Security Now! #466 - 07-29-14

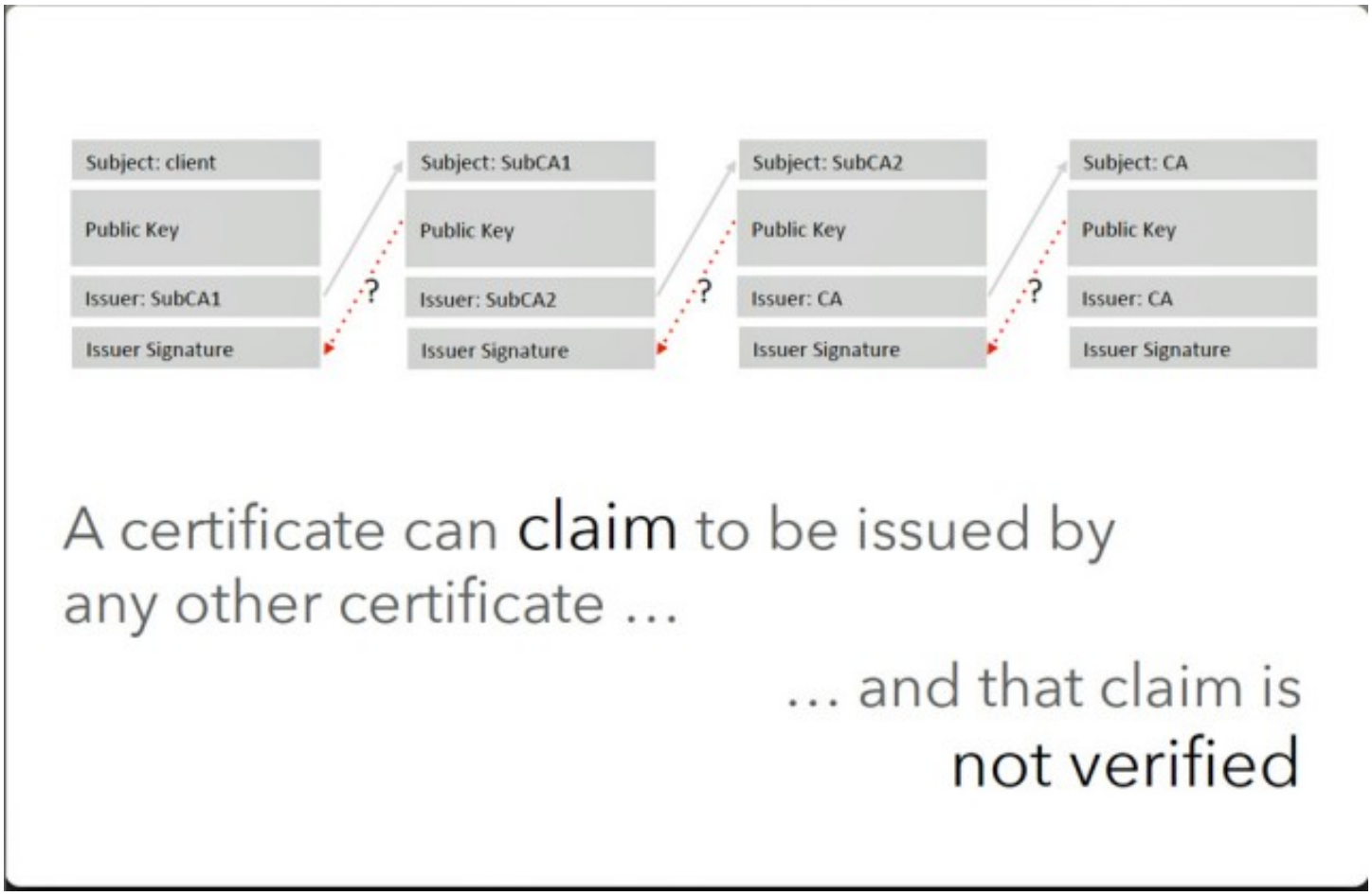
Q&A #193

Link Tracking Warning!
This document was first authored in Google Docs, then Downloaded as a PDF. So, Google has thoughtfully (ha!) added "tracking" redirections to all of the links here. (I have no idea why, but that's Google.) If that bothers you, simply copy the text of the link into your browser's URL field.

This week on Security Now!

- iOS v7 HAS been Jailbroken -- more often than not!
- Some quick follow-ups to iOS backdoors and Canvas fingerprinting
- WhisperSystems' truly secure "RedPhone" comes to iPhone as "Signal"
- Android found not to be checking certificate chains
- Some further clarification in the Verizon vs Level3 argument, and an apparent resolution
- Miscellaneous tidbits, including news of the emerging next-generation memory technology
- And ten thought-provoking questions and comments from our listeners

Android's "Fake ID" vulnerability (Slide from next week's BlackHat Presentation)



Errata:

- iOS v7 Jailbroken

Security News:

Apple "Nefarious Data Spilling Process Drama"

- Apple responds with additional service clarification
  - http://support.apple.com/kb/HT6331
- Jonathan is not moved
- Dan Goodin at ArsTechnica continues to report.
- A very sane top blog posting by "TheShark"
- "TheShark" wrote:
  I'm trying to get upset over this latest 'revelation' but somehow I just can't. Take the pcapd capability for example. Why should I be worried that a computer which I've already configured to sync my phone with and which is on the same WiFi network can activate pcapd on my phone? That computer is almost certainly in a position to run pcapd locally and capture the WiFi traffic. There's no reason to think that the pcapd on the phone is going to see traffic that the computer can't. It's the same thing with most of the other data which is accessible. A computer which I've chosen to sync with can actually access my contacts, photos and other data which I want to sync? This is a concern? I can imagine some app developers getting worried that authentication tokens which they don't sync and don't want users to be able to directly access are now available but it's also easy to imagine how useful it would be in debugging your app to get access to those files as well. Sorry Johathan, but I'll be more impressed when you find an actual backdoor. This seems far more like a useful tool than a nefarious one to me.

