Imperfect Forward Secrecy": How Diffie-Hellman Fails in Practice
  - Security Now! #509 (22 weeks ago)
- https://weakdh.org
- Logjam was a encryption strength downgrade attack
  - forcing 512 bit "export grade" Diffie-Hellman key agreement.
- The same authors noted that most servers are only using a few common 1024-bit primes.
- <quote> Threats from state-level adversaries.
  Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve—the most efficient algorithm for breaking a Diffie-Hellman connection—is dependent only on this prime. After this first step, an attacker can quickly break individual connections.

  We carried out this computation against the most common 512-bit prime used for TLS and demonstrate that the Logjam attack can be used to downgrade connections to 80% of TLS servers supporting DHE_EXPORT. We further estimate that an academic team can break a 768-bit prime and that a nation-state can break a 1024-bit prime.

  Breaking the single, most common 1024-bit prime used by web servers would allow passive eavesdropping on connections to 18% of the Top 1 Million HTTPS domains. A second prime would allow passive decryption of connections to 66% of VPN servers and 26% of SSH servers. A close reading of published NSA leaks shows that the agency's attacks on VPNs are consistent with having achieved such a break.

- https://www.eff.org/deeplinks/2015/10/how-to-protect-yourself-from-nsa-attacks-1024-bit-DH
- Check any website: https://weakdh.org/sysadmin.html

Let's Encrypt is now "trusted" -- cross-signed

- Mozilla, Akamai, Cisco, EFF, InenTrust, Internet Society & others.
- https://letsencrypt.org/2015/10/19/lets-encrypt-is-trusted.html
- <quote> We're pleased to announce that we've received cross-signatures from IdenTrust, which means that our certificates are now trusted by all major browsers. This is a significant milestone since it means that visitors to websites using Let's Encrypt certificates can enjoy a secure browsing experience with no special configuration required.

  Both Let's Encrypt intermediate certificates, Let's Encrypt Authority X1 and Let's Encrypt Authority X2, received cross-signatures. Web servers will need to be configured to serve the appropriate cross-signature certificate as part of the trust chain. The Let's Encrypt client will handle this automatically.

SHA-1 Ballot Update

- Geoff Keating <geoffk at apple.com>
  - We've discussed this ballot within Apple, and based on what is known about SHA-1 security, and the impact on an orderly industry-wide removal of SHA-1 support, we are against extension of certificate issuance until the end of 2016, and so intend to vote against the ballot.

- Erwann Abalea <erwann.abalea at opentrust.com>
  - Was just reading it. The complete (80 rounds) SHA1 compression function is broken. Some could argue that we still have a small security margin because of the choice of IV, or the difference in work factor between collision and choosen-prefix collision, etc. But it took too many years to get rid of MD5 (at least 7 years after collision were publicly demonstrated). Let's do things better with SHA1.

- Rick Andrews <Rick_Andrews at symantec.com>
  - Symantec and the endorsers withdraw this ballot.

- Gervase Markham <gerv at mozilla.org>
  - I'm not sad to see this ballot go.

Miscellany:

Bridge of Spies -- was FABULOUS!!!

A new "meme" for SN to join "TNO": "Doing it wrong"

A listener in the UK wrote:

- Subject: Lings Cars

  On last week's episode I noticed you found Lingscars.com

  Ling is something of a minor celebrity here in the UK and is probably best known for using an old mobile ICBM missile launcher as an advertising billboard.

  The BBC did a piece on her some time ago:
  https://www.youtube.com/watch?t=672&v=cc1ktZRZ5ZM

A belated birthday shout out...

From: "Michael Cykowski" Rochester Hills, Michigan
Date: Tue, 13 Oct 2015 05:57:10 -0000

Dear Steve,

This email is about my father Mark Cykowski. His 70th birthday is October 19, 2015. He has spent his life working in technology and hasn't missed an episode of Security Now since 2008.

I realize you aren't Ryan Seacrest, but is there anything I could do to convince you to give him a birthday "shout out" on Security Now ? Could I donate to your favorite charity?

We have already purchased a copy of Spinrite and it saved my butt twice!

In any event, thank you for doing what you do. Your show is consistently one of the top tech podcasts out there.

Sincerely,
A big Security Now fan on behalf of his security obsessed father.
Michael Cykowski

SpinRite:

http://slickdeals.net/f/8159236-grc-steve-gibson-s-spinrite

GRC & Steve Gibson's Spinrite

dale_101798:
In the past I have recommended Spinrite to recover data from unresponsive hard drives. Some Slickdeals users complained that on the Huge hard drives we use today Spinrite is simply too slow.

However if you want to recover data from any hard drive you should at least know about Spinrite.

Yesterday I found myself in the unenviable position of needing Spinrite to correct a failed hard drive in my wife's computer, it gave a blue screen error on every attempt to boot. Yes we have backups but restoring a backup on a new hard drive takes a long time too. {Gotta go to the store buy the HD, install the HD, and fire up Acronis True Image & wait for it to do it's magic}.

Instead Spinrite did it's magic on a 1TB HD in 2 hours and I was once again the in-house miracle worker / computer genius. If you would like to learn more about Spinrite go to GRC and view the video.