Meltdown and Spectre

A Modern Processor Problem

Introduction

- This vulnerability has certainly made the news.
- It is absolutely not just a APPLE Problem per certain news reports!
- It is serious due to its scope but not the end of the world.
- It affects modern powerful microprocessor chips that use speculative execution to provide performance.
- It is not a operating system problem per se (Mac, IOS, Windows, Linux, Android, etc) problem but these systems will need updates to deal with the inability to retroactively fix and retrofit all the hardware.
- Intel, AMD, and ARM processors are affected. Macs and I devices don't use AMD processors.

What is it?

- I wish I could fully understand it myself. It is complex.
- Here is a general FAQ:

https://www.pcworld.com/article/3245606/security/intel-x86-cpu-kernel-bug-faq-how-it-affects-pc-mac.html

- Here is what Apple says about it.
  - I link and read the whole thing.
- https://support.apple.com/en-us/HT208394

Some more points:

- Meltdown affects Intel and some ARM chips
  - Apples IOS chips are ARM, and are affected
- Spectre affects all
- Spectre is hard to implement but to quote Bart Busschots it is "whack a mole" Todays fixes to Browsers helps, but it not to say its permanently fixed. A new vulnerability to imessage, or some other third party app a year from now will need to be patched.

Apple's Patches:

- If you have automatic updates turned on this should apply all needed patches. If you don't have them install automatically or worse have updates turned off then:
- High sierra OS 10.13.2 addressed some of the issues.
  - Supplemental update for 10.13.2 High sierra patched more.
  - Finally OSX 10.13.3 just released further adds to fixes.
- IOS 11.2.2 addressed some of the issues on IOS
  - IOS 11.2.5 patched more. (Tvos also updated)
- Safari 11.0.2 (now 11.0.3) took care of the browser. Chrome and Firefox have had updates
- Apple released two more updates for Sierra OS 10.12 and El Capitan 10.11

Apple's Patches: (cont'd)

- Sierra (10.12):

- https://support.apple.com/kb/DL1956

- El Capitan (10.11):

- https://support.apple.com/kb/DL1955

- This handles many 2007-2009 Macs

- Apple has not yet made any patches to 10.7.5 that would take care of the first Intel macs. Will they support EOL machines?

Apple's Patches: (cont'd)

- G3,G4, G5 Macs may or may not be vulnerable. One source said not affected, another researcher said G3, G4 lack to the power to exploit, maybe on G5 machines.

Conclusion:

- I've mentioned patching. But this vulnerability is not just patching.   Be careful about what you download. "Speeds up your mac 1000X and will prevent hardware failures"   Oh goody lets download it ….NOT
  - Macdownloader (state sponsored malware targeting US citizens) type of Malware etc
  - Word macro –viruses be careful on opening Word Docs in Microsoft word
- Security is not just Meltdown –Spectre…Plenty of earlier threats and there will be new ones in the future!