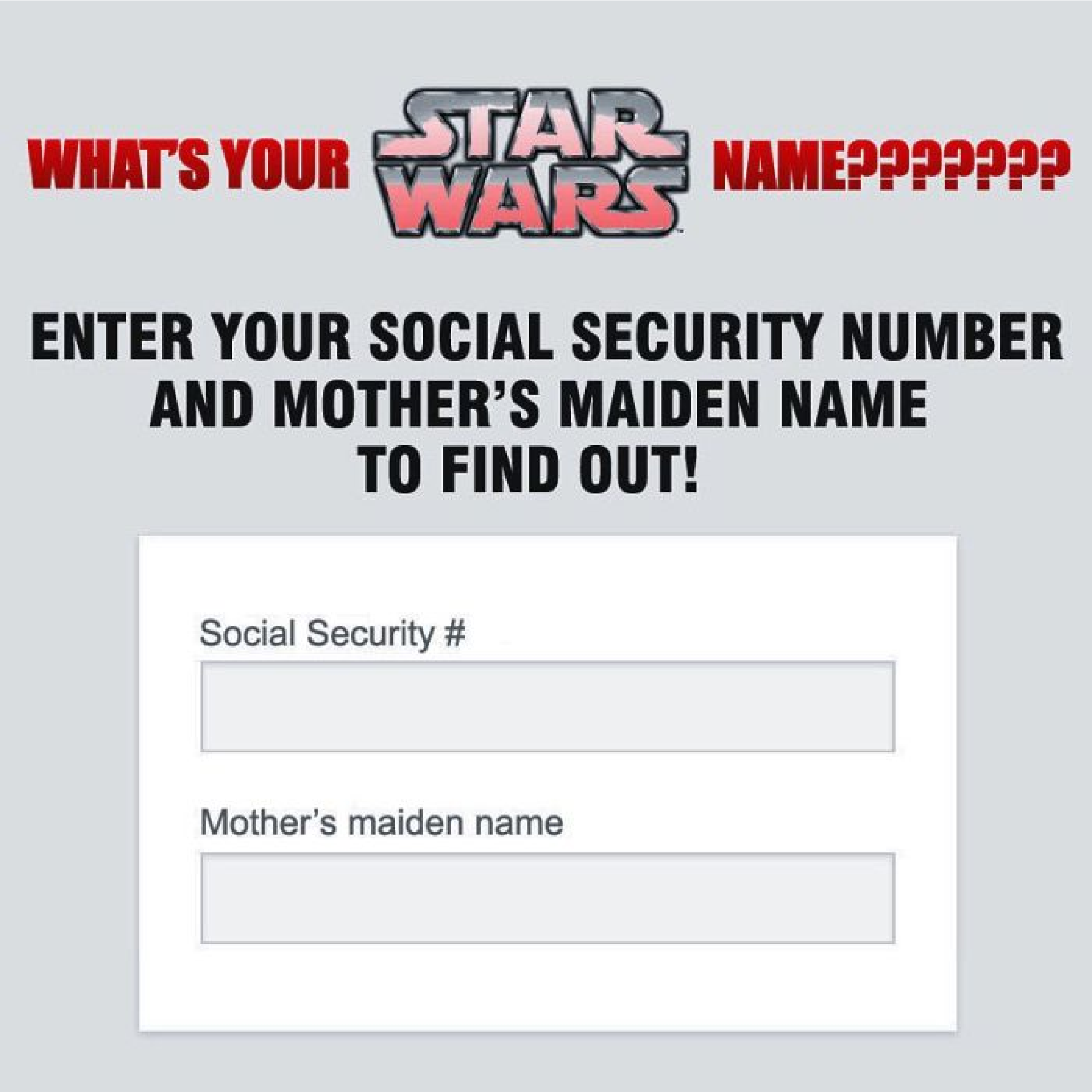
Security Now! #591 - 12-20-16

Law Meets Internet

This week on Security Now!

Russia’s hacking involvement in the US Election; incredibly, it gets even worse for Yahoo!; misguided anti-porn legislation in South Carolina; troubling legislation from Australia; legal confusion from the Florida appellate court; some good news from the U.S. Supreme Court; Linux security stumbling; why Mac OS X got an important fix last week; the Steganography malvertising attack that targets home routers; news of a forthcoming inter-vehicle comms mandate; professional cameras being called upon to provide built-in encryption; LetsEncrypt gets a worrisome extension; additional news, errata, miscellany… and how exactly DOES that “I really really promise I'm not a robot (really!)” non-CAPTCHA checkbox CAPTCHA work?



WHAT'S YOUR STAR WARS NAME???????

ENTER YOUR SOCIAL SECURITY NUMBER AND MOTHER’S MAIDEN NAME TO FIND OUT!

Social Security #

Mother’s maiden name

(Courtesy of P.T. Barnum)

Security News

Russian Election Hacking

Yahoo Says 1 Billion User Accounts Were Hacked more than three years ago, in August of 2013.

- http://mobile.nytimes.com/2016/12/14/technology/yahoo-hack.html

- Fool me once, shame on you. Fool me twice, shame on me.
  - If I refuse to learn from my mistakes... well... who's fault is that?
  - What security-conscious person could possibly still be using Yahoo!?

