Rowhammer

Conor Patrick
Jean-Philippe Ouellet
Noah Luther

What is Rowhammer?

A vulnerability in DRAM hardware

Analyzed in a paper by researchers CMU and Intel Labs in 2014

Exploits developed by Google Project Zero engineers in March 2015 allow

- Escapes from Native Client sandboxing
- Privilege escalation

This is a hardware problem that allows the exploitation of software.

Because every bug must have a logo...

(and a website)

Such trend

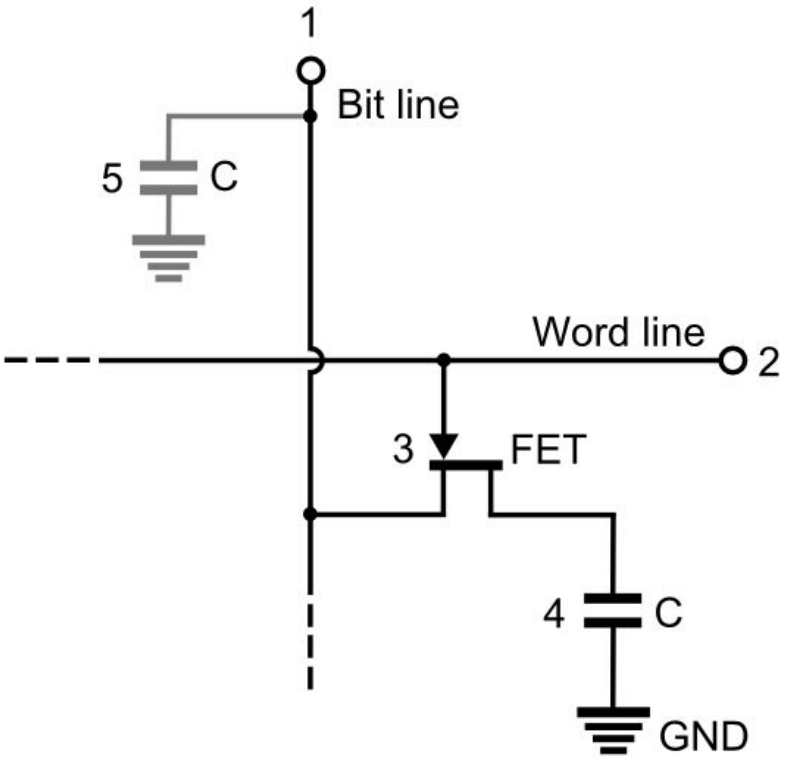
very inform

WOW

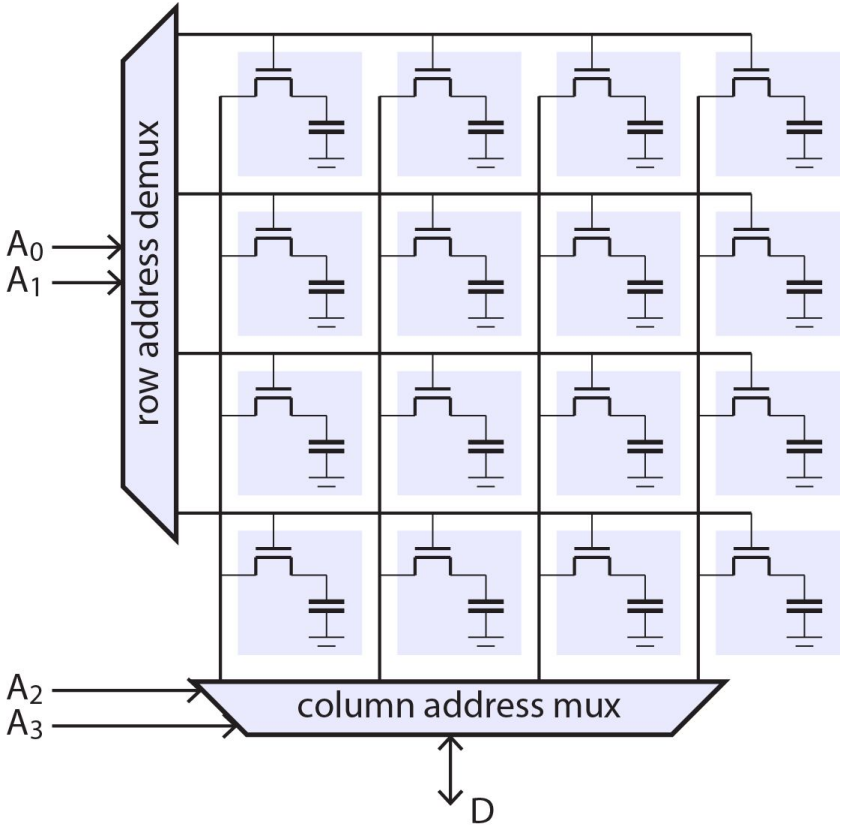
http://www.rowhammer.com/

What’s this fancy “RAM” I keep hearing about?

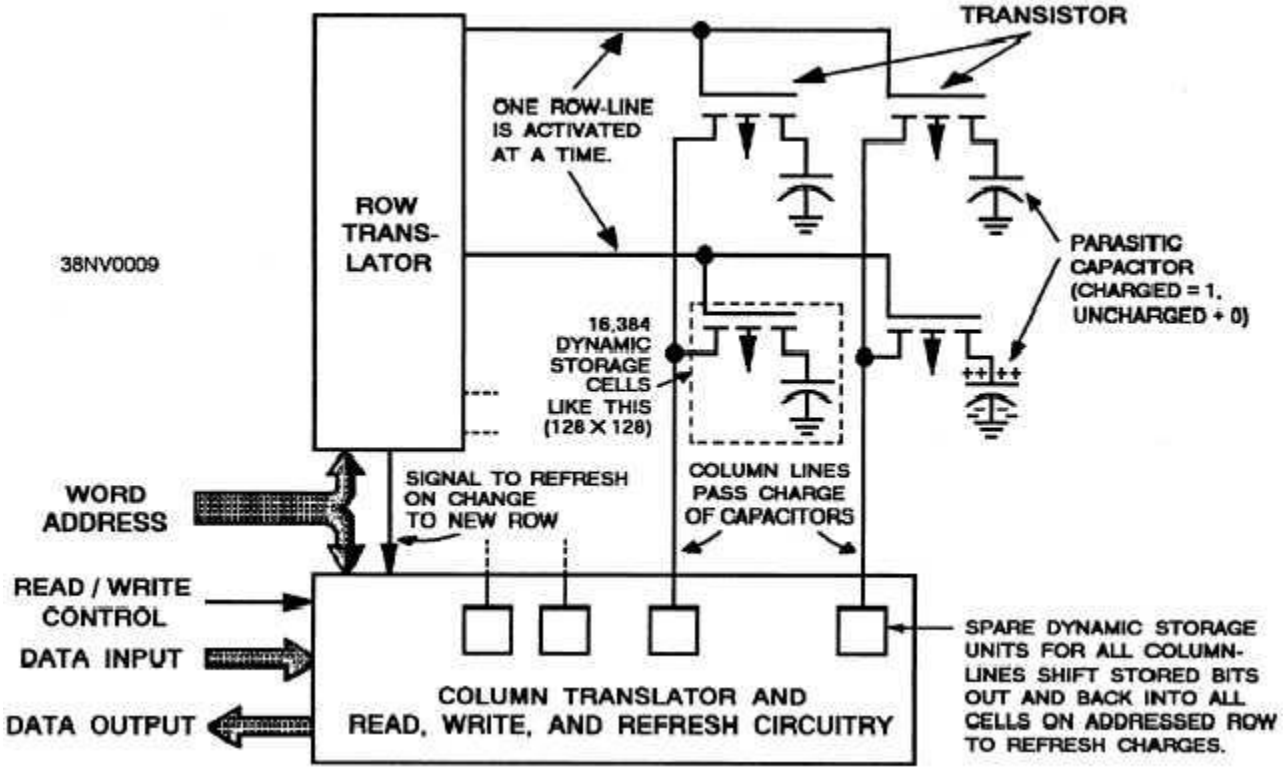
How does ram even? (just a “bit” of background)



