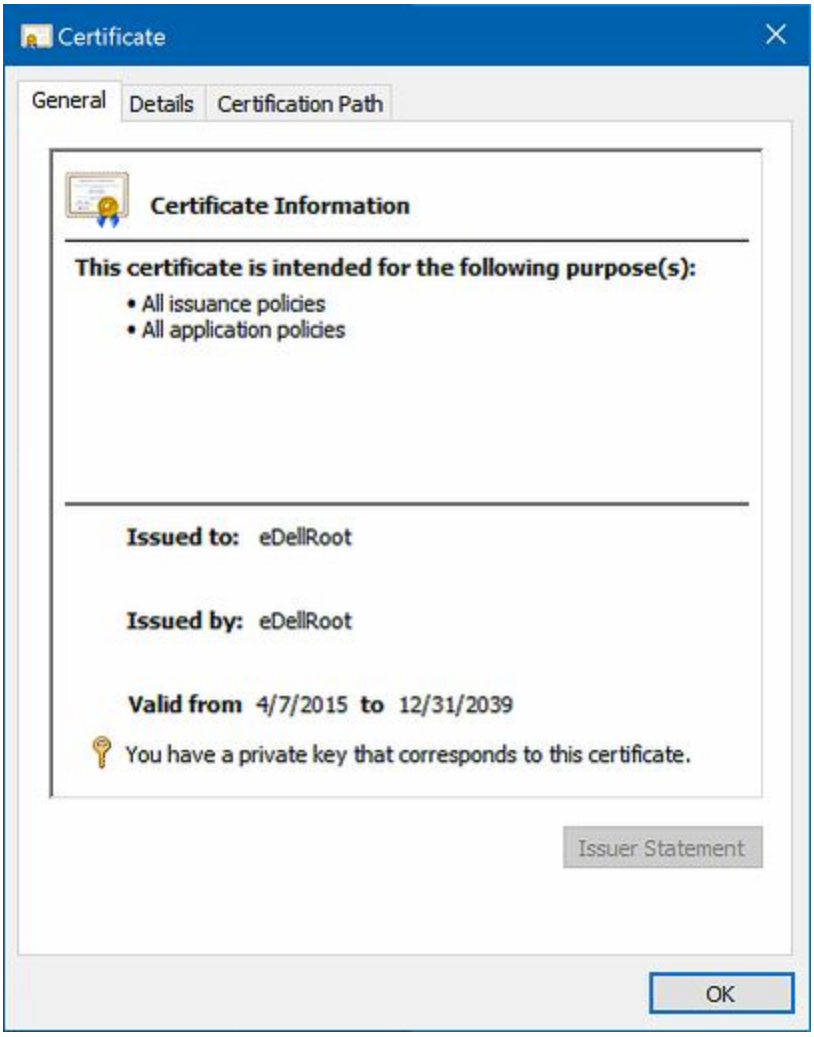
Security Now! #535 - 11-24-15

Listener Feedback, Q&A #223

This week on Security Now!

- Dell steps in it big time...
- Has LastPass stepped in something too?
- Windows 10's various recent struggles
- A report of the Manhatten DA's office about Smartphone Encryption
- Various updates and miscellany, including an Errata
- Ten listener thoughts, and questions

Dell's Massive Mistake



Security News:

Dell really steps in it.

- ArsTechnica
  - http://arstechnica.com/security/2015/11/dell-does-superfish-ships-pcs-with-self-signed-root-certificates/
  - [Dan Goodin]
    "Dell does a Superfish, ships PCs with easily cloneable root certificates"

    In a move eerily similar to the Superfish debacle that visited Lenovo in February, Dell is shipping computers that come preinstalled with a digital certificate that makes it easy for attackers to cryptographically impersonate Google, Bank of America, and any other HTTPS-protected website.

    The self-signed transport layer security credential, which was issued by an entity calling itself eDellRoot, was preinstalled as a root certificate on at least two Dell laptops, one an Inspiron 5000 series notebook and the other an XPS 15 model. Both are signed with the same private cryptographic key. That means anyone with moderate technical skills can extract the key and use it to sign fraudulent TLS certificates for any HTTPS-protected website on the Internet. Depending on the browser used, any Dell computer that ships with the root certificate described above will then accept the encrypted Web sessions with no warnings whatsoever. At least some Dell Inspiron desktops, and various Precision M4800 and Latitude models are also reported to be affected.

- Robert Graham of Errata Security:
  http://blog.erratasec.com/2015/11/some-notes-on-edellroot-key.html#.VlNppoS3Bqs

  It was discovered this weekend that new Dell computers, as well as old ones with updates, come with a CA certificate ("eDellRoot") that includes the private key. This means hackers can [trivially] eavesdrop on the SSL communications of Dell computers.

