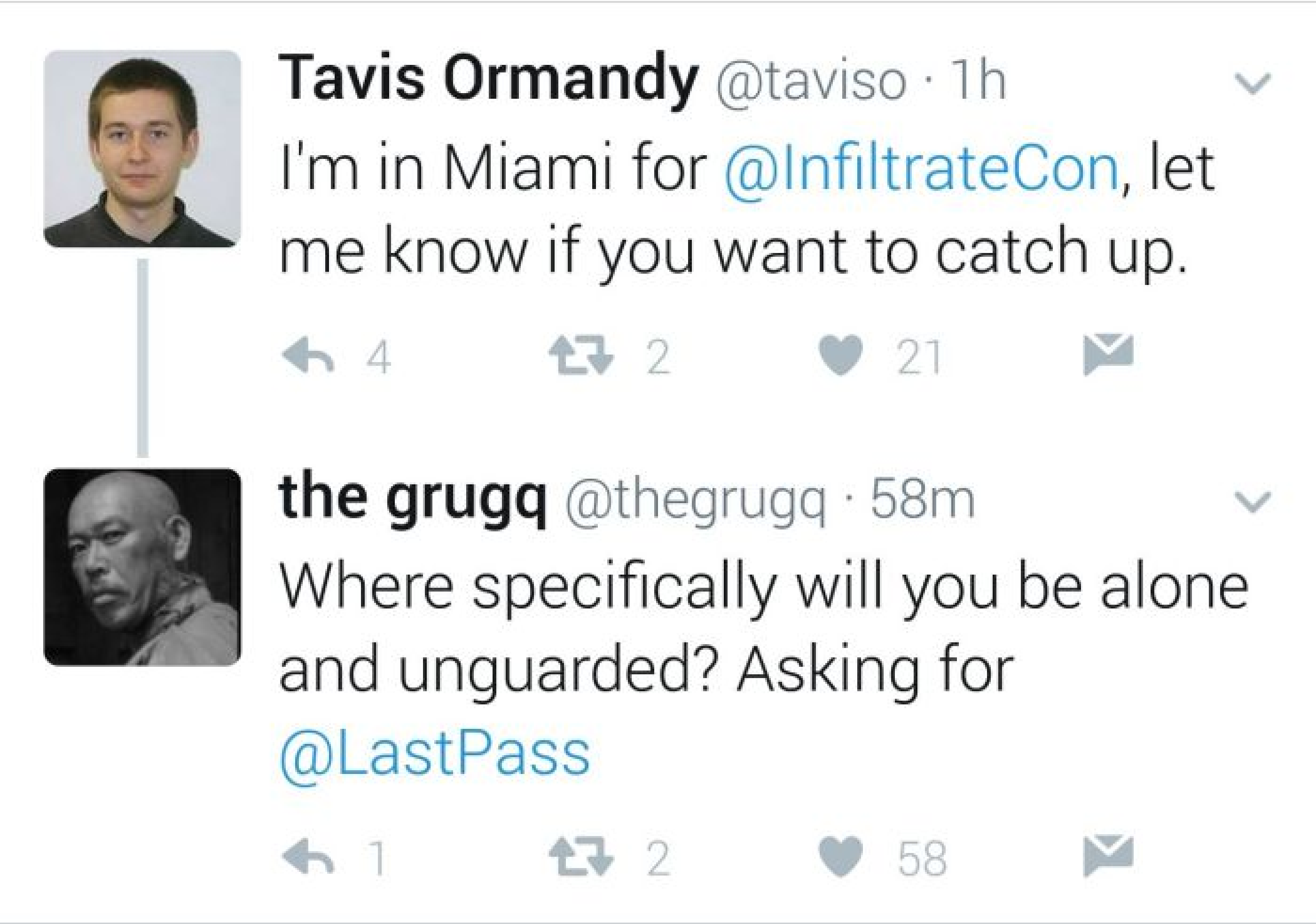
Security Now! #607 - 04-11-17

Proactive Privacy, Really!

This week on Security Now!

