Security Now! #562 - 05-31-16

IoT Infancy

This week on Security Now!

- Over-the-top Feinstein-Burr encryption bill dies in the Senate
- Google's fair use API defense prevails
- Google's increasing pressure on its Android partners
- Bluecoat Systems obtains an Intermediate CA cert from Symantec/Verisign
- The insecurity of add-on Laptop bloatware
- The insecurity of Laptop custom updating software
- A promised update on SQRL

- Rapid7's sobering analysis of Internet-connected baby monitors

- (After the End): Healthy Sleep Formula news
    - Including an unexpected phone call from France

Security News

Nutty Feinstein-Burr encryption bill has lost support in Congress

http://www.reuters.com/article/us-usa-encryption-legislation-idUSKCN0YI0EM

- After a rampage that left 14 people dead in San Bernardino, key U.S. lawmakers pledged to seek a law requiring technology companies to give law enforcement agencies a "back door" to encrypted communications and electronic devices, such as the iPhone used by one of the shooters.

  Now, only months later, much of the support is gone, and the push for legislation dead, according to sources in congressional offices, the administration and the tech sector.

  Draft legislation that Senators Richard Burr and Dianne Feinstein, the Republican and Democratic leaders of the Intelligence Committee, had circulated weeks ago likely will not be introduced this year and, even if it were, would stand no chance of advancing, the sources said.

- The short life of the push for legislation illustrates the intractable nature of the debate over digital surveillance and encryption, which has been raging in one form or another since the 1990s.

- The CIA and NSA were ambivalent, according to several current and former intelligence officials, in part because officials in the agencies feared any new law would interfere with their own encryption efforts.

- A half dozen people familiar with the White House deliberations said they were hamstrung by a long-standing split within the Obama Administration, pitting Comey and the DOJ against technology advisors and other agencies including the Commerce and State Departments.

- They also said there was reluctance to take on the tech industry in an election year.

Google's Fair Use defense prevails

- Jury in Oracle suit unanimously finds Google's use of Java APIs in Android was fair use; Oracle vows to appeal
- http://arstechnica.com/tech-policy/2016/05/google-wins-trial-against-oracle-as-jury-finds-android-is-fair-use/
- Thursday (of last week): A two-week trial concluded with three days of jury deliberations, after which its federal jury unanimously deciding that Google's Android operating system

implementation does NOT infringe Oracle-owned copyrights because its re-implementation of 37 Java APIs is protected by "fair use."

- Oracle vowed to appeal.
    - Dorian Daley, Oracle's general counsel, said in a statement: "We strongly believe that Google developed Android by illegally copying core Java technology to rush into the mobile device market. Oracle brought this lawsuit to put a stop to Google's illegal behavior. We believe there are numerous grounds for appeal and we plan to bring this case back to the Federal Circuit on appeal."

- What is Fair Use?
  Stanford Law: In its most general sense, a fair use is any copying of copyrighted material done for a limited and "transformative" purpose, such as to comment upon, criticize, or parody a copyrighted work. Such uses can be done without permission from the copyright owner. In other words, fair use is a defense against a claim of copyright infringement. If your use qualifies as a fair use, then it would not be considered an illegal infringement.