- 3 months ago, in September, 500 million accounts hacked in 2014.

- Last Wednesday we learned that a year earlier, more than 1 BILLION accounts were compromised.

- This most recently revealed attack disclosed sensitive user information, including names, telephone numbers, dates of birth, hashed passwords and unencrypted password reset security questions.

- Although in September Yahoo declined to require password changes and to reset security questions, it is doing so this time. (Again... how is anyone still there?)

- What to do?
  - Leave Yahoo forever.
  - If you ever reused your Yahoo password, change it everywhere.

- Press coverage:
  - http://mobile.nytimes.com/2016/12/14/technology/yahoo-hack.html
  - https://yahoo.tumblr.com/post/154479236569/important-security-information-for-yahoo-users
  - https://www.bloomberg.com/news/articles/2016-12-15/stolen-yahoo-data-includes-government-employee-information
  - http://www.theregister.co.uk/2016/12/14/one_billion_yahoo_accounts_stolen/

[Misguided] South Carolina legislation proposes to block computers purchased in S.C. from accessing porn.

- South Carolina state representative Bill Chumley has filed a bill to require computer sellers to install digital blocking capabilities on computers and other devices that access the internet to prevent the viewing of obscene content.

- The proposal also would prohibit access to any online hub that facilities prostitution and would require manufacturers or sellers to block any websites that facilitate trafficking.

- Both sellers and buyers could get around the limitation, for a fee:
    - The bill would fine manufacturers that sell a device without the blocking system, but they could opt out by paying $20 per device sold.
    - Buyers could also verify their age and pay $20 to remove the filter.

- The money collected would go toward the Attorney General Office’s human trafficking task force.

- Chumley’s bill has been referred to the House Judiciary Committee.

- The weird "Adults may pay $20 and have the filter removed" gives the legislation more the character of a fund-raising extortion racket for the human trafficking task force.

Meanwhile, an Australian court ruled last week that The Pirate Bay and other sites must be blocked by local Internet providers.

- Thursday, December 15th, 2016:
- http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2016/2016fca1503

- The measures have not yet been implemented, but many Internet users are arranging to find ways around them. Data from Google shows a big surge in "VPN" searches, and VPN services also report a significant increase in Aussie interest.

- Justice John Nicholas of the Australian Federal Court has ordered Australian ISPs to block The Pirate Bay, Torrentz, TorrentHound, IsoHunt, SolarMovie, plus many proxy and mirror services in a move that marks the start of mass-Internet censorship Down Under.

- Following a case brought by Roadshow Films, Foxtel, Disney, Paramount, Columbia, and 20th Century Fox, more than fifty ISPs are now required to start barring subscriber access to ‘pirate’ sites.

- In an order handed down a few hours ago, Justice John Nicholas of the Federal Court ruled that The Pirate Bay, Torrentz, TorrentHound, IsoHunt and streaming service SolarMovie will all have to be rendered inaccessible to consumers in Australia. And this also applies to dozens of affiliated and non-affiliated proxy and mirror sites.

- Even though Torrentz, TorrentHound, and Solarmovie have all shut down since the beginning of the legal action, the judgement stated that since they could resurface in the future, they needed to be preemptively blocked anyway.

- Australian ISPs have just 15 days to come into compliance with the order.

- ISPs were given latitude about how to block, including blocking DNS, IP addresses, URL blocking or "any alternative means approved by the coalition of copyright holders."

- The requirement included notifying users about what is happening... so web browsers will be redirected either to an ISP explanation or to a copyright holder's page.

- ISPs must bear the brunt of the cost for blocking, but copyright holders collectively pay $50 per blocked domain.

- When copyright holders spot domains, URLs or IP addresses that facilitate access to blocked sites, a streamlined process has been pre-defined to facilitate fast action: They must merely file an affidavit with the Court stating which locations the sites are attempting to operate from. The ISPs listed in the original court order will be required to block these new additions within 15 days.

Florida Court Denies Protection for iPhone Passcode

- Last Tuesday (December 2nd, 2016) a Florida appeals court ruled, in a case of a man suspected of voyeurism, that police may lawfully compel the disclosure of a mobile device's passcode for the purpose of searching it for incriminating evidence.

- Here's some context:
  Aaron Stahl was arrested after a woman who was shopping in a store saw him crouch down and extend an illuminated cellphone under her skirt, according to court records.

  When she confronted him, Stahl told her he had dropped his phone. He ran out of the store when she yelled for help, but police were able to identify him using his car’s license plate number. He was later arrested for third-degree voyeurism.

  In a police interview, Stahl initially gave verbal consent to a search of his cellphone, an Apple iPhone 5, but withdrew his consent before telling police his four-digit passcode.

  Once police obtained a warrant for the phone, they were still unable to access the photos on the phone.

- (Okay… so the guy’s a creep. No one’s suggesting otherwise.)

- At trial, the judge denied the state’s motion to compel Stahl to give up his passcode, finding that it would be tantamount to forcing him to testify against himself in violation of the Fifth Amendment.

