Hardware security

DRAM as Achilles' Heel, Data Leak and Back Door

03.06.2020 | Author / Editor: Hans W. Diesing* / Dr. Jürgen Ehneß

It has been public knowledge since June 2019: Since the introduction of the DDR3 generation, DRAMs have not only been corruptible in their data integrity from the outside by the exploitation of a hardware weakness known as the "row hammer" (or: "rowhammer"), but can even read 2,048-bit decryption codes, passwords or other secret data in memory areas that the operating system should protect from unauthorized access by more complex attacks.

An academic research team had published the refined method of this eavesdropping attack as the "RAMBleed" project on its website https://rambleed.com/ on the Internet, triggering an avalanche of concerned comments in specialist media and forums worldwide.

The U.S. Department of Homeland Security's Data Protection Agency was then compelled to register and assess the threat in its public database under the identifier CVE-2019-0174. While the national authority assesses the threat risk with a moderate 3.3 out of 10 maximum points, the Red Hat Linux distribution assesses the threat probability at a still moderate 3.8 points, arguing that the attack is not only extremely time-consuming, but also requires detailed architectural knowledge of the victim's system that would hardly be available to a casual hacker.

However, the experience of the Stuxnet worm from ten years ago teaches us that there are organizations for which hardly any effort is too great, if the goal and purpose justify an attack, no matter how complex, especially if one does not have to wait for practically usable quantum computers to do so. At the time, a Simatic S7 controller at the Iranian uranium enrichment plant Natanz had been infected in such a way that normal operation was faked on the control monitors while the centrifuges in the basement went haywire and self-destructed.

Aggravated side channel attacks

In addition to the Red Hat statement in the assessment, the US National Threat Database refers to statements from Oracle that "do not assume" a threat because they only use DDR4 DRAM modules in their servers, which are protected because of the Target Row Refresh (TRR) introduced with this generation, which can make these side channel attacks more difficult under increased RAM power consumption, but which has been proven not to provide complete protection - not even by integrated error correction (ECC), which can compensate for individual sporadic bit flips, but which fails under massive side channel attacks when multiple parallel bit flips occur.

Finally, the manufacturer Intel is quoted as listing all its processor platforms concerned and advising to use only Row Hammer resistant DRAM modules, but without any indication as to which ones they might be. Upon request, the Intel Security Incident Response Team has indicated that if you can't find anything in Intel's platform/DRAM validation archive, you should contact the DRAM manufacturers directly. Since all of this validation data is older than the RAMBleed publication, it is obvious that such side channel attacks could not be recorded there either. The fact that the reference to DRAM manufacturers is an elegant way of avoiding the issue is understandable when considering the liability risks, in particular for critical IT and IoT infrastructures.

How and why does a Row-Hammer side channel attack work?

Over the years, the DRAM IC generations according to the JEDEC DDR standard (Double Data Rate) were accompanied by shrinking chip structures in favor of higher memory densities despite limited chip area and higher data rates despite limited power consumption, which thus became increasingly sensitive to crosstalk between adjacent word lines. Two animated GIFs from the University of Manchester provide a particularly impressive illustration of the difference between the conventional one-sided http://apt.cs.manchester.ac.uk/projects/ARMOR/RowHammer/images/row-hammer_error.gif and a two-sided rowhammer attack on a DRAM module, nicknamed "Flip Feng Shui" http://apt.cs.manchester.ac.uk/projects/ARMOR/RowHammer/images/double-row-hammer_error.gif as required for a RAMBleed attack.

Sporadic bit flips - i.e. randomly flipped bits - could be compensated by integrated error-correcting code (ECC), as is common in critical servers. Since the introduction of the third DDR generation in 2012, it was found that extremely frequent row activation, so-called "row hammering", during the data hold phases between refresh cycles could provoke bit flips from outside and corrupt the data integrity of the RAM in order to disrupt or sabotage a victim system. Responsible for this crosstalk between the bits in adjacent lines were the smaller capacitances of the shrunk bit memory capacitors, which must be imagined as cone-shaped cavities in the chip surface and which therefore come correspondingly closer together, also in interaction with the ever narrower bit lines along the data matrix columns, which thus become correspondingly high-impedance and thus additionally promote capacitive dynamic crosstalk.

