Technology Flash...

January 2, 2018

J.Gold Associates, LLC 6 Valentine Road, Northborough, MA 01532 USA
www.jgoldassociates.com +1-508-393-5294
Research, Analysis, Strategy, Insight

Meltdown and Spectre exploits: Cutting through the FUD

A Publication of J.Gold Associates

There is lots of information circulating about the new exploits of computer chips from Intel and others announced in the past few days. Some of it has been accurate and some has been sensationalist and overblown. There is much technical information with high level of details available for both Meltdown and Spectre, so I won't get into a lot of technical detail here. Rather, I'll focus on the higher level issues affecting business and personal computer users.

First, to be clear, these exploits affect all the major computer chip architectures. The major chip makers, AMD, ARM and Intel have decided to work together to mitigate the potential effects of a common enemy that affects most modern computer chips – a good sign for future industry collaboration. And all the major software vendors of Linux, Microsoft for Windows, Apple for MacOS, and virtualization software suppliers like VMware and Citrix have all collaborated to mitigate this threat. But what are the threats? There are potentially 3 different threats exposed in the disclosure, collectively described by Meltdown and Spectre.

> *"…The major chip makers, AMD, ARM and Intel have decided to work together to mitigate the potential effects of a common enemy that affects most modern computer chips… major software vendors of Linux, Microsoft for Windows, Apple for MacOS, and virtualization software suppliers like VMware and Citrix have all collaborated to mitigate this threat........"*

Meltdown and Spectre are not exactly the same, but they are related and use a similar exploit mechanism to gain access to computer data. Nearly all modern chip architectures from the major suppliers (Intel, AMD, ARM) are affected and this includes nearly all modern computer systems from data center to PC to smartphones. And it affects nearly all operating systems like Windows, Linux, MacOS and even Android, as well as virtualized environments like VMware and Citrix, but not lower level or real time operating systems (like QNX) that don't use this particular feature, nor in lower level controller chips used for IoT. Basically, the exploit involves reading memory locations that are supposed to be protected and reserved for use by the computer kernel. It exploits an architectural technique known as "speculative execution" which is a key feature of things like look-ahead instructions and data, which significantly improves computer performance.

With a potential to read kernel data, what's the real threat level behind Meltdown and Spectre? Let's look at what it is, what it's not, and what you should do about it.

What it is:

- It's an exploit, not a chip design flaw, operating against computer architecture that's been designed into chips for decades. It accesses protected areas of memory to potentially decode and read. While this may contain sensitive information like passwords, it also may simply be variable instructions and data from application processes that are not of much value.
- It has the potential to read protected memory locations used by the device and applications (including browsers) that store information in the kernel memory, including potentially sensitive data. It does not read memory in mass storage devices like disk drives. But it may not be possible to even read the captured data in real time as it requires understanding the relationship

between data locations which are highly variable and actual data content, and requires a good amount of processing/decoding.

- It must be run locally on the machine and must be loaded through some form of application. Therefore, it's not easy to do this via a "drive by attack" that does not launch a machine specific application targeted at this vulnerability.

What it's not:

- It does not allow take-over or modification of machines and operating systems, so it is not a traditional malware actor. This is important as it does not expose the machine to any modifications of its operations or "hijacking".
- It is not an easy thing to do as some have suggested. It takes a good deal of effort to access and discover the actual content of memory and make it meaningful, as mentioned earlier. For this reason, this is likely not a "high volume" approach to malware like more traditional approaches that take over the operation of the machine for nefarious purposes.
- It does not allow data access and retrieval of stored data sets on disk drives, (e.g., databases) like many normal malware attacks would, nor does it allow machine takeovers for DDOS attacks. So the actual risks to corporate or personal data are much more limited than typical of malware attacks that capture full content of mass storage systems.
- It's not something that smaller scale computers, like PCs and Smartphones, need to worry much about as the amount of effort involved would highly favor exploitation at large data center machines rather than personal machines. It's about "bang for the buck" for the hacker.

What's the risk?

To date there are no known uses of the exploit in the wild. And it's not as easy to deliver a payload to a machine to use this exploit as it is with more common malware that's sent via an email or errant application download. Further, all of the major OS vendors are patching their software to dramatically limit the ability of this exploit to cause harm, and firmware is being updated by the chip and machine vendors. So while there is a potential real risk, in my opinion it's not as great as many of the more traditional malware attacks we've seen in the recent past.

What should you do?

All the major OS and cloud companies are working on fixes for this vulnerability and have or are in process of providing software updates. It may be impossible to eliminate all risk without turning off some of the fundamental features of modern computers, like look ahead functions, which isn't practical. Even with the software patches, most users won't see a major impact on their programs, as it only affects memory access to the kernel system, and many apps only use that feature occasionally. Speculation that the patches will cause a 30% decline in performance is, in my opinion, highly overstated. I estimate for the average user on a PC, the performance degradation may not even be noticeable, or will likely be in the 3%-5% range. For large data centers where there are many operations to the kernel memory, the impact may be somewhat greater, but I still estimate it will be well under 10%, although for very large data sets, that may be negatively impactful.

Bottom Line: While these new exploits are troublesome, as are all potential security risks, users and organizations affected should not panic. Many of the fixes are already being implemented as software/firmware upgrades and should mitigate the vast majority of any potential exploitation. Future chips will also incorporate more protections against these exploits. But as with all major current and future architectures enhancements, there is no guarantee that everything will be 100% secure even though the chip, OS and app vendors do all they can to protect systems.

Jack Gold is the founder and principal analyst at J.Gold Associates, LLC., an information technology analyst firm based in Northborough, MA., covering the many aspects of business and consumer computing and emerging technologies. Follow him on Twitter @jckgld or LinkedIn at https://www.linkedin.com/in/jckgld.

"…… While these new exploits are troublesome, as are all potential security risks, users and organizations affected should not panic. Many of the fixes are already being implemented as software/firmware upgrades and should mitigate the vast majority of any potential exploitation…….."

J.Gold Associates

J.Gold Associates, LLC
6 Valentine Road
Northborough, MA 01532 USA

Phone:
+1-508-393-5294

Web:
www.jgoldassociates.com

Research, Analysis, Strategy, Insight