Security Now! #553 - 03-29-16

Too Much News

This week on Security Now!

- U.S. Says It Has Unlocked iPhone Without Apple
- California Assembly Bill AB-1681
- Was TrueCrypt originally created by an international arms dealer?
- A major flaw in the StartSSL Certificate Authority
- Two more Hospitals hit with ransomware
- A problem found in the SAMBA protocol
- Finally, some good news on the IoT device setup front
- Announcing GRC's Never10 freeware
- A bit more about the new monster PC I built

US Government Filing to Drop Case Against Apple

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA LICENSE PLATE #5KGD203	ED No. CM 16-10 (SP) GOVERNMENT'S STATUS REPORT

Applicant United States of America, by and through its counsel of record, the United States Attorney for the Central District of California, hereby files this status report called for by the Court's order issued on March 21, 2016. (CR 199.)

The government has now successfully accessed the data stored on Farook's iPhone and therefore no longer requires the assistance from Apple Inc. mandated by Court's Order Compelling Apple Inc. to Assist Agents in Search dated February 16, 2016.

Security News

U.S. Says It Has Unlocked iPhone Without Apple
http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html
The Justice Department said on Monday that it had found a way to unlock an iPhone without help from Apple, allowing the agency to withdraw its legal effort to compel the tech company to assist in a mass-shooting investigation.

Yet law enforcement's ability to now unlock an iPhone through an alternative method raises new uncertainties, including questions about the strength of security in Apple devices. The development also creates potential for new conflicts between the government and Apple about the method used to open the device and whether that technique will be disclosed. Lawyers for Apple have previously said the company would want to know the procedure used to crack open the smartphone, yet the government might classify the method.

A staff attorney at the American Civil Liberties Union was quoted: "I would hope they would give that information to Apple so that it can patch any weaknesses, but if the government classifies the tool, that suggests it may not."

F.B.I. investigators have begun examining the contents of the phone but would not say what, if anything, they have identified so far. A senior federal law enforcement official who spoke on the condition of anonymity said it was possible that law enforcement might not find anything useful on the phone.

Given that the F.B.I. may never tell Apple how it forced open the iPhone, Apple said that it would "continue to increase the security of our products as the threats and attacks on our data become more frequent and more sophisticated."

BUT!... it is also decrypted?

Glenn Marston / @glennmarston

Hi, Steve: I would be interested in hearing on today's "Security Now" your estimate of how long it might take the FBI to decrypt the data it says it retrieved from the San Bernadino iPhone. Most news reports assume that the FBI retrieved all the information, as opposed to only the data in encrypted form. However, NBC News says the data remain encrypted. A Mashable quote of an FBI statement says there is more work to be done. The government's court filing says only that it accessed the data. Following are the specifics:

In the topmost video on the NBC News page "Government Says It Got Data Off Terrorist's iPhone Without Apple," at 48 seconds, correspondent Pete Williams says, "Officials say tonight that the data they extracted from the phone is encrypted and will take some time to decode."

http://www.nbcnews.com/tech/apple/fbi-doesn-t-think-it-needs-apple-s-help-unlocking-n546876

In a statement made Monday, March 28, at 9:58 p.m., and reported by Mashable, FBI Assistant Director David Bowdich said, "The full exploitation of the phone and follow-up investigative steps are continuing."
http://mashable.com/2016/03/28/fbi-cracks-san-bernardino-iphone/#7k3nwkg3fmqF

In its March 28 filing to the U.S. District Court for the Central District of California, U.S. attorneys said, "The government has now successfully accessed the data stored on Farook's iPhone." They made no mention of decrypting the data.
http://apps.npr.org/documents/document.html?id=2778267-Apple-Status-Report

If the iPhone data indeed remain encrypted, how long might it take for the government or one of its contractors to decrypt it?

Thank you. / Glenn Marston / Bushnell, Florida

California Assembly Bill (AB-1681)

- https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB1681
- Originally introduced on January 20th, 2016 by California Assembly Member Cooper
    - Amended on March 8th, Corrected on march 18th
- "An act to add Section 22762 to the Business and Professions Code, relating to smartphones."
- LEGISLATIVE COUNSEL'S DIGEST (Executive Summary)
  AB 1681, as amended, Cooper. Smartphones.
  Existing law requires that a smartphone that is manufactured on or after July 1, 2015, and sold in California after that date, include a technological solution at the time of sale, which may consist of software, hardware, or both software and hardware, that, once initiated and successfully communicated to the smartphone, can render inoperable the essential features, as defined, of the smartphone to an unauthorized user when the smartphone is not in the possession of an authorized user.