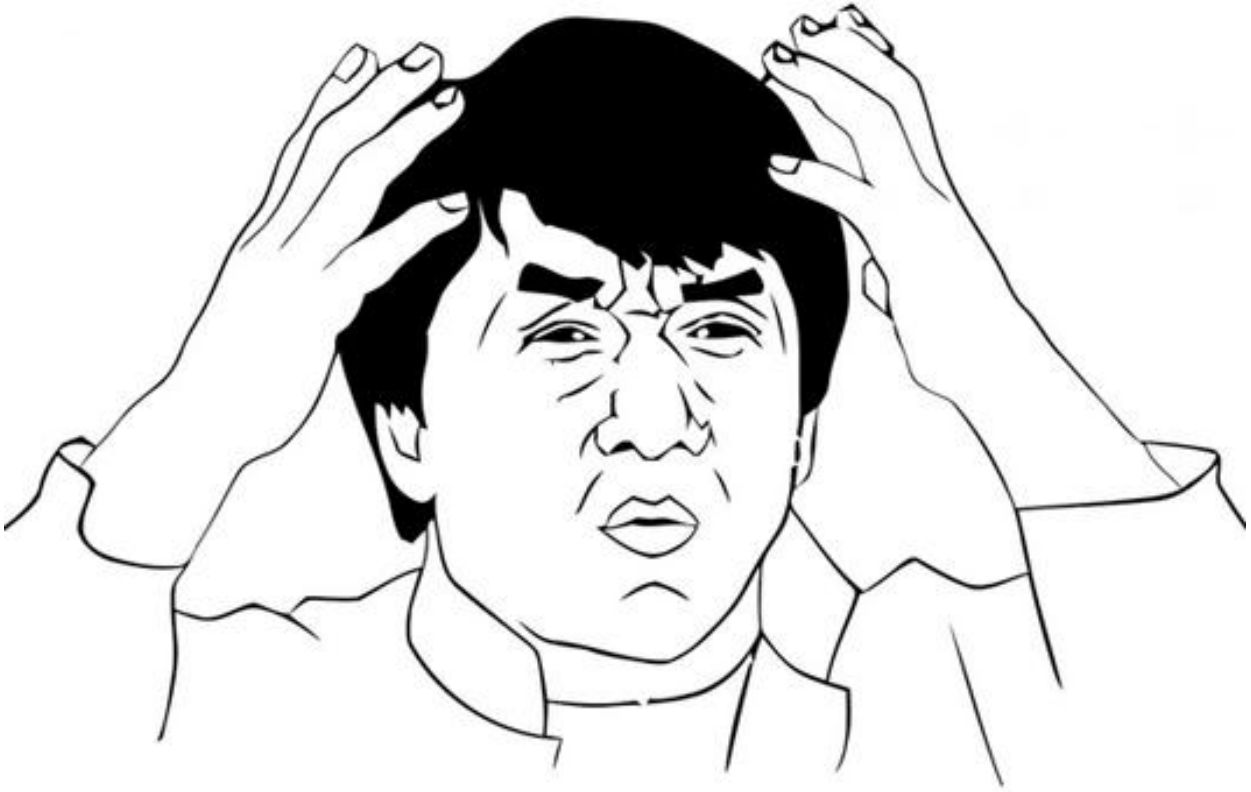
No but really, how does ram even?



(N)and then what?



And that’s exploitable!?



How does Rowhammer work?

