Security Now! #432 - 11-27-13

Coin, CryptoLocker, Patent Trolls & More

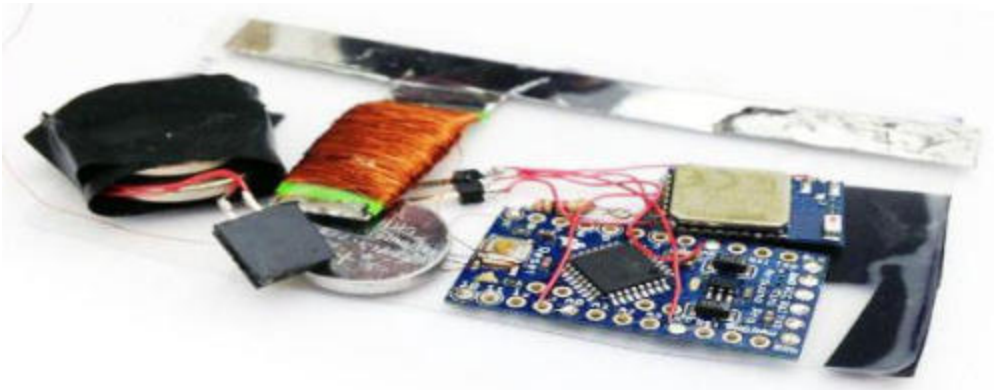
Today on Security Now:

- COIN, take II (now we really know what they're doing, and how)
- A CryptoLocker Update, including GRC now offering CL for forensic experimentation
- The EFF is tracking whose encrypting what
- Massive "whole Internet" MITM attacks?... or not
- Who invented public key encryption with a look at a very high profile Patent Troll case
- What the hell happened to my Twitter feed?
- ... and much more!

Security News:

COIN payment -- Magstripes CAN be rewritten

- https://onlycoin.com (17 days remaining for 50% discount)
- Many listeners noted that the proxy model I was proposing would not, could not, handle gift and loyalty card operation which COIN had specifically stated they did support.
- I found references back in September of 2010 of a company called "Dynamics" announcing dynamically re-writable magstripe technology.
- http://randomoracle.wordpress.com/2012/11/13/programmable-magnetic-stripes-in-search-of-a-problem/
- http://news.cnet.com/8301-1035_3-57612054-94/inside-coins-techie-vision-for-the-all-in-one-credit-card/



- https://www.grc.com/miscfiles/ISO_IEC_7811-2-2001.pdf
- Simple self-clocking Frequency Modulation (FM) like early diskettes.
- Three Stripes:
    - 1. Alphanumeric Track @ 210 bpi - 7 bits/char. (6 data + parity)
        - Uppercase alpha, numeric, many special symbols, some reserved
        - Max character count: The data characters, control characters, start and end sentinels, and longitudinal redundancy check character shall together not exceed 79 characters.
    - 2. Numeric Track @ 75 bpi - 5 bits/char. (4 data + parity)
        - Numbers 0-9 plus control characters.
        - The data characters, control characters, start and end sentinels, and longitudinal redundancy check character shall together not exceed 40 characters.
    - 3. Numeric Track @ 210 bpi - 5 bits/char. (4 data + parity)
        - The data characters, control characters, start and end sentinels, and longitudinal redundancy check character shall together not exceed 107 characters.

- Error Detection:
    - Parity:
        - A parity bit for each encoded character shall be used. The value of the parity bit is defined such that the total quantity of one bits recorded, for each character, including the parity bit, shall be odd.
    - Longitudinal redundancy check (LRC)
        - Longitudinal EVEN parity.

Also from last week: (SpinRite and SQRL status)
From: "Rick Brooks"
Subject: Spinrite success story
Date: Fri, 18 Oct 2013 02:42:32 -0000
X-Location: Columbia, SC

Steve,

I just purchased a copy of SpinRite 6 to use on a Macbook Air that had a dead SSD drive. I had already tried every type of scan I could find and could not get any data. The machine would not boot up and the Mac drive utility failed to do any repairs.

This was a friend's machine, and she had her life on the drive with no time machine backup. She was really upset. After getting an adapter to convert the drive to use on a SATA interface, I ran SpinRite. I put the drive back in the machine and it booted up. Wow! I completed a time machine backup today and the laptop is running great. Thanks for the great software.

Rick

P.S. Please get back to SpinRite ASAP. I know you're out saving the world via SQRL, but you got me waiting on the new release, now so please hurry.

