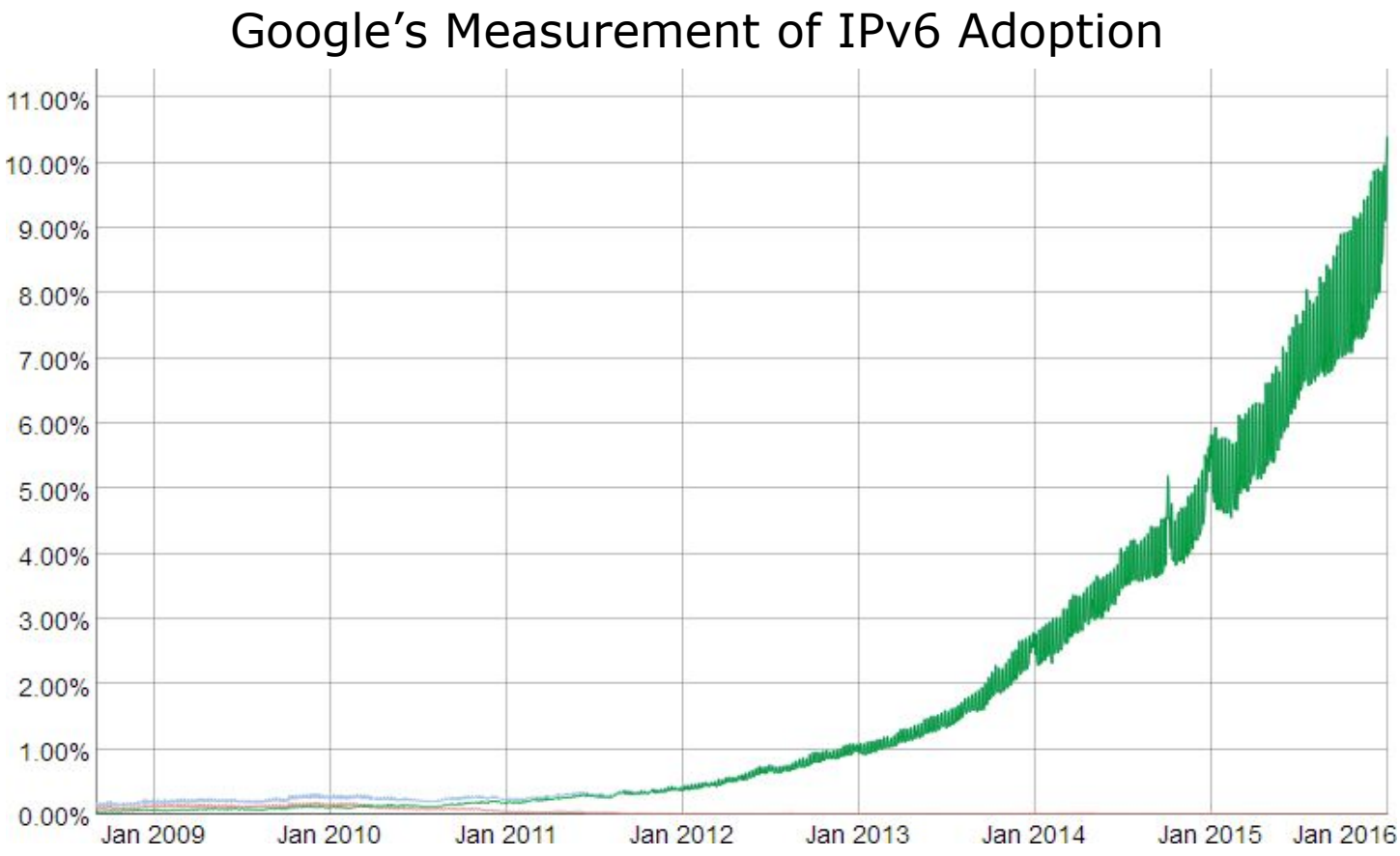
Security Now! #541 - 01-05-15

New Years News

This week on Security Now!

