Security Now! #573 - 08-16-16

News, Memory & Micro Kernels

This week on Security Now!

Did Microsoft lose control of their secure boot "Golden Key"? AdBlock, unblock, counter-unblock, and counter-counter-unblock is well underway, Leo's story from the field about Avast A/V, a "security is hard to do" mistake in an update to the Internet's TCP protocol, Microsoft's evolving Windows Update policies, an uber-cool way for developers to decrypt and inspect their Firefox and Chrome local TLS traffic, a nice write up of our three-dumb-routers solution, trouble with Windows Identity leak mitigation, yet another way of exfiltrating data from an air-gapped PC, some fun miscellany, and discussion of micro kernels and Intel's forthcoming memory breakthrough! (And more! :)

Whoopsie! Microsoft let their secure boot key out of the bag ... or did they???

(This slick image taken from the threatpost coverage of this fiasco.)

Security News

Did Microsoft really leak their secure boot "Golden Key"??
https://threatpost.com/microsoft-mistakenly-leaks-secure-boot-key/119828
https://9to5mac.com/2016/08/12/proof-apple-was-right-to-fight-the-fbi/
http://arstechnica.com/security/2016/08/microsoft-secure-boot-firmware-snafu-leaks-golden-key/
The reporting on this has been 1000% inflammatory and incorrect.
The hackers who discovered this are undoubtedly very talented, and they did a terrific job of cleverly uncovering an exploit for a mistake Microsoft made, but no keys were leaked in the process… Golden or otherwise.

- It's an implementation design error in the handling of boot permission policies which can be used to trick older UEFI secure boot managers.
- Windows 10 v1607 'Redstone' (the Anniversary Update) added new "supplemental" secure boot policies that can, for example, allow for test signing of development code... which could also be malicious rootkits, etc.
- This was all fine and was properly managed and checked by the newer Win10 v1607.
- But PREVIOUS boot managers, such as Win10 v1511, DO NOT KNOW about these supplemental policies, and they will be accepted when they should not be... thus exposing the secure boot before the Anniversary Update updated the secure boot to an exploit.
- The hackers wrote: "You can see the irony. Also the irony in that MS themselves provided us several nice "golden keys" (as the FBI would say ;) for us to use for that purpose :) About the FBI: are you reading this? If you are, then this is a perfect real world example about why your idea of backdooring cryptosystems with a "secure golden key" is very bad! Smarter people than me have been telling this to you for so long, it seems you have your fingers in your ears. You seriously don't understand still? Microsoft implemented a "secure golden key" system. And the golden keys got released from MS own stupidity. Now, what happens if you tell everyone to make a "secure golden key" system? Hopefully you can add 2+2... Anyway, enough about that little rant, wanted to add that to a writeup ever since this stuff was found ;)

Adblock Plus has already defeated Facebook's new ad blocking restrictions

- http://www.theverge.com/2016/8/11/12439990/facebook-unblockable-ads-defeated-by-adblock-plus
- https://adblockplus.org/blog/fb-reblock-ad-blocking-community-finds-workaround-to-facebook
- 1st party / 3rd party *and* URL blocking.

Leo... Could you share your story from The Tech Guy (Avast TLS proxy)

Linux traffic hijack flaw also affects most Android phones, tablets

- http://www.zdnet.com/article/linux-traffic-hijack-flaw-also-affects-most-android-phones-tablets/
- A difficult-to-exploit flaw affects all Android phones and tablets that are running Android 4.4 KitKat and later, which comes with the affected Linux kernel 3.6 or newer.
- That's about 1.4 billion devices, including the developer previews of Nougat.
- 25th Usenix Security Conference Paper
    - "Off-Path TCP Exploits: Global Rate Limit Considered Dangerous"
    - https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/cao

- Abstract: In this paper, we report a subtle yet serious side channel vulnerability (CVE-2016-5696) introduced in a recent TCP specification. The specification is faithfully implemented in Linux kernel version 3.6 (from 2012) and beyond, and affects a wide range of devices and hosts. In a nutshell, the vulnerability allows a blind off-path attacker to infer if any two arbitrary hosts on the Internet are communicating using a TCP connection. Further, if the connection is present, such an off-path attacker can also infer the TCP sequence numbers in use, from both sides of the connection; this in turn allows the attacker to cause connection termination and perform data injection attacks. We illustrate how the attack can be leveraged to disrupt or degrade the privacy guarantees of an anonymity network such as Tor, and perform web connection hijacking. Through extensive experiments, we show that the attack is fast and reliable. On average, it takes about 40 to 60 seconds to finish and the success rate is 88% to 97%. Finally, we propose changes to both the TCP specification and implementation to eliminate the root cause of the problem.