- Tortured Logic:
  But subsequently the Florida Court of Appeal’s Second District reversed that decision, Wednesday, finding that the passcode is not related to any criminal photos or videos found on the phone.

  Judge Anthony Black, writing for the three-judge panel: “Providing the passcode does not ‘betray any knowledge [Stahl] may have about the circumstances of the offenses’ for which he is charged. Thus, ‘compelling a suspect to make a nonfactual statement that facilitates the production of evidence’ for which the state has otherwise obtained a warrant based upon evidence independent of the accused’s statements linking the accused to the crime does not offend the privilege.”

- In other words... they assert that a passcode is not testimonial... it is, instead, "surrender."

- In the U.S. Supreme Court's 1988 Doe v. U.S. decision, Justice John Paul Stevens wrote a much-repeated line, saying that an accused person may be "forced to surrender a key to a strongbox containing incriminating documents," but cannot "be compelled to reveal the combination to his wall safe."

- The trial judge similarly found that Stahl could not be forced to use the "contents of his mind" to unlock the phone.

- The appeals court, however, questioned this reasoning, which would grant protections for cellphone users that use a passcode, but not for those who use a fingerprint to unlock their phone.

  "We question whether identifying the key which will open the strongbox – such that the key is surrendered – is, in fact, distinct from telling an officer the combination," Black said. "More importantly, we question the continuing viability of any distinction as technology advances."

- Black concluded, "Unquestionably, the State established, with reasonable particularity, its knowledge of the existence of the passcode, Stahl's control or possession of the passcode, and the self-authenticating nature of the passcode. This is a case of surrender and not testimony."

- Links:
  - http://courthousenews.com/florida-court-denies-protection-for-iphone-passcode/
  - https://consumerist.com/2016/12/13/court-rules-that-police-can-force-you-to-tell-them-your-phones-passcode/
  - http://appleinsider.com/articles/16/12/15/florida-appeals-court-orders-man-to-surrender-iphone-passcode

U.S. Supreme Court Agrees to Hear Case that Could End Texas' Grip on Patent Cases

- https://www.eff.org/deeplinks/2016/12/supreme-court-agrees-hear-case-could-end-texas-grip-patent-cases

- In the case TC Heartland v. Kraft Foods, the case effectively asks the court to decide whether patent owners can sue in practically any corner of the country.

  The EFF supported TC Heartland, the petitioner, at the Court of Appeals for the Federal Circuit and as well in asking the Supreme Court to hear the case. The petition to the Supreme Court became necessary after the Federal Circuit issued a disappointing decision that maintained the status quo.

  The current law allows patent owners to pick and choose between federal courts, often opting for courts that are perceived to have rules and procedures favorable to their position. The result [writes the EFF] has been astounding: Last year, almost 45% of all cases were filed in the Eastern District of Texas, a rural part of the country that has no major technology industry.

When patent owners can drag defendants into court in far-flung corners of the country it can cause significant harm, especially for those who are on the receiving end of a frivolous lawsuit. Patent owners can pick a forum that is less inclined to grant fees, keep costs down, or stay cases. As a result, oftentimes it is cheaper to settle even a frivolous case than to fight.

EFF Writes: "We’re glad to see that the Supreme Court has agreed to hear this important case that could significantly curtail some of the worst actors in the patent game. EFF will be there to urge the Court to restore balance and fairness in patent litigation."

Linux in the crosshairs: Multiple (many) 0-day remote execution flaws are surfacing.

- We're up to four Linux desktop vulnerabilities in recent weeks, three from security researcher Chris Evans who has been having too much fun with the widely used GStreamer media library.

- Back in mid November (15th), Chris posted to his "Scarybeasts" blob:
  - https://scarybeastsecurity.blogspot.com/2016/11/0day-poc-risky-design-decisions-in.html
  - [0day] [PoC] "Risky design decisions in Google Chrome and Fedora desktop enable drive-by downloads"

  - Overview
    A confluence of two risky design choices, combined with various implementation issues, makes drive-by downloads possible with Google Chrome on Fedora.

    - Chrome will auto download files to a user’s desktop with no confirmation.
    - Fedora’s “tracker” software will auto crawl downloaded files to index them, including media files.
    - The “gstreamer” framework, as used to handle media in the Fedora desktop, has questionable implementation quality from a security perspective.
    - The “tracker” component responsible for parsing media files does not appear to be sandboxed (e.g. with SELinux).
    - The Fedora default desktop install includes a range of fairly obscure media decoders that confer risk but are not necessary for a thorough desktop experience.
      (Which is a very polite way of saying that there's a bunch of crap in there, installed by default, that few, if any, people will need, but which expands the attack surface needlessly.)

- About a week later (21st) Chris published another found and exploited another problem in GStreamer which is also able to bypass the ASLR and DEP (NX) protections.
  - https://scarybeastsecurity.blogspot.com/2016/11/0day-exploit-advancing-exploitation.html
  - [0day] [exploit] Advancing exploitation: a scriptless 0day exploit against Linux desktops

    - Overview
      A powerful heap corruption vulnerability exists in the gstreamer decoder for the FLIC file format.

