January 9, 2018

TLP White
After a calm holiday, we have started the year in total Meltdown. We will look at the Spectre of the chip vulnerability and much more in this week's *Hacking Healthcare:*

Hot Links –

1. ***Chip Flaw:*** The biggest security story[1] in the new year is the disclosure of twin vulnerabilities – Meltdown[2] and Spectre[3] – that have been identified in Intel, AMD, and ARM processors. Researchers have produced proof-of-concept attacks that enable non-privileged users to read the cached memory in the systems kernel. It appears this is made possible by a performance feature on the chips that anticipates and "speculatively" executes future commands. Typical security controls are not applied to commands in speculative execution.

   Chip and OS manufactures, as well as independent security researchers, believe the impact of an attack that leverages Meltdown or Spectre is likely limited to data theft and not operational control of systems (since the security controls kick in before the machine runs those speculatively executed commands).

   Intel[4], AMD[5], and ARM[6] all have press pages devoted to tracking the flaws and their fixes. Intel ARM has noted that it's Cortex-M line of processors (which are used in some medical devices) have not been impacted.

---

[1] https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/
[2] https://meltdownattack.com/meltdown.pdf
[3] https://spectreattack.com/spectre.pdf
[4] https://newsroom.intel.com/news/intel-responds-to-security-research-findings/
The folks at *The Register* who broke the story, are not that impressed with Intel:
http://www.theregister.co.uk/2018/01/04/intel_meltdown_spectre_bugs_the_registers_annotations/
Ars Technica has a look at all responses: https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-heres-what-intel-apple-microsoft-others-are-doing-about-it/
[5] https://www.amd.com/en/corporate/speculative-execution
[6] https://developer.arm.com/support/security-update

Microsoft[7], Apple[8], and Linux[9] developers[10] are all pushing out patches through their own processes. It appears that software fixes at the OS level can limit speculative execution and mitigate the threat of data theft. But such fixes will come at a performance cost. And there is some indication that the windows patch may be bricking some AMD machines[11].

There is concern[12] that cloud service providers represent the greatest risk for attack – where an attacker could use the flaws to read kernel memory on a server that contains private information from and about other customers virtual environments. Amazon[13] and Google[14] have put out statements addressing the issue.

Finally, the OS updates may cause some problems[15] with AV and other security software that is running in your environment. Security researcher Kevin Beaumont has put together a useful table of different vendors' releases to address these issues: https://docs.google.com/spreadsheets/d/184wcDt9I9TUNFFbsAVLpzAtckQxYiuirADzf3cL42FQ/htmlview

NH-ISAC has issued several bulletins on the matter. You can find the latest here: https://nhisac.org/wp-content/uploads/2018/01/TIC-Chip-Vulnerability-Update-1-5-18.pdf

2. ***Trusted Data Exchange:*** On January 5, HHS released[16] its draft Trusted Exchange Framework[17], which outlines principles and requirements for national exchange of electronic health information. The goal is to create a single federal "on-ramp" for everyone in the healthcare community (from patients to providers to researchers) to access health data. The hope is to unite the various Health Information Networks (HINs) that have sprung-up in the last few years under a common set of standards, controls, and APIs.

---

[7] https://support.microsoft.com/en-us/help/4056892/windows-10-update-kb4056892
Microsoft also has a powershell script to verify that a system is properly patched: https://support.microsoft.com/en-hk/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in

[8] https://support.apple.com/en-us/HT208394

[9] https://lwn.net/Articles/741878/

[10] https://lwn.net/Articles/740393/

[11] https://www.theregister.co.uk/2018/01/08/microsofts_spectre_fixer_bricks_some_amd_powered_pcs/

[12] https://www.theverge.com/2018/1/4/16850120/meltdown-spectre-vulnerability-cloud-aws-google-cpu

[13] https://aws.amazon.com/security/security-bulletins/AWS-2018-013/

[14] https://support.google.com/faqs/answer/7622138#chrome

[15] https://www.theregister.co.uk/2018/01/04/microsoft_windows_patch_meltdown/

[16] https://www.hhs.gov/about/news/2018/01/05/draft-trusted-exchange-framework-and-common-agreement-released-hhs.html

[17] https://beta.healthit.gov/topic/interoperability/trusted-exchange-framework-and-common-agreement

To get there, HHS plans to formalize a set of principles and requirements for data exchange in a finalized version of this draft. They will then bid out to a private entity responsibility to "operationalize the framework." The private sector entity (called a Recognized Coordinating Entity) will be responsible for managing stakeholders, ensuring compliance with the principles and requirements, and updating the framework as necessary.

The Framework is divided into two parts – principles and requirements. Part A (Principles) are pretty intuitive and high-level (Standardization; Transparency; Cooperation and Non-Discrimination; Privacy, Security, and Patient Safety; Access; Data-driven Accountability). The section also contains select "sub-principles," which provide an interesting view into HHS priorities. For instance, the privacy, security, and patient safety principle gets two sub-principles, neither of which is really focused on data security. Instead the sub-principles look at accurately pairing data to the correct patient identity, as well as capturing appropriate consent from patients. Assurance over identity pairing is certainly important, but maybe it could be broadened to reflect the need to maintain assurance over data integrity (which is a focus in Part B).