  If I were a black-hat hacker, I'd immediately go to the nearest big city airport and sit outside the international first class lounges and eavesdrop on everyone's encrypted communications. I suggest "international first class", because if they can afford $10,000 for a ticket, they probably have something juicy on their computer worth hacking.

  I point this out in order to describe the severity of Dell's mistake. It's not a simple bug that needs to be fixed, it's a drop-everything and panic sort of bug. Dell needs to panic. Dell's corporate customers need to panic.

  Note that Dell's spinning of this issue has started, saying that they aren't like Lenovo, because they didn't install bloatware like Superfish. This doesn't matter. The problem with Superfish wasn't the software, but the private key. In this respect, Dell's error is exactly as bad as the Superfish error.

- Exploitability testing sites:
  - https://bogus.lessonslearned.org/
    Security guy Kenn White created a certificate for a test site. Google Chrome, Microsoft Edge and IE establish an encrypted Web session with no warnings, even though the certificate was clearly fraudulent.
  - Firefox generated an alert warning that the certificate was not trusted.

    - https://edell.tlsfun.de/
    - Hanno Bock: Dell laptops ship with a preinstalled root certificate and a private key. This is a very severe security risk and has the potential to compromise all encrypted HTTPS connections. This test will check whether you are vulnerable.

- Cert is valid for "All issuance policies" and "All application policies"
    - In other words... it's a FULL WILDCARD certificate with no constraints.
    - This allows, for example, code signing.
    - Normally a certificate i s issued with constraints permitting no greater usage than is required:
    - GRC: "Web server authentication" / "Web client authentication"

- Dan Goodin: "What is clear now is that the eDellRoot certificate was generated two months after the Superfish debacle came to light and that it poses a risk to at least some Dell customers."

- SANS Security's post: Superfish 2.0: Dell Windows Systems Pre-Installed TLS Root CA
  https://isc.sans.edu/forums/diary/Superfish+20+Dell+Windows+Systems+PreInstalled+TLS+Root+CA/20411/
  Recently shipped Dell systems have been found to include a special Root CA Certificate and private key, "eDellRoot". All systems apparently use the same key and certificate. Using the "secret" key, anybody could create certificates for any domain, and Dell systems with this eDellRoot certificate would trust it. The key is part of "Dell Foundation Services".

  To remove the certificate if you are affected:
    o Stop and disable Dell Foundation Services
    o Delete the eDellRoot CA (start certmgr.msc, select "Trusted Root Certification Authorities" and "Certificates". Look for eDellRoot)

  For details about managing Root CAs see
  https://technet.microsoft.com/en-us/library/cc754841.aspx

  It is not sufficient to just remove the CA. Dell Foundation Services will reinstall it. This is why you need to disable Dell Foundation Services first, or delete the Dell.Foundation.Agent.Plugins.eDell.dll.

- **Dell Responded yesterday (11/23):**
  http://en.community.dell.com/dell-blogs/direct2dell/b/direct2dell/archive/2015/11/23/response-to-concerns-regarding-edellroot-certificate
  Today we became aware that a certificate (eDellRoot), installed by our Dell Foundation Services application on our PCs, unintentionally introduced a security vulnerability. The certificate was implemented as part of a support tool and intended to make it faster and easier for our customers to service their system. Customer security and privacy is a top concern and priority for Dell; we deeply regret that this has happened and are taking steps to address it.
  The certificate is not malware or adware. Rather, it was intended to provide the system service tag to Dell online support allowing us to quickly identify the computer model, making it easier and faster to service our customers. This certificate is not being

used to collect personal customer information. It's also important to note that the certificate will not reinstall itself once it is properly removed using the recommended Dell process.

We have posted instructions to permanently remove the certificate from your system here. We will also push a software update starting on November 24 that will check for the certificate, and if detected remove it. Commercial customers who reimaged their systems without Dell Foundation Services are not affected by this issue. Additionally, the certificate will be removed from all Dell systems moving forward.

Your trust is important to us and we are actively working to address this issue. We thank customers such as Hanno Böck, Joe Nord and Kevin Hicks, aka rotorcowboy, who brought this to our attention. If you ever find a potential security vulnerability in any Dell product or software, we encourage you to visit this site to contact us immediately.

- Dell's official remover:
  https://dellupdater.dell.com/Downloads/APP009/eDellRootCertFix.exe

- Windows Apps by FS1:
  - http://trax.x10.mx/apps.html
  - RCC: Tiny 40k .EXE
    Scans and audits the trusted root CA stores in Microsoft Windows and Mozilla Firefox. Highlights potentially rogue root certificates based on trusted baselines and timestamp metadata.