MITM Traffic Hijacking:

- Renesys: Since February, 38 distinct events in which large blocks of traffic were improperly redirected to routers at Belarusian or Icelandic ISPs.
- http://www.renesys.com/2013/11/mitm-internet-hijacking/
- http://arstechnica.com/security/2013/11/repeated-attacks-hijack-huge-chunks-of-internet-traffic-researchers-warn/
- Dan Goodin: <quote> The ease of altering or deleting authorized BGP routes, or of creating new ones, has long been considered a potential Achilles Heel for the Internet. Indeed, in 2008, YouTube became unreachable for virtually all Internet users after a Pakistani ISP altered a route in a ham-fisted attempt to block the service in just that country. Later that year, researchers at the Defcon hacker conference showed how BGP routes could be manipulated to redirect huge swaths of Internet traffic. By diverting it to unauthorized routers under control of hackers, they were then free to monitor or tamper with any data that was unencrypted before sending it to its intended recipient with little sign of what had just taken place.

Forward Secrecy @ Twitter

- twitter.com, api.twitter.com, and mobile.twitter.com
- https://blog.twitter.com/2013/forward-secrecy-at-twitter-0
- http://www.forbes.com/sites/larrymagid/2013/11/22/twitter-improves-encryption-against-nsa-and-other-snopes
- 75% of Twitters connections are now ECDHE.

Microsoft joins the group of corporations who are visibly tightening their security.

- Washington Post, yesterday:
    - <quote> Microsoft is moving toward a major new effort to encrypt its Internet traffic amid fears that the National Security Agency may have broken into its global communications links, said people familiar with the emerging plans.-

      Suspicions at Microsoft, while building for several months, sharpened in October when it was reported that the NSA was intercepting traffic inside the private networks of Google and Yahoo, two industry rivals with similar global infrastructures, said people with direct knowledge of the company's deliberations. They said top Microsoft executives are meeting this week to decide what encryption initiatives to deploy and how quickly.

- Evidence?
    - Hotmail address books collected:
        - The NSA's list of sources for the collection of online address books includes Hotmail (along with Google, Yahoo and Facebook.)
    - A Hotmail message:
        - In one of the slides there was a reference to a hotmail message.
    - An instant message from Windows Live Messenger:
        - One slide appears to show the interception of a communication on Windows Live Messenger. Since this appears non-encrypted, it is not clear whether this happened on the public Internet or as traffic moved between Microsoft data centers.

EFF: Fabulous chart showing who's encrypting what:

- Google the phrase: "encrypt the web report"
- https://www.eff.org/deeplinks/2013/11/encrypt-web-report-whos-doing-what

Newegg vs Patent Troll

- Erich Spangenberg / Span'-Gen-Berg and "TQP Development"
- TQP is just one of nine pure patent licensing companies owned by Spangenberg.
- TQP has sued hundreds of companies saying it has patented combining the RC4 cipher with SSL.
- Nearly 140 companies have paid a total of $45,370,000.
- Target had a website; Target got sued by TQP. It got out of the case by paying $40,000.
- Some paid less than that—but most paid more.
    - Dodge & Cox, a mutual fund, paid a bit more than $25,000.
    - Pentagon Credit Union paid $65,000.
    - QVC paid $75,000.
    - MLB Advanced Media paid $85,000.
    - PetSmart paid $150,000.
    - PMC paid $400,000.
    - Cigna paid $425,000.
    - Bank of America paid $450,000.
    - First National paid $450,000.
    - Visa paid $500,000.
    - Amazon, Newegg's much larger competitor, paid $500,000.
    - UPS paid $525,000.
    - IBM paid $750,000.
    - Allianz Insurance paid $950,000.
    - Microsoft paid $1,000,000.

- Profile of a patent troll:
    - All in all, Spangenberg has squeezed $45.37 million out of licenses for this one patent, which almost certainly does not actually cover the encryption used in online shopping, as Spangenberg claims.
    - Spangenberg's deal with the original inventor of the patent? The inventor gets 2.5% of the money, plus $350/hour for consulting.
    - So the inventor has made $588,000, while Spangenberg keeps the rest -- all on a patent he bought for about $750,000.

- The patent has expired, so companies are being sued for the "damages incurred" by their non-licensing of the patent while it was in effect.

- Newegg said no.

- Expert Witnesses took the stand:
- First, Ron Rivest testified, via videotaped deposition, about how he invented the RC4 cipher while at RSA Security in 1987, two years before the TQP patent application was filed.

- Then former Microsoft CTO Ray Ozzie described demonstrating Lotus Notes to Bill Gates in 1988.

- Alan Eldridge, who worked on the Notes product, flew down to Marshall in person to describe how he put RC4 in the software.

