Security Now! #606 - 04-04-17

Proactive Privacy

This week on Security Now!

This week Steve and Leo discuss another iOS update update, more bad news and some good news on the IoT front, the readout on Tavis Ormandy's shower revelation, more worrisome anti-encryption saber rattling from the EU, a look at a recent Edward Snowden tweet, Samsung's S8 mistake, an questionable approach to online privacy, celebrating the 40th anniversary of Alice and Bob, some quickie feedback loops from our listeners, an update on my projects, and a comprehensive examination of proactive steps users can take to enhance their online privacy.

Our Picture of the Week

Security News

iOS updated again, yesterday, to v10.3.1

- https://support.apple.com/en-us/HT207688
- Released April 3, 2017
- Wi-Fi

  Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

  Impact: An attacker within range may be able to execute arbitrary code on the Wi-Fi chip

  Description: A stack buffer overflow was addressed through improved input validation.

  CVE-2017-6975: Gal Beniamini of Google Project Zero

From the: "We should have seen this one coming" Department:

- As many as 90% of Smart TVs are probably vulnerable to wireless hacking via rogue TV signals

- The "Weeping Angel" attack disclosed in Wikileaks' Vault 7 documents required physical access. No so this latest attack.

- Security researcher Rafael Scheel, with the Swiss cyber security consulting company Oneconsult, has developed and demonstrated an over-the-air remote exploit of a Samsung television.

- https://www.youtube.com/watch?v=bOJ_8QHX6OA

- The proof-of-concept exploit uses a low-cost transmitter to embed malicious commands into a television broadcast. When received by a television set (in this case two different fully patched Samsung models) it was able to exploit two known security flaws in the Web browsers running in the background to obtain root privilege access to the TVs

- Rafael notes that by modifying the attack to target similar browser bugs found in other sets, the technique would likely work on a much wider range of TVs.

- Rafael said: "Once a hacker has control over the TV of an end user, he can harm the user in a variety of ways. Among many others, the TV could be used to attack further devices in the home network or to spy on the user with the TV's camera and microphone."

- This particular PoC was based upon DVB-T, which is the European digital broadcasting standard. In the US we use ATSC for over-the-air (OTA) digital broadcasting. But there's nothing at all specific about DVB-T, it was merely what the researcher had. There should be zero doubt that ATSC-based receivers are every bit as vulnerable.

- Our Security Now takeaway: Seriously look into creating isolated network segments and security perimeters.

- PC's have vastly more mature security and also vastly more sensitive data.

- IoT's have vastly less mature security and also much less sensitive data.

- And those two domains have very little need to connect with one another.

- They should be placed into separate isolated network domains and blinded to each other's presence.

- Get a cheap cheesy WiFi-only tablet or retired Smartphone to use on the IoT side for control... and never use it for sensitive tasks.

- Links:
  - https://www.bleepingcomputer.com/news/security/about-90-percent-of-smart-tvs-vulnerable-to-remote-hacking-via-rogue-tv-signals/
  - https://www.techworm.net/2017/04/smart-tvs-can-hacked-embedding-code-air-signals.html
  - https://arstechnica.com/security/2017/03/smart-tv-hack-embeds-attack-code-into-broadcast-signal-no-access-required/
  - http://thehackernews.com/2017/03/hacking-smart-tvs.html
  - https://thenextweb.com/security/2017/04/03/hackers-can-now-attack-your-smart-tvs-by-tapping-over-the-air-signals/

Z-Wave's "Wave Alliance" introduces S2 - "Security 2"

- http://z-wavealliance.org/mandatory-security-implementation-z-wave-certified-iot-devices-takes-effect-today/

- A state-of-the-art specification built into the latest SDK.

- Uses efficient DTLS (Datagram TLS), public and private keys for every device

- ECDH key derivation.

- Everything is built into the lower-level protocol, supported by the supplied SDK... so this allows security to be built-in from the start, not optionally tacked-on as an afterthought.

