Security Now! #559 - 05-10-16

Dumb SmartThings

This week on Security Now!

- Today's Mega Patch Tuesday for Windows
- Closing the chapter on Dr. Craig Wright
- Lenovo, Microsoft and Qualcomm all in separate doghouses.
- Another fun bit on Curl Bashing
- The unintended consequences of "Terrorist Math."
- An expensive but possibly useful gizmo
- Some catchup-update miscellany, including:
  - The Temperfect Mug actually arrived
  - A significant breakthrough with the Healthy Sleep Formula
  - Last week's "The Sequence" puzzle/game
  - The new companion Android software for the Zeo is released
  - Plus a few more tidbits... then...
- A look at Samsung's Not Ready for Prime Time "SmartThings."

Security News

Windows Patch Tuesday Bonanza!

- Critical RCE in Internet Explorer
  - This security update resolves vulnerabilities in Internet Explorer. The most severe of the vulnerabilities could allow remote code execution if a user views a specially crafted webpage...
- Critical RCE in Microsoft Edge
  - This security update resolves vulnerabilities in Microsoft Edge. The most severe of the vulnerabilities could allow remote code execution if a user views a specially crafted webpage...
- Critical RCE in JScript ad VBScript
  - This security update resolves vulnerabilities in the JScript and VBScript scripting engines in Microsoft Windows. The vulnerabilities could allow remote code execution if a user visits a specially crafted website.
- Critical RCE in Microsoft Office
  - This security update resolves vulnerabilities in Microsoft Office. The vulnerabilities could allow remote code execution if a user opens a specially crafted Microsoft Office file.

- Critical RCE in (some generic) Microsoft Graphics Component
  - This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a specially crafted website.
- Critical RCE in Windows Journal
  - This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted Journal file.
- Critical RCE in Windows Shell
  - This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if an attacker successfully convinces a user to browse to a specially crafted website that accepts user-provided online content, or convinces a user to open specially crafted content.
- And continuing like that for:
  - IIS
  - Windows Media Center
  - Windows Kernel
  - Microsoft PRC
  - Kernel-Mode Drivers
  - Adobe FLash Player
  - .Net Framework
  - Virtual Secure Mode
  - Volume manager

Closing the chapter on Dr. Craig Wright

One week ago: Steve Gibson @SGgrc

- "I sure hope this clown is NOT Satoshi. Get a load of this latest spew of nonsense: ...."

And now, finally… http://www.drcraigwright.net/

I'm Sorry

I believed that I could do this. I believed that I could put the years of anonymity and hiding behind me. But, as the events of this week unfolded and I prepared to publish the proof of access to the earliest keys, I broke. I do not have the courage. I cannot.

When the rumors began, my qualifications and character were attacked. When those allegations were proven false, new allegations have already begun. I know now that I am not strong enough for this.

I know that this weakness will cause great damage to those that have supported me, and particularly to Jon Matonis and Gavin Andresen. I can only hope that their honour and credibility is not irreparably tainted by my actions. They were not deceived, but I know that the world will never believe that now. I can only say I'm sorry.

And goodbye.

Microsoft, Windows 7, ASUS and SecureBoot

- http://m.windowsitpro.com/windows-10/asus-issues-support-workaround-non-booting-windows-7-computers-affected-kb3133977
- ASUS motherboards enable Secure Boot by default.
- Secure Boot was introduced with Vista, so it's always been built into the successor Windows 7.
- Therefore, when Windows 7 systems are installed on ASUS motherboards having Secure Boot enabled, those Win7 OSes are configured with Secure Boot by default.
- Then... Microsoft reclassified KB3133977 from Optional to Recommended.
- What does KB3133977 do? It removes Windows 7 support for secure boot since it is not longer "supported."
- After that, when the next reboot, affected ASUS motherboard users were greeted with a frightening BIOS red warning screen stating: "Secure Boot Violation - The system found unauthorized changes on the firmware, operating system or UEFI drivers."

Privilege Escalation Vulnerabilities within Lenovo Solution Center

- https://support.lenovo.com/us/en/product_security/len_4326
- Vulnerabilities were discovered in the Lenovo Solution Center (LSC) software which could allow a remote attacker or local user to execute arbitrary code with SYSTEM privileges. We urgently completed an assessment of this issue and prepared and tested fixes that eliminate these vulnerabilities. These updates are now posted and available for download through various update channels described in the mitigation strategy below.