Vulnerable smartphones

Since March 2020, the University of Amsterdam, in collaboration with the ETH Zurich and the SoC manufacturer QualComm, has published further research under the project name "TRRespass" on the vulnerability of DDR4 SDRAMs, also taking into account the low-power versions as in the more recent smartphones, with the result that all makes of the three largest manufacturers, which together cover about 95 percent of the market, are vulnerable, by extending between three and 19 aggressor word lines. Despite TRR-based security measures, these are even several times more susceptible than previous DDR3 versions, namely after just under 50,000 activations. There they will soon also provide an app for the self-test of current smartphones. Since March 10, the threat has also been recorded and explained in the US Department of Homeland Security database under CVE-2020-10255 - but so far without an assessment. However, the threat database cxsecurity rates 10 out of 10 possible points as "impact score" for data integrity, 9.3 for confidentiality and 8.6 for availability of the threat. At the "2020 IEEE Symposium on Security and Privacy", both submitted academic papers "TRRespass" and "RAMBleed " were presented to a relevant expert audience online, as can be followed on YouTube.

Exchange of DRAMs

While software security vulnerabilities can be averted by updates and patches, a DRAM hardware weakness can only be ultimately remedied by replacing the DRAM modules or DRAM chips. For this purpose, Row-Hammer-resistant (RH-free) DDR3 SDRAM ICs have recently become available. These are fully functionally compliant and footprint compatible with conventional versions based on the relevant JEDEC standard and are therefore easily interchangeable, but still do not show any significant degradation in performance and power consumption. This is ensured by an integrated trapping circuit based on counter trees or counter-based adaptive trees (CAT), which detects and blocks Row-Hammer-typical attacks before they can even take effect.

Conventional DDR3 SDRAM ICs need more than 200,000 activation cycles before the next refresh of the addressed word line to trigger and register bit flips in their neighboring lines. The number of bit flip errors is charted in the diagram shown (Fig. 1) for three temperatures, at +95 degrees Celsius (Hot), +25 degrees Celsius (Room temperature) and -10 degrees Celsius (Cold). By about 900,000 activations, the error rate goes into saturation with 45 bit flips, while the Row-Hammer-immunized version still has no bit flip errors after one million activations during the data hold cycle.