The full story on Travis Ormandy' fruitful shower weekend before last.

- https://bugs.chromium.org/p/project-zero/issues/detail?id=1225&desc=6
  Content Scripts:
  Different from extensions, Content Scripts are JavaScript injected into a page for performing work on the page itself -- finding URLs that are not links and turning them into HREF links, changing font sizes, adding fields to forms, etc. In short, modifying the page's content.

- Google's own documentation states:
  Content scripts execute in a special environment called an isolated world. They have access to the DOM of the page they are injected into, but not to any JavaScript variables or functions created by the page. It looks to each content script as if there is no other JavaScript executing on the page it is running on. The same is true in reverse: JavaScript running on the page cannot call any functions or access any variables defined by content scripts.

  Isolated worlds allow each content script to make changes to its JavaScript environment without worrying about conflicting with the page or with other content scripts. For example, a content script could include JQuery v1 and the page could include JQuery v2, and they wouldn't conflict with each other.

  Another important benefit of isolated worlds is that they completely separate the JavaScript on the page from the JavaScript in extensions. This allows us to offer extra functionality to content scripts that should not be accessible from web pages without worrying about web pages accessing it.
    - ... Except that's not completely true.

- In JavaScript, variables can have values, or they can be left undefined.
  In fact, all variable are undefined until they are defined.
  The "undefined-ness" can be tested for using the "typeof" function:
    - if (typeof trusted != "undefined") { something }

- The LastPass coders relied upon the enforcement of content scripts "isolated worlds" and also upon variables' undefined-ness, to control the availability and execution of privileged LastPass code.

- But it turns out that there actually IS some very subtle cross-world isolation leakage.

- During his now-infamous shower on the morning of Saturday, March 25th, as Tavis was lathering up he was doubtless ruminating over the LastPass code he had been studying. He was thinking about how LastPass was using the "undefined" property of variables to control access to sensitive Content Script code... and he suddenly realized that there WAS A WAY for code on the page to influence isolated world code by causing the "undefined" property to become false:

- Although a page cannot directly define variables, the isolated worlds *do* share the same DOM (the Document Object Model), and DOM element ids automatically become properties of window! Whoops!!
    - el = document.createElement("exploit")
    - el.setAttribute("id", "trusted");
    - document.body.appendChild(el);

- We only know all of this because the LastPass folks jumped on it immediately, found and fixed some 3,000 individual instances throughout their code where this had been done, and everyone now has updated versions of LastPass.

EU to propose new rules targeting encrypted apps in June

- http://www.euractiv.com/section/data-protection/news/eu-to-propose-new-rules-on-police-access-to-encrypted-data-in-june/

- Last week we covered how the UK's Home Secretary Amber Rudd publicly announced that encrypted messaging services should be forced to give access to police. Rudd singled out Facebook-owned WhatsApp just as British media reported that the attacker in last week's London terrorist attack used the messaging app.

- EU Justice Commissioner Vera Jourová said last Tuesday that the European Commission is planning to propose new measures in June to make it easier for police to access data on internet messaging apps such as like WhatsApp.

  Jourová said she will announce "three or four options" including binding legislation and voluntary agreements with companies to allow law enforcement authorities to demand information from internet messaging apps "with a swift, reliable response".

  The announcement comes as interior ministers from EU countries have amped up pressure on the Commission to introduce new rules to help police crack through secure encryption and demand private data for investigations.

  Non-legislative measures will be provisional "to have a quick solution", since negotiations over EU laws can drag on for years before they are passed.

  Jourova said: "At the moment, prosecutors, judges, also police and law enforcement authorities, are dependent on whether or not providers will voluntarily provide the access and the evidence. This is not the way we can facilitate and ensure the security of Europeans, being dependent on some voluntary action." Jourová also said that the measures would make it easier for law enforcement authorities to request and access data from online services that are registered outside their jurisdictions.

