Security Now! #445 - 03-04-14

Q&A #184

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!

- Bruce Schneier's comment on the Apple SSL flaw.
- Another major Certificate mistake found and just fixed.
- Another Bitcoin exchange wiped out and gone.
- Edward Snowden's latest "Peeping Tom" revelation.
- A Threema UI mistake & hack.
- SQRL goes multi-lingual.

Security News:

Bruce Schneier on the iOS flaw:
https://www.schneier.com/blog/archives/2014/02/was_the_ios_ssl.html
February 27, 2014 (Thursday)
Was the iOS SSL Flaw Deliberate?

Last October, I speculated on the best ways to go about designing and implementing a software backdoor. I suggested three characteristics of a good backdoor: low chance of discovery, high deniability if discovered, and minimal conspiracy to implement.

The critical iOS vulnerability that Apple patched last week is an excellent example. Look at the code. What caused the vulnerability is a single line of code: a second "goto fail;" statement. Since that statement isn't a conditional, it causes the whole procedure to terminate.

The flaw is subtle, and hard to spot while scanning the code. It's easy to imagine how this could have happened by error. And it would have been trivially easy for one person to add the vulnerability.

Was this done on purpose? I have no idea. But if I wanted to do something like this on purpose, this is exactly how I would do it.

EDITED TO ADD (2/27): If the Apple auditing system is any good, they would be able to trace this errant goto line not just to the source-code check-in details, but to the specific login that made the change. And they would quickly know whether this was just an error, or a deliberate change by a bad actor. Does anyone know what's going on inside Apple?

It's not just Apple who has Certificate Verification Troubles...

- http://www.gnutls.org/security.html#GNUTLS-SA-2014-2
- <quote> A vulnerability was discovered that affects the certificate verification functions of all gnutls versions. A specially crafted certificate could bypass certificate validation checks. The vulnerability was discovered during an audit of GnuTLS for Red Hat.
- Who is affected by this attack?
  - Anyone using certificate authentication in any version of GnuTLS.
- How to mitigate the attack?
  - Upgrade to the latest GnuTLS version (3.2.12 or 3.1.22), or apply the patch for GnuTLS 2.12.x.
- For three years, Apache could be configured to use GnuTLS to get TLS v1.2 support.
- GNOME, CenterIM, Exim, Weechat, Mutt, wireshark, slrn, Lynx, CUPS and gnoMint.
- OpenSSL's license is not GPL-compatible, driving the need for GnuTLS.
  - https://people.gnome.org/~markmc/openssl-and-the-gpl.html

Via Edward Snowden Documents: UK Spy Agency Collected Webcam Images From Yahoo Users With The Help Of NSA, Report Says

- Program: "Optic Nerve"
- Began in prototype form in 2008, went live, still active in 2012.
- http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo
- Documents dating between 2008 and 2010 explicitly state that a surveillance program codenamed Optic Nerve collected still images of Yahoo webcam chats in bulk and saved them to agency databases, regardless of whether individual users were an intelligence target or not.
- In one six-month period in 2008 alone, the agency collected webcam imagery – including substantial quantities of sexually explicit communications – from more than 1.8 million Yahoo user accounts globally.
- Yahoo: 'A whole new level of violation of our users' privacy'
- GCHQ does not have the technical means to make sure no images of UK or US citizens are collected and stored by the system, and there are no restrictions under UK law to prevent Americans' images being accessed by British analysts without an individual warrant.
- The documents describe GCHQ's struggle to keep the large store of sexually explicit imagery collected by Optic Nerve away from the eyes of its staff, though there is little discussion about the privacy implications of storing this material in the first place.
- Optic Nerve was based on collecting information from GCHQ's huge network of internet cable taps, which was then processed and fed into systems provided by the NSA. Webcam information was fed into NSA's XKeyscore search tool, and NSA research was used to build the tool which identified Yahoo's webcam traffic.
- Sexually explicit webcam material proved to be a particular problem for GCHQ, as one document delicately put it: "Unfortunately … it would appear that a surprising number of people use webcam conversations to show intimate parts of their body to the other person. Also, the fact that the Yahoo software allows more than one person to view a webcam stream without necessarily sending a reciprocal stream means that it appears sometimes to be used for broadcasting pornography."

