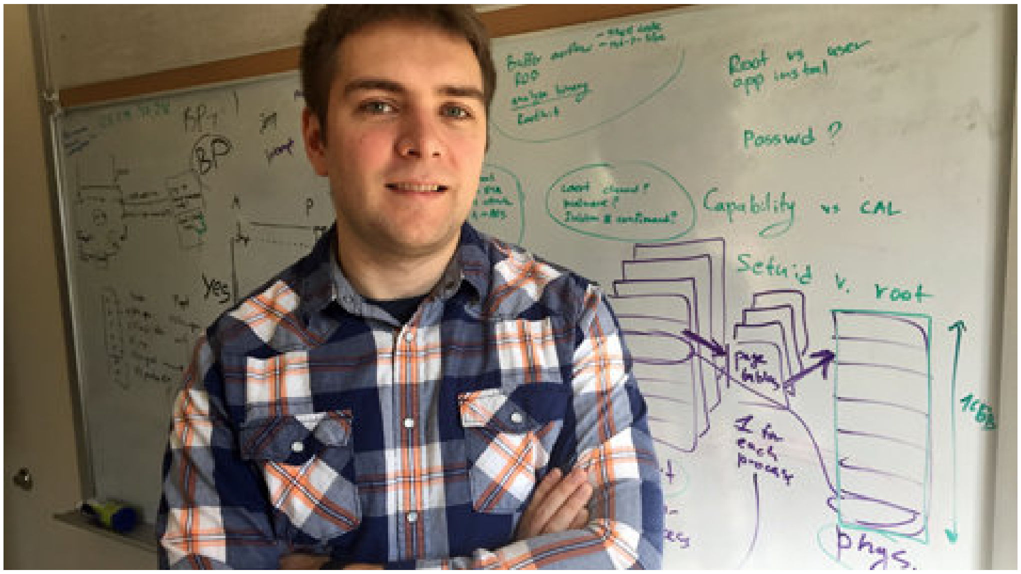
PHYS.ORG

Exposing the biggest computer chip vulnerability ever discovered

March 13 2018, by Adrienne Berard



Dmitry Evtyushkin, an assistant professor in William & Mary's Department of Computer Science, has been studying the security vulnerabilities of speculative execution. Credit: Adrienne Berard

The threat started making headlines around New Years. Publications around the globe warned of the biggest computer chip vulnerability ever discovered, a series of security flaws affecting any device with a microprocessor—from laptops to smartphones.

Researchers had found that in an effort to make computer chips more efficient, major manufacturers had inadvertently inserted an opening that would allow hackers to spy on sensitive data. In two papers that were published on Jan. 3, researchers coined the cyber security threats Meltdown and Spectre.

The name Meltdown was chosen for the attack's ability to "melt" the security system typically enforced by a processor's hardware. The name Spectre was based on the root cause of the security vulnerability, speculative execution, a speed-enhancing technique in which the processor tries to predict what part of code it will be required to execute next and starts executing it. And, much like a real spectre, the attack is nearly impossible to detect.

By the end of January, hardware companies like Intel, ARM Holdings Plc. and Advanced Micro Devices Inc. had released microcode updates to address the vulnerabilities. The companies also worked with operating systems developers, such as Windows and Linux, to design and release software updates. The flaws were physical, part of computer processing hardware. Entirely eliminating the problem would require modifying millions of computer chips.

Instead, developers and manufacturers opted to try their hand at fixing hardware flaws with software updates. The updates slowed performance and, in some cases, made systems inoperable, but the coordinated effort appeared to have been successful in guarding against Meltdown and lowering vulnerability to a Spectre attack.

The world quickly moved on, but Dmitry Evtyushkin couldn't. He had known about Spectre-like processor flaws for years. In fact, his research had helped shine a light on them in the first place. And Spectre, like its name, still lurks out there.

"Researchers still are not completely sure what the real impact of Spectre is," said Evtyushkin, an assistant professor in William & Mary's

Department of Computer Science. "They don't know the full scope of what they're dealing with. There are so many different processors and so many different ways of exploiting this type of vulnerability."

Think of a Spectre attack as a kind of sonar inside a computer. In order to see how the processing works, an attacker bounces programs off one another and maps a picture based on those collisions. The attacker then uses that picture, as well as other side effects from the collisions, to gain access to sensitive data inside the computer.

"We have different processes that are responsible for different activities," Evtyushkin said. "You can think about them as your apps. For example, you have your email client, your password manager, your games. All of them need to be isolated. They shouldn't interfere with each other."

