Security Now! #437 - 01-07-14

New Years News Catch Up

Today on Security Now!

- New Years Eve at the Brick House!
- 2013 was certainly NOT the end of annoying NSA news... not by a LONG shot!
- (Truly unsettling NSA news.)
- Routers listening on port 32764 (32768-4)
- Mozilla's screaming native code progress.
- Here come the CryptoLocker clones!
- SnapChat's massive 4.6 million username and phone number disclosure.
- AND... Steve's Long-Awaited Sci-Fi Reading Guide!

================= Sponsor Insert! =================

Security Now! Holiday Special was a HUGE HIT!...

- ***This*** year (2014)... Tuesday is Dec. 30th

New Years Eve at the Brick House!

- Simon Zerafa @SimonZerafa: "@SGgrc The TWiT producers are uploading 1 hour segments of the NYE special to the Inside TWiT YouTube account."
- "Recent Uploads"
- Game Of Geeks: Alpha Episode 4
- TWiT Live NYE 2014 24 hour live stream 2 of 24
- Game Of Geeks: Alpha Episode 5

Security News:

Concern over no more NSA coverage!

- Don't worry... we'll still cover the NSA if anything new happens! :)

MOST disturbing news of the Old and New Year:

- RSA accepted $10 million dollars to make NIST's Dual Elliptic Curve Deterministic Random Bit Generator their corporate-wide BSAFE default!
- http://bit.ly/nsabribe
- *Note that, at the time, $10M was 1/3rd of RSA's annual revenue.*
- An algorithm called Dual Elliptic Curve, developed inside the [NSA] agency, was on the road to approval by the National Institutes of Standards and Technology (NIST) as one of four acceptable methods for generating random numbers. NIST's blessing is required for

many products sold to the government and often sets a broader de facto standard.

RSA adopted the [Dual_EC_DRBG] algorithm even before NIST approved it.

According to an official familiar with the proceedings: The NSA then cited the early use of Dual Elliptic Curve inside the government to argue successfully for NIST approval.

RSA's contract made Dual Elliptic Curve the DEFAULT OPTION for producing random numbers in the RSA toolkit. No alarms were raised, former employees said, because the deal was handled by business leaders rather than pure technologists.

"The labs group had played a very intricate role at BSafe, and they were basically gone," said labs veteran Michael Wenocur, who left in 1999.

Within a year, major questions were raised about Dual Elliptic Curve. Cryptography authority Bruce Schneier wrote that the weaknesses in the formula "can only be described as a back door."

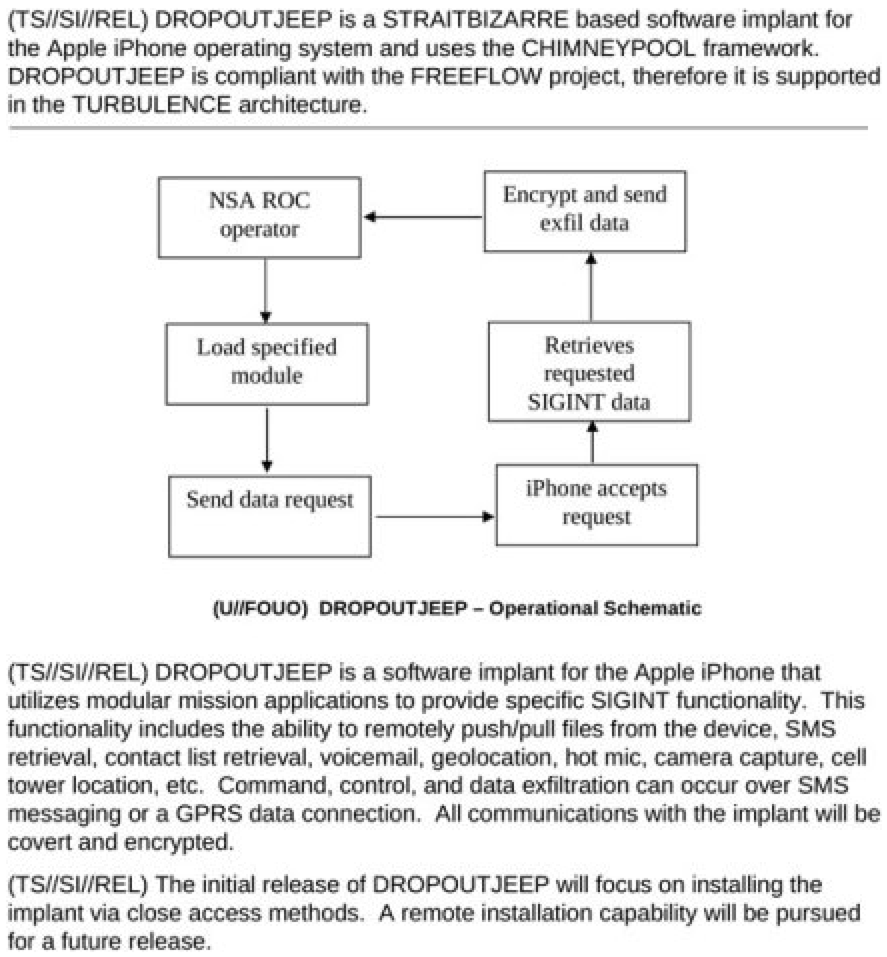
- Several speakers have pulled out of the upcoming 2014 RSA Security Conference in protest of RSA’s complicity in the NSA PRNG-weakening…
  - (Though **Stephen Colbert** has been announced as the closing keynote. :)

