TRRespass: Exploiting the Many Sides of Target Row Refresh

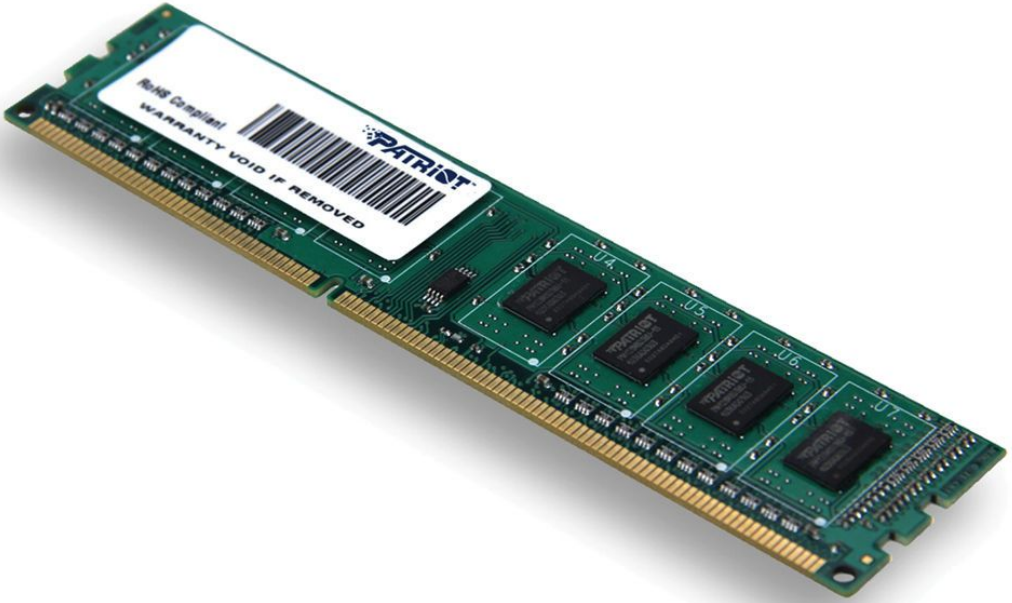
P. Frigo, E. Vannacci, H. Hassan, V. Van der Veen,
O. Mutlu, C. Giuffrida, **H. Bos**, K. Razavi

