# Microprocessor designers realize security must be a primary concern

July 18 2018, by Mark Hempstead


Credit: Jorge Jesus from Pexels

Computers' amazing abilities to entertain people, help them work, and

even respond to voice commands are, at their heart, the results of decades of technological development and innovation in microprocessor design. Under constant pressure to extract more computing performance from smaller and more energy-efficient components, chip architects have invented a dizzying array of tricks and gadgets that make computers faster. But 50 years after the founding of Intel, engineers have begun to second-guess many of the chip-making industry's design techniques.

Recently, security researchers have found that some innovations have let secrets flow freely out of computer hardware the same way software vulnerabilities have led to cyberattacks and data breaches. The best known recent examples were the chip flaws nicknamed Spectre and Meltdown that affected billions of computers, smartphones and other electronic devices. On July 10, researchers announced they discovered new variants of those flaws exploiting the same fundamental leaks in the majority of microprocessors manufactured within the last 20 years.

This realization has led to calls from microchip industry leaders, including icons John Hennessy and David Patterson, for a complete rethinking of computer architecture to put security first. I have been a researcher in the computer architecture field for 15 years – as a graduate student and professor, with stints in industry research organizations – and conduct research in power-management, microarchitecture and security. It's not the first time designers have had to reevaluate everything they were doing. However, this awakening requires a faster and more significant change to restore users' trust in hardware security without ruining devices' performance and battery life.

## Not so secure

A single modern microprocessor chip can have more than a billion tiny components, including transistors and switches, that form their own little

network on a piece of silicon deep inside a computer or electronic gadget. The main problem stems from the fact that tidbits of useful information can leak out from one component to others nearby, just like neighbors often know what's going on in each other's houses without asking.

A dedicated observer could, for instance, notice that your home's lights go on and off at a particular times each workday and infer your family's work schedules. This sort of indirect approach, using an apparently harmless type of data to infer a useful conclusion, is often called a "side-channel attack." These vulnerabilities are particularly significant because they exploit weaknesses designers didn't think to secure – and may not have thought of at all. Also, attacks like this are hardware problems, so they cannot be easily patched with a software update.

Security researchers have found that certain types of internet traffic, temperature changes, radio emissions or electricity usage can provide similar clues to what electronic components are doing. These are external clues revealing information the home's residents – or the device's users – never intended to share. Even a little information can be enough to reveal important secrets such as users' passwords.

Many – perhaps even most – of these information leaks are the accidental results of chip designers' efforts to speed up processing. One example was the nearly universal practice of letting a piece of software read data from the computer's memory before checking whether that program had permission to do so. As other commentators have pointed out, this is much like a security guard letting someone into a building while still checking their credentials.

## Innovation as the solution

These are serious problems with no clear – or simple – answers, but I'm

confident they'll be solved. About 15 years ago, the microprocessor architecture research community faced another seemingly insurmountable challenge and found solutions within a few years – just a few product generations.

At that time, the challenge was that the amount of power microchips consumed was climbing rapidly as components got ever smaller. That made cooling incredibly difficult. Dire charts were presented at major professional conferences comparing the problem of cooling microprocessors to the challenges of preventing nuclear reactors from overheating.

The industry responded by focusing on power consumption. It's true that early designs that were more power efficient did computations more slowly than their power-hungry predecessors. But that was only because the initial focus was on redesigning basic functions to save power. It wasn't long before researchers developed various processing shortcuts and tricks that accelerated performance even beyond what had been possible before.

## Security principles

I anticipate a similar response to this newly understood security concern: A rapid response that temporarily degrades performance, followed by a return to normal processing speeds. However, the improvement in security may be harder to express clearly than, say, the amount of energy a system uses.

Security is based on a set of principles the designers must follow reliably. One principle could be, for instance, that software cannot read data from memory without permission. This is very hard to implement because at every level of the microprocessor and every place that data could reside, the architects would need to build in permissions checks.

Just one mistake in just one circuit could leave the entire system vulnerable.

As the research community shifts its priority to security, there are several potential lines of inquiry already developing. One method could involve, as Princeton microchip engineer Ruby Lee suggests, inserting randomness into processing, offering observers timing, power and temperature values that – like setting a timer to turn your house lights on and off at random intervals while you're away. But adding randomness would likely degrade a processor's performance – unless researchers can find a way to avoid doing so.

Identifying and securing these newly identified hardware vulnerabilities and side-channels will be challenging, but the work is important – and a reminder that designers and architects must always think about other ways attackers might try to compromise computer systems.

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

Provided by The Conversation

Citation: Microprocessor designers realize security must be a primary concern (2018, July 18) retrieved 2 May 2024 from https://phys.org/news/2018-07-microprocessor-primary.html