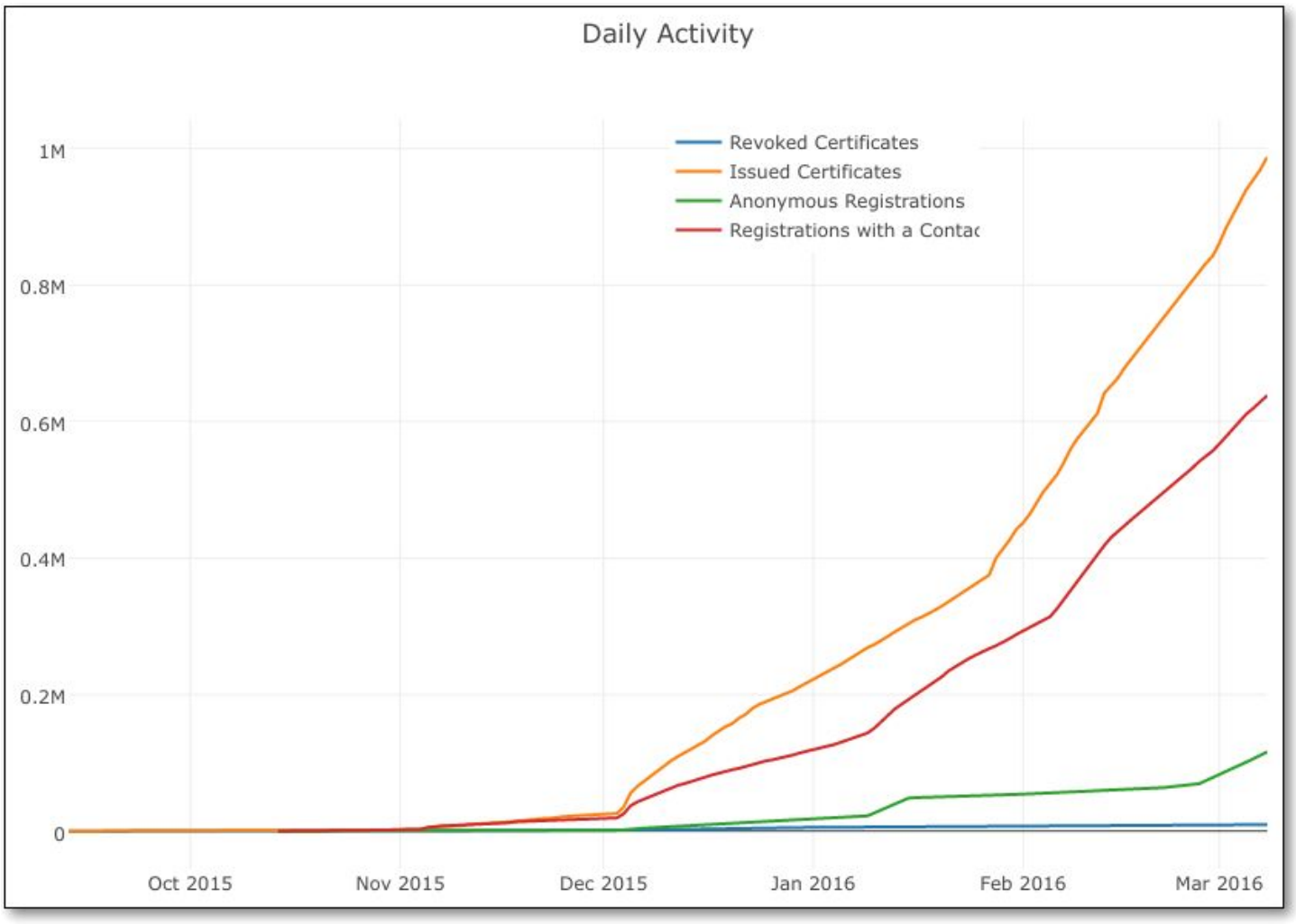
Security Now! #550 - 03-08-16

CacheBleed

This week on Security Now!

- Brief Apple decryption dispute update
- First Mac OS X ransomware strikes
- Will quantum computing mean the end of encryption?
- Verizon gets a barely noticeable slap on the wrist.
- Facebook missed a huge security hole.
- Next-gen fingerprint spoofing with an inkjet printer
- John McAfee
- RSA
- A wonderful Let's Encrypt milestone
- A look at the CacheBleed attack



Security News

Smartphone encryption update
Justice department is appealing last month's pro-Apple decision regarding the crackable iPhone 5C running iOS 7. Apple had successfully appealed the original order on the grounds that it relied on an unsupportable interpretation of the All Writs Act (AWA). The court agreed.

