Apple, Android and PC chip problem – why your smartphone and laptop are so at risk

January 5 2018, by Siraj Ahmed Shaikh

Credit: Yan Krukau from Pexels

Less than a week into 2018 and we may have already seen the year's biggest technology story. Researchers have identified a security flaw in the computer processors made by three of the world's biggest chip

designers, Intel, AMD and ARM, and a second flaw in Intel chips. This means that almost every smartphone, tablet, laptop and business computer in the world could be vulnerable to having sensitive data including passwords stolen. The cloud servers that store websites and other internet data are also at risk.

This is one of the biggest cyber security vulnerabilities we're ever seen in terms of the potential impact to personal, business and infrastructure computer systems. What's more, because the flaw is located in such a fundamental part of the computer, there's no way to know whether or not a machine has been targeted and what data might have been accessed.

Both the main flaw (Spectre), and the Intel-only flaw (Meltdown) have been created by a design technique intended to enhance the chips' performance known as "speculative execution". The problem means hackers can access parts of the computer's memory that should be inaccessible. Sensitive data including passwords, email, documents and photos could all be at risk.

Most cyber attacks involve finding a flaw in a computer's software that allows hackers to access the machine's memory or operating system. For example, in 2017 an attack known as "WannaCry" exploited a flaw in older versions of Windows. It affected around 300,000 computers in 150 countries and had a devastating effect on businesses and organisations including the UK's National Health Service (NHS).

But the Spectre and Meltdown flaws could let hackers cut through all the layers of software to violate the very heart of a computer, the processor chip that powers its fundamental workings. Because similar designs are used by all the major chip makers, almost every computer in the world could be affected, from Apple iPhones and Android devices, to MacBooks, large desktop PCs and internet servers.

The process is also so fundamental that it doesn't create any log of its operations, meaning there is no record of whether a particular chip has been hacked or not. This makes it harder to spot cyber attacks at an early stage in order to prevent them happening again, or to investigate what data might have been accessed or stolen.

Luckily, tech companies have already begun releasing software patches that they say will solve the problems without a significant impact on performance. But some have claimed any fix could dramatically slow down computer processing speed. We will have to wait to see the long-term impact.

Responsible disclosure

The story also raises an important issue about the responsible disclosure of such security flaws. Reports suggest the industry has known of the problem for months but only limited details have been disclosed so far. You could argue that consumers have the right to know about such flaws as soon as they are discovered so they can try to protect their data. Of course, the problem is this could end up fuelling cyber attacks by also making hackers aware of the flaw.

In the past, this debate has forced tech companies to use the law to prevent researchers disclosing security problems. For example, scientists from the University of Birmingham faced a legal injunction from car manufacturer Volkswagen stopping them publishing details of flaws in car keyless entry systems.

The preferred route is "responsible disclosure". When researchers discover a problem, they tell a small number of relevant people who can then work on a solution. The manufacturer can then reveal the problem to the public once the solution is ready, minimising the potential for hacking and damage to the company's share price.

In this case, a researcher at Google who found the flaws seems to have alerted Intel in June 2017, and the two companies had been planning on announcing a fix. But details of the flaw were then published by technology website The Register, forcing the firms to reveal what they knew earlier than planned, and hitting Intel's share price. While this kind of revelation arguably undermines responsible disclosure, the counter argument is that it forces manufacturers to fix the problem faster.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation