Security Now! #444 - 02-25-14
Goto: Fail

This week on Security Now!

- Apple's "difficult to rationalize" SSL screw-up. (and another newly discovered threat!)
- WhatsApp, Telegram, TextSecure & Threema
- Netflix / Cogent / Comcast & Verizon
- Mt.Gox apparently goes under
- Stats on the benefit of not running an Admin account.

Security News:

Last Week Follow-Up:

- Belkin WeMo users ARE (and have been) safe:
- http://www.techhive.com/article/2099002/belkin-fixes-wemo-security-holes-that-gave-hackers-access-to-home-appliances.html

Apple's phenomenal SSL screw up:

```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffersignedParams,
uint8_t *signature, UInt16 signatureLen)

{
        OSStatus     err;
        ...

        if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
                goto fail;
        if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
                goto fail;
                goto fail;
        if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
                goto fail;
        ...

fail:
        SSLFreeBuffer(&signedHashes);
        SSLFreeBuffer(&hashCtx);
        return err;
}
```

- (Adam Langley's Weblog) https://www.imperialviolet.org/2014/02/22/applebug.html
- http://arstechnica.com/security/2014/02/extremely-critical-crypto-flaw-in-ios-may-also-affect-fully-patched-macs/
- http://www.imore.com/understanding-apples-ssl-tls-bug
- http://daringfireball.net/2014/02/apple_prism
- Firefox and Chrome on OS X both use NSS (Netscape Security Suite)
- OS X v10.9.2
    - 460 MB
    - Fixes the problem: http://gotofail.com
- THE BIG QUESTION: Was it deliberate?
- No regression testing? Huh???

iOS Device UI Event Monitoring - POC - All iOS versions

- http://arstechnica.com/security/2014/02/new-ios-flaw-makes-devices-susceptible-to-covert-keylogging-researchers-say/
- FireEye
    - http://www.fireeye.com/blog/technical/2014/02/background-monitoring-on-non-jailbroken-ios-7-devices-and-a-mitigation.html
    - Press & Release Coordinates
    - Screen, Volume Up/Down, TouchID, Home, Power

WhatsApp?

- Facebook recently changed their TOS to obtain explicit permission to read text messages.
- … then Facebook purchased WhatsApp

Telegram

- TechCrunch @TechCrunch
- Telegram Saw 8M Downloads After WhatsApp Got Acquired tcrn.ch/MpZ2do by @alexia
- http://techcrunch.com/2014/02/24/telegram-saw-8m-downloads-after-whatsapp-got-acquired/
- BUT... the most bizarre home-grown security protocol I've ever seen.
    - AES-IGE: Infinite Garble Extension
    - SHA-1 (which is no longer sufficiently secure) was used in the name of performance... thus sacrificing the security they claim to treasure.
    - Then, they use that SHA-1 to hash the plaintext for the generation of the encryption key. WHAT??

- **"Secret Chats"**
  Q: How are secret chats different?
  A: Secret chats are meant for people who really want secure messaging. All messages in secret chats use end-to-end encryption. This means only you and the recipient can read those messages — nobody can decipher or intercept them, including us here at Telegram. Messages cannot be forwarded from secret chats. You can also order your messages to self-destruct in a set amount of time after they have been read by the recipient. The message will then disappear from both your and your friend's devices.

One last difference between secret and ordinary chats in Telegram is that secret chats are not stored in our cloud. This means you can only access messages in a secret chat on their device of origin.

- Q: Why not just make all chats ‘secret’?
  A: The idea behind Telegram is to bring something more secure to the masses, who understand nothing about security and want none of it. Being merely secure is not enough to achieve this — you also need to be fast, powerful and user friendly. Telegram is a secure and powerful alternative to mass market messengers and a fast and user-friendly alternative to secure messengers. Hence the two types of chats that we have: ordinary chats and Secret Chats.

  The important thing to remember is that all Telegram messages are always securely encrypted. The difference between messages in Secret Chats and ordinary Telegram messages is in the encryption type: client-client in case of Secret Chats, client-server/server-client for ordinary chats. This enables your ordinary Telegram messages to be both secure and available in the cloud so that you can access them from any of your devices — which is very useful at times.

Geoffroy Couprie Blog…

- http://unhandledexpression.com/2013/12/17/telegram-stand-back-we-know-maths/
  Edit 4: Someone found a flaw in the end to end secret chat. The key generated from the Diffie-Hellman exchange was combined with a server-provided nonce: key = (pow(g_a, b) mod dh_prime) xor nonce. With that, the server can perform a MITM on the connection and generate the same key for both peers by manipulating the nonce, thus defeating the key verification. Telegram has updated their protocol description and will fix the flaw. (That nonce was introduced to fix RNG issues on mobile devices).

  To sum it up: avoid at all costs. There are no new ideas, and they add their flawed homegrown mix of RSA, AES-IGE, plain SHA1 integrity verification, MAC-Then-Encrypt, and a custom KDF.

Moxie Marlinspike:

- http://www.thoughtcrime.org/blog/telegram-crypto-challenge/
- "A Crypto Challenge For The Telegram Developers"
  Dec 19, 2013

  Earlier this week, a company called Telegram announced a “secure” mobile messaging product. How secure? In their words of their FAQ, ”very secure.” Curious to learn more, I went to look at the protocol, and immediately had a number of questions and concerns. However, when pressed on technical details by others, they responded with the academic credentials of their developers (math Ph.Ds) instead of engaging in a more reasonable dialog. They also declined my suggestions for collaboration of any kind.

  Most recently, they’ve chosen to respond to the concerns of the security community with… a crypto cracking contest!

The Fallacy Of The Crypto Contest

As always, these things are a bad sign. By framing the contest the way they have, the Telegram developers are leveraging a rigged challenge to trick the public. They wasted no time in updating their FAQ to point to the challenge as solid proof of their absolute security, even when it's essentially meaningless.

So Telegram developers, by way of a response, I have my own crypto cracking contest for you. Below is a horrifically bad "secure" protocol that wouldn't last a second in a real world environment, but becomes "unbreakable" when presented in the exact same framework as the Telegram challenge…

- Moxie is "WhisperSystems" (http://whispersystems.org)
  - TextSecure (Android Only) released yesterday:
  - https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms
  - iPhone coming

Taylor Hornby (FireXware) - Defuse Security

- Some problems are immediately apparent:
  - They use the broken SHA1 hash function.
  - They include a hash of the plaintext message in the ciphertext. Essentially, they are trying to do "Mac and Encrypt" which is not secure. They should be doing "Encrypt then Mac" with HMAC-SHA512.
  - They rely on an obscure cipher mode called "Infinite Garble Extension."
  - Some really weird stuff about factoring 64-bit integers as part of the protocol.
  - They do not authenticate public keys.

- Taylor: "If their protocol is secure, it is so by accident, not because of good design."
  They claim the protocol was designed by "six ACM champions" and "Ph.Ds in math." Quite frankly, the protocol looks like it was made by an amateur. The tight coupling between primitives suggests the designer was not familiar with basic constructs, like authenticated encryption, that you can find in any cryptography textbook.

- What should Telegram do?

  Telegram's crypto is bad, and it needs to be scrapped. I know it's tough to throw away all of that work, but if they want to build a trustworthy product, it's what they need to do. Their protocol is already too complex to analyze (let alone prove secure), and adding band-aid fixes is only going to make it worse.

  They should switch to an existing well-studied protocol like the one used by TextSecure. They need to bring in a real cryptographer to audit their design (and design process), and they need to make sure the programmers they've hired are qualified to write crypto code (most programmers are not).

If telegram wants, they can email me and I'll offer as much advice as I can. I think their hearts are in the right place, they just goofed on the crypto.

Threema

- https://threema.ch/en/
- DOUBLED its user base in 24 hours.
- https://www.os3.nl/_media/2013-2014/courses/ssn/projects/threema_report.pdf

SPINRITE:

- Nathan Huebener in Marion, Iowa
  Subject: Spinrite violates the laws of physics
  Date: 25 Feb 2014 01:33:22

  My brother's laptop was very slow when booting and while being used. The hard drive was suspected as being bad, Norton Ghost tried to clone it and failed. It was not pretty. I ran Spinrite at level 2, and then was able to clone it to another drive. It cloned over perfectly and no bits were lost. After the new drive was installed and running, I opened up the bad drive and looked inside. Inside were tiny metal shavings. From what I understand, if a piece of dust goes between the head and the platter it's game over for the drive. Somehow, Spinrite was able to fix the drive just long enough to clone it.

  Spinrite has also fixed my Intel X-25 Extreme 64gb SSD, it was showing some sector access times over 600ms.

