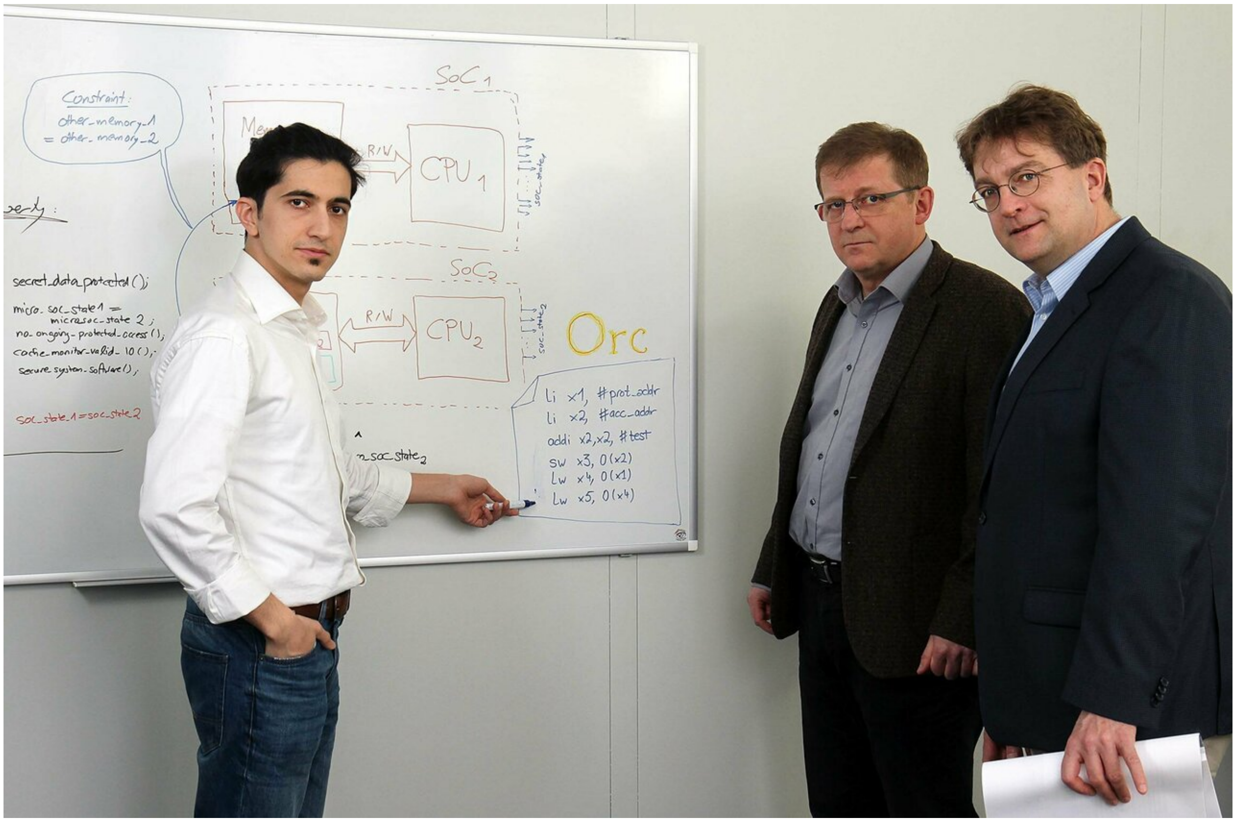
PHYS.ORG

Spotting hacks automatically, before the hackers do

March 25 2019



Mohammad R. Fadiheh (from left to right), Professor Wolfgang Kunz and Dominik Stoffel have developed the new algorithm in collaboration with scientists at Stanford. Credit: Koziel/TUK

In early 2018, cybersecurity researchers discovered two security flaws they said were present in almost every high-end processor made and used by major companies. Known ominously as Spectre and Meltdown, these flaws were troubling because they represented a new type of breach not previously known that could allow hackers to infer secret data—passwords, social security numbers, medical records—from the way computers pre-calculate certain data using architectural features called "out-of-order execution" and "speculative execution" to speed up their processes.