NSA's ANT Division Catalog lists EXPLOITS for nearly every major software & hardware

- http://bit.ly/nsa-ant
- http://leaksource.wordpress.com/2013/12/30/nsas-ant-division-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware/
- Bruce is doing a blog-post-a-day
- https://www.schneier.com/blog/archives/2013/12/more_about_the.html
- DeityBounce / IronChef / FeedThrough / GourmetTrough / HalluxWater / JetPlow SouffleTrough / HeadWater / SchoolMontana / SierraMontana / StuccoMontana CTX4000 / LoadAuto / NightStand / NightWatch / PhotoAnglo / Sparrow II / TawdryYard Ginsu / HowlerMonkey / IrateMonk / JuniorMint / Maestro-II / SomberKnave / Swap Trinity / WistfulToll / SurlySpawn / DropoutJeep / GopherSet / MonkeyCalendar Picasso / ToteChaser / ToteGhostly 2.0 . CandyGram / CrossBeam / Cyclone Hx9 / EBSR Entourage / Genesis / Nebula / Typhon HX / WaterWitch / CottonMouth (I, II & III) FireWalk / RageMaster

NSA has total iPhone access?

- *DropoutJeep*
- NSA had worked on software that would allow it to remotely retrieve virtually all the information on an iPhone including text messages, photos, contacts, location, voice mail and live calls.
- The software, DropoutJeep, was first disclosed by Der Spiegel and security researcher Jacob Appelbaum. The NSA slides are dated 2008, a year after the first iPhone was launched.



(TS//SI//REL) DROPOUTJEEP is a STRAITBIZARRE based software implant for the Apple iPhone operating system and uses the CHIMNEYPOOL framework. DROPOUTJEEP is compliant with the FREEFLOW project, therefore it is supported in the TURBULENCE architecture.

NSA ROC operator
Encrypt and send exfil data
Load specified module
Retrieves requested SIGINT data
Send data request
iPhone accepts request

(U//FOUO) DROPOUTJEEP – Operational Schematic

(TS//SI//REL) DROPOUTJEEP is a software implant for the Apple iPhone that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device, SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control, and data exfiltration can occur over SMS messaging or a GPRS data connection. All communications with the implant will be covert and encrypted.

(TS//SI//REL) The initial release of DROPOUTJEEP will focus on installing the implant via close access methods. A remote installation capability will be pursued for a future release.

Monitoring a Laptop's Camera without the Light?

- Q: When is a power light is not a power light??
  - A: When it's separately controlled by firmware.

- http://www.wired.co.uk/news/archive/2013-12/19/macbook-light-bypass

- One [signal wire] line joins the USB [interface] chip, to an input on the imaging sensor called standby. When the line is held high by the interface chip, the sensor is put into standby mode and stops producing data. When it's held low, the sensor is taken out of standby mode and starts producing data. The same line is also wired to the negative side of an LED. Accordingly, when the line is high (and the imaging chip off), the LED is off. When the line is low, the LED is turned on.

