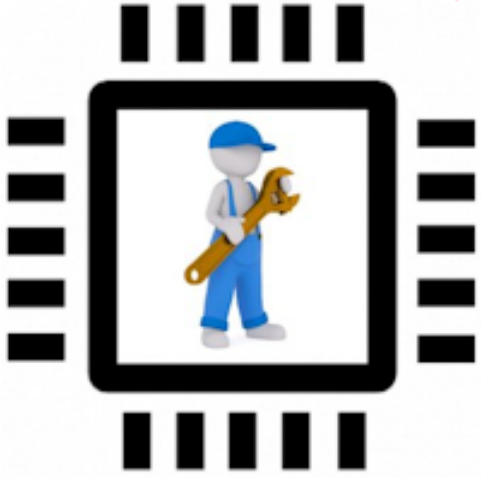


Micro-Renovator

Bringing Processor Firmware up to Code

Bio

Matt (a.k.a. Syncsrc)

- Recovering EE / CompE
- Builder and user of hardware debug features
- Uses “BIOS” and “UEFI” interchangeably
- Currently responsible for platform security of a cloud
- Religiously updates firmware
- Formerly a product security validation lead at Intel

Background



Meltdown

Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory, and thus also the secrets, of other programs and



Spectre

Spectre breaks the isolation b
different applications. It allow
attacker to trick error-free pro
which follow best practices, ir
leaking their secrets. In fact, t
checks of said best practices

the INQUIRER

tificial Intelligence | Internet of Things | Open Source | Hardware | Software | Security

etmaster hack | iOS 12 | Galaxy Note 9 | iPhone 9 | World Cup

Intel, ARM and AMD all affected by security-bypassing, kernel-bothering CPU bugs

Fixes exist but it looks like fundamental processor designs are borked

ars TECHNICA

BIZ & IT | TECH | SCIENCE | POLICY | CARS | GAMING & CULTURE

TECH —

"Meltdown" and "Spectre": Every modern processor has unfixable security flaws

Immediate concern is for Intel chips, but everyone is at risk.

PETER BRIGHT - 1/3/2018, 4:30 PM

Background - Patches for Spectre & Meltdown

- Kernel Only
  - Meltdown: PTI (Linux), KVA Shadow (Windows)
- Kernel and Application
  - Spectre v1: Lfence insertion
  - Spectre v2: Retpoline (an incomplete fix, per Intel)
- Kernel and Microcode
  - Spectre v2: New SPEC_CTRL and PRED_CMD MSRs
  - Spectre v4: SSBD bit added to SPEC_CTRL MSR
  - *Microcode updates are necessary to expose these new registers*

What is Microcode?

- Can be thought of as “Processor Firmware”
  - A Brief History of Microprogramming
- Can be patched to fix bugs & errata
  - However, processors don’t have any non-volatile storage
  - Any applied patches are lost on reset or power-down
- Stored and applied by the *BIOS* or *Operating System*
  - Reloaded on every boot, reset, S3 resume, etc...
  - Intel 64 and IA-32 Architectures SDM Volume 3A, section 9.11.6

Obtaining Microcode Patches

- From BIOS Updates
  - MacBook and Surface users are covered
- From Operating System Updates
  - Linux: redistributed by most distros (via microcode_ctl.rpm or intel-microcode.deb)
    - Users can also download and install microcode.dat directly from Intel
  - Microsoft didn’t start distributing microcode until 2 months after it was released
    - Still only distributing for some processor and Windows versions
- *Patches exist, but are impossible to apply to many systems*


FOX

Systems Unable to Patch Spectre

- Still no way to mitigate Spectre v2 on millions of systems
  - Other than buying a new OS (or a new computer)
- Windows PCs that are 3 to 9 years old *
  - Mostly shipped with Windows 7 or 8 pre-installed
  - BIOS updates delayed or unavailable
- 3rd-party microcode update drivers are ineffective

* CPUs more than 9 years old are not receiving microcode updates from Intel

Systems Unable to Patch Spectre

CPU	BIOS Updates	Windows 7 & 8	Windows 10
8th Gen	Available	N/A	None
7th Gen	Available	N/A	None
6th Gen	Available	Negligible	None
5th Gen	Available *	49 Million	None
4th Gen	Available *	114 Million	None
3rd Gen	Xeon Only	141 Million	None
2nd Gen	Xeon Only	149 Million	None
1st Gen	Xeon Only	216 Million	216 Million

Are there any other options?