In 2016, while completing his Ph.D. at Binghamton University, Evtyushkin and two other researchers found a way to force processes to interfere. Their study, titled "Jump Over ASLR: Attacking the Branch Predictor to Bypass ASLR," was part of a collection of research that detailed processor flaws similar to those shown in studies about Meltdown and Spectre.

"I discovered that it is possible to create collisions inside these multiple domains," Evtyushkin said, "which contributes to the discovery of memory layout."

Computer systems are designed to make a program's memory layout extremely hard to find. It's hidden through a hardening technique known as Address Space Layout Randomization (ASLR). The security measure protects a program's memory structure by randomizing positions of key program components, making it next to impossible for an attacker to know the specific addresses where those components are located. The

ASLR is like a combination of a safe. An attack that gets through the ASLR would reveal a program's entire data structure – every piece of information it contains.

Evtyushkin found that a hacker could bypass the ASLR using a central component of computer chip hardware, the Branch Predictor. The BP was introduced to make computer processors – or CPUs – operate more efficiently by streamlining the way programs run. When a program is executed, it is sent along a path known as a branch. The first time a program is executed, the processor can't figure out the branch's final target. So it relies on a hardware mechanism, the BP, which predicts a target based on previous branch behavior.

If attackers gain access to the BP, they can control how branches are handled by the processor and cause all kinds of collisions. A knowledgeable attacker can detect such collisions and bypass the randomization-based protection that hides a program's layout.

"I discovered that many mechanisms in today's computers are shared between different programs," Evtyushkin said. "An attacker can execute code that causes changes inside internal data structures in the hardware. By doing this, they can either detect branch instructions in a victim program or trigger some speculative execution in a way that it starts to leak security sensitive data."

In the controlled environment of the lab, Evtyushkin and his team executed a series of attacks through the BP. In December 2016, the team published their results. Their work became part of an international body of research large enough to create a surge of global media attention.

"This design flaw was there for a long time and I just discovered one way to use it," Evtyushkin said. "There are other ways to manipulate speculative execution, which turn out to be more serious in terms of security."

Since publishing his findings in 2016, Evtyushkin has continued researching Branch Predictors. His current area of focus is another part of the BP's job: telling programs which direction to take. The specifics of his research cannot be disclosed until a paper on his work is released at the end of March. He said Intel has been notified about the flaws he's discovered and is reviewing the research before the paper is released.

Evtyushkin is not optimistic about a quick fix. He, along with scores of other researchers, has spent the past several years telling hardware manufacturers they need to redesign their processors in order to solve security flaws. Currently, the companies have released a few software updates, but the hardware has not been updated to address the problem. Evtyushkin says there needs to be a broad, systematic fix to address multiple issues in modern hardware design.

"This whole culture of prioritizing performance, rather than security, is to blame," Evtyushkin said. "There is high competition in computer hardware production. Developers want to make faster chips, so they have to add aggressive speculative execution. They are giving up on security checks in order to make it fast."

On the bright side, there are no known incidents of Spectre-type attacks, but Evtyushkin says an attack could occur without the knowledge of even a savvy operator. A Spectre attack can come in through myriad of different avenues such as a website, a file download, a cell phone application or a media player. Once it's in, it's invisible.

"One of the problems with Spectre is that it's completely silent," Evtyushkin said. "You don't see anything happening. Compared to traditional attacks, where an application usually crashes and you can see the damage, with microarchitecture attacks you won't see it or know it happened."

To guard yourself against any kind of attack, Evtyushkin encourages safe computing practices such as not executing untrusted code and regularly updating your systems.

"Usually, the people who are responsible for these updates know more about vulnerabilities and hopefully can do something about it," Evtyushkin said.

Evtyushkin says his work is bringing awareness and eventually the required hardware updates will follow. He's currently working with collaborators to develop more systemic protection methods, such as restructuring speculative execution and Branch Predictor hardware to make it more secure while maintaining high performance.

"This research used to be considered extremely geeky, but now the public is paying attention to it," Evtyushkin said. "It's helping address the problem, because everybody knows about it. It motivates all of these big companies to take things more seriously."

Provided by The College of William & Mary

Citation: Exposing the biggest computer chip vulnerability ever discovered (2018, March 13) retrieved 20 March 2024 from https://phys.org/news/2018-03-exposing-biggest-chip-vulnerability.html