- Finally, On Friday Newegg's star witness, cryptographer Whitfield Diffie, took the stand. Diffie's goal was to knock out the Jones patent with "clear and convincing" evidence (which is the standard for invalidating a patent).

- Diffie looked the part of the eccentric genius, resplendent with his long white hair and beard. He spoke with a booming voice but carefully articulated manner; he was professorial but not overbearing. He could have been the amiable professor you wished you'd had in college.

- TQP's patent, invented alongside Michael Jones' failed modem business, wasn't much of an invention at all according to Diffie's telling. It was a pre-Internet patent, describing an old method of encoding data. Internet security needed "public key" cryptography.

- "We've heard a good bit in this courtroom about public key encryption," said Albright. "Are you familiar with that?"

- "Yes, I am," said Diffie, in what surely qualified as the biggest understatement of the trial.

- "And how is it that you're familiar with public key encryption?"

- "I invented it."

- **Then Diffie was attacked:**
- Marc Fenster, the TQP lawyer:
- "You never completed a master's degree, correct?" he asked Diffie.
    - "That's correct," said Diffie.
- "Other than the honorary degree, you don't have an earned doctorate or Ph.D. correct?"
    - "That is correct," said Diffie.
- And even though he taught a few courses, "you never had a real professorship, correct?" asked Fenster.
    - "I never had a full-time academic job, no."

- Fenster noted that while Diffie was testifying in court for the first time, he had other expert witness work lined up. His rate varies from $500 to $600 per hour, and it's $700 for testifying in court.

- And Newegg LOST.

- $5.1 in damages was claimed, $2.3 was awarded.
- Newegg has lost before, and won on appeal. They are appealing again.
-

- Newegg's Anti-Patent Troll T-shirt:
    - http://www.newegg.com/Product/Product.aspx?Item=N82E16800996221

- http://arstechnica.com/tech-policy/2013/11/newegg-trial-crypto-legend-diffie-takes-the-stand-to-knock-out-patent/
- http://arstechnica.com/tech-policy/2013/11/jury-newegg-infringes-spangenberg-patent-must-pay-2-3-million/

CryptoLocker laboratory experimentation samples available from GRC:

- https://www.GRC.com/malware
- What do we know?
- Jasen (@aliencg)
- Jasen: http://www.aliencg.com/journal/2013/11/24/cryptolocker
    - Sandboxie does indeed protect from CL.
    - Encrypted copies of the files appear inside the sandbox.

CryptoPrevent v4.3:

- http://www.foolishit.com/vb6-projects/cryptoprevent/
- "CryptoPrevent Premium" (with automatic updating)

CryptoLocker file format & 3rd party decryptor

- http://www.kyrus-tech.com/cryptolocker-decryption-engine/
- Kyrus has reverse engineered the CryptoLocker application to determine how the CryptoLocker file format works and build an open-source decryption engine. The decryption engine only works if you have the private key. Given the encryption algorithms in use by CryptoLocker, there is no known way to recover the private key without paying the ransom.

- Each file encrypted by CryptoLocker is encrypted with a unique AES-256 key. The unique symmetric key is then encrypted with the public RSA-2048 key unique to the infected host. Therefore, the only way to decrypt files encrypted with CryptoLocker is to obtain the private RSA-2048 key.

- Encrypted file header:
    - 20-byte ID cookie
    - AES key encrypted with RSA-2048
    - Remainder of the file.

Soaring price of Bitcoin prompts CryptoLocker discount
http://arstechnica.com/security/2013/11/soaring-price-of-bitcoin-prompts-cryptolocker-ransomware-price-break/

Pogoplug bring us "Safeplug": $49 TOR-in-a-box anonymous surfing

- http://gigaom.com/2013/11/21/say-hello-to-safeplug-pogoplugs-49-tor-in-a-box-for-anonymous-surfing/
- $49 TOR in a box.
- Whole home TOR anonymizing.
- Specific sites can be whitelisted (banks dislike TOR exit node IPs)
- Specific web browsers can be whitelisted: FF for TOR, Chrome for direct.

Sci-Fi News:

"Almost Human" on FOX -- OMG!!!

- Three episodes down
- Amazing 8.6 rating on IMDB

Miscellany:

- "Masters of Sex" / William Masters & Virginia Johnson on Showtime

- Steve's changed Twitter usage:
  - Timeline is now conversations.

- A Twitter Syntax guide in "manpage" format:
  - http://bit.ly/tweetfmt
  - http://aprescott.github.io/twitter-format/twitter-format.7

- Bitcoin crossed $1,000 USD for the first time. Unbelievable.