Security Now! #646 - 01-16-18

The InSpectre

This week on Security Now!

This week we discuss more trouble with Intel's AMT, what does Skype's use of Signal really mean, the UK's data protection legislation gives researchers a bit of relief, the continuing winding down of HTTP, "progress" on the development of Meltdown attacks, Google successfully tackles the hardest-to-fix Spectre concern with a Return Trampoline, some closing the loop feedback with our terrific listeners, and the evolving landscape of Meltdown and Spectre, including Steve's just completed "InSpectre" test & explanation utility.

Our Picture of the Week :)

Security News

A typical Intel AMT configuration flow allows attackers to gain full control of corporate laptops in 30 Seconds

https://thehackernews.com/2018/01/intel-amt-vulnerability.html
http://www.tomshardware.com/news/intel-amt-bitlocker-bios-bypass,36321.html
https://press.f-secure.com/2018/01/12/intel-amt-security-issue-lets-attackers-bypass-login-credentials-in-corporate-laptops/
https://threatpost.com/intel-amt-loophole-allows-hackers-to-gain-control-of-some-pcs-in-under-a-minute/129408/

Insecure defaults in Intel AMT allow an intruder to completely bypass user and BIOS passwords, the TPM, and Bitlocker PINs to backdoor almost any corporate laptop in a matter of seconds.

Intel's AMT -- Active Management Technology -- system is a little too active.

AMT, which permits remote management of devices within a corporate environment is protected with its own, typically default "admin" password.

When booting the machine, pressing "P" switches to the AMT BIOS extension. "Admin" can be entered and AMT's remote access password can be changed or set, access enabled and setting AMT's user opt-in to 'None'.

This leaves the laptop vulnerable to remote connections by attackers on the same network segment as the machine... which is not difficult to arrange.

Recommendations for end users:

- Do not leave your laptop unwatched in an insecure location such as a public place.
- Contact your IT service desk to handle the device.
- If you're an individual running your own device, change the AMT password to a strong one, even if you don't plan on using AMT. If there's an option to disable AMT, use it. If the password is already set to an unknown value, consider the device suspect.

For organizations:

- Adjust the system provisioning process to include setting a strong AMT password, and disabling AMT if this option is available.
- Go through all currently deployed devices and configure the AMT password. If the password is already set to an unknown value consider the device suspect and initiate incident response procedure.

Skype and Signal Partner on End-to-End Encryption
https://signal.org/blog/skype-partnership/

Signal's Announcement:

> In collaboration with Signal, Microsoft is introducing a Private Conversations feature in Skype, powered by Signal Protocol.
>
> At Signal, our goal is to make private communication simple and ubiquitous. With hundreds of millions of active users, Skype is one of the most popular applications in the world, and we're excited that Private Conversations in Skype will allow more users to take advantage of Signal Protocol's strong encryption properties for secure communication.
>
> The Private Conversations feature is available now in preview for Skype Insiders. There's (still) more to come
>
> Microsoft joins a growing list of organizations including WhatsApp, Google, Facebook, and Signal itself that have integrated the open source Signal Protocol into their messaging platform.
>
> We're going to continue our efforts to advance the state of the art for frictionless private communication, in our own app and in others. We're excited about the future of Signal Protocol and the places it is going.

https://support.skype.com/en/faq/FA34824/what-are-private-conversations-in-the-new-skype

The one reminder is that this only provides actual protection against communications interception. Both endpoints see the decrypted communications. And nothing prevents malware, local system compromise, or a court-ordered undocumented feature from being implemented.

Signal is Open Source and implements a beautiful and clever design. But Skype itself is not.

Data protection bill amended to protect security researchers
Exemption added after researchers said efforts to demonstrate inadequate anonymisation could fall foul of law
https://www.theguardian.com/technology/2018/jan/09/data-protection-bill-amended-to-protect-security-researchers

The government is to amend the data protection bill to protect security researchers who work to uncover abuses of personal data, quelling fears that the bill could accidentally criminalise legitimate research.

