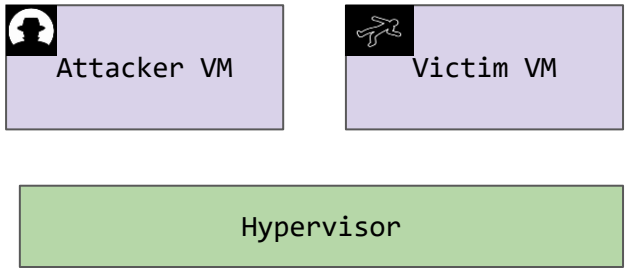
How to exploit a bit flip in order to own the cloud

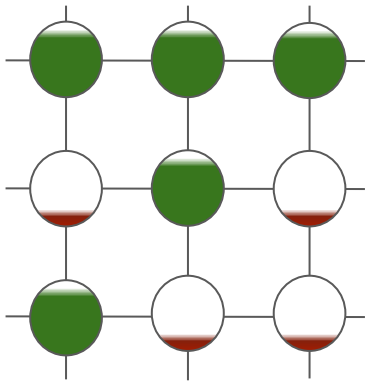
Kaveh Razavi

Cloud Threat Model(s) under Rowhammer



Possible today under **certain conditions**
with **Rowhammer** bit flips

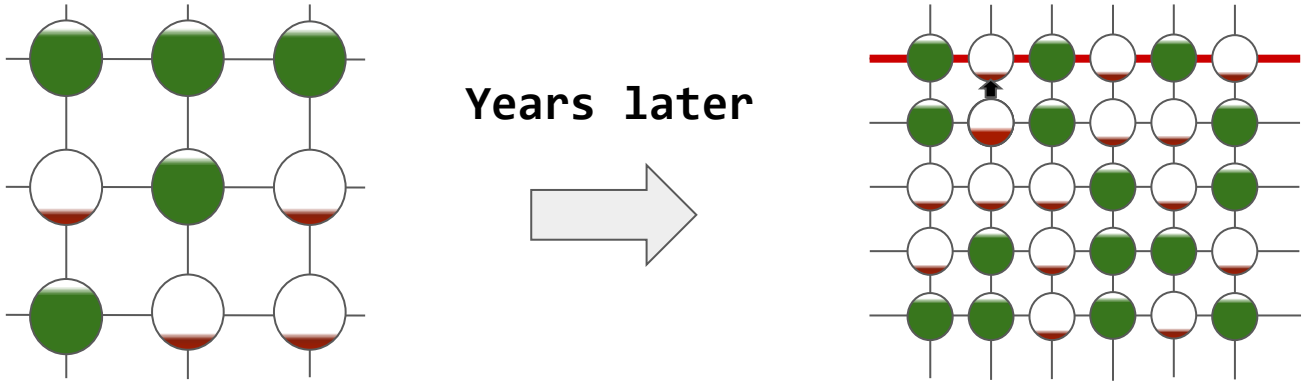
Dynamic Random Access Memory (AKA DRAM)



Each cell needs to be refreshed once in while (typically 64ms)

The Rowhammer Problem

Smaller capacitors are creating reliability problems.



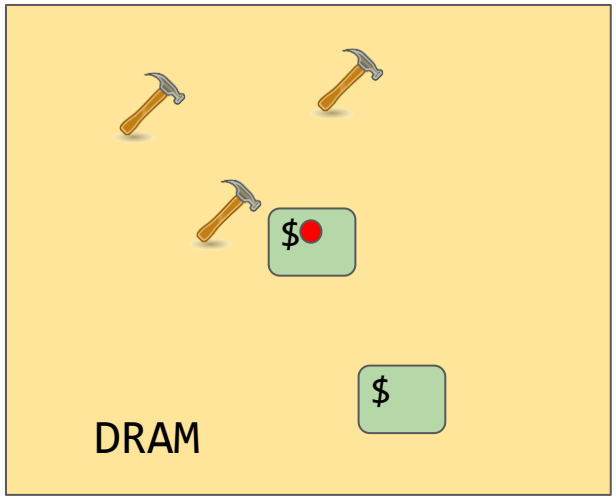
Rowhammer: affects 87% of deployed DDR3 memory, DDR4 as well.