  Spinrite user and Security Now listener since episode 1,

  Nathan Huebener,
  Marion, Iowa

Netflix & Comcast

- During evenings, Netflix accounts for about 32% of downstream traffic in North America.
- Netflix's FREE "Open Connect" program places Netflix servers within the ISP's network or gives free access to content providers.
- Comcast and Verizon have NOT participated.
- Netflix PAID Comcast for the privilege of putting its servers in Comcast data centers.
- http://ispspeedindex.netflix.com/usa

Cogent vs Verizon

- "Netflix packets being dropped every day because Verizon wants more money"
  - "Verizon wants to be paid by consumers and Cogent, but Cogent refuses to pay."
- http://arstechnica.com/information-technology/2014/02/netflix-packets-being-dropped-every-day-because-verizon-wants-more-money/
  - Jon Brodkin -- TERRIFIC ARTICLE
  - http://bit.ly/444peer

- Verizon customers complaining that their Netflix experience is bad.
    - When "peering" agreements go bad.

Mt.Gox & Bitcoin

- "Crisis Strategy Draft" -- Apparently from Mt.Gox
- Claiming the company had lost 744,408 Bitcoins in a theft that had gone unnoticed for years.
- (6% of the 12.4 million bitcoins currently in circulation.)
- A statement from the chief executives of Bitcoin companies like Coinbase, Circle, Blockchain.info and Payward, said that the “tragic violation of the trust of users of Mt. Gox was the result of one company’s abhorrent actions and does not reflect the resilience or value of Bitcoin and the digital currency industry.”
- https://www.mtgox.com/
    - Dear MtGox Customers,

      In the event of recent news reports and the potential repercussions on MtGox's operations and the market, a decision was taken to close all transactions for the time being in order to protect the site and our users. We will be closely monitoring the situation and will react accordingly.
      Best regards,
      MtGox Team

- Fascinating BlockChain Info: https://blockchain.info/
    - What *is* all of that going on???

To Admin or Not to Admin -- That really isn't a question.

- Avecto's Analysis of last year's Patch Tuesday vulnerabilities...
- "Mitigating Risk by Removing User Privileges"
- "Analysis of Microsoft Security Bulletins from 2013 highlights that 92% of Critical vulnerabilities would be mitigated by removing admin rights."
- October 2013 was the 10th Anniversary of Microsoft's Auto Update system.
- Summary:
  Of the 147 vulnerabilities published by Microsoft in 2013 with a Critical rating:
    - 92% were concluded to be mitigated by removing administrator rights.
    - 96% of Critical vulnerabilities affecting Windows operating systems could be mitigated by removing admin rights.
    - 100% of all vulnerabilities affecting Internet Explorer could be mitigated by removing admin rights.
    - 91% of vulnerabilities affecting Microsoft Office could be mitigated by removing admin rights.
    - 100% of Critical Remote Code Execution vulnerabilities and 80% of Critical Information Disclosure vulnerabilities could be mitigated by removing admin rights.

- Windows "Standard User"
    - Everyone runs as "Standard User"
    - Create one Admin Account no one uses.
    - Provide the account's Admin password only when needed.

(Yesterday) **Malware distributed via YouTube:**

- http://thehackernews.com/2014/02/caphaw-banking-malware-distributed-via_24.html
- More than one billion unique visitors spend about 6 billion hours monthly on YouTube.
- YouTube In-Stream Ads were redirecting users to malicious websites, hosting the 'Styx Exploit Kit' and leveraging a more than year-old known Java vulnerability to infect users' computer with the Caphaw Banking Trojan.
- Researchers said: "We don't yet know the exact bypass the attackers used to evade Google's internal advertisement security checks. Google has informed us that they're conducting a full investigation of this abuse and will take appropriate measures."

Miscellany:

"Steve Jobs: The Lost Interview

- October 23, 2012
- Links to The Lost Interview:
- http://www.cringely.com/2012/07/02/steve-jobs-the-lost-interview-itunes-dont-tell-anyone-okay/
- www.youtube.com/watch?v=F4L26Jp_AT4
- http://www.amazon.com/dp/B008GJVAW4
- https://itunes.apple.com/us/movie/steve-jobs-the-lost-interview/id536749587

"Rails" on the App Store: http://bit.ly/sgrails

SQRL's "Create New Identity" user-interface walk-though is finished.

- https://www.grc.com/sqrl/operation.htm
- https://bit.ly/sqrlui
- Jan 30th, public Feb 2nd... Three weeks!
- Brought about some significant simplifications in the system's operation.