      Presented here, is an 0day exploit for this vulnerability.

      This decoder is generally present in the default install of modern Linux desktops, including Ubuntu 16.04 and Fedora 24. Gstreamer classifies its decoders as “good”, “bad” or “ugly”. Despite being quite buggy, and not being a format at all necessary on a modern desktop, the FLIC decoder is classified as “good”, almost guaranteeing its presence in default Linux installs.

      Thanks to solid ASLR / DEP protections on the (some) modern 64-bit Linux installs, and some other challenges, this vulnerability is a real beast to exploit.

      Most modern exploits defeat protections such as ASLR and DEP by using some form of scripting to manipulate the environment and make dynamic decisions and calculations to move the exploit forward. In a browser, that script is JavaScript (or ActionScript etc.) When attacking a kernel from userspace, the “script” is the userspace program. When attacking a TCP stack remotely, the “script” is the program running on the attacker’s computer. In my previous full gstreamer exploit against the NSF decoder, the script was an embedded 6502 machine code program.

      But in order to attack the FLIC decoder, there simply isn’t any scripting opportunity. The attacker gets, once, to submit a bunch of scriptless bytes into the decoder, and try and gain code execution without further interaction…

      … and good luck with that! Welcome to the world of scriptless exploitation in an ASLR environment. Let’s give it our best shot.

- And most recently, last Tuesday, December 13th, Chris posted:
    - http://scarybeastsecurity.blogspot.com/2016/12/redux-compromising-linux-using-snes.html
    - TL;DR: full reliable 0day drive-by exploit against Fedora 25 + Google Chrome, by breaking out of Super Nintendo Entertainment System emulation via cascading side effects from a subtle and interesting emulation error. Very full details follow.

- I mentioned FOUR vulnerabilities…
  Another researcher (who knows Chris) recently posted:
    - "Reliably compromising Ubuntu desktops by attacking the crash reporter"
    - https://donncha.is/2016/12/compromising-ubuntu-desktop/
    - In this post I’ll describe how I found a remote code execution bug in Ubuntu Desktop which affects all default installations >= 12.10 (Quantal). The bug allows for reliable code injection when a user simply opens a malicious file. The following video demonstrates the exploit opening the Gnome calculator. The executed payload also replaces the exploit file with a decoy zip file to cover its tracks.

      The full source code for this exploit is available on Github.

This research was inspired by Chris Evan's great work on exploiting client-side file format parsing bugs in the gstreamer media library on Ubuntu. We will look for other default file handlers on Ubuntu which may be vulnerable to exploitation. I'm not a binary exploitation guru like Chris so instead we'll try find bugs which are exploitable without memory corruption.

Apple's Mac OS file encryption could be readily bypassed until last week

- Blog (Thursday, December 15th): "macOS FileVault2 Password Retrieval"
- http://blog.frizk.net/2016/12/filevault-password-retrieval.html
- <quote> macOS FileVault2 let attackers with physical access retrieve the password in clear text by plugging a $300 Thunderbolt device into a locked or sleeping mac. The password may be used to unlock the mac to access everything on it. To secure your mac just update it with the December 2016 patches.

  [Until then] anyone including, but not limited to, your colleagues, the police, the evil maid and the thief will have full access to your data as long as they can gain physical access - unless the mac is completely shut down. If the mac is sleeping it is still vulnerable.

  Just stroll up to a locked mac, plug in the Thunderbolt device, force a reboot (ctrl+cmd+power) and wait for the password to be displayed in less than 30 seconds!

  How is this possible?
  At the very core of this issue there are two separate issues.

  The first issue is that the mac does not protect itself against Direct Memory Access (DMA) attacks before macOS is started. EFI which is running at this early stage enables Thunderbolt allowing malicious devices to read and write memory. At this stage macOS is not yet started. macOS resides on the encrypted disk - which must be unlocked before it can be started. Once macOS is started it will enable DMA protections by default.

  The second issue is that the FileVault password is stored in clear text in memory and that it's not automatically scrubbed from memory once the disk is unlocked. The password is put in multiple memory locations - which all seem to move around between reboots, but within a fixed memory range.

  This makes it easy to just plug in the DMA attack hardware and reboot the mac. Once the mac is rebooted the DMA protections that macOS previously enabled are dropped. The memory contents, including the password, is still there though. There is a time window of a few seconds before the memory containing the password is overwritten with new content.

- The disclosure timeline is as follows:
  - End of July: Issue found.
  - August 5th: PCILeech presented and released at DEF CON 24. (FileVault issue not mentioned).
  - August 15th: Apple notified.

    - August 16th: Apple confirmed issue and asked to hold off disclosure.
    - December 13th: Apple released macOS 10.12.2 which contains the security update. At least for some hardware - like my MacBook Air.

- Conclusion
  The solution Apple decided upon and rolled out is a complete one. At least to the extent that I have been able to confirm. It is no longer possible to access memory prior to macOS boot. The mac is now one of the most secure platforms with regards to this specific attack vector.