  In principle, then, this should serve as a hardware interlock. The LED is clearly hardwired, and its state should directly reflect whether the imaging chip is in standby or not. Unfortunately, the whole system is controlled by a layer of software.

  When the driver for the webcam is loaded, the host PC uploads a small program to the USB controller (it has no permanent firmware storage of its own, so it has to be uploaded each time the camera driver is loaded). This small program in turn configures the imaging chip. The imaging chip doesn't have too many configurable properties, but one thing it ***DOES HAVE...*** [emphasis Steve's] is whether it pays any attention to the standby input.

Apple's own drivers set a configuration where standby is respected. But other configurations are possible -- such as one where the chip ignores standby entirely and always produces image data.

With this knowledge in hand, the researchers wrote a new piece of software to upload to the webcam. This piece of software was much like the normal webcam software but with two differences: first, it told the imaging sensor to ignore the standby input. Second, it ensured that the standby line was always held high to prevent the LED from illuminating.

The result: a webcam with a hardwired indicator LED that nonetheless allowed image capture without lighting the indicator LED.

32764

- A known hacker named Eloi Vanderbeken posted up a note on GitHub:
- His Linksys WAG200G wireless DSL gateway was listening on the unknown TCP port 32764.
- He discovered that this was also true on Linksys, Netgear, Cisco & others.
- http://www.ghacks.net/2014/01/06/find-router-listening-backdoor-port-32764/
- https://github.com/elvanderb/TCP-32764
- CONFIRMED EXPOSED TO THE INTERNET:
    - Cisco WAP4410N-E 2.0.1.0, 2.0.3.3, 2.0.4.2, 2.0.6.1
    - Linksys WAG120N
    - Netgear DG834B V5.01.14
    - Netgear DGN2000 1.1.1, 1.1.11.0, 1.3.10.0, 1.3.11.0, 1.3.12.0
    - OpenWAG200 maybe a little bit TOO open ;)
- Add an explicit firewall rule and retest.
- Quick check: http://yourGatewayIP:32764/ (192.168.1.1)
- "ScMM" or "MMcS"
- Google: 32764
- (Zip code of Deltona & Osteen, Florida... ignore that one.)

THREE CryptoLocker follow-ons...

CryptoLocker 2:

- The Question: *NEW or "Improved?"*
- http://www.welivesecurity.com/2013/12/19/cryptolocker-2-0-new-version-or-copycat/
- CLv1: RSA-2048 / CLv2: Claims 4096, uses 1024
- CLv1: C++ / CLv2: C#
- CLv1: BTC, MoneyPal, UKash, cashU. / CLv2: BTC only
- CLv1: doesn't encrypt image, video, music files. / CLv2 does.
- CLv1: AES / CLv2: 3DES
- CLv1: Encrypted Key added to encrypted version header / CLv2: Keys in *.k "key" files. Also... CLv2 contains various fake "activators" and "cracks" for proprietary software, including Windows, Office, Team Viewer, Photoshop, ESET Smart Security, and others.
- CLv2 can also spread via removable media by replacing the EXE's on removable drives with its own executable code.

"PrisonLocker" / "PowerLocker"

- http://arstechnica.com/security/2014/01/researchers-warn-of-new-meaner-ransomware-with-unbreakable-crypto/
- Dan Goodin:
  - "Researchers warn of new, meaner ransomware with unbreakable crypto"
  - "Move over, CryptoLocker. Criminals are talking up more advanced PowerLocker."
- http://malwaremustdie.blogspot.jp/2014/01/threat-intelligence-new-locker-prison.html?m=1
- ICQ ID tracked back to a 23 year old "David Klukinski" (Pisces)

"Locker" - Reported by The Register

- http://www.theregister.co.uk/2013/12/13/locker_ransomware/
- Written in Delphi using the TurboPower LockBox crypto library to encrypt files in ASES-CTR mode... but apparently non-payment decryption IS possible.

SnapChat's 4.6 Million-user data breach!

- http://gibsonsec.org/snapchat/fulldisclosure/
- SnapChat was warned about five months in advance.
- Amateur-League toy obfuscation:
  - “Secret” that never changes = iEk21fuwZApXlz93750dmW22pw389dPwOk
  - “Pattern” that never changes = "0001110111101110001111010101111011010001001110011000110001000110"
  - “Login” means get a session token from the snapchat server.
  - “Authenticate” means:
    - Hash the time of day with the token and convert to hex.
    - Hash the “secret” with the token and convert to hex.
    - Make an authentication token by selecting characters from either the first or the second hash strong based upon whether the “Pattern” is 0 or 1.