The revised bill contains a clause making it a criminal offence to "intentionally or recklessly re-identify individuals from anonymised or pseudonymised data" which bad guys -- but not legitimate researchers -- would run afoul of.

Researchers want to be able to responsibly test and verify anonymization systems without such work, itself, being a crime for its own sake.

The winding down of HTTP:
https://blog.mozilla.org/security/2018/01/15/secure-contexts-everywhere/

What is a "Secure Context" ??

A secure context is a Window or Worker for which there is reasonable confidence that the content has been delivered securely (via HTTPS/TLS), and for which the potential for communication with contexts that are not secure is limited. Many Web APIs and features are only accessible in a secure context. The primary goal of secure contexts is to prevent man-in-the-middle attackers from accessing powerful APIs that could further compromise the victim of an attack.

Why should some features be restricted?

Some APIs on the web are very powerful giving an attacker the ability to do the following and more:

- Invade a user's privacy.
- Get low level access to a user's computer.
- Get access to data like user credentials.

The Mozilla blog posting: "Mozilla Security Blog / Secure Contexts Everywhere"

Since Let's Encrypt launched, secure contexts have become much more mature. We have witnessed the successful restriction of existing, as well as new features to secure contexts. The W3C TAG is about to drastically raise the bar to ship features on insecure contexts. All the building blocks are now in place to quicken the adoption of HTTPS and secure contexts, and follow through on our intent to deprecate non-secure HTTP.

Requiring secure contexts for all new features

Effective immediately, all new features that are web-exposed are to be restricted to secure contexts. Web-exposed means that the feature is observable from a web page or server, whether through JavaScript, CSS, HTTP, media formats, etc. A feature can be anything from an extension of an existing IDL-defined object, a new CSS property, a new HTTP response header, to bigger features such as WebVR. In contrast, a new CSS color keyword would likely not be restricted to secure contexts.

Requiring secure contexts in standards development

Everyone involved in standards development is strongly encouraged to advocate requiring secure contexts for all new features on behalf of Mozilla. Any resulting complication should be raised directly against the Secure Contexts specification.

Exceptions to requiring secure contexts

There is room for exceptions, provided justification is given to the dev.platform mailing list. This can either be inside the "Intent to Implement/Ship" email or a separate dedicated thread. It is up to Mozilla's Distinguished Engineers to judge the outcome of that thread and ensure the

dev.platform mailing list is notified. Expect to be granted an exception if:

- other browsers already ship the feature insecurely
- it can be demonstrated that requiring secure contexts results in undue implementation complexity.

Secure contexts and legacy features

Features that have already shipped in insecure contexts, but are deemed more problematic than others from a security, privacy, or UX perspective, will be considered on a case-by-case basis. Making those features available exclusively to secure contexts should follow the guidelines for removing features as appropriate.

"Progress" on the Meltdown/Spectre fronts:

- Raphael Carvalho @raphael_scarv
  F*ck, I can barely believe that I was able to read non-cached data from other process efficiently. Removed iteration and issued flush on secret. Thanks @misc0110, @aionescu for all the tips. Not releasing it or somebody could definitely set the world on fire with this! #meltdown

- Alex Ionescu @aionescu
  I can finally efficiently (fast) and reliably (no errors) read paged pool/non-L1 data. Time for MeltiKatz/MimiDown. I'll sit on this a few weeks before setting the world on fire and watching it burn. Or probably someone will do it first ??

Google Technique Offers Spectre Vulnerability Fix with No Performance Loss
http://www.itprotoday.com/google/google-technique-offers-spectre-vulnerability-fix-no-performance-loss

Retpoline: Google' software construct for preventing branch-target-injection:
https://support.google.com/faqs/answer/7625886

Retpoline - Return Trampoline

Variant CVE-2017-5715 (this is the one that requires a microcode update!) triggers the speculative execution by utilizing branch target injection. It relies on the presence of a precisely-defined instruction sequence in the privileged code as well as the fact that memory accesses may cause allocation into the microprocessor's data cache even for speculatively executed instructions that never actually commit (retire). As a result, an unprivileged attacker could use this flaw to cross the syscall and guest/host boundaries and read privileged memory by conducting targeted cache side-channel attacks.