Critical Qualcomm flaw puts millions of Android devices at risk

- http://thehackernews.com/2016/05/android-hacking.html
- This was patched for current devices by Google's May Day Android Security Patch.
- However, the vulnerability was introduced in 2011 when Qualcomm released a new set of APIs for a network manager system service with an updated "netd"daemon. Qualcomm's changes to netd added some new network capabilities, including tethering. But the modification also introduced a critical flaw that allows low-privileged applications to obtain access to private data including SMS and call history, changing system settings, disabling the lock screen, etc.
- The good news is, it's a local privilege elevation that requires a malicious application to be installed. But it does break application containment.
- The vulnerability is most worrisome on devices running Android 4.3 Jelly Bean, and earlier, that are unlikely to ever be patched. But all unpatched devices are at risk of exploitation.
- NOTE: The FCC and FTC are both asking Apple, Google and others for clarification of "the factors they consider in deciding whether to patch a vulnerability on a particular mobile device."

KB3035583 Disables Windows 10 Upgrade Blocking?

http://windowsitpro.com/windows-10/kb3035583-disables-windows-10-upgrade-blocking

- Anecdotal reports only.
- Didn't hear from a single user of Never10. (312K downloads / >4600/day)
- Windows IT Pro, one day later follow-up:
- This issue has only be reproducible in a few reported instances and does not seem to be widespread. If you are experiencing this problem, let us know so we can help determine if its environment or configuration specific.

Still more Curl Bashing:

- https://www.idontplaydarts.com/2016/04/detecting-curl-pipe-bash-server-side/
- Phil: “Detecting the use of "curl | bash" server side”
- Installing software by piping from curl to bash is obviously a bad idea, and a knowledgeable user will most likely check the content first. So wouldn't it be great if a malicious payload would only render when piped to bash? A few people have tried this before by checking for the curl user agent which is by no means fail safe - the user may simply curl the url on the command line revealing your malicious code. Luckily the behavior of curl (and wget) changes subtly when piped into bash. This allows an attacker to present two different versions of their script depending on the context :)
- "sleep 10" will cause bash to sleep for 10 seconds... but piping to a file won't interpret.

Ivy League economist ethnically profiled, interrogated for doing math on American Airlines flight

https://www.washingtonpost.com/news/rampage/wp/2016/05/07/ivy-league-economist-interrogated-for-doing-math-on-american-airlines-flight/

Economist Removed from Plane for Algebra

http://marginalrevolution.com/marginalrevolution/2016/05/economist-removed-from-plane-for-algebra.html

(Generated more than 4700 comments.)

Gizmodo: When Your Internet Goes Out, This Smart Plug Resets Your Router Until It Works Again

http://gizmodo.com/when-your-internet-goes-out-this-smart-plug-resets-you-1774424411

- <quote> When your internet goes out, resetting your wi-fi router and cable modem often seems to fix the problem. Instead of getting up from the couch to fiddle with power cords, why not let a tiny outlet adapter power cycle your hardware for you?
- You might balk at the ResetPlug's $60 price tag, but it's not an awful idea for people who hate having to get up when the internet goes out. You plug the device into an outlet, and then plug your wi-fi router, modem, or both, into the ResetPlug itself. It constantly monitors your home's internet connection, and when it detects a problem, it automatically cycles power to your router and modem until the internet returns.
- http://resetplug.com/
- Do you have devices that depend on your WiFi to be working?
  - Security cameras / Thermostat / Smart appliances / Smoke alarms
  - CO alarms / Smart TV/DVR / Remote computers / Sensors / Security alarm
  - Smart lighting / File servers / Other IoT devices
- (Patent pending... because that's an invention.)

Miscellany

Temperfect Mug Arrived!

- I purchased and received mug #2 - Titiana (Titanium dioxide) with a very nice hand-written note.

A significant breakthrough in the Healthy Sleep Formula

The Sequence:

- #22 was so fun.
- #23 was amazing!
- #29 currently staring at level #29…

Martin Bergek @martinbergek
@SGgrc I just had to complete level 22 before this week's SN. Brilliant! No more game reviews today, right? I need to work :-)

Hi Martin.
Yes!... #22 and #23 are truly wonderful. I solved #29 using only 3 of the provided 7 pieces, using a trick I had noticed way back on an earlier level. :)

No more puzzles today. We're not finished with this one yet! :)

The "Companion for Zeo" is now at v1.0.1: See https://www.grc.com/zeo.htm

How am I cooling my HDD's in the new MegaMachine?