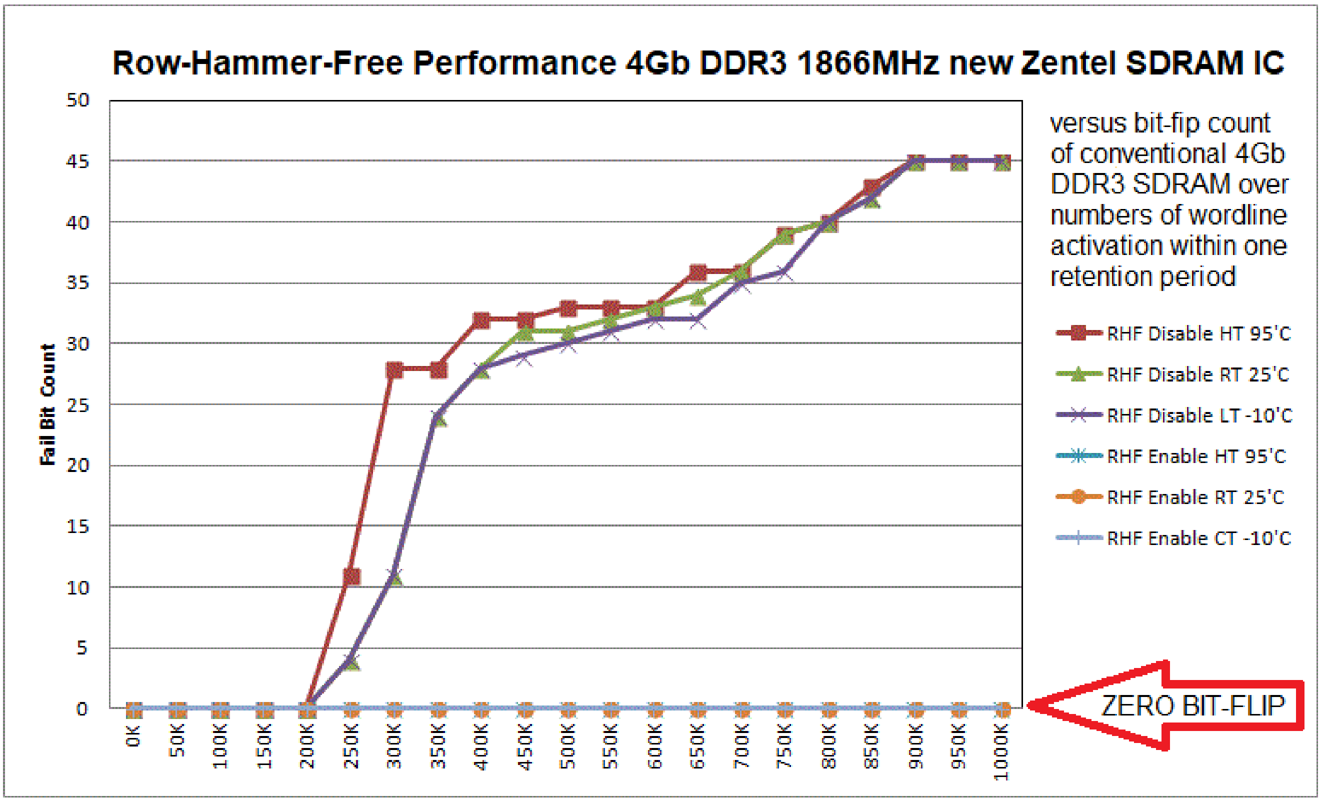

Fig. 1: Number of bit flip errors at three temperatures.
(Picture: Zentel)

The Row Hammer stress test, on the basis of which the diagram was generated, was performed on an auto-test equipment with a special operating system. In principle, however, such a test can be executed on any target platform according to the flow chart shown (Figs. 2 and 3) and programmed based on the respective operating system to verify the application's susceptibility to Row Hammer-based side channel attacks. In the first step of the initialization all bits are set to 0 and the activation signals are given. Afterwards it is checked whether bit flips have occurred. The frequent activation signals are known to cause minimal partial charges to spill over into previously discharged adjacent bit memory cells. Since this vulnerability is a prerequisite for the success of a RAMBleed attack, such a test also provides the necessary assurance in this regard.

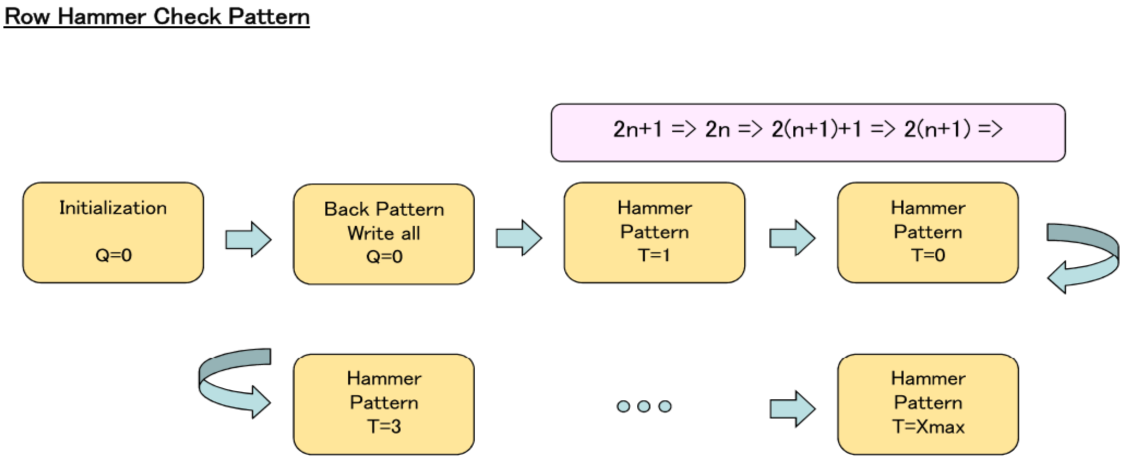

Figure 2: Row Hammer Check Pattern.
(Picture: Zentel)

