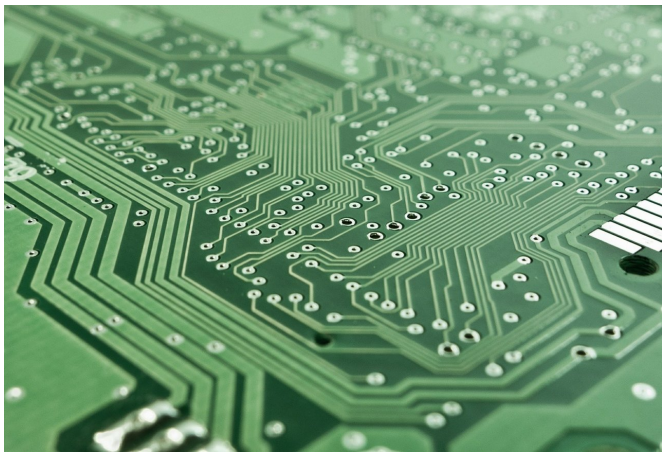
Are you vulnerable to newly discovered online security risks?

9 January 2018, by Lois Yoksoulian



Credit: CC0 Public Domain

Last week, experts discovered two serious computer security flaws that could leave nearly all computer users vulnerable to hacking of personal information while online. The culprits, called Meltdown and Spectre, could wreak havoc on personal security if ignored. Physical Sciences editor Lois Yoksoulian spoke with computer science professor Chris Fletcher about the issue.

What exactly are Meltdown and Spectre?

Meltdown and Spectre are new vulnerabilities that allow hackers to steal your private information through malware. The culprit is a hardware feature called "speculative execution," a feature found in modern processor chips. Speculative execution is a performance technique where processors predict and perform work that they think will be needed in the future.

Suppose you are logging into your computer account, and that you are currently typing in your password. With speculative execution, your processor can predict that you correctly type your password, thereby allowing it to speculatively obtain your account details ahead of time. If this really is your account, and the prediction is correct, your account information appears faster. If this is not your account, and the prediction is incorrect, your processor will throw out the speculative work. Despite this, however, the account details were prepared and lived on your computer for a short period. The Meltdown and Spectre vulnerabilities are ways for hackers to grab this information before it gets thrown out.

How were these vulnerabilities discovered?

Meltdown and Spectre were discovered independently by several teams of researchers in academia and industry, including Google, Cyberus Technology, the University of Graz and several others. These teams became aware of each other's work through their responsible disclosure of the vulnerabilities to Intel, which worked with its major clients (Microsoft, Amazon, etc.) to prepare a software patch, before the attacks were publicly announced last week.

Right now, the patch defends against Meltdown but not for all forms of Spectre. This was a critical first step. Meltdown is the more immediate danger in that it is relatively easy for a hacker to exploit. Spectre is harder to exploit but also harder to mitigate. As it stands, Meltdown only impacts Intel processors, whereas Spectre impacts processors from Intel as well as those from other vendors such as ARM and AMD.

Is it true that everybody is vulnerable?

Yes. Hardware speculative execution has been around in commercial chips since the 1990s. Nowadays, everyone (Intel, AMD, ARM, etc.) uses it for performance reasons.

What can everyday computer and mobile device users do to protect themselves?

The most important action to take is to check and keep rechecking all of your devices – laptops, desktops, mobile phones – for security updates. The major operating system vendors are pushing out the software patch for Meltdown, but not all vendors are there yet. Keep an eye out for updates in the next week. Even better, check online as to whether your current operating system is sufficiently up to date. There have been reports about third-party software that have been inadvertently blocking the updates. So, it is good to be proactive.

A hacker simply needs to run malware on your machine to perform the attacks. The easiest way for malware to creep into your system is through your web browser – for example, if you accidentally visit a malicious website due to phishing. Therefore, in the immediate future, it is also a good idea to be extra vigilant about which web pages you visit and which links you follow.

Even if there is a fix now, are future devices at risk?

Unfortunately, speculative execution is here to stay, as it is too vital to a processor's performance. Furthermore, Meltdown and Spectre are only the first attacks that exploit speculative execution. Even after fixing these two, it is likely that new speculative execution-based attacks will crop up in the future.

The recent events are also a wake-up call that we must take what are called "microarchitectural side channel attacks" more seriously. MASCAs are an essential ingredient in both Meltdown and Spectre, and have been an active area of research for at least the last decade. Over the years, there has been a steady trickle of malicious things done with MASCAs (for example, they can steal a user's keystrokes or password), but these occurred mostly in a lab setting due to the steep requirements they imposed on attackers. One of the novelties in Meltdown and Spectre is to amplify the damage of MASCAs to steal more data than was possible before.

Thus, a compelling direction to protect future systems is to implement protection against MASCAs. MASCA protection and speculative execution are not mutually exclusive. Multiple research proposals from the computer architecture and security communities support both. The catch is that for real, long-term protection, chip vendors must commit to broad MASCA protection. Point defenses against specific MASCAs are doomed to fail: Attackers will simply find another MASCA to exploit. We must invest in provable protections against broad classes of MASCAs, without making assumptions about which MASCA the attacker will try to use next.

Provided by University of Illinois at Urbana-Champaign

APA citation: Are you vulnerable to newly discovered online security risks? (2018, January 9) retrieved 26 November 2022 from https://techxplore.com/news/2018-01-vulnerable-newly-online.html