Newsletter – January 2018

Well, I was going to write about Net Neutrality, but… the recent revelations about the Intel, AMD, and ARM processor flaws have taken center stage. **This is the most serious security issue ever in the history of the personal computer and mobile devices.** Affecting virtually every processor made in the last 20 years, the "Meltdown" and "Spectre" processor hacks have the capability to bleed any information from the sacred and previously believed to be impenetrable processor cores.

Calm Down: let me say one thing before proceeding – there are no known hacks that are "out in the wild" as yet. The researchers who discovered the flaws worked closely with processor makers and software companies to get the fixes in place prior to informing the public (this keeps hackers in the dark as well). The hacks do work, but they exist only in the controlled environment of the research labs. For now.

Next, a short summary of how processors operate. Inside each processor, software programs allocate processor core time and memory to themselves. These reservations are "walled off" from other programs so that they do not interfere with each other, nor can other programs read information in reserved cores. This, for example, allows you to use Excel, Word, and your browser at the same time, but none of them can obtain information from each other unless you allow them to do so via copy/paste, download, or other transfer method you initiate. Further, this processor core isolation is the foundation of safe web surfing, as your browser theoretically does not allow interaction from within the core to the wider internet, again, unless you initiate the action.

Now we can describe what Meltdown and Spectre do. Simply put, they take advantage of a flaw in the processor designs to break through the walled-off core isolation and read whatever data is in active usage. The design flaw is one that allows the processor to "skip ahead" and make calculations based on a prediction of most likely result. That speeds up processing overall, and it has been a great innovation. But the method used is a hardware flaw, not a software flaw, and that is an important difference. Hardware flaws are almost impossible to rectify without replacing the hardware. **Wait, what did I say?** Yep, to be completely 100% certain of eliminating this flaw, everyone will have to buy new processors/computers that do not contain it. How's that for a shocker?

Next, think about the ramifications across the wider internet: can you imagine every computer the world over being replaced? Every government agency, every web operator, every network provider: **everything must be replaced.** Well, in a practical sense, that's not going to happen, at least not for years, so the short-term answer is a software patch that will partially fix the problem, but there are some drawbacks. The software patch disables the hardware flaw, but doing so slows down the processor significantly. The processor can no longer "skip ahead" to predict an answer, and will be slower as a result. But that is what we will have to live with.

Are individuals in immediate danger, and what should I do? The first thing to do is the old, tried and true advice: don't surf to sketchy websites, don't click links in emails you were not expecting to receive, don't open attachments, and don't download "free stuff" from the internet. The second thing to do is make sure your computers are up-to-date with the latest security patches. That's all we can do until more is known…
-John Becker