  This bill would require a smartphone that is manufactured on or after January 1, 2017, and sold in California, to be capable of being decrypted and unlocked by its manufacturer or its operating system provider. The bill would, except as provided, subject a seller or lessor would subject a manufacturer or operating system provider that knowingly failed to comply with that requirement to a civil penalty of $2,500 for each smartphone sold or leased. The bill would prohibit a seller or lessor manufacturer or operating system provider who has paid this civil penalty from passing any portion of the

penalty on to purchasers of smartphones. The bill would authorize only the Attorney General or a district attorney to bring a civil suit to enforce these provisions. This bill would make findings and declarations related to smartphones and criminal activity.

The weird history of TrueCrypt

This morning, Matthew Green, our Johns Hopkins cryptographer, who drove the TrueCrypt auditing project, among many other things, tweeted:

- Truecrypt was originally written by a multi-millionaire international arms dealer named Paul LeRoux.
  https://mastermind.atavist.com/he-always-had-a-dark-side

And in subsequent tweets:

- Paul LeRoux wrote E4M, which Truecrypt was based on. It's unclear if he funded Truecrypt itself. He was arrested in 2012/3.
- Coincidentally, Truecrypt development ceased around the same time LeRoux was arrested.

<quote> Confident in the connection between the two Le Roux's, I burrowed into the world of encryption. Le Roux, it seemed, had started building E4M—Encryption for the Masses—in 1997. It followed that a talented young man so absorbed with the challenges of code, one who had gotten himself into trouble with law enforcement in the past, would tackle a problem as technically knotty as digital privacy. Le Roux's software allowed users to encrypt their entire hard drives—and to conceal the existence of encrypted files, so that prying eyes wouldn't even know they were there. After two years of development, he released it to the world with a post to the alt.security.scramdisk board. According to his own account, the software was written "from scratch," and "thousands of hours went into its development and testing."

[...] In 2004, a group of anonymous developers did exactly what Hafner had feared: They released a new and powerful, free file-encryption program, called TrueCrypt, built on the code for E4M. "TrueCrypt is based on (and might be considered a sequel to)" E4M, a release announcement stated. The program combined security and convenience, giving users the ability to strongly encrypt files or entire disk drives while continuing to work with those files as they would a regular file on their computer.

FWIW, it DOES comport with every scrap tidbit of fact we've had about TrueCrypt's origins... so I give this reporting full credence.

UNBELIEVALBE stupidity in StartSSL (CA) domain validation allows any certs to be obtained!
http://news.softpedia.com/news/flaw-in-startssl-validation-allowed-attackers-to-get-ssl-certs-for-any-domain-502257.shtml

- How to prove domain ownership?
  - Place a specific file on the root of the server. (ala Let's Encrypt)
  - Receive an eMail to an address at that domain:
    - postmaster@domain.com
    - hostmaster@domain.com
    - webmaster@domain.com
- The chosen destination eMail address was SENT by that form!
- The article notes that this was the same technique used by the ComodoHacker, who issued tens of thousands of SSL certificates for domains around the globe. And that the hacker used a similar flaw in the Diginotar CA, which had to file for bankruptcy because of the damage done to its reputation by this incident.

Another hospital hit by RansomWare
http://arstechnica.com/security/2016/03/kentucky-hospital-hit-by-ransomware-attack/

- "Locky" malware holds medical data hostage for a four-bitcoin ransom.
- A month after the Hollywood Presbyterian Medical Center in Los Angeles was crippled by crypto-ransomware, a Methodist Hospital in Henderson, Kentucky, initiated an "internal state of emergency" and shut down its desktop computers and Web-based systems in an effort to fight the spread of the Locky crypto-ransomware after discovering an infection of its network.
- The hospital's IT staff posted a scrolling message at the top of Methodist's website, announcing that "Methodist Hospital is currently working in an Internal State of Emergency due to a Computer Virus that has limited our use of electronic web-based services. We are currently working to resolve this issue, until then we will have limited access to web-based services and electronic communications."
- Methodist Hospital's information systems director told Brian Krebs that the Locky malware, which came in as an attachment to a spam e-mail, attempted to spread across the network after it had infected the computer it was triggered on. Locky has been known to use malicious scripts in Microsoft Office documents as a means of infecting victims' computers. The malware succeeded in infecting several other systems, prompting the hospital staff to shut down all the hospital's computers. Each PC is brought back online individually after being scanned for telltale signs of Locky while off the network.
- The Locky guys only want 4 bitcoins - about $1600. That's a BARGAIN! After being offline for 10 days and with no other solution, the Hollywood Presbyterian paid a 40 bitcoin (~$17,000) ransom.

