Security Now! #511 - 06-09-15

Q&A #214

This week on Security Now!

- Where's the patches? Patch Tuesday?
- Federal backdoor development funding
- The massive 4.1 OPM breach
- A real HDD firmware bootkit
- iOS v9
- "Let's Encrypt" news
- A new certificate authority
- Miscellany and a great Q&A

No explanation needed

Security News

Patch Tuesday??... but nothing posted yet from Microsoft.

House Overwehelmingly Passes Amendments Blocking Funding For Undermining Encryption

- https://www.techdirt.com/articles/20150603/17332431213/house-overwehelmingly-passes-amendments-blocking-funding-undermining-encryption.shtml
- By a 383 to 43 vote, the US House of Representatives voted in favor of an amendment to an appropriations bill which would block the funding for the NIST (National Institute of Science and Technology) to work with the NSA and CIA on undermining or backdooring encryption.

Federal Government Suffers Massive Hacking Attack

- http://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident
- http://www.huffingtonpost.com/2015/06/04/government-data-breach_n_7514620.html
- http://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html
- http://www.politico.com/story/2015/06/personal-data-of-4-million-federal-employees-hacked-118655.html
- Hackers broke into the U.S. government personnel office and stole identifying information of at least 4 million federal workers. The Department of Homeland Security said in a statement Thursday that at the beginning of May, data from the Office of Personnel Management and the Interior Department was compromised. <quote> "The FBI is conducting an investigation to identify how and why this occurred," the statement said.
- None of the data that was exfiltrated was encrypted.
- OPM, CIO, Donna Seymour said:
    - "Encryption and data obfuscating techniques are new capabilities that we're building into our databases."
- (... and they want us to turn over a spare set of keys to our encryption. No thank you.)

Federal Data Breach: Can the Government Protect Itself From Hackers?

- http://www.nbcnews.com/tech/security/federal-data-breach-can-government-protect-itself-hackers-n370556
- Richard Blech, CEO of cybersecurity firm Secure Channels, which works with many federal agencies:
    - "It's not even the money, as much as the process involved; everything gets caught in government glue."
    - "I've worked with these guys, and you have to go through layers and layers of groups and committees to get anything done. It practically takes an act of Congress to change the computer system."
    - Blech said, he is "mystified" the data in these federal breaches are not encrypted.

- Government networks are an exponentially growing sprawling mess and they are nearly impossible to protect.
- The EINSTEIN intrusion detection system senses network behavior events. But if you don't know what's normal... how can you detect what's abnormal?

MalwareTech SBK - A Bootkit Capable of Surviving Reformat

- http://www.malwaretech.com/2015/06/hard-disk-firmware-rootkit-surviving.html
- <paraphrased> Since I got into firmware hacking, I've been working on a little project behind the scenes: A hard disk firmware based rootkit which allows malware to survive an operating system re-install or full disk format. Unfortunately I can't post a proof of concept for many reasons (people have even contacted me just to tell me not to post it), so instead I've written a presentation overviewing and explaining the rootkit, which I've dubbed MT-SBK (Superpersistent Boot Kit.)

  The general purpose of MT-SBK is to provide a "framework" for my previous project, TinyXPB, A demonstration bootkit. This new firmware framework enables my TinyXPB to be stored and loaded from within the hard disk firmware, preventing it from being removed by: antiviruses, operating system re-installs, or even full disk reformats.

  This rootkit is designed for a major brand of hard disk and can infect the firmware from within the operating system (no physical access required), it's also completely undetectable to software running on the host computer.

  Once it's installed, the only way to remove MT-SBK is by replacing that hard disk's PCB or connecting an EEPROM programmer directly to the flash chip and flashing it with the original firmware.
- http://malwaretech.net/MTSBK.pdf

iOS 9

- 6-digit passcodes under iOS v9.
- iPad split screen
- Keyboard improvements - text editing and trackpad mode with two fingers.
- Bill (@BillyInDallas) As with all previous OS X releases, 10.11 defaults with the firewall off.