LastPass

- http://www.martinvigo.com/even-the-lastpass-will-be-stolen-deal-with-it/
- Martin Vigo & Alberto Garcia presented at the recently concluded (Hamster)Amsterdam Blackhat "Even the LastPass Will be Stolen, Deal with It!"

- **Local Attacks:**
  - They reverse engineered the technology and exploited required features:
  - **Vault Decryption Attack:**
    - IF the user is statically logged-in their browser has access to the user's local vault, so, then, could a malicious takeover of the Lastpass plug-in. (This is true of all and any password manager.)
    - The only way to be safe would be to never remain statically logged into Lastpass.

  - **Disabled OTP Attack:**
    - Used for account recovery if the user loses their key.
    - Everything required must be present.
    - Metasploit module now created

- **LastPass side attacks:**
  - They discovered that LastPass has the ability to inject a helper custom_js into a page where they're unable to parse the DOM (document object model) to find the username and password fields. This facility could be suborned to steal user credentials.
  - Could the NSA, having read this work, compel Lastpass to inject malicious code into a user's browser in order to access their passwords?
  - (This is an inherent problem with ANY centralized cloud-based system. Two years ago, when I first disclosed the way SQRL operates, I explained that its 2-party system specifically avoided this problem.)

- **Attacks from the outside:**
  - Firefox's "prefs.js" contains all browser settings... and the ENCRYPTED Lastpass credentials.
  - Users are unwittingly posting their whole browser prefs.js on forums asking for help.
  - Google can find them.
  - But... a full brute force decryption is still required.

- **Recommendations for LastPass users:**
  - Use the binary version of the plugin
  - Do not store the master password
  - Activate the new Account Recovery over SMS
  - Audit your vault for malicious JS payloads
  - Don’t use “password reminder”
  - Activate 2FA
  - Add country restrictions
  - Disallow TOR logins

- **Recommendations for LastPass:**
  - Get rid of custom_js!
  - Encrypt the entire vault in one chunk
  - Don’t use ECB
  - Use PBKDF2 between client and LastPass also
  - Use cert pinning
  - Embrace open source
  - Adopt a retroactive, cash rewarded bug bounty program ;)

- **Conclusions:**
  [quote] Password managers are a great tool that everyone should use. Even though we exposed weaknesses in LastPass, it is still a solid tool and a better option than using the same password, or only changing the last characters of your password, everywhere. There are ways to harden your LastPass configuration that can avoid some of the explained attacks. Watch the talk and slides for more details on that. To finish, we want to point out that the security team at LastPass responded very quickly to all our reports and lot of the issues were fixed in just a couple days. It was very easy to communicate and work with them.

Windows 10 - Becoming a bit heavy handed?

- http://venturebeat.com/2015/11/23/windows-10s-fall-update-is-deleting-certain-apps-without-asking/
- Windows 10 appears to be making unwanted changes without asking.

  [paraphrasing] Microsoft's first big update for its operating-system-as-a-service is deleting some user-installed apps without asking Windows owners for permission, according to dozens of complaints on message boards and forums. The affected programs include hardware monitoring tools CPU-Z and Speccy as well as the AMD Catalyst Control Center for tweaking your Radeon graphics cards. In these instances, the programs apparently no longer functioned properly with the newest version of Windows 10, and Microsoft claims the apps were causing crashes and the blue screen of death. While this may help most people who don't want to deal with troubleshooting their system to figure out what is wrong with it, some PC power users are taking issue with Windows 10 removing software without asking.

- Reddit poster Bright-Spark put it thus:
  "Microsoft should ask for permission, and not for forgiveness. I would be fine with it if Windows 10 said 'Hey, this application can cause problems and we recommend that you uninstall it. Do you want us to do that for you?' and then shuts it's mouth about it if you say 'No,' but they shouldn't just uninstall it without prior warning."

- Windows is evolving into a different beast. It's evolving into a connected service.

"REPORT OF THE MANHATTAN DISTRICT ATTORNEY'S OFFICE ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY"

- http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf
- http://bit.ly/sn-535a (42
- ArsTechnica: ArsTechnica: Manhattan DA demands Congress require mobile phone backdoors / DA says encryption thwarted him 111 times in a year from accessing suspects' data.
  - http://arstechnica.com/tech-policy/2015/11/manhattan-da-demands-congress-require-mobile-phone-backdoors/

- **Forward:**
  Most people today live their lives on smartphones, and, in this regard at least, criminals are no different. While in the past criminals may have kept evidence of their crimes in file cabinets, closets, and safes, today that evidence is more often found on smartphones. Photos and videos of child sexual assault; text messages between sex traffickers and their customers; even a video of a murder victim being shot to death – these are just a few of the pieces of evidence found on smartphones and used to prosecute people committing horrific crimes.