Source can be recompiled with a Spectre-aware compiler to produce modified subroutine return code whose prediction cannot be externally manipulated.

SpinRite

Torkel Hasle / Location: Sandefjord, Norway
Subject: Spinrite saved the dentist for $60 000 investment
Date: 15 Jan 2018 01:13:19

My daughter works for a group of dentists, and called me when the old PC that runs the machine did not boot. The machine operated a huge OPG (panoramic radiograph), costing around $60 000, and installed around 10 years ago. No support for newer versions of the OS. This expensive machine was dead. Period.

But I offered to run SpinRite for a few hours. It worked for a long time with defective blocks, but after finishing the machine booted and did a file check. All was good and the $60,000 panoramic radiograph was alive again.

Since the machine was so valuable, and they had no backup, I bought a new harddisk (SSD), cloned the old disk which SpinRite made readable with Clonezilla (Linux freeware), blewed dust away, and booted with the new disk. All set! Hopefully the OPG will last another 3-5 years, and postpone the $60 000 investment.

Regards / Torkel Hasle / Sandefjord, Norway

Closing the loop

- Russ Johnson (L) @AJBlue98
  Why not just code modern OSes to run the kernel on one core and keep user-mode applications on (the) other(s)? Or do cores share caches?

- Simon Zerafa @SimonZerafa
  @SGgrc And on the subject of obscure internet data storage schemes here is DNS-FS. Store data in DNS Caches!

  Ben Cox @Benjojo12
  Introducing DNSFS, true cloud storage! Store your files in other peoples DNS Caches!

- @SGgrc Attempted to add SessionManager per your recommendation to Firefox. It appears to not yet be compatible with Quantum or I've got the wrong Add-On. Not sure if you were aware.
  "Tab Session Manager"

- Philip O'Connell @PhilipOConnell
  @SGgrc Hey Steve, I remember in a Security Now episode you mentioned something you used to monitor web pages. When you wanted to be notified of any updates to the monitored page. Do you recall the name of whatever it was you used? Thanks.

  - 1: Check4Change in FF.
  - 2: WebMon

- Grant Taylor @DrScriptt
  @SGgrc Firefox's tracking protection always on even helped with uBlock Origin enabled.

  Also FF's tracking can be disabled per site.

The "InSpectre"

What is InSpectre?

Brian Yates @BrianYates71 (three hours ago)
Replying to @SGgrc
Thank You sir, My work laptop went to a crawl after latest win update, seen your tweet about the freeware, it showed my performance slower, yeah no joke, so disabled meltdown fix, restarted back to normal

Patching Microcode on Linux... and Windows?

https://labs.vmware.com/flings/vmware-cpu-microcode-update-driver

https://downloadcenter.intel.com/download/27431/Linux-Processor-Microcode-Data-File?product=122139

Lenovo Carbon X1 and Dell E7440's both patched.

But none of my older Thinkpads -- some not that old and still useful -- have BIOS updates.

It seems clear that just as the security model for after-sales IoT device security updating is badly broken (with a few exceptions), so, too, is the security model for after-sales PC security. Until now, important threats were generated by, and could thus be removed from and mitigated at, the OS level. But here we have a threat that requires chip hardware level changes for its mitigation... and we again find that nearly all of the hardware currently in use has no channel for such maintenance.

Spectre mitigations in MSVC
https://blogs.msdn.microsoft.com/vcblog/2018/01/15/spectre-mitigations-in-msvc/
Microsoft is aware of a new publicly disclosed class of vulnerabilities, called "speculative execution side-channel attacks," that affect many operating systems and modern processors, including processors from Intel, AMD, and ARM. On the MSVC team, we've reviewed information in detail and conducted extensive tests, which showed the performance impact of the new /Qspectre switch to be negligible. This post is intended as a follow-up to Terry Myerson's recent Windows System post with a focus on the assessment for MSVC. If you haven't had a chance to read Terry's post you should take a moment to read it before reading this one.