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

FuturePlus Systems
010011001010101000000110110001110101
Power Tools for Bus Analysis

Outline

- What is Row Hammer?
- What Research has been done?
  - CMU
  - Google Project Zero
  - Java Script
  - Third IO
- ECC
- Mitigation Strategies
- Software that creates Row Hammer
- Summary

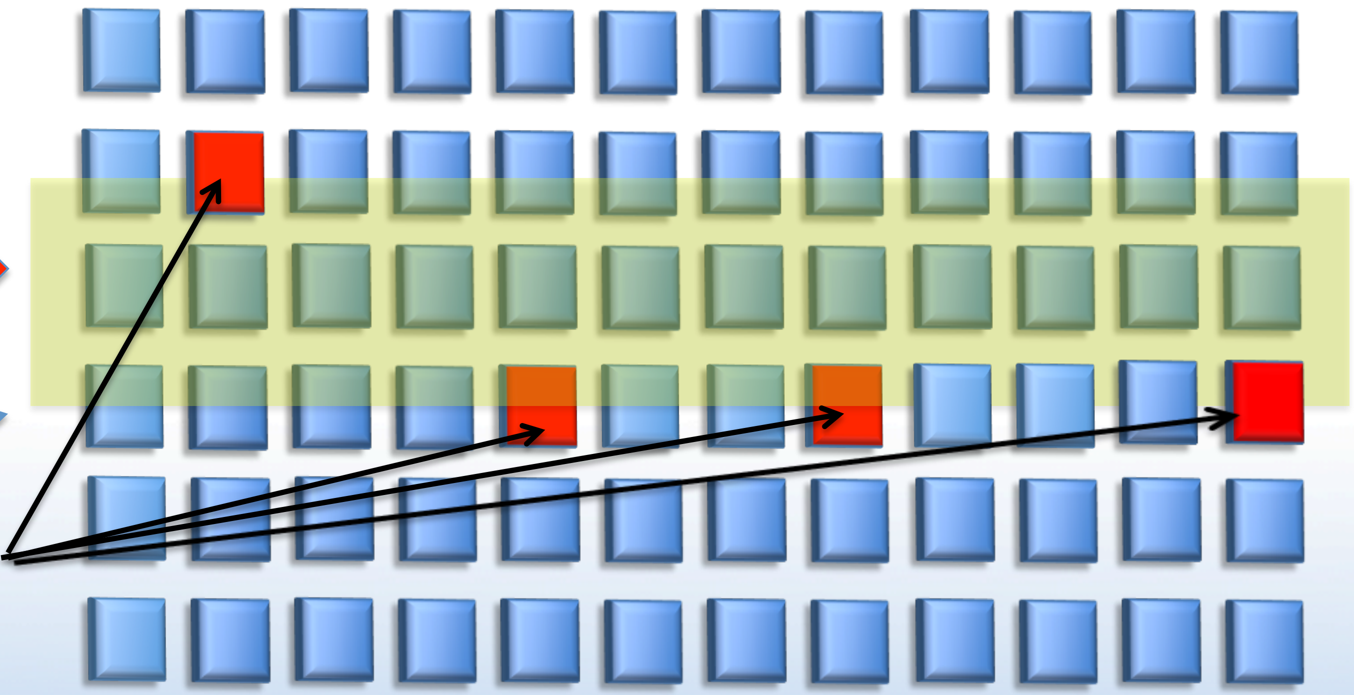
What is Row Hammer?