The Installer for "Transmission -- a Fast, Easy and Free BitTorrent Client" offering native Mac GUI options... was delivering the first Mac Ransomware.
Palo Alto Networks:
http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/
<quote> On March 4, we detected that the Transmission BitTorrent client installer for OS X was infected with ransomware, just a few hours after installers were initially posted. We have named this Ransomware “KeRanger.” The only previous ransomware for OS X we are aware of is FileCoder, discovered by Kaspersky Lab in 2014. As FileCoder was incomplete at the time of its discovery, we believe KeRanger is the first fully functional ransomware seen on the OS X platform.

Attackers infected two installers of Transmission version 2.90 with KeRanger on the morning of March 4. When we identified the issue, the infected DMG files were still available for downloading from the Transmission site (https://download.transmissionbt.com/files/Transmission-2.90.dmg) Transmission is an open source project. It’s possible that Transmission’s official website was compromised and the files were replaced by re-compiled malicious versions, but we can’t confirm how this infection occurred.

The KeRanger application was signed with a valid Mac app development certificate; therefore, it was able to bypass Apple’s Gatekeeper protection. If a user installs the infected apps, an embedded executable file is run on the system. KeRanger then waits for for three days before connecting with command and control (C2) servers over the Tor anonymizer network. The malware then begins encrypting certain types of document and data files on the system. After completing the encryption process, KeRanger demands that victims pay one bitcoin (about $400) to a specific address to retrieve their files. Additionally, KeRanger appears to still be under active development and it seems the malware is also attempting to encrypt Time Machine backup files to prevent victims from recovering their back-up data.

Palo Alto Networks reported the ransomware issue to the Transmission Project and to Apple on March 4. Apple has since revoked the abused certificate and updated XProtect antivirus signature, and Transmission Project has removed the malicious installers from its website. Palo

Alto Networks has also updated URL filtering and Threat Prevention to stop KeRanger from impacting systems.

Interesting details:

- The two KeRanger infected Transmission installers were signed with a legitimate certificate issued by Apple. The developer listed this certificate is a Turkish company with the ID Z7276PX673, which was different from the developer ID used to sign previous versions of the Transmission installer. In the code signing information, we found that these installers were generated and signed on the morning of March 4.

- After connecting to the C2 server and retrieving an encryption key, the executable will traverse the "/Users" and "/Volumes" directories, encrypt all files under "/Users", and encrypt all files under "/Volumes" which have certain file extensions.

- There are 300 different extensions specified by the malware, including:
  - Documents: .doc, .docx, .docm, .dot, .dotm, .ppt, .pptx, .pptm, .pot, .potx, .potm, .pps, .ppsm, .ppsx, .xls, .xlsx, .xlsm, .xlt, .xltm, .xltx, .txt, .csv, .rtf, .tex
  - Images: .jpg, .jpeg,
  - Audio and video: .mp3, .mp4, .avi, .mpg, .wav, .flac
  - Archives: .zip, .rar., .tar, .gzip
  - Source code: .cpp, .asp, .csh, .class, .java, .lua
  - Database: .db, .sql
  - Email: .eml
  - Certificate: .pem

Users who have directly downloaded Transmission installer from official website after 11:00am PST, March 4, 2016 and before 7:00pm PST, March 5, 2016, may be been infected by KeRanger. Palo Alto Networks page has "How to protect yourself" in the announcement linked above.

Will Quantum Computing mean the end of Cryptography?

http://spectrum.ieee.org/tech-talk/computing/hardware/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment

- Someday the will presumably kill the use of "factoring huge numbers" as "the thing that's hard".
- There was a recent breakthrough MIT and the University of Innsbruck who successfully used a device known as an Ion Trap containing 5 atoms to successfully compute the factors of the number 15.
- They claim this technology could be scaled in the future -- though not for a long long time.
- Quantum-resistant Crypto is already "a thing" that researchers are beginning to tackle as something that will eventually need their attention.

Verizon Wireless pays $1.35 Million (nothing) in fine for their use of "Super Cookies"
http://www.nbcnews.com/tech/tech-news/verizon-slapped-1-35m-fine-supercookies-privacy-violation-n533781

- Verizon Wireless agreed to get consumer consent before sending data about "supercookies" from its more than 100 million users, under a settlement.
- Verizon (the largest U.S. mobile company) inserted unique tracking codes in its users traffic for advertising purposes.
- The FCC said on Monday that Verizon Wireless failed to disclose the practice from late 2012 until 2014, violating a 2010 FCC regulation on Internet transparency.
- IMO -- The fine should have been FAR HIGHER. $1.35 Million is unnoticeable to them... making the overall enterprise highly profitable.
- Under the agreement, consumers must opt in to allow their information to be shared outside Verizon Wireless, and have the right to "opt out" of sharing information with Verizon.
- The FCC has also said that it plans to unveil new proposed privacy protections for broadband as soon as later this month.

