Security Now! #532 - 11-03-15

Verifying iOS App Conduct

This week on Security Now!

- Brief glitch with uBlock Origin in the Chrome store
- Symantec screws up cert issuance
- "The Hacking Team" returns
- "Tor Messenger" becomes "a thing" and enters first beta
- US and UK take differing cybersecurity paths
- A clever new browser fingerprinting hack
- JavaScript (ECMAScript) 6 peek
- Threema gets an independent audit
- Miscellany: NASA, StartTrek, Fargo and more
- **The disconcerting result of my analysis of iOS Application Vetting**

Has the "Internet of Things" (IoT) gotten out of control??

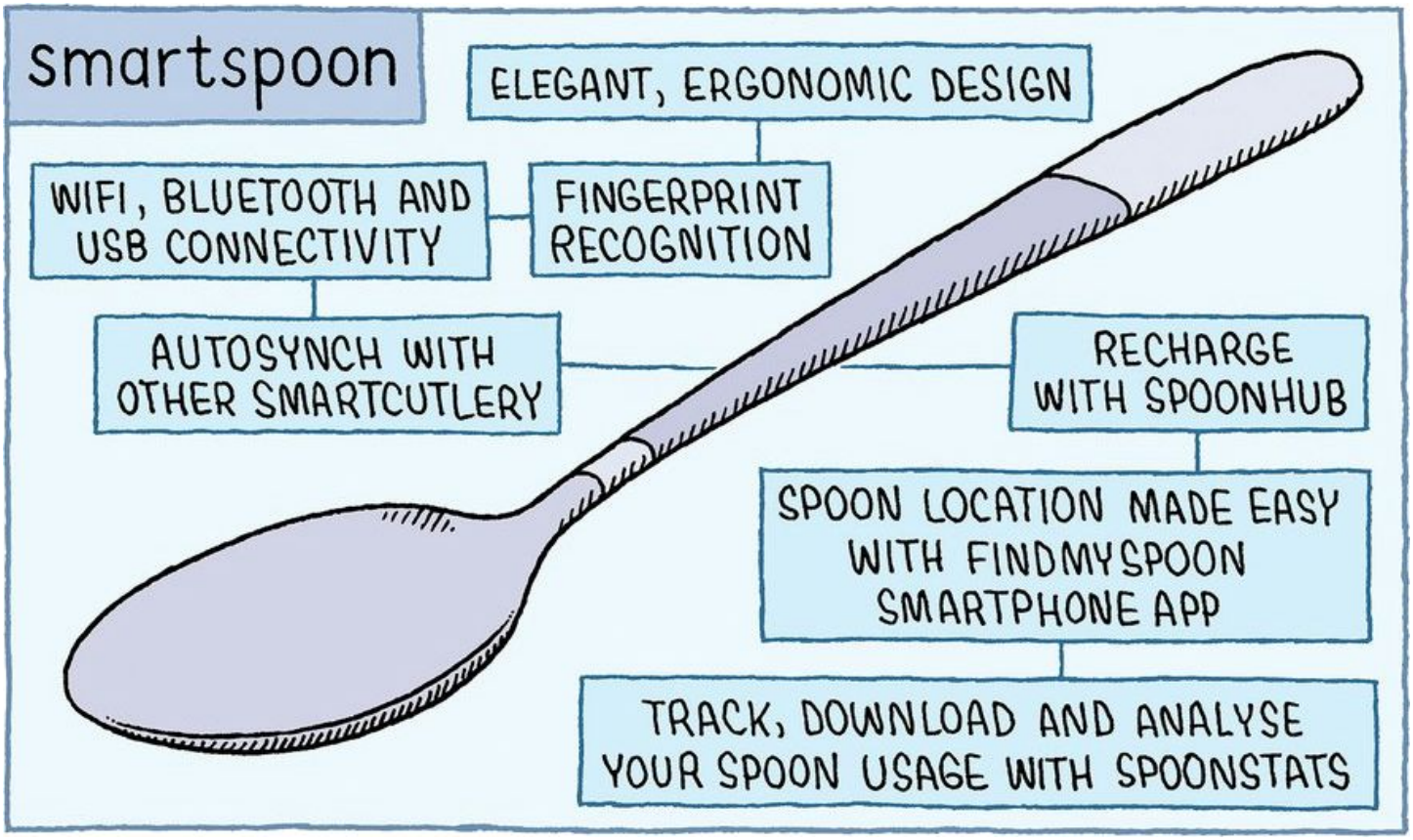

Image credit: Tom Gauld, New Scientist (@newscientist)

Security News:

uBlock Origin removed from Chrome -- or perhaps not

- https://github.com/gorhill/uBlock/issues/880
- Google: (5 days ago)
  - Dear Developer,
    Your Google Chrome item, "uBlock Origin," with ID: cjpalhdlnbpafiamejdnhcphjbkeiagm did not comply with the following section of our Program policies: "Where possible, make as much of your code visible in the package as you can. If some of your app's logic is hidden and it appears to be suspicious, we may remove it."
- Gorhill: (hybrid of John Dvorak & Richard Stalman)
  - This amounts to: "There is somewhere one or more pieces of code I don't understand, but I won't tell you what it is. Your challenge is to find what I am talking about and modify it so that in my next review I will maybe understand it."
- Google:
  - Dear Developer,
    We apologize that the update was rejected due to an snag in the review system. The updated item will be available in the Chrome Web Store within 30 minutes.
    Thank you for your cooperation,
    Google Chrome Web Store team
- Gorhill:
  - Sorry for this, that really got me worried. If this happens again I will at wait a bit more for feedback from the Chrome store before reporting here. Unclear though whether making such issue widely known sooner than later helps with its resolution, or at least a faster one.

Chrome won't trust Symantec-backed SSL as of Jun 1, 2016 unless...

- Links
  - http://boingboing.net/2015/11/01/chrome-wont-trust-symantec-b.html
  - http://www.zdnet.com/article/google-to-symantec-clean-up-your-certificates-or-be-branded-unsafe/
