Spectre and Meltdown Exploits

Max Weimer

CSCI 460

Spectre Attacks: Exploiting Speculative Execution

- 2 variants, for the sake of presentation simplicity and cohesivity look at only variant 1
- Branch prediction in the name of performance, unintended side-effects
- Demonstrate desire for branch prediction with pipelining to illustrate the crux of the issue
    - Why the exploit exists

Spectre Mitigations

- Application specific - where sandboxing is needed
- Javascript engines
    - Chrome - simple
    - Webkit - complex

Meltdown: Reading Kernel Memory from User Space

- Describe base of how and OOE CPU breaks instructions down and how things might be run differently than written for performance reasons
- Look at how operating system optimizations are partially responsible through kernel memory mapping
- Explore unintended side effects of optimizations

Meltdown Mitigations

- Software: Kernel PTI
    - Only real way to mitigate through software
    - You have to take the performance hit if you want safety
- Hardware: Fundamental hardware changes
    - Intel 9th gen implemented
    - Other mitigations for related attacks implemented sooner/differently

Sources

Official Spectre and Meltdown documentation papers
https://meltdownattack.com/meltdown.pdf
https://spectreattack.com/spectre.pdf

US-Cert security alert
https://www.us-cert.gov/ncas/alerts/TA18-004A

Debian Security overview for linux details
https://wiki.debian.org/DebianSecurity/SpectreMeltdown

Useful exploit overview
https://www.youtube.com/watch?v=I5mRwzVvFGE

Performance hit overview
https://www.extremetech.com/computing/291649-intel-performance-amd-spectre-meltdown-mds-patches

AMD security
https://www.amd.com/en/corporate/product-security

Webkit changes
https://webkit.org/blog/8048/what-spectre-and-meltdown-mean-for-webkit/

Intel CPU-specific mitigations

https://www.intel.com/content/www/us/en/architecture-and-technology/engineering-new-protections-into-hardware.html

Linux Kernel PTI details
https://www.kernel.org/doc/html/latest/x86/pti.html