Kim et al., “Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors,” ISCA’14

Exploiting These Flips

Random, previously unknown locations, single flips.

1) Templating
2) Massaging
3) Exploitation



Razavi et al., “Flip Feng Shui: Hammering a Needle into the Software Stack,” SEC’16

Compromising Cloud Virtual Machines

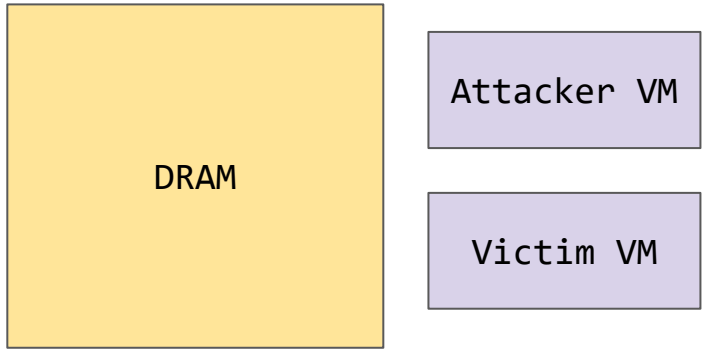
1) Templating

   Attacker's own memory

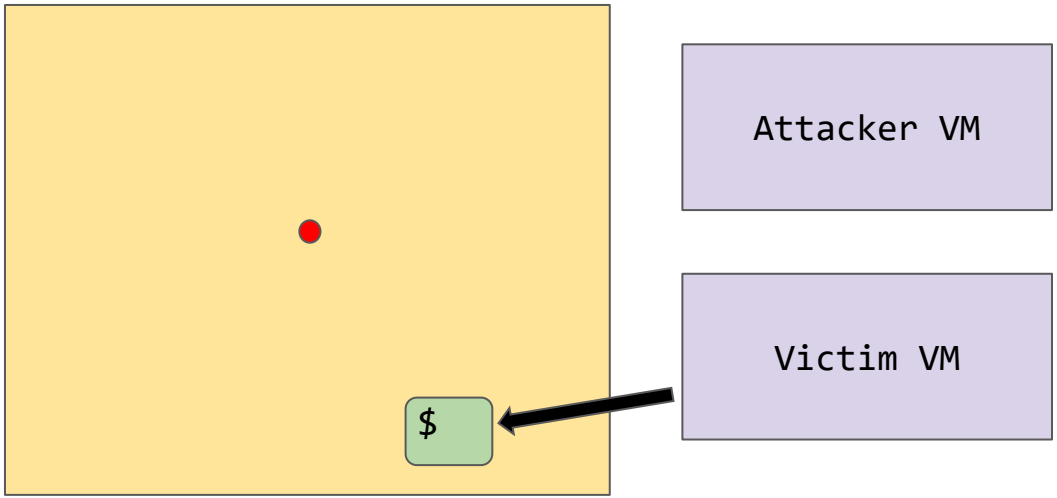
