Security Now! #520 - 08-11-15

The Quest for Surfing Safety

This week on Security Now!

- StageFright Android Exploit Update
- Windows 10 Privacy Watch
- Was TrueCrypt Cracked?
- Need to Update Firefox
- How bad is "The Memory Sinkhole"?
- Nice "PushBullet" addition
- Oracle bizarreness
- EFF releases v1.0 of a privacy-enforcing plug-in.
- Miscellany
- And... where my quest for safe surfing is taking me...

Security News

StageFright Watch

- https://blog.zimperium.com/zha-zimperiums-initiative-to-fill-the-gaps-in-android-security/
- Wormable!
- Zimperium **were** planning to release their exploit test/demo no later than 2 weeks from now, Monday, August 24th.
    - https://blog.zimperium.com/stagefright-vulnerability-details-stagefright-detector-tool-released/
- ZIP containing Proof-Of-Concept MP4 files:
    - https://s3.amazonaws.com/zhafiles/Zimperium-Handset-Alliance/ZHA-Crash-PoC.zip
    - How the Stagefright bug changed Android security
- Google's latest security problem might actually make Android safer
    - http://www.theverge.com/2015/8/5/9099627/google-stagefright-android-vulnerability-protect-patch
- StageFright Detection:
    - Zimperium:
        - https://play.google.com/store/apps/details?id=com.zimperium.stagefrightdetector
    - Lookout Mobile Security:
        - https://play.google.com/store/apps/details?id=com.lookout.stagefrightdetector

Windows 10 Tracking Update

- Want Windows 10 to stop tracking you? Now there's an app for that
  The open-source app is available to download for free.
- http://www.zdnet.com/article/want-to-limit-windows-10-tracking-there-is-an-app-for-that/
- Github: Windows Tracking Disable Tool
  - https://github.com/10se1ucgo/DisableWinTracking/releases
  - Now at v1.5 -- evolving and being fine-tuned
- The application makes certain changes including:
  - Disables Telemetry services:
    - Set the AllowTelemetry string in HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection to 0
  - Delete or Disable tracking services: (Remove the services, or set to Disable)
    - DiagTrack Diagnostics Tracking Service
    - dmwappushsvc WAP Push Message Routing Service
  - Disabling logging that is enabled by certain trackers after clearing it.
    - Clears and disables writing to the log located in C:\ProgramData\Microsoft\Diagnosis\ETLLogs\AutoLogger
  - Blocking tracking servers by editing the host file.
    - Append known tracking domains to the HOSTS file located in C:\Windows\System32\drivers\etc
- Written in Python:
- Either run the EXE which includes a Python runtime bound into the executable -or-
- If you have Python installed, run the Python script.

Very nice Windows 10 Lockdown guide

- VERY nice Windows 10 lockdown guide:
- https://fix10.isleaked.com/
- Is Leaked are the people who check for leaked eMail addresses.

TrueCrypt Cracked?

- Wait, what? TrueCrypt 'decrypted' by FBI to nab doc-stealing sysadmin
- Do the Feds know something we don't about crypto-tool? Or did bloke squeal his password?
- http://www.theregister.co.uk/2015/08/04/truecrypt_decrypted_by_fbi/
- <quote> Discontinued on-the-fly disk encryption utility TrueCrypt was unable to keep out the FBI in the case of a US government techie who stole copies of classified military documents. How the Feds broke into the IT bod's encrypted TrueCrypt partition isn't clear.
  It raises questions about the somewhat sinister situation surrounding the software team's sudden decision to stop working on the popular project last May.
- Note that not **one** other news outlet mentioned this “story”.

Firefox Vulnerability -- v39.0.3 ==> v40.

- Security researcher Cody Crews discovered that a malicious advertisement on a Russian news site was exploiting a vulnerability in Firefox's PDF Viewer to search for sensitive files on users' local file systems.
- The vulnerability does not enable the execution of arbitrary code, but the exploit was able to inject a JavaScript payload into the local file context. This allowed it to search for and upload potentially sensitive local files.
- Files search for are: subversion, s3browser, Filezilla, and libpurple configuration files on Windows systems; whereas on Linux, the payload looks through global configuration files in /etc/ as well as .bash_history, .mysql_history, .pgsql_history, .ssh files, any text files with "pass" and "access" in the names, and any shell scripts.
- Initially only Windows and Linux were the only targets. Now a variant is searching Macs similarly.
- The exploit leaves no trace it has been run on the local machine.
- Files found uploaded to a server reportedly in Ukraine
- Only FF with built-in PDF reader is vulnerable, thus =not= Android.
- I'll discuss NoScript vs Sandboxie and the solution I'm aiming for...

Firefox v40

- Improved appearance and usability under Win10.
- Easier to use on a touchscreen.
- "Close" buttons on tabs are larger
- Address bar uses larger font.
- Smoother scrolling and animation.
- Security:
- Warnings for unsigned browser extensions (entirely blocked at v41)
- https://www.mozilla.org/en-US/firefox/releases/

BlackHat & DefCon and a ReTweet by Matthew Green:

- Retweeted by Matthew Green: Thomas H. Ptacek @tqbf
- (Founder: Matasano Security)
- "There is nothing you will learn at BH or DC that you won't learn quicker online."