Two German freemail sites (web.de & gmx.net) trick Firefox & Chrome users into removing AdBlock

- http://gebloggendings.wordpress.com/2014/02/27/german-freemail-sites-trick-firefox-chrome-users-into-removing-adblock/
- <<image>>
- Presents a false browser alert.
- Linked-to page "warns" users about the "dangers" of using Adblock.
- "Filters the content of pages" / "Induces false security alerts."
- Mozilla's security team is reportedly looking into it.

Mt.Gox formally filed for bankruptcy.

- Coinbase CEO, Brian Armstrong, wrote a piece for TechCrunch:
  - What's NOT being said about Bitcoin?
  - http://techcrunch.com/2014/02/28/whats-not-being-said-about-bitcoin/
  - An open payment network is a game changer.
    - What was needed was a system to prevent duplicate spending without a single centralized clearinghouse. Bitcoin invented that.

  - **Bitcoin is gaining traction with merchants.**
    - Overstock.com: > $1million in two years.
    - Average cart of $216... 30% higher than USD customers.

  - <quote> Around San Francisco, New York City and other major cities across the globe, Bitcoin acceptance is rapidly moving into brick-and-mortar shops, restaurants and even professional businesses like dentists and law firms. Consumers are paying with a quick scan of a QR code or using technologies like NFC and Bluetooth low energy. Merchants are enjoying instant transactions at lower fees, and this momentum will only accelerate in 2014 – with thousands more companies beginning to accept Bitcoin.

  - **It's just beginning:**
    <quote> A new wave of Bitcoin companies – Coinbase, Bitstamp.net, Kraken, BTC China, Blockchain.info, Circle, The Bitcoin Foundation and more – represent trustworthy and responsible companies and groups involved in Bitcoin that are proactive about engaging on regulation and policy and independently auditing and testing security measures to ensure consumer confidence.

    Mt.Gox is in no way the end of Bitcoin — quite the opposite, in fact. Just as the closing of Silk Road in 2013 led to the biggest boost in value of the Bitcoin to date, weeding out immature companies and bad actors is paving the way for a legitimate Bitcoin marketplace. While it may be coincidence that during the Mt.Gox debacle, Coinbase hit 1 million consumer wallets, it is also representative of what legitimate Bitcoin companies have known through the big ups and the low lows – Bitcoin is fundamentally the best payment system for the Internet era.

"Flexcoin" exchange wiped out by theft.

- http://flexcoin.com/
- <quote>
  Flexcoin is shutting down.

  On March 2nd 2014 Flexcoin was attacked and robbed of all coins in the hot wallet. The attacker made off with 896 BTC, dividing them into these two addresses:
  1NDkevapt4SWYFEmquCDBSf7DLMTNVggdu
  1QFcC5JitGwpFKqRDd9QNH3eGN56dCNgy6

  As Flexcoin does not have the resources, assets, or otherwise to come back from this loss, we are closing our doors immediately.

  Users who put their coins into cold storage will be contacted by Flexcoin and asked to verify their identity. Once identified, cold storage coins will be transferred out free of charge. Cold storage coins were held offline and not within reach of the attacker. All other users will be directed to Flexcoin's "Terms of service" located at "Flexcoin.com/118.html" a document which was agreed on, upon signing up with Flexcoin.

  Flexcoin will attempt to work with law enforcement to trace the source of the hack. Updates will be posted on twitter as soon as they become available.

Threema UI Glitch:

- A 4-digit PIN is used for protecting sensitive data.
- "Delete data after ten failed attempts" -- bypass possible.
- But... the data is not actually deleted until "OK" is pressed.
- "Modality" of the OK dialog can be bypassed... allowing unlimited (though painful) guessing.
- Shutting down the app, and restarting it, creates a half-second window of opportunity.

SQRL:

Multilanguage Support via Crowdin.net

SpinRite Note:

Caleb Marble in Rockford, IL (Save me from this place)

Date: 21 Feb 2014 10:31:08

Thank you for a fantastic product, in the few months I've used SpinRite it has recovered four drives from failure, including one hard drive for a local non-profit whose VID (very important documents) dating back to 2002 were stored on a single shared NAS from the early 2000 era with no backups (I later introduced them to Carbonite, thank Leo for me).

Thanks again, Another satisfied customer