Emanuele Vannacci

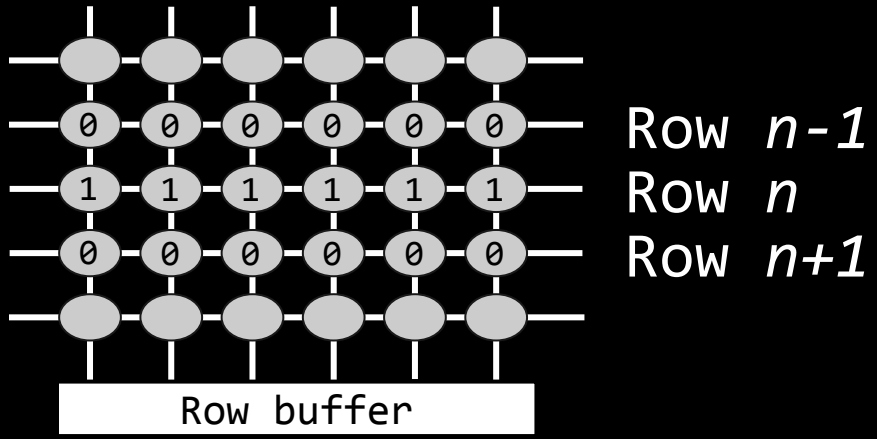
Pietro Frigo

The rise and rise and rise of

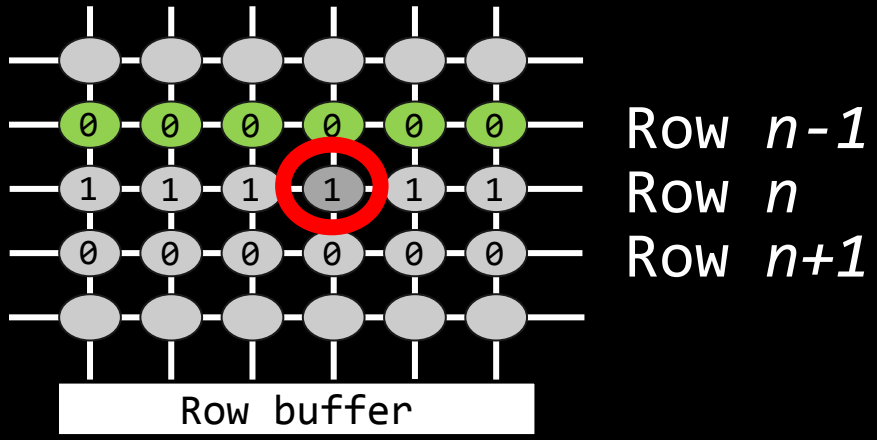
Rowhammer


RoHS Compliant
WARRANTY VOID IF REMOVED
PATRIOT

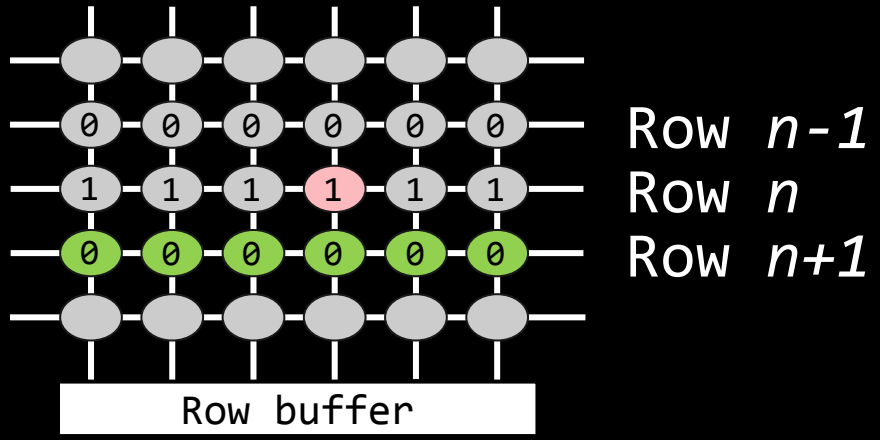
Rowhammer



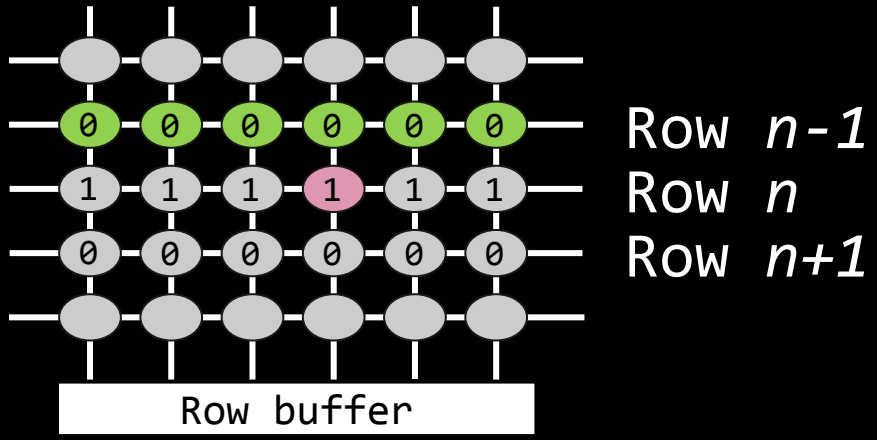
Rowhammer



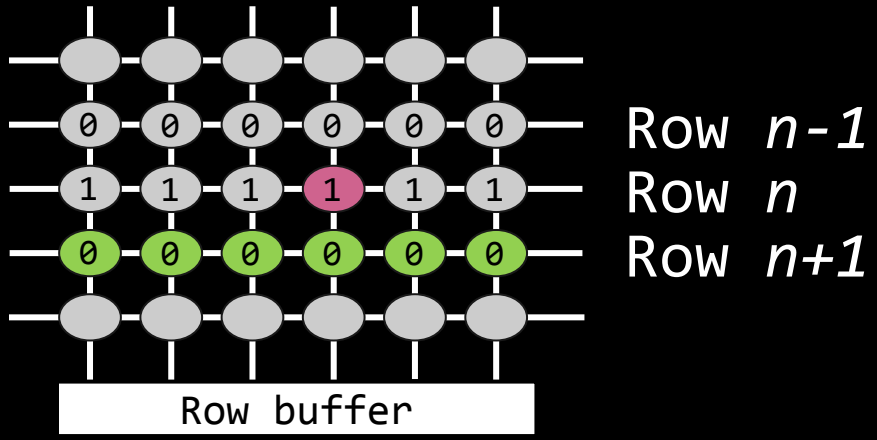
Rowhammer



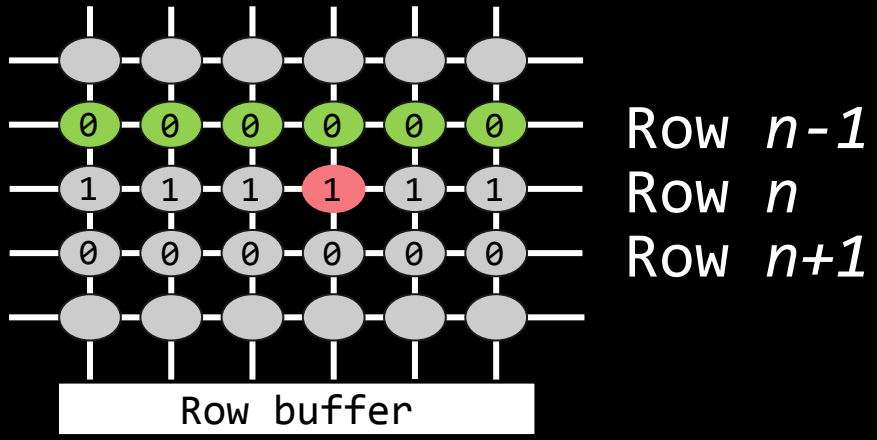
Rowhammer



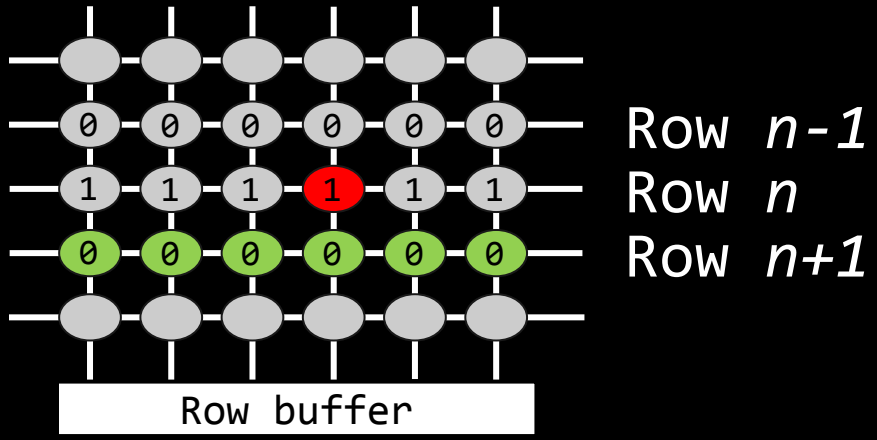
Rowhammer



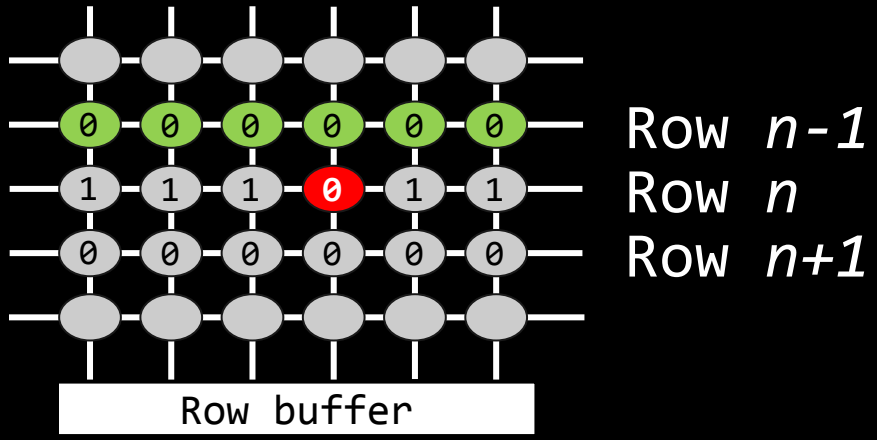
Rowhammer



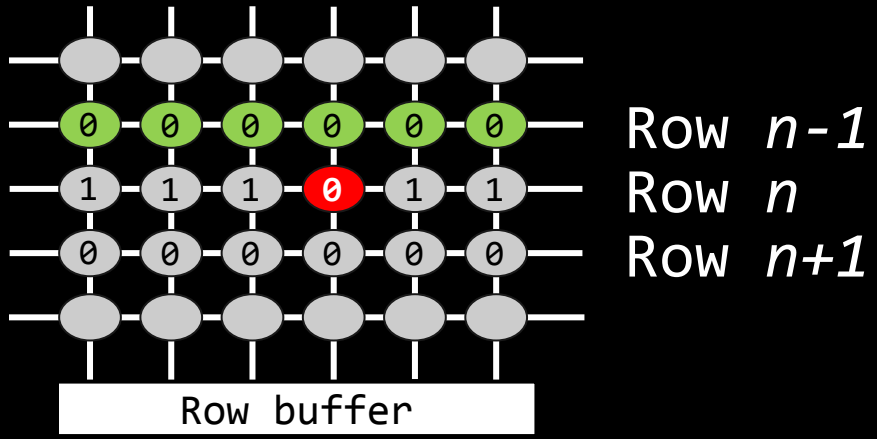
Rowhammer



Rowhammer

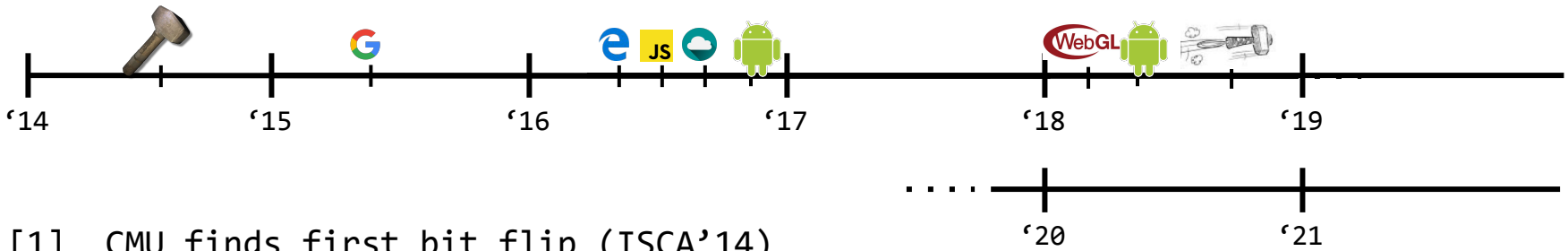


Rowhammer



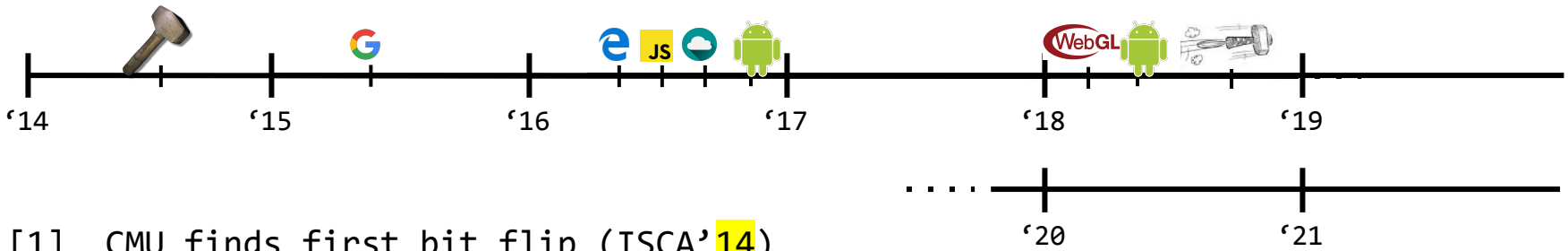
Don’t know in advance which flips, but if it flips once, it will flip again