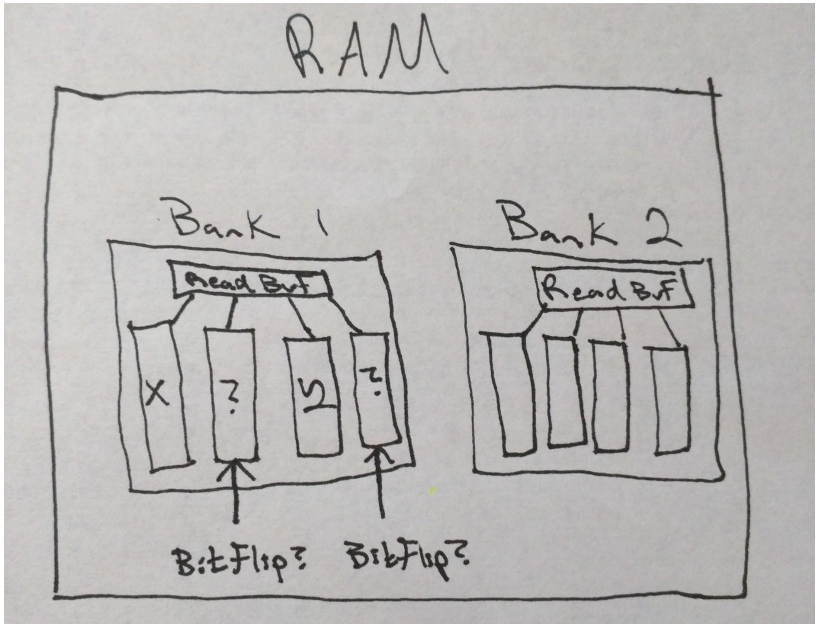
Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors

(Yoongu Kim)

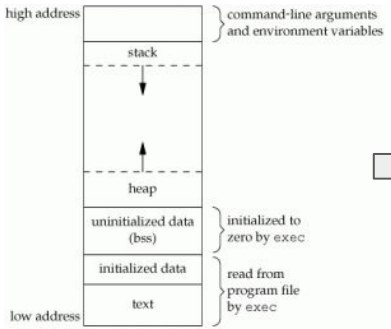
This tiny bit of code can cause bit flips in memory:

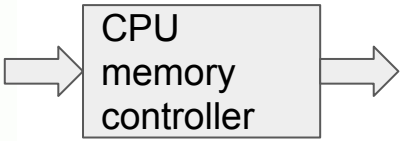
```
code1a:
  mov (X), %eax  // Read from address X
  mov (Y), %ebx  // Read from address Y
  clflush (X)    // dont stay in CPU cache!
  clflush (Y)    // dont stay in CPU cache!
  jmp code1a     // Again!
```

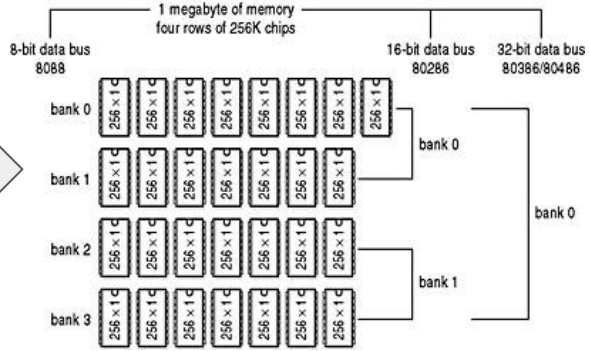
Requirement: X & Y are in different rows in the same bank



How does one find addresses to hammer?







- Yoongu Kim: Intel and AMD processors map rows in the same block such that Y=8 Mbyte + X
- So Y is logically 8 MBytes after X.

- But pages are typically only given to processes in 4k - 2Mbyte sizes!
- Do we really need to follow the specific mappings of a CPU architecture?

Bring down the hammer! (randomly!)

1. Allocate 1 GiByte of memory.
2. Randomly pick 2 addresses to hammer
3. If you're using a typical dim stick like this one, then you have a ⅛ chance of getting 2 addresses in the same bank!
4. There's so many rows in each bank, they'll almost never be in the same row.


STOP
HAMMER
TIME

You ***can*** touch this!

Github: git@github.com:google/rowhammer-test.git

Clone this repo

Run make.sh

Run rowhammer_test

- It will hammer continually, and then stop if it finds a bit flip.

DEMO TIME!

Mitigations

Error-Correcting Code (ECC) RAM

Virtualization (may raise the bar)

New Hardware

Increased Refresh Rates

Perf monitoring → look for repeated accesses

References

http://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html

http://users.ece.cmu.edu/~yoonguk/papers/kim-isca14.pdf

http://blog.erratasec.com/2015/03/some-notes-on-dram-rowhammer.html

https://www.cs.princeton.edu/~appel/papers/memerr.pdf

https://users.ece.cmu.edu/~yoonguk/papers/kim-isca14.pdf

https://github.com/google/rowhammer-test