- Some GWX (Get Windows X) (whether you want it or not) news updates
- A Windows 10 Market share snapshot
- Hysteria over Windows 10 sending disk encryption to Microsoft
- Looking back at the security vulnerability counts of 2015
- Google issues critical updates for recent Android versions.
- Ransomeware goes multi-platform with JavaScript
- The next IoT Wi-Fi standard is ratified
- Smartwatch side-channel attacks
- IPv6 adoption at its 20 year mark
- A whole bunch of Miscellany!



Security News:

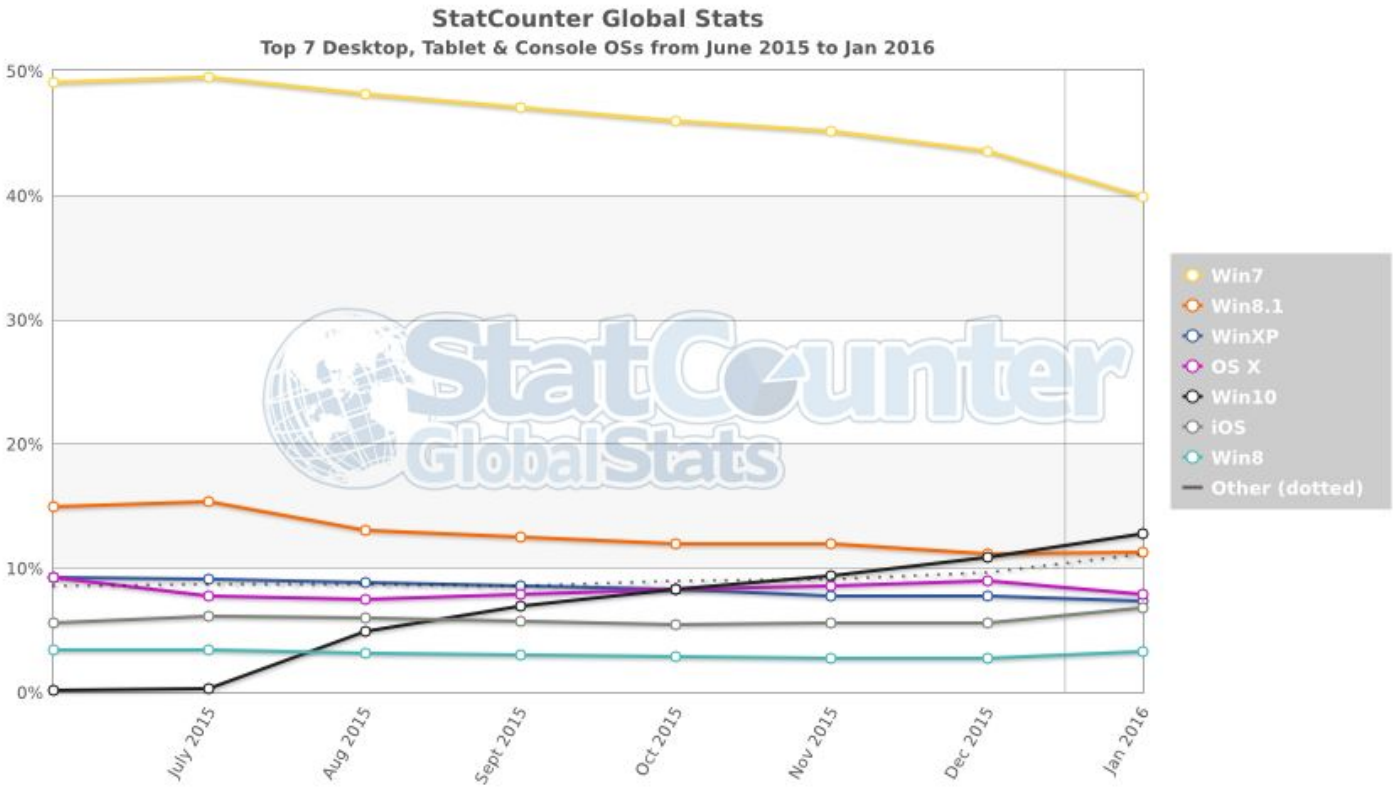
First listener report of GWX switching itself back on...

