Spectre and Meltdown

**Spectre** and **Meltdown** are the names given to different variants of the same fundamental underlying vulnerability that affects nearly every computer chip manufactured in the last 20 years and could, if exploited, allow attackers to get access to data previously considered completely protected. Security researchers discovered the flaws late in 2017 and publicized them in early 2018. Technically, there are three variations on the vulnerability, each given its own  CVE number; two of those variants are grouped together as  **Spectre** and the third is dubbed  **Meltdown**.

All of the variants of this underlying vulnerability involve a malicious program gaining access to data that it shouldn't have the right to see, and do so by exploiting two important techniques used to speed up computer chips, called  speculative execution and  caching.

If you want a much more technical description of how Spectre and Meltdown work, you should check out the post on Google’s project zero site that was most of the world's introduction to it. To keep it short and simple, both Spectre and Meltdown could allow potential attackers to get access to data they shouldn't have access to using the techniques outlined above, but their effects are somewhat different.

* Meltdown got its name because it “melts” security boundaries normally enforced by hardware. By exploiting Meltdown, an attacker can use a program running on a machine to gain access to data from all over that machine that the program shouldn't normally be able to see, including data belonging to other programs and data that only administrators should have access to. Meltdown doesn't require too much knowledge of how the program the attacker hijacks works, but it only works with specific kinds of Intel chips. This is a pretty severe problem but fixes are being rolled out.
* By exploiting the Spectre variants, an attacker can make a program reveal some of its own data that should have been kept secret. It requires more intimate knowledge of the victim program's inner workings, and doesn't allow access to other programs' data, but will also work on just about any computer chip out there. Spectre's name come from speculative execution but also derives from the fact that it will be much trickier to stop — while patches are starting to become available, other attacks in the same family will no doubt be discovered. That's the other reason for the name: Spectre will be haunting us for some time

Spectre and Meltdown both open up possibilities for dangerous attacks. For instance, JavaScript code on a website could use Spectre to trick a web browser into revealing user and password information. Attackers could exploit Meltdown to view data owned by other users and even other virtual servers hosted on the same hardware, which is potentially disastrous for cloud computing hosts.

But beyond the potential specific attacks themselves lies the fact that the flaws are fundamental to the hardware platforms running beneath the software we use every day. Even code that is formally secure as written turns out to be vulnerable, because the assumptions underlying the security processes built into the code — indeed, built into all of computer programming — have turned out to be false.

The fundamental vulnerability exists at the hardware level and cannot be patched. However, most vendors are releasing software patches that work around the problems. The KAISER patch, developed coincidentally in 2017 to improve Linux security, actually has the side effect of preventing meltdown attacks. Major cloud vendors have by and large patched their servers. Patches have already been rolled out by Intel, Microsoft, Apple, and Google (see more below) and more are on the way. CSO's J.M. Popup has a good roundup of steps you should take in the short term. Rendition Infosec also has a great resource on establishing a strategy for your organization that will, among other things, harden your systems and practices to prevent further damage if you do fall victim to an attack exploiting Spectre or Meltdown.

Since JavaScript in the browser is one particularly dangerous vector for Spectre attacks, it's also important keep your browsers up to date.

Notably, older systems, particularly Windows XP, will almost certainly never be patched. Also left in the lurch are the millions of Third-party. Low cost android phones that don’t get security updates from google, many of which are not particularly old.

Researchers, chipmakers and computer companies all say there are no known examples of hackers using these weaknesses to attack a computer. However, now that the details of the design flaws and how to exploit them are publicly available, the chances of hackers using them are much higher.

The good news is that hackers would first need to install malicious software on your computer to take advantage of these flaws. That means they need to select their targets and hack each one of them before running a sophisticated attack to steal a computer's sensitive information.