- Disturbance Errors: Row to Row Coupling

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/

memcon

01001100101010100000110110001110101

Power Tools for Bus Analysis

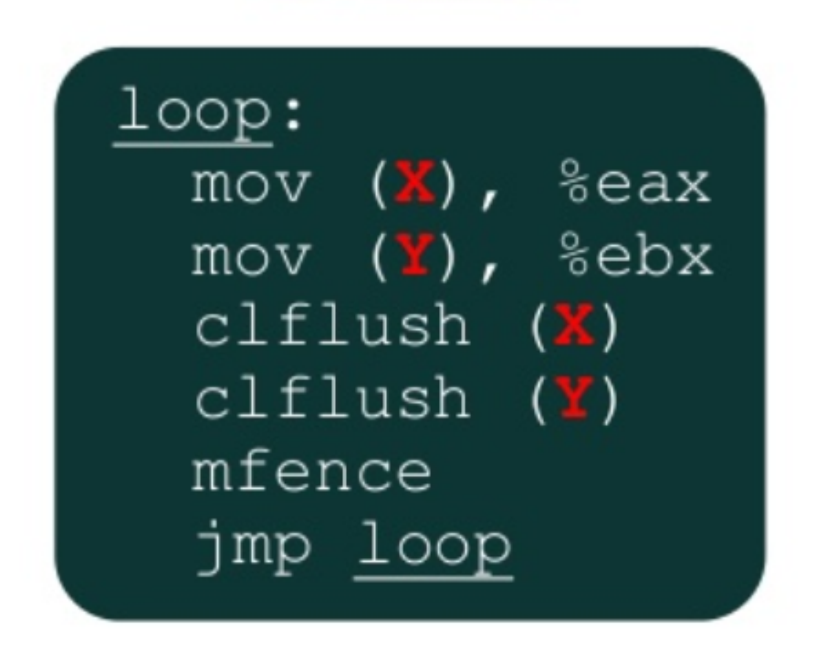
FuturePlus Systems

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

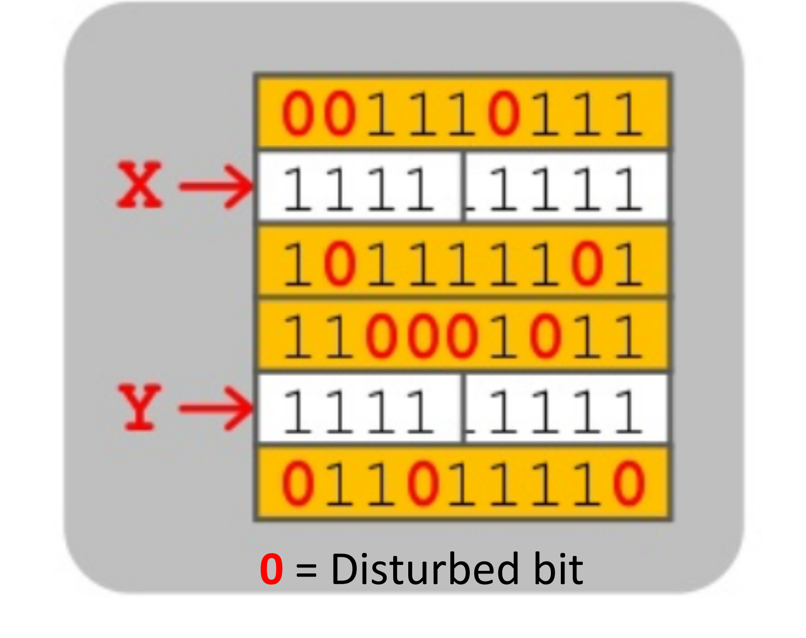
Yoongu Kim[1] Ross Daly* Jeremie Kim[1] Chris Fallin* Ji Hye Lee[1]
Donghyuk Lee[1] Chris Wilkerson[2] Konrad Lai Onur Mutlu[1]

[1]Carnegie Mellon University [2]Intel Labs

July 2014



```
loop:
  mov   (X), %eax
  mov   (Y), %ebx
  clflush (X)
  clflush (Y)
  mfence
  jmp loop
```