The "Memory Sinkhole" Exploit, redux / BlackHat

- The Memory Sinkhole - Unleashing an x86 Design Flaw Allowing Universal Privilege Escalation
- In x86, beyond ring 0 lie the more privileged realms of execution, where our code is invisible to AV, we have unfettered access to hardware, and can trivially preempt and modify the OS. The architecture has heaped layers upon layers of protections on these negative rings, but 40 years of x86 evolution have left a labyrinth of forgotten backdoors into the ultra-privileged modes. Lost in this byzantine maze of decades-old architecture improvements and patches, there lies a design flaw that's gone unnoticed for 20 years. In one of the most bizarre and complex vulnerabilities we've ever seen, we'll release proof-of-concept code exploiting the vast, unexplored wasteland of forgotten x86 features, to demonstrate how to jump malicious code from the paltry ring 0 into the deepest,

darkest realms of the processor. Best of all, we'll do it with an architectural 0-day built into the silicon itself, directed against a uniquely vulnerable string of code running on every single system.

- https://github.com/xoreaxeaxeax/sinkhole
- http://blog.jacobtorrey.com/mitigations-to-the-memory-sinkhole
- APIC is an I/O device, but it's memory-mapped for high-speed access
    - 4K page can be relocated on 4K boundary anywhere in memory.
- SMM
    - What?
    - Scattering-matrix method
    - Scots Musical Museum
    - Science Museum of Minnesota
    - Shanghai Metals Market
    - Single-molecule magnets
    - Single Monthly Mortality, a measurement for Prepayment of loan
    - Social Media Marketing
    - Soft Magnetic Materials
    - Solar Maximum Mission
    - Stepwise Mutation Model
    - Storage Modification Machine
    - System Management Mode, a computer operating mode

- An ultra-privileged "second world" which exists underneath the OS to interface with and manage the motherboard hardware resources.
    - APM - Advanced Power Mode
    - Memory and chipset errors.
    - Emulation of older peripherals such as the PS/2 mouse or USB keyboard.
    - Access the TPM (trusted platform module)
- SMM can only be entered through SMI (System Management Interrupt) and ONLY from code that's already running in Ring-0.
- The processor executes the SMM code in a separate address space inaccessible to other operating modes of the CPU.
- The sky is not falling:
    - Intel independently found and fixed this in SandyBridge and all successive micro-architectures in 2011.
    - Incredibly difficult to exploit:
    - Ring 0
    - Depends upon the exact SMM code bytes which vary wildly with every motherboard and firmware release.

PushBullet adds E2E encryption

- http://www.androidpolice.com/2015/08/11/pushbullet-now-supports-end-to-end-encryption-for-notification-mirroring-sms-and-copy-paste-sync/
- DH?... could still suffer from a MITM attack.
- Password used to generate a symmetrical 256-bit AES key which is never sent to the server.

Oracle insists their customers trust them

- In a blog post by Oracle's Chief Security Officer (which has since been taken down but was caught and archived, see below), Mary Ann Davidson tells Oracle users to stop reverse engineering Oracle products in search of security vulnerabilities.
- Security researcher Matt Blaze thought the blog entry was so bizarre that he assumed Oracle had been hacked and the story posted as a parody.
- Matt Tweeted:
  - My first assumption after reading this was that Oracle's web server was hacked and this article is a parody.
  - Oracle should get an honorary membership in the Locksmithing Guild for their heroic "security by not looking" policy.
- Owen Williams, writing for "The Next Web" wrote...
  - http://thenextweb.com/opinion/2015/08/11/oracle-drinking-the-kool-aid/
  - <quote> Oracle's Chief Security Officer, Mary Ann Davidson, took to her corporate blog today to rant about security, and how Oracle has been pursuing its own clients that break its license terms to ensure software security.
  - I have such a hard time believing this post is real that I've reached out to Oracle PR to ask if it's authentic or not.
  - Until then, the post says that some customers have been hiring security consultants to do research on Oracle's tools, who often use 'static analysis' tools to reverse engineer software and find security vulnerabilities.
- Original posting:
  - https://archive.is/oJMWO
- Assertions:
  - It is an intellectual property violation for security researchers to "decompile" Oracle's code looking for undiscovered security vulnerabilities.
  - Oracle already does this and we're good at it, so you don't need worry.
- Wait, wait... doesn't Oracle publish Java? How's that been going?
- So out of touch with reality - Noteworthy quotes from Mary Ann Davidson's blob posting:
  - <quote> I want to reiterate that customers Should Not and Must Not reverse engineer our code. However, if there is an actual security vulnerability, we will fix it. We may not like how it was found but we aren't going to ignore a real problem – that would be a disservice to our customers. We will, however, fix it to protect all our customers, meaning everybody will get the fix at the same time. However, we will not give a customer reporting such an issue (that they found through reverse engineering) a special (one-off) patch for the problem. We will also not provide credit in any advisories we might issue. You can't really expect us to say "thank you for breaking the license agreement."
  - <quote> If we determine as part of our analysis that scan results could only have come from reverse engineering (in at least one case, because the report said, cleverly enough, "static analysis of Oracle XXXXXX"), we send a letter to the sinning customer, and a different letter to the sinning consultant-acting-on-customer's behalf – reminding them of the terms of the Oracle license agreement that preclude reverse engineering, So Please Stop It Already.