Rowhammer Evolution



[1] CMU finds first bit flip (ISCA’14)
[2] Google Project Zero : 1st Rowhammer root exploit (flipping PTEs)
[3] Dedup Est Machina (S&P’16) : RH in MS Edge
[4] Rowhammer.js (DIMVA’16) : 1st RH bit flip in JavaScript
[5] Flip Feng Shui (USENIX SEC’16): co-located VMs in cloud
[6] DRAMMER (CCS’16) : ARM / Smartphones
[7] Grand Pwning Unit (S&P’18) : Attack from JavaScript on ARM via the GPU
[8] HammerTime (RAID’18) : RH on many DIMMS + emulator/simulator
[9] Rampage/GuardION (DIMVA’18) : DMA-based RH without ION kmalloc heap
[10] Throwhammer (USENIX ATC’18) : RH across network

Rowhammer Evolution



[1] CMU finds first bit flip (ISCA’14)
[2] Google Project Zero : 1st Rowhammer root exploit (flipping PTEs)
[3] Dedup Est Machina (S&P’16) : RH in MS Edge
[4] Rowhammer.js (DIMVA’16) : 1st RH bit flip in JavaScript
[5] Flip Feng Shui (USENIX SEC’16): co-located VMs in cloud
[6] DRAMMER (CCS’16) : ARM / Smartphones
[7] Grand Pwning Unit (S&P’18) : Attack from JavaScript on ARM via the GPU
[8] HammerTime (RAID’18) : RH on many DIMMS + emulator/simulator
[9] Rampage/GuardION (DIMVA’18) : DMA-based RH without ION kmalloc heap
[10] Throwhammer (USENIX ATC’18) : RH across network

Memory integrity is **dead**

I am not worried

server memory is much better!

ECC?

Challenge Accepted

Lucian Cojocar

I flip bits in
ECC memory!

I win awards!

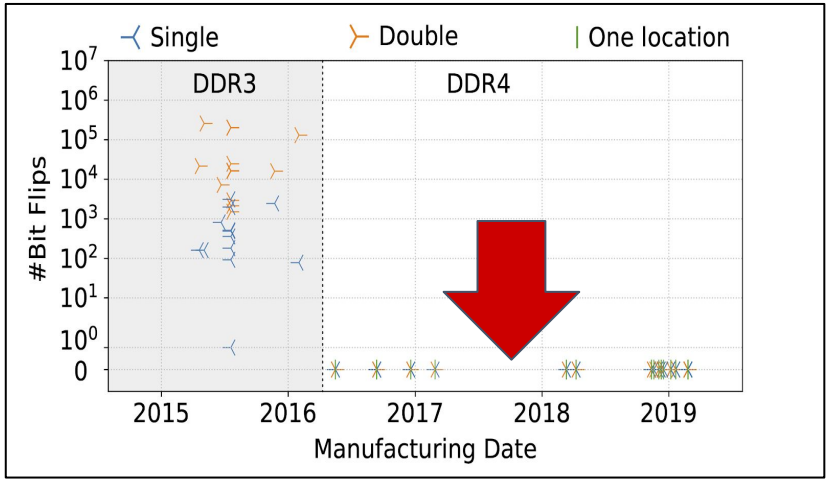
I am still not worried

new memory is much better still!