This week Steve and Leo discuss Symantec finding 40 past attacks explained by the Vault7 document leaks, an incremental improvement coming to CA certificate issuance, Microsoft patches a 0-day Office vulnerability that was being exploited in the wild, what's a "BricketBot"?, why you need a secure DNS registrar, This Week in IoT Tantrums, a head shaker from our "You really can't make this stuff up" department, the present danger of fake VPN services, an older edition of Windows reaches end-of-patch-life, some "closing the loop" feedback from our listeners, a bit of miscellany, and a comprehensive survey of privacy encroaching technologies and what can be done to limit their grasp.

Our Picture of the Week



Tavis Ormandy @taviso · 1h

I'm in Miami for @InfiltrateCon, let me know if you want to catch up.

4 2 21

the grugq @thegrugq · 58m

Where specifically will you be alone and unguarded? Asking for @LastPass

1 2 58

Security News

Reuters: Symantec attributes 40 cyber attacks to CIA-linked hacking tools

- http://mobile.reuters.com/article/idUSKBN17C1FK
- Symantec has said that past cyber attacks against at least 40 organizations around the world were conducted with top-secret hacking tools that were exposed recently by the Web publisher Wikileaks. Symantec had connected at least 40 attacks in 16 countries to the tools obtained by WikiLeaks, though it followed company policy by not formally blaming the CIA.

CAA checking becomes mandatory for SSL/TLS certificates

- Ivan Ristic (SSL Labs)
  https://blog.qualys.com/ssllabs/2017/03/13/caa-mandated-by-cabrowser-forum

  Certification Authority Authorization (CAA), specified in RFC 6844 in 2013, is a proposal to improve the strength of the PKI ecosystem with a new control to restrict which CAs can issue certificates for a particular domain name. Although CAA had been in the proposed-standard state for more than 4 years, there was little obvious happening until very recently, with only a hundred or two hundred sites adopting it. But that's going to change, because the CA/Browser Forum recently voted to mandate CAA support as part of its certificate issuance standard Baseline Requirements. The changes will become effective in September 2017.

  The fact that any CA can issue a certificate for any domain name is commonly cited as the weakest aspect of the PKI ecosystem. Although CAs want to do the right thing, there are no technical controls that prevent them from doing whatever they choose to do. That's why we say that the PKI ecosystem is as weak as the weakest link. With hundreds of CAs, there are potentially many weak links.

  CAA creates a DNS mechanism that enables domain name owners to whitelist CAs that are allowed to issue certificates for their hostnames.

  It operates via a new DNS resource record (RR) called CAA (type 257). Owners can restrict certificate issuance by specifying zero or more CAs; if a CA is allowed to issue a certificate, their own hostname will be in the DNS record.

- RFC6844 - DNS Certification Authority Authorization (CAA) Resource Record
  - https://tools.ietf.org/html/rfc6844#section-5.2

- nocerts.example.com   CAA 0 issue ";"
  - This CAA record requests that no certificates be issued for the domain 'nocerts.example.com' by any certificate issuer.

- certs.example.com   CAA 0 issue "digicert.com"
  - This CAA record requests that no certificates be issued for the domain 'certs.example.com' by any certificate issuer other than digicert.com.

- More good technical stuff:
    - https://gist.github.com/roycewilliams/1710ade469c05eb0b090d268470aa741

Attacks Detected with New Microsoft Office Zero-Day

Fortunately, today is April's Patch Tuesday and this is being fixed…

The guys at FireEye recently detected malicious Microsoft Office RTF documents leveraging a previously unknown vulnerability. This vulnerability allows a malicious attacker to execute a Visual Basic script when the user opens a document containing an embedded exploit. FireEye found several Office documents exploiting the vulnerability that download and execute malware payloads from different well-known malware families.

- An attacker emails a Microsoft Word document to a targeted user containing an embedded OLE2link object.

- When the user opens the document, winword.exe issues an HTTP request to a remote server to retrieve a malicious .hta (HTML Application) file, which appears as a fake RTF (Rich Text Format) file.

- The Microsoft HTA application loads and executes the malicious script.

- In the observed documents, the malicious script terminated the winword.exe process, downloaded additional payload(s), and loaded a decoy document for the user to see.