- API allows non-rate-limited querying of the entire SnatChat database.
  - A random phone number can be looked up and used to retrieve the account’s corresponding username… without limitation.
  - This… 4.6 Million numbers were looked up

"Gibson Security" vs "GRC"

- “Gibson Security” (in Australia) has NO RELATIONSHIP to me or GRC.
- It originates from “Hacking The Gibson” from the cult classic movie “Hackers.”

Renaming: "McAfee Security" to "Intel Security"

- Embarrassed by Big John... distancing themselves from the McAfee brand after purchasing McAfee for more than $7 billion.
- So… When you start hearing “Intel Security”, think old “McAfee Security”

Anti-porn politician's website blocked by porn filters she advocated

- BGR: http://bgr.com/2013/12/26/uk-porn-filter-controversy/
- As was predicted by just about everyone, the United Kingdom's initiative to get U.K. ISPs to add default pornography filters has been a complete and utter disaster so far.

  Not only have the filters been blocking access to pornographic content, but they've also been blocking access to health information websites and charity websites among other unintended targets.

  There is some justice to come out of all this, however: The Independent reports that the filters have also blocked access to the website of Conservative MP Claire Perry, who has been one of the leading crusaders for implementing porn filters in the U.K. It seems that Perry's website contained information on her assorted anti-pornography campaigns, which was apparently enough to get her site caught in the porn filter dragnet.

- 1964 - Supreme Court Justice Potter Stewart: "I know it when I see it"
- Could not "define it" -- so how can we expect a computer to recognize it?
- (With bots taking over the Internet... we have enough of a problem answering the question: "Are you a human being?")

Mozilla's Asm.js goes from x2 slower to only 1.5x slower than native code!

- http://techcrunch.com/2013/12/21/mozillas-asm-js-gets-another-step-closer-to-native-performance/
- "Asm.js" is a strict subset of JavaScript which allows for massive execution performance improvement.
- Google has chosen a different path: "Native Client" -- An open-source technology that allows web applications to be built to seamlessly execute native compiled code inside the browser.

SpinRite: Jonathan Bailey in New Orleans, LA

- Subject: SpinRite Testimonial
- Date: Thu, 26 Dec 2013 16:56:45 -0000
- I was at a friends house on Christmas Day when she told us the hard drive on her laptop wasn't working. It wouldn't boot and even booting it off of a Live CD didn't give access to the data on it.

  While the laptop was old and she didn't care about it much, it had a lot of important stuff, most notable the photos of her son's wedding a few years ago and there were no known complete backups.

  I took the laptop home and, using my receipt, downloaded a fresh copy of SpinRite. Immediately, on the first sector, it seemed to freeze and it spent so long at zero percent that I considered aborting it.

However, being a listener of Security Now, I knew to be patient and put my faith in the SpinRite gods so I went to bed with it running. I awoke to the green "SpinRite Complete!" screen. Took the CD out, rebooted and huzzah the laptop booted right into Windows.

It was a true (day after) Christmas miracle! Thank you so much for your great product, after four years of ownership, I finally get to share my "SpinRite saved me" story!

Miscellany:

Blackberry Sues "Typo" over their Blackberry-like keyboard

- http://www.engadget.com/2014/01/03/blackberry-sues-typo-over-its-familiar-looking-iphone-keyboard/
- http://www.marketwired.com/press-release/blackberry-files-suit-against-typo-nasdaq-bbry-1866087.htm
- NBC News this morning said that it was EXCELLENT… but that they could not say any more due to the BlackBerry lawsuit.

"Intelligence" premieres tonight on CBS (9pm)

- Re-airs Friday.

Steve's Sci-Fi Reading Guide

- http://bit.ly/sgscifi
- (It's a PDF... why is that fine? (not a security problem?))

Honor Harrington, books #1 & #2 free everywhere!!

A sample of my assembly language for SQRL:

- http://bit.ly/SqrlSign

SQRL project update

- All Crypto libraries are up and running.
- Currently settling upon a cryptographic export and host-storage format.
- Nail down some details of the way we’re going to use the SCrypt PBKDF.