  - http://arstechnica.com/security/2015/10/still-fuming-over-https-mishap-google-gives-symantec-an-offer-it-cant-refuse/

- Symantec / September 18th "A Tough Day as Leaders"
  http://www.symantec.com/connect/blogs/tough-day-leaders
  We learned on Wednesday that a small number of test certificates were inappropriately issued internally this week for three domains during product testing. All of these test certificates and keys were always within our control and were immediately revoked when we discovered the issue. There was no direct impact to any of the domains and never any danger to the Internet. Further, we are in the process of proactively notifying the domain owners and our major partners.

  In light of these events, we must reassert our commitment to stand behind our values and our position as a trusted industry leader. While our processes and approach are based on

the industry best practices that we helped create, we have immediately put in place additional processes and technical controls to eliminate the possibility of human error. We will continue to relentlessly evolve these best practices to ensure something like this does not happen again.

In addition, we discovered that a few outstanding employees, who had successfully undergone our stringent on-boarding and security trainings, failed to follow our policies. Despite their best intentions, this failure to follow policies has led to their termination after a thoughtful review process. Because you rely on us to protect the digital world, we hold ourselves to a "no compromise" bar for such breaches. As a result, it was the only call we could make.

As much as we hate to lose valuable colleagues, we are the industry leader in online safety and security, and it is imperative that we maintain the absolute highest standards. At the end of day, we hang our hats on trust, and that trust is built by doing what we say we're going to do.

- Google / October 28th (last Wednesday)
  https://googleonlinesecurity.blogspot.com/2015/10/sustaining-digital-certificate-security.html
  Following our notification, Symantec published a report in response to our inquiries and disclosed that 23 test certificates had been issued without the domain owner's knowledge covering five organizations, including Google and Opera.

