Security Now! #558 - 05-03-16

Q&A #233

This week on Security Now!

- The US Congress passed a new eMail privacy act
- Edward Snowden and Fareed Zakaria debate
- The still unresolved fingerprint question
- Android's continuing troubles with “Stagefright”
- Brazilian judge shuts down WhatsApp for three days
- Will the real Satoshi Nakamura please stand up?
- A wonderful new puzzle game discovery and some other miscellany

```
var coffee = new Coffee();
if(coffee.empty) {
coffee.refill();
} else {
coffee.drink();
}
```

Security News

House unanimously passes the Email Privacy Act

- https://www.eff.org/deeplinks/2016/04/house-advances-email-privacy-act-setting-stage-vital-privacy-reform
- House unanimously passes Email Privacy Act, requiring warrants for obtaining emails
  - http://techcrunch.com/2016/04/27/house-unanimously-passes-email-privacy-act-requiring-warrants-for-obtaining-emails/
- Everything You Need to Know About Congress' New Email Privacy Bill
  - http://motherboard.vice.com/read/everything-you-need-to-know-about-congress-new-email-privacy-bill
- House unanimously passes Email Privacy Act, requiring warrants for obtaining emails
  - http://techcrunch.com/2016/04/27/house-unanimously-passes-email-privacy-act-requiring-warrants-for-obtaining-emails/
- Unanimous Passage
  - The U.S. House of Representatives passed the Email Privacy Act (H.R. 699)
  - Requires the government to get a probable cause warrant from a judge before obtaining private communications and documents stored online with companies such as Google, Facebook, and Dropbox.
  - But it DOES NOT require the government to notify users when it seeks their online data. This is considered important so that users may obtain legal counsel to lobby for their rights.
  - Provides long-overdue update to the 30-year old Electronic Communications Privacy Act (ECPA).
  - And formally codifies a Sixth Circuit’s ruling which held that the Fourth Amendment demands that the government first obtain a warrant before accessing emails stored with cloud service providers.

Edward Snowden and Fareed Zakaria (CNN:GPS) - Debates of the century series

- The Motion: "Government should have lawful access to any encrypted message or device."
- https://www.youtube.com/watch?v=-yoyX6sNEqs
- http://bit.ly/sn-558
- Before the debate: No: 77% / Yes: 13 / Undecided: 10
- Boils down to:
  - Snowden took the position that encryption is binary.
  - Fareed took the position that encryption can be used to implement whatever policy we wish.
- After the debate: After: No: 69% / Yes: 22% / Undecided: 9%

The still unresolved fingerprint question

- https://nakedsecurity.sophos.com/2016/05/02/la-judge-forces-woman-to-unlock-iphone-with-fingerprint/
- http://arstechnica.com/tech-policy/2016/05/should-the-govt-be-able-to-force-you-to-open-your-phone-with-just-your-fingerprint/
- http://www.dailygazette.com/news/2016/may/01/government-wants-fingerprints-unlock-phones/
- http://www.engadget.com/2016/05/01/judge-orders-iphone-fingerprint-unlock/
- Law encorcement authorities obtained a search warrant compelling the girlfriend of an alleged Armenian gang member to press her finger against an iPhone that had been seized from a Glendale home.
- The Supreme Court has ruled that police can search your phone if they have a warrant, and that they can order you to produce fingerprints without a court order. However, it's not certain the two can be combined.
- The precedent set by the 2014 Virginia case, which determined that fingerprints are okay, but passcodes are not, but there's no guarantee police can order fingerprint access going forward.
- Up in the air is whether or not using your fingerprint to unlock your phone is a violation of the Constitution's 5th Amendment, which protects against self-incrimination. While a fingerprint isn't the same as testifying, UNLOCKING YOUR PHONE could be treated that way.
- Mary Fan, a law professor at the University of Washington, wrote: "This is why I tell my criminal procedure students that they have more protections if they use a passcode rather than fingerprint to guard entry to their phones. While I don’t conduct crimes on my cell phone, I still decline to use my fingerprint out of an abundance of caution."
- Meanwhile, a 17-year veteran and former sergeant of the Philadelphia Police Department who’s suspected of – but not formally charged with – possession of child abuse images was found in contempt of an order to decrypt two hard drives. He has been imprisoned for 7 months in Philadelphia’s Federal Detention Center on charges of contempt... where, the judge says, he will remain locked up indefinitely until he decrypts the drive, saying that "he carries the keys to his prison in his own pocket.”