Target Row Refresh (TRR)

Track row activations: too many?→ refresh victims
Many possible implementations → unknown

DDR4 that is Rowhammer-free



pTRR DDR3

Intel reports pTRR on DDR3 server systems

In-DRAM TRR

Earliest manufacturing date of RH-free DRAM modules

'12 *'13* *'14* *'15* *'16* *'17* *'18* *'19*

DIMMs we focused on

pTRR DDR4

First DDR4 generation is pTRR protected

Reverse engineering

Analysis from CPU not possible

FPGA-based memory controller

SoftMC: A Flexible and Practical Open-Source Infrastructure for Enabling Experimental DRAM Studies

Hassan et al., HPCA'17

Reverse engineering

Analysis from CPU not possible

FPGA-based memory controller

Discovered 3 things

- sampler : keeps set of rows
- inhibitor : refreshes victims
- regret : about life choices

SoftMC: A Flexible and Practical Open-Source Infrastructure for Enabling Experimental DRAM Studies

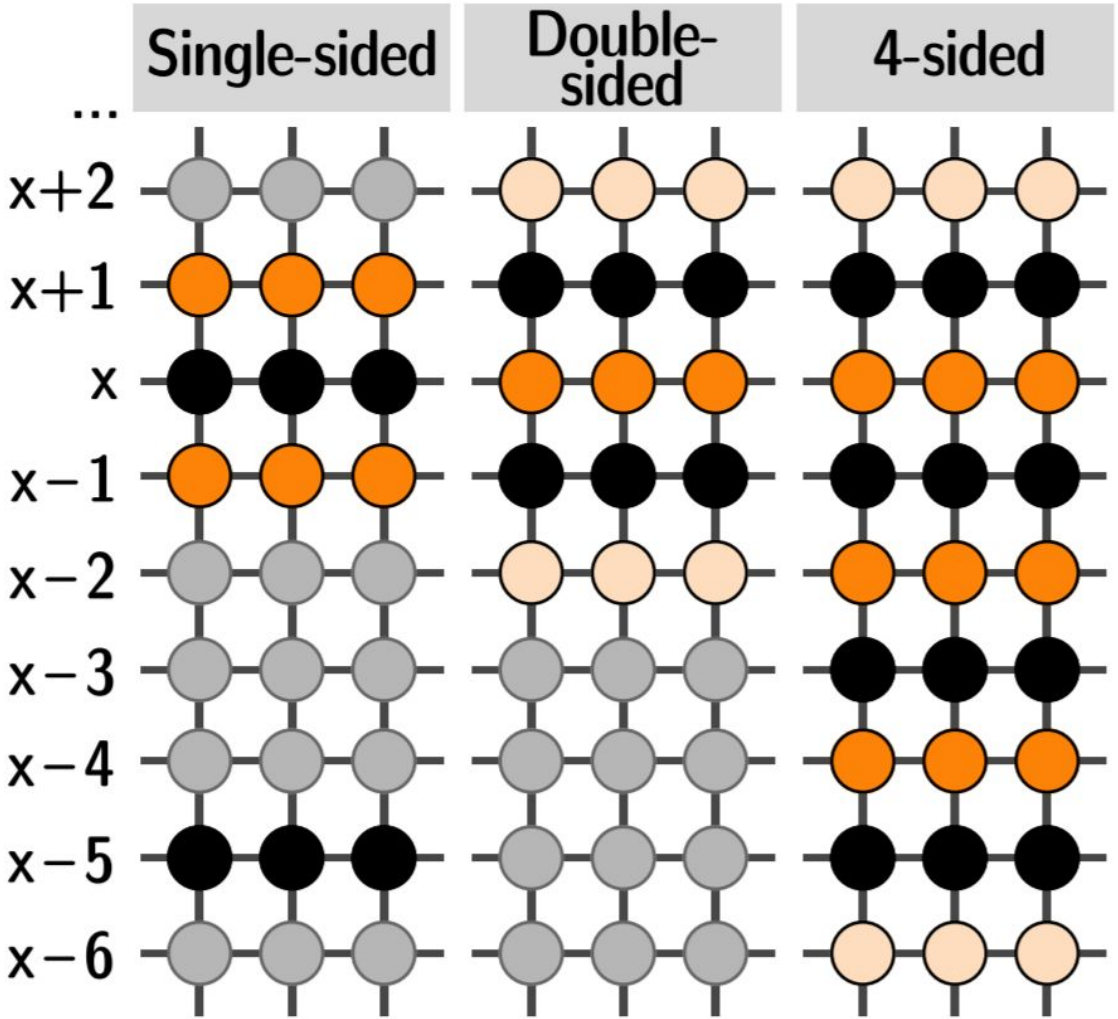
Hasan Hassan[1,2,3] Nandita Vijaykumar[3] Samira Khan[4,3] Saugata Ghose[3] Kevin Chang[3]
Gennady Pekhimenko[5,3] Donghyuk Lee[6,3] Oguz Ergin[2] Onur Mutlu[1,3]