That was last week… Yesterday: Virus infects MedStar Health system's computers, forcing an online shutdown

https://www.washingtonpost.com/local/virus-infects-medstar-health-systems-computers-hospital-officials-say/2016/03/28/480f7d66-f515-11e5-a3ce-f06b5ba21f33_story.html

- The Washington health-care behemoth, MedStar Health which operates 10 hospitals and more than 250 outpatient facilities in the Washington region -- with revenues of $5 Billion annually.
- Without access to sophisticated online systems, hospital staff have had to revert to seldom-used paper charts and records.
- One employee who asked that her name not be used because she was not authorized to speak about the incident said: "Even the lowest-level staff can't communicate with anyone. You can't schedule patients, you can't access records, you can't do anything."

Pre-Announce Mystery: **"BadLock" - Samba / SMB**

http://badlock.org/

Here's what we know:

- Two weeks from TODAY, on April 12th:
- A crucial security bug in Windows and Samba will be disclosed. We call it: Badlock.
- Engineers at Microsoft and the Samba Team are working together to get this problem fixed. Patches will be released on April 12th.
- Admins and all of you responsible for Windows or Samba server infrastructure: Mark the date.
- Please get yourself ready to patch all systems on this day. We are pretty sure that there will be exploits soon after we publish all relevant information.
- Patches will be available for Samba 4.2, 4.3, 4.4.
- FAQ: Why announce Badlock before April 12th, 2016?
  The main goal of this announcement is to give a heads up and to get you ready to patch all systems as fast as possible and have sysadmin resources available on the day the patch will be released. Vendors and distributors of Samba are being informed before a security fix is released in any case. This is part of any Samba security release process.
  Weighting to the respective interests of advance warning and utmost secrecy we chose to warn you beforehand, so that everyone has a chance to be ready to install the fixes as soon as they are available. Once the patch is released to the public, it will point to attack vectors and exploits will be in the wild in no time.
- FAQ: Who found the Badlock Bug?
  Badlock was discovered by a member of the international Samba Core Team working at SerNet on Samba. He reported the bug to Microsoft and has been working closely with them to fix the problem.
- "BadLock" ???
  - File locking is a required part of any file system.

Device Provisioning Protocol (DPP)

http://www.wi-fi.org/who-we-are/current-work-areas

- With the increase in Wi-Fi CERTIFIED devices available, end users have the ability to add a more diverse set of devices to their Wi-Fi networks, including a growing range of devices that do not have a rich user interface. Wi-Fi Alliance Device Provisioning Protocol will enhance the user experience with a simple, secure, and consistent method for on- and off-boarding any type of device on a Wi-Fi network.

http://www.networkworld.com/article/3046132/internet-of-things/wi-fi-access-for-the-internet-of-things-can-be-complicated.html

- Meanwhile, the WLAN should be protected against intruders impersonating IoT sensors, and real sensors infected with malware: this means sensors should follow the same security regime as enterprise smartphones and PCs. Especially where PSKs are used, the sensor's identity should be established so the WLAN knows what it is, where it needs to connect, and permitted traffic patterns. Identity can be a user id, MAC address or X.509 certificate.

  But hooking each sensor in turn up to a PC, for instance, and configuring it with SSID, credentials and identity is incredibly time-consuming. IoT vendors are applying their creativity to the problem, and we are beginning to see proprietary solutions; but we would prefer vendor-independent standards.

  Garage door openers, home thermostats and the like are often configured by making a point-to-point Wi-Fi connection from a smartphone and entering information on the screen. This model is also applicable to enterprise deployments where an employee is able to stand next to each sensor and configure it. But if credentials are entered on the smartphone screen, they are visible to the employee and prone to error.