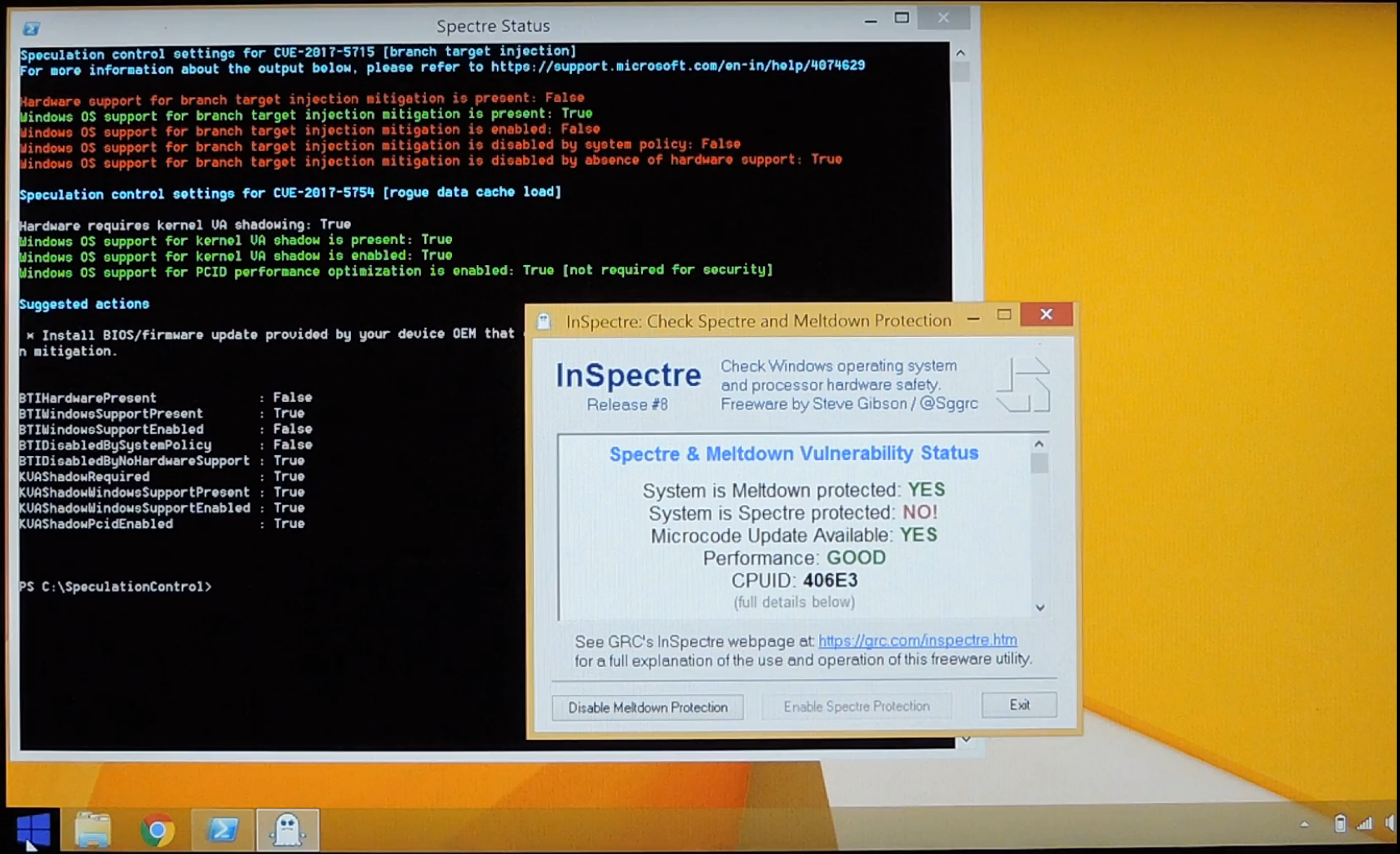
- When can microcode patches be applied?
  - BIOS - users can’t modify
  - OS - microcode drivers run too late
  - Bootloader - *maybe?*
- No existing EFI utility to load microcode
  - TianoCore is open source though
  - And already has code that applies microcode updates
  - How hard could it be?

