Security Now! #474 - 09-23-14
Q&A #197

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!

- Apple's iOS8 security and an interesting analysis of the iOS trusted root store
- Cloudflare announces "Keyless SSL"
- Google and Dropbox team up in a new venture.
- Google shuts down a "Malvertiser" who was using its DoubleClick network.
- A HUGE THANKS to all Android Users Everywhere!!... and...
- Q&A #197

Security News:

Apple's iOS8 Security

- http://www.wired.com/2014/09/apple-iphone-security/
- https://gigaom.com/2014/09/18/apples-warrant-canary-disappears-suggesting-new-patriot-act-demands/
- http://reason.com/blog/2014/09/18/apples-new-marketing-plan-screw-the-poli
- http://gizmodo.com/police-can-still-get-data-off-your-ios-8-device-without-1636831283
- http://bgr.com/2014/09/19/iphone-6-security-and-privacy/

iOS8's Trust Root Store

- http://karl.kornel.us/2014/09/an-analysis-of-the-cas-trusted-by-ios-8-0/
- 222 certificates:
  - 4096-bit RSA: 44 CAs
  - 2048-bit RSA: 138 CAs
  - 1024-bit RSA: 27 CAs
  - 384-bit ECC: 12 CAs
  - 256-bit ECC: 1 CA

- How are these certs SIGNED by they CA's?
  - SHA-512: 1 CA
  - SHA-384: 17 CAs (including 12 of the CAs using ECC keys)
  - SHA-256: 42 CAs (including 1 of the CAs using ECC keys)
  - SHA-1: 149 CAs
  - MD-5: 10 CAs
  - MD-2: 3 CAs

- The following vendors have more than 3 CAs in iOS 8.0:
    - AC Camerfirma SA: 4 CAs
    - Apple: 4 CAs
    - Comodo: 4 CAs
    - Digicert: 8 CAs
    - Entrust: 5 CAs
    - Geotrust: 4 CAs
    - Globalsign: 6 CAs
    - Netlock Kft: 5 CAs
    - Symantec: 6 CAs
    - TC Trustcenter GMBH: 6 CAs
    - Thawte: 12 CAs
    - The Usertrust Network: 5 CAs
    - Verisign: 17 CAs

- Governments: A number of governments have CAs in iOS 8.0:
  (Those that were obvious to Karl were):
    - China: 1 CA, via the China Internet Network Information Center
    - Hong Kong: 1 CA, via the Hongkong Post e-Cert.
    - Japan: 3 CAs, via GPKI and the Ministry of Public Management, Home Affairs, Posts, and Telecommunications (MPHPT)
    - Netherlands: 3 CAs, via PKIoverheid
    - Taiwan: 1 CA, via the Government Root Certification Authority
    - Turkey: 1 CA, via the Scientific and Technological Research Council of Turkey
    - United States: 5 CAs, via the Department of Defense

CloudFlare's Keyless SSL
https://blog.cloudflare.com/keyless-ssl-the-nitty-gritty-technical-details/
http://blog.cloudflare.com/announcing-keyless-ssl-all-the-benefits-of-cloudflare-without-having-to-turn-over-your-private-ssl-keys/
https://gigaom.com/2014/09/18/cloudflare-launches-new-way-to-enforce-security-with-keyless-ssl/
http://arstechnica.com/information-technology/2014/09/in-depth-how-cloudflares-new-web-service-promises-security-without-the-key/

Google & Dropbox launch new joint venture: "Simply Secure"

- https://simplysecure.org/who-we-are/
- http://www.theguardian.com/technology/2014/sep/18/google-dropbox-simply-secure-security-tech
- Searching for ways to bring "security in the lab" to the real world.

Google takes down a Malvertiser:

- http://arstechnica.com/security/2014/09/google-stops-malicious-advertising-campaign-that-could-have-reached-millions/
- http://www.zedo.com/
- Advertiser Zedo was using Google's DoubleClick to load the "Zermot" downloader onto victim machines. The ads were being served to "Last.fm", "The Times of Israel", and "The Jerusalem Post." So visitors to those sites ran the risk of having their machines infected.
- Zemot: Well known to Microsoft, Windows Defender, and Microsoft Security Essentials.

Miscellany

- iPhone 6+:
  - I found myself comfortably reading PDF and actually using Safari on the 6+.
  - Looking back at the 5S... it's SO TINY!
  - Swype:
    - Fully functional without allowing "full access"
    - Running on iPads -- SwiftKey says iPad doesn't give them enough memory alloc.
    - Swype is not free, but I'm happy to have paid for it.
    - More powerful with shortcuts and hold-delay vs shift key for symbols.

SpinRite:

- From: "Martin" <interwebss@me.com>
  Subject: Level2 "Look but don't touch" actually DOES save the day! Spinrite story
  Date: Wed, 10 Sep 2014 12:09:23 -0000
  Location: Frankfurt / Germany

  Hello Steve,

  Thanks for answering my question about how Spinrite on level 2 actually fixes things on one of the last shows! Only a few days later I was witness to it actually fixing a huge problem by using level 2.

  A friend's work PC refused to boot and his company's IT department gave up on it, without being able to recover ANY of his valuable data. Of course the backup had failed without him or any one else noticing and his data was gone... So we gave SpinRite a try on level two and it slowed down and started working a lot harder about a quarter of the way in, seemingly not to move any further. So my friend lost patience after a while and turned the machine off. I told him to not give up and just let Spinrite run for however long it takes. After about 8 hours of chewing on the drive, it finished, the PC booted again with complete data recovery. Hooray to SpinRite! Now I am his hero, but actually you are! Thank you very much on behalf of my friend who got all of his data back thanks to SpinRite.

  Martin