- The original winword.exe process is terminated in order to hide a user prompt generated by the OLE2link.

- The vulnerability was successfully bypassing most mitigations.

You can block the Word RCE by setting:

- Software\Microsoft\Office\15.0\Word\Security\FileBlock\RtfFiles to 2 and OpenInProtectedView to 0

Press Coverage:

- https://www.bleepingcomputer.com/news/security/attacks-detected-with-new-microsoft-office-zero-day/
- http://thehackernews.com/2017/04/microsoft-word-zero-day.html
- https://www.helpnetsecurity.com/2017/04/10/ms-office-zero-day/
- https://www.fireeye.com/blog/threat-research/2017/04/acknowledgement_ofa.html
- https://arstechnica.com/security/2017/04/booby-trapped-word-documents-in-the-wild-exploit-critical-microsoft-0day/

“BrickerBot” Results In Permanent Denial-of-Service
https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/

RadWare:
Imagine a fast moving bot attack designed to render the victim’s hardware nonfunctional. Called "Permanent Denial-of-Service" or PDoS, this form of cyber-attack is becoming increasingly popular in 2017 as more incidents involving this hardware-damaging assault occur.

Also known loosely as “phlashing” in some circles, PDoS is an attack that damages a system so badly that it requires replacement or reinstallation of hardware. By exploiting security flaws or misconfigurations, PDoS can destroy the firmware and/or basic functions of a system.

Over a four-day period, Radware’s honeypot recorded 1,895 PDoS attempts performed from several locations around the world. Its sole purpose was to compromise IoT devices and corrupt their storage. Besides this intense, short-lived bot (BrickerBot.1), Radware’s honeypot recorded attempts from a second, very similar bot (BrickerBot.2) which started PDoS attempts on the same date – both bots were discovered less than one hour apart –with lower intensity but more thorough and its location(s) concealed by TOR egress nodes.

The Bricker Bot PDoS attack used Telnet brute force - the same exploit vector used by Mirai - to breach a victim’s devices. Bricker does not try to download a binary, so Radware does not have a complete list of credentials that were used for the brute force attempt, but were able to record that the first attempted username/password pair was consistently 'root'/'vizxv.’ (Dahua brand DVR DH-DVR3104H telnet password?)

Upon successful access to the device, the PDoS bot performed a series of Linux commands that would ultimately lead to corrupted storage, followed by commands to disrupt Internet connectivity, device performance, and the wiping of all files on the device.

The use of the 'busybox' command combined with the MTD and MMC device names demonstrates that this attack is targeted specifically at Linux/BusyBox-based IoT devices with open Telnet ports publically exposed to the Internet. These match the devices targeted by Mirai or related IoT botnets.

The PDoS attempts originated from a limited number of IP addresses spread around the world. All devices are exposing port 22 (SSH) and running an older version of the Dropbear SSH server. Most of the devices were identified by Shodan as Ubiquiti network devices; among them are Access Points and Bridges with beam directivity.

In parallel, Radware’s honeypot recorded over 333 PDoS attempts with a different command signature. The source IP addresses from these attempts are TOR Nodes, so there's no identifying the actual source of the attacks. It's worth noting that these attacks are still ongoing and the attacker/author is using TOR egress nodes to conceal its bot(s). The commands used in these second PDoS attempts are more thorough than the first ones. The targeted storage devices are much broader and there is no use of 'busybox' while attempting both 'dd' and 'cat,’ ... whichever is available on the breached device.

Destruction:

The final commands at the end are identical in both edition of BrickerBot. They attempt to remove the default gateway, wipe the device through rm -rf /* and limit the maximum number of kernel threads to one. The iptables firewall and NAT rules are flushed and a rule is added to drop all outgoing packets.

How Hackers Hijacked a Bank's Entire Online Operation

At 1pm on Saturday of October 22nd last year, hackers changed the DNS registration of all 36 of a Brazilian bank's online properties, commandeering the bank's desktop and mobile web domains to take all visitors to their perfectly constructed fake/spoofed site... where the bank's victim customers dutifully handed over all of their account information.

