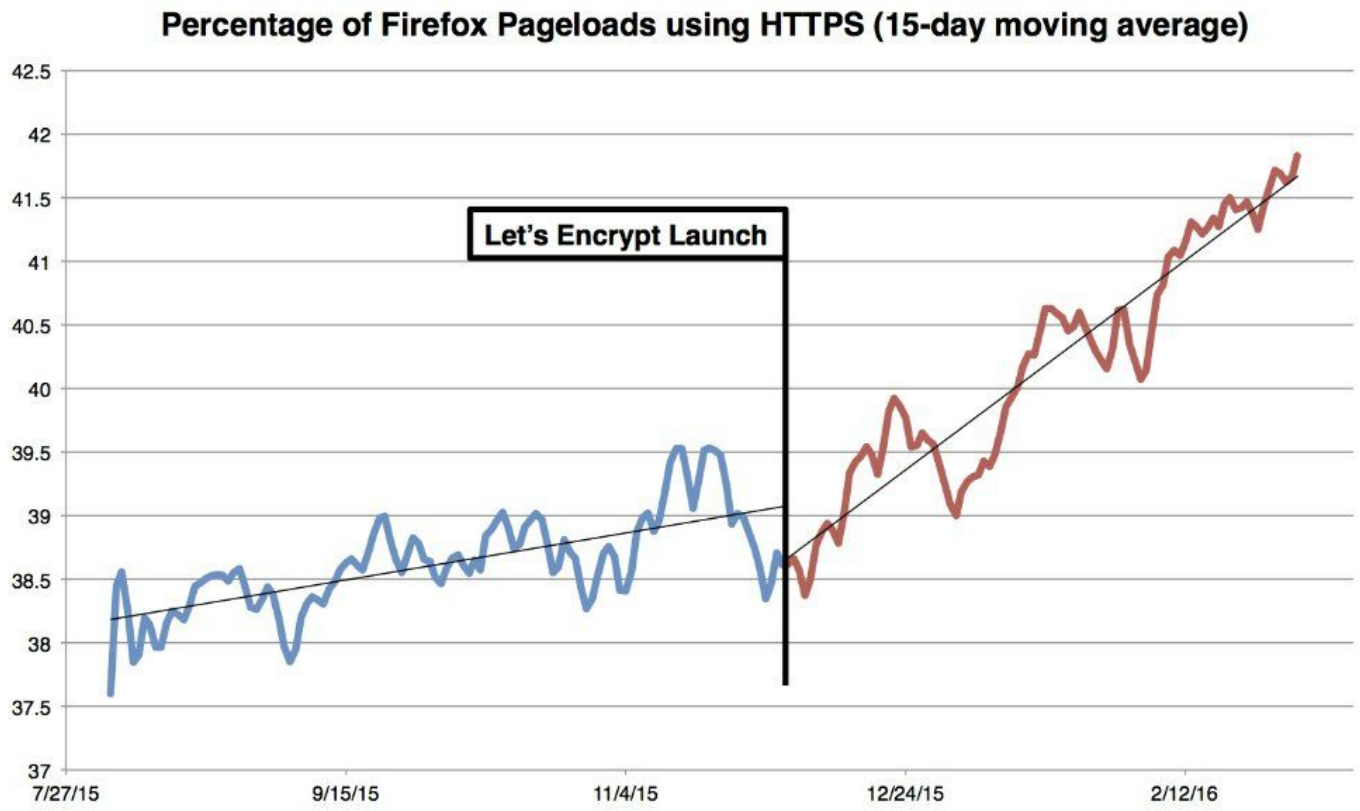
Security Now! #551 - 03-15-16

Q&A #230

This week on Security Now!

- Encryption -- Dispute or Dispute?
- John Oliver Sunday Night
- David Pogue on TWiT and my Blog post
- A specific IoT nightmare example
- BleepingComputer gets sued and asks for help
- A new and horrifying DDoS attack amplifier
- Microsoft pushes Windows 10 even harder
- Some Windows Update Update Follow-up Follow-up
- Some miscellany, fun and 10 questions from our followers



Mozilla @mozilla
Bending the curve for HTTPS adoption, which has quadrupled since @letsencrypt launched!

Security News

The DOJ's Nuclear Option in Apple v FBI
http://www.reuters.com/article/us-apple-encryption-sourcecode-analysis-idUSKCN0WH01N

- The legal rhetoric keeps escalating.
- The latest filing in the legal war between the planet's most powerful government and its most valuable company gave one indication of how the high-stakes confrontation could escalate even further: In what observers of the case called a carefully calibrated threat, the U.S. Justice Department last week suggested that it would be willing to demand that Apple turn over the "source code" that underlies its products as well as the so-called "signing key" that validates software as coming from Apple.

The Apple issue has always been a "data-at-rest" issue, which is distinct from "data-in-flight"...

WhatApp is also in the DoJ's crosshairs
http://mobile.nytimes.com/2016/03/13/us/politics/whatsapp-encryption-said-to-stymie-wiretap-order.html?&mod=djemCIO_h&_r=1

- New York Times:
  WASHINGTON — While the Justice Department wages a public fight with Apple over access to a locked iPhone, government officials are privately debating how to resolve a prolonged standoff with another technology company, WhatsApp, over access to its popular instant messaging application, officials and others involved in the case said.

  No decision has been made, but a court fight with WhatsApp, the world's largest mobile messaging service, would open a new front in the Obama administration's dispute with Silicon Valley over encryption, security and privacy.

