Newsletter – January 2018, Issue #2
Processor Flaw Update

I dislike being the messenger when it's bad news… So let's start with Good News:

Product Of The Month: ClipGrab
My wife recently needed to embed a YouTube video into a PowerPoint presentation. It's embarrassing to say how long I spent trying to get it to work. I ended up with either a clip that showed video but no sound, or sound but no video. I finally happened upon ClipGrab, a wonderful little program that easily and flawlessly downloaded the clip I wanted. It's free, but you can donate to the cause… www.clipgrab.org

The previous issue dealt with the processor flaw discovered late in 2017, and "patched" by making changes to operating system software in early January 2018. I related that it is a big deal, and despite the efforts by Intel, AMD, and other processor manufacturers to downplay the flaw, my assertion that you cannot fix hardware flaws with software remains on the table. A "software patch" is like putting a Band-Aid on a hole in your car tire. It might hold for awhile, but you cannot consider it "fixed".

Now that we have two weeks of experience under our belts, I will detail why my assertion holds true:

#1: The software patch reduces performance: Depending on what you are doing with the computer, your performance hit is between 2% up to 10%. It's like an 8-cylinder engine running on 7 cylinders (or a 24-cell battery-electric car running on 20 cells?). You are not getting the performance you paid for.

#2: The patches break other things: many organizations are reporting unexplained reboots or shutdowns after the patches are applied. These are not from gamers running bleeding edge games, these reports are from businesses running servers that were stable prior to the patch, but are not now.

#3: No guarantee that the Patch will stay "Patched": Now that the patch has been released to the public, it has been thoroughly dissected and reverse-engineered by legitimate researchers, and most certainly the dark side hackers. That in turn reveals the exact method used to stop the flaw, *and also how to enable it.* That knowledge can be re-used to engineer viruses or other hacks to *disable the patch*, and then we are back where we started.

#4: The Wild Card: taking point #3 a step further, (and perhaps into "tin foil hat" territory) the cat is out of the bag on how to leverage hardware issues to exploit weaknesses in designs. Today it is processor flaws, tomorrow it might be the same type of hack on video cards – an area ripe for exploitation. Think about it: the video card in your computer also has a processor – a video flaw can be used to mirror your computer screen to another machine without your knowledge. OK, I'll take off my tin foil hat now.

The good news: there are no known attacks that are out in public yet. All this has stayed safely inside the research environment so far. However, it does not hurt to think ahead and be prepared…
Reminder: My Newsletter Archive: http://medofficesystems.com/newsletter_tips.htm
-John Becker