- Arctic Alumina Thermal Adhesive 5g
- http://www.amazon.com/dp/B0009IQ1BU
- Carefully peel the adhesive label off the drive.
- If there's a vent hole be sure to leave it uncovered.

Transferring domains with time remaining

- From Network Solutions to Hover - pay for one year.

SpinRite

Kev Blythe
Subject: SpinRite Success Story

Hello Steve. I would to say thank you for that magical item of software you call SpinRite.

A local garage called in a panic, a old diag laptop had failed with a BSOD and was going round in circles (like the owner). So I picked it up for a look.

I confirmed a hard drive issue, and having worked in a local PC repair shop where I often witnessed the proof of the power of your software to get hard drives back into a boot-able state, I headed to GRC for my own copy of SpinRite. I grabbed a copy and before lunchtime the machine was repaired, imaged, returned and smiles all round.

Many thanks
Kev Blythe, UK... and a local garage

Samsung’s Dumb SmartThings

Samsung SmartThings hacked
http://arstechnica.com/security/2016/05/samsung-smart-home-flaws-lets-hackers-make-keys-to-front-door/

Home Automation -- IoT (Internet of Targets)

- Samsung’s SmartThings
- Apple’s HomeKit
- Vera Control’s Vera3
- Google’s Weave/Brillo
- AllSeen Alliance’s2 AllJoyn (https://allseenalliance.org/framework)
- AllJoyn is an open source software framework that makes it easy for devices and apps to discover and communicate with each other. Developers can write applications for interoperability regardless of transport layer, manufacturer, and without the need for Internet access. The software has been and will continue to be openly available for developers to download, and runs on popular platforms such as Linux and Linux-based Android, iOS, and Windows, including many other lightweight real-time operating systems.
    - 200+ members -- see: https://allseenalliance.org/alliance/members
    - Canon, Electrolux, LG, Microsoft, Philips, Qualcomm, Sharp, Sony
    - Buffalo, ASUS, AT&T, Cisco, DigiCert, Honeywell, IBM, LiteOn, Netgear, Panasonic,

SmartThings Protocol Problems:
"Security Analysis of Emerging Smart Home Applications"
https://iotsecurity.eecs.umich.edu/img/Paper27_CameraReady_SmartThings_Revised_IEEEGen.pdf
2 x U of Michigan + Microsoft Research

Event-driven platform.

- Devices can register to receive notification of events.

Analysis of current SmartThing ecosystem:

- 499 SmartThings apps (SmartApps) were analyzed.
- 132 device handler were examined.

Findings:

- Though SmartThings implements a privilege separation model the system's design forces significant overprivilege.
- 55% of SmartApps are overprivileged due to capabilities being too coarse-grained.
- Once installed a SmartApp is granted FULL access to a device even if it specifies needing only limited access to the device.
- The SmartThings event subsystem, which devices use to communicate asynchronously with SmartApps via events, does not sufficiently protect events that carry sensitive information such as lock codes.
- The researchers exploited framework design flaws to construct four proof-of-concept attacks. They:
    - Remotely exploited an existing SmartApp available on the app store to program backdoor pin-codes into a connected door lock. Their attack made use of the LockCodes capability that the SmartApp never requested—the SmartApp was automatically overprivileged due to the SmartThings capability model design.
    - They eavesdropped on the event subsystem to snoop on lock pin-codes of a Schlage smart lock when the pincodes were being programmed by the user, and leaked them using the unrestricted SmartThings-provided SMS API. Their attack SmartApp advertises itself as a battery monitor and only requests the battery monitoring capability.
    - They disabled an existing vacation mode SmartApp available on the app store using a spoofed event to stop vacation mode simulation. No capabilities were required for this attack.
    - They caused a fake fire alarm using a spoofed physical device event. The attack shows how an unprivileged SmartApp can escalate its privileges to control devices it is not authorized to access by misusing the logic of benign SmartApps.