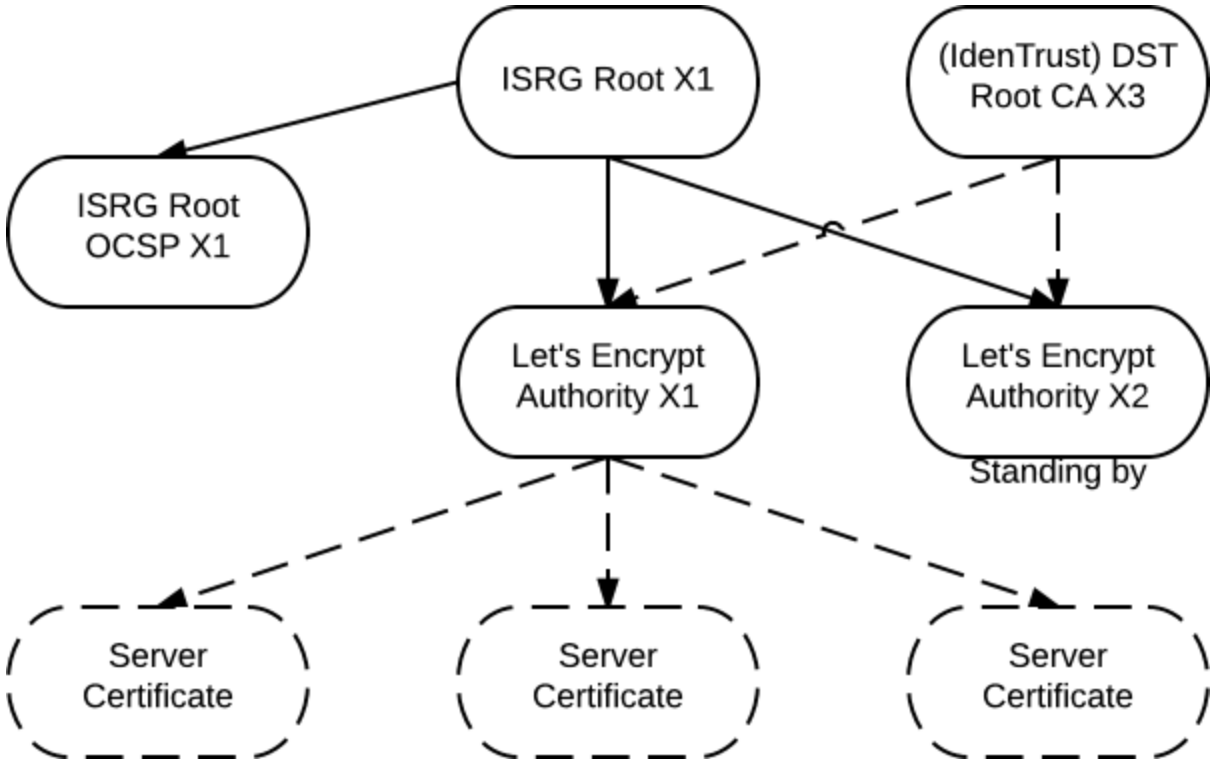
Amazon applies to become a Certificate Authority (CA)

- The Amazon PKI to be run by Amazon Web Services.
- Makes sense for them to offer certs for AWS properties.
- Publicly known to have applied to be included in the Mozilla and Android root stores.
- Microsoft and Apple applications are not public. But it's certainly likely.
- Proposed certs to be offered:
  - Standard and EV certs.
  - Roles:
    - Server authentication
    - Client authentication
    - email (both signing and encrypting)
    - Code signing.

- Certs to be sold to the general public worldwide w/o any restrictions.

Let's Encrypt generated its Root and Intermediate certificates (last Thursday)

- https://letsencrypt.org//2015/06/04/isrg-ca-certs.html
- Intermediate certs cross-signed by IdenTrust to bootstrap until LE's root is in all root stores.