Home Routers Under Attack via Malvertising on Windows, Android Devices

- https://www.proofpoint.com/us/threat-insight/post/home-routers-under-attack-malvertising-windows-android-devices
- Overview

  Proofpoint researchers have reported frequently this year on the decline in exploit kit (EK) activity. EKs, though, are still vital components of malvertising operations, exposing large numbers of users to malware via malicious ads.

  Since the end of October, we have seen an improved version of the “DNSChanger EK” used in ongoing malvertising campaigns. DNSChanger attacks internet routers via potential victims’ web browsers; the EK does not rely on browser or device vulnerabilities but rather vulnerabilities in the victims' home or small office (SOHO) routers. Most often, DNSChanger works through the Chrome browser on Windows desktops and Android devices. However, once routers are compromised, all users connecting to the router, regardless of their operating system or browser, are vulnerable to attack and further malvertising.

  The router attacks appear to happen in waves that are likely associated with ongoing malvertising campaigns lasting several days. Attack pattern and infection chain similarities led us to conclude that the actor behind these campaigns was also responsible for the “CSRF (Cross-Site Request Forgery) Soho Pharming” operations in the first half of 2015.

  However, we uncovered several improvements in the implementation of these attacks, including:
    - External DNS resolution for internal addresses
    - Steganography to conceal an AES key to decrypt the list of fingerprints / default credentials and local resolutions
    - The layout for the commands sent to attack the targeted routers.
    - The addition of dozens of recent router exploits: There are now 166 fingerprints, some working for several router models, versus 55 fingerprints in 2015. For example, some like the exploit targeting “Comtrend ADSL Router CT-5367/5624" were a few weeks old (September 13, 2016) when the attack began around October 28.
    - When possible (in 36 cases) the exploit kit modifies the network rules to make the administration ports available from external addresses, exposing the router to additional attacks like those perpetrated by the Mirai botnets

- The malvertising chain is now accepting Android devices as well.

Inter-Vehicle communication mandate coming

- NHTSA (National Highway Traffic Safety Administration) has published a Notice of Proposed Rulemaking.
- 392-page PDF: http://www.safercar.gov/v2v/pdf/V2V%20NPRM_Web_Version.pdf
- It mandates vehicle to vehicle (V2V) communication systems in all new cars and trucks. Once the rule is finalized, car makers will have two model years to begin including V2V systems, with some a big of slack to synchronize product cycles. V2V-equipped cars will communicate with each other at short ranges to prevent the kinds of accidents where current advanced driver assistance systems, most of which depend on line of sight, are not effective.

- V2V, and the related vehicle to infrastructure (V2I), relies on the Dedicated Short-range Radio Communication (DSRC) wireless protocol to communicate between devices at ranges of up to 984 feet (300m). Vehicles will send out standardized "basic safety messages" that trigger driver alerts or even emergency avoidance actions to prevent crashes.

- What could possibly go wrong? (Ars coverage writes):
  Recognizing the immense implications of an insecure protocol, the notice asks industry and the public for input on the proposed security specifications and proposes that "vehicles contain “firewalls” between V2V modules and other vehicle modules connected to the data bus to help isolate V2V modules being used as a potential conduit into other vehicle systems." Privacy is also given due attention, and the proposed rule would prevent cars from sending out identifiable data like a vehicle's VIN or a driver's name or address.

Photographers And Filmmakers Call For Encryption To Be Built Into Cameras As Standard

Over 150 filmmakers and photojournalists call on major camera manufacturers to build encryption into their cameras

- https://freedom.press/news/over-150-filmmakers-and-photojournalists-call-major-camera-manufacturers-build-encryption-their-cameras/
- https://www.documentcloud.org/documents/3238288-Camera-Encryption-Letter.html

Last Wednesday, Trevor Timm, Executive director, Freedom of the Press Foundation:

Today, Freedom of the Press Foundation is publishing an open letter to the world’s leading camera manufacturers—including Nikon, Sony, Canon, Olympus, and Fuji—urging them to build encryption into their still photo and video cameras to help protect the filmmakers and photojournalists who use them.

The letter is signed by over 150 documentary filmmakers and photojournalists from around the world, including fifteen Academy Award nominees and winners, such as Laura Poitras, Alex Gibney, Joshua Oppenheimer, and many more.

Documentary filmmakers and photojournalists work in some of the most dangerous parts of the world, often risking their lives to get footage of newsworthy events to the public. They face a variety of threats from border security guards, local police, intelligence agents, terrorists, and criminals when attempting to safely return their footage so that it can be edited and published. These threats are particularly heightened any time a bad actor can seize or steal their camera, and they are left unprotected by the lack of security features that would shield their footage from prying eyes.

The magnitude of this problem is hard to overstate: Filmmakers and photojournalists have their cameras and footage seized at a rate that is literally too high to count. The Committee to Protect Journalists, a leading organization that documents many such incidents, told us:

"Confiscating the cameras of photojournalists is a blatant attempt to silence and intimidate them, yet such attacks are so common that we could not realistically track all these incidents. The unfortunate truth is that photojournalists are regularly targeted and threatened as they seek to document and bear witness, but there is little they can do to protect their equipment and their photos."

