(idw)

idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Universität Duisburg-Essen
Dr. Thomas Wittek

07/15/2022
http://idw-online.de/en/news798523

Research results
Information technology
transregional, national

Fingerprint sensors and crypto wallets: Security vulnerabilities revealed

Security experts from paluno, the Ruhr Institute for Software Technology at the University of Duisburg-Essen (UDE) have developed a new technique that, for the first time, enables fuzz testing of protected memory areas in modern processors. Their method revealed many vulnerabilities in security-critical software. The research was funded within the cluster of excellence CASA*.

Intel's "Software Guard Extension" (SGX) is a widely used technology to protect sensitive data from misuse. It helps developers in shielding a certain memory area from the rest of a computer. A password manager, for example, can be executed safely in such an enclave, even if the rest of the system is corrupted by malware.

However, it is not uncommon for errors to creep in during the programming of the enclaves. Already in 2020, the paluno team from Prof. Dr. Lucas Davi discovered and published several vulnerabilities in SGX enclaves. Now, together with partners form the CASA cluster of excellence, the researchers have achieved another breakthrough in the analysis techniques: Their latest development enables the fuzz testing of enclaves, which is much more effective than the previously used symbolic execution. The idea behind fuzz testing is to feed a large number of inputs into a program in order to gain insights into the structure of the code.

"As enclaves are meant to be non-introspectable, fuzzing cannot easily be applied to them," paluno scientist Tobias Clooster explains the challenge. "Moreover, fuzzing requires nested data structures, which we dynamically reconstruct from the enclave code." His research partner Johannes Willbold from from the research college SecHuman from the Ruhr-Universität Bochum adds: "This way, the shielded regions can be analyzed without accessing the source code."

Thanks to modern fuzzing technology, the researchers were able to detect many previously unknown security problems. All tested fingerprint drivers as well as wallets for storing cryptocurrency were affected. Hackers could exploit these vulnerabilities to read biometric data or steal the entire balance of the stored cryptocurrency. All companies were informed. Three vulnerabilities have been added to the publicly available CVE directory**.

* The Cluster of Excellence CASA (Cyber Security in the Age of Large-Scale Adversaries) is funded by the German Research Foundation (DFG) since 2019. Prof. Lucas Davi from paluno is principal investigator within the cluster of excellence, which is based at the Horst Görtz Institute for IT Security (HGI) at the Ruhr-Universität Bochum.

** CVE stands for Common Vulnerabilities and Exposures and lists major, publicly known vulnerabilities. The vulnerabilities referenced have the CVE entries CVE-2021-3675 (Synaptics Fingerprint Driver), CVE-2021-36218 (SKALE sgxwallet) and CVE-2021-36219 (SKALE sgxwallet)

Editor: Birgit Kremer, Paluno, Tel. +49 201/18 3-4655, birgit.kremer@paluno.uni-due.de

contact for scientific information:
Prof. Dr. Lucas Davi, Informatik, Tel. +49 201/18 3-6445, lucas.davi@uni-due.de