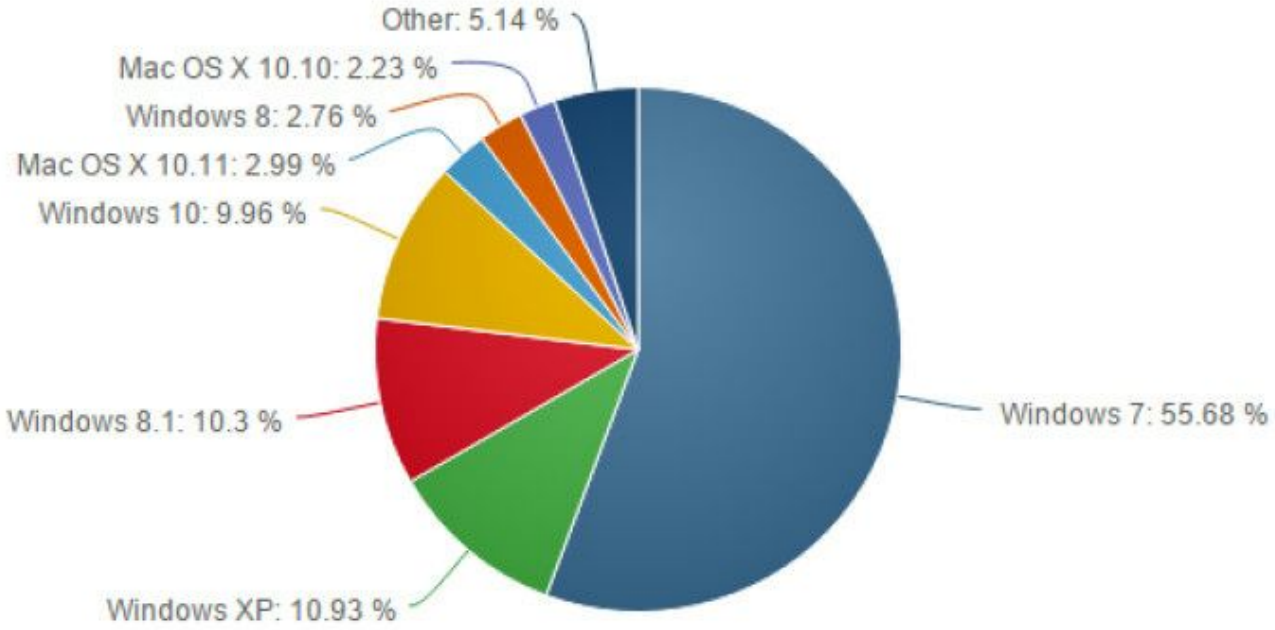
- Charles Killmer (@charleskillmer)
  This morning the GWX Control Panel alerted me to OS Updates being re-enabled. I have not installed anything recently. Update history show only Windows defender updates. Thanks for the tip on GWX Control Panel.
- http://blog.ultimateoutsider.com/2015/08/using-gwx-stopper-to-permanently-remove.html