Camera manufacturers are behind the times compared to other technology companies. All iPhones and many Android phones come with encryption built into their devices. Communications services like Apple’s iMessage and FaceTime, plus Facebook’s WhatsApp, encrypt texts messages and calls by default. And major operating systems on PCs and Macs give users the ability to encrypt the hard drives on their computers. Yet footage stored on the professional cameras most commonly used today are still left dangerously vulnerable.

Finding the right way to provide encryption in their products will take some research and development from these camera manufacturers, and we welcome having a conversation with Nikon, Sony, Canon and others about how to best move forward on this important initiative. However, we are hopeful they will publicly respond with a commitment to building encryption into their products to protect many of their most vulnerable customers.

"SSL for Free" using the Lets Encrypt ACME server.

- https://www.sslforfree.com/
- How It Works:
  We generate certificates using their ACME server by using domain validation.

  Private Keys are generated in your browser and never transmitted.

  For modern browsers we generate a private key in your browser using the Web Cryptography API and the private key is never transmitted. The private key also gets deleted off your browser after the certificate is generated.

  If your browser does not support the Web Cryptography API then the keys will be generated on our server using the latest version of OpenSSL and outputted over SSL and never stored.

For the best security you are recommended to use a supported browser for client generation. You can also provide your own CSR (Certificate Signing Request) when using manual verification in which case the private key is handled completely on your end.

Introducing WebKay:

- http://webkay.robinlinus.com/
- A demonstration of all the data your browser knows about you.
- All this data can be accessed by any website without asking you for any permission (just as this one has).
- Most of the data points are educated guesses and not considered to be accurate.
- The page has become too popular and exceeded its Google Geolocation API allotment.

The current Google Contributor it is being terminated... maybe to be replaced.

- Email being received:
  Thank you for being a part of Google Contributor, a service that helps readers enjoy fewer ads while funding the sites they love.

  Early next year we are launching a new and improved Contributor -- your input throughout testing has been invaluable! As we build this new service, we will discontinue the current version of Contributor.

  What this means for you

  Starting in mid-January 2017, you will no longer see Contributor ad replacements as you browse the web and you will be unable to access your Contributor account.

  About payments and billing

  You will no longer be billed for the Contributor service starting mid-January 2017, and we will refund your remaining account balance to your credit or debit card on file.

- Google is soliciting eMail addresses for notification of any relaunch of the service:
  https://docs.google.com/forms/d/e/1FAIpQLSfr49AJt5Ky3lXO3DGsrZc5zP6m5PJb-4eGVdU8VY8R_UtBig/viewform

SG-1000 microFirewall pfSense Security Gateway

- https://store.pfsense.org/SG-1000.aspx
- $150

Errata

IPv6 subscribers don't get 64k IPs… they get 64 BITS of IPs!

- In other words, IPv6 has so many bits, that we're back to simply splitting the 128-bit address in half.

- The most significant 64 bits is the "network number", of which there can be 2^64.

- Every IPv6 network has space for 18,446,744,073,709,551,616 IPv6-connected machine addresses.

- https://tools.ietf.org/html/rfc3177

- 1. Introduction
  There have been many discussions between IETF and RIR experts on the topic of IPv6 address allocation policy. This memo addresses the issue of the boundary in between the public and the private topology in the Internet, that is, how much address space should an ISP allocate to homes, small and large enterprises, mobile networks and transient customers.

- 2. Background
  The technical principles that apply to address allocation seek to balance healthy conservation practices and wisdom with a certain ease of access. On one hand, when managing a potentially limited resource, one must conserve wisely to prevent exhaustion within an expected lifetime. On the other hand, the IPv6 address space is in no sense as limited a resource as the IPv4 address space, and unwarranted conservatism acts as a disincentive in a marketplace already dampened by other factors. So from a market development perspective, we would like to see it be very easy for a user or an ISP to obtain as many IPv6 addresses as they really need without a prospect of immediate renumbering or of scaling inefficiencies.

  The IPv6 address, as currently defined, consists of 64 bits of "network number" and 64 bits of "host number". The technical reasons for this are several. The requirements for IPv6 agreed to in 1993 included a plan to be able to address approximately 2^40 networks and 2^50 hosts; the 64/64 split effectively accomplishes this.

- 3. Address Delegation Recommendations
  The IESG and the IAB recommend the allocations for the boundary between the public and the private topology to follow those general rules:

  - /48 in the general case, except for very large subscribers.
  - /64 when it is known that one and only one subnet is needed by design.
  - /128 when it is absolutely known that one and only one device is connecting.

- In particular, we recommend:
  - Home network subscribers, connecting through on-demand or always-on connections should receive a /48.

- ○ Small and large enterprises should receive a /48.
- ○ Very large subscribers could receive a /47 or slightly shorter prefix, or multiple /48's.
- ○ Mobile networks, such as vehicles or mobile phones with an additional network interface (such as bluetooth or 802.11b) should receive a static /64 prefix to allow the connection of multiple devices through one subnet.
- ○ A single PC, with no additional need to subnet, dialing-up from a hotel room may receive its /128 IPv6 address for a PPP style connection as part of a /64 prefix.