[1]ETH Zürich [2]TOBB University of Economics & Technology [3]Carnegie Mellon University
[4]University of Virginia [5]Microsoft Research [6]NVIDIA Research

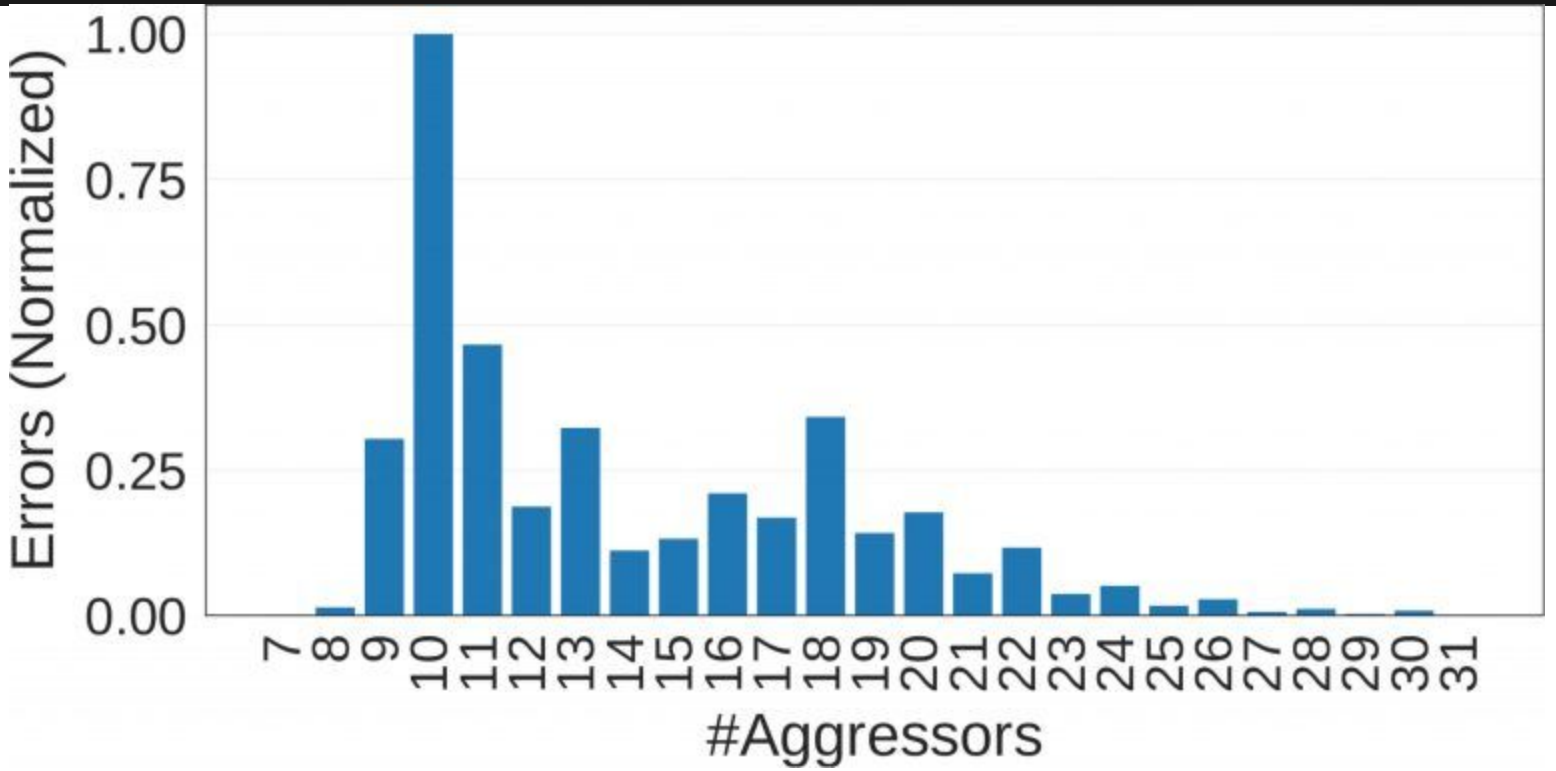
Hassan et al., HPCA'17

We need different patterns!