- Gist: "The root cause of the vulnerability is the introduction of the challenge ACK responses [26] and the global rate limit imposed on certain TCP control packets. The feature is outlined in RFC 5961, which is implemented faithfully in Linux kernel version 3.6 from late 2012. At a very high level, the vulnerability allows an attacker to create contention on a shared resource, i.e., the global rate limit counter on the target system by sending spoofed packets. The attacker can then subsequently observe the effect on the counter changes, measurable through probing packets.

  Through extensive experimentation, we demonstrate that the attack is extremely effective and reliable. Given any two arbitrary hosts, it takes only 10 seconds to successfully infer whether they are communicating. If there is a connection, subsequently, it takes also only tens of seconds to infer the TCP sequence numbers used on the connection. To demonstrate the impact, we perform case studies on a wide range of applications.

  The contributions of the paper are the following:
    - We discover and report a serious vulnerability unintentionally introduced in the latest TCP specification which is subsequently implemented in the latest Linux kernel.

    - We design and implement a powerful attack exploiting the vulnerability to infer 1) whether two hosts are communicating using a TCP connection; 2) the TCP sequence number currently associated with both sides of the connection.

    - We provide a thorough analysis and evaluation of the proposed attack. We present case studies to illustrate the attack impact.

    - We identify the root cause of the subtle vulnerability and discuss how it can be prevented in the future. We propose changes to the kernel implementation to eliminate or mitigate the side channel.

- Patches released last month (July 11th) but won't be pushed until the September update.

Microsoft Further simplifies their patching models for Windows 7 and Windows 8.1

- https://blogs.technet.microsoft.com/windowsitpro/2016/08/15/further-simplifying-servicing-model-for-windows-7-and-windows-8-1/
- http://arstechnica.com/business/2016/08/windows-7-8-1-moving-to-windows-10s-cumulative-update-model/
- Instead of a handful of individual incremental updates, starting with this coming October's patch Tuesday, all updates will be merged into a single monthly update.
- Each successive month will add to that new patch base, offering one single update.
- Over time, Microsoft will also move backward in time, incorporating earlier and earlier patches until, eventually, the monthly update will take an original Windows 7 SP1 machine and bring it current.
- Since Windows Update HAS dramatically changed since then, it will need to be updated for awareness of the new methodology, then the single mega-rollup can be applied.
- Note that nice as this is, it is also removing some user control. For instance, the GWX 3035583 patch could not be have been selectively avoided... and we have no idea what other mischief Microsoft might have planned up its sleeves between now and 2020.

Microsoft's Windows support U-turn: New Skylake PCs get all security patches

- http://www.techrepublic.com/article/microsofts-windows-7-support-u-turn-now-new-skylake-pcs-get-security-patches-until-2020/
- In January of this year, Microsoft had announced that Win7 & 8.1 systems running on Intel Skylake generation processors would stop receiving security updates next summer (2017), then they moved it back to the summer of 2018. Now it's been moved all the way back to 2020 for Win7 and 2023 for Win8.1, when all updates for those platforms are set to end.

How to decrypt Firefox TLS connection traffic!

- https://jimshaver.net/2015/02/11/decrypting-tls-browser-traffic-with-wireshark-the-easy-way/
- An amazingly cool hack: TLS Key logging is enabled by setting the environment variable SSLKEYLOGFILE <FILE> to point to a file. This file is a series of lines. Comment lines begin with a sharp character ('#'). Otherwise the line takes one of these formats:
    - RSA <space> <16 bytes of hex encoded encrypted pre master secret> <space> <96 bytes of hex encoded pre master secret>
    - CLIENT_RANDOM <space> <64 bytes of hex encoded client_random> <space> <96 bytes of hex encoded master secret>

- https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/Key_Log_Format
  (Long discussion in Mozilla-land about disabling... but those wanting it won.)