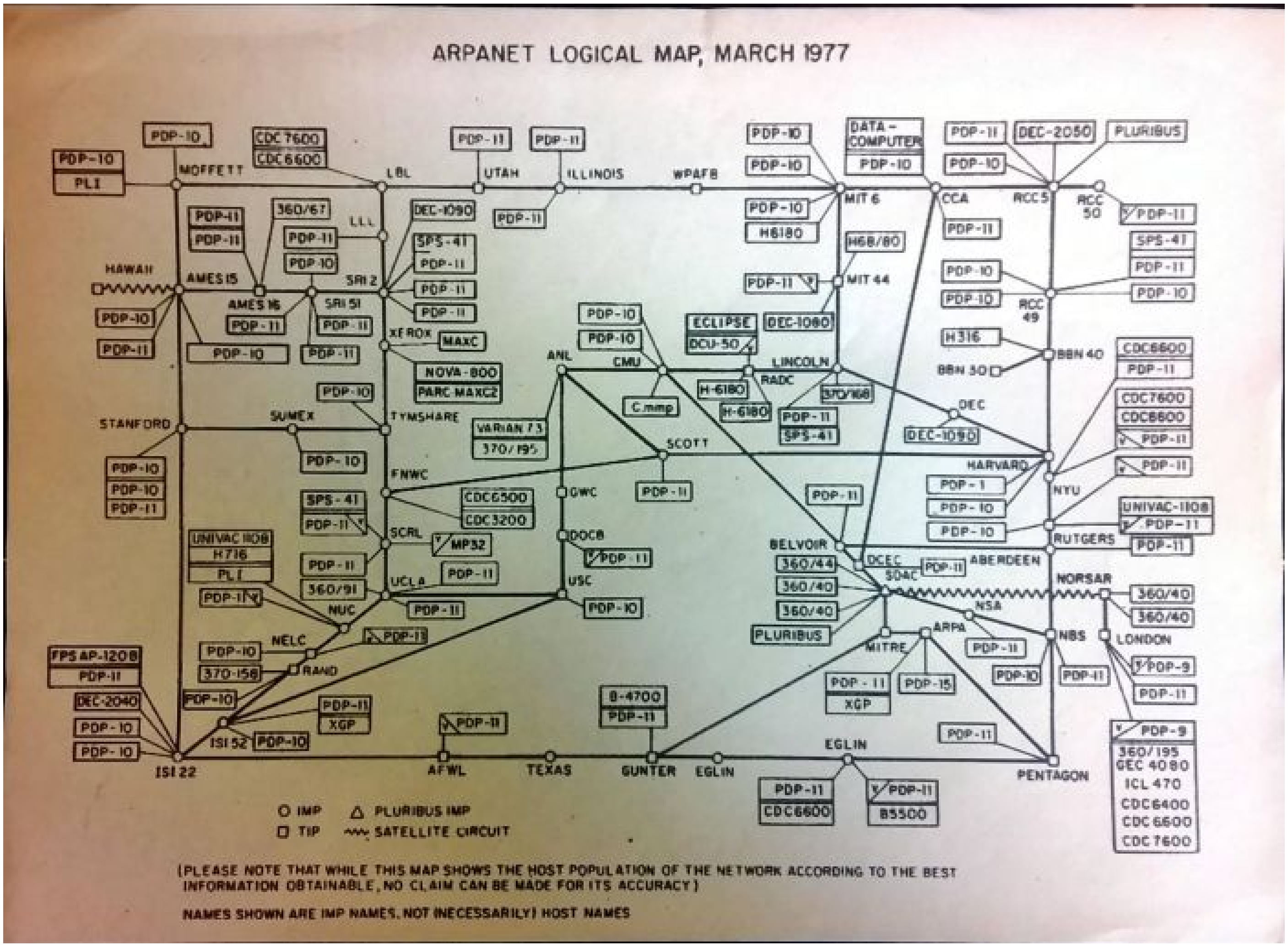
@SGgrc you do realize that decimal 123123 needs 17 binary digits, and won't fit in a TCP port? #sn590

@SGgrc I think you made up "steganometry".

- Steganography comes from "hidden writing".
- Steganometry must be the measurement of hidden things

Miscellany

@SGgrc Hi Steve, Loved the ARPAnet diagram from '73. Here is one from four years later, 1977. Can't remember where I got it from…



