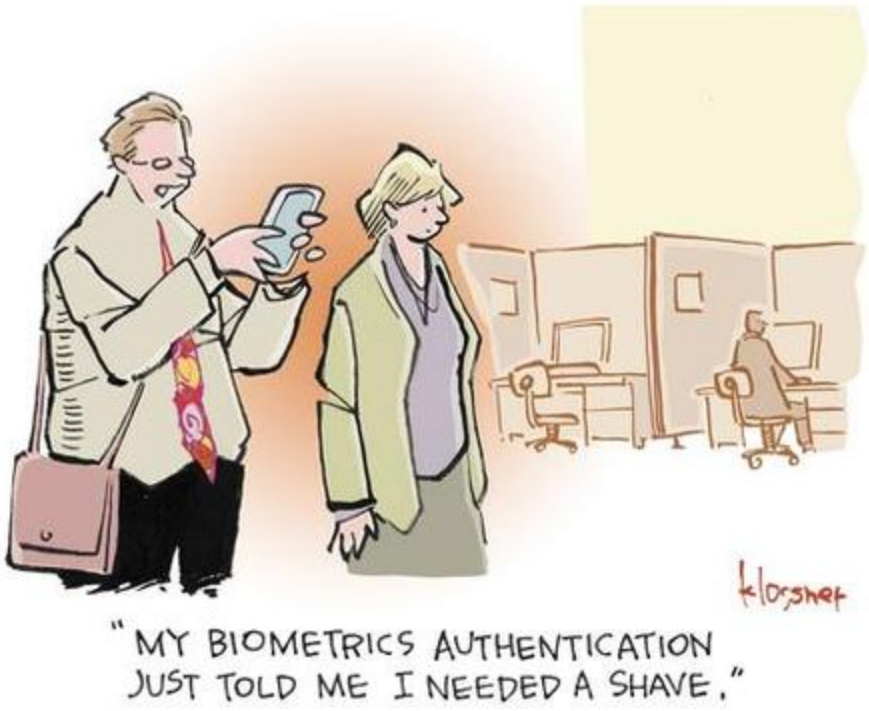
Security Now! #505 - 04-28-15

Q&A #211

This week on Security Now!

- A bunch of interesting revelations from last week's RSA Conference:
  - WiFi access points can crash iOS devices.
  - Samsung's S5 fingerprint reader leaks biometrics like a sieve.
  - CryptoWall installed via malicious ads for two months.
- Another (worse) problem in the iOS AFNetworking library.
- An Open Source bug bites the Yubikey NEO.
- Some thoughts about ad blocking... and more!



Security News!

RSA: **"No iOS Zone" Vulnerability allows a DoS attack on iOS devices**

- "Skycure" during RSA Conference last Tuesday revealed the flaw in iOS.
- Bad Headlines:
  - "Security Flaw in iOS 8 Can Permanently Crash Your iPad Or iPhone"
  - "iOS bug sends iPhones into endless crash cycle when exposed to rogue Wi-Fi"
  - "Researchers find another terrifying iOS flaw"

    - "Potentially ‘catastrophic’ weakness allows targeted attacks against iPhones"
- https://www.skycure.com/blog/ios-shield-allows-dos-attacks-on-ios-devices/
- An SSL certificate parsing vulnerability.
- It has been confirmed fixed in v8.3.
- AT&T phones automatically connect to any WiFi network named "attwifi"
- Malicious hotspot named "attwifi" would DoS all iOS devices within range.

Samsung S5 Fingerprint Reader Flaw Discovered

- RSA Conference, Friday...
- FireEye: "To Swipe or Not to Swipe: A Challenge or Your Fingers."
- https://www.rsaconference.com/writable/presentations/file_upload/hta-f01-to-swipe-or-not-to-swipe-a-challenge-for-your-fingers_final.pdf
- Points:
    - Password leaked, change it.
    - Fingerprint image leaked…
- Three attacks on Android Fingerprints:
    - Confused Authorization Attack
    - Fingerprint DB Manipulating
    - Fingerprint Sensor Spying Attack
- <quote> Android phones typically store sensitive data such as fingerprint information in a walled-off area of memory known as the Trusted Zone.