001110111
1111 1111
101111101
110001011
1111 1111
011011110

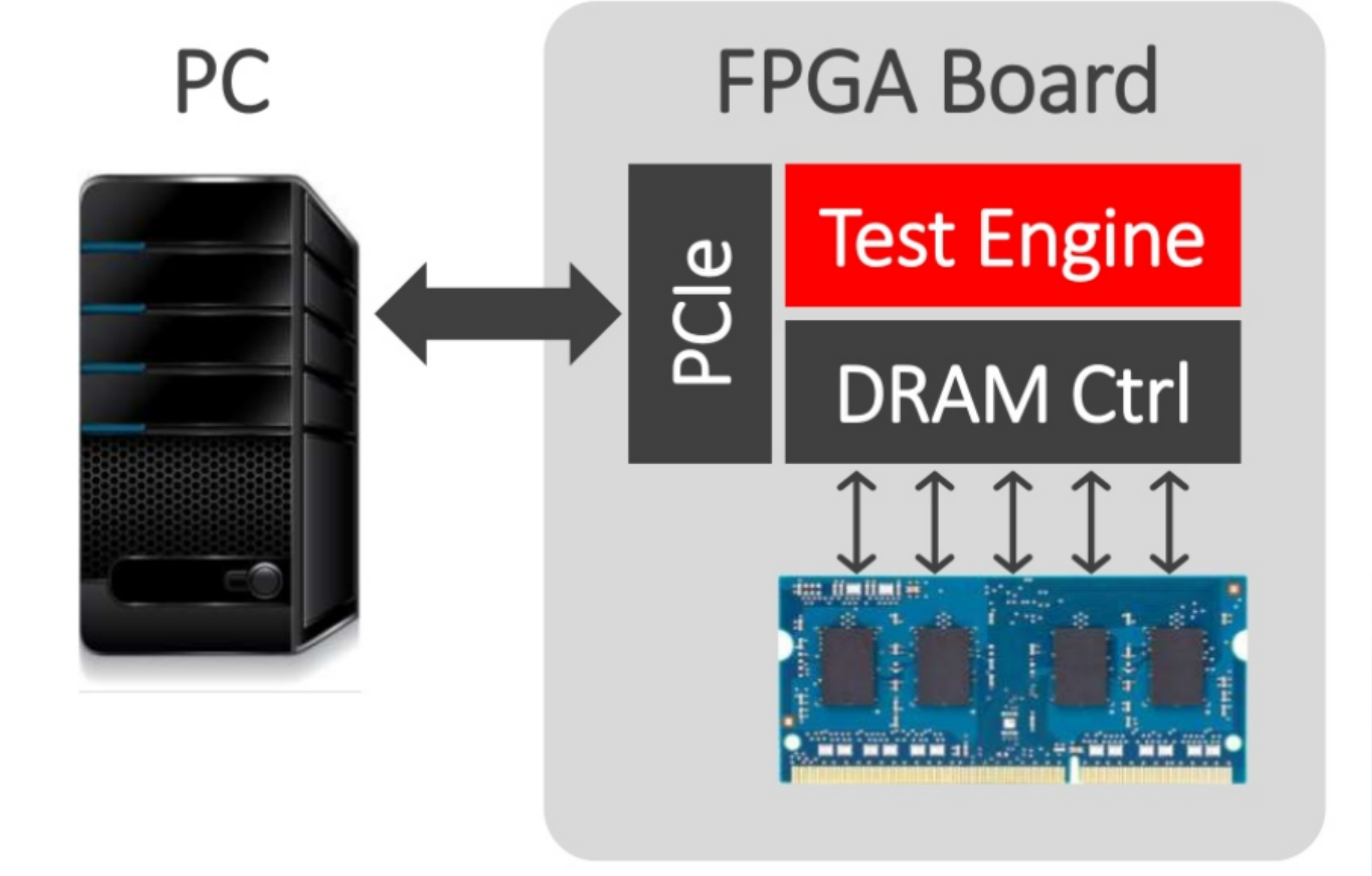
0 = Disturbed bit

Security Implications

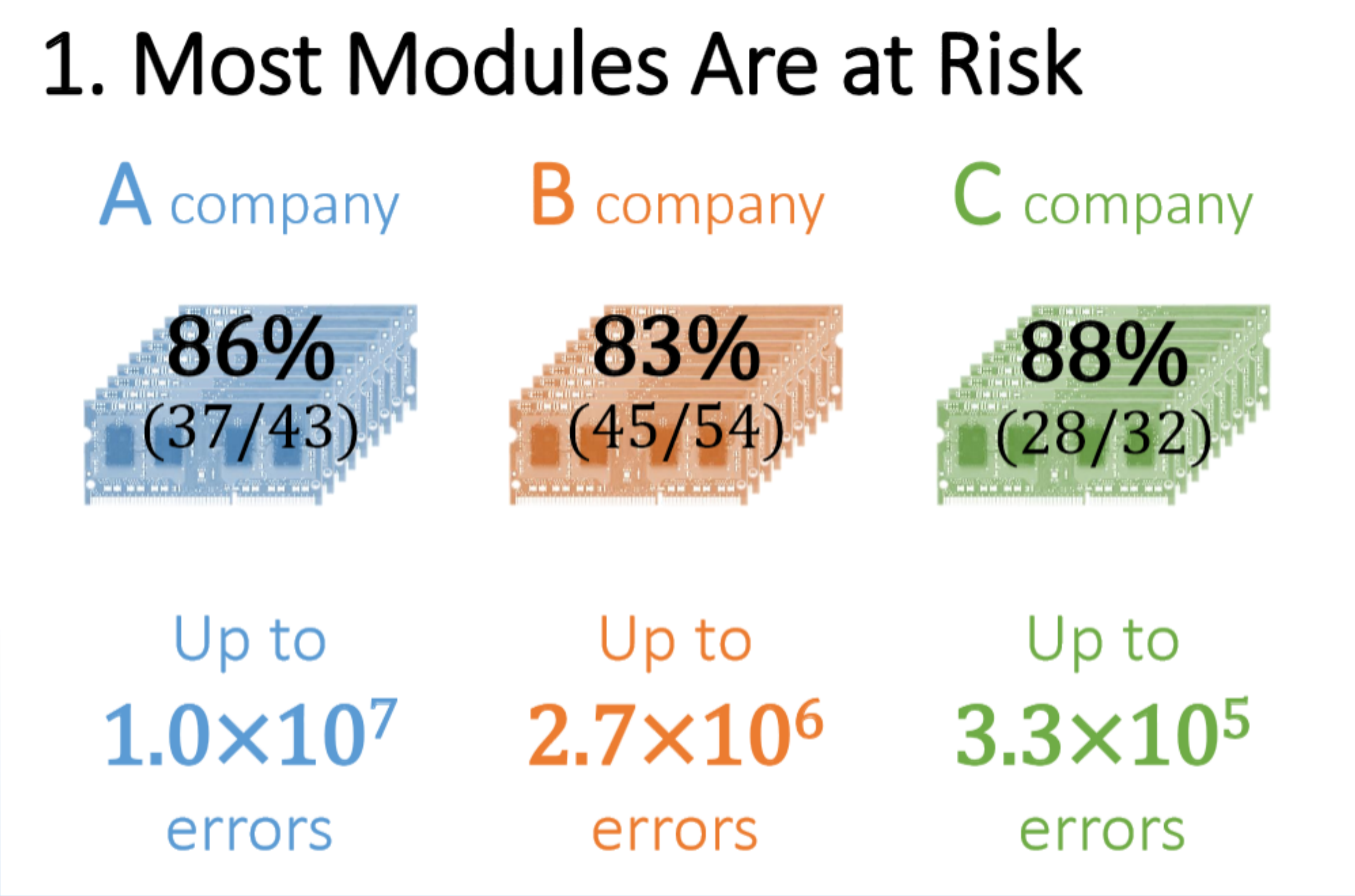
Source: CMU: Flipping bits in Memory without accessing them

- Breach of memory protection
  - OS page (4KB) fits inside DRAM row (8KB)
  - Adjacent DRAM row is a different OS page
- Vulnerability: disturbance attack
  - By accessing its own page a program can corrupt pages belonging to another program

CMU then induced errors with an FPGA based system



Results



1. Most Modules Are at Risk

A company	B company	C company
86% (37/43)	83% (45/54)	88% (28/32)
Up to 1.0×10^7 errors	Up to 2.7×10^6 errors	Up to 3.3×10^5 errors

Source: https://users.ece.cmu.edu/~omutlu/pub/dram-row-hammer_kim_talk_isca14.pdf

How many errors did CMU find?