  Also, both German and French Interior Ministers said that they want police to have the same legal right to access online services as they do to demand phone call information from telecoms companies.

  Officials said: "Germany and France have asked the European Commission to study the possibility of making internet operators subject to the same requirements as telephone operators."

Edward Snowden

- "Huge: USG confirms cyber offense funded at 9x rate of defense.
  Wonder why we can't stop foreign hacks? This is why.
  http://www.reuters.com/article/us-usa-cyber-defense-idUSKBN17013U"

- No… that's not why. Not at all.

- The trouble is, Offense and Defense are not the same. Not at all.
- Offense and Defense ***sound*** reciprocal, but that's only true if it's one-on-one.
- When it's many-to-many, when on the offense, anyone can attack anyone else…
- But when on defense, everyone must prevent attacks from everyone else.
- Offense is easy -- Defense of far far more difficult and diffuse.

Samsung's new S8 with "facial recognition" unlocks when shown a photo.

- Facial Recognition, Fingerprint & Iris security.
- Facial Recognition can be unlocked with a photo or a sleep person's face.
- Samsung is defending the facial recognition technology, saying that it's just for fun and that it cannot be used to unlock the phone's more security services, such as payment.
- Still... I think it's unwise to have "toy" security.
  Links:
  - https://9to5google.com/2017/03/31/samsung-galaxy-s8-facial-recognition-security-questioned/
  - https://www.usatoday.com/story/tech/talkingtech/2017/03/31/photo-fools-samsung-s8-facial-recognition-feature/99889228/

Hide your actual Internet usage in the noise...

- https://noiszy.com/
- https://chrome.google.com/webstore/detail/noiszy/immakaidhkcddagdjmedphlnamlcdcbg
- The Chrome Extension Description:

  They're listening. Make some noise.

  Whatever you do online, you leave digital tracks behind. These digital footprints are used to market to you - and to influence your thinking and behavior.

  Congress has voted to allow ISPs to collect and sell your online information without your consent. Erasing these footprints - or not leaving them in the first place - is becoming more difficult, and less effective. Hiding from data collection isn't working.

  Instead, we can make our collected data less actionable by leaving misleading tracks, camouflaging our true behavior. We can resist being manipulated by making ourselves harder to analyze - both individually, and collectively.

  We can take back the power of our data.

  Noiszy is a browser plugin that creates meaningless web data - digital "noise."

  It visits and navigates around websites, from within your browser, leaving misleading digital footprints around the internet. Noiszy only visits a list of sites that you approve, and only works when you turn it on. Run Noiszy in the background while you're working, or start Noiszy when you're not using your browser, and it sends meaningless data to these sites for as long as you let it run.

This meaningless data dilutes the significance of your "real" data, by creating a campaign of misinformation. You become more difficult for an algorithm to understand, market to, or manipulate. You can outsmart the "filter bubble".

- To use Noiszy:
  - Open a new tab.
  - Click the Noiszy icon.
  - Choose the sites you want Noiszy to randomly browse, and click Start.

- Noiszy randomly chooses from your list of sites. Then, it randomly chooses from and clicks on links within those pages, choosing only onsite links that don't open new windows. There are delays between clicks of about 1 minute; this makes web traffic appear to be more real and engaged. After about 2-5 onsite clicks, Noiszy randomly chooses another site from the list, and repeats the process. This continues (even when your tab is in the background) until you close the tab or click Stop.

Alice and Bob turn 40 this month.

- Mikko Hypponen (@mikko) F-Secure's chief security research officer tweeted:
  "Happy 40th birthday to Alice and Bob! They were introduced in this April 1977 paper by Rivest, Shamir and Adleman."

- http://people.csail.mit.edu/rivest/Rsapaper.pdf

- A Method for Obtaining Digital Signatures and Public-Key Cryptosystems
  R.L. Rivest, A. Shamir, and L. Adleman

  Abstract
  An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

  1. Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.

  2. A message can be "signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in "electronic mail" and "electronic funds transfer" systems.

