Meltdown and Spectre

SNAFU or FUBAR

Agenda

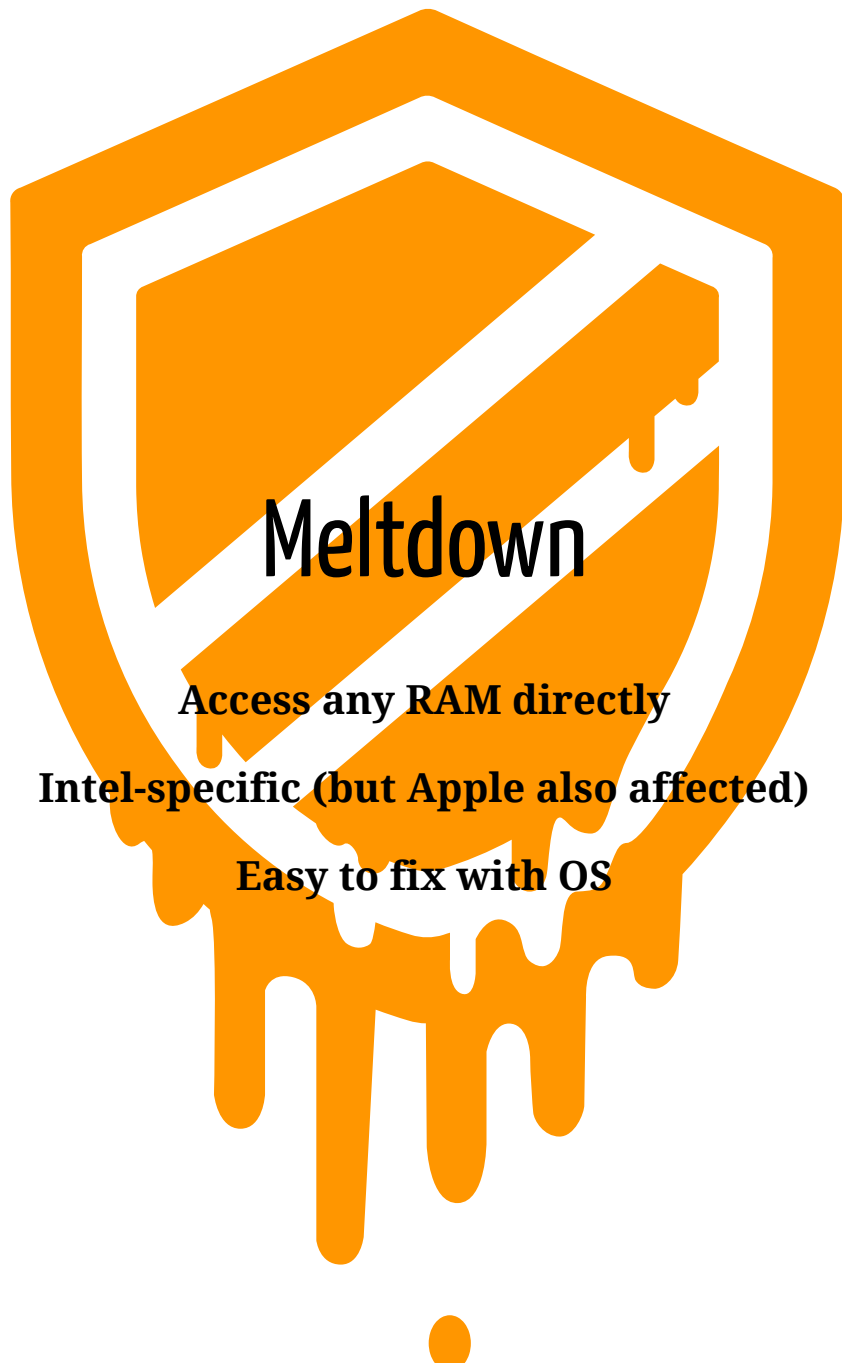**Meltdown**

Spectre

What can we do about it?