Don't rely upon Microsoft to back you out of an unwanted Windows X

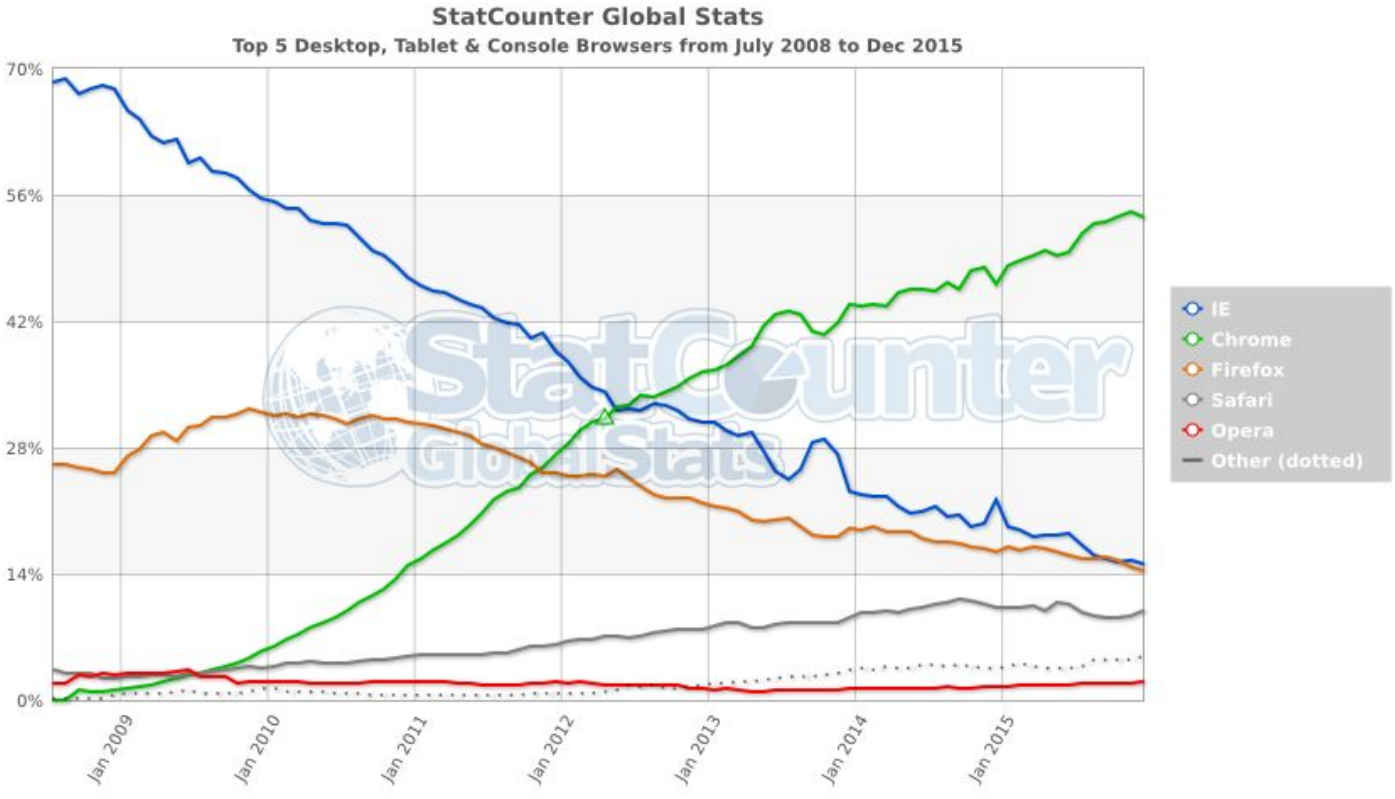
- OneEye Rabbit (@OneEyeRabbit)
  Steve in #539 you talked about GWX for me I tried WinX from 07-DEC-2015 thru 22-DEC-2015 -- Finally, I had enough and tried to revert [to my previous Windows 7.] MS said you have 30 days to revert, but for me after two weeks that option was NO LONGER AVAILABLE -- I used a restore point to get back to Win7. Now I'll have to deal with GWX again.

Windows 10: Market share is climbing, now getting close to Windows 8.1
http://www.neowin.net/news/windows-10-market-share-is-climbing-now-getting-close-to-windows-81





And while we're looking at charts… here's browser utilization history:



http://gs.statcounter.com/

Windows 10 Disk Encryption Keys in the Cloud

- "Recently Bought a Windows Computer? Microsoft Probably Has Your Encryption Key"
  - https://theintercept.com/2015/12/28/recently-bought-a-windows-computer-microsoft-probably-has-your-encryption-key/
- First of all... this is NOT a new concern in Windows 10. "Device Encryption" with key escrow was initially introduced with Windows 8.1 in 2013.
- <quote> ONE OF THE EXCELLENT FEATURES of new Windows devices is that disk encryption is built-in and turned on by default, protecting your data in case your device is lost or stolen. But what is less well-known is that, if you are like most users and login to Windows 10 using your Microsoft account, your computer automatically uploaded a copy of your recovery key — which can be used to unlock your encrypted disk — to Microsoft's servers, probably without your knowledge and without an option to opt out.