EFF Released "Privacy Badger v1.0"

- https://www.eff.org/deeplinks/2015/08/privacy-badger-10-here-stop-online-tracking
- NOT a broad stroke ad blocker... rather a tracking blocker.
- EFF is excited to announce that today we are releasing version 1.0 of Privacy Badger for Chrome and Firefox. Privacy Badger is a browser extension that automatically blocks hidden trackers that would otherwise spy on your browsing habits as you surf the Web.

  As you browse the Web, Privacy Badger looks at any third party domains that are loaded on a given site and determines whether or not they appear to be tracking you (e.g. by setting cookies that could be used for tracking, or fingerprinting your browser). If the same third party domain appears to be tracking you on three or more different websites, Privacy Badger will conclude that the third party domain is a tracker and block future connections to it.

  For certain websites, if Privacy Badger were to block an embedded domain entirely it would break the site's core functionality. For example, if Privacy Badger were to block 'licensebuttons.net,' Creative Commons buttons would no longer load. In these cases Privacy Badger blocks the domain from setting or receiving any cookies or 'referer' headers, but allows the embedded content to load.

  To be clear, EFF isn't against websites seeking to build businesses around advertising. More business models means a more vibrant Web. But advertising cannot come at the expense of user privacy and the inviolable principle of consent. Until the online tracking industry changes its ways, the only option for users is to protect themselves by installing tools such as Privacy Badger.

  Privacy Badger 1.0 works in tandem with the new Do Not Track (DNT) policy, announced earlier this week by EFF, Disconnect, Medium, Mixpanel, Adblock, and DuckDuckGo. Installing Privacy Badger also enables the DNT flag as a clear signal to sites that the user wants to opt-out of online tracking. Privacy Badger inspects third party sites for a commitment to honor that request under the DNT Policy; if it finds one, it will unblock that third party by default. That way, web services that do the right thing by users can continue to collect anonymous data or show anonymous ads, while those that don't will be foiled by the Badger's protections.

EFF's Clear Rules of the Road with the Do Not Track Policy"

- https://www.eff.org/deeplinks/2015/08/clear-rules-road-do-not-track-policy-0
- EFF's "A privacy-friendly Do Not Track (DNT) Policy "
  - https://www.eff.org/dnt-policy
- It's a "conduct pledge"
- Q&A:
  - I'm an advertising/tracking company and my business practices require me to set unique cookies or fingerprint everyone, even if they have the DNT flag set. Is this policy for me?

    No. This policy is not intended to be compatible with businesses practices that involve the non-consensual collection of Internet users' reading habits or online activities. It is a document intended to give users strong privacy protections, which means that in the current Web environment only some companies are going to be willing and able to post it.

FLASH now at v18.0.0.232

- http://www.adobe.com/software/flash/about/
- With no NoScript... Flashblock!

Tweets:

- Jonny @aDaemon
  @SGgrc will you consider using Windows 10 after applying "private" settings?

- George Palfi @jorjitop
  @SGgrc reskin Win 10, use Classic Shell. I have on Win 8/8.1 and it looks and works like Win7 or Win XP as you wish. http://classicshell.net

Miscellany

- How to clean the inside of my Contigo thermos?
- Puro Caff
- http://www.amazon.com/Urnex-02031-Puro-Caff-20oz/dp/B0016C2NZG

Media

- "Humans" on AMC.

SpinRite and ECC:

- Michael Coyne in Rayleigh, Essex. United Kingdom
- Subject: SpinRite ecc readout

- Dear Steve,
  I'm no propeller head, but I really stay up on the security side of things and I'm so glad I stumbled upon Security Now about 5 years ago.
  SpinRite increased the ECC maximum number on my old 250GB computer by about 5 points over several years and as it says on one of the GRC SpinRite pages a 100% healthy drive shows no red. My old computer was certainly healthy in that respect.
  My 2TB drive isn't quite as healthy, as I always see some red blocks on the ECC readout while SpinRite is working the drive. And the seek error maximum has increased three points in the six months I've owned the computer.
  Best wishes,
  Michael Coyne

The Quest for Surfing Safety

NoScript vs Sandoxie --> Lightweight full VM.

- Recent Mozilla breach shows
- TinyCoreLinux
- http://tinycorelinux.net/

And so we wrap up episode #520... 10 years of Security Now!

- First episode was "As the Worm Turns" - August 19th, 2005.