Security Now! #549 - 03-01-16

Q&A #229

This week on Security Now!

- The ongoing Apple iPhone battle
- A formal definition of a "Backdoor"
- iPhone Passcode length helps a lot!
- ... So does not running as Admin under Windows
- Local network scanning tools.
- Miscellany and a dozen Questions and comments from our followers

Security News

Apple's Formal Filed Reply:

- https://assets.documentcloud.org/documents/2722199/5-15-MJ-00451-SP-USA-v-Black-Lexus-IS300.pdf

There are two important and legitimate interests in this case: the needs of law enforcement and the privacy and personal safety interests of the public. In furtherance of its law enforcement interests, the government had the opportunity to seek amendments to existing law, to ask Congress to adopt the position it urges here. But rather than pursue new legislation, the government backed away from Congress and turned to the courts, a forum ill-suited to address the myriad competing interests, potential ramifications, and unintended consequences presented by the government's unprecedented demand. And more importantly, by invoking "terrorism" and moving ex parte behind closed courtroom doors, the government sought to cut off debate and circumvent thoughtful analysis.

The order demanded by the government compels Apple to create a new operating system—effectively a "back door" to the iPPhone—that Apple believes is too dangerous to build. Specifically, the government would force Apple to create new software with functions to remove security features and add a new capability to the operating system to attack iPhone encryption, allowing a passcode to be input electronically. This would make it easier to unlock the iPhone by "brute force," trying thousands or millions of passcode combinations with the speed of a modern computer. In short, the government wants to compel Apple to create a crippled and insecure

product. Once the process is created, it provides an avenue for criminals and foreign agents to access millions of iPhones. And once developed for our government, it is only a matter of time before foreign governments demand the same tool.

The government says: "Just this once" and "Just this phone." But the government knows those statements are not true; indeed the government has filed multiple other applications for similar orders, some of which are pending in other courts. And as news of this Court's order broke last week, state and local officials publicly declared their intent to use the proposed operating system to open hundreds of other seized devices—in cases having nothing to do with terrorism. If this order is permitted to stand, it will only be a matter of days before some other prosecutor, in some other important case, before some other judge, seeks a similar order using this case as precedent. Once the floodgates open, they cannot be closed, and the device security that Apple has worked so tirelessly to achieve will be unwound without so much as a congressional vote. As Tim Cook, Apple's CEO, recently noted: "Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks—from restaurants and banks to stores aand homes. No reasonable person would find that acceptable." Despite the context of this particular action, no legal principle would limit the use of this technology to domestic terrorism cases—but even if such limitations could be imposed, it would only drive our adversaries further underground, using encryption technology made by foreign companies that cannot be conscripted into U.S. government service4—leaving law-abiding individuals shouldering all of the burdens on liberty, without any offsetting benefit to public safety. Indeed, the FBI's repeated warnings that criminals and terrorists are able to "go dark" behind end-to-end encryption methods proves this very point.

Finally, given the government's boundless interpretation of the All Writs Act, it is hard to conceive of any limits on the orders the government could obtain in the future. For example, if Apple can be forced to write code in this case to bypass security features and create new accessibility, what is to stop the government from demanding that Apple write code to turn on the microphone in aid of government surveillance, activate the video camera, surreptitiously record conversations, or turn on location services to track the phone's user?

Nothing.

"Apple Wins Ruling in New York iPhone Hacking Order"

- http://www.nytimes.com/2016/03/01/technology/apple-wins-ruling-in-new-york-iphone-hacking-order.html
- Began last October / iPhone 5s seized by the DEA

James Orenstein:

- <quote> For the reasons set forth below, I conclude that under the circumstances of this case, the government has failed to establish either that the AWA permits the relief is seeks or that, even if such an order is authorized, the discretionary factors I must consider weigh in favor of granting the motion.

NYT: <quote>
A federal magistrate judge on Monday denied the United States government's request that Apple extract data from an iPhone in a drug case in New York, giving the company's pro-privacy stance a boost as it battles law enforcement officials over opening up the device in other cases.

The ruling, from Judge James Orenstein in New York's Eastern District, is the first time that the government's legal argument for opening up devices like the iPhone has been put to the test. The denial could influence other cases where law enforcement officials are trying to compel Apple to help unlock iPhones, including the standoff between Apple and the F.B.I. over the iPhone used by one of the attackers in a mass shooting in San Bernardino, Calif., last year.

Judge Orenstein, in his 50-page ruling on Monday, took particular aim at a 1789 statute called the All Writs Act that underlies many government requests for extracting data from tech companies. The All Writs Act broadly says that courts can require actions to comply with their orders when not covered by existing law. Judge Orenstein said the government was inflating its authority by using the All Writs Act to force Apple to extract data from an iPhone seized in connection with a drug case.

Judge Orenstein wrote: "The government's view of the All Writs Act is so expansive as to cast doubt on its constitutionality if adopted."

Jonathan Ździarski (@JZdziarski) / 2/29/16, 1:35 PM

- The first uses of my iOS forensics tools were in terrorism and kidnapping cases. Not long after, cops were using it for girlfriends' phones.

Formal Definition of "Backdoor"
Jonathan Zdziarski (@JZdziarski)
<quote> A backdoor is a component of a security mechanism, where the component is active on a computer system without consent of the computer's owner, performs functions that subvert purposes disclosed to the computer's owner, and is under the control of an undisclosed actor.

Complex iPhone passcodes

- 80ms / guess is VERY slow!
- iOS Security / February, 2014
- *Passcodes*
  By setting up a device passcode, the user automatically enables Data Protection. iOS supports four-digit and arbitrary-length alphanumeric passcodes. In addition to unlocking the device, a passcode provides the entropy for encryption keys, which are not stored on the device. This means an attacker in possession of a device can't get access to data in certain protection classes without the passcode.