  However, we were still able to find several more questionable certificates using only the Certificate Transparency logs and a few minutes of work. We shared these results with other root store operators on October 6th, to allow them to independently assess and verify our research.

  Symantec performed another audit and, on October 12th, announced that they had found an additional 164 certificates over 76 domains and 2,458 certificates issued for domains that were never registered.

  It's obviously concerning that a CA would have such a long-running issue and that they would be unable to assess its scope after being alerted to it and conducting an audit. Therefore we are firstly going to require that as of June 1st, 2016, all certificates issued by Symantec itself will be required to support Certificate Transparency. In this case, logging of non-EV certificates would have provided significantly greater insight into the problem and may have allowed the problem to be detected sooner.

  After this date, certificates newly issued by Symantec that do not conform to the Chromium Certificate Transparency policy may result in interstitials or other problems when used in Google products.

Hacking Team Is Back with a Bold Pitch to Police

- http://motherboard.vice.com/en_uk/read/hacking-team-is-back-with-a-bold-pitch-to-police
- Four months ago, "PhineasFisher" hacked into their server and leaked 400GB of internal data, including eMails, customer lists, source for the RCS - Remote Control System - spyware.
- Sent to its mailing list on October 19th:
  - Hacking Team's CEO David Vincenzetti wrote: "Most law enforcement agencies in the US and abroad will become 'blind,' they will 'go dark' they will simply be unable to fight vicious phenomena such as terrorism." "Only the private companies can help here, we are one of them."
  - "It is crystal clear that the present American administration does not have the stomach to oppose the American IT conglomerates and to approve unpopular, yet totally necessary, regulations."
  - Hacking Team is "finalizing brand new and totally unprecedented cyber investigation solutions."
- Some customers have remained, others have or are leaving...

Tor Messenger / Thursday / Oct 29th

- http://arstechnica.co.uk/security/2015/10/how-to-use-tor-messenger-the-most-secure-chat-program-around/
- First public beta of "Tor Messenger"
- Easy-to-use
- A combination of Tor (for anonymity) and OTR (off the record chat protocol) for privacy.
- Supports many chat carriers and protocols.

EFF / Thursday / Oct 29, 2015

- VICTORY: State Department Decides Not to Classify "Cyber Products" as "Munitions"
- https://www.eff.org/deeplinks/2015/10/victory-state-department-decides-not-classify-cyber-products-munitions
- <quote> This week, the U.S. Department of State's "Defense Trade Advisory Group" (DTAG) met to decide whether to classify "cyber products" as munitions, placing them in the same export control regime as hand grenades and fighter planes. Thankfully, common sense won out and the DTAG recommended that "cyber products" not be added to the control list.

In the UK:
Internet firms to be banned from offering unbreakable encryption under new laws

- http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11970391/Internet-firms-to-be-banned-from-offering-out-of-reach-communications-under-new-laws.html
- Companies such as Apple, Google and others will no longer be able to offer encryption so advanced that even they cannot decipher it when asked to under the Investigatory Powers Bill.
- It will also require internet companies to retain the web browsing history of their customers for up to a year.

- The bill is expected to face a tough route through parliament but Mr Cameron urged critics to back the measures. He told ITV's This Morning: "As Prime Minister I would just say to people 'please, let's not have a situation where we give terrorists, criminals, child abductors, safe spaces to communicate'.
- "It's not a safe space for them to communicate on a fixed line telephone or a mobile phone, we shouldn't allow the internet to be a safe space for them to communicate and do bad things."

- Lord Carlile, the former terrorism laws watchdog, said there had been a "lot of demonization" of the police and security services over their intentions for such information.
- "I think it is absurd to suggest the police and the security services have a kind of casual desire to intrude on the privacy of the innocent," he said. "They have enough difficulty finding the guilty. No-one has produced any evidence of casual curiosity on part of the security services."