Steve Gibson's Three Router Solution to IOT Insecurity

- http://www.pcper.com/reviews/General-Tech/Steve-Gibsons-Three-Router-Solution-IOT-Insecurity
- We need the same thing for the Ubiquity EdgeRouter X and for pfSense... anyone?? <g>

Showstopping side effects of disabling the Windows SMB credential leakage

- Donn Edwards (@donnedwards)
  Hi Steve, the "fix" for IE user names mentioned here bleepingcomputer.com/news/security/… causes more problems than it solves.

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0]
  "RestrictSendingNTLMTraffic"=dword:00000002

  This effectively isolates the PC on the LAN, so that it cannot see or connect to any other PC or file share on the LAN. You have to enable connecting with every other PC or server as an exception.

  It also interferes with Remote Desktop connections, so that even if you connect with RD and use saved credentials, you still have to input the credentials again.

  Please could you alert users to this issue, since the article itself is not particularly clear or explicit. Keep up the good Security Now! Work

- Steve's proper solution: block all traffic across ports 137-139 and 445 at your LAN/WAN egress point. This is where having a strong border hardware firewall comes in so handy.

- pfSense: https://doc.pfsense.org/index.php/What_are_UPnP_and_NAT-PMP
  <quote> UPnP is short for Universal Plug and Play and is commonly found on Windows, BSD and Linux systems.

  NAT-PMP is short for NAT Port Mapping Protocol and is similar to UPnP but found more commonly on Apple devices and programs.

  A growing number of programs support both methods.

  pfSense supports both, and the service may be configured at Services > UPnP & NAT-PMP.

  UPnP and NAT-PMP both allow devices and programs that support them to automatically add dynamic port forwards and firewall entries. The most common uses are in gaming systems (XBox, Playstation, etc) and BitTorrent programs like uTorrent, which both rely on allowing inbound connections to a local service.

!!! WARNING !!! Potential Security Risk!

If UPnP or NAT-PMP are enabled, use only devices and programs which are trusted. These mechanisms will allow these entities to bypass the firewall to allow incoming connections with no additional control or authorization. Do not be surprised when this happens.

Access permissions for the service may be crafted in the options on pfSense. The format of these is shown in the GUI at Services > UPnP & NAT-PMP in the User specified permissions boxes. Using these, access could be restricted to a specific workstation or device.

- Another good thread about UPnP w/XBOX: https://forum.pfsense.org/index.php?topic=13887.0

Yet another way of exfiltrating data from a computer: HD head movement sounds.

- ArsTechnica: New air-gap jumper covertly transmits data in hard-drive sounds: "DiskFiltration" siphons data even when computers are disconnected from the Internet.
- http://arstechnica.com/security/2016/08/new-air-gap-jumper-covertly-transmits-data-in-hard-drive-sounds/
- The method has been dubbed "DiskFiltration" by its creators because it uses acoustic signals emitted from the hard drive of the air-gapped computer being targeted.
- Manipulates the hard drive's head actuator to generate sounds that can transfer passwords, cryptographic keys, and other sensitive data stored on the computer to a nearby microphone.
- Has worked at six feet and a speed of 180 bits per minute, fast enough to steal a 4,096-bit key in about 25 minutes.

Miscellany

IPMI == CUJO!

- Gratuitous ARP packets: The Intelligent Platform Management Interface (IPMI)!!
- The more I use FreeBSD the more I love it. UNIX is where I will wind up.

Codex Silenda: The Book of Puzzles

- https://www.kickstarter.com/projects/2119414279/codex-silenda-the-book-of-puzzles

A puzzle for our clever listeners:

- Jimmy G (@TheRedTech)
  @NakedSecurity @SGgrc I just bought a USB from a friend but hes a hacker of sorts. How would you safely format it? In case of a joke... or worse.
- A chromebook will do it safely (you could then powerwash) or a UNIX would be safe since any nonsense it might have would assume a mainstream OS's over-featured vulnerabilities.