Kaspersky researchers believe the hackers also simultaneously redirected all transactions at ATMs or point-of-sale systems to their own servers, collecting the credit card details of anyone who used their card that Saturday afternoon.

Kaspersky's Dmitry Bestuzhev said "Absolutely all of the bank's online operations were under the attackers' control for five to six hours." They watched malware infecting customers from what appeared to be the bank's fully valid domain.

Kaspersky is not releasing the name of the bank that was targeted in the DNS redirect attack. But the firm says it's a major Brazilian financial company with hundreds of branches, operations in the US and the Cayman Islands, 5 million customers, and more than $27 billion in assets. And though Kaspersky says it doesn't know the full extent of the damage caused by the takeover, it should serve as a warning to banks everywhere to consider how the insecurity of their DNS might enable a nightmarish loss of control of their core digital assets.

Bestuzhev said "This is a known threat to the internet, but we've never seen it exploited in the wild on such a big scale."

Details:
The traffic was redirected to servers the attackers had set up on Google's Cloud Platform.

With that domain hijacking in place, anyone visiting the bank's website URLs were redirected to lookalike sites. And those sites had valid HTTPS certificates issued in the name of the bank, so visitors' browsers would show a green lock and the bank's name, just as they would with the real sites. Kaspersky found that the certificates had been issued six months earlier by ...(wait for it)... Let's Encrypt.

Let's Encrypt founder, Josh Aas, said: "If an entity gained control of DNS, and thus gained effective control over a domain, it may be possible for that entity to get a certificate from us. Such issuance would not constitute mis-issuance on our part, because the entity receiving the certificate would have been able to properly demonstrate control over the domain."

(Note that any other CA would also be fooled to issue a DV cert for a hijacked domain... just not a quickly.)

What would CAA prevent in this instance?

This Week's IoT Tantrum

A Maker of Smart Garage Openers Responded to a Bad Amazon Review by Remotely Disabling the Customer's Device

The customer had left a comment on the support forum complaining about technical issues, "Wondering what kind of piece of [crap] I just purchased here." They then followed it up with a negative Amazon review, saying: "Junk - DO NOT WASTE YOUR MONEY - iPhone app is a piece of junk, crashes constantly, start-up company that obviously has not performed proper quality assurance tests on their products."

Garadget did not like that one bit.

The company disabled the disgruntled customer's device by denying it access to its servers—and announced it had done as such on its forum:

> Martin,
>
> The abusive language here and in your negative Amazon review, submitted minutes after experiencing a technical difficulty, only demonstrates your poor impulse control. I'm happy to provide the technical support to the customers on my Saturday night but I'm not going to tolerate any tantrums.
>
> At this time your only option is return Garadget to Amazon for refund. Your unit ID 2f0036... will be denied server connection.

Garadget defended itself in a subsequent post, saying it took action to "distance from the toxic individual":

> Ok, calm down everybody. Save your pitchforks and torches for your elected representatives. This only lacks the death threats now.
>
> The firing of the customer was never about the Amazon review, just wanted to distance from the toxic individual ASAP. Admittedly not a slickest PR move on my part. Access restored, note taken.

From our "You can't make this stuff up" Department:
“Rensenware” is a new twist on ransomware... Instead of requiring infected users to pay a sum of money to regain access to their locked files, Rensenware requires them to reach a high score of 200 million points in the anime bullet hell shooter known as "TH12 - Undefined Fantastic Object" when played on the “Lunatic” difficulty level.

(In other words, either invite your grandson over, or beg Paul Thurrott to come unlock your machine!)

This was apparently a joke gone wrong. The creator of Rensenware has apologized for the software. “I made it joke, just laughing with people who like Touhou Project Series,” says Tvple Eraser, who also released a tool to bypass the lock on the files for anyone who may have downloaded the original version by mistake. He has also replaced the ransomware version with a safer “cut” version that doesn’t lock your files by forcibly encrypting them.

Phony VPN Services Are Cashing in on America's War on Privacy

Motherboard's Nicholas Deleon wrote-up a terrific 3-part story about fraudsters attempting to cash-in on the new worries over online privacy.