  Last fall, a decision by a single company changed the way those of us in law enforcement work to keep the public safe and bring justice to victims and their families. In September 2014, Apple Inc. announced that its new operating system for smartphones and tablets

would employ, by default, what is commonly referred to as "full-disk encryption," making data on its devices completely inaccessible without a passcode. Shortly thereafter, Google Inc. announced that it would do the same.

Apple's and Google's decisions to enable full-disk encryption by default on smartphones means that law enforcement officials can no longer access evidence of crimes stored on smartphones, even though the officials have a search warrant issued by a neutral judge.

Apple and Google are not responsible for keeping the public safe. That is the job of law enforcement. But the consequences of these companies' actions on the public safety are severe. That is why my Office has been working with our law enforcement partners around the world to craft the solution recommended in this Report. We believe there is a responsible way to balance safety and security.

- **Executive Summary:**
  - ***Part V*** sets forth a proposed solution: Congress should enact a statute that requires any designer of an operating system for a smartphone or tablet manufactured, leased, or sold in the U.S. to ensure that data on its devices is accessible pursuant to a search warrant. Such a law would be well within Congress's Commerce Clause powers, and does not require costly or difficult technological innovations.

- **The Difficulty Of Getting Passcodes From Defendants**

Case law holds almost universally that a defendant cannot be compelled (by, e.g., a grand jury subpoena or order of the court) to provide the government with her or his passcode, because such compulsion would violate the defendant's Fifth Amendment right against self-incrimination. There are two potential exceptions to this rule.

First, it is an open question whether, instead of being compelled to provide the government with a passcode, the defendant might be compelled to unlock her or his phone using the passcode. There have been no cases considering this precise question, and although a court might conclude that it is no different from the situation in which a defendant is compelled to provide the government with the passcode, it might also determine that the situations are somewhat different.

Second, if the existence of evidence on the phone is a foregone conclusion, then the defendant may have no Fifth Amendment privilege with respect to the contents of the phone, and thus may be compelled to provide the government with the passcode.16 It would be difficult in most circumstances, however, for the government to establish with the requisite degree of certainty the existence of evidence in a phone that would clear the "foregone conclusion" hurdle.

In any event, even if the government could lawfully compel a defendant to disclose her or his passcode – or to open her or his phone using the passcode – there is a substantial likelihood that any defendant who faces potentially serious criminal charges would simply refuse to comply with the subpoena or order, and go into contempt.

- **A Proposed Solution: Make Smartphones Amenable To Search Warrants**

  There is no provision of the U.S. Constitution, or of any state constitution, that would require producers of smartphones and operating systems to make smartphones amenable to governmental searches. A federal statute could, however, compel such amenability. The Commerce Clause gives the federal government the authority to "regulate Commerce . . . among the several States," and "with foreign Nations." Because smartphones are part of interstate and foreign commerce, a federal statute regulating smartphones would comfortably fall within the power of Congress to regulate activities "that substantially affect interstate commerce."

  Any state could also regulate smartphones sold or used within its borders. Each of the 62 District Attorneys in New York State have, indeed, proposed such legislation. It is clear, however, that federal legislation is preferable to state legislation. The problem under consideration here requires a nationwide solution, and only federal legislation can provide it.

  The federal legislation would provide in substance that any smartphone manufactured, leased, or sold in the U.S. must be able to be unlocked, or its data accessed, by the operating system designer. Compliance with such a statute would not require new technology or costly adjustments. It would require, simply, that designers and makers of operating systems not design or build them to be impregnable to lawful governmental searches.

~30~

Reports from multiple followers of receipt of LetEncrypt Beta invitations.