  WhatsApp, which is owned by Facebook, allows customers to send messages and make phone calls over the Internet. In the last year, the company has been adding encryption to those conversations, making it impossible for the Justice Department to read or eavesdrop, even with a judge's wiretap order.

  As recently as this past week, officials said, the Justice Department was discussing how to proceed in a continuing criminal investigation in which a federal judge had approved a wiretap, but investigators were stymied by WhatsApp's encryption.

THE HILL: Week ahead: Senators close to unveiling the "Burr-Feinstein" encryption bill
http://thehill.com/policy/cybersecurity/272734-week-ahead-senators-close-to-unveiling-encryption-bill

- "Our" California senator Diane Feinstein & North Carolina's Richard Burr.
- The Hill: While some argue that a judge should order WhatsApp to help investigators obtain the information they need in a readable format, others are hesitant to escalate the dispute given that some lawmakers are expected to introduce legislation to give law enforcement access to encrypted data as early as this week.

Meanwhile...

John Oliver, Sunday night, on Encryption:
https://www.youtube.com/watch?v=zsjZ2r9Ygzw

David Pogue on TWiT was asking precisely the right questions.

- We need to separate the issue of -encryption- from -access-.
- http://steve.grc.com

Krebs on Security: IoT
Cisco's Talos Team: http://blog.talosintel.com/2016/02/trane-iot.html
Brian Krebs: http://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/

- Before purchasing an "Internet of things" (IoT) device — a thermostat, camera or appliance made to be remotely accessed and/or controlled over the Internet — consider whether you can realistically care for and feed the security needs of yet another IoT thing.

  In April 2014, researchers at Cisco alerted HVAC vendor Trane about three separate critical vulnerabilities in their ComfortLink II line of Internet-connected thermostats. These thermostats feature large color LCD screens and a Busybox-based computer that connects directly to your wireless network, allowing the device to display not just the temperature in your home but also personal photo collections, the local weather forecast, and live weather radar maps, among other things.

  Cisco researchers found that the ComfortLink devices allow attackers to gain remote access and also use these devices as a jumping off point to access the rest of a user's network. Trane has not yet responded to requests for comment.

  One big problem is that the ComfortLink thermostats come with credentials that have hardcoded passwords. By default, the accounts can be used to remotely log in to the system over "SSH."

The two other bugs Cisco reported to Trane would allow attackers to install their own malicious software on vulnerable Trane devices, and use those systems to maintain a persistent presence on the victim's local network.

Bleeping Computer being sued over a negative review of "SpyHunter." Asks for help.
http://www.bleepingcomputer.com/announcement/frivolous-lawsuits/help-bleepingcomputer-defend-freedom-of-speech/

TFTP devices in DDoS amplification attacks

- "Evaluation of TFTP DDoS amplification attack"
- Published in Computers & Security, March 2016, Pages 67-92
- The latest vector for DDoS amplification.
- Researchers at Edinburgh Napier University have discovered that the TFTP protocol (Trivial File Transfer Protocol) might be abused in a similar way.
- Unlike DNS and NTP, TFTP has no business being exposed on internet-facing systems. Yet port scanning research indicated that there about 599,600 publicly open TFTP servers.
- TFTP offers a higher amplification factor than other internet protocols. (60x)
- TFTP uses UDP and well-known port 69.
- TFTP is small & easy to implement.
- Lacks advanced features offered by more robust file transfer protocols.
- Only reads & writes files from or to a remote server.
- Cannot list, delete, or rename files or directories.
- HAS NO PROVISIONS FOR USER AUTHENTICATION.
- Wikipedia: Today TFTP is generally only used on local area networks (LAN).
- https://en.wikipedia.org/wiki/Trivial_File_Transfer_Protocol

Last week's KB3035583 <sigh>

- Yesterday's security update KB3139929 also includes KB3146449.
- The page for the latter states: "This update adds functionality to Internet Explorer 11 on some computers that lets users learn about Windows 10 or start an upgrade to Windows 10."
- So Microsoft is now hiding their over-the-top push to force users to Windows 10 in security updates.
- Woody Leonhard wrote, "putting an ad generator inside a security patch crosses way over the line."
  http://www.infoworld.com/article/3042155/microsoft-windows/windows-patch-kb-3139929-when-a-security-update-is-not-a-security-update.html

GRC's Server 2008 R2

- UNBELIEVABLE that Microsoft would modify GRC's production server IN ANY WAY!

On the funny side:

- Chris Pifer (@selfuntitled)
  The ad block arms race escalates again, an ad block, blocker blocker:
  http://reek.github.io/anti-adblock-killer

Errata:

Setting up new Windows 7 machines

- Anytime Upgrade has been shutdown to force migration to Windows 10
- http://bit.ly/no-gwx
- Windows Update Update (google that)
- 1st search result: How to update the Windows Update Agent to the latest version
- https://support.microsoft.com/en-us/kb/949104
- http://bit.ly/wupup

Miscellany

HSF Update

- Universal positive results
- Taurine helps some, hinders others.
- L-Tryptophan … promising replacement for Taurine but ONLY w/o anti-depressants.
- FDA and "Healthy Sleep Formula"

House of Cards

- Heard Leo during TNS pre-show... started on Season 3. Written for me!
- Robin Wright is phenomenal!

The Magicians (on SyFy)

SpinRite