Need to trick TRR into tracking wrong rows!



Many-sided Rowhammer



Lawyers

Proxies

National Cyber Security Center

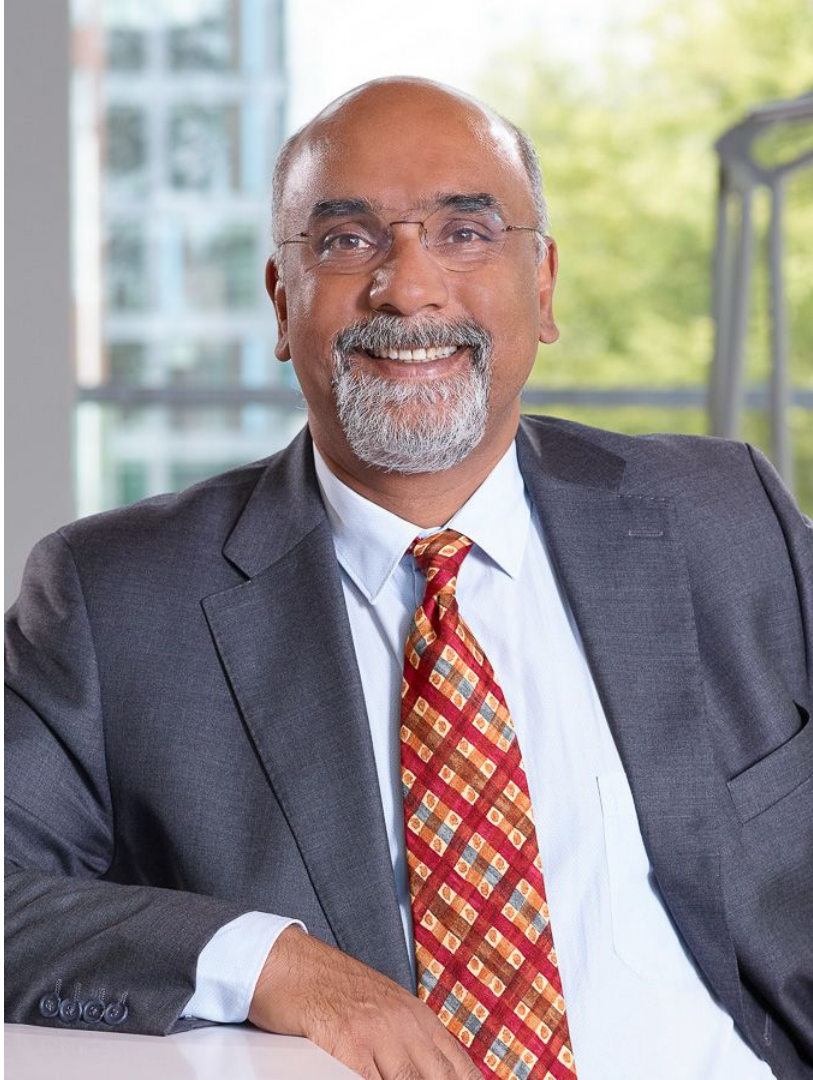
Anonymous email

Rector

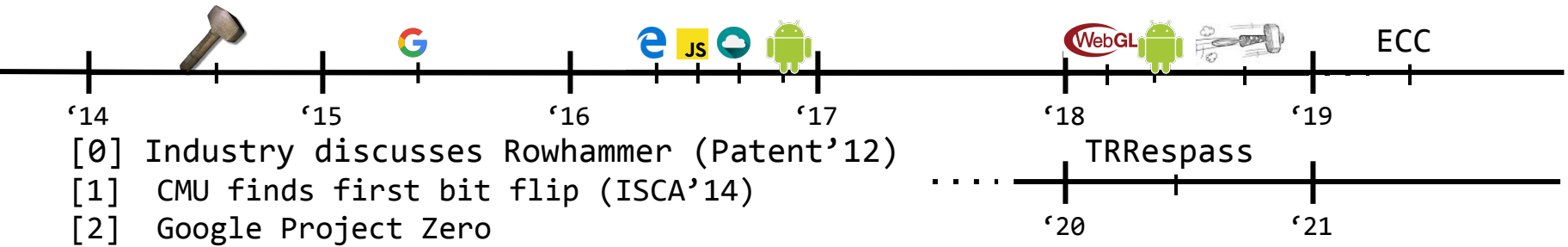
Vinod Subramaniam (rector)

Awesome

Read our paper. Twice.