Facebook fixes a rather glaring hole in their login security
http://www.anandpraka.sh/2016/03/how-i-could-have-hacked-your-facebook.html?m=1

- This could have allowed an attacker to set a new password, view messages, see the accounts creditd card stored under the payments section, personal photos, etc. -- full account impersonation.
- Whenever a user Forgets their password on Facebook, they have an option to reset the password by entering their phone number / email address at https://www.facebook.com/login/identify?ctx=recover&lwv=110
- Facebook then sends a (becoming standard) 6-digit code to their phone number/email address, which user has to enter in order to set a new password.
- Brute forcing the 6 digit code on Facebook's www.facebook.com production domain was blocked after 10-12 invalid attempts.
- Query is: lsd=AVoywo13&n=XXXXXX
- BUT!!! ... neither the beta.facebook.com nor mbasic.beta.facebook.com had the brute force blocking in place, allowing for high-speed brute-forcing of the 6-digit code... and cracking into anyone's account (given their eMail address or phone number) was trivial.
- THE LESSON: Short and simple "out of band" codes ONLY WORK when guessing is strictly blocked.
- (Even Facebook's 10-12 make no sense in this instance. It should be 1 or 2 then request another.)

Spoof a finger to unlock Samsung and Huawei biometrically-locked smartphones.
(Samsung Galaxy S6 and a Huawei Honor 7)
Two researchers at Michigan State university's Department of computer science and engineering
Using special AgIC conductive Ink and AgIC "circuit paper"
http://www.cse.msu.edu/rgroups/biometrics/Publications/Fingerprint/CaoJain_HackingMobilePhonesUsing2DPrintedFingerprint_MSU-CSE-16-2.pdf

- https://agic.cc/en
- http://shop.agic.cc/products/a6-circuit-paper-10-sheets
- This circuit paper works with AgIC ink to make circuits. This pack contains 10 sheets of A6 size (4.1" x 5.8"), which is a good size for drawing with Circuit Marker.
- http://shop.agic.cc/products/circuit-printer-cartridge-set
- Circuit Printer Cartridge Set is a set of 3 cartridges (CMY) filled with AgIC's conductive ink. Replace cartridges in a compatible printer and print circuits with home inkjet printers.
- (They also list the compatible printers.)
- Recall: Germany's Chaos Computer Club previously did this using a 2.5D printed gummy finger.
- Now: Researchers say that anyone can lift a smartphone's owner fingerprint, even from the stolen phone itself, scan it at 300 dpi, flip it horizontally, and then print it on the glossy side of the special AgIC paper.
- Tip: Use a finger less likely to be pressed against your phone. And smear your print on the reader as you remove it after registering your print after each use.

McAfee acknowledges that he lied to generate YouTube traffic (700,000 views).
http://www.dailydot.com/politics/john-mcafee-lied-iphone-apple-fbi
https://www.inverse.com/article/12277-john-mcafee-challenges-reddit
McAfee Originally: "I speak through the press, to the press, and to the general public. For example, last night I was on RT, and I gave a vastly oversimplified explanation of how you would hack into the iPhone. I can't possibly go in and talk about the secure spaces on the A7 chip. I mean, who's going to understand that crap? Nobody. But you gotta believe me: I understand it. And I do know what I'm doing, else I would not be where I am. This is a fact. Someone who does not understand software cannot start a multibillion dollar company. This is just a fact of life. So, if I look like an idiot, it is because I am speaking to idiots. But I promise you this: You get me on a coding table, against somebody? I will kick your ass.

Interviewer: Anything else you'd like to talk about?

McAfee: "Yeah, if you're on Reddit, tell those guys: Cut me a little bit of slack; that I am not quite as stupid as they think. I mean, I may be pretty damn stupid. But nowhere near what they

think. And if anybody wants to test me, please. Bring a laptop, a coding pencil, or ask them how to … Here's one: If you have a computer with no memory and only two registers, how do you exchange register A with register B? And all you have are Boolean operators. Now, you ask them that: How many people can do that within one minute? That's the question I used to ask everybody who came to work for me at McAfee. If you can't solve that in a minute, you're an idiot; you shouldn't be programming. And I guarantee you that 99 percent cannot do it. Alright? Two registers, only Boolean operators, no memory — and you must exchange the contents of those two registers. So you don't have adds and subtracts — no: only Boolean. 'AND.' 'OR.' 'XOR.' You got it?