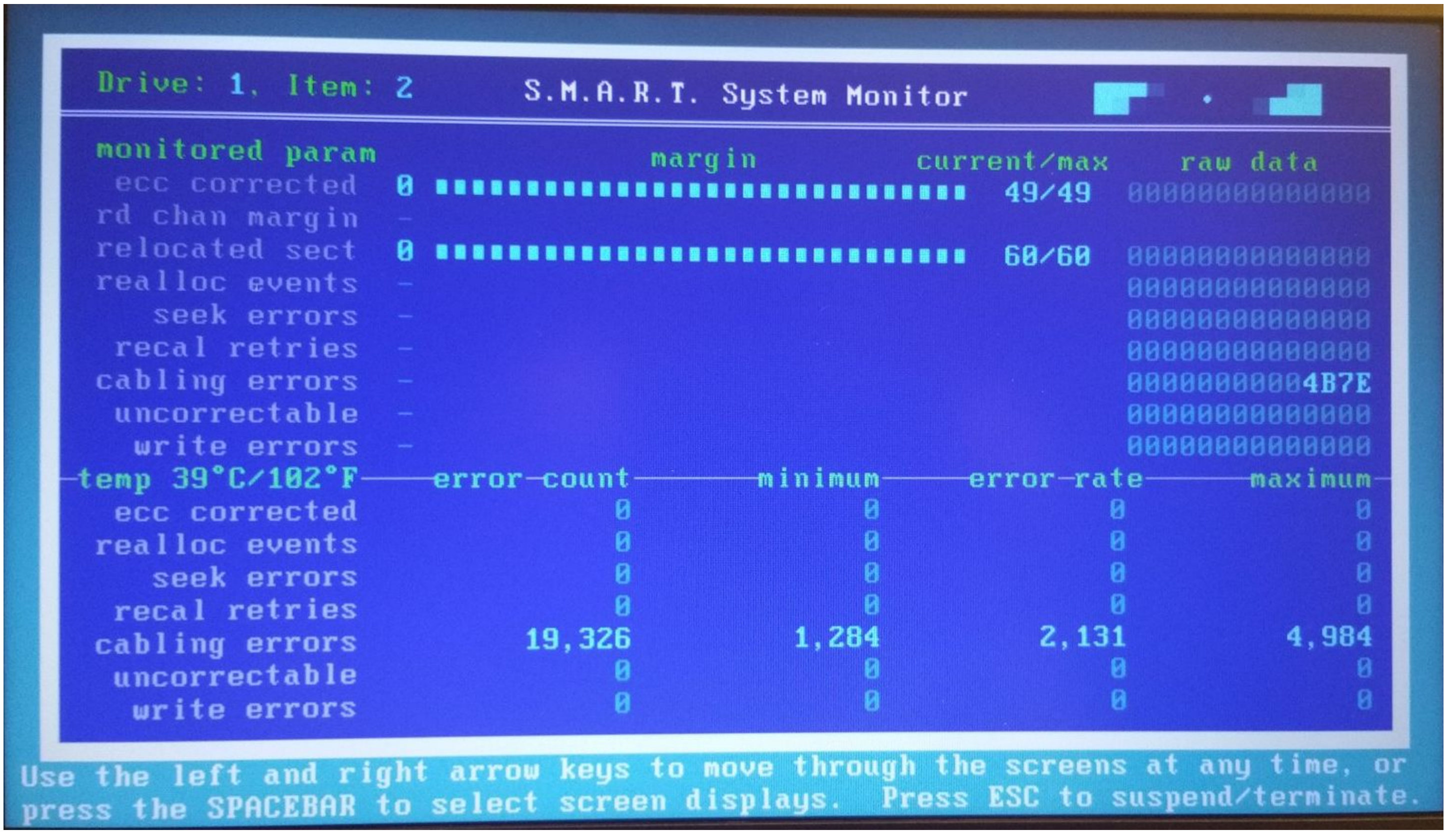
ARPANET LOGICAL MAP, MARCH 1977

(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

SpinRite

SpinRite cabling errors!
https://twitter.com/Keposet/status/810682216820797440/photo/1
Jason (@Keposet) / 12/18/16, 7:04 PM
@SGgrc friend of mine says he's never seen cabling errors before, what's going on here? #spinrite pic.twitter.com/jCdsWYINB5



```
  Drive: 1, Item: 2          S.M.A.R.T. System Monitor

  monitored param              margin         current/max    raw data
    ecc corrected  0 ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■   49/49   00000000000000
  rd chan margin   -
  relocated sect   0 ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■   60/60   00000000000000
  realloc events   -                                          00000000000000
     seek errors   -                                          00000000000000
    recal retries  -                                          00000000000000
  cabling errors   -                                          00000000004B7E
    uncorrectable  -                                          00000000000000
     write errors  -                                          00000000000000
-temp 39°C/102°F---error-count---------minimum-------error-rate--------maximum-
    ecc corrected              0             0              0              0
  realloc events               0             0              0              0
     seek errors               0             0              0              0
    recal retries              0             0              0              0
  cabling errors          19,326         1,284          2,131          4,984
    uncorrectable              0             0              0              0
     write errors              0             0              0              0
Use the left and right arrow keys to move through the screens at any time, or
press the SPACEBAR to select screen displays.  Press ESC to suspend/terminate.
```

I really really promise that I'm not a Robot!

Google Online Security Blog: Are you a robot? Introducing "No CAPTCHA reCAPTCHA"
https://security.googleblog.com/2014/12/are-you-robot-introducing-no-captcha.html

- Google isn’t telling us exactly how they are doing this.
- One investigator believes that incognito mode blocks the easy checkbox mode.
- Another investigator has partically spoofed by using a B-spline mouse path with randomized waypoints and destination.
- The user’s browser must be able to render the canvas.