Uload.efi

- Built using EDK2
- Mostly code appropriated from MicrocodeUpdateDxe
  - Made into an EFI shell app
- Loads microcode to all Processors/Threads

Inserting Uload into EFI Boot

- POST: Power On Stuff That-happens
- Determine bootloader from NVRAM variables
- Locate boot device & partition
  - Involves UUIDs somehow
- Run Bootloader (eg: bootx64.efi, shim.efi)
  - Bootloader is just an EFI application, it can be replaced
- Bootloader launches kernel


Spectre Status
Speculation control settings for CVE-2017-5715 [branch target injection]
For more information about the output below, please refer to https://support.microsoft.com/en-in/help/4074629
Hardware support for branch target injection mitigation is present: False
Windows OS support for branch target injection mitigation is present: True
Windows OS support for branch target injection mitigation is enabled: False
Windows OS support for branch target injection mitigation is disabled by system policy: False
Windows OS support for branch target injection mitigation is disabled by absence of hardware support: True
Speculation control settings for CVE-2017-5754 [rogue data cache load]
Hardware requires kernel VA shadowing: True
Windows OS support for kernel VA shadow is present: True
Windows OS support for kernel VA shadow is enabled: True
Windows OS support for PCID performance optimization is enabled: True [not required for security]
Suggested actions
* Install BIOS/firmware update provided by your device OEM that
n mitigation.
BTIHardwarePresent : False
BTIWindowsSupportPresent : True
BTIWindowsSupportEnabled : False
BTIDisabledBySystemPolicy : False
BTIDisabledByNoHardwareSupport : True
KVAShadowRequired : True
KVAShadowWindowsSupportPresent : True
KVAShadowWindowsSupportEnabled : True
KVAShadowPcidEnabled : True
PS C:\SpeculationControl>
InSpectre: Check Spectre and Meltdown Protection
InSpectre
Release #8
Check Windows operating system and processor hardware safety.
Freeware by Steve Gibson / @Sggrc
Spectre & Meltdown Vulnerability Status
System is Meltdown protected: YES
System is Spectre protected: NO!
Microcode Update Available: YES
Performance: GOOD
CPUID: 406E3
(full details below)
See GRC's InSpectre webpage at: https://grc.com/inspectre.htm
for a full explanation of the use and operation of this freeware utility.
Disable Meltdown Protection
Enable Spectre Protection
Exit

Micro-Renovator



- Script to automatically update EFI boot partition
  - Runs from a Linux Live CD
- Finds EFI partition and bootloader
  - Copies microcode and Uload.efi to the boot partition
  - Installs Shell.efi and sets as the primary boot option
  - On boot, startup script runs Uload prior to the OS bootloader

https://github.com/syncsrc/MicroRenovator

Limitations

- Breaks Sleep (S3)
    - Hibernation still works
- No secure boot support (yet)
- Occasional inconsistent behavior after booting into Windows
- Microsoft appears to be actively reverting the changes made by earlier versions of MicroRenovator

Summary

- Firmware patching is an unsolved problem
  - UEFI should have made things better, but didn’t
- Component vendors needs to focus on enabling patching for end-users
  - Not system builders (they aren’t incentivized)
  - IoT and Mobile spaces have the same issue
- *It shouldn’t take bootloader hacks to apply security patches to operating systems that are still under support*

Questions?