  However, FireEye researchers found it was possible to grab identification data before it is locked away in the secure area. This method of stealing data was available on all phones running version 5.0 or older versions of Android provided the attacker got high level access to a phone.

  They also found that on Samsung Galaxy S5 phones, attackers did not need this deep access to a phone. Instead, just getting access to the gadget's memory could reveal finger scan data.

  Using this information an attacker could make a fake lock screen that makes victims believe they are swiping to unlock a phone... when they are actually authorizing a payment.

  In addition, they found, it was possible for attackers to upload their own fingerprints, then authenticate to the device, since devices did not keep good records of how many prints were being used on each device.

  The flaws they uncovered were widespread throughout handsets running Android 5.0 and below. Updating to the latest version of Android, version 5.1.1, should eliminate the vulnerabilities.

CryptoWall installed via malicious ads for two months

- http://www.darkreading.com/attacks-breaches/zero-day-malvertising-attack-went-undetected-for-two-months/d/d-id/1320092
- RSA presentation by researchers at MalwareBytes
- Cybercriminals used an Adobe FLASH player zero-day vulnerability.
  - Use-after-free vulnerability, CVE 2015-0313. Patched by Adobe on Feb. 2
  - The next day the attack campaign stopped.
- First seen on December 10, 2014.
- Attackers used the #1 online advertising network to host malicious ads on, at least:
  - Dailymotion, Huffington Post, answers.com, New York Daily News, HowToGeek.com, tagged.com, and others.
- Each of the affected websites ran the malicious ads for approximately two days.
- The attackers used the HanJuan exploit kit, hosted on rotating domains to evade detection.
- US consumers behind residential IP addresses.
- NO ACTION needed for infection. If FLASH ran, you were infected.

Another (worse) problem discovered in the iOS AFNetworking library

- http://arstechnica.com/security/2015/04/24/critical-https-bug-may-open-25000-ios-apps-to-eavesdropping-attacks/
- This time 25,000 to 50,000 apps are at risk. (Last week, 1,500 apps.)
- The domain name of the presented certificate is never compared with the remote server's.
- Any attacker can present ANY valid certificate for ANY domain and ANY iOS app compiled with the AFNetworking library prior to the just released v2.5.3 won't notice.
- The previous bug (from last week) was just introduced in the previous January release.
- THIS bug as been present in all v2.x... thus affecting MANY more apps.
- Free search tool: http://searchlight.sourcedna.com/
- A quick check found that apps from Bank of America, Wells Fargo, and JPMorgan Chase were likely affected, although some of those reports may be false positives. It's possible that some apps flagged by SourceDNA use custom code or secondary measures such as certificate pinning that prevents attacks from working.
- WHY DID THIS HAPPEN?
  - Unbelievably: The library's configuration default was changed NOT TO CHECK the domain name.
  - "validatesDomainName" -- defaulted to 'NO'

Yubikey NEO PIN bypass...

- Security advisory 2015-04-14
- There was a logical mistake in the code Yubico inherited from the JavaCardOpenPGP project.
- The source code contains a logical flaw related to user PIN (aka PW1) verification that allows an attacker with local host privileges and/or physical proximity (NFC) to perform security operations without knowledge of the user's PIN code.
- In a conjunction, the logical AND '&&' should have been a logical OR '||'.
  - if (!pw1.isValidated() && !pw1_modes[PW1_MODE_NO8x])

```
ISOException.throwIt(SW_SECURITY_STATUS_NOT_SATISFIED);
// otherwise execution continues
```

- The JavaCardOpenPGP project has been notified.
- <quote> Yubico will replace your YubiKey NEO if you are using the OpenPGP applet version 1.0.9 or earlier (as described in this advisory). Go to https://yubi.co/support to learn how to log a support ticket and receive a replacement.