Under the hood

Processor caches

Out-of-order execution

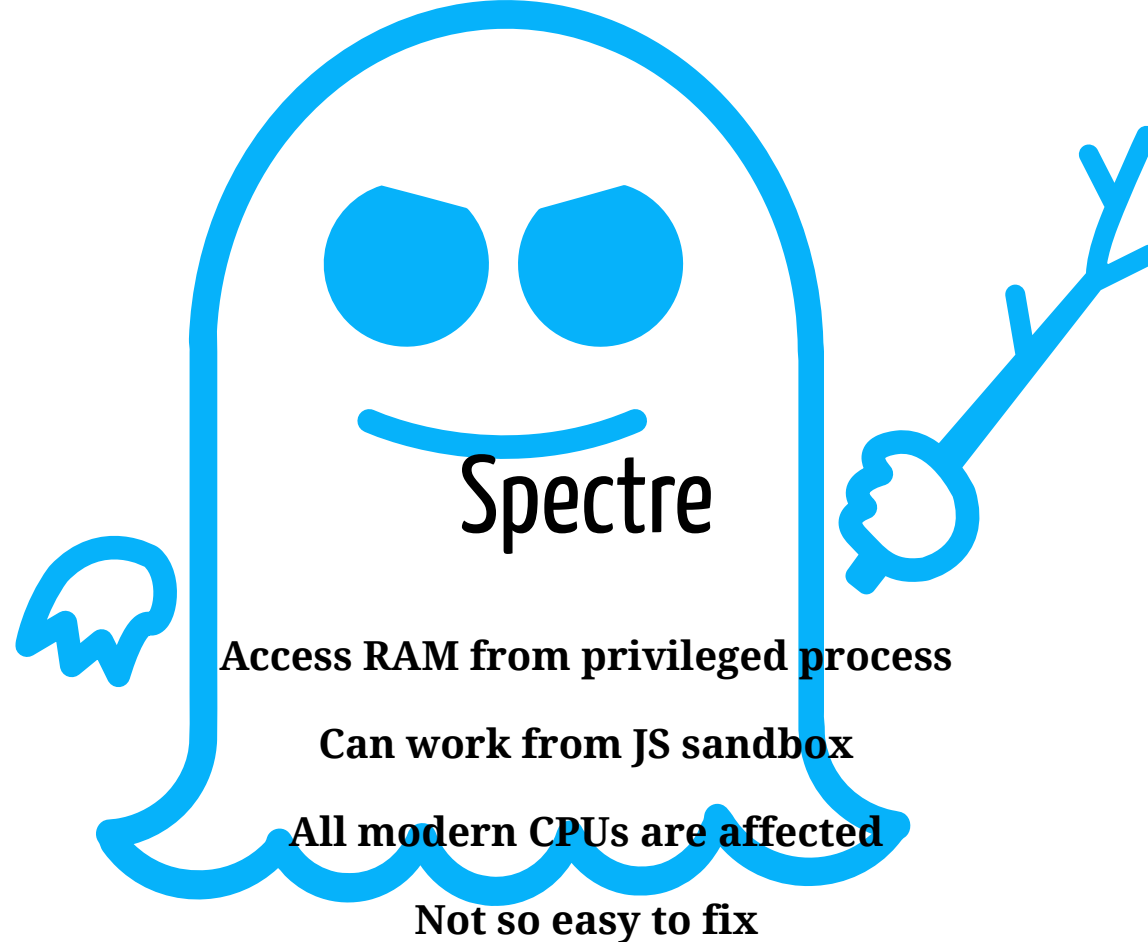**Branch prediction**

Speculative execution

Meltdown

Access any RAM directly

Intel-specific (but Apple also affected)

Easy to fix with OS

Spectre

Access RAM from privileged process

Can work from JS sandbox

All modern CPUs are affected

Not so easy to fix

SPECTRE

What can we do about it?

OS patches (KAISER)

Update browsers Firefox and Chrome have been fixed

What can we do about it?

Performance cost

Docker and Virtualization affected

So what now?

Military situational indicators progression

SNAFU

Situation Normal, All Fucked Up

Thing are running normally.

TARFUN

Things Are Really Fucked Up Now

Houston, we have a problem.

FUBAR

Fucked Up Beyond All Recognition

Burn it to the ground and start over from scratch; it's totally destroyed.

Questions?

Useful links

- https://www.youtube.com/watch?v=IPhvL3A-e6E

Most complete and user-friendly explanation in 48 mins

- https://www.youtube.com/watch?v=8FFSQwrLsfE

Most complete and non user-friendly explanation in 55 mins

- https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-heres-what-intel-apple-microsoft-others-are-doing-about-it/

Meltdown and Spectre: Here's what Intel, Apple, Microsoft, others are doing about it

- https://www.ivanti.com/blog/meltdown-spectre-need-know/

The impact and potential issues with current solutions

- https://gist.github.com/a0viedo/282f9fce9cfa7fecb8edced71451a77a

A gist of useful links about Meltdown and Spectre with official reports