Canvas Fingerprinting

- https://www.browserleaks.com/canvas
- 1847 unique signatures (10.851 effective bits)
- Local JS always required for "canvassing"

"Open WhisperSystems"

- WhisperSystems (Moxie Marlinspike) acquired by Twitter (Nov 28, 2011), but some software then made open source (July 2012).
- Open Whispersystems Project now moving forward.
- Everything is free and open source
- <quote> "Secure Calls Are Just The Beginning:"
  "Signal" will be a unified private voice and text communication platform for iPhone, Android, and the browser. Later this summer, Signal for iPhone will be expanded to support text communication compatible with TextSecure for Android. Shortly after, both TextSecure and RedPhone for Android will be combined into a unified Signal app on Android as well. Simultaneously, browser extension development is already under way.

- And the price is right... FREE!

Android "Fake ID" vulnerability

- To be shown during next week's BlackHat Conference
  - by Jeff Forristal, CTO of Bluebox Security
  - http://bluebox.com/technical/android-fake-id-vulnerability/
- Dan Goodin for ArsTechnica:
  - Android Fake ID Vulnerability Lets Malware Impersonate Trusted Applications, Puts All Android Users Since January 2010 At Risk
  - <quote> The majority of devices running Google's Android operating system are susceptible to hacks that allow malicious apps to bypass a key security sandbox so they can steal user credentials, read e-mail, and access payment histories and other sensitive data, researchers have warned.
- Since v2.1, January of 2010.
- Exists in the Android 'L' preview.
- App certificates allow selective app-sandbox bypass for authorized apps.
- For example, Adobe's FLASH is allowed to act as a plug-in for any other app installed on the phone, presumably to allow it to provide animation and graphics.
- Or Google Wallet is permitted access to NFC hardware for payment processing.
- But any maliciously developed app can simply include an invalid certificate CLAIMING to be Flash or Wallet... and thus gain those privileged application app permissions.
- Jeff Forristal, the CTO of Bluebox Security said: "All it really takes is for an end user to choose to install this fake app, and it's pretty much game over. The Trojan horse payload will immediately escape the sandbox and start doing whatever evil things it feels like, for instance, stealing personal data."
- Google Responded to this news:
  - <quote> We appreciate Bluebox responsibly reporting this vulnerability to us; third-party research is one of the ways Android is made stronger for users. After receiving word of this vulnerability, we quickly issued a patch that was distributed to Android partners, as well as to AOSP. Google Play and Verify Apps have also been enhanced to protect users from this issue. At this time, we have scanned all applications submitted to Google Play as well as those Google has reviewed from outside of Google Play, and we have seen no evidence of attempted exploitation of this vulnerability.
- Google bug 13678484
- Bluebox Security Scanner checks for Fake ID Vulnerability:
  - https://play.google.com/store/apps/details?id=com.bluebox.labs.onerootscanner

Verizon Policy Blog: Level 3's Selective Amnesia on Peering

- http://publicpolicy.verizon.com/blog/entry/level-3s-selective-amnesia-on-peering

To: HTTPS Fingerprinting Feedback

- From: "G Evans"
  Subject: machine-resident interception
  Date: Thu, 24 Jul 2014 00:45:58 -0000

  In your paragraph about machine-resident interception, you can add Avast antivirus to the list. There is an innocuous settings checkbox that says "Scan secure connections" with no

other explanation. Sounds like a good idea, until I read your fingerprints page in Firefox and noticed the lack of a green label in the address bar. When I hovered over the lock symbol, it said "Verified by Avast" as opposed to "Verified by DigiCert". Oops. I immediately turned off that option in Avast, and now it's back to normal.

Miscellany:

High-Speed Construction of the Brickhouse…

- In some high speed scenes the camera's position is smoothly changing... how?

"Lucy"

Memristors

- http://www.technologyreview.com/news/529386/super-dense-computer-memory/
- http://www.technologyreview.com/news/517996/denser-faster-memory-challenges-both-dram-and-flash/
- https://www.crossbar-inc.com/
- Current FLASH technology allows for about 16 gigabytes on a 200 mm^s chip.
- Resistive RAM (RRAM) allows for one terabyte in the same space.
- NNAND is a 3-terminal technology, RRAM is two terminal.
- This allows not only for much greater per-cell density, but also 3D ram (stacking layers).
- <quote from Crossbar> With 20X higher performance and 20X lower power than NAND, and 10x the endurance at half the die size, Crossbar has shattered traditional technology barriers for NOR (code), NAND (data) and embedded memory applications and will enable a new wave of electronics innovation for consumer, enterprise, mobile, industrial and connected device applications.

SpinRite:

Ron Tyska (@rontyska) · 5:21pm · 28 Jul 2014 · Tweetbot for iOS
@SGgrc Spinrite revived a completely dead ssd, saved me $400. Thanks!

Note: Anything SpinRite can fix... it WOULD have prevented.

On to our Q&A!...