  The fact that new Windows devices require users to backup their recovery key on Microsoft's servers is remarkably similar to a key escrow system, but with an important difference. Users can choose to delete recovery keys from their Microsoft accounts... But they can only delete it after they've already uploaded it to the cloud.

- Matthew Green (Johns Hopkins cryptographer)
  "The gold standard in disk encryption is end-to-end encryption, where only you can unlock your disk. This is what most companies use, and it seems to work well. There are certainly cases where it's helpful to have a backup of your key or password. In those cases you might opt in to have a company store that information. But handing your keys to a company like Microsoft fundamentally changes the security properties of a disk encryption system."

  "Your computer is now only as secure as that database of keys held by Microsoft, which means it may be vulnerable to hackers, foreign governments, and people who can extort Microsoft employees."

- After you finish setting up your Windows computer, you can login to your Microsoft account and delete the recovery key. Is this secure enough? Matthew says: "If Microsoft doesn't keep backups, then maybe. But it's hard to guarantee that. And for people who aren't aware of the risk, opt-out seems risky."

- Also in the article:
  - How to delete your recovery key from your Microsoft account
  - Generate a new encryption key without giving a copy to Microsoft

- ArsTechnica: Microsoft may have your encryption key; here's how to take it back
  - http://arstechnica.com/information-technology/2015/12/microsoft-may-have-your-encryption-key-heres-how-to-take-it-back/

- Cory Doctorow / BoingBoing / Windows 10 covertly sends your disk-encryption keys to Microsoft
  - https://boingboing.net/2015/12/29/windows-10-covertly-sends-your.html
- SlashGear:
  - http://www.slashgear.com/microsoft-backs-up-windows-encryption-keys-to-the-cloud-29420239/

MSFT Defends Windows 10 Policy to Copy Hard Drive Keys

- https://www.infopackets.com/news/9752/ms-defends-windows-10-policy-copy-hard-drive-keys
- Microsoft has confirmed it automatically uploads Windows 10 disk encryption keys to its servers. The company says it was a deliberate decision based on weighing up the worst case scenarios.

Software with the most vulnerabilities in 2015: Mac OS X, iOS, and Flash

- http://venturebeat.com/2015/12/31/software-with-the-most-vulnerabilities-in-2015-mac-os-x-ios-and-flash/
- CVE - Common Vulnerabilities & Exposures / National Vulnerability Database
    - #1 - Mac OSX with 384
    - #2 - iPhone iOS with 375
    - #3 - Flash Player with 314
- ... see the rest of the list ...
- (Way down at the bottom is OpenSSL with only 34... but they were doozies!)

Google patches five critical Android security flaws

- http://www.zdnet.com/article/google-fixes-five-critical-android-flaws-in-monthly-updates/#ftag=RSSbaffb68
- Five of the dozen are rated as "Critical" -- allowing remote code execution -- and, not surprisingly, several are in the troubled "Mediaserver."
- http://source.android.com/security/bulletin/2016-01-01.html
- <quote> The most severe of these issues is a Critical security vulnerability that could enable remote code execution on an affected device through multiple methods such as email, web browsing, and MMS when processing media files.
- We have released a security update to Nexus devices through an over-the-air (OTA) update as part of our Android Security Bulletin Monthly Release process.

RansomeWare moves to JavaScript

- http://www.computerworld.com/article/3018972/security/ransom32-first-of-its-kind-javascript-based-ransomware-spotted-in-the-wild.html
- NW.js (previously known as node-webkit)
- "Build native desktop applications for Windows, Mac OS, or Linux using the latest web technologies"
- Fabian Wosar, a security researcher for Emsisoft, explained that by using NW.js, “Ransom32 could easily be packaged for both Linux and Mac OS X,” even though he has only seen it in a Windows executable (exe) format.
- Although JavaScript in the browser is heavily sandboxed, NW.js allows for much more control and interaction with the underlying operating system, enabling JavaScript to do almost everything ‘normal’ programming languages like C++ or Delphi can do.”

