Schneier on Security

Spectre and Meltdown Attacks Against Microprocessors

The security of pretty much every computer on the planet has just gotten a lot worse, and the only real solution -- which of course is not a solution -- is to throw them all away and buy new ones.

On Wednesday, researchers just announced a series of major security vulnerabilities in the microprocessors at the heart of the world's computers for the past 15-20 years. They've been named Spectre and Meltdown, and they have to do with manipulating different ways processors optimize performance by rearranging the order of instructions or performing different instructions in parallel. An attacker who controls one process on a system can use the vulnerabilities to steal secrets elsewhere on the computer. (The research papers are here and here.)

This means that a malicious app on your phone could steal data from your other apps. Or a malicious program on your computer -- maybe one running in a browser window from that sketchy site you're visiting, or as a result of a phishing attack -- can steal data elsewhere on your machine. Cloud services, which often share machines amongst several customers, are especially vulnerable. This affects corporate applications running on cloud infrastructure, and end-user cloud applications like Google Drive. Someone can run a process in the cloud and steal data from every other users on the same hardware.

Information about these flaws has been secretly circulating amongst the major IT companies for months as they researched the ramifications and coordinated updates. The details were supposed to be released next week, but the story broke early and everyone is scrambling. By now all the major cloud vendors have patched their systems against the vulnerabilities that can be patched against.

"Throw it away and buy a new one" is ridiculous security advice, but it's what US-CERT recommends. It is also unworkable. The problem is that there isn't anything to buy that isn't vulnerable. Pretty much every major processor made in the past 20 years is vulnerable to some flavor of these vulnerabilities. Patching against Meltdown can degrade performance by almost a third. And there's no patch for Spectre; the microprocessors have to be redesigned to prevent the attack, and that will take years. (Here's a running list of who's patched what.)

This is bad, but expect it more and more. Several trends are converging in a way that makes our current system of patching security vulnerabilities harder to implement.

The first is that these vulnerabilities affect embedded computers in consumer devices. Unlike our computer and phones, these systems are designed and produced at a lower profit margin with less engineering expertise. There aren't security teams on call to write patches, and there often aren't mechanisms to push patches onto the devices. We're already seeing this with home routers, digital video recorders, and webcams. The vulnerability that allowed them to be taken over by the Mirai botnet last August simply can't be fixed.

The second is that some of the patches require updating the computer's firmware. This is much harder to walk consumers through, and is more likely to permanently brick the device if something goes wrong. It also requires more coordination. In November, Intel released a firmware update to fix a vulnerability in its Management Engine (ME): another flaw in its microprocessors. But it couldn't get that update directly to users; it had to work with the individual hardware companies, and some of them just weren't capable of getting the update to their customers.

We're already seeing this. Some patches require users to disable the computer's password, which means organizations can't automate the patch. Some anti-virus software blocks the patch, or -- worse -- crashes the computer. This results in a three-step process: patch your andi-virus software, patch your operating system, and *then* patch the computer's firmware.

The final reason is the nature of these vulnerabilities themselves. These aren't normal software vulnerabilities, where a patch fixes the problem and everyone can move on. These vulnerabilities are in the fundamentals of how the microprocessor operates.

It shouldn't be surprising that microprocessor designers have been building insecure hardware for 20 years. What's surprising is that it took 20 years to discover it. In their rush to make computers faster, they weren't thinking about security. They didn't have the expertise to find these vulnerabilities. And those who did were too busy finding normal software vulnerabilities to examine microprocessors. Security researchers are starting to look more closely at these systems, so expect to hear about more vulnerabilities along these lines.

Spectre and Meltdown are pretty catastrophic vulnerabilities, but they only affect the confidentiality of data. Now that they -- and the research into the Intel ME vulnerability -- have shown researchers where to look, more is coming -- and what they'll find will be worse than either Spectre or Meltdown. There will be vulnerabilities that will allow attackers to manipulate or delete data across processes, potentially fatal in the computers controlling our cars or implanted medical devices. These will be similarly impossible to fix, and the only strategy will be to throw our devices away and buy new ones.

This isn't to say you should immediately turn your computers and phones off and not use them for a few years. For the average user, this is just another attack method amongst many. All the major vendors are working on patches and workarounds for the attacks they can mitigate. All the normal security advice still applies: watch for phishing attacks, don't click on strange e-mail attachments, don't visit sketchy websites that might run malware on your browser, patch your systems regularly, and generally be careful on the Internet.

You probably won't notice that performance hit once Meltdown is patched, except maybe in backup programs and networking applications. Embedded systems that do only one task, like your programmable thermostat or the computer in your refrigerator, are unaffected. Small microprocessors that don't do all of the vulnerable fancy performance tricks are unaffected. Browsers will figure out how to mitigate this in software. Overall, the security of the average Internet-of-Things device is so bad that this attack is in the noise compared to the previously known risks.

It's a much bigger problem for cloud vendors; the performance hit will be expensive, but I expect that they'll figure out some clever way of detecting and blocking the attacks. All in all, as bad as Spectre and Meltdown are, I think we got lucky.

But more are coming, and they'll be worse. 2018 will be the year of microprocessor vulnerabilities, and it's going to be a wild ride.

Note: A shorter version of this essay previously appeared on CNN.com. My previous blog post on this topic contains additional links.

Posted on January 5, 2018 at 2:22 PM • 77 Comments

Comments

Jonathan Wilson • January 5, 2018 2:38 PM

In a world where even a supposedly safe website can be serving up nasty code thanks to a dodgy ad, staying away from all questionable code is hard. Malvertising is the #1 reason I run an ad blocker.

Jonathan • January 5, 2018 3:08 PM

As you say, Bruce: unsurprising. For years, CPU hardware problems have largely flown under the radar for most people. They are used to thinking of software as the buggy stuff that gets updated, and the hardware as the rock solid trustworthy side. Most people are unaware, for example, than 2015-era i7 processors have roughly 50 pages of "errata" (hardware bugs).

And even a lot of "software" updates are actually CPU microcode updates, or workarounds for hardware errata (many of those 50 pages of bugs have no workarounds listed).

But today's digital chips, like CPUs, usually start out as computer code written in VHDL or Verilog. They are among the most complex and intricate devices ever created. And hardware vendors are under no less pressure to get product out the door than are software vendors. Bugs -- even catastrophic -- should be unsurprising.

Jonathan • January 5, 2018 3:12 PM

One additional comment: Google's Project Zero, which led the way discovering these bugs, did absolutely brilliant work on them. They are wizards, and I'm glad they're on our side.

---

tobi • January 5, 2018 3:21 PM

Maybe it's in the noise for automated attacks but is it maybe more relevant for targeted attacks against individuals or corporations?

Also it seems to me that cloud security is restored by patching against Meltdown. Spectre should not apply to cloud because tenants do not share memory pages, right? And the hypervisor does not share pages with the tenant.

Grauhut • January 5, 2018 3:37 PM

@Bruce: We shouldn't believe in luck!