  The Wi-Fi Alliance is working to improve this method. The Device Provisioning Protocol (DPP) will allow an already-authenticated user's smartphone to bring a new device onto the network, similar to a visitor given guest access by a sponsoring employee. The key feature is to maintain security, keeping the new device's unique credentials hidden from the sponsor and encrypted over the air.

Never10

In this morning's Sydney Morning Herald, Adam Turner's "Digital Life" column starts off:
http://www.smh.com.au/technology/gadgets-on-the-go/never10-keeps-windows-10-at-bay-20160328-gnst5k.html

As Microsoft ramps up efforts to force Windows 10 on to older PCs, Never10 helps you maintain the status quo.

Lunch with my parents on the weekend turned into an unexpected tech support visit when my Dad started up his computer to discover it had upgraded from Windows 7 to Windows 10 against his wishes.

After months of harassment from Microsoft's nagware I assumed that he'd accidentally clicked Upgrade, despite his vigilance in closing the pop-up notifications rather than dealing with the Hobson's choice of Upgrade Now or Upgrade Later. After a quick online search I realised I owed Dad an apology, as there's been a spate of unwanted Windows 10 upgrades recently from people who swear they never authorised it.

As Microsoft becomes more persistent, **Never10** offers an easy way to put the freeze on Windows 10. It's free software for Windows 7 and 8.1 which makes it simple for anyone to tweak the advanced settings on their computer to ward off the upgrade – something I wish I'd installed on my Dad's computer before it was too late.

- Paul & MaryJo both immediately jumped on it and covered it ***THANKS!!!***
- What I learned last week
    - GWX vs hiding updates
    - Hiding non-present updates
    - Hiding is unreliable
- What it does.
- Registry vs Group Policy
- Read-Only Keys & Values
- v1.1 - signed w/SHA256 also set keys to read-only.
- SHA1 vs SHA256 -- DigiCert to the rescue, again!
- Other GRC Freeware:
    - DNS Benchmark - 2,530,000 downloads (1,661 / day)
    - SecurAble - 3,675,000 downloads (1,112 / day)
    - UnPlug n' Pray - 3,963,000 downloads (377 / day)
    - LeakTest - 7,964,051 downloads (153 / day)

Miscellany

The Tech Guy: How to monitor household's data usage -

- Routers publish their interface byte traffic counters through SNMP
- NetWorx (freeware) monitors and accrues this wonderfully!!
    - (Tip: Use Log scaling instead of auto-scaling)

Temperfect mugs are reportedly just weeks away.