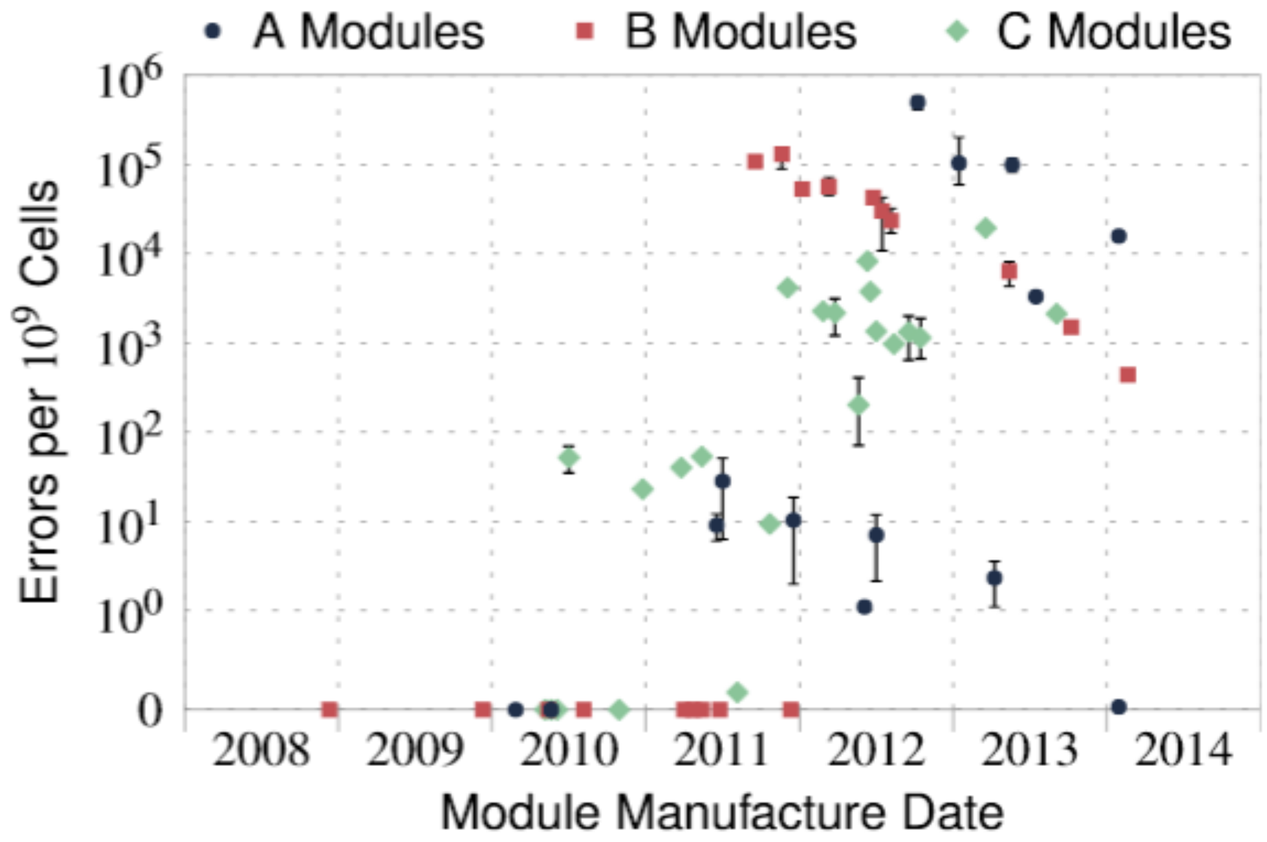


Figure 3. Normalized number of errors vs. manufacture date

Source: https://users.ece.cmu.edu/~omutlu/pub/dram-row-hammer_kim_talk_isca14.pdf

CMU Study Summary

- Temperature did not play a role in bit flips
- *“Disturbance errors are widespread in DRAM chips sold and used today”*
- *“Due to difficulties in DRAM scaling, new and unexpected types of failures may appear”*
- *Recommends a mitigation strategy of ACT or REF adjacent rows when accesses are made*
  - *Requires changes to memory controllers*
  - *Knowledge of DRAM layout*

Google: Project Zero

Exploiting the DRAM rowhammer bug to gain kernel privileges

Mark Seaborn and Thomas Dullien

- March 2015
- Demonstrated using the Row Hammer failures as an exploit to gain kernel privileges
- Used CLFLUSH instruction

Double Sided Hammering

- Increases bit flips in row n by hammering row n+1 and n-1
- Produced failures much faster
  - One machine had 25 bit flips in a single row using this technique
- Need to understand the physical geometry
  - Need to know physically adjacent row addresses
  - Was able to figure this out by hammering rows 256K below and above and observing increased bit flips

Row Hammer Exploit #1

- Native Client Sandbox in Google Chrome escape
  - Uses the CLFLUSH instruction
  - Escape from the sandbox
  - Exploit works by triggering bit flips in the indirect jump instructions

Row Hammer Exploit #2

- Page Table Entry method
  - Use Row Hammer to flip bits in PTEs
  - Causes the PTE to point to another PTE
    - To increase probability of jumping to attacking code
      - Find bits that have failed and use them since they most likely will fail again
      - Spray Memory with page tables so if you jump you will most likely hit a PTE that points to attacking code

Bit Flips in Laptops

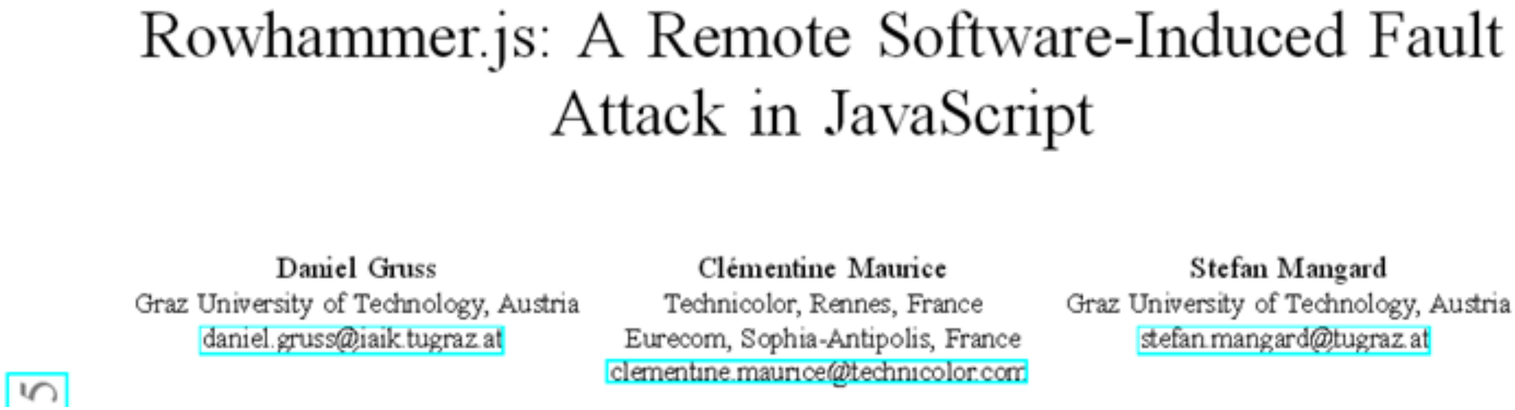
- Google tested 29 laptops (without ECC)
  - 8 different models
  - 5 different memory vendors
  - Laptops ranged in date from 2010 to 2014
  - 15 of 29 laptops showed bit flips

Project Zero Summary

- Many bugs that appear to be difficult to exploit have turned out to be exploitable
  - The poisoned NUL byte, 2014 edition
    - a off-by-one NUL byte overwrite could be exploited to gain root privileges from a normal user account
  - Using Random bit flips: "Using Memory Errors to Attack a Virtual Machine" by Sudhakar Govindavajhala and Andrew W. Appel 2004

Project Zero Summary

- Recommends disallowing the CLFLUSH for use in unprivileged code
  - Was removed from Google Chrome Native Client
- Points out several less likely methods that might succeed even without CLFLUSH
- Points at the need for more research especially using a JavaScript….this proves to be fortuitous….