2) Massaging

   Memory deduplication

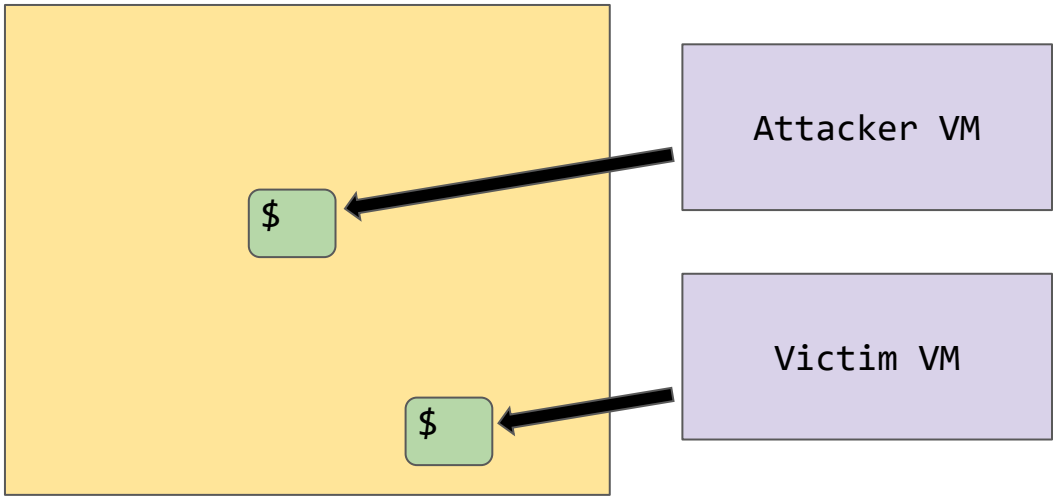
3) Exploitation



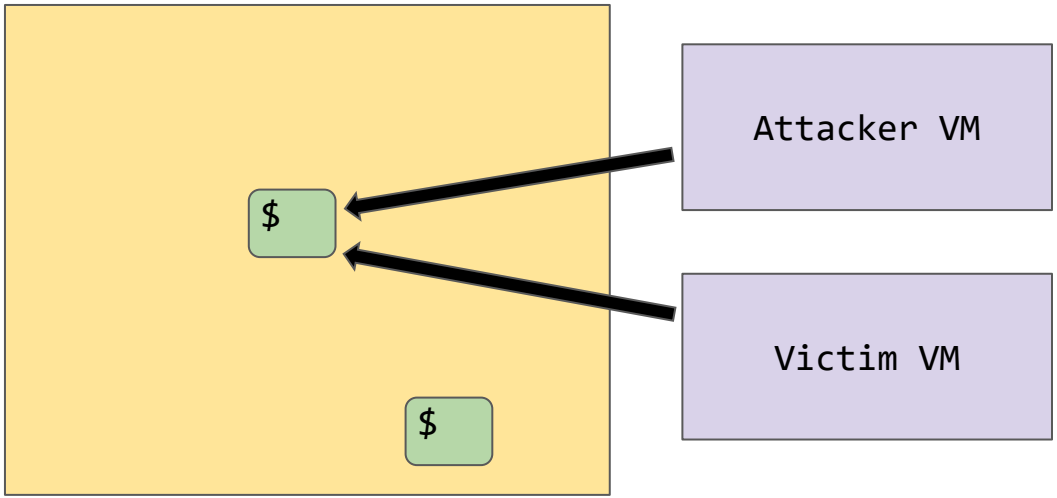
Memory Deduplication



Memory Deduplication



Memory Deduplication



Compromising Cloud Virtual Machines

1) Templating

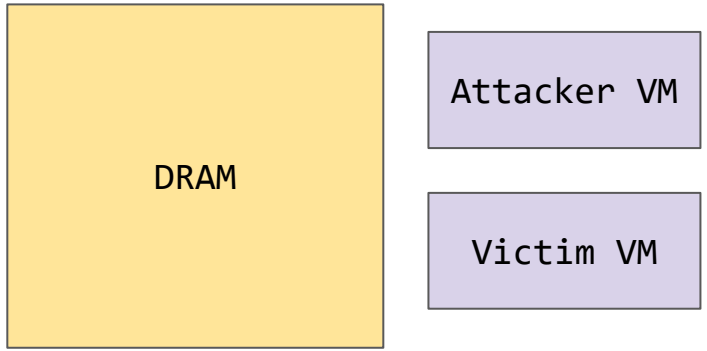
   Attacker's own memory

2) Massaging

   Memory deduplication

3) Exploitation

   Corrupt RSA public keys (OpenSSH)



