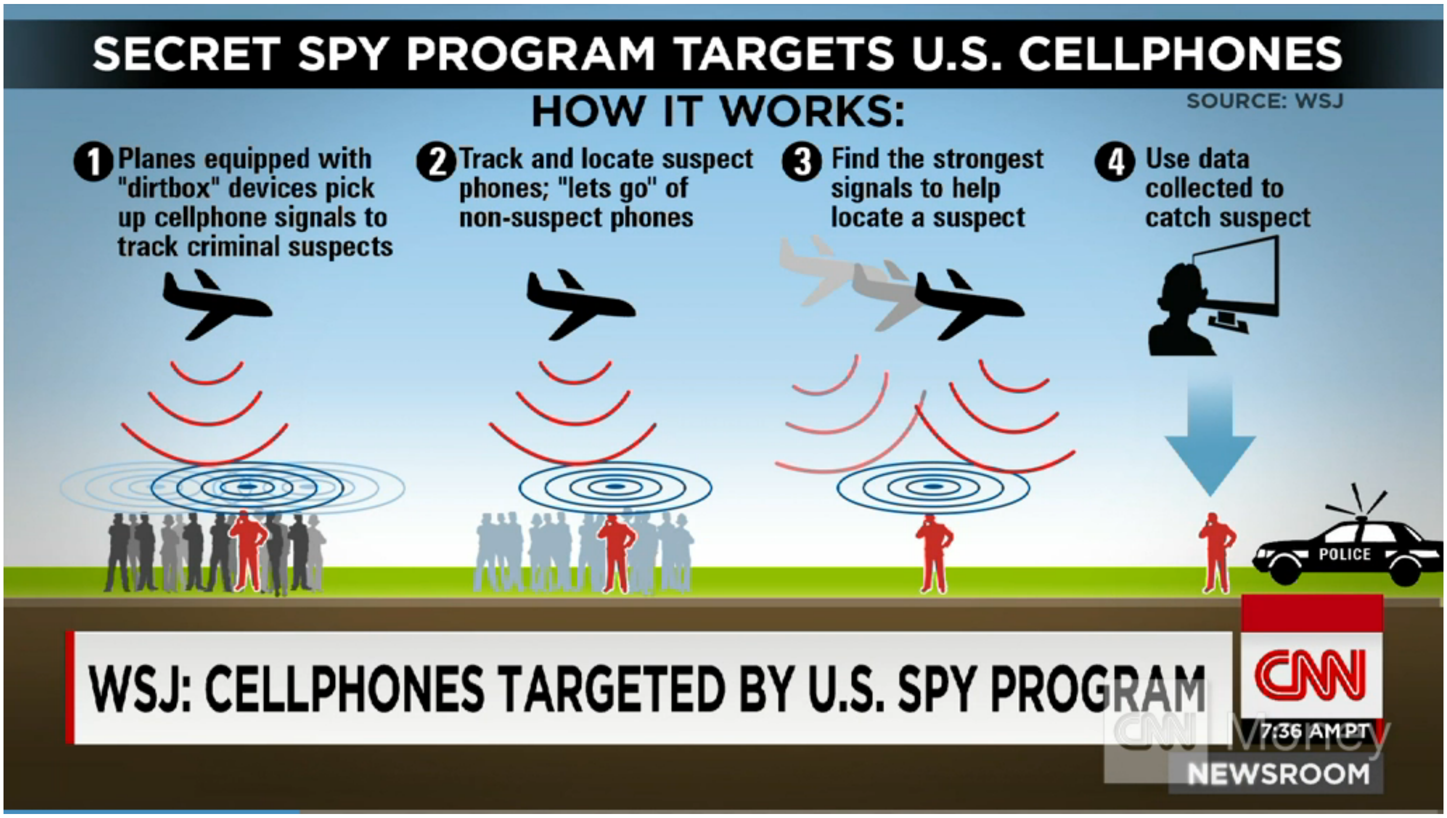
Security Now! #482 - 11-18-14
Q&A #201

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!

- Microsoft is having a rough November,
- A nifty new feature in the latest Firefox update (v33.1.1)
- Flying "Dirtboxes",
- Cellular Super-Cookie Update,
- Free Certificates coming soon from the EFF and Mozilla
- News about WhatsApp and BitTorrent Sync
- Miscellany and our Q&A...