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

Daniel Gruss
Graz University of Technology, Austria
daniel.gruss@iaik.tugraz.at

Clémentine Maurice
Technicolor, Rennes, France
Eurecom, Sophia-Antipolis, France
clementine.maurice@technicolor.com

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

- Replaces CLFLUSH with a cache eviction strategy that gives a 99.99% successful eviction rate
- First remote software-induced hardware fault attack
  - Does not require physical access to the machine
  - Does not use native code or special instructions
- Via a web page can be performed on millions of users simultaneously without their knowledge
- Demonstration used Firefox v39 on a Linux machine

Eviction Strategy

- Replaces the CLFLUSH instruction
- Uses large pages
  - Developed a tool to convert JavaScript array indices to physical addresses
  - This helps find the weak locations where the bit flips can be exploited
- Verified its eviction strategy for Sandy Bridge, Ivy Bridge and Haswell CPUs

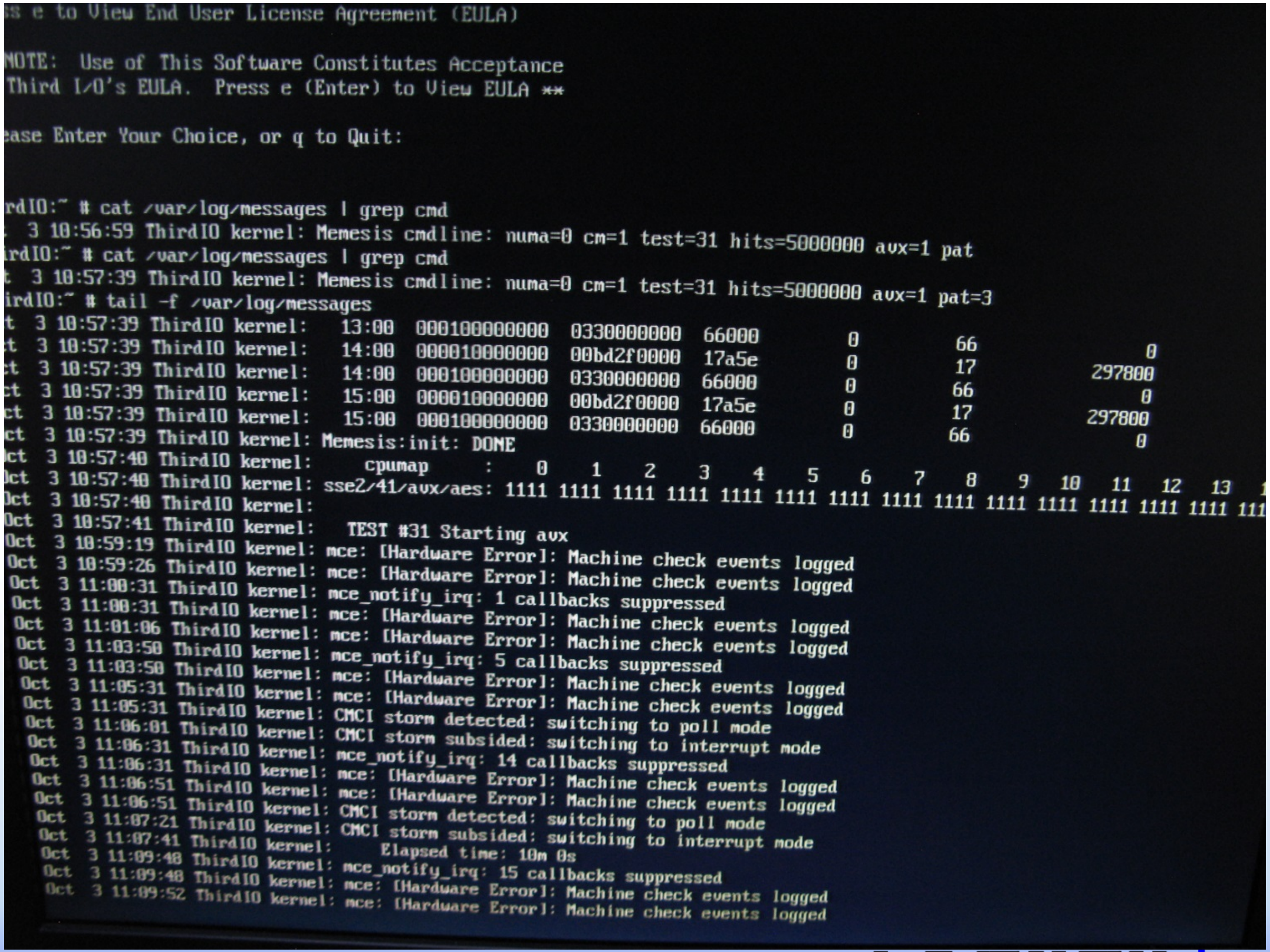
Results

- JavaScript code performed as well as native code, but not as well as CLFLUSH
  - – Haswell
    - No success unless the refresh rate was lowered
  - – Ivy Bridge laptop
    - Produced significant bit flips

Row Hammer Failures in Servers

- Third IO Mark Lanteigne
  - Memesis: A enterprise memory test
    - It is Linux Kernel Embedded, Lower Overhead and Is Closer to Hardware
    - Uses the e820 memory map and ACPI NUMA for precise memory targeting
    - HPC Parallel Processing – uses the full power of all CPU cores
    - Provides higher DRAM bandwidth versus the Stream benchmark (verified)