Android's continuing troubles with the Mediaserver (Stagefright) module.

- Google renamed "Nexus Security Bulletin" to "Android Security Bulletin", saying: These bulletins encompass a broader range of vulnerabilities that may affect Android devices, even if they do not affect Nexus devices."
- https://threatpost.com/google-patches-more-trouble-in-mediaserver/117758/
- Yesterday Google OTA-patched 32 vulnerabilities in Nexus devices.
- Carriers were sent the patches a month ago, on April 4th.

- Google patched two privately disclosed flaws in the Mediaserver module which exposed devices to remote code execution in versions: 4.4.4, 5.0.2, 5.1.1, 6.0, and 6.0.1.
- Attackers have a number of avenues by which they can exploit these vulnerabilities, most commonly by using malicious MMS and browser playback of media files.
- The crux of the problem is that we're dealing with a shared multimedia processing library that needs to handle a wide range of different input file types and formats. Stagefright is accessible in a number of different ways and media parsers have historically been very problematical. The attack surface is huge because the media decoding library's usage is implied throughout Android, and the rewards are potentially high for a successful attack because the mediaserver runs with privileges to many other parts of the device, like the camera and microphone.

WhatsApp ordered shutdown for 72 hours... back up the next day.

- https://theintercept.com/2016/05/02/whatsapp-used-by-100-million-brazilians-was-shut-down-nationwide-today-by-a-single-judge/
- Same judge as last time.
- From this we learn that "PQP!" is Portuguese for "WFT!"
- http://www.theverge.com/2016/5/3/11580948/brazil-court-order-overturn-whatsapp-service-restored

  A Brazilian judge has overturned the country's blackout of the WhatsApp texting service, restoring service to over 100 million people in the country. The reversal comes just one day into the mandated blackout period, which was initially scheduled to last for 72 hours. The blackout order specifically targeted Brazilian wireless carriers, which were forbidden from transmitting WhatsApp data for the duration of the blackout period. Any carrier found violating the order would have been fined 500,000 reals, or roughly $140,000.

  The blackout began yesterday, after a long fight over an order served to WhatsApp by Brazil's civil police. Because of WhatsApp's end-to-end encryption system, the company has no records of what users say within the app, and cannot fulfill warrants requesting that information. In a Facebook post yesterday, WhatsApp founder Jan Koum defended the system saying, "we have no intention of compromising the security of our billion users around the world."

Who is Satoshi?

Linkfest:

- http://digg.com/2016/craig-wright-satoshi-nakomoto
- https://www.wired.com/2016/04/prove-youre-bitcoin-creator-satoshi-nakamoto/
- http://thehackernews.com/2016/05/bitcoin-founder.html
- http://www.drcraigwright.net/jean-paul-sartre-signing-significance/

- https://github.com/patio11/wrightverification/blob/master/README.md
- http://www.bbc.com/news/technology-36168863

"Extraordinary Claims Require Extraordinary Proof"
@SGgrc: I sure hope this clown is NOT Satoshi. Get a load of this latest spew of nonsense:
http://www.drcraigwright.net/extraordinary-claims-require-extraordinary-proof/
Robert Graham / Errata Security

- Satoshi: how Craig Wright's deception worked
  - http://blog.erratasec.com/2016/05/satoshi-how-craig-wrights-deception.html

Follow ups

Ando David Roots (@SQrooted) / 4/29/16, 11:18 PM
In the latest Security Now episode you and Leo agreed that turning off the computer adds no real security. This is not the case when we're not talking of a home computer which is in a "safe" environment - your house. I work in a bank; my workstation stays in the office after I leave for the day. I always turn it off each day, even though it adds a minute of boot time for tomorrow. The reasons are as follows: - I do not know who has physical access to the PC when I'm gone - I've set BIOS passwords (boot and admin) which should at least make it more difficult to boot the OS or from USB - I've encrypted my HDD which has to be "unlocked" before boot - I have no real faith in the Ubuntu "lock screen" - there are ways to bypass it - When shut off, there is nothing in the RAM - no loaded SSH keys (SSH agent), no login passwords