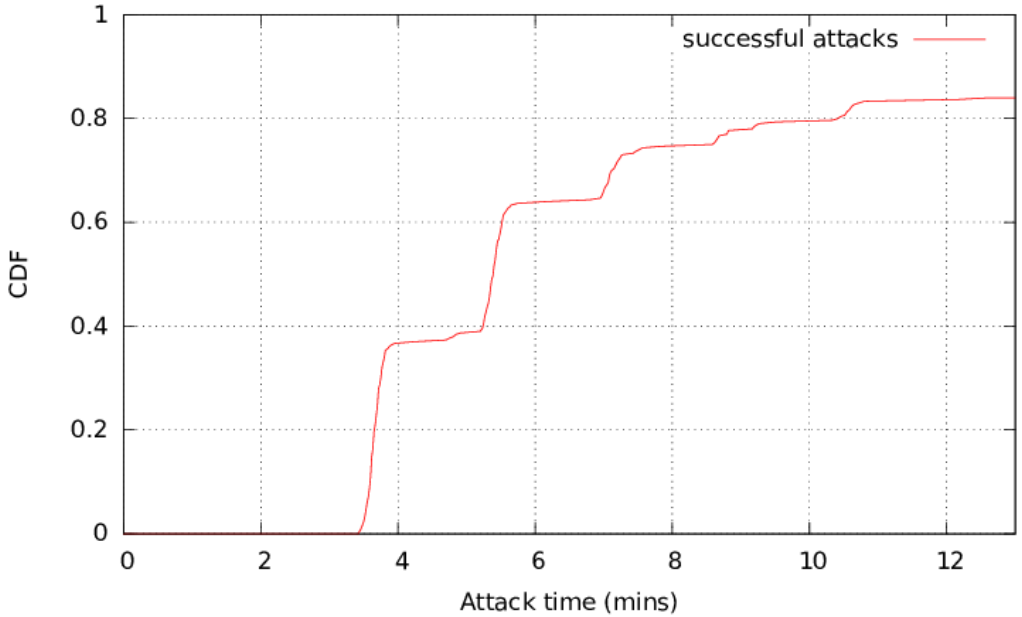
Factorizing Corrupted RSA Public Keys

$$n = p \times q \rightarrow PK \text{ (public key)}$$

$$PK \xrightarrow{FFS} PK'$$

$$PK' \rightarrow n' = p' \times q' \times z' \times \ldots$$

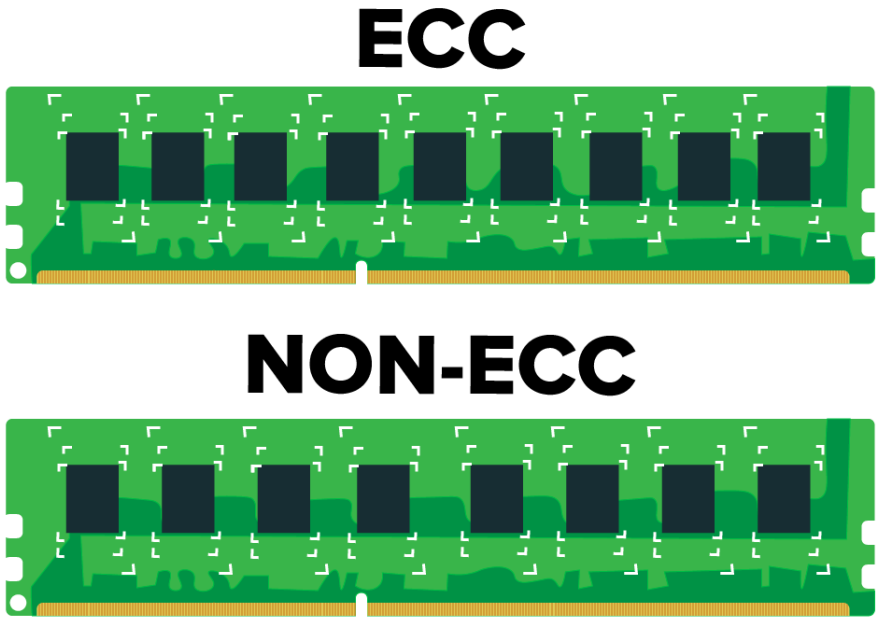
Attack’s