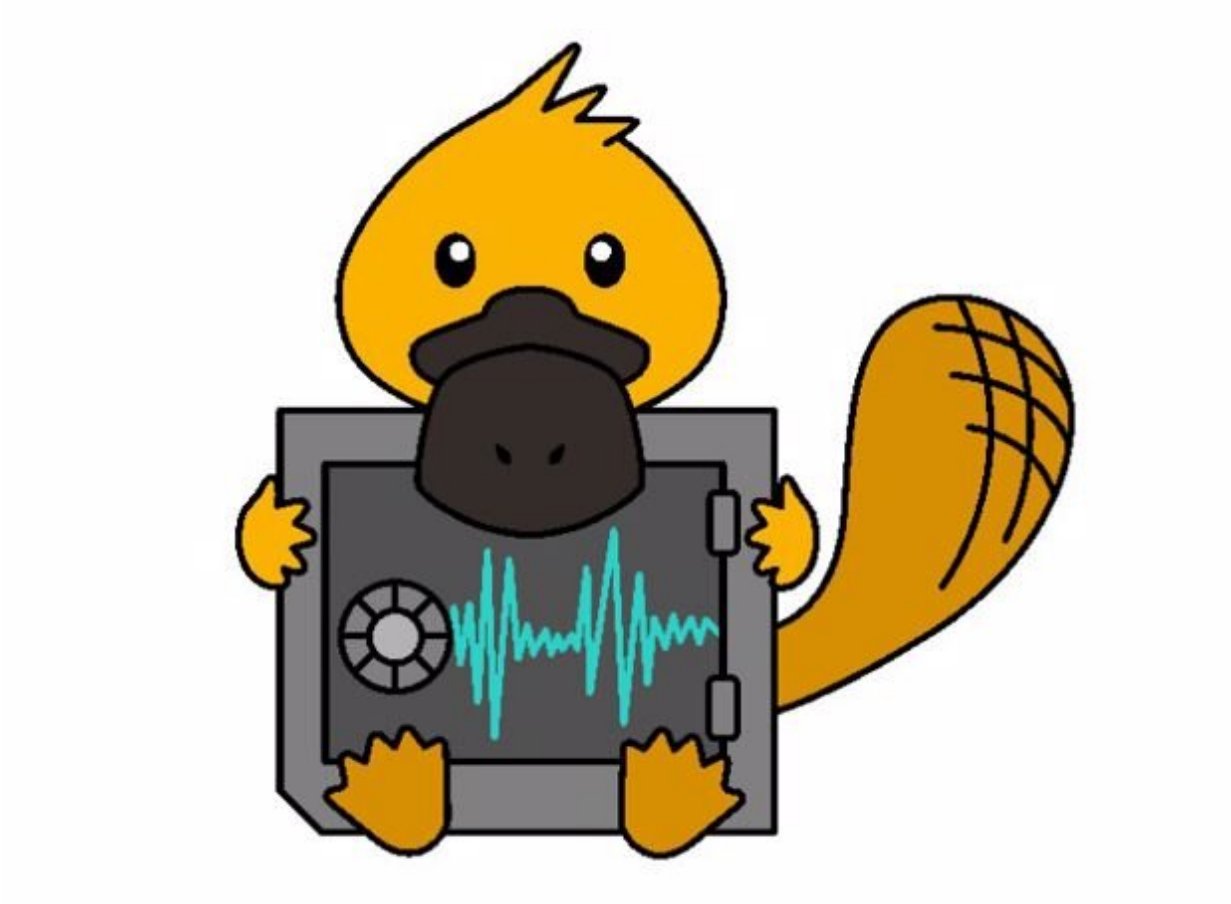
PLATYPUS reveals new vulnerabilities discovered in Intel processors

November 11 2020



Credit: University of Birmingham

An international team of security researchers, including experts from the University of Birmingham, is presenting new side-channel attacks, which

use fluctuations in software power consumption to access sensitive data on Intel CPUs.

Power side-channel attacks are attacks that exploit fluctuations in power consumption to extract sensitive data such as cryptographic keys. Because power measurements by malware were previously very inaccurate, such attacks required physical access to the target device and special measurement tools such as an oscilloscope.

The project, called PLATYPUS, is led by the Institute of Applied Information Processing and Communications at Graz University of Technology together with the University of Birmingham, UK and the Helmholtz Center for Information Security (CISPA), shows a method that allows power side-channel attacks that can access sensitive data with unprecedented accuracy—even without physical access.

The team have demonstrated their method can affect devices including desktop PCs, laptops and cloud computing servers from Intel and AMD.

Dr. David Oswald, senior lecturer in Cyber Security at the University of Birmingham, says: "PLATYPUS attacks show that power side channels—which were previously only relevant to small embedded devices like payment cards—are a relevant threat to processors in our laptops and servers. Our work connects the dots between two research areas and highlights that power side channel leakage has much wider relevance than previously thought."

RAPL interface and SGX enclaves as key

The researchers used two key approaches. In the first, they used the RAPL interface (running average power limit), which is built into Intel and AMD CPUs. This interface monitors the energy consumption in the devices and ensures that they don't overheat or consume too much

power. RAPL has been configured so that power consumption can be logged even without administrative rights. This means that the measured values can be read out without any authorizations.

In the second approach, the group misuses Intel's security function Software Guard Extensions (SGX). This functionality moves data and critical programs to an isolated environment (called an enclave) where they are secure—even if the normal operating system is already compromised by malware.

Combination leads to (un)desired result

The researchers combined these two techniques in their methods of attack. Using a compromised operating system targeting Intel SGX, they made the processor execute certain instructions tens of thousands of times within an SGX enclave. The power consumption of each of these commands was measured via the RAPL interface. The fluctuations in the measured values finally allow to reconstruct data and cryptographic keys.

In further scenarios, the researchers also show that even attackers without administrative rights can attack the operating system and steal secret data from it.

New security updates resolve the threat

The TU Graz computer scientists Moritz Lipp, Andreas Kogler and Daniel Gruss together with their ex-colleague Michael Schwarz (researching at CISPA in Saarbrücken since summer 2020) and with David Oswald from the University of Birmingham informed Intel about their discoveries in November 2019. The company has now developed solutions that users should definitely adopt. A security update for

operating systems permits access to the RAPL measurement functions only with administrator rights. And further updates for the affected processors themselves ensure that the power consumption is returned in such a way that the subtle differences in the power consumption of programs are no longer visible.

Provided by University of Birmingham