xyone Cyber Security

CAS CYBER ADVISORY SERVICE

Meltdown & Spectre

I. INTRODUCTION

Meltdown[1] and Spectre[2] are recently-discovered hardware vulnerabilities present in a range of modern microprocessors. They were initially disclosed to vendors on Jul 28 2017 and publicly announced early on Jan 3rd 2018 following leaks in *The Register* [1].

II. EXPLOITED TECHNOLOGIES

Out-of-order processing refers to the CPU's low-level re- arranging of multiple instructions into a more efficient order- ing. Speculative execution attempts to predict data that will be moved into memory and executes waiting instructions on it. A correct guess means the processing is already complete when the actual data arrives; an incorrect guess means the instruc- tions must be run now on the real data, which would have been the case anyway. This execution produces measurable side effects.

III. MELTDOWN

Meltdown exploits out-of-order processing to retrieve data before access checks are performed against the user, 'allowing [one] to read arbitrary physical memory from an unprivileged user program' [2]. An attacker can use this to read restricted kernel memory space addresses, which may contain sensitive data such as passwords. Meltdown impacts almost 'every [Intel] processor since 1995' [3] and some ARM processors [4].

Patches are available for affected CPUs, relying on Kernel Page Table Isolation—moving the kernel address space out of each individual process' space. There is some debate as to exactly how much of a performance impact the implementation of these patches will have, but it appears to be between 5–30%, depending on the jobs being performed [5][6].

IV. SPECTRE

Spectre abuses speculative execution and timing attacks to determine the content of arbitrary memory addresses, allowing for inter- and intra-process data exfiltration. This is a particular issue for cloud service providers using shared infrastructure, as an attacker could conceivably access data stored on any legitimate client's instance. Two variants of Spectre vulnerabilities have been identified thus far.

This vulnerability is harder to patch against. Not only does it potentially affect 'all modern processors' [2], but it is a hardware-level exploit. The original CERT vulnerability note simply stated that 'fully removing the vulnerability requires replacing vulnerable CPU hardware.' [7] The original paper states that 'sound solutions will require fixes to processor designs as well as updates to instruction set architectures' [8]. The impact of Spectre is likely to be long-felt; 'we'll be playing whack-the-vulnerability with Spectre until at least the next generation of silicon.' [9] Program recompilation, kernel- level countermeasures and CPU microcode updates are already required to mitigate just these first two variants.

I. THE FUTURE

Both of these vulnerabilities are poised to remain a headache for the foreseeable future, moreso Spectre. Whilst Meltdown is patchable, the hefty performance tax it can impose and the difficulty (if not impossibility) of patching all vulnerable devices may lead to limited protection.

Schnier writes that this, coupled with the discovery of Intel Management Engine vulnerabilities, has announced the age of 'attacks against hardware, as opposed to software, [becoming] more common.' [10] *The Register* goes further, proselytizing about the death of Moore's Law as 'the computer science behind microprocessor design . . . learns that its

[1] CVE-2017-5754

[2] CVE-2017-5753 and CVE-2017-5715

optimisation techniques can be weaponised' [11].

The RISC-V Foundation wasted no time pointing out that their chips were among the few not affected by the vulnerabilities, and reiterated the benefits of open-source development on security [12].

In the short-term, expect to see some organisations' plans to migrate data onto public cloud services delayed— particularly those dealing with sensitive data, such as health- care providers—and possibly a trend towards dedicated servers over shared infrastructure. In a year or two, redesigned chips should be ready for release. Cloud providers in particular will begin upgrading their hardware *en masse*. With its near- monopoly, Intel will be the primary beneficiery of this pur- chasing, and any drop in its share price after the Meltdown and Spectre disclosures will be duly forgotten.

REFERENCES

[1] J. Leyden and C. Williams, *Kernel-memory-leaking intel processor design flaw forces linux, windows re- design*, 2018. [Online]. Available: https : / / www . theregister.co.uk/2018/01/02/intel cpu design flaw/.

[2] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas,
S. Mangard, P. Kocher, D. Genkin, Y. Yarom, and M. Hamburg, 'Meltdown', *ArXiv e-prints*, Jan. 2018. arXiv: 1801.01207.

[3] Graz University of Technology, *Meltdown and spectre*, 2018. [Online]. Available: https://meltdownattack.com/ #faq-systems-meltdown/.

[4] R. Grisenthwaite, Cache Speculation Side-channels. 2018. [Online]. Available: https://developer.arm.com/ support/security-update.

[5] L. Torvalds, Lkml: Linus torvalds: Re: Linux 4.15-rc6, 2018. [Online]. Available: https://lkml.org/lkml/2018/1/ 2/703.

[6] D. Hansen, Lkml: Dave hansen: [patch 00/23] [v4] kaiser: Unmap most of the kernel from userspace page tables, 2018. [Online]. Available: https://lkml.org/lkml/ 2017/11/22/956.

[7] CERT, Vulnerability note vu#584653, 2018. [Online]. Available: https://www.kb.cert.org/vuls/id/584653.

[8] P. Kocher, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom, 'Spectre attacks: Exploiting speculative exe- cution', ArXiv e-prints, Jan. 2018. arXiv: 1801.01203.

[9] T. Pott, You can't ignore spectre. look, it's press- ing its nose against your screen, 2018. [Online]. Available: https : / / www . theregister . co . uk / 2018 / 01/29/you cant ignore the spectre pressing its nose against your glass/.

[10] B. Schneier, The new way your computer can be attacked, 2018. [Online]. Available: https : / / www . theatlantic . com / technology / archive / 2018 / 01 / spectre - meltdown-cybersecurity/551147.

[11] [M. Pesce, Death notice: Moore's law. 19 april 1965 – 2 january 2018, 2018. [Online]. Available: https://www. theregister.co.uk/2018/01/24/death notice for moores law/.

[12] K. Asanovic´ and R. O'Connor, Building a more secure world with the risc-v isa, 2018. [Online]. Available: https://riscv.org/2018/01/more-secure-world-risc-v-isa/.

For up to date threat intelligence please sign up here:

http://www.cyberadvisoryservice.co.uk