What could go wrong dept: "Amazon to deliver packages direct to vehicle trunks"
http://www.ft.com/intl/cms%2Fs%2F0%2F53247f78-e8da-11e4-87fe-00144feab7de.html

- *Amazon to deliver parcels to Audi "boots" (car trunks) in Germany*
  <quote> Together with delivery partner DHL, [Amazon and Audi] aim to ease a common frustration among commuters: never being at home when the delivery company brings goods that were purchased online.

  "Parcel-to-vehicle" delivery might help reduce the number of failed delivery attempts and temper a parcel logjam in large offices caused by employees who input their employers' address when ordering goods.

  Carmakers are seeking to offer an array of add-on "connected" services to retain tech-savvy customers and ensure the profits accrue to them, and not to software companies.

  Audi said there were no vehicle insurance implications because the delivery agent will not be able to access the vehicle cabin.

  The carmaker said that in future customers would also be able to send letters or parcels left in the trunk of their car and Amazon said it was working on a solution to allow goods to also be returned via the boot.

  When ordering, Amazon customers will indicate the rough location of the vehicle and desired delivery time. A DHL delivery agent will later be notified of the exact location via a smartphone app.

  The agent is granted one-time keyless access to the boot of the vehicle and when the boot is shut again, it locks automatically. The customer must agree for their vehicles to be tracked for a specific timeframe and is notified via email upon successful delivery.

"Why Ad Blocking is devastating to the sites you love"

- Ken Fisher, founder & Editor-in-Chief of Ars Technica, March 6th, 2010
- http://arstechnica.com/business/2010/03/06/why-ad-blocking-is-devastating-to-the-sites-you-love/
- Article begins…
  - Did you know that blocking ads truly hurts the websites you visit? We recently learned that many of our readers did not know this, so I'm going to explain why.
- Github: uBlock
  - https://github.com/chrisaljoudi/uBlock

- What:
  - uBlock is a general-purpose blocker — not an ad blocker specifically.
  - uBlock blocks ads through its support of the Adblock Plus filter syntax.
  - uBlock extends the syntax and is designed to work with custom rules and filters.
  - uBlock's main goal is to help users neutralize privacy-invading apparatus — ads being one example.
- Where:
  - Safari: available to install from the homepage, or from the Safari Extension Gallery.
  - Chrome: available on the Chrome Web Store or for manual installation.
  - Opera: available on the Opera Store.
  - Firefox: available on the Firefox Add-ons homepage, or for manual installation.
- Comparisons to AdBlockPlus:
  - Lower memory usage, lower CPU usage, significantly lighter weight.
  - Still pulls from Easylist.
- Manifesto:
  - The user decides what web content is acceptable or not in their browser.
  - Users are best placed to know what is or is not acceptable to them.
  - uBlock's sole purpose is to give users the means to enforce their own choices.

Installing TrueCrypt on Yosemite 10.10

- Truecrypt 7.1a requires Mac OS X 10.4 or later... on Yosemite 10.10
- http://apple.stackexchange.com/questions/173879/truecrypt-7-1a-requires-mac-os-x-10-4-or-later-on-yosemite-10-10/173880#173880
- Google: "truecrypt requires mac osx or later"

Miscellany

HOOK -- OMG!

- http://playthehook.com
- HTML/JS version on Kongregate

Apple Watch:

- How can it possibly be that the $300 band is too small?

PDP-8/I

- http://bit.ly/pdp8kit
- http://obsolescence.wix.com/obsolescence#!pidp-8-get-one/ctny
- *VERY* affordable PDP-8 kit using Raspberry PI and well-known emulator.

"The Americans" on FX

- Season 3 ended... OMG!

SpinRite:

	**Steve Gibson (@SGgrc)**
4/2/14, 12:57 PM RT @seanmmccormack: Thank you @SGgrc ! pic.twitter.com/J11Q76RLiB (With SpinRite, "R" stands for "Recovered" an unreadable sector! :)