Serious security vulnerabilities in DRAM memory devices

November 16 2021, by Oliver Morsch

A few of the DRAM memory modules tested by the ETH researchers. Credit: ETH Zurich / Computer Security Group

Researchers at ETH Zurich have discovered major vulnerabilities in DRAM memory devices, which are widely used in computers, tablets and smartphones. The vulnerabilities have now been published together with the National Cyber Security Centre, which for the first time has assigned an identification number for it.

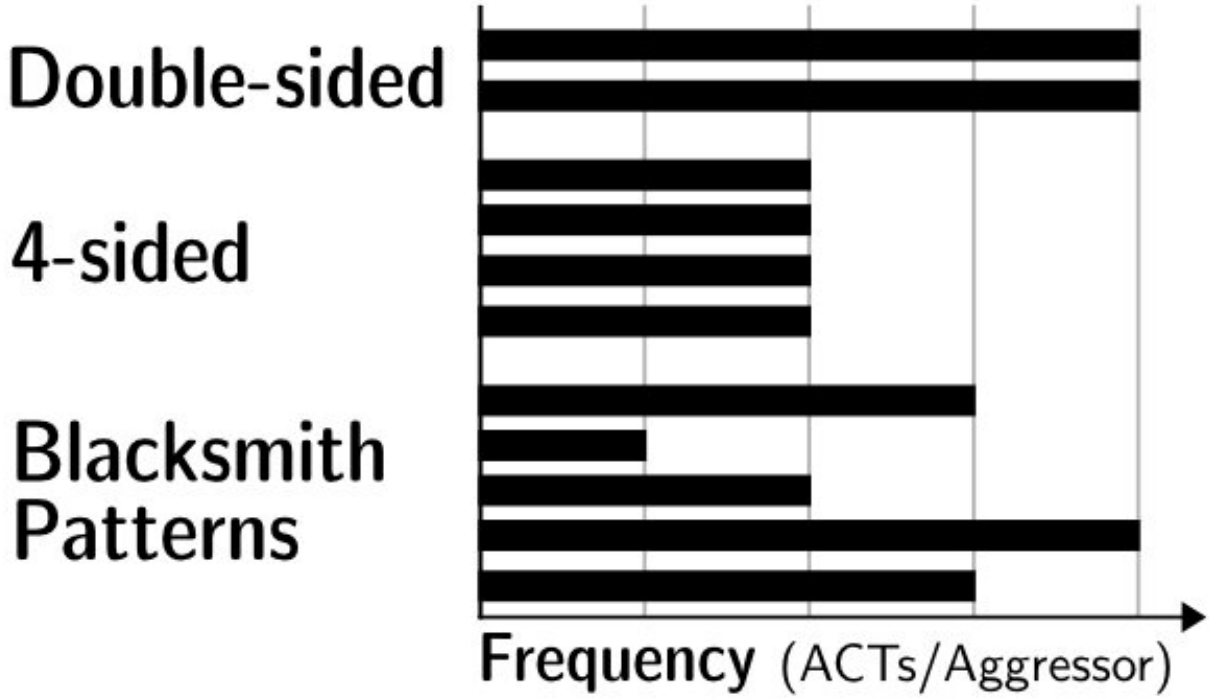
When browsing the internet on a laptop computer or writing messages on a smartphone, we all like to think that we are reasonably safe from hacker attacks as long as we have installed the latest software updates and anti-virus software. But what if the problem lies not with the software, but with the hardware? A team of researchers led by Kaveh Razavi at ETH Zurich, together with colleagues at the Vrije Universiteit Amsterdam and Qualcomm Technologies, have recently discovered fundamental vulnerabilities affecting the memory component called DRAM at the heart of all modern computer systems.

The results of their research have now been accepted for publication at a flagship IT security conference, and the Swiss National Cyber Security Centre (NCSC) has issued a Common Vulnerabilities and Exposures (CVE) number. This is the first time that a CVE identification has been issued by the NCSC in Switzerland (see box below). On a scale of 0 to 10, the severity of the vulnerability has been rated as 9.

