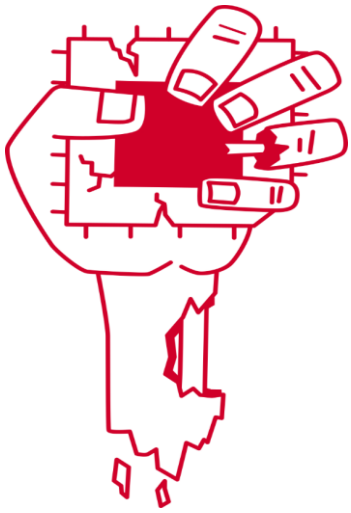
SUCCESS STORY

DeSSnet,
Dependable, secure and time-aware sensor networks

Programme: COMET – Competence Centers for Excellent Technologies

Programme line: COMET-Project

DeSSnet, Key Enabling Technologies for Security, 06/2017-05/2021, strategisch multi-firm



Copyright: Natascha Eibl

ZOMBILOAD: THE NEW CPU VULNERABILITY

With the beginning of 2018, the disclosure of the security vulnerabilities ‘Meltdown’ and ‘Spectre’ turned the entire IT industry upside down. Attackers were able to read arbitrary memory and therefore, passwords, and other sensitive documents. Solely the way modern processors are built allowed adversaries to mount these attacks without exploiting any software vulnerabilities. Since these processors are used everywhere, the question for the DeSSnet project arises in which scenarios and with which consequences they apply. While researching the attacks and countermeasures, new CPU vulnerabilities were discovered that attracted worldwide media attention; among them, the newest attack named ZombieLoad.

In January 2018 a team of scientists of Graz University of Technology published in international cooperation the security vulnerabilities ‘Meltdown’ and ‘Spectre’. Among the discoverers were Moritz Lipp and Stefan Mangard that are involved in the DeSSnet project. They showed how an unprivileged attacker could steal sensitive information of desktop computers, mobile devices, and servers without exploiting a software bug. Solely the way how modern processors are build allows an attacker to manipulate the processors in a way to disclose passwords and other sensitive documents.

As these vulnerabilities affect different CPU manufacturers and, thus, almost every device that we use nowadays, those attacks gained attention not only in the research community but in the entire public. Hence, the question arises for the DeSSnet project if these vulnerabilities imply problems in the project-related scenarios and which impact they can have. In further research, we systematically analyzed the attacks and existing countermeasures and discovered new security vulnerabilities that attracted worldwide media attention.

Federal Ministry
Republic of Austria
Transport, Innovation and Technology

Federal Ministry
Republic of Austria
Digital and Economic Affairs

Version 01/2019

SUCCESS STORY

Meltdown and Spectre in a nutshell: In the past years, processors have been solely optimized for their performance in order to execute applications as fast as possible in order to fulfill the customers and industries needs. However, these optimizations yield unintended side effects that an attacker can observe. So-called side channel attacks exploit these side effects like power consumption or the execution time of an algorithm to draw conclusions about sensitive information. As a typical example serves a bandit in the wild west trying to crack a safe. Using a stethoscope, the attacker listens to the clicking noises of the safe in order to deduce the secret information and, therefore, opening the safe. The described attacks, however, don't require physical access to the targeted device but exploit such side effects in modern processors to transmit information. In the concrete implementation of the processor (the so-called microarchitecture) some manufacturers ignore certain security guarantees of the defined architecture while trying to execute programs as fast as possible. Here, the processor tries to predict the program flow of the running application. In the case of a correct prediction, the results have been calculated upfront and, thus, the execution time is faster. In the case of a misprediction, the CPU dismisses all unrightfully calculated results and does not expose them to the user. However, by utilizing side channels, an attacker can reconstruct these results and therefore steal sensitive information like passwords.

As these attacks do not exploit any software bugs, implementing mitigations is difficult. In order to mitigate Meltdown and Spectre successfully, not only updates to the CPUs microcode had to be performed, but also updates to the operating system and the running applications had to be performed. If one component has not or only partially been updated, attacks were still possible.

ZombieLoad - The new attack: With the disclosure of Meltdown and Spectre, a new research field opened up and, thus, new attacks exploiting other hardware optimizations followed. While updates of the operating system and the CPU microcode allowed to secure existing systems, the newest generation of CPUs already deployed mitigations in hardware. The new attack ZombieLoad allows to spy data processed by other running applications and even works on CPUs with hardware mitigations against Meltdown and Spectre. The attack has been found by the same team of Graz University of Technology and gained worldwide media attention.

Impact and effects: The research results did not only attracted worldwide media attention but were also published on top tier conferences. The attacks and their resulting countermeasures also have also an impact on the industry as the mitigations yield a measurable performance loss on existing systems. Furthermore, hardware designs and hardware configurations have to be reviewed in order to fulfil certain security guarantees. Furthermore, the new research area that developed out of these attacks is currently one of the most attractive ones in system security.

Project coordination (Story)
Univ.-Prof. DI Dr. Stefan Mangard
Graz University of Technology
Institute of Applied Information Processing and Communication
Stefan.Mangard@iaik.tugraz.at

DeSSnet / COMET-Project
JOANNEUM RESEARCH Forschungsgesellschaft mbH/ Consortium leader
Steyrergasse 17
8010 Graz
Herwig.Zeiner@joanneum.at
www.dessnet.at

Project partner

- Infineon Technologies Austria AG, Austria

This success story was provided by the consortium leader/centre management and by the mentioned project partners for the purpose of being published on the FFG website. Further information on COMET: www.ffg.at/comet

Federal Ministry Republic of Austria Transport, Innovation and Technology

Federal Ministry Republic of Austria Digital and Economic Affairs

Austrian Research Promotion Agency
Sensengasse 1, A-1090 Vienna
P +43 (0) 5 77 55 - 0
office@ffg.at
www.ffg.at