Interviewer: I will pass that challenge along.

McAfee: "And tell them, the first time somebody asked me that question, I popped out the answer instantly."

(Okay, John… and we'll try to ignore the fact that it is so commonly known among ALL programmers that it has its own Wikipedia page.)

At RSA:

- The Cryptographer's Panel (47:12)
- http://bit.ly/rsacrypto
- https://www.youtube.com/watch?v=k76qLOrna1w

EFF Issues the MILLIONTH Free HTTPS Cert

https://www.eff.org/deeplinks/2016/03/lets-encrypt-has-issued-million-certificates
http://www.infosecurity-magazine.com/news/eff-releases-millionth-free-https/
Three months from the first beta version of the service becoming available, Lets Encrypt has passed this significant landmark and is helping to ensure websites are more secure with encryption.

Moreover, since a single certificate can cover more than one domain, the million certs Let's Encrypt CA has issued are actually valid for 2.5 million fully-qualified domain names.

<quote> Much more work remains to be done before the Internet is free from insecure protocols, but this is substantial and rapid progress. It is clear that the cost and bureaucracy of obtaining certificates was forcing many websites to continue with the insecure HTTP protocol, long after we've known that HTTPS needs to be the default. We're very proud to be seeing that change, and helping to create a future in which newly provisioned websites are automatically secure and encrypted.

(GRC will continue using DigiCerts certs. We obtained new certs two weeks ago for 2 years.)

Miscellany

Toby (@tweekedinsd)
Hey @SGgrc & @leolaporte! Updated Windows 10 & hating it. What operating system would you recommend? FreeBSD or Linux Mint?

Toby...
For the time being I'm staying with Win7. I think it's perfect. It predates Microsoft's switch to OS-as-an-overcommunicating-social-media-service, it will be kept updated until 2020, it runs a recent model IE for talking to Microsoft, it supports all of the latest communications security standards (forward secrecy, TLSv1.2, SHA-256, etc.), it's available in mature 32 and 64 bit versions, so plenty of RAM expansion space. It's supported by current laptop and desktop hardware. It runs the user with reduced rights which can be easily and transiently elevated... and, of course, it also manages all peripheral I/O, storage and networking, launches all 32- and 64-bit Windows apps, includes a free built-in VM for running XP and much older 16-bit apps if needed. It can be easily tweaked to never upgrade to Windows 10. What's not to love?... and what more could anyone want?

Healthy Sleep Formula

- Linked from GRC's main menu: Research / Health / Healthy Sleep Formula
- Google: "Healthy Sleep Formula"
- http://bit.ly/sg-hsf

SpinRite

Jeff in Ontario, Canada
Subject: Not a security question. :)

Hi Steve,

I have a WD My Passport 1TB portable USB HDD. I had bought a copy of SpinRite some time ago to support you and your podcast which I thoroughly enjoy every week. I partitioned the aforementioned portable HDD with 3 primary partitions and a bunch of logical partitions. I made the drive bootable and installed a bootloader. The drive held a number of useful PC diagnostic, maintenance, and repair tools including SpinRite, some live Linux distros, memtest, etc.

