Security Now! #440 - 01-28-14
Q&A #182

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!

- More Point-of-Sale (Point of Fail?) Malware News
- How to overtrain Apple's TouchID for reliability
- CryptoLocker is far from dead
- The never ending NSA news machine
- How BlueTooth Low Energy's "Just Works" pairing is "Just Broken"
- A couple useful security sites.

Security News:

PoS Malware

- 1100-branch Arts & Framing "Michaels" stores appear to have been breached
- Brian Krebs:
  - Multiple sources in the banking industry say they are tracking a pattern of fraud on cards that were all recently used at Irving, Texas-based Michaels Stores, an arts-and-crafts retailer that has more than 1,100 stores in the United States and Canada.
    On Friday, KrebsOnSecurity heard from a fraud analyst at a large credit card processor that was seeing fraud on hundreds of cards over the previous two days that all been recently used at Michaels. The fraudulent purchases on those cards, the source said, took place at the usual big box stores like BestBuy and Target.

Overtraining the Applie iPhone 5S fingerprint scanner.

- Open Settings App
  - General
    - TouchID & Passcode
      - TouchID
        - At the bottom is a list of registered fingerprints…
        - and training is still active.
        - How to demonstrate that for yourself.

New versions of CryptoLocker no longer being well detected. (thanks to Simon)

- https://www.grc.com/malware.htm

Cellular phone metadata collection ineffective:

- http://www.wired.com/threatlevel/2014/01/watchdog-phone-spying-illegal/
- www.firstpost.com/world/us-government-panel-urges-end-to-phone-data-spying-1356787.html
- Washington: A government review panel warned Thursday that the National Security Agency's daily collection of Americans' phone records is illegal and recommended that President Barack Obama abandon the program and destroy the hundreds of millions of phone records it has already collected.
- <quote>
  In addition to concluding that the daily collection of phone records was illegal, the board also determined that the practice was ineffective.

  "We have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation," it said, and added, "We are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack."

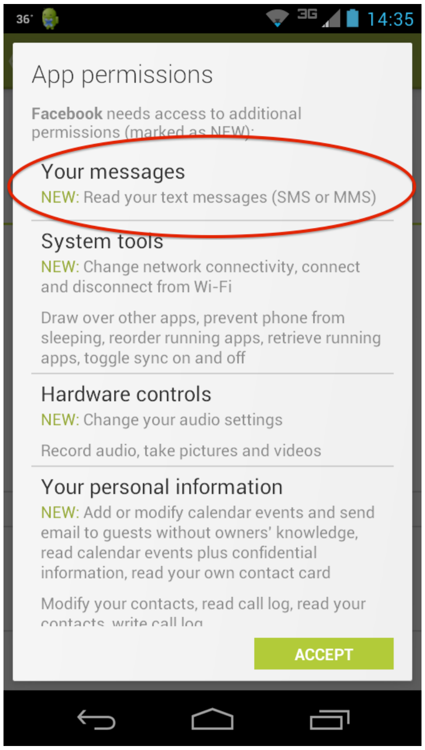
  It said the NSA should instead seek individual records relevant to terror cases directly from phone service providers under existing laws.

NSA May Want Mobile Data, Including Info From Angry Birds And Maps

- http://techcrunch.com/2014/01/27/nsa-may-want-mobile-data-including-info-from-angry-birds-and-maps/
- Project "Golden Nugget"
- Rovio, makers of Angry Birds, vigorously denied cooperating with the NSA.

Facebook's update for Android requires permission to access all text messages.

- http://tony.calileo.com/fb/



App permissions

Facebook needs access to additional permissions (marked as NEW):

Your messages
NEW: Read your text messages (SMS or MMS)

System tools
NEW: Change network connectivity, connect and disconnect from Wi-Fi

Draw over other apps, prevent phone from sleeping, reorder running apps, retrieve running apps, toggle sync on and off

Hardware controls
NEW: Change your audio settings

Record audio, take pictures and videos

Your personal information
NEW: Add or modify calendar events and send email to guests without owners' knowledge, read calendar events plus confidential information, read your own contact card

Modify your contacts, read call log, read your contacts, write call log

Beware Bluetooth LE (BLE) "Just Works" pairing

- http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3478807/
- Pairing comprises three phases. In the first phase, the two connected devices announce their input/output capabilities and, based on these, they choose a suitable method for the second phase.