SECRET SPY PROGRAM TARGETS U.S. CELLPHONES
HOW IT WORKS:
SOURCE: WSJ
1 Planes equipped with "dirtbox" devices pick up cellphone signals to track criminal suspects
2 Track and locate suspect phones; "lets go" of non-suspect phones
3 Find the strongest signals to help locate a suspect
4 Use data collected to catch suspect
POLICE
WSJ: CELLPHONES TARGETED BY U.S. SPY PROGRAM
CNN
7:36 AM PT
CNN Money
NEWSROOM

Security News:

Microsoft is having a rough November...

- Patch Tuesday Part II and a big Whoops from Part I
    - Critical Privilege Elevation patch, MS14-068, held back from last week's mega-drop, releases today.
    - SERVERS ONLY, and even then, <Microsoft> "An attacker must have valid domain credentials to exploit this vulnerability. The affected component is available remotely to users who have standard user accounts with domain credentials; this is not the case for users with local account credentials only." (Nor for users connecting and browsing a server's offered Website.)
    - Being offered to workstations only for the sake of completeness (and because both are really the same underlying operating system.)

- Cipher Suite Update
    - MS14-066 fix... added four new **broken** cipher suites.
    - Updated advice warns to turn them off.
    - AWS, IIS, and other servers were crashing.

- MS14-066's defect looks to be as bad as was feared and predicted.
    - A number of hackers wearing hats of varying shades from white through grey to black, have been releasing analyses and sample crashes in Microsoft's SChannel TLS handling.
    - Reason for Revision: V2.0 (November 18, 2014): Bulletin revised to announce the reoffering of the 2992611 update to systems running Windows Server 2008 R2 and Windows Server 2012. The
    - reoffering addresses known issues that a small number of customers experienced with the new TLS cipher suites that were included in the original release.
    - Customers running Windows Server 2008 R2 or Windows Server 2012 who installed the 2992611 update prior to the November 18 reoffering SHOULD REAPPLY THE UPDATE! See Microsoft Knowledge Base Article 2992611 for more information.
        - - Originally posted: November 11, 2014
        - - Updated: November 18, 2014
        - - Bulletin Severity Rating: Critical
        - - Version: 2.0

Firefox v33.1.1

- "Forget" -- the previous 5 minutes, 2 hours, 24 hours
- (Forget... or "Regret") vs Incognito
- "DuckDuckGo" built-in for anonymous searching
- Great results with no tracking

"Dirtboxes"

- http://money.cnn.com/2014/11/13/technology/security/federal-planes-spy/index.html?sr=tw111414usplanesspy630pVODtopPhoto
- Fake airborne "cell towers" dragnet and inspect ALL phones below.
- ACLU is unhappy:
    - Nathan Freed Wessler, an American Civil Liberties Union attorney in New York told CNNMoney: "This is a disturbing progression of the federal government's use of this technology. What's different about this... is that it vastly increases the number of completely innocent bystanders whose information is being swept up by law enforcement."
- CNNMoney contacted the DoJ for comment: An official at the Department of Justice would not confirm or deny the use of flying spoof cell towers. He said any discussion would let criminals and foreign governments "determine our capabilities and limitations." The [DoJ] official told CNNMoney that any tactics used comply with federal law.

AT&T (temporarily) ends Super-Cookie Injection "testing" -- Verizon Presses On.

- http://www.techrepublic.com/article/att-ends-controversial-use-of-perma-cookies-to-track-users/
- AT&T's statements are less strong than we would hope.
    - They talk about perhaps changing a code every 24 hours.
- Verizon? Still present.
- 3rd-Party use of the Verizon super-cookie:
    - "MoPub", acquired by Twitter in 2013, bills itself as the 'world's largest mobile ad exchange.' It uses Verizon's tag (perma-cookie) to track and target cellphone users for ads, according to instructions for software developers posted on its website:
    - https://dev.twitter.com/mopub-demand/overview/openrtb

(Announced Today) **EFF's "Let's Encrypt" a new free certificate authority launching in summer 2015**

