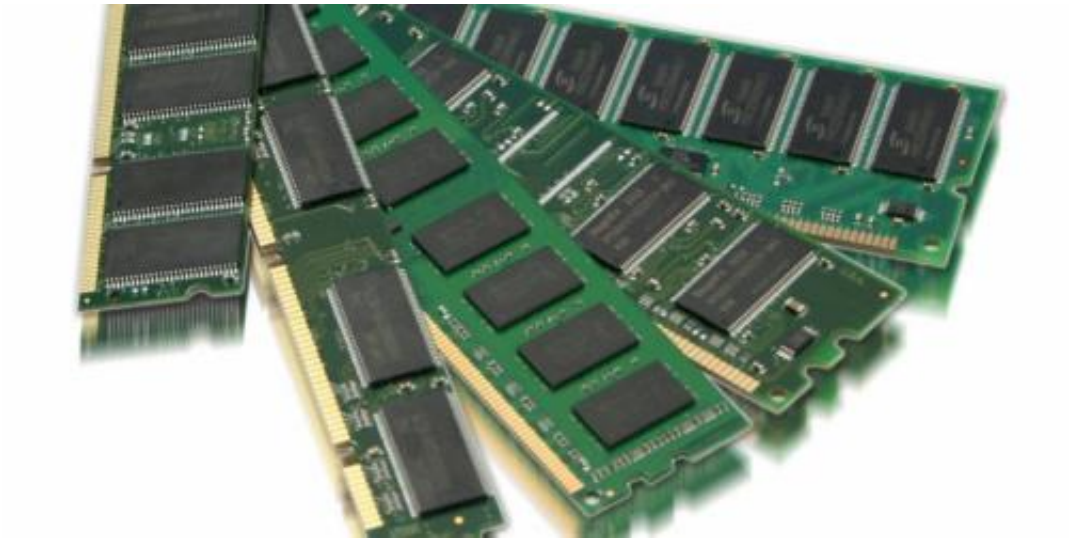
Project Zero sheds more light on rowhammer problem

March 11 2015, by Nancy Owano



Researchers have discussed exploits with some DRAM memory devices, allowing attackers access to target machines. That was a Tuesday report from *Threatpost*'s editor-in-chief Dennis Fisher, who is also security evangelist for Kaspersky Lab Americas. This is the "rowhammer" problem; Fisher described it as a method for "repeatedly hammering on rows of cells of memory in DRAM devices to induce cells to flip from one state to another."

Fisher detailed the problem further, writing that "the cells of memory on DRAM devices have become closer and closer together over time,

meaning that it has become more difficult to prevent electrons from jumping from one cell to another. By accessing target cells in DRAM over and over again, an attacker can disturb a cell adjacent to the target cells, causing it to 'bit flip' under some circumstances."

Researchers at Google have shed detailed light on this rowhammer problem. In a guest post on Monday from the Project Zero team at Google, Mark Seaborn and Thomas Dullien discussed exploiting the DRAM rowhammer bug to gain kernel privileges. Also, turning to the vulnerability of machines, they said, "We encourage vendors to publicly release information about past, current and future devices so that security researchers, and the public at large, can evaluate them with reference to the rowhammer problem." The authors then listed the types of information that would be helpful. Questions, for example, were "Is the DRAM device susceptible to rowhammer-induced bit flips at the physical level? What rowhammer mitigations does the DRAM device implement?" Regarding the CPU model, questions included, "Is it possible to read or write the memory controller's settings after startup, to verify mitigations or enable mitigations?"

They said that with more information, "it would be easier to assess which machines are vulnerable. It would be easier to evaluate a negative test result, i.e., the absence of bit flips during testing." The industry is less accustomed to hardware bugs than to software bugs, they added, but they wanted to encourage hardware vendors to take the same approach: "thoroughly analyze the security impact of 'reliability' issues, provide explanations of impact, offer mitigation strategies and—when possible—supply firmware or BIOS updates. Such discussion will lead to more secure hardware, which will benefit all users."

Serdar Yegulalp, senior writer for *InfoWorld*, similarly said that "Project Zero is asking that DRAM manufacturers, CPU makers, and BIOS creators release more data about the steps they've taken to mitigate

rowhammer-like issues on their devices. Not only would this aid in screening out false negatives, but it might give software and OS makers a way to guard against such issues."

In 2014, researchers from Carnegie Mellon and Intel Labs wrote a paper, "Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors." They explained that "The continued scaling of DRAM process technology has enabled smaller cells to be placed closer to each other. Cramming more DRAM cells into the same area has the well known advantage of reducing the cost-per-bit of memory. Increasing the cell density, however, also has a negative impact on memory reliability."

They said that "high-density DRAM is more likely to suffer from disturbance, a phenomenon in which different cells interfere with each other's operation." The authors also stated that "disturbance errors are an emerging problem likely to affect current and future computing systems." What about DDR4? Marc Greenberg of Synopsys, a company focused on electronic design automation and semiconductor intellectual property, had some interesting notes on what one may expect out of DDR4. He said, "Looking forward to DDR4, Row Hammering may be a thing of the past."

Greenberg said there was "some evidence that next-generation CPUs will either not be capable of issuing row hammering data patterns, or may mitigate them with TRR, [Targeted Row Refresh] or both." (DDR4 stands for double data rate fourth generation, which is the next evolution in DRAM [dynamic random-access memory].)

More information: googleprojectzero.blogspot.com … mer-bug-to-gain.html