BBC News: UK sells off unused net addresses

- http://www.bbc.com/news/technology-32826353
- The UK government has started selling off internet addresses that it no longer uses.
- The first group of 150,000 addresses has been snapped up by a Norwegian firm called Altibox for about £600,000.
- If the UK government sells off all the surplus addresses it owns it could get up to £15m.
- The UK's Department of Work and Pensions obtained a full Class 'A' network in 1993.
- Earlier this year, the DWP initiated a project to see how many of these IP addresses could be freed.
- It's investigation suggested that 70% of the 16,777,216 addresses are in use by the UK government's internal network, leaving about five million free for disposal.
- IPv4 Market Group
  - http://ipv4marketgroup.com/
  - Sandra Brown, President said:
  - "Regional caches of IPv4 addresses have all but run dry, meaning many firms have to look elsewhere for them."
  - "Trading in IPv4 had been brisk in Europe because the organisation that oversees net addresses in the region had approved policies that allowed transfers. In the busiest months, about two million IPv4 addresses were being traded in Europe."
  - "Supply has met demand, but we are reaching a point where supply is about to fall

short and we have seen prices escalate because of that."
    - Single IP addresses sold in volume were going for $11 (£7), though "quantity discounts" apply for large deals.
    - Sandra indicated that the sense in the industry is that another five to ten years will be needed for most of the conversion to take place. At this time only pilot programs are underway.
- Some companies are analyzing, consolidating, freeing up and selling their IPv4 space in order to fund their migration to IPv6.

Mozilla's SSL/TLS Server Configuration Page

- https://wiki.mozilla.org/Security/Server_Side_TLS
- Description of logic used in setting cipher choice priorities
- Wizard for generating server config files
- LOTS of interesting charts, comparisons and tables

SuperCapacitor News:

- Supercapacitors Take Huge Leap in Performance
- http://spectrum.ieee.org/nanoclast/semiconductors/materials/supercapacitors-take-huge-leap-in-performance
- New Graphene-based super-capacitor
- 131 watt-hours per kilogram... 4x the previous record for graphene-based supercaps.
- Today's Li-Ion is ataround 200 Wh/Kg

Media Update:

Mr. Robot was a MASSIVE success with our listeners.

Psy-Fi: Netflix new 12-episode series "Sense8"

- Only the gay people seem to be having any sex
    - (and even then, VERY little is left to the imagination.)
- Unbelievable plot mistake made halfway though the final (12th) episode!

Ridley Scott's "The Martian" first trailer

- https://www.youtube.com/watch?v=Ue4PCI0NamI
- https://www.youtube.com/watch?v=-8WIzEHxKAA

SQRL:

Mind-Blow of the week...

SpinRite:

John McCarthy in Buffalo, New York
Subject: SpinRite Saved Newspaper Publishers Hard Drive Data
Date: Fri, 05 Jun 2015 14:01:22 -0000

Steve (and crew)

As the Chief Stationary Engineer (aka head boiler room guy) for a major metropolitan newspaper in western New York State and a proud owner of SpinRite for many years, I've got a testimonial that's "one for the books." Yesterday I received a rather panicked call from the head our company's IT support crew.

Usually such calls would involve cooling issues in the server room, a heat complaint in his office, or even worse, a plugged toilet in the men's room. Low and behold it was neither. Instead he asked if I had "that recovery program that you had told me about?"

"Sure. Why? What's up" I responded as I always carry a copy of SpinRite with me (though not on my tool belt).

He went on to explain that the paper's Publisher/President's Windows 7 laptop REFUSED to boot past the splash screen. Remembering my glowing recommendation of SpinRite he hoped he could borrow it for a last ditched effort to recover The Boss's data, as none of their utilities could fix the problem. Confidently, I gave him the CD with the agreement that if successful he would purchase the "corporate version" of your "magic disk." He agreed.

Two hours later: BANG IT WORKED LIKE A CHARM!!! He was able to boot off the previously unresponsive drive, backup all the data, and even make an image of it for later transfer to a replacement SSD. The long and the short of it is you should be hearing 4 "Yabba Dappa Do's" soon, as the entire IT department was simply astounded by your excellent product!!!

I've been listening and promoting SecurityNow and the TWIT network for many years, and while I have the opportunity, I want to thank both you and Leo for allowing me to NOT BE the dumbest guy in the server room even if I'm the only one holding a pipe wrench.

Next week I'll clue them in on Harry's shavers!!!

Thanks Again,
John