DDR Memory Errors Caused by Row Hammer

Barbara P. Aichinger
Vice President New Business Development

FuturePlus Systems Corporation
15 Constitution Drive
Bedford NH 03110 USA
What is DDR3 Memory?

- The 3rd generation of the Double Data Rate DRAM (Dynamic Random Access Memory)
- Most pervasive technology used in cloud computing and general computing design
- Billions of DDR3 DRAM parts have been shipped since ~ 2006.
Where is it used?

- Laptops
- Desktops
- Servers
- Embedded Applications
  - Defense
  - Medical
  - Automotive
  - Anywhere lots of memory is needed.
DDR3 is at the heart of Cloud Computing Servers

There are over 1 million servers on the planet. Each one have 16-24 DIMMs full of DDR3 memory.
What is the problem?

• Charge leakage from one row into another

Excessive ACTIVATE commands apply repeated charge to the memory cells

Electromagnetic field induced by applied voltage

Cells lose charge by repeated nearby electromagnetic field, causing a coupled bit

Source: http://www.eurosoft-uk.com/eurosoft-test-bulletin-testing-row-hammer/
What research has been done?

- **July 2014**
  - Carnegie Mellon

- **March 2015**
  - Google

- **July 2015**
  - University of Technology
  - Austria and France

---

**Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors**

Yoongu Kim¹ Ross Daly* Jeremie Kim¹ Chris Fallin* Ji Hye Lee¹ Donghyuk Lee¹ Chris Wilkerson² Konrad Lai Onur Mutlu¹

¹Carnegie Mellon University ²Intel Labs

---

**Project Zero**

News and updates from the Project Zero team at Google

---

**Exploiting the DRAM rowhammer bug to gain kernel privileges**

Posted by Mark Seaborn, sandbox builder and breaker, with contributions by Thomas Dullien, reverse engineer

---

**Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript**

Daniel Gruss
O exiting University of Technology, Austria
daniel.gruss@hac.k.tugraz.at

Clemence Maurice
Technicolor, Sophia-Antipolis, France
clementine.maurice@technicolor.com

Stefan Mangard
O exiting University of Technology, Austria
stefan.mangard@tugraz.at

---

IEEE HPEC 2015 Conference

FuturePlus Systems

Power Tools for Bus Analysis
Additional Press

Row Hammer DRAM Bug Now Exploitable via JavaScript, Most DDR3 Memory Chips Vulnerable

In March, security researchers have published a report detailing a problem with some memory chips that can be exploited to give attackers access to any computer using the latest DDR3 DRAM chips.

The DDR3 Row Hammer Bug
by EvilDead
6 months ago
5 comments

EvilDead
It's a hack. Get an

I recently acquired a new PC and while running memtest86 it would fail during the "RowHammer" test. However it would pass memtest86 and Windows memory diagnostics with flying colors but they haven't been updated in a while. From what I'm reading it is very unlikely to ever occur in normal computing because it requires hammering rows of memory repeatedly to flip an adjacent bit.

But because I don't like the sound of "very unlikely," I put some very old DDR3 memory into it and it passed (2x 2GB sticks). So, as a next step, I purchased another set of 16GB (SODIMM Ripjaws) (newegg customer award winner) only to find out they also fail the row hammer test. I'm now reading that this is widespread in DDR3 memory especially in higher capacity sticks due to how tightly everything needs to be packed. I have read numbers as high as 8% of the RAM out there purchased from 2010 through 2014 and likely a lot of the chips that are currently being produced.

Errata Security
Advanced persistent cybersecurity

Some notes on DRAM (#rowhammer)
By Robert Graham
My twitter feed is full of comments about the "rowhammer" exploit. I thought I'd write some quick notes about DRAM. The TLDU version is this: you probably don't need to worry about this, but we (the designers of security and of computer hardware/software) do.

There are several technologies for computer memory. The densest, and hence cheapest-per-bit, is "DRAM." It consists of a small capacitor for each bit of memory. The thing about capacitors is that they lose their charge over time and must be refreshed. In the case of DRAM, every bit of memory must be read and rewritten every 64 milliseconds or it becomes corrupt.