  The second phase has the purpose of generating the Short-Term Key (STK), which will be used in the third phase to secure the distribution of key material. In the second phase, the pairing devices first agree on a Temporary Key (TK), by means of the Out Of Band, the Passkey Entry or the Just Works methods. The Out of Band method uses out of band communication means (e.g., NFC [9]) for the TK agreement. In the Passkey Entry method, the user passes six numeric digits as the TK between the devices. When none of the first two methods can be used, the Just Works method is employed, although it is not authenticated and it does not provide protection against Man In The Middle (MITM) attacks [10]. Based on the TK, and on random values generated by each pairing device, the STK is obtained by both devices, which leads to the end of the second phase.

  In the third phase, each endpoint of the connection may distribute to the other endpoint up to three 128-bit keys called the Long-Term Key (LTK), the Connection Signature Resolving Key (CSRK) and the Identity Resolving Key (IRK). The LTK is used to generate the 128-bit key employed for Link Layer encryption and authentication. The CSRK is used for the data signing performed at the ATT layer. The third key (i.e., the IRK), is used to generate a private address on the basis of a device public address. The message exchange required for distributing the LTK, the CSRK or the IRK is encrypted by using the STK obtained in the second phase.

- https://developer.bluetooth.org/TechnologyOverview/Pages/LE-Security.aspx
- Association Models:
  Bluetooth Smart (low energy) technology uses three association models referred to as Just Works, Out of Band and Passkey Entry. Bluetooth low energy technology does not have an equivalent of Numeric Comparison. Each of these association models is similar to Secure Simple Pairing with the following exception; Just Works and Passkey Entry do not provide any passive eavesdropping protection. This is because Secure Simple Pairing uses Elliptic Curve Diffie-Hellman and Bluetooth Smart (low energy) does not. The use of each association model is based on the I/O capabilities of the devices in a similar manner as Secure Simple Pairing.

- http://blog.lacklustre.net/posts/BLE_Fun_With_Ubertooth:_Sniffing_Bluetooth_Smart_and_Cracking_Its_Crypto/
- https://lacklustre.net/bluetooth/Ryan_Bluetooth_Low_Energy_USENIX_WOOT.pdf
- Mike Ryan: Bluetooth: With Low Energy comes Low Security
- Section: 6 - Bypassing the Encryption
  BTLE features encryption and in-band key exchange. Rather than relying on a well-established key exchange protocol such as one based on Elliptic Curve Diffie-Hellmann (ECDH) [3], the Bluetooth SIG invented their own key exchange protocol. We demonstrate that this key exchange protocol has fundamental weaknesses that undermine the privacy of communication against passive eavesdroppers.

TSA Precheck

- I received my "Known Traveller Number" last Wednesday, so after exactly one week.
- From a listener named Martin Ruby:

  Steve,

  I have been a TSA Pre flyer since the day's when it was a test.

  There are two ways to get TSA Pre, the first is the way you did by applying for it the second is by being an airline frequent flyer. If your airline participates is TSA Pre they can submit you information to the TSA vouching for you as a KNOWN TRAVELER on that airline. The difference between the two is when you apply to the TSA it is good on any airline that participates in the program and if it is by the airline submitting your information it is only valid on that airline.

  I'm a proud owner of SpinRite since the days of OCIPUG when you would come and present and have used it many times to fix drive issues.

  Thank you for a great product and a fantastic podcast.

  Martin Ruby

- Favorite Feedback Comment: (Anonymous)
  Subject: TSA Pre screen
  Steve... It is almost certain you have a file and a set of agents assigned to you. Of course they don't need to interview you. The file probably says "smart guy, mostly harmless. Best not to annoy him"

Two useful security sites:

- **How's My SSL:**
  - https://www.howsmyssl.com/
  - Ratings:
    - Firefox: Your SSL client is Bad.
      - TLS v1.1 not TLS v1.2
      - Supports: SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
      - "This cipher was meant to die with SSL 3.0 and is of unknown safety."
    - Opera (Latest version): Your SSL client is Bad.
      - TLS v1.0
      - Improvable: No session ticket support.
    - IE 11: Your SSL client is Improvable.
      - Improvable: No session ticket support.
    - Safari: Your SSL client is Improvable.
    - Chrome: Your SSL client is Probably Okay.
      - "Good" on everything.
  - The site's "About" page is useful.

- **TrueCrypt's Audit Status:**
    - http://istruecryptauditedyet.com/

SQRL Project Update:

- **SQRL / EnScrypt page completed - rather complete password tutorial.**
- https://www.grc.com/sqrl/scrypt.htm (page #10 of 18)
- Now working on thinking about the user's experience.

A Short SpinRite Shoutout:

James Cavanaugh in Dresden, Germany: I just wanted to say THANKS for recovering my apparently dead drive's data when nothing else could. I tried so many other programs, unsuccessfully! And after all of them, SpinRite's apparent ease-of-success really convinced me. What a difference! Also intuitive and easy to use. It just does the job. Great product!