Errata

Paddy Kerley / @LegendaryPatMan / 11:00am · 27 Apr 2016 · Twitter Web Client

- @SGgrc Really Steve!? Pipe this random script from a guy called Infection to install something?! What happened to TNO?

Miscellany

Steve has a new puzzle passion

Steve's Prior Puzzle Picks:

- Rails
- Blockwick
- Hook
- Osmos HD
- Infinite Loop
- Auralux

"The Sequence"

- Pete Shanahan 1.0.1? @petesh
    - @SGgrc you are the only person who's game recommendations get immediately purchased/downloaded. You have stellar taste sir.
- Thank you, Pete. Because people have figured out that I love puzzles, I get lots of recommendations. But only a few make it through my own filter. So I'm always excited to share those that do. My criteria are clear: No hurry, no timers, no reflexes tested, no unnecessary punishment, under-designed not over-designed, no hidden stuff that you need to poke at to find. Just the kind of thing where everything you need to know is in front of you so that you can stare at the screen for a long time running possibilities through your mind. This one goes a bit further and is actually charming/humorous in its execution. I think people who have enjoyed my previous discoveries will find this one equally wonderful. Thanks again.
- WARNING! Another joyful productivity sink ahead: "The Sequence" gets my absolute
- http://ombgames.com/
- https://twitter.com/OneManBand300
- [the Sequence] is a Grand Prize Winner in the Unity Game Developer Contest 2016! https://unity3d.com/contest/windows #indiedev #gamedev #unity3d
- Here's an animated GIF to give you a taste of what "The Sequence" (see previous tweet) looks like: http://bit.ly/1YVUjj2
- http://1.bp.blogspot.com/-qLwxIGTA0Gc/VNx3IxIEj7I/AAAAAAAAAH8/opETkOeIqAo/s1600/gameplay1.gif
- Not a great video: https://www.youtube.com/watch?v=bq3Q0OR1NeU
- http://onemanbandgames.blogspot.com/2015/07/the-sequence.html
- iOS: https://itunes.apple.com/us/app/the-sequence/id1035217840?mt=8
- Android: https://play.google.com/store/apps/details?id=com.onemanband.thesequence&hl=en
- Steve Gibson @SGgrc
    - Total Puzzle Toy Win!: "The Sequence" 99 cents and worth every penny!
    - iOS: http://j.mp/seq99a
    - Android: http://j.mp/seq99b
    - Really!!
    - First 13 levels FREE on Android: http://j.mp/seq00b
- https://play.google.com/store/apps/details?id=com.onemanband.thesequence
- https://play.google.com/store/apps/details?id=com.onemanband.thesequencelite
- Pusher
- Revolver
- Spinner
- Shuttle
- Polarity reverser

- Hard Logic:
    - https://play.google.com/store/apps/details?id=com.onemanband.hardlogicfree
    - https://play.google.com/store/apps/details?id=com.onemanband.hardlogic

KB3035583 - Changing again. WHY?? !!!!

The BEST multi-port high-current USB charger i've found:

- ANKER
- 60W, 6-Port Desktop Charger (available in black or white)
- http://www.amazon.com/dp/B00P936188
- 2,057 5-Star reviews

SpinRite

Simon Willcock in Manchester UK

Subject: Is a disk is good if SpinRite finds no faults?

:

Steve a quick question - I have a friend whose introduction to her laptop was "The disk is dead; can you get me a new one?" I asked if I could run SpinRite on it, she agreed and I ran it at both at level 2 & 4 and no errors were found! She is convinced that she needs a new disk (PC World tech guy told her so) - from what I can see - there is no problem with the disk. How confident can I be?

Thanks, Simon

Next Week: Samsung SmartThings hacked