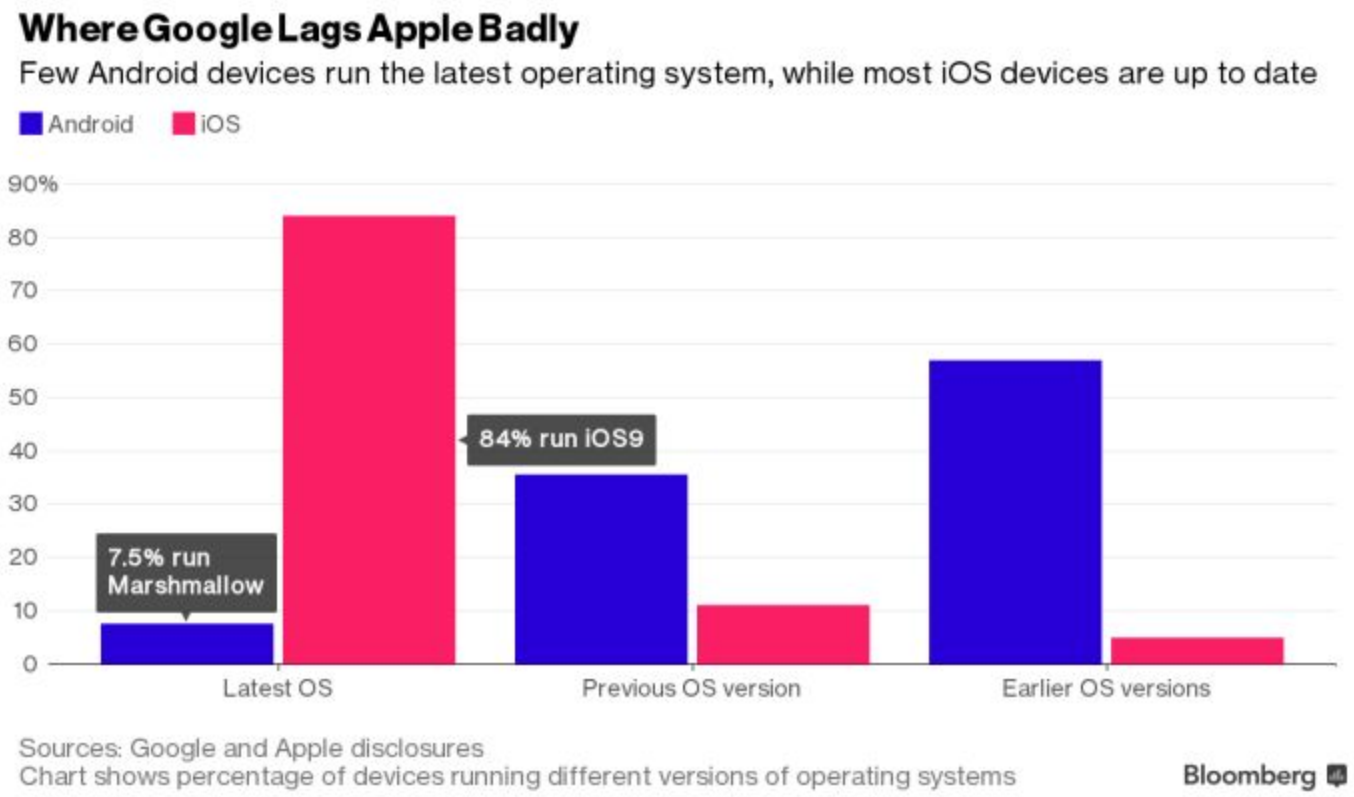
  So what is a "transformative" use? If this definition seems ambiguous or vague, be aware that millions of dollars in legal fees have been spent attempting to define what qualifies as a fair use. There are no hard-and-fast rules, only general rules and varied court decisions, because the judges and lawmakers who created the fair use exception did not want to limit its definition. Like free speech, they wanted it to have an expansive meaning that could be open to interpretation.

  Most fair use analysis falls into two categories: (1) commentary and criticism, or (2) parody. Commentary and Criticism:

- If you are commenting upon or critiquing a copyrighted work — for instance, writing a book review — fair use principles allow you to reproduce some of the work to achieve your purposes. Some examples of commentary and criticism include:
    - quoting a few lines from a Bob Dylan song in a music review
    - summarizing and quoting from a medical article on prostate cancer in a news report
    - copying a few paragraphs from a news article for use by a teacher or student in a lesson, or
    - copying a portion of a Sports Illustrated magazine article for use in a related court case.

- The underlying rationale of this rule is that the public reaps benefits from your review, which is enhanced by including some of the copyrighted material. Additional examples of commentary or criticism are provided in the examples of fair use cases.

Google Steps Up Pressure on Partners Tardy in Updating Android



- http://www.bloomberg.com/news/articles/2016-05-25/google-steps-up-pressure-on-partners-tardy-in-updating-android

- Google is using more forceful tactics. It has drawn up lists that rank top phone makers by how up-to-date their handsets are, based on security patches and operating system versions, according to people familiar with the matter. Google shared this list with Android partners earlier this year. It has discussed making it public to highlight proactive manufacturers and shame tardy vendors through omission from the list, two of the people said. (The people requested anonymity to maintain their relationships with Google.)

- Google is reducing its reliance on the update process too. New features, such as the Allo messaging service, are increasingly packaged as standalone apps, rather than part of a new version of the Android operating system. Users can obtain these, and Google can refresh them, without carrier tests.