Three article drama:

- https://motherboard.vice.com/en_us/article/phony-vpn-services-are-cashing-in-on-americas-war-on-privacy
- https://motherboard.vice.com/en_us/article/scam-vpn-service-online-privacy-fcc
- https://motherboard.vice.com/en_us/article/mysafevpn-offline-phishing-warning-online-privacy

Over the course of a few days he received several different phishing eMails from "MySafeVPN" with convincing (to anyone else) technical details. But Nicholas smelled a rat... and a story… and he got one. The phishing eMails refered to Plex and Boxee, both whose online forums had been hacked years before and lost their users’ names and email addresses… thus perfect phishing fodder. So Nicholas exchanged eMails, had phone calls, found a physical site thanks to Google street view... and ultimately apparently spooked the crooks into shutting down.

But where will they surface next?

End of Patch-Life for Windows Vista.

- Today's Patch Tuesday marks the first month that Windows Vista will not receive any further updates.
- (Does anyone care?)
  - A troubled OS from (before) the start.
  - WinFS -- aborted.
  - All sorts of fabulous new features -- rolled back.
  - A far far too aggressive and intrusive UAC.
  - Windows 7 inherited many of Vista's innovations, and tempered its over-the-top UAC.

Closing the Loop

ReliefTwitcher (@ReliefTwitcher)
@SGgrc Have had media.autoplay OFF in FF about a year. Found same as you with YouTube and other video sites. Easy solution: Click a tiny bit into the progress bar, then click play. "Autoplay off" is great for sites where you don't want to block ads totally.

Steve & JavaScript

- Rasmus Beck (@1v1MeInTetris)
  Watching SecurityNow episode 606, getting the feeling @SGgrc doesn't quite like Javascript…

- Kyle (@kboyington)
  @SGgrc but tell us how you really feel about Javascript!! Ha

Don't get me wrong... I can think that JavaScript is an abomination, while at the same time understanding why it is so, and managing to write my own beautiful code in JavaScript.

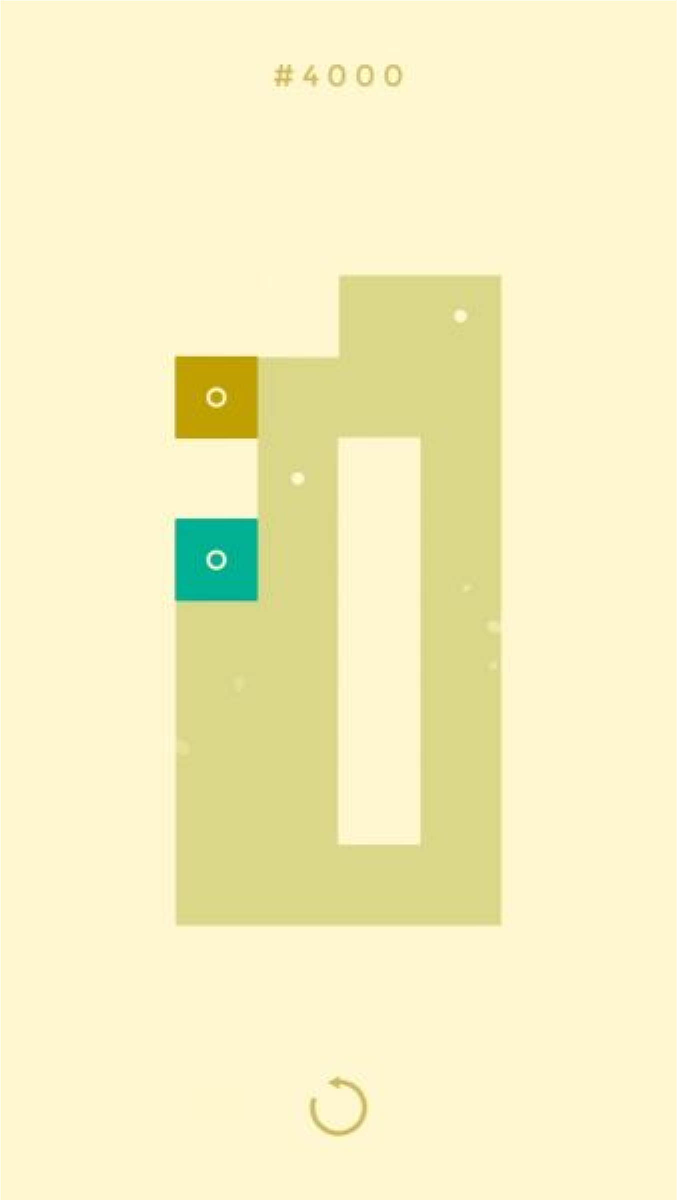
- Password Haystacks:
  https://www.grc.com/haystack.htm (3844 times/day)
- Off The Grid Latin Square Solver
  https://www.grc.com/offthegrid.htm
- UHEPRNG (Ultra High Entropy PRNG)
  https://www.grc.com/otg/uheprng.htm
- Magnetic recording animation
  https://www.grc.com/animation.htm
- Slow and deep breathing pacer
  https://www.grc.com/breathe.htm