Several years ago another researcher trivially jammed the ZigBee radio frequency used by SmartThings and was able to enter a "protected" home, tripping Window and door entry and interior motion sensors without tripping any warning of any sort from the system.

SmartThings FAQ:
https://support.smartthings.com/hc/en-us/articles/208201243-ZigBee-Insecure-Rejoin-FAQ

ZigBee "Insecure Rejoin" FAQ
Fundamental ZigBee v1.2 underlying security technology insufficient:
https://community.smartthings.com/t/security-of-smartthings-ecosystem/30827/4

Dan Lieberman / Head of Research & Standards at SmartThings / Dec 2015

There are really two distinct things at play here, and I'll do my best to describe them, what their potential impacts are, and what we're doing at SmartThings to eliminate or mitigate them. I apologize in advance if this is overly dense, but there's a lot to get to here.

What are the issues?

First, as has been pointed out in this thread, there is a designed "moment of insecurity" in the Zigbee Home Automation v1.2 specification that uses a well-known symmetric encryption key known as the Trust Center Link Key to distribute a unique network key when a device first joins the network. This is a tradeoff that the ZigBee Alliance chose to make between security and simplicity - with a mitigated impact given that an attacker would have to be capturing ZigBee network traffic at the same time that a new device is being joined to the network.

This method has been removed from the upcoming ZigBee 3.0 specification and replaced with a process that requires a per-device installation code that is used to generate a unique joining key, which is then used to acquire the ZigBee network key. The install code may be printed on the device, be a 2D barcode that is scanned by a camera, or some other out-of-band method of passing the code from the end-device to the ZigBee Coordinator device (in our case, the SmartThings Hub) such as NFC or Bluetooth Smart.

The second issue described by CognoSec is with a method known as "insecure rejoin." Insecure rejoin also exists in the ZigBee HA 1.2 specification as a tradeoff between security and simplicity. This method allows a previously paired device to rejoin a network using the same well-known Trust Center Link Key in the event that the network key changed since the last time the device joined the network. This enables battery powered devices that aren't always listening for commands from the ZigBee Coordinator (otherwise known as "sleepy" devices) to rejoin a network if the network key changed, as the sleeping device wouldn't have received the new key from the ZigBee Coordinator.

So if an end-device such as a motion sensor or contact sensor fails to join the network using their stored network key, they can ask for the new key which is transmitted using the well-known Trust Center Link Key. The specific issue that CognoSec describes in their publication is the ability to spoof a device on the network to send a false insecure rejoin request, triggering the network key to be sent using the well-known Trust Center Link Key. This bypasses the mitigation effect described above, as an attacker could potentially cause the network key to be transmitted at will.

How is SmartThings impacted, and what are we doing about it?

SmartThings currently supports insecure rejoin, as many ZigBee HA devices will only attempt to rejoin once with their stored key before reverting to an insecure rejoin mode. This means that without insecure rejoin, if there are any issues rejoining the network after a Hub reboots or a router in the mesh goes away, the device would not be able to rejoin the network and would be effectively stranded. The only way to resolve a stranded device would be to delete it from SmartThings, perform a factory reset on the device, and put it back through the initial join process.

We do recognize the security concerns presented by spoofed insecure rejoin requests, and since the issue was brought to our attention we've been developing an update that will give users the option of turning off insecure rejoin while we work to understand the broader negative impact of simply disabling it by default. We hope to have this update in place within the next 60 days. Once the feature is available, we'll let you know how to go about disabling insecure rejoin. In the longer term, the ZigBee 3.0 specification eliminates the insecure rejoin process.

As for the initial joining process, SmartThings must support the standard ZigBee HA 1.2 Trust Center Link Key join process because it's how nearly all ZigBee HA 1.2 certified devices join a ZigBee network, and as an open platform we support many ZigBee HA certified devices from many manufacturers. As mentioned above ZigBee 3.0 will eliminate the "moment of insecurity", but we're also exploring methods for enhancing communication security and add the ability to validate and trust devices that join the network - but this will be limited to our own devices whose firmware we directly control, as the solution will be outside of the ZigBee specification.

I hope this helps, and thank you for taking the time to read this far. As always, please let us know here if there are further questions we can answer or clarifications we can make.

CognoSec
http://bsidesvienna.at/slides/2015/zigbee_smart_homes_a_hackers_open_house.pdf