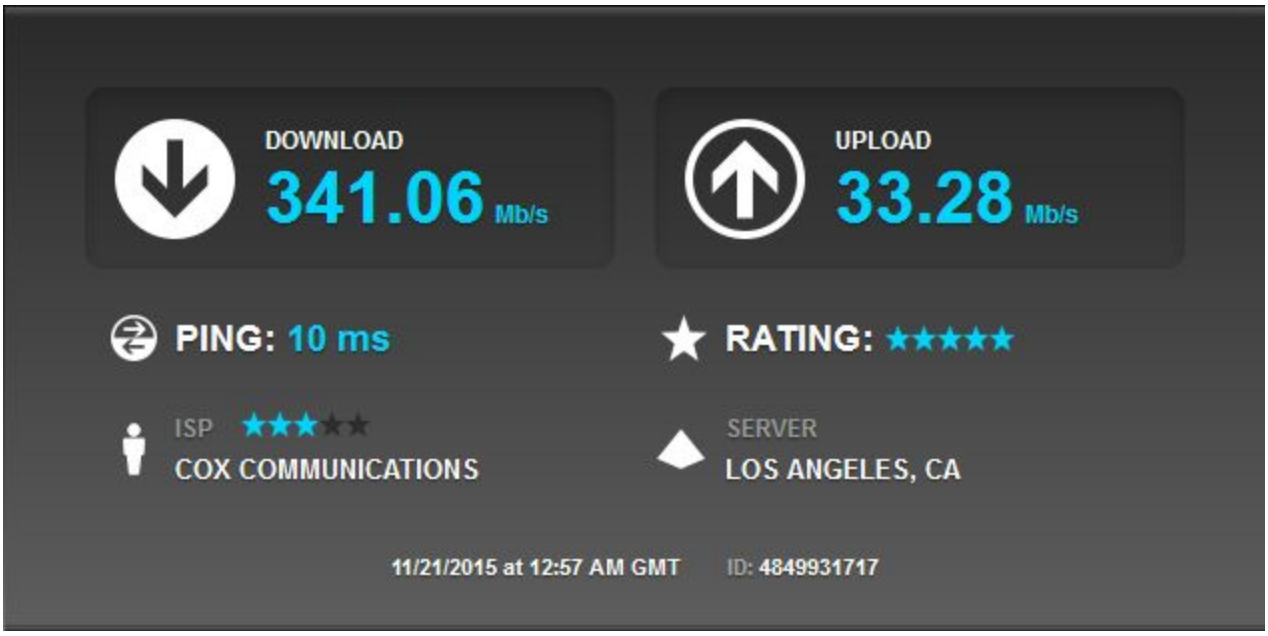
Miscellany

Based upon much feedback, last week's rehashing of the crypto controversy *was* very useful to many.

- A clear and pithy explainer of the problem:
  Ben Hughes @benjammingh
  If banning encryption would stop terrorists from using it, why don't they just make terrorism illegal and be done with it?

COX reliability and new bandwidth (Netgear CM600) 24 downstream & 8 upstream channels

- http://www.speedtest.net/my-result/4849931717
  341.06 Mbits down / 33.28 Mbits up



Auralux Followup:

- Productivity among a significant subset of our listeners has reportedly collapsed this past week... as a consequence of "Auralux." Thank goodness we have a four-day weekend coming up!

"The Expanse" on SyFi

- Apple TV, iTunes, Google Play Store, Comcast On Demand
- Opening vignette was extremely awkward and unclear.
- A lot of narrative in the book which may not translate well visually.

This week's difficult-to-beat "You're Doing It Wrong!"

- http://wogcc.state.wy.us/SundryPassWord.cfm
- http://bit.ly/sn-535
- Wyoming Oil & Gas Conservation Commission
- This Page Requires A Pass Word, which allows the user to locate wells for filing of Sundry(s); Form 4. Please call if you have any questions or Problems
- Brett follows SGgrc... and he's in Laramie, Wyoming

For non-Twitter users

- In the US text "follow sggrc" to 40404.
- To discontinue, text "OFF sggrc".
- Elsewhere: https://support.twitter.com/articles/20170024#
- See: "SMS Follow" https://support.twitter.com/articles/20170004#

Errata!

From: "HÃ¥kan"
Subject: Wildcard certs do not need SNI
X-Location: Sweden

Hi,

Regarding wildcard certificates, I think you mixed things up a bit. Wildcard certificates do not require SNI.

SNI only matters if the server wants to use multiple /certificates/ on the same IP, there's no problem with just multiple names supported by the same certificate on a single IP.

You can use a single wildcard certificate (supporting all the subdomains you like) with no need for SNI.

Cheers

SpinRite

Keegan R. Griffiths
Location: Australia
Subject: SpinRite and SSDs
Date: 20 Nov 2015 22:41:05
:
Hello Steve,
I have been watching/listening to SN for about 6 months now and absolutely love it. I have a question about SpinRite, in recent podcast some SpinRite stories have mentioned running it on SSDs and I would like to ask if and how SpinRite can repair issues on SSDs as it was developed for mechanical drives that are quite different to their solid state counterparts.
Keep up the great work, I hope Leo and yourself continue this wonderful service for many years to come.