A really excellent USB explainer:
http://www.logicsupply.com/explore/io-hub/usb-type-c-and-usb-3-1-explained/

USB Standard	Max Transfer Speed	Power Output	Logo	Symbol
USB 2.0	480 Mbit/s	2.5W		
USB 3.0 (USB 3.1 Gen 1)	5 Gbit/s	4.5W		
USB 3.1 (USB 3.1 Gen 2)	10 Gbit/s	100W		

- Physical connectors, Power delivery capabilities, data rates, USB 3.0/3.1 1st & 2nd gen. Good comments, too. :)

The truth about the "Internet of Things":
John Adams @netik (one of the early twitter employees: "I helped build this thing.")
"There is no Internet of Things. There are only many unpatched, vulnerable small computers on the Internet."

SpinRite

David L in Omaha, Nebraska
Subject: SpinRite saved me once again... and our high school yearbook!

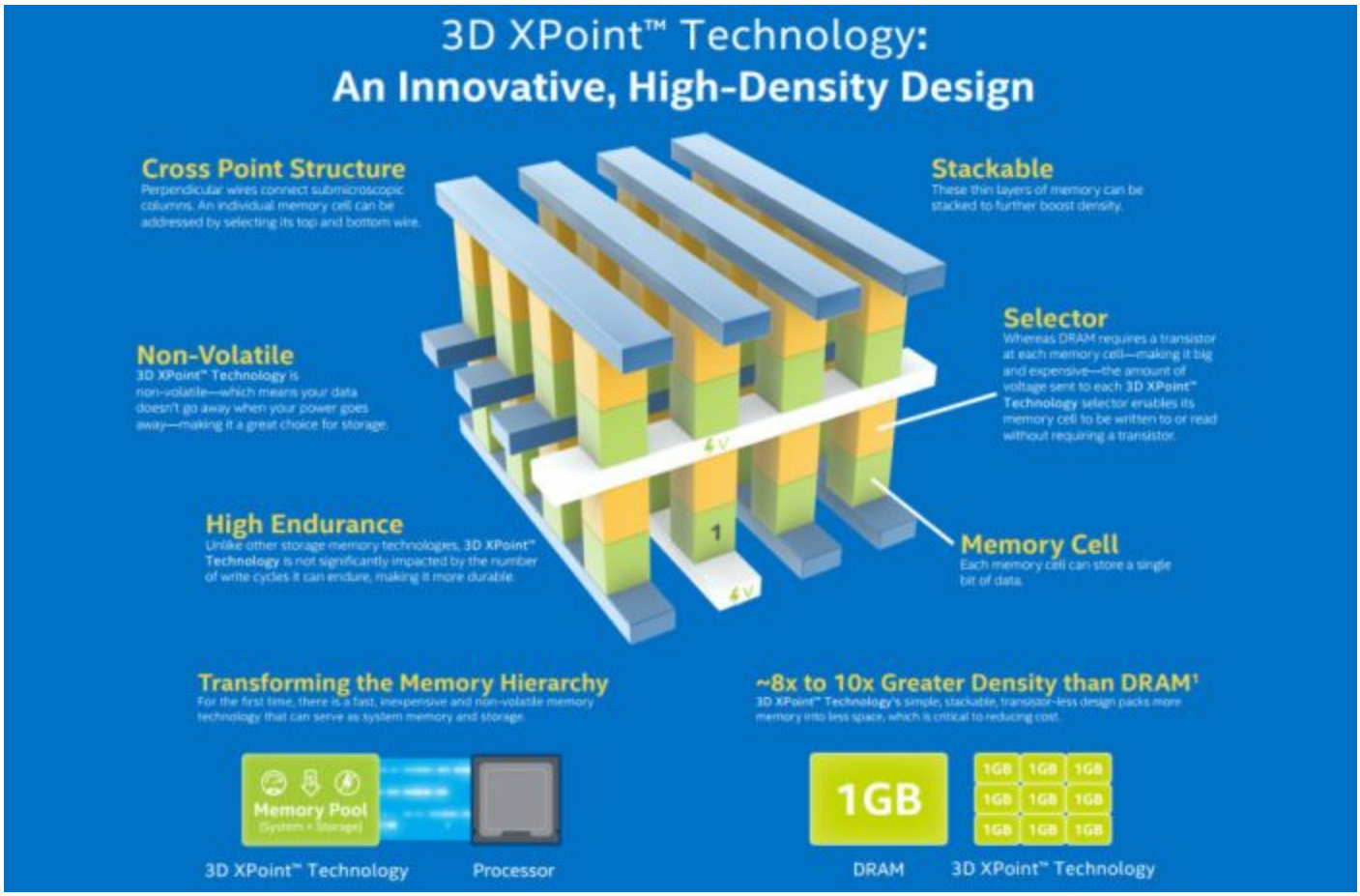
Hello Steve, I am a high school student who really enjoys listening to you and Leo on Security Now every Wednesday. Love the depth you go into your topics! Anyway, I was working on a paper due the next day on my desktop and everything on my computer had been running very smoothly, as if nothing was wrong. I noticed that some updates were waiting for me to install. I didn't have time to install them right away, so I decided that I would let them install when I head off to school. In the morning it boots up just fine, but when I come home, I'm greeted by a screen that read "No active partition found." Normally I need to confirm to restart the computer, as it was sitting on the Windows Update screen when I left. I began to panic, as most of my schoolwork had resided on that computer along with some photos that I needed to copy to a flash drive for the high school yearbook. Trying to figure out what to do, I was Googling the error message. It turns out that others have fixed it through the Windows 7 install DVD. I didn't want to do that as I was afraid it might corrupt the drive even more. So I ran SpinRite. I selected my drive, and ran it on Level 2. I let it run. About an hour or two later, I was greeted that SpinRite found no errors. I was prepared for the worst then, as I did not back up this computer (even though I should) as we do not have the best Internet speed. I was afraid I was going to lose everything and let our yearbook staff down. I rebooted the computer, only to find it prompting me to select "Last Known Good Configuration or Profile 1". I selected Profile 1, and the computer started right up into Windows. I am in the process of backing up my data to a safe place and giving the important photos to our yearbook staff like nothing even happened. Thank you Steve for your amazing work!