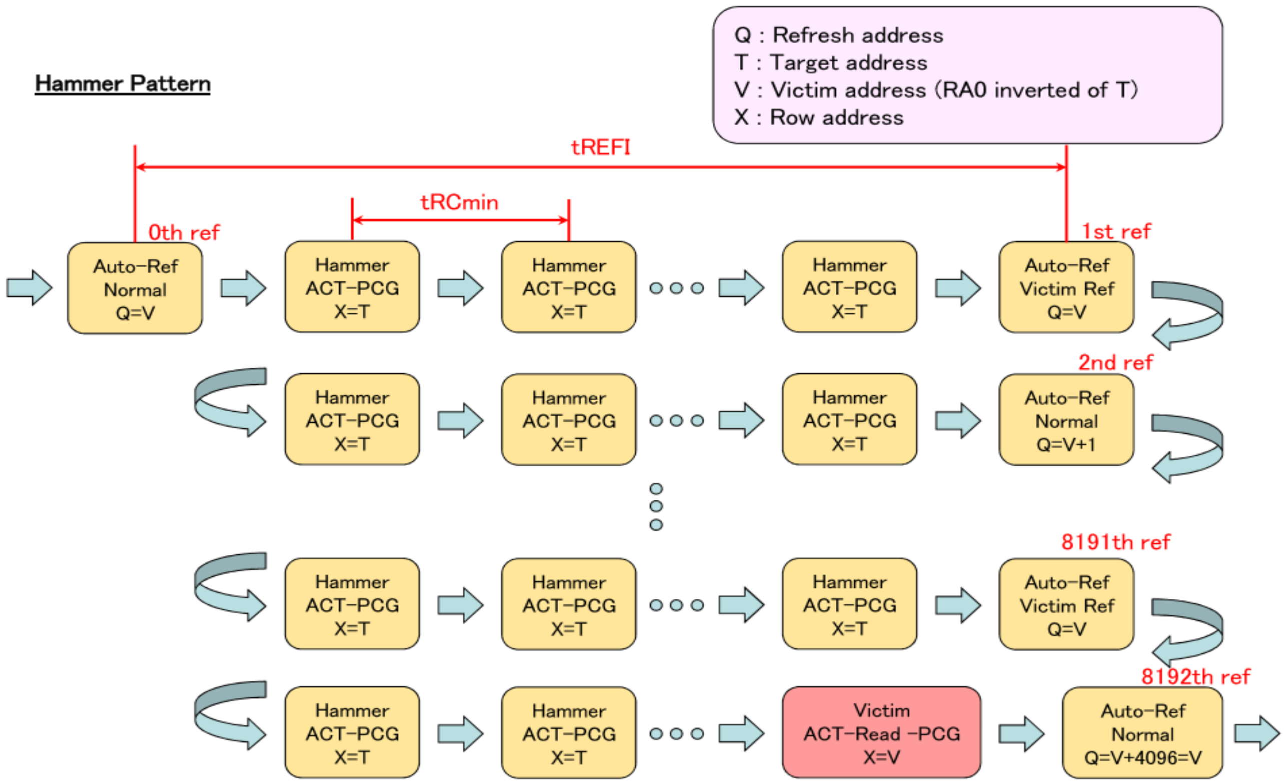

Fig. 3: Hammer Pattern.
(Picture: Zentel)

*Author: Hans W. Diesing, Director of Sales Zentel EMEA