Probe of the browser's HSTS Cache State

- A timing attack against HSTS
- https://zyan.scripts.mit.edu/sniffly/
- http://thehackernews.com/2015/10/track-online-users.html
- https://zyan.scripts.mit.edu/presentations/toorcon2015.pdf
- "Sniffing browser history using HSTS + CSP"
    - HTTP Strict Transport Secrecy
    - Content-Security-Policy
        - Set CSP to "img-src http://*"
        - HTTPS image requests are blocked and trigger an error event.
- Sniffly is an attack that abuses HTTP Strict Transport Security and Content Security Policy to allow arbitrary websites to sniff a user's browsing history. It has been tested in Firefox and Chrome.
- Steve explains:
    - It's a way for any remote web server to probe an HSTS-supporting browser to determine whether its holding an HSTS rule.
    - If an HSTS rule exists, an attempted fetch of an HTTP image will be instantly converted into HTTPS, but then the CSP rule will block that and force an instant error WITH NO NETWORK USAGE.
    - If no HSTS rule exists, the browser will attempt to fetch the HTTP image over the Internet.

- How it works:
    - User visits Sniffly page
    - Browser attempts to load images from various HSTS domains over HTTP.
    - Sniffly sets a CSP policy that restricts images to HTTP, so image sources are blocked before they are redirected to HTTPS. This is crucial! If the browser completes a request to the HTTPS site, then it will receive the HSTS pin, and the attack will no longer work when the user visits Sniffly.
    - When an image gets blocked by CSP, its onerror handler is called. In this case, the onerror handler times how long it took for the image to be redirected from HTTP to

HTTPS. If this time is on the order of a millisecond, it was an HSTS redirect (no network request was made), which means the user has visited the image's domain before. If it's on the order of 100 milliseconds, then a network request probably occurred, meaning that the user hasn't visited the image's domain.

- Caveats:
  - Not supported yet in Safari, IE, or Chrome on iOS.
  - Extensions such as HTTPS Everywhere will mess up results.
  - Doesn't work reliably in Tor Browser since timings are rounded to the nearest 100-millisecond.
  - Users with a different HSTS preload list (ex: due to having an older browser) may not see accurate results.

ECMAScript 6 (ES6):

- http://babeljs.io/docs/learn-es2015/
- ECMAScript 6 is the newest version of the ECMAScript standard.
- Ratified in June 2015.
- ES2015 is a significant update to the language.
- First major update to the language since ES5 was standardized in 2009.
- Implementation of these features in major JavaScript engines is underway now.
- What's New in the next version of JavaScript
  - http://www.smashingmagazine.com/2015/10/es6-whats-new-next-version-javascript/
  - "let" for local block scoping (instead of function scoping).
  - CONST (block scoped invariants)
  - A bunch of handy new Array, Math, String methods (operations)
  - Default function parameters
  - Nice, instead of needing to test for 'undefined' in the function and manually assign.
  - Formal support for MODULES with export and import
  - "import { sum, pi } from "lib/math";
  - Formal support of user-defined Classes
  - Constructor
  - Methods
  - // Create an instance
  - let myVehicle = new Vehicle('rocky');
  - Inherit from and Extend a base class.
  - Access to the base "super" class.

- TRANSPILATION
  - Current language Support:
  - http://kangax.github.io/compat-table/es6/
  - Microsoft's EDGE browser leads ALL OTHERS!!

Results of an independent audit of Threema:

- https://threema.ch/en/blog
- Audit Methodology:
  - A well-respected independent Swiss IT research lab states: "We confirm the quality of the system as claimed by Threema in their public specification".
  - For its thorough investigation, the auditing agency was granted full access to Threema app's source code as well as the servers, and our developer team provided any assistance needed.
  - Two of Threema's main promises are: The whole communication – including group chats, media, files and status messages – is end-to-end encrypted. Threema is designed to limit users' data track to a bare minimum (e.g., groups and contact lists are handled on users' devices instead of our servers). Both of these assertions were confirmed by the audit.
- The auditing agency attests in its report:
  - Threema's concepts meet the requirements for truly secure and trustworthy messaging.
  - The application of the encryption is correct and implemented as documented by Threema.
  - The used protocols are free of vulnerabilities.
  - The app's local data is stored in a safe and secure manner.
  - The server components only store data that is absolutely necessary for message delivery.
  - The servers are located in Switzerland.
- Audit PDF:
  - https://threema.ch/press-files/2_documentation/external_audit_security_statement.pdf