Row Hammer Failures resulting in Machine Checks



```
ss e to View End User License Agreement (EULA)

NOTE:  Use of This Software Constitutes Acceptance
 Third I/O's EULA.  Press e (Enter) to View EULA **

ease Enter Your Choice, or q to Quit:


rdIO:~ # cat /var/log/messages | grep cmd
  3 10:56:59 ThirdIO kernel: Memesis cmdline: numa=0 cm=1 test=31 hits=5000000 avx=1 pat
irdIO:~ # cat /var/log/messages | grep cmd
t  3 10:57:39 ThirdIO kernel: Memesis cmdline: numa=0 cm=1 test=31 hits=5000000 avx=1 pat=3
irdIO:~ # tail -f /var/log/messages
t  3 10:57:39 ThirdIO kernel:   13:00  000100000000  0330000000  66000        0        66            0
t  3 10:57:39 ThirdIO kernel:   14:00  000010000000  00bd2f0000  17a5e        0        17       297800
t  3 10:57:39 ThirdIO kernel:   14:00  000100000000  0330000000  66000        0        66            0
ct  3 10:57:39 ThirdIO kernel:   15:00  000010000000  00bd2f0000  17a5e        0        17       297800
ct  3 10:57:39 ThirdIO kernel:   15:00  000100000000  0330000000  66000        0        66            0
ct  3 10:57:39 ThirdIO kernel: Memesis:init: DONE
ct  3 10:57:40 ThirdIO kernel:     cpumap     :    0    1    2    3    4    5    6    7    8    9   10   11   12   13   1
ct  3 10:57:40 ThirdIO kernel: sse2/41/avx/aes: 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 111
Oct  3 10:57:40 ThirdIO kernel:
Oct  3 10:57:41 ThirdIO kernel:   TEST #31 Starting avx
Oct  3 10:59:19 ThirdIO kernel: mce: [Hardware Error]: Machine check events logged
Oct  3 10:59:26 ThirdIO kernel: mce: [Hardware Error]: Machine check events logged
Oct  3 11:00:31 ThirdIO kernel: mce_notify_irq: 1 callbacks suppressed
Oct  3 11:00:31 ThirdIO kernel: mce: [Hardware Error]: Machine check events logged
Oct  3 11:01:06 ThirdIO kernel: mce: [Hardware Error]: Machine check events logged
Oct  3 11:03:50 ThirdIO kernel: mce_notify_irq: 5 callbacks suppressed
Oct  3 11:03:50 ThirdIO kernel: mce: [Hardware Error]: Machine check events logged
Oct  3 11:05:31 ThirdIO kernel: mce: [Hardware Error]: Machine check events logged
Oct  3 11:05:31 ThirdIO kernel: CMCI storm detected: switching to poll mode
Oct  3 11:06:01 ThirdIO kernel: CMCI storm subsided: switching to interrupt mode
Oct  3 11:06:31 ThirdIO kernel: mce_notify_irq: 14 callbacks suppressed
Oct  3 11:06:31 ThirdIO kernel: mce: [Hardware Error]: Machine check events logged
Oct  3 11:06:51 ThirdIO kernel: mce: [Hardware Error]: Machine check events logged
Oct  3 11:06:51 ThirdIO kernel: CMCI storm detected: switching to poll mode
Oct  3 11:07:21 ThirdIO kernel: CMCI storm subsided: switching to interrupt mode
Oct  3 11:07:41 ThirdIO kernel:     Elapsed time: 10m 0s
Oct  3 11:09:48 ThirdIO kernel: mce_notify_irq: 15 callbacks suppressed
Oct  3 11:09:48 ThirdIO kernel: mce: [Hardware Error]: Machine check events logged
Oct  3 11:09:52 ThirdIO kernel: mce: [Hardware Error]: Machine check events logged
```

ECC Systems are Vulnerable

- Third I/O often encounters ECC protected servers that can be extremely vulnerable to Row Hammer
- Even after 2X refresh mitigation in place
- ECC errors (with thresholding, means hundreds of errors before first reporting)
- CMCI Storms (too many ECC errors reported)
  - ECC is broken! No reporting standards
- Performance problems, reboots, lockups, halts