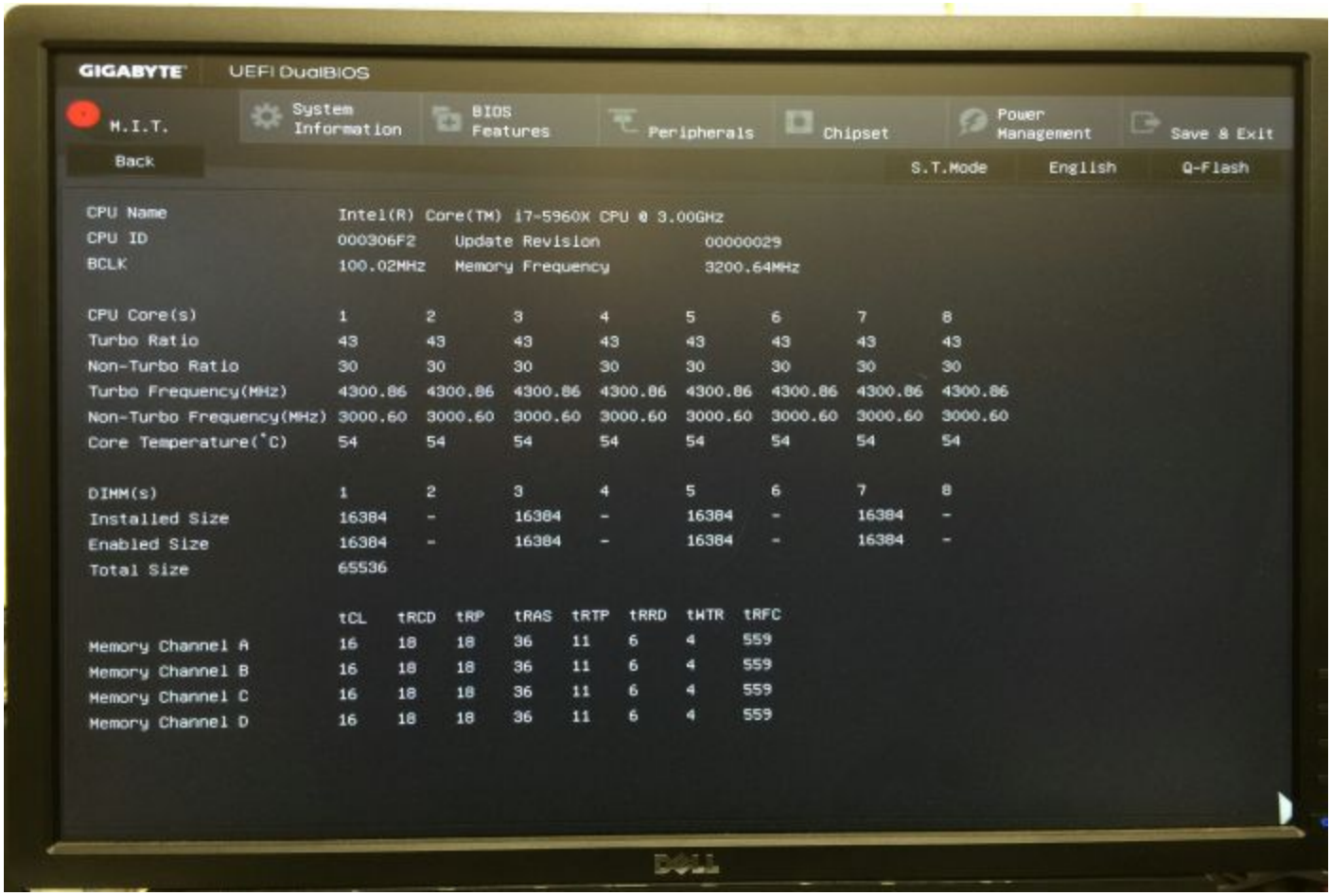
Subject: Steve's "Last PC"
"Chandler" in Kentucky

Steve, I'm an avid listener to your and Leo's Security Now podcast. I tune in every week and love to hear the latest in security news. I did have a question after watching last week's episode. You described that your new PC's motherboard supports NVMe and RAID on-board. Could you divulge the make and model motherboard for us listeners who are looking to build a PC with those features?


Ultra Durable
Socket 2011-3
GIGABYTE
GA-X99P-SLI
Intel GbE LAN
USB 3.1
32Gb/s
M.2
UEFI DualBIOS
Ultra Durable
GIGABYTE
CORSAIR
RM850

CORSAIR
RM850
GIGABYTE
SAMSUNG
950 PRO

CORSAIR
RM850
GIGABYTE
NVIDIA
QUADRO NVS 450


GIGABYTE UEFI DualBIOS
M.I.T.
System Information
BIOS Features
Peripherals
Chipset
Power Management
Save & Exit
Back
S.T.Mode
English
Q-Flash
CPU Name Intel(R) Core(TM) i7-5960X CPU @ 3.00GHz
CPU ID 000306F2 Update Revision 00000029
BCLK 100.02MHz Memory Frequency 3200.64MHz
CPU Core(s) 1 2 3 4 5 6 7 8
Turbo Ratio 43 43 43 43 43 43 43 43
Non-Turbo Ratio 30 30 30 30 30 30 30 30
Turbo Frequency(MHz) 4300.86 4300.86 4300.86 4300.86 4300.86 4300.86 4300.86 4300.86
Non-Turbo Frequency(MHz) 3000.60 3000.60 3000.60 3000.60 3000.60 3000.60 3000.60 3000.60
Core Temperature(°C) 54 54 54 54 54 54 54 54
DIMM(s) 1 2 3 4 5 6 7 8
Installed Size 16384 - 16384 - 16384 - 16384 -
Enabled Size 16384 - 16384 - 16384 - 16384 -
Total Size 65536
tCL tRCD tRP tRAS tRTP tRRD tWTR tRFC
Memory Channel A 16 18 18 36 11 6 4 559
Memory Channel B 16 18 18 36 11 6 4 559
Memory Channel C 16 18 18 36 11 6 4 559
Memory Channel D 16 18 18 36 11 6 4 559
DELL

:)