- Google is also making some new features compatible with earlier versions of the operating system. Instant Apps, unveiled last week, works on phones running versions as old as Jellybean, which came out in 2012.... so 95 percent of the current Android user base will get access to the newer technology.

- But Google's many efforts may be stymied due to competing interests: Google wants Android phones kept up to date, but carriers want to sell new phones: Bloomberg wrote: "Extra investments of time and money are a hard sell for Android phone makers, which are seeing margins slide and get most of their profits when people buy new phones, rather than update existing devices.

Bluecoat obtains Intermediate CA from Symantec

- https://crt.sh/?id=19538258
- Sometimes you want Snark... so The Register.Co.UK:
  Blue Coat sells network equipment that does just this kind of espionage: the gear intercepts connections to websites and strips the encryption away so secured communications can be monitored. This is useful for corporations that want to keep tabs on their staff at work. Unfortunately, Blue Coat's HTTPS-snooping products have been used by repressive regimes to spy on activists online and quash dissent.

  To tear away the encryption and peek inside people's packets, Blue Coat's man-in-the-middle gear masquerades as legit websites – and this is so much easier to pull off when the manufacturer is an intermediate certificate authority because it will have the flexibility to generate trusted certificates as required. It paves the way for seamless surveillance by Blue Coat-built equipment.

  We asked Blue Coat how it planned to use its new powers – and we were assured that its intermediate certificate was only used for internal testing and that the certificate is no longer in use.

  - The two firms said in a statement: "Symantec has reviewed the intermediate CA issued to Blue Coat and determined it was used appropriately."

  - "Consistent with their protocols, Symantec maintained full control of the private key and Blue Coat never had access to it. Blue Coat has confirmed it was used for internal testing and has since been discontinued. Therefore, rumors of misuse are unfounded."

- STEVE: But... even if not with THIS Intermediate CA, Bluecoat is an HTTPS Proxy building company and ANY GOVERNMENT can purchase that hardware and have any one of their own CAs provide an intermediate certificate for the Bluecoat MITM hardware.

Bloatware Insecurity Continues to Haunt Consumer, Business Laptops

OEM vendor and software version	Manifest Transmitted Over TLS	Signed Manifest	Updates Transmitted Over TLS	Authenticode Validation
Acer	✗	✗	✗	✗
Asus	✗	✗	✗	✗
Dell DFS 2.1.3.1	✓	✗	✓	✗
Dell DFS 2.4.3.0	✓	✗	✓	✓
Dell Update 1.8.114.0	✓	✗	✓	✓
Hewlett-Packard HPSF 8	✗	✗	✓	✓
Lenovo UpdateAgent 1.0.0.4	✗	✗	✗	✗
Lenovo Solution Center 3.1.001	✓	✓	✓	✓

- https://threatpost.com/bloatware-insecurity-continues-to-haunt-consumer-business-laptops/118356/

- Researchers at Duo Labs today published a report on their findings after pulling apart the bloatware from 10 new laptops, all running either Windows 8.1 or Windows 10, including some Microsoft Signature edition machines that are supposed to be bloatware free, but still include some of these components.
- All of these updaters specify their own update manifests where the system grabs a XML file over HTTP (Dell downloads its updates over HTTPS).
- None of the manifests are signed and they don’t use proper engineering practices to make sure the integrity of the manifests is validated properly.

- All of (the manifests) include commands to ensure the updates run properly. A bad guy can simply hijack those commands and execute whatever they wish with system level permission.
- Most of these updaters run with system-level privileges, meaning they're going to bypass any security protection on the machine
- Most are implementation and design issues where things are fundamentally broken by design. They will not be easily mitigated without rewriting how the software works. There are not a lot of controls to prevent this.
- The bloatware in question is primarily there for feature updates for the respective OEM components, things that manufacturers receive monetary incentives to pre-install on computers.
- Some vendors made no attempts to harden their updaters, while others tried to, but were tripped up by a variety of implementation flaws and configuration issues. In total the researchers identified and reported twelve unique, vulnerabilities across all of the vendors, and identified a number of concerning trends:
    - Every vendor shipped with a preinstalled updater that had at least one vulnerability resulting in arbitrary remote code execution as SYSTEM, allowing for a complete compromise of the affected machine.
    - Vendors often failed to make even basic use of TLS, properly validate update integrity, or verify the authenticity of update manifest contents.
    - Vendors sometimes had multiple software updaters for different purposes and different implementations; some more secure than others.
    - The large attack surface presented by ancillary OEM software components makes updater-specific bugs easier to exploit in practice by providing the missing pieces of the puzzle through other tools bundled with their systems.
    - The level of sophistication required to exploit most of the vulnerabilities we found is somewhere between that possessed by a coffee stain on the Duo lunch room floor and your average potted plant - meaning, trivial.