  The passcode is "tangled" with the device's UID, so brute-force attempts must be performed on the device under attack. A large iteration count is used to make each attempt slower. The iteration count is calibrated so that one attempt takes approximately 80 milliseconds. This means it would take more than 5½ years to try all combinations of a six-character alphanumeric passcode with lowercase letters and numbers.

  The stronger the user passcode is, the stronger the encryption key becomes. Touch ID on iPhone 5s can be used to enhance this equation by enabling the user to establish a much stronger passcode than would otherwise be practical. This increases the effective amount of entropy protecting the encryption keys used for Data Protection without adversely affecting the user experience of unlocking an iOS device multiple times throughout the day.

  To further discourage brute-force passcode attacks, the iOS interface enforces escalating time delays after the entry of an invalid passcode at the Lock screen. Users can choose to have the device automatically wiped if the passcode is entered incorrectly after 10 consecutive attempts. This setting is also available as an administrative policy through mobile device management (MDM) and Exchange ActiveSync, and can also be set to a lower threshold.

  On a device with an A7 processor, the key operations are performed by the Secure Enclave, which also enforces a 5-second delay between repeated failed unlocking requests. This provides a governor against brute-force attacks in addition to safeguards enforced by iOS.

Avecto / RSA Conference Analysis

Analysis of Microsoft "Patch Tuesday" Security Bulletins from 2015 highlights that 85% of Critical Microsoft vulnerabilities would be mitigated by removing admin rights across an enterprise, with a 52% increase in the total volume of vulnerabilities compared to 2014.

Key findings:

- Of the 251 vulnerabilities in 2015 with a Critical rating, 85% were concluded to be mitigated by removing administrator rights
- There has been a 52% year on year rise in the volume of vulnerabilities since 2014
- 86% of Critical vulnerabilities affecting Windows, mitigated by removing admin rights
- 99.5% of all vulnerabilities in Internet Explorer, mitigated by removing admin rights
- 82% of vulnerabilities affecting Microsoft Office, mitigated by removing admin rights
- 85% of Remote Code Execution vulnerabilities, mitigated by removing admin rights
- 82% Critical vulnerabilities affecting Windows 10, mitigated by removing admin rights
- 63% of all Microsoft vulnerabilities reported in 2015, mitigated by removing admin rights.

Local network scanning:

Christian Turri (@cdturri)

Hey Steve here is a quick question for the Q&A podcast. Shields Up is great and I use it all the time but do you have any tools you can recommend to do internal port scans? Basically I want to do internal port scans on some IoT devices to see what they are opening. Thanks!

- Foundstone -> McAfee -> Intel
- Robin Kier
- SuperScan v3.0
    - http://www.mcafee.com/us/downloads/free-tools/superscan3.aspx
- SuperScan v4.1
    - Raw sockets removal neutered this scanner
- McAfee Free Tools
    - http://www.mcafee.com/us/downloads/free-tools/index.aspx
- Advanced Port Scanner
    - http://www.advanced-port-scanner.com/

Next week: The DROWN Attack

- DROWN stands for: Decrypting RSA with Obsolete and Weakened eNcryption

Miscellany

SlySoft.com & AnyDVD shutdown

https://torrentfreak.com/popular-blu-ray-ripper-shuts-down-following-legal-pressure-160224/

Zeo Update

- Zeo CSV
- Zeo viewer (30 seconds versus 5 min resolution)

Setting up new Windows 7 Systems

- Windows Update has changed since Win7/SP1

ZDNet / SSD's in the Data Center / Google's Experience

http://www.zdnet.com/article/ssd-reliability-in-the-real-world-googles-experience

- 14th USENIX Conference on File and Storage Technologies
- The FAST 2016 paper: "Flash Reliability in Production: The Expected and the Unexpected":
- Millions of drive days over 6 years
- 10 different drive models
- 3 different flash types: MLC, enterprise MLC and SLC
- Enterprise and consumer drives

Points:

- Raw Bit Error Rate (RBER) increases slower than expected from wearout and is not correlated with UBER or other failures.
- High-end SLC drives are no more reliable that MLC drives.
- SSDs fail at a lower rate than disks, but UBER rate is higher.
- SSD age, not usage, affects reliability.
- Bad blocks in new SSDs are common, and drives with a large number of bad blocks are much more likely to lose hundreds of other blocks, most likely due to die or chip failure.
- 30-80 percent of SSDs develop at least one bad block and 2-7 percent develop at least one bad chip in the first four years of deployment.

SpinRite

Rick Harvey in Melbourne, Australia
Subject: Odd SpinRite story
Date: 11 Feb 2016 22:33:35
:
Hi Steve (and Leo)

Did you know that SpinRite can save your power bill? Yes, this is bizarre.. But I'll let you try to work out why...

I have an old (sentimental) testing laptop (Dell Studio) that pretty much spends its day idle, sleeping between test runs. But annoyingly, it's always running the fan. Task manager shows the CPU barely getting off the baseline. I've even tried reinstalling the OS. No difference. Just noise and heat. Not so great during the summer!

I bought a copy of SpinRite last year just to support your show and give you the pleasure of a Yabba Dabba Doo. So it finally occured to me to give that machine a spin. Also because I'm curious about your SpinRite powerhouse fitting into just 170K of code.

So created a boot USB and off SpinRite went on Level 4. When it finished everything was green. I rebooted and all was quiet. OMG! No more fan running. The icing was a comment by my wife who hadn't realized the screen was blanked. She quipped: "So, you've finally turned off that heap of junk?". Shhhhh! (Let's not tell her!)

Awesome show. Yada, Yada...

Best regards...Rick