ThirdIO Contact Information

- Mark Lanteigne
- lant@thirdio.com
- (512) 422-4254

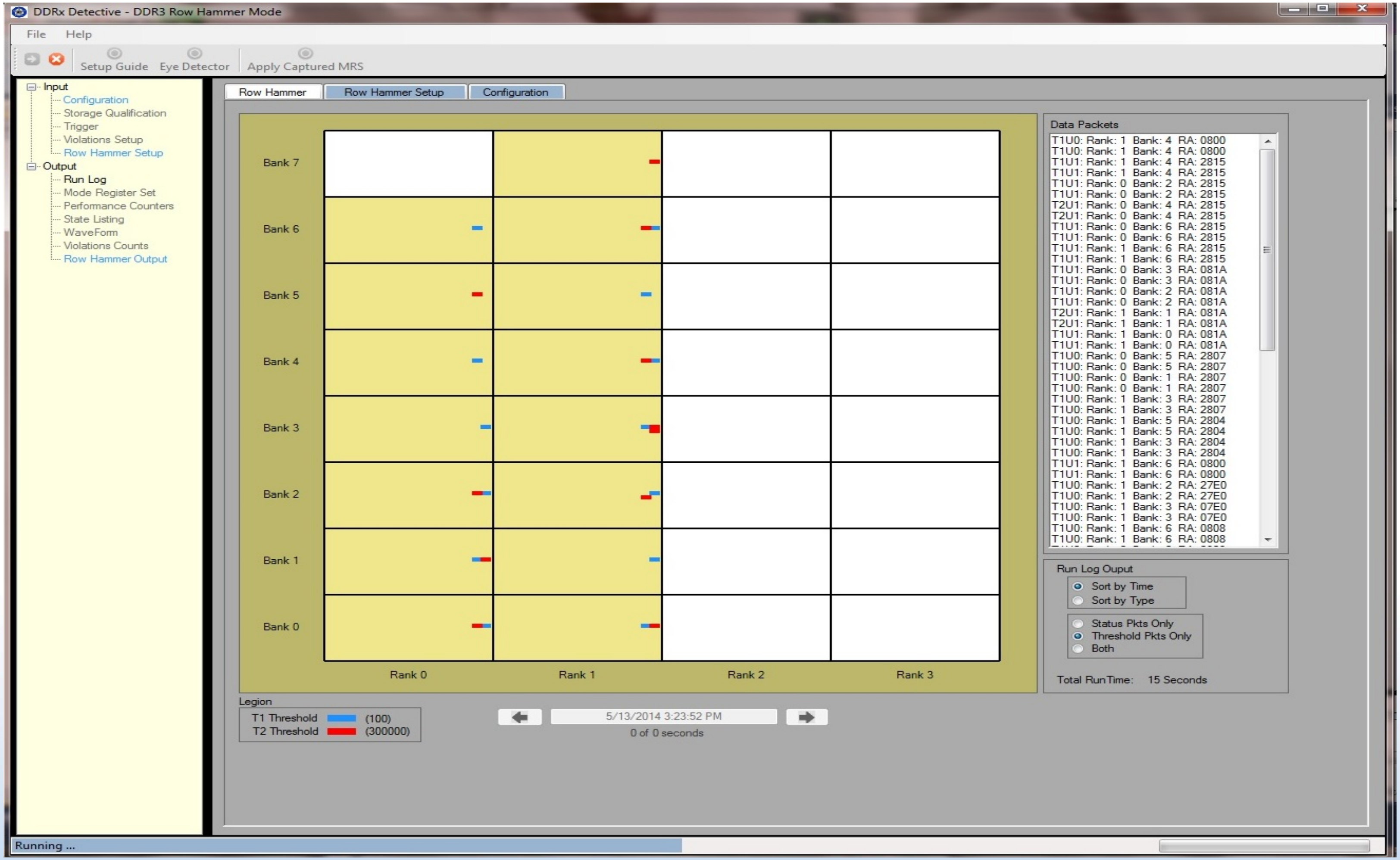
Row Hammer Software

- Passmark MemTest86 Test 13
- Github: Mark Seaborn's code
  - https://github.com/google/rowhammer-test
- Github: CMU code
  - https://github.com/CMU-SAFARI/rowhammer
- Github: Rowhammer.js
  - https://github.com/IAIK/rowhammerjs
- ThirdIO: Memesis for Servers

Testing the system for excessive ACTIVATE commands

- Repurposed our DDR Detective® Protocol Analyzer to count ACT commands to unique Row Addresses (Row Hammer feature)

Running the Google code



Data Packets

```
T1U0: Rank: 1  Bank: 4  RA: 0800
T1U0: Rank: 1  Bank: 4  RA: 0800
T1U1: Rank: 1  Bank: 4  RA: 2815
T1U1: Rank: 1  Bank: 4  RA: 2815
T1U1: Rank: 0  Bank: 2  RA: 2815
T1U1: Rank: 0  Bank: 2  RA: 2815
T2U1: Rank: 0  Bank: 4  RA: 2815
T2U1: Rank: 0  Bank: 4  RA: 2815
T1U1: Rank: 0  Bank: 6  RA: 2815
T1U1: Rank: 0  Bank: 6  RA: 2815
T1U1: Rank: 1  Bank: 6  RA: 2815
T1U1: Rank: 1  Bank: 6  RA: 2815
T1U1: Rank: 0  Bank: 3  RA: 081A
T1U1: Rank: 0  Bank: 3  RA: 081A
T1U1: Rank: 0  Bank: 2  RA: 081A
T1U1: Rank: 0  Bank: 2  RA: 081A
T2U1: Rank: 1  Bank: 1  RA: 081A
T2U1: Rank: 1  Bank: 1  RA: 081A
T1U1: Rank: 1  Bank: 0  RA: 081A
T1U1: Rank: 1  Bank: 0  RA: 081A
T1U0: Rank: 0  Bank: 5  RA: 2807
T1U0: Rank: 0  Bank: 5  RA: 2807
T1U0: Rank: 0  Bank: 1  RA: 2807
T1U0: Rank: 0  Bank: 1  RA: 2807
T1U0: Rank: 1  Bank: 3  RA: 2807
T1U0: Rank: 1  Bank: 3  RA: 2807
T1U0: Rank: 1  Bank: 5  RA: 2804
T1U0: Rank: 1  Bank: 5  RA: 2804
T1U0: Rank: 1  Bank: 3  RA: 2804
T1U0: Rank: 1  Bank: 3  RA: 2804
T1U1: Rank: 1  Bank: 6  RA: 0800
T1U1: Rank: 1  Bank: 6  RA: 0800
T1U0: Rank: 1  Bank: 2  RA: 27E0
T1U0: Rank: 1  Bank: 2  RA: 27E0
T1U0: Rank: 1  Bank: 3  RA: 07E0
T1U0: Rank: 1  Bank: 3  RA: 07E0
T1U0: Rank: 1  Bank: 6  RA: 0808
T1U0: Rank: 1  Bank: 6  RA: 0808
```

Run Log Ouput

● Sort by Time
○ Sort by Type

○ Status Pkts Only
● Threshold Pkts Only
○ Both

Total RunTime: 15 Seconds

Legion

T1 Threshold	🟦	(100)
T2 Threshold	🟥	(300000)