Manuel Cheta (@manuelcheta)

- @SGgrc Will these tools actually help against ransomware?
  No More Ransom — 15 New Ransomware Decryption Tools Available for Free
  https://thehackernews.com/2017/04/decrypt-ransomware-files-tool.html

Gengar (@infoSecGengar)

- @SGgrc If I fail school because of this game, can I come work for you?
- Square It!
- http://squareit.io/
  - 500,563 downloads in one month.
  - https://itunes.apple.com/us/app/square-it/id1160380201
  - https://play.google.com/store/apps/details?id=com.infinitygames.squareit



He's on Level 4000!

Michael Surette

- @SGgrc What's up w/ShieldsUp? My open ports 22,25 show as stealth unless I do a comma separated custom probe.

Tom Corwine (@TomCorwine)

1. @SGgrc RE: All this talk about ISPs forcing us to install their own CA cert — how would our IOT devices use secure connections?
2. @SGgrc Come to think of it, those IOT devices don't even need to use a public CA, their manufacturers can mint their own certs.

That's EXACTLY correct. We need the public CA system only so that clients and servers don't need to have any foreknowledge of each other. They BOTH rely upon a mutually known 3rd party. But the IoT model is different. The devices CAN embed a cert for ONLY the manufacturer's servers.

Errata

Whoops!!

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

Miscellany

- Ryk Brown: "The Frontier Saga" - Kindle Unlimited (15-book series)
- http://www.frontierssaga.com/
- Honor Harrington / David Weber
- Tanis Richards / M. D. Cooper (Outsystem: The Intrepid Saga)
- Nathan Scott

This week's Pithy Slogan:

- "When in doubt, encrypt.
  When not in doubt, be in doubt."

SpinRite

From: Brett Parks
Subject: SPINRITE saves the day, yet again.

I've been using SpinRite for, what, 20 years now or more. When all else fails, it will =at least= bring a HD back to where it will at least boot or be readable. And it just did that again with the 1TB HD on my primary machine went belly up, and took my accounting, taxes, email & client lists, yadda yadda yadda along with it.

It took a couple of runs, but SpinRite got it back to where I could get EVERYTHING off it.

Not bad for "old school", eh?

Thanks yet AGAIN!

Brett Parks
Lexington, SC

Podcast listeners who already own SpinRite will have access to the v6.x series when each edition is in stable prerelease.

FIrst priority is to free it from the BIOS and make it run like a bat out of hell -- half a terabyte per hour, but first for the PC platform. That will immediately be followed by Mac support. Then native USB support

Proactive Privacy Roundup

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

The Tracking Hooks:

- The great grandaddy of them all: IP address.
    - These days it's "household granularity"... but much better than nothing.
    - Over time, ISPs will have increasing incentive to keep our (their subscriber's) IPs FIXED specifically for the added value of longer-term tracking and identification. And, sadly, governments might be requesting this, too.

- Browser Cookies
    - First-Party:
        - Originally conceived by Netscape as a means for maintaining "session state" and still used for that today.