With that, a race started in the hardware community as chip designers hurried to find fixes to Spectre and Meltdown and to reveal as-yet-undiscovered flaws before hackers did. In the year since, numerous variants of these attacks have emerged, and more are expected.

In these "covert channel attacks," no data ever changes hands between the hacked processor and the attackers trying to steal data. The information is inferred in the way answers in a crossword puzzle can been guessed without knowing the actual answer to the clue. These hacks, therefore, are nearly impossible to spot.

Rising to this emerging threat, a team led by computer scientists at TU Kaiserslautern, Germany, in collaboration with researchers from Stanford University in California, has taken a novel approach to exposing potential flaws in new chip designs. It is an algorithm, Unique Program Execution Checking, or UPEC, for short.

"UPEC is a form of automated security verification that will alert designers to potential flaws in their microarchitectures, long before the chips are mass produced," says lead Professor Wolfgang Kunz, Chair of Electronic Design Automation at TU Kaiserslautern.

What's more important is that they've shown that such security holes exist in a much wider spectrum of processors than previously thought, affecting not just high-end processors but even the simple processors that are omnipresent in numerous applications of daily life, such as in the Internet of Things.

In essence, UPEC analyzes microarchitectural side effects of design decisions and detects if they can be exploited to create covert channels. What is particularly key is that UPEC is exhaustive. It takes into account all possible programs that can run on the processor. The researchers believe UPEC can expose any potential covert channel vulnerabilities in future chip designs, even those that designers had not anticipated.

In real-world tests, the research team had UPEC analyze several open source chip designs and identified a number of previously unknown flaws. The team created and analyzed different design variations of these processors and demonstrated that such weaknesses easily result from normal design processes and can affect virtually any processor, particularly simple processors not just the class of high-end processors analyzed in the Spectre/Meltdown attacks.

"The key point here is that even simple design steps, like adding or removing a buffer, can inadvertently introduce covert channel vulnerabilities in pretty much any processor," says Mo Fadiheh, member of the Kaiserslautern team.

One prominent attack UPEC has revealed is what the team has dubbed the "Orc" attack that could be present on chips that are already being used as the backbone in many safety- and security-critical applications in the Internet-of-Things and in autonomous systems, like self-driving cars and airplanes.

"Theoretically, a hacker could use an Orc attack to assume control of an autonomous vehicle or to commandeer networked computers on the Internet-of-Things," says team member Subhasish Mitra, professor of electrical engineering and computer science at Stanford University.

Orc is the first unanticipated attack to be discovered automatically by software alone. The Orc discovery demonstrates that covert channel attacks are possible in simple processors. Whether Orc vulnerabilities are baked into chips already on the market the researchers can't say for certain because they lack the proprietary source code to make such evaluations.

"We suggest that companies making these simpler processors use UPEC to be certain they don't carry Orc and other vulnerabilities," Kunz recommends.

UPEC does not require a designer to have existing knowledge of potential attacks and provides demonstrable guarantees of security. Notably, for the processor design community, UPEC requires no dramatic changes to standard design processes. So far, UPEC works for processors of up to medium complexity. Further research is under way on high-end processors. The current implementation of UPEC has been built by making extensions to an existing formal verification environment provided by Onespin Solutions.

"Orc demonstrates that serious flaws can result from seemingly innocuous design decisions chip designers make every day," says Professor Mark D. Hill, a computer architecture expert from the University of Wisconsin-Madison. "With UPEC, designers can be much more confident that they will find and eliminate all potential covert channel flaws in their designs."

More information: Andrew Ferraiuolo et al, Verification of a Practical Hardware Security Architecture Through Static Information Flow Analysis, *Proceedings of the Twenty-Second International Conference on Architectural Support for Programming Languages and Operating Systems - ASPLOS '17* (2017). DOI: 10.1145/3037697.3037739

Provided by Technische Universität Kaiserslautern

Citation: Spotting hacks automatically, before the hackers do (2019, March 25) retrieved 17 April 2024 from https://phys.org/news/2019-03-hacks-automatically-hackers.html