5/13/2014 3:23:52 PM
0 of 0 seconds

memcon

0100110010101010000011011000111010101

FuturePlus Systems

Power Tools for Bus Analysis

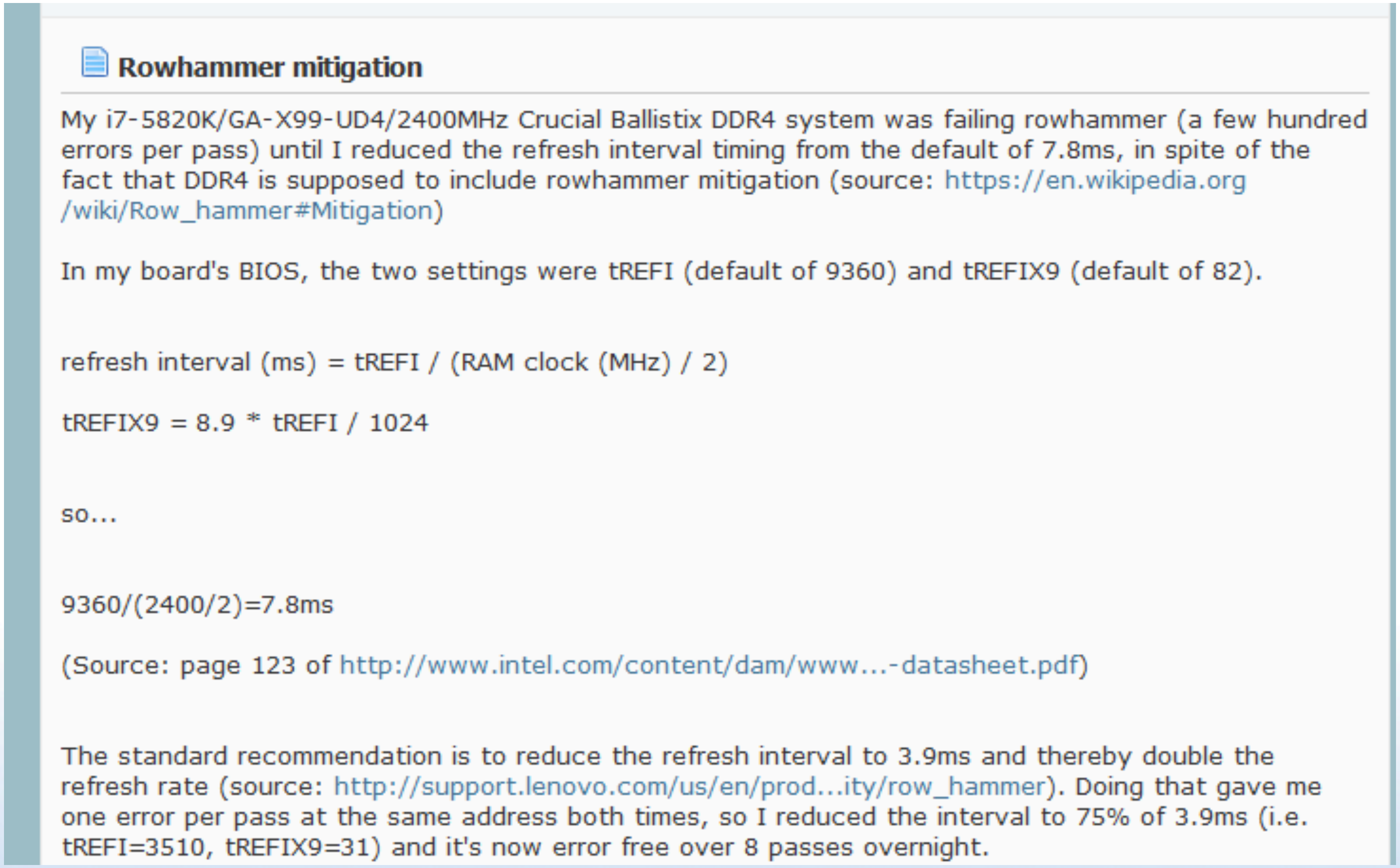
ECC helps but will not prevent undetected data corruption

- 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 (CMU): Memory controller issues dummy ACT commands to neighboring Rows
  - Requires changes to the memory controller and knowledge of the DRAM layout
- Targeted Row Refresh
  - Requires special DRAM and changes to memory controller
- Double the Refresh Rate
  - Best Solution for existing hardware: Performance and power penalty

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 * tREFI / 1024

so...

9360/(2400/2)=7.8ms

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

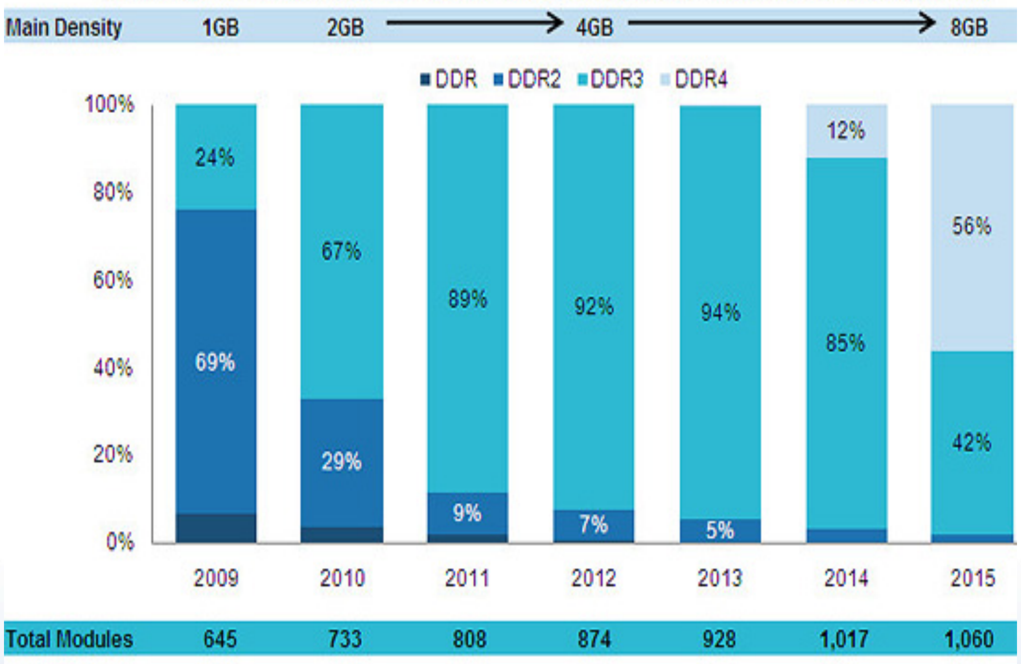
The standard recommendation is to reduce the refresh interval to 3.9ms and thereby double the refresh rate (source: http://support.lenovo.com/us/en/prod...ity/row_hammer). Doing that gave me one error per pass at the same address both times, so I reduced the interval to 75% of 3.9ms (i.e. tREFI=3510,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

Passmark Blog

Summary

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

Technology Percentage Share of DRAM Module Market (Share of Global Module Unit Shipments)



Source: IHS iSuppli Research

Contact Information

Barbara P. Aichinger

FuturePlus Systems

Barb.Aichinger@FuturePlus.com

603-472-5905

www.FuturePlus.com

www.DDRDetective.com