These tiny capacitors are prone to corruption from other sources. One common source of corruption is cosmic rays. Another source is small amounts of radioactive elements in the materials used to construct memory chips. So, chips must be built with...
Row Hammer failures on DDR4?

Rowhammer mitigation

My i7-5820K/GA-X99-UD4/2400MHz Crucial Ballistix DDR4 system was failing rowhammer (a few hundred errors per pass) until I reduced the refresh interval timing from the default of 7.8ms, in spite of the fact that DDR4 is supposed to include rowhammer mitigation (source: https://en.wikipedia.org/wiki/Row_hammer#Mitigation).

In my board’s BIOS, the two settings were tREFI (default of 9360) and tREFIX9 (default of 82).

refresh interval (ms) = tREFI / (RAM clock (MHz) / 2)

\[ tREFIX9 = 8.9 \times \frac{tREFI}{1024} \]

so...

\[ 9360 / (2400 / 2) = 7.8ms \]

(Source: page 123 of http://www.intel.com/content/dam/www...-datasheet.pdf)

The standard recommendation is to reduce the refresh interval to 3.9ms and thereby double the refresh rate (source: http://support.lenovo.com/us/en/products/row_hammer). Doing that gave me one error per pass at the same address both times, so I reduced the interval to 75% of 3.9ms (i.e. tREFI=3510, tREFIX9=31) and it’s now error free over 8 passes overnight.

Passmark Blog
How big of a problem is it?

Figure 3. Normalized number of errors vs. manufacture date

## Results of the CMU Study

1. Most Modules Are at Risk

<table>
<thead>
<tr>
<th>Company</th>
<th>Percentage</th>
<th>Error Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>86% (37/43)</td>
<td>Up to $1.0 \times 10^7$ errors</td>
</tr>
<tr>
<td>B</td>
<td>83% (45/54)</td>
<td>Up to $2.7 \times 10^6$ errors</td>
</tr>
<tr>
<td>C</td>
<td>88% (28/32)</td>
<td>Up to $3.3 \times 10^5$ errors</td>
</tr>
</tbody>
</table>

ECC helps but will not prevent undetected data corruption

- Error Correction Codes on DDR3 are Single Error Detection and Correction and Double Error Detection

- Research showed more than 2 bits on a single 64 bit access
  - However the rate of failures was much less

- Multibit errors will not be detected or erroneously flagged as SEDC
Mitigation Strategies

• Row Activate Counters: Counts Activates to ROWS and issues dummy ACT to neighboring rows
  — Requires significant changes the memory controller/DRAM

• Probabilistic Row Activation: Memory controller issues dummy ACT commands to neighboring rows
  — Requires changes to the memory controller and knowledge of the DRAM layout

• Double the Refresh Rate
  — Best Solution: Performance and power penalty

• Targeted Row Refresh
  — Requires special DRAM and changes to memory controller
FuturePlus Systems Response

• Re-purposed our DDR Detective® Protocol Analyzer to count ACT commands to unique row addresses
Testing the system for excessive ACTIVATE commands
The industries response

• Blog Posts
  – Several that list failing parts
• Websites with Row Hammer mitigation
• Software to recreate the problem
  – Github [https://github.com/google/rowhammer-test](https://github.com/google/rowhammer-test)
• FuturePlus Systems working to form an industry group to produce quality information
A call to action

- If you are using DDR memory in your designs be aware of this issue
- Promote standards that include compliance testing of DDR Memory
- If you are concerned about this problem contact me
  - Industry groups are forming
Summary

- DDR3 Memory is everywhere!
- Critical Applications need to be aware of this issue
  - It’s both a reliability issue and a security issue
- ECC protected memory should be used but is not a fix for this problem
Contact Information

Barbara P. Aichinger
FuturePlus Systems
Barb.Aichinger@FuturePlus.com
603-472-5905
www.FuturePlus.com
www.DDRDetective.com