INTERACTIVE SESSION TECHNOLOGY

Meltdown and Spectre Haunt the World's Computers

In early January 2018, computer users all over the world were shocked to learn that nearly every computer chip manufactured in the last 20 years contained fundamental security flaws that make it possible for attackers to obtain access to data that were thought to be completely protected. Security researchers had discovered the flaws in late 2017. The flaws arise from features built into the chips that help them run faster. The vulnerability enables a malicious program to gain access to data it should never be able to see.

There are two specific variations of these flaws, called Meltdown and Spectre. Meltdown was so named because it "melts" security boundaries normally enforced by hardware. By exploiting Meltdown, an attacker can use a program running on a computer 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 to which only administrators should have access. (A system administrator is responsible for the upkeep, configuration, and reliable operation of computer systems.) Meltdown only affects specific kinds of Intel chips produced since 1995.

Spectre is not manufacturer-specific and affects nearly all modern processors. It requires more intimate knowledge of the victim program's inner workings. Spectre's name comes from speculative execution, in which a chip is able to start work on predicted future operations in order to work faster. In this case, the system is tricked into incorrectly anticipating application behavior. The name also suggests that Spectre will be much more difficult to neutralize. Other attacks in the same family will no doubt be discovered, and Spectre will be haunting us for some time.

With both Meltdown and Spectre, an attacker can make a program reveal some of its own data that should have been kept secret. For example, Spectre could harness JavaScript code on a website to trick a web browser into revealing user and password information. Meltdown could be exploited to view data owned by other users and also virtual servers hosted on the same hardware, which is especially dangerous for cloud computing host computers. The most worrisome aspect of Meltdown and Spectre is that security vulnerabilities are not from flawed software but from the fundamental design of hardware platforms beneath the software.

There is no evidence that Spectre and Meltdown have been exploited, but this would be difficult to detect. Moreover, the security flaws are so fundamental and widespread that they could become catastrophic, especially for cloud computing services where many users share machines. According to researchers at global security software firm McAfee, these vulnerabilities are especially attractive to malicious actors because the attack surface is so unprecedented and the impacts of leaking highly sensitive data are so harmful. According to Forester, performance of laptops, desktops, tablets, and smartphones will be less affected. The fundamental vulnerability behind Meltdown and Spectre is at the hardware level, and thus cannot be patched directly. Technology software vendors are only able to release software fixes that work around the problems. Such fixes mitigate vulnerabilities by altering or disabling the way software code makes use of speculative execution and caching features built into the underlying hardware. (Caching is a technique to speed computer memory access by locating a small amount of memory storage on the CPU chip rather than from a separate RAM chip for memory.) Since these features were designed to improve system performance, working around them can slow systems down. Experts initially predicted system performance could be degraded as much as 30 percent, but a slowdown of 5 to 10 percent seems more typical.

Major software vendors have rolled out workaround patches. Cloud vendors have taken measures to patch their underlying infrastructures, with their customers expected to install the patches for their operating systems and applications. Microsoft released operating system patches for Windows 7 and all later versions, which also apply to Microsoft's Internet Explorer and Edge browsers. Apple released patched versions of its Safari browser and iOS, macOS, and tvOS operating systems. Google provided a list of which Chromebook models will or won't need patches and released a patch for its Chrome browser. Older operating systems such as Windows XP and millions of third-party low-cost Android phones that

don't get security updates from Google will most likely never be patched. Organizations should apply updates and patches to browser software as soon as they are available. And since these vulnerabilities could enable attackers to steal passwords from user device memory when running JavaScript from a web page, it is recommended that users be instructed to always close their web browsers when not in use. Forrester also recommends that enterprises should use other techniques to protect data from users and organizations that have not applied the fixes.

However, the only way to truly fix Meltdown and Spectre is to replace affected processors. Redesigning and producing new processors and architectures may take five to ten years to hit the market. If anything good can be said about Spectre and Meltdown, it is that they have focused more global attention on software and hardware security and the need to develop more robust system architectures for secure computing.

Sources: Josh Fruhlinger, "Spectre and Meltdown Explained: What They Are, How They Work, What's at Risk," *CSO*, January 15, 2018; Warwick Ashford, "Meltdown and Spectre a Big Deal for Enterprises," *Computer Weekly*, January 9, 2018; Laura Hautala, "Spectre and Meltdown: Details You Need on Those Big Chip Flaws," CNET, January 8, 2018.

CASE STUDY QUESTIONS

1. How dangerous are Spectre and Meltdown? Explain your answer.
2. Compare the threats of Spectre and Meltdown to cloud computing centers, corporate data centers, and individual computer and smartphone users.
3. How would you protect against Spectre and Meltdown if you were running a public cloud computing center, if you ran a corporate data center, and if you were an individual computer user?