- What's new:
  - https://threema.ch/en/whats-new
  - iOS:
    - Send any type of file (pdf, animated gif, mp3, doc, zip, etc.) *
      - * if supported by the recipient's phone. Up to 20MB.
  - Group chats now support up to 30 members
  - Many improvements and bug fixes

Miscellany

NASA looking for 60-year old engineers who still remember FORTRAN and Assembly Language..
http://www.popularmechanics.com/space/a17991/voyager-1-voyager-2-retiring-engineer/
Larry Zottarelli, the last original Voyager engineer still on the project, is retiring after a long and storied history at JPL. While there are still a few hands around who worked on the original project, the job of keeping this now-interstellar spacecraft going will fall to someone else. And that someone needs to have some very specific skills....
WARNING: "Only" 64K of memory!

We're FINALLY GETTING A NEW StarTrek Series on CBS!
http://www.startrek.com/article/new-star-trek-series-premieres-january-2017
New Star Trek Series Premieres January 2017
Executive Producer: Alex Kurtzman
Alex did the new StarTrek (2009) movie, the "Into Darkness", Spider-Man 2, FRINGE!, MI3, Cowboys & Aliens... and so on.
Just watched: "The Inner Light" / Season 5 / Episode 23 (2nd to last)

Fargo -- The BEST series on television: IMDB 9.0/10
Writing, acting.
1st season was amazing... 2nd season is even better!

Free this week on iTunes: ROP

- Relaxing, combinatorial puzzle/game

Chromebook -- 100% agree with Leo... it's a WIN for so many.

Errata:

The boiled-frog myth

- Mark Sidell (@msidell)
- http://www.theatlantic.com/technology/archive/2006/09/the-boiled-frog-myth-stop-the-lying-now/7446/
- Everyone who has heard a political speech knows this story: You put a frog into a pot of boiling water, and it jumps right out. But if you put it in a pot of nice comfortable water and then turn on the heat, the frog will complacently let himself be boiled. One standard version of the story is here. The reason it's so popular in politics is that it's an easy way to warn about the slow erosion of liberties or any other slow threat you want to talk about.

  Here's the problem. It just isn't true. If you throw a frog into a pot of boiling water, it will (unfortunately) be hurt pretty badly before it manages to get out -- if it can. And if you put it into a pot of tepid water and then turn on the heat, it will scramble out as soon as it gets uncomfortably warm.

SpinRite

Maik Musall (@maikm)
@SGgrc Spinrite Q for SN: After fixing a faulty disk, is it wise to replace it ASAP, or is it as good as a non-faulty one afterwards?

>>> SMART <<<

Verifying iOS App Behavior

- The current iOS Application model, which uses Objective-C as an option, is FUNDAMENTALLY UNSECURABLE against rogue apps accessing privileged platform functions.
  Why?... Because it wasn't originally built to support untrusted applications!!
  ...And, thus, it cannot do so securely.

- Apple actually **depended** upon the "obscurity" of not documenting restricted APIs in the file headers.

- Strict process controls, known as "Entitlements" exist, but since the public API libraries also need to use private APIs, the private APIs MUST be accessible within the unprivileged process space.

- "Dynamic code generation" must be provided for Safari's JIT compiler, but it CAN and IS denied for other apps. But… dynamic code generation is not needed.

- As long as Objective-C, with its dynamic string-based dictionary lookup binding is supported, iOS will be vulnerable.