- https://letsencrypt.org/
- https://www.eff.org/deeplinks/2014/11/certificate-authority-encrypt-entire-web
- A new CA initiative put together with Mozilla, Cisco, Akamai, Identrust, and University of Michigan.
- <quote> Let's Encrypt is a new free certificate authority, which will begin issuing server certificates in 2015. Server certificates are the anchor for any website that wants to offer HTTPS and encrypted traffic, proving that the server you are talking to is the server you intended to talk to. But these certificates have historically been expensive, as well as tricky to install and bothersome to update. The Let's Encrypt authority will offer server certificates at zero cost, supported by sophisticated new security protocols. The certificates will have automatic enrollment and renewal, and there will be publicly available records of all certificate issuance and revocation.
- The Let’s Encrypt CA will be operated by a new non-profit organization called the Internet Security Research Group (ISRG). EFF helped to put together this initiative with Mozilla and the University of Michigan, and it has been joined for launch by partners

including Cisco, Akamai, and Identrust.

- New "ACME" protocol between servers and the "Let's Encrypt" CA.
    - ACME: Automated Certificate Management Environment
    - ACME is a protocol for automating the management of domain-validation certificates, based on a simple JSON-over-HTTPS interface. (GitHub)
- Also leverages the EFF's decentralized SSL Observatory and Google's Certificate Transparency database system to make "higher security" decisions about certificate issuance.

WhatsApp *(acquired by Facebook for $19 billion early this year)* **integrates the recently audited Open Whisper Systems' "TextSecure" into WhatsApp for Android.**

- Strong end-to-end encryption enabled by default.
- 600 Million users worldwide.
- iOS integration timing unknown at this time.
    - (iMessage offers convenience at the cost of true security.)
- How does TextSecure Authenticate?
    - https://github.com/WhisperSystems/TextSecure/wiki/Using-TextSecure
    - First: Secure Messaging:
        - TextSecure automatically detects when a message is received from another TextSecure user and prompts you to initiate a secure session. If you choose to initiate the secure session, a key exchange will ensue, and a lock icon will be displayed in the title bar of the conversation view as well as on the send button itself. A lock icon will also be displayed next to each encrypted message received, in order to confirm that it was transmitted securely.
- "Verifying Keys" <quote>:
    - It is prudent to verify the identity key of conversation's recipient, in order to ensure that no "man in the middle" attack has occurred. From the menu in a conversation, select "Secure Session Options" --> "Verify Recipient Identity." This will present you with an option to manually verify the recipient key's fingerprint, or to verify it by QR code scanning. If you're physically located in the same space as the recipient, you can select QR code scanning to quickly verify each-other's fingerprints. If you're remotely located, you can manually read the fingerprints to each-other over the phone.

      Once you verify that the recipient's identity is correct, this information is saved and used to automatically authenticate future secure sessions with that recipient.

Worries about BitTorrent Sync's security and privacy.

- http://www.networkworld.com/article/2848723/microsoft-subnet/hackers-claim-bittorrent-sync-should-not-be-used-for-sensitive-data.html
- Users like BitTorrent Sync. BitTorrent claims: “Sync performed 8 times faster than Google Drive, 11 times faster than OneDrive and 16 times faster than Dropbox.”
- Hacker group "Hackito Ergo Sum" (Cogito Ergo Sum) finds much to be worried about and concludes that BiTTorrent Sync should not be used for sensitive data.
- They claim that there are probable vulnerabilities in the client and that the protocol can leak potentially sensitive hash and client IP data.

- BitTorrent adamantly disagrees and is preparing a detailed rebuttal.

Miscellany:

As expected, a FABULOUS Net Neutrality Discussion on TWiT

"Interstellar"

- Call it a gravitational spacial "anomaly"... NOT a "BlackHole"

"The Imitation Game" Movie.com

- November 28th - A tribute to Alan Turing.

SpinRite

Greg sent a question about SpinRite and full-disk-encryption with SSDs:

My routine before I do full-disk-encryption is to SpinRite the HDD with Level-5. The idea being to expose as much of the disk as possible before overwriting it with pseudo random data. Following this I install the encryption container (using linux's dm-crypt and LUKS).

Considering the wear that SSDs incur from Level-5 SpinRite, do you think this is a good idea to do on SSDs prior to overwriting them? For security, the SSD HAS to be overwritten prior to putting the encryption on. So the wear incurred is necessary. But does my use of Level-5 before overwriting make sense to you from a security perspective? Or do you recommend I just use Level-2 for SSDs that I want to encrypt?

M•DISC
US Pat 7,613,869
MILLENNIATA