Never10 Stats:

- >35,000 copies downloaded per day
- >777,000 downloaded just from GRC.
- ***Has WILDLY broken every record in GRC's long history of very popular freeware.***

SQRL Update

- SQRL's Identity Management - How it works
  - (Completely missing from FIDO - "Someone else's problem")
- SQRL's Textual Input Control
  - Base56
  - per-line validation
- Bottom of page Logo
- Linux / WINE
  - Logo (unimplemented GDI+ function)
  - Completely non-functional Font mapper
- What's next?
  - "Rekeying" terminology
  - Cleaning up final bits
  - Linux / WINE

Miscellany: Three Tweets

Pat @thetweetguy99

Steve, I recently listened to your discussion of Chrome vs Firefox in SN episode 557 and I was struck by your comment that "most users would be better served by Chrome." I'm a Sys Admin for a small company (~50 employees) and I check all of our end-user machine logs each week. In reviewing those logs, two things stand out each and every week - (1) Internet Explorer is by far the application that crashes the most, and (2) virtually all of the malware events we experience are drive-by infections by legitimate websites hosting malicious ads. So I thought, it's time to deploy Chrome to everyone. They've made it fairly easy for enterprises to deploy (msi installers, group policy templates, etc). and so I've begun rolling out test installations of Chrome *with* our favorite ad blocker preloaded (uBlock Origin). We're already seeing positive results, even had one user go back to a website that tried to download malicious code onto his machine via Internet Explorer just 30 minutes prior, and was pleased to see that no installation was even attempted when using Chrome w/uBlock Origin.

Rob Woodruff @fulori

Hey Steve I just listened to the podcast from Tuesday and Carl in Indiana with a Netgear cable modem probably needs to get a firmware update. I've seen a lot of Netgear cable modems with Comcast have that exact same problem, whereas the SMC cable modems that Comcast provided prior to the Netgear cable modems work just fine. Comcast worked with Netgear to develop a firmware update that was supposed to alleviate that symptom. I'm not sure who Carl's Cable modem provider in Indiana is, but he might want to check with them to see about a firmware update. Either that, or ask for a different brand of cable modem.

Stijn Crevits / @DezeStijn
Steve,
Don't you think NOT allowing the filtering of Win Updates through APIs is more secure?
For one, malware would otherwise be able to block Security Updates.
Kr, Stijn

SpinRite

Sitbit
Location: London, Ontario, Canada
Subject: YAST! (Not a Suse package manager!)
Date: 25 May 2016 09:05:32
:
Yet Another SpinRite Testamonial!

Hello Steve and Leo!

Love you guys; the show is fantastic, yadda etc.

Just a short and sweet SpinRite story. I had an old 320 GB spinning disk salvaged from a laptop that I used to store some of my data. It wasn't terribly important, but I didn't want to lose it, so I had it mirrored to a backup drive. Well, the drive failed, so the directory I had it hanging off of showed up as empty so my mirroring software dutifully DELETED MY BACKUP, thinking the files had been purposely removed. Long story short, I caused Steve to hear a Yabba-Dabba-Do and two hours later my drive was back in action.

Thank you for this wonderful product!
Thanks again,

Sitbit.

IoT (in its) Infancy

http://cve.mitre.org/

CVE - Common Vulnerabilities and Exposures (CVE)

- CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known cyber security issues. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this "common enumeration."

UPDATE

The recent explosion of Internet-enabled devices—known as the Internet of Things—as well as the propagation of software-based functionality in systems has led to a huge increase in the number of CVE requests we have been receiving on a daily basis. We did not anticipate this rate of growth, and, as a result, were not as prepared for the latest surge in requests over the past 12 months as we had hoped. The result has been some of the delay in CVE assignments that the software security community has recently witnessed. We recognize the inconvenience that has resulted, and are working hard to come up with a solution. Last week, we proposed a possible option to our CVE Editorial Board, but some members raised concerns about the approach, and we have withdrawn it from consideration. We are working diligently to come up with a solution that will meet the needs of all the various use cases of CVE.