Mark Russinovich's SigCheck v2.3

- v2.4 now in beta... adding a check for non-Microsoft root certs.

Honest Achmed's Root Certificate Request

- https://bugzilla.mozilla.org/show_bug.cgi?id=647959
- **Bug 647959** - Add Honest Achmed's root certificate
- 2011-04-06 02:31 PDT by Honest Achmed

This is a request to add the CA root certificate for Honest Achmed's Used Cars and Certificates. The requested information as per the CA information checklist is as follows:

1. Name
   Honest Achmed's Used Cars and Certificates

2. Website URL
   www.honestachmed.dyndns.org

3. Organizational type
   Individual (Achmed, and possibly his cousin Mustafa, who knows a bit about computers).

4. Primary market / customer base
   Absolutely anyone who'll give us money.

5. Impact to Mozilla Users
   Achmed's business plan is to sell a sufficiently large number of certificates as quickly as possible in order to become too big to fail (see "regulatory capture"), at which point most of the rest of this application will become irrelevant.

Technical information about each root certificate

1. Certificate Name
   Honest Achmed's Used Cars and Certificates

2. Certificate Issuer Field
   Honest Achmed's Used Cars and Certificates

3. Certificate Summary
   The purpose of this certificate is to allow Honest Achmed to sell bucketloads of other certificates and make a lot of money.

15. Requested Trust Bits
   All of them of course. The more trust bits we get, the more certificates we can sell.

16. SSL Validation Type
   All of them. The more types, the more certificates we can sell.

1. CA Hierarchy
   Honest Achmed plans to authorise certificate issuance by at least, but not limited to, his cousin Osman, his uncles Mehmet and Iskender, and possibly his cousin's friend Emin.

Gizmodo: (Leo, show the video on this page)

- Your Smartwatch can determine what you type (with that hand)
- http://gizmodo.com/your-smartwatchs-motion-sensors-can-reveal-everything-y-1750442236
- You can now add smartwatches to the list of potential ways your private data could be leaked. Tony Beltramelli, a Master's students at the IT University of Copenhagen, has shown that even your wearable could be used to compromise your privacy by tracking your every keystroke.

  That's not to say that out of the box your fancy new Apple Watch will leak your every last secret to hackers. What Beltramelli has been able to demonstrate through his Master's thesis project is that the seemingly random motions tracked by a smartwatch's motion sensors can be analyzed and used to extract what the wearer might be typing, or inputting on a numerical keypad.

- Other hacks:
  - Lipreading through a window.
  - Lifting a fingerprint from a glass and reusing it for access.
  - Power consumption of a chip when decrypting information.
  - Smartphone lying near a keyboard.
  - Taking a high-res photo of a metal door key.

Wi-Fi Alliance introduces "HaLow" -- low power, long range WiFi for IoT

- http://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-low-power-long-range-wi-fi-halow
- IEEE 802.11ah
  - Sub 1 GHz (900 MHz) license-exempt bands.
  - Provides extended range, lower energy consumption, Wi-Fi networks.
  - Supports large groups of stations or sensors sharing a signal - IoT.
  - Competitive with Bluetooth in power consumption but with larger coverage
- COMPLETELY different network topography
  - Contention minimization.
  - Inter-node relaying to create mesh networks.
  - Lower power with predefined waking and dozing.
  - Able to negotiate for higher bandwidth bursting.
  - Antenna segmentation and Radio beam synthesizing.
  - Built upon the 802.11a/g specification, down sampled to provide 26 channels of 100 kbit/s throughput.
  - Can cover a radius of 1 kilometer.
  - Intended to provide connectivity to thousands of devices under a single access point.

IPv6 is now 20 years old... and the last 5 years have been good ones:

- Now at 10% penetration
- http://arstechnica.com/business/2016/01/ipv6-celebrates-its-20th-birthday-by-reaching-10-percent-deployment/
- http://www.google.com/intl/en/ipv6/statistics.html

GRC dropped SHA-1 and switched to SHA-256

- No drama. No apparent effect. Chrome will now be happy forever.