The weakness of DRAM

"An underlying, well-known problem with DRAMs is called Rowhammer and has been known for several years," Razavi explains. Rowhammer is an attack that exploits a fundamental weakness of modern DRAM memories. DRAM is short for Dynamic Random Access Memory, where "dynamic" means that all the data stored in it is volatile and has to be refreshed quite often—in fact, more than ten times per second. This is because DRAM chips only use a single capacitor-transistor pair to store and access one bit of information.

The capacitors leak charge over time, and once they have leaked too much charge, the computer no longer knows whether the value of the stored bit was "1" (which might correspond to high charge) or "0" (low charge). On top of that, every time a memory row is activated in order to be read out or written onto (the bits are arranged in a checkerboard-like pattern of rows and columns), the currents that flow inside the chip can cause the capacitors in neighboring rows to leak charge faster.



Conventional hammering attacks (for instance, double-sided or four-sided) use regular patterns in which the aggressor rows are activated at a constant frequency. Blacksmith, by contrast, finds complex patterns with varying activation frequencies capable of inducing bit errors. Credit: Computer Security Group

Problem not solved

"This is an unavoidable consequence of the constantly increasing density of electronic components on the DRAM chips," says Patrick Jattke, a Ph.D. student in Razavi's group at the Department for Information Technology and Electrical Engineering. It means that by repeatedly activating—or "hammering"—a memory row (the "aggressor"), an attacker can induce bit errors in a neighboring row, also called the "victim" row. That bit error can then, in principle, be exploited to gain access to restricted areas inside the computer system—without relying on any software vulnerability.

"After Rowhammer was first discovered around ten years ago, chip manufacturers implemented mitigation measures inside the DRAM modules in order to solve the problem," Razavi says: "Unfortunately, the problem still hasn't been solved." The Target Row Refresh (TRR) mitigation Razavi refers to consists of different circuits built into the memory that can detect unusually high activation frequencies of particular rows and hence guess where an attack is being launched. As a countermeasure, a control circuit then refreshes the presumed victim row prematurely and hence forestalls possible bit errors.

Sophisticated hammering

Razavi and his colleagues have now found that this hardware-based "immune system" only detects rather simple attacks, such as double-sided attacks where two memory rows adjacent to a victim row are targeted but can still be fooled by more sophisticated hammering. They devised a software aptly named "Blacksmith" that systematically tries out complex hammering patterns in which different numbers of rows are activated with different frequencies, phases and amplitudes at different points in the hammering cycle. After that, it checks if a particular pattern led to bit errors.

The result was clear and worrying: "We saw that for all of the 40

different DRAM memories we tested, Blacksmith could always find a pattern that induced Rowhammer bit errors," says Razavi. As a consequence, current DRAM memories are potentially exposed to attacks for which there is no line of defense—for years to come. Until chip manufacturers find ways to update mitigation measures on future generations of DRAM chips, computers continue to be vulnerable to Rowhammer attacks.

The ethical dimension

Razavi is well aware of the ethical dimension of his research: "We obviously want to make the world safer, and we believe that it is important that potential victims be aware of this kind of threat so that they can make informed choices." Luckily, he adds, those victims are unlikely to be ordinary users, as there are much simpler ways to hack most computers (a reminder that using the latest anti-virus software and updating devices are still important). Nevertheless, it is possible that nation states or powerful organizations could use such attacks for high-profile targets. To give producers time to react to the new vulnerabilities, Razavi and his colleagues already informed them several months ago. They also cooperated closely with the NCSC, which is responsible for the coordinated publication of discovered vulnerabilities in Switzerland.

In the future, the ETH researchers want to explore even more sophisticated ways of inducing bit errors. That could help chip manufacturers to test their devices and address all possible hammering attacks. "Of course, although we are releasing code that shows how to trigger bit errors, we are not currently disclosing any code that abuses these errors," Razavi says.

More information: P. Jattke et al, Scalable Rowhammering in the Frequency Domain. *Proceedings of the IEEE Symposium on Security and Privacy 2022*. comsec.ethz.ch/wp-content/file … /blacksmith_sp22.pdf

Provided by ETH Zurich