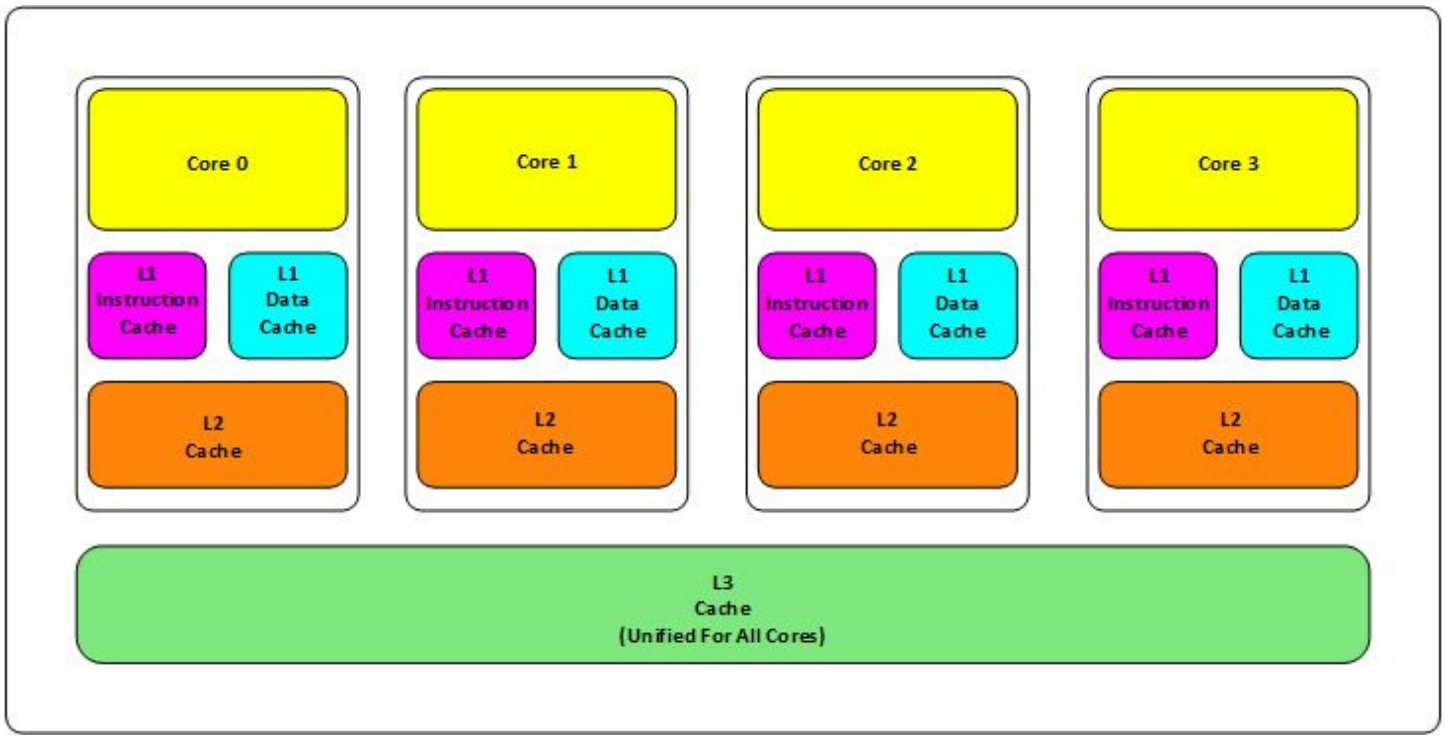
A few weeks ago I clumsily dropped my portable HDD. It fell from about waist height. A few days later I noticed I was unable to save some files to the drive from a Linux machine. The OS

was showing me I/O errors. I was also unable to copy some large (over 2GB) files from the drive to my Windows 7 laptop. The Windows copy dialog was getting stuck and claiming an ETA of a couple decades :P.

I plugged the HDD into a spare workstation at work and booted spinrite from the drive's first partition. I then set spinrite to work on all the partitions of the same drive. I'm not sure if it is a good idea to have spinrite test the same media it booted from? It is plugged in by USB (not SATA).

Do you think SpinRite can breath new life into a HDD that has suffered physical trauma (ie. has been dropped)? It did not hold any data that wasn't backed up so I'm not concerned with data recovery but I'd love to have the drive working again. Maybe I'll just get one of those shockproof portable HDDs (Those ones with the rubber bumpers). Those things are going for less than $80 these days. :)

CacheBleed



The well-understood rules for avoiding/preventing side-channel attacks which depend upon "secret-based" alterations in the code path:

- User only fixed-time instructions with arguments that depend on secret (key) data.
- Do not use conditional branches that depend on secret (key) data.

But to be REALLY CLEAN, the crypto implementation should also...

- Not use memory access patterns that depend on secret (key) data

CacheBleed targets software that has some specific memory access patterns which depend on secret (key) data.

Cache-bank conflicts

To facilitate access to the cache and to allow concurrent access to the L1 cache, cache lines are divided into multiple *cache banks*. On the processor we tested, there are 16 banks, each four bytes wide. The cache uses bits 2-5 of the address to determine the bank that a memory location uses.

In the Sandy Bridge microarchitectures, the cache can handle concurrent accesses to different cache banks, however it cannot handle multiple concurrent accesses to the same cache bank. A *cache-bank conflict* occurs when multiple requests to access memory in the same bank are issued concurrently. In the case of a conflict, one of the conflicting requests is served immediately, whereas other requests are delayed until the cache bank is available.

CacheBleed issues a long sequence of read requests to memory addresses in a single cache bank and measures the time it takes to serve all of these requests. This time depends on many factors, one of which is the number of cache-bank conflicts. The diagram below shows histograms of the time to read 256 memory locations under several scenarios. (All examples taken on an Intel Xeon E5-2430 processor.)