David L
Omaha, Nebraska

Crosspoint Memory... is like CORE.

- https://www.youtube.com/watch?v=gMwz1eWQzno
- http://www.intel.com/content/www/us/en/architecture-and-technology/3d-xpoint-unveiled-video.html
- Directly addressable memory.
- Static RAM
- Dynamic RAM
- Historically, MASS memory was TEMPORAL and that means sequential.
    - Mercury delay line.
    - Drum.
    - Tape.
    - Disc.
- We developed Interfaces that were natural representations because they reflected the physical architecture of the device. Engineers did this. Since we needed every bit of possible performance, no ABSTRATCTION was possible since an abstraction would have hidden the underlying details... and those details could be leveraged for benefit.

- An example is that drum memory which stored instructions and data, had the instructions arrayed around the drum so that the data was becoming available as it was needed.
- RAM - Random Access Memory (NOT sequential in any way!)
    - Static RAM (CPU registers) Many transistors (about 6)
    - Dynamic RAM (DRAM) 1 transistor and 1 capacitor
    - Crosspoint memory -- no transistors!!



- It's essentially an array of X/Y addressable resistors
- http://www.intel.com/content/www/us/en/architecture-and-technology/non-volatile-memory.html
    - x1000 faster than NAND
    - x1000 more endurance than NAND
    - x10 more dense than DRAM
    - Bulk Material Property Change.
    - 128 gigabit dies (16GB chip)

- Even in an iPad, there's working memory and storage.

What is a Microkernel?

- "No battle plan survives contact with the enemy."
- Some things cannot be done by apps:
  - Program Loader
  - Scheduler (process & thread)
- System resources are global and shared:
  - Memory management
- ----------
- OS API services?
- Device drivers?
- File system abstractions?
- Higher level functions? e.g. graphics