- Third-Party
    - A side-effect of 1st-party cookies:
        - Advertisements
        - Web Beacons
        - Tracking Pixels
        - "Like" buttons
        - Google Analytics
    - ... *anything* that a 1st-party page refers to that's "off site" can, by default, plant a tracking cookie on your machine.

- GRC & Cookies: https://www.grc.com/cookies/cookies.htm
    - The tyranny of the default:
      Of the 43,576 unique visitors to GRC last week…
        - 79.21% had 3rd-party cookies enabled.
        - But among Safari users, only 18.83% had 3rd-party cookies enabled.
        - Apple's Safari is alone in the industry in disabling 3rd-party cookies by default.

    - Five years ago, Google agreed to pay a $22.5 million civil penalty after FTC caught them deliberately using JavaScript to leverage a small flaw in Safari's Iframe handling to place tracking cookies on Safari browsers.

    - A discussion among developers who are being thwarted by Safari:
      Safari 3rd party cookie iframe trick no longer working?
    - http://stackoverflow.com/questions/9930671/safari-3rd-party-cookie-iframe-trick-no-longer-working

    - https://www.grc.com/cookies
    - https://www.grc.com/cookies/forensics.htm

- Firefox hides the 3rd-party cookie setting
    - Tools / Options / Privacy
        - History: Use custom settings for history
        - Accept cookies from sites:
            - Accept third-party cookies: Never.

- Even today problems remain:
    - https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2015/january/analysis-of-setting-cookies-for-third-party-websites-in-different-browsers/
    - tl;dr
      This post discusses the results from our research into the ability of third party websites setting cookies for first party websites across different web browsers. The ability to set cookies in this manner not only facilitates tracking but also opens up other opportunities and avenues of attack.

- However…
    - HTTP Redirection chains, which are becoming much more prevalent, thwart 3rd-party blocking by allowing 1st-party queries.

    - Allied partners can pass identity linkage data via GET parameters.

- Plug-ins have historically violated and/or been readily exploitable.
    - "Flash Cookies" were a thing for a long time.

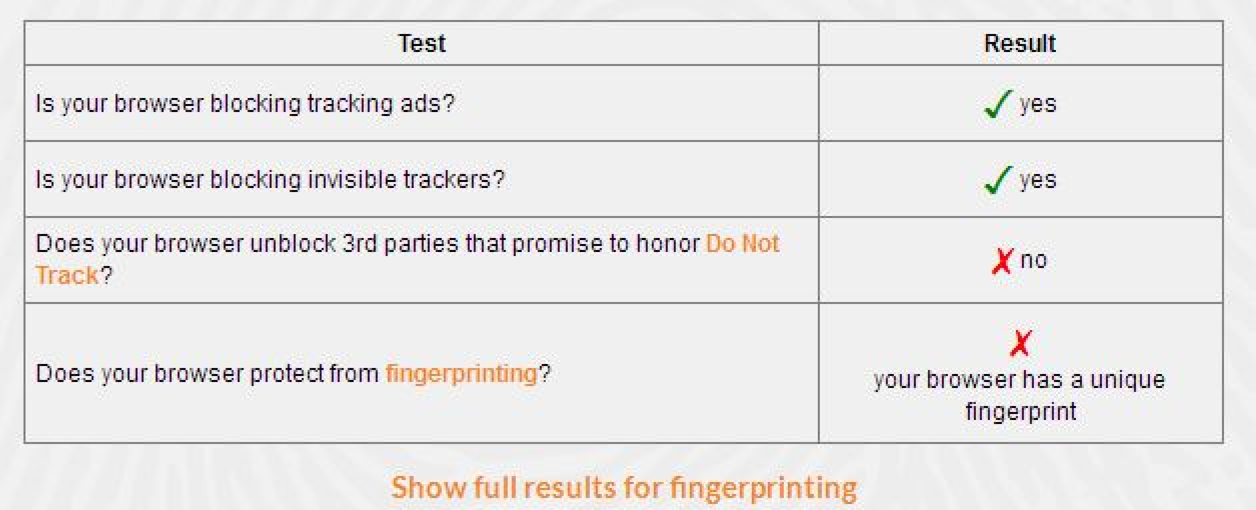
User-Agent header with high-res version numbers.