Miscellany

Leo: "Everyone you know is on Facebook except for a few weird grumpy people."

- During This Week in Google
- Facebook as the messaging platform??
- What we need is a universal inter-platform messaging bridge.

Sci-Fi:

- "Colony" on USA Network - Premiering Jan 14th
    - Post alien invasion of Los Angeles. Collaborators vs resistance.

- I am two episodes behind (3 tonight) on "The Expanse" on SyFy.

The Vitamin D Podcast

- Strongly positive response.
- Many people want more --> once SpinRite is updated.

Twitter following without an account:

- Nick Lozano (@Tridotexe)
  Steve- I was listening to the podcast a few weeks back and heard that some people would like to follow you on twitter but they don't want to create an account. There is an iOS and Android app called Hooks that lets you follow a twitter user and sends you a push notification when the person you select to follow sends a tweet. You then click on the push alert and it opens a web version of twitter right in the app. No account needed. There is also a bunch of other neat things you can do with it. Just thought some other listeners might find the app useful for following you on twitter without having a twitter account. Love the podcast Listen every week.

Something to consider for the New Year --

- A DM'er requesting anonymity sent to me:
  I've been thinking for a long time about giving my LastPass password to a trusted individual (such as a friend). In the event of my death, I'd like for them to be able to access my accounts without having to go through the rigmarole of proving my death to each site. However while I'm still alive I would still like to keep my LastPass account secure. I've been pondering using Shamir's Secret Sharing algorithm and giving parts to 5 different trusted people where 4 of them would be required to successfully recombine my LastPass password. Note I'm presuming my phone would still be intact, so the 2FA part of my LastPass account would be simple to access. What do you think about this proposition?

What are the downsides I'm not seeing? What are upsides of this tactic? Instead of going on this complex route, what might be a simpler way to ensure my LastPass legacy lives on?

- LastPass just releases v4.0
  - Revamps the UI and adds Emergency Recovery feature.

Is the NSA "Law Enforcement" ??

- Hey Steve, just wondering if you consider the NSA to be US law enforcement. I ask because you refer to 'law enforcement' when mentioning the Snowden 'revelations'.

- re: Is NSA law enforcement?
  I agree... I'm using that term loosely to mean "Entities with governmental powers" While the NSA doesn't have "enforcement" powers, it certainly has investigatory powers. So, yeah, I do mean to include them as well.

ArsTechnica / Files on nearly 200 floppy disks belonging to Star Trek creator recovered

- http://arstechnica.com/information-technology/2016/01/files-on-nearly-200-floppy-disks-belonging-to-star-trek-creator-recovered/
- <quote> According to a press release from DriveSavers data recovery, information on nearly 200 floppy disks that belonged to Star Trek creator Gene Roddenberry has been recovered.

  The information on the disks belongs to Roddenberry's estate and has not been disclosed to the general public. DriveSavers notes, however, that Roddenberry used the disks to store his work and "to capture story ideas, write scripts and [take] notes." VentureBeat reports that the disks, containing 160KB of data each, were likely used and written in the '80s.

  The circumstances of the information recovery are particularly interesting, however. Several years after the death of Roddenberry, his estate found the 5.25-inch floppy disks. Although the Star Trek creator originally typed his scripts on typewriters, he later moved his writing to two custom-built computers with custom-made operating systems before purchasing more mainstream computers in advance of his death in 1991.

  The floppy disks were used with the custom computers, but unfortunately one of those computers had been auctioned off and the other one was no longer operational. Roddenberry's estate sent the floppies to DriveSavers, which spent three months writing software that could read the disks in the absence of any documentation or manuals for the custom-built OS.

  The data recovery comes just as Star Trek is entering its 50th anniversary year.

Elaine... above and beyond

- Christy Ramsey (@christyramsey)
  Elaine Farris at edigitaltranscription.com corrected my Hebrew when she transcribed my sermon. The. best. @SGgrc