Home IoT devices are wide open, security provider discovers

http://www.networkworld.com/article/3051691/internet-of-things/home-iot-is-wide-open-security-provider-discovers.html

Bitdefender recently examined four popular IoT devices:

The popular WiMo products used to control lights and wallsockets.

- They found that the switch communicates with the smartphone without authentication. The only thing encrypted is the password, but the password is composed of elements of the MAC address and the device ID, both which are already transmitted without encryption... since only the password is encrypted. (And that encryption uses a preset knowable static key.)
- Six months after notifying the vendor, nothing has changed.

The Lifx Bulb was another Wi-Fi device tested.

- Bitdefender found that its hotspot function suffered from insufficient authorization and authentication. When setting up the mood-effect bulb, a "bootstrap" hotspot is created to manage initial configuration with the phone. But by later creating an identical fake

"bootstrap" hotspot, a hacker could capture the username and password of the existing broader actual Wi-Fi network.
- As with the WeMo, that vulnerability has not been fixed after six months.

LinkHub, the third device, also ran into hotspot issues.
- The GE Link lightbulb hub, for remote control of lighting, lacked transport encryption when configuring it through the hotspot. The data is transmitted in clear text.
- No repair of this six months after notifying the vendor.

The fourth, the MUZO Cobblestone audio receiver, fared slightly better than the others in that some of its vulnerabilities have been repaired since the tests.
- However, the initial issue was pretty scary. The device created a new WiFi hotspot that was never disabled. Although users could create a password, they were not told that. Although that issue is now fixed, a second issue—a open telnet service with the User ID of "admin" and password of "admin"—still exists. This allows open access to the home's original Wi-Fi network, bypassing the any need for credentials.

First-generation IoT devices are trying to do the impossible:
Be a limited use purpose-specific appliance... with all of the sophisticated communications and connectivity power of a general purpose computer hidden inside... but without ANY of the responsibility "baggage" that all of our experience has taught us NECESSARRILY comes along with any powerful, connected, general purpose computer.
It really is a brave new world when a lightbulb is running a telnet server.

Rapid7 put it perfectly:
For our purposes, we can think of a "Thing" with "Internet" as simply any device, regardless of size, use, or form factor, that contains a CPU and memory, runs software, and has a network interface which allows it to communicate to other devices, usually as a client, sometimes as a server. In addition, these Things tend not to resemble traditional computers. They lack a typical keyboard and mouse interface, and they often have a user interface not centered around a monitor or other text-filled screen. Finally, these devices are marketed and treated as if they are single purpose devices, rather than the general purpose computers they actually are.

This last distinction is often the most dangerous one to make when it comes to deploying IoT devices. In his keynote address to the Chaos Computer Club titled "Lockdown: the coming war on general- purpose computing", Cory Doctorow makes the case that with today's technology and current computer science thinking, we cannot yet create a computer that is anything other than a general purpose computer. End users may have devices that are nominally prohibited from performing certain actions according to the manufacturer, and those manufacturers sometimes go to great lengths to foil modification efforts. In the end, though, it is not possible

to build and sell a computing device that cannot be coerced into rebelling against a manufacturer's intentions.

The problem is...
Any system based upon a stored-program MUST be able to have that program changed when bugs and security vulnerabilities are found. But that same need for the WARE to be SOFT inherently opens the device to abuse.

Next week we'll look at what Rapid7 found when they looked closely at Baby Monitors. The details of the vulnerabilities should be of great interest to our listeners.

Healthy Sleep Formula Update

- Seriphos
    - Interplexus is unhappy with the caution I immediately posted on Amazon.

- Enerphos
- T.E. Neesby, Inc. / Fresno
  It was good to talk with you last week! Thank you for reaching out to us and giving us a heads up on the new demand we can expect for Enerphos. Brian worked all weekend making more product. We have a few hundred bottles in route to Emerson now and expect to be able to ship more by Friday. We will keep you informed of our shipments to our suppliers and you can keep us updated on the feedback you get from your readers.

  Thank you again for your thoughtfulness in contacting us directly.
  Sheryl

- Amazon?? Anyone within reach of my voice have any influence over what Amazon carries?