- Show Browser Query Headers:
    - https://pgl.yoyo.org/http/browser-headers.php
    - The infamous EarthLink Custom Browser Token
    - March 17th, 2001... sixteen years ago!
    - https://www.grc.com/su/earthlink.htm
    - ELNSB50::0000811505000400029802c3000000000505000b00000000

Metadata (or side-effects)

- DNS queries (OSes DO cache them)
- NO native encryption
- Even if ISP DNS is not used, the traffic still passes by.
    - DNSCrypt: https://dnscrypt.org/
    - Multiplatform: Windows, MacOS, Linux, Android, iOS, Routers
    - Server and Clients are open source
    - Many available public resolvers around the world.

- Browser Fingerprinting.
    - Panopticlick
    - https://panopticlick.eff.org/results?



Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✓ yes
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no
Does your browser protect from fingerprinting?	✗ your browser has a unique fingerprint

Show full results for fingerprinting

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
  - Through collusion with their client, they, too, know you.

The power of the "incognito" browsing modes.

- History wipe
- Cookie Wipe

The need to use a 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
    - The Crypto is rock solid and bulletproof.
    - Using OpenVPN, an account can be setup with a client certificate that, from a brute force attack standpoint, eliminates the need for a password since a 256-bit certificate is going to be as strong as any non-pure-entropy password when hashed. And MUCH stronger than any non-pure-entropy password.
    - The best solution for protecting traffic from the "local" internet carrier:
        - Your ISP, Hotel, Cafe, Airport, etc.
    - So this nicely prevents local eavesdropping.

- The bad news
    - ... VPNs don't proactively do anything more than that.
    - Traffic concentrated at VPN "exit nodes" (VPN server sites).
    - Some VPNs only tunnel specific protocols, such as HTTP and HTTPS... so they might be leaking DNS which runs outside of the tunnel.

- How to choose a VPN provider:
    - Should be using OpenVPN system
    - Should have a large range of VPN endpoints for geographical dispersion and increased interception.

- (Sonic Net offers a free, OpenVPN-based VPN to all sonic connectivity customers.)

VPNs:

- https://danielmiessler.com/blog/vpn-recommendations/#gs.uB=MLxc
- Mullvad: OpenVPN-based, out of Sweden.
- Zipline: This is an IPSEC, hardware-based VPN run by a buddy of mine, Dan Tentler.
- IVPN: OpenVPN-based, lots of configuration options, including multi-hop.
- AzireVPN: Another solid OpenVPN-based solution, also with significant configuration options.
- OVPN.se: Yet another solid and highly-rated OpenVPN-based solution.
- SoftEther.org
- https://thatoneprivacysite.net/vpn-comparison-chart/
- https://blog.trailofbits.com/2016/12/12/meet-algo-the-vpn-that-works/
- https://thebestvpn.com/resources/

The power of TOR

- The concern about Exit Node Surveillance.
- Since TOR is frequently used by those wish to actively hide themselves, it's of much greater interest to those who like to monitor and watch others.
- And it doesn't do anything, itself, proactively about privacy.
- The TOR browser -- made from Firefox -- has tweaks to mildly enhance privacy, but nothing very special: NoScript, HTTPS-Everywhere, some default settings changed.

Another bogus "Filter" router on IndieGoGo

- https://www.indiegogo.com/projects/flter-privacy-security-router-technology#/
- Oversells what it can actually do, due to prevalent HTTPS.

Strategies and Tactics for Maximize your Online Privacy

- Due to the tremendous pressure to track and profile, and the massive amounts of money behind that, we should assume that everything that CAN be done to track and profile IS being done.

- (When not in doubt, be in doubt.)

- You MUST change your public IP. Either:
    - Go to another location,
    - Shutdown your cable modem long enough to obtain a new IP or "renew DHCP lease" if available,
    - Or use a VPN.

- You MUST use incognito mode.

- You COULD wipe and freshly setup an Ubuntu Linux system on a retired laptop for browsing via VPN.

- You SHOULD change your browser vendor.

- You SHOULD always encrypt your DNS with DNSCrypt.