This week on Security Now!

- The HSTS Super-Cookie
- Gogo's inflight cert spoofing
- "ThunderStrike"
- A quick note about CryptoLocker's successor
- 10 questions and thoughts from our podcast's terrific listeners.
Security News:

HSTS Super-Cookie

- http://www.radicalresearch.co.uk/lab/hstssupercookies
- Strict-Transport-Security: max-age=31536000; includeSubDomains
- *.trackme.com
- Chrome, Firefox, Opera erase HSTS when they erase cookies
  - ...but NOT when crossing over into "incognito" or "private" mode.
- Safari - iPhone & iPad - no way the users to clear HSTS flags and iCloud syncs HSTS.
- But... client-side JavaScript is needed in order to probe the client's HSTS flags.

Inflight Internet provider "Gogo" is MITMing with a spoofed Google cert.

- Gogo's Home Page says: "Save up to 20% with an Unlimited Access Plan"
- ... but it's THEY who get the unlimited access!
- *.google.com
  - SAN: Server Alternate Name: www.youtube.com
- ArsTechnica: <quote> Gogo has been caught issuing a fake digital certificate for YouTube, a practice that in theory could allow the inflight broadband provider to view passwords and other sensitive information exchanged between end users and the Google-owned video service. </quote>
- Still... very unclear why they're doing this.

"ThunderStrike" / Trammel Hudson @ the Chaos Computer Congress in Hamburg

- Just like FireWire... Thunderbolt is an internal bus extension.
- "EFI" -- Extensible Firmware Interface -- brings new meaning to "extensible"
- Wikipedia's "DMA Attack:
  - <quote> Examples of connections that may allow DMA in some exploitable form include FireWire, ExpressCard, Thunderbolt, PCI and PCI Express.
- Video:http://media.ccc.de/browse/congress/2014/31c3--6128--en--saal_1--201412291830--thunderstrike_efi_bootkits_for_apple_macbooks_trammell_hudson.html#video

CryptoWall 2.0 ... CryptoLocker


Miscellany

GRC & SSL Labs - Steve rebooted his server!

- With judicious finagling of SHA1 cert expiration and TLS suite ordering, I've got GRC.com back up to an 'A' (though no longer an A+) rating on SSL Labs... while remaining compatible with Windows XP/SP2 that only supports SHA1 and TLS v1.0.
Whew.

- (And keeping Chrome happy through all of this year, too. :)

**Project Update #20: The Temperfect Mug: Coffee and Tea at The Perfect**

- <quote> The Temperfect Kickstarter campaign was funded one year ago today, on January 1st, 2014.
- I considered doing a "year in review" update for you, but decided that would just be long and tedious. In short, 2014 was the year we learned how hard it can be to work with a factory 8 (12?) time zones away, with a very different language, different ways of working, and a different concept of what a quality product is.

That leaves me with just the last month to review for you: we made a lot of progress in December, and things are starting to come together.

- BUT!!.... After all the back and forth with the mug factory in the last months, we found ourselves with enough sample parts to assemble a few mugs ourselves. So we did. Logan and I put together a mug and tested it to see how its performance would compare to computer model predictions and prototype measurements: the performance is better than predicted, and the temperature hold time was over an hour even WITHOUT vacuum insulation.

**Leo:** CES??... Any big news so far??

**SpinRite**

Tim Green in Germany / Subject: Spinrite fixes PS3s too

Just for a change, Spinrite also fixes PlayStations: We have a relatively old PS3 that we use mainly as a DVD and BluRay player and media center. It started acting up recently, hanging on bootup and exhibiting other strange stutters and pauses at unexpected times. So I took out the hard drive, connected it to a PC and let SpinRite at it on level 2. Just over an hour later I put the drive back in the PS3 and booted up for a complete transformation. Not only has it stopped hanging on startup, but it now also feels generally snappier and smoother.

Thanks once again for the only really useful hard disk maintenance and recovery utility I have ever encountered. And also of course for all your insight, information and wisdom in the show every week, which I have listened to as unfailingly as you have produced it ever since episode 1.

All the best to you, Leo and all of both of your loved ones for a happy and joyful Christmas break and thanks again!

Tim Green