Security Now Feedback Loop

The Fat Vegan Chef (@thefatveganchef)
@SGgrc Can ISP install a certificate that will give them access to secure traffic unencrypted? If/then... browsing securely is mute & they can data mine all they want.

From Simon Zerafa:
@SGgrc FYI on LibSodium ??

> Frank Denis @jedisct1
> Support for random[.]org as a CSPRNG was added to libsodium (will be the default soon). Note that this requires libcurl built with openssl.

- Yuck!!! What a kludge! :(
  Though, I suppose in an environment where there is absolutely no good local source of entropy... reaching out would be better than nothing. But it's also easy to see how a spoofed cert and DNS intercept could redirect to a fraudulent source of entropy.
  /Steve.

Mark Gottselig (@markgottselig)
@SGgrc Is there an IoT security grade or review website you trust we might be able to use to find secure IoT devices?

Isaac (@koruptid)
@SGgrc if you are so worried about what the gov't might do in the future to weaken crypto... duty to create it. duty to resist. >$ profit.

Troy Carlson (@troy_carlson)
@SGgrc the S in IOT stands for security. and the P stands for privacy.

DrSuarez (@DrSuarez)
Hi @SGgrc Does 3 router solution protect privacy from ISPs if traffic is HTTPS and originates from internal router?
https://www.pcper.com/reviews/General-Tech/Steve-Gibsons-Three-Router-Solution-IOT-Insecurity

Jim Clark (@jimclark97321)
My wife asked me to stop commercials from auto playing in Firefox. We have "privacy badger", "ublock origin", and "https everywhere", and nothing else. I started thinking of all the trouble of "no script". I searched about:config and found media.autoplay.enabled was set to true. I changed it to false. She is happy now, Love Spinrite.

Jon M (@Liquidretro)
@SGgrc I just checked some of my businesses rebate gift cards 1 had been drained due to fraud. Thanks for the heads up.

Alastair Campbell (@alastc)
@SGgrc I'm skeptical that ISPs will be able to force install ssl certs, thanks to proliferation of iot devices with no interface for that.

> Ah, yes... that's a good point. And TV's and TiVo's and many other devices that may be working over TLS. :)

(((lbutlr))) @lbutlr
@SGgrc The reason the companies want SMS "security" is so if they have your phone number

Please remember that I cannot reply to you if you're not following me. I reply by DM's.

SQRL Update

- Server side is finished.
- I'm working on the self Install / Remove / Update
- Final functionality verification and UI-jargon consistency.
- Public release for everyone here to play with it. (English-only at first.)
- Then I synchronize the online documentation with the final operation.
- ... and return to work on SpinRite v6.1 while we see whether SQRL gains traction.
- If it does... it's ready for multi-lingual support.

SpinRite

Available FIRST to everyone who already owns v6.0

Proactive Privacy

The ideal:

- A separate 1-to-1 relationship with each site and no possibility for crossover or tracking.

The power of major web players

- Browsers populate pages with content from all over the web.
- Each fetch has query headers which we've seen can be used as a fingerprint.
- Each fetch returns any cookies matching the fetched site's domain.
- Google Analytics
  - Google KNOWS who we are.
- Facebook
  - Facebook KNOWS who we are.
- Major advertising networks

The power of the "incognito" browsing modes.

Separate browser

- The Accepts and User-Agent headers disclose add-ons and plug-ins and versions.

The need for a different IP address. :(

- Long-term transient, short-term fixed.

The power of the ISP

- HTTP vs HTTPS
- DNS?
  - Use GRC's Spoofability test to check DNS with and without VPN.
- What if they force subscribers to install their "ISP" certificate?

The power of the VPN

- The good news - instantly a new public IP
- The bad news - traffic emerges from fewer points of concentration.
- How to choose a VPN provider:
  - Should be using OpenVPN system (nothing proprietary).
  - Should have a large range of VPN endpoints for geographical dispersion and increased interception.