Part B ("Minimum Required Terms and Conditions for Trusted Exchange") is a more detailed and prescriptive set of controls. Security gets a more involved treatment here. The headline is that under the agreement participants have a maximum of 15 calendar days to report any data breach to the HIN. The HIN then has 7 days to further notify other participants affected by the breach. The same timeline (15/7 days) is required of HINs to the RCE, and the RCE to other HINs. This is more stringent than HIPAA's breach notification requirement. Part B also has an affirmative requirement for HINs to evaluate its security program annually and utilize HHS tools such as the OCR cross-walk[18] between NIST CSF and the HIPAA security rule. This is more aggressive than typical OCR requirements, which only offer the crosswalk as a non-mandatory reference guide. There are detailed sections outlining system and individual access controls and logging requirements.

The development of the Framework was mandated by Congress in Section 4003 of the 21st Century Cures Act. In order to develop the draft product, HHS has held three listening sessions, as well as soliciting a round of written feedback. Feedback on the draft is due by February 18. You can submit that feedback here: exchangeframework@hhs.gov

3. ***Medical Device Security:*** The American Hospital Association sent a letter[19] to FDA in December asking for increased oversight of medical device manufacturers, saying "Manufacturers must be held accountable to ***proactively minimize risk***…" That is an

[18] https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf
[19] http://www.aha.org/advocacy-issues/letter/2017/171207-let-aha-fda-regulation-device-security.pdf

interesting phrasing – is AHA suggesting manufacturer liability for vulnerabilities in products?

Congress –

Tuesday, January 9:
--Hearings to examine the anticipated nomination of Alex Michael Azar II, of Indiana, to be Secretary of Health and Human Services (Senate Finance)[20]
--Hearing: Evaluating CFIUS: Challenges Posed by a Changing Global Economy (House Financial Services)[21]
--Hearing: China's Pursuit of Emerging and Exponential Technologies (House Armed Services)[22]

Conferences and Webinars –

--Health IT Summit – San Diego, CA (2/1) <https://vendome.swoogo.com/san-diego-hitsummit-2018/>
--Medical Device Workshop at Philips Healthcare – Andover, MA (3/20) <https://nhisac.org/events/nhisac-events/medical-device-workshop-at-philips-healthcare-andover-ma/>
--Health IT Summit – Cleveland, OH (3/27) <https://vendome.swoogo.com/2018-Cleveland-Health-IT-Summit>
--Health IT Summit – San Francisco, CA (4/5) <https://vendome.swoogo.com/2018-San-Francisco-HIT-Summit>
--Security Workshops at Intermountain Health – Park City, UT (4/24) <https://nhisac.org/events/nhisac-events/security-workshop-at-intermountain-park-city-ut/>
--2018 NH-ISAC Spring Summit – Sawgrass, FL (5/14-17) <http://www.marriott.com/hotels/travel/jaxsw-sawgrass-marriott-golf-resort-and-spa/>
--Health IT Summit – Philadelphia, PA (5/21) <https://vendome.swoogo.com/2018-Philly-HITSummit>
--Health IT Summit – Minneapolis, MN (6/13) <https://vendome.swoogo.com/2018-Minneapolis-Health-IT-Summit>
--Health IT Summit – Nashville, TN (6/28) <https://vendome.swoogo.com/2018-Nasvhille-HITSummit>
--Health IT Summit – Denver, CO (7/12) <https://vendome.swoogo.com/2018-Denver-HITSummit>
--Health IT Summit – St. Petersburg, FL (7/24) <https://vendome.swoogo.com/StPetersburg-HITSummit-2018>
--Health IT Summit – Boston, MA (8/7) <https://vendome.swoogo.com/2018-Boston-Health-IT-Summit>

[20] https://www.finance.senate.gov/hearings/hearing-to-consider-the-anticipated-nomination-of-the-honorable-alex-michael-azar-ii-of-indiana-to-be-secretary-of-health-and-human-services
[21] https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=402841
[22] https://armedservices.house.gov/legislation/hearings/china-s-pursuit-emerging-and-exponential-technologies

January 9, 2018

--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>
--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29)
<https://www.destinationhotels.com/la-cantera-resort-and-spa>

Sundries –

--**How Antivirus Software Can Be Turned Into a Tool for Spying**
<https://www.nytimes.com/2018/01/01/technology/kaspersky-lab-antivirus.html?_r=0>
--**China is reportedly building a $2 billion AI park** <http://www.businessinsider.com/china-is-reportedly-building-a-2-billion-ai-park-in-beijing-2018-1#0ktPhU9q2CY7kgYe.99>
--**Google and Intel Beware: China Is Gunning for Dominance in AI Chips**
<https://www.wsj.com/articles/google-and-intel-beware-china-is-gunning-for-dominance-in-ai-chips-1515060224>
--**NSA's top talent is leaving because of low pay, slumping morale and unpopular reorganization** <https://www.washingtonpost.com/world/national-security/the-nsas-top-talent-is-leaving-because-of-low-pay-and-battered-morale/2018/01/02/ff19f0c6-ec04-11e7-9f92-10a2203f6c8d_story.html?utm_term=.dd33912f6649>
--**10 Cybersecurity Trends: What to Expect in 2018** <http://www.databreachtoday.com/10-cybersecurity-trends-what-to-expect-in-2018-a-10549>
--**Cybersecurity in 2018 looks messy** <http://www.healthcareitnews.com/news/iot-risks-insider-threats-password-hacks-biometric-cracks-cybersecurity-2018-looks-messy>

Contact us: follow @NHISAC and email at bflatgard@nhisac.org