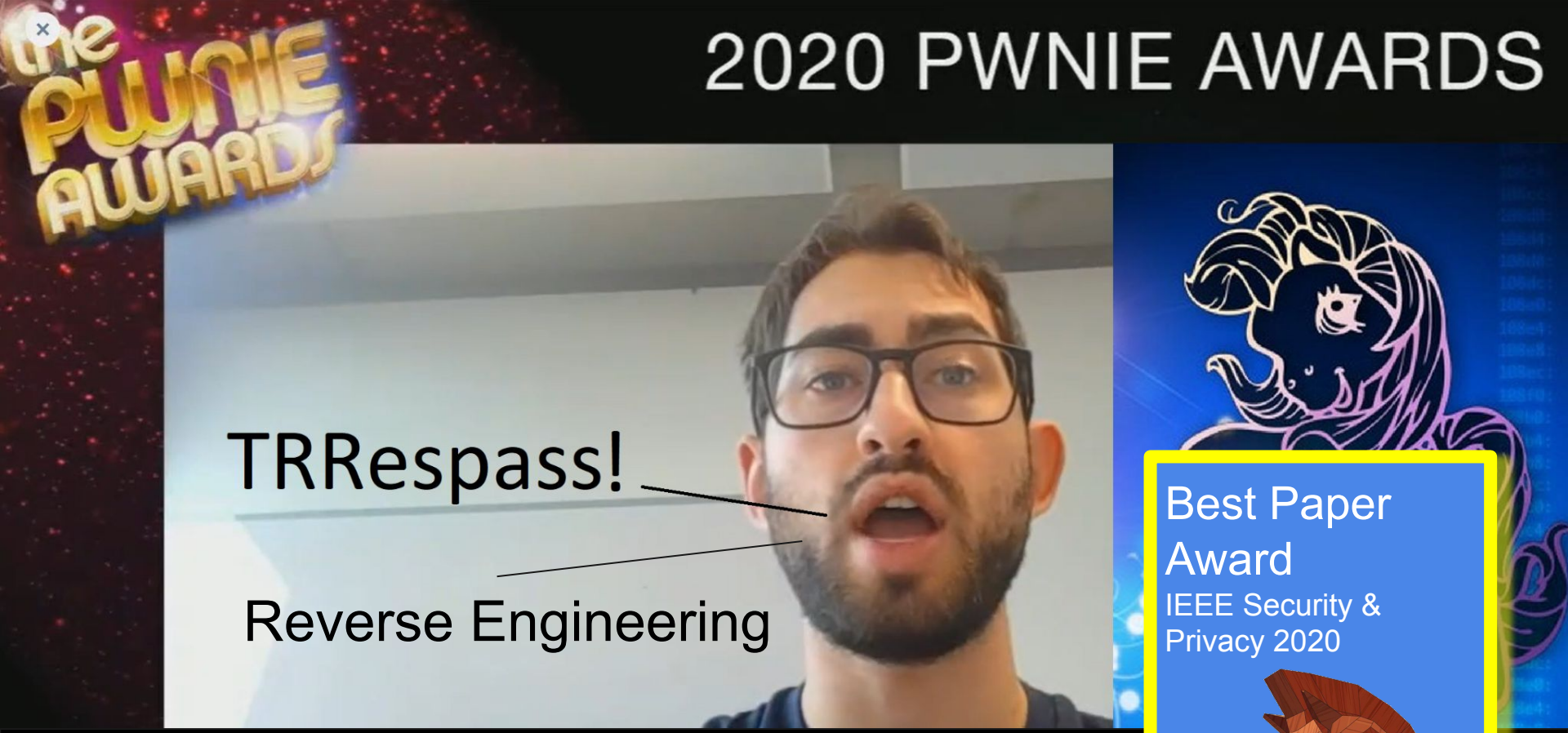


Rowhammer Evolution



[0] Industry discusses Rowhammer (Patent’12)
[1] CMU finds first bit flip (ISCA’14)
[2] Google Project Zero
[3] Dedup Est Machina (S&P’16) : RH in MS Edge
[4] Rowhammer.js (DIMVA’16) : 1st RH bit flip in JavaScript
[5] Flip Feng Shui (SEC’16) : co-located VMs in cloud
[6] DRAMMER (CCS’16) : ARM / Smartphones
[7] Grand Pwning Unit (S&P’18) : Attack from JavaScript on ARM via the GPU
[8] HammerTime (RAID’18) : RH on many DIMMS + emulator/simulator
[9] Rampage/GuardION (DIMVA’18) : DMA-based RH without ION kmalloc heap
[10] Throwhammer (USENIX ATC’18) : RH across network
[11] ECCploit (S&P’19) : RH on ECC memory
[12] TRRespass (S&P’20) : RH on DDR4 with TRR

2020 PWNIE AWARDS



TRRespass effective on **13** out of **42** tested DIMMs

The DDR4 substrate is much more vulnerable!

- Bit flips with less activations compared to RH on DDR3 devices

TRR is not secure

- TRR can track a limited number of rows at the same time.
- Thus, victim rows are not refreshed

DDR4 devices are even more vulnerable than previous versions

All major vendors are affected

- 90% of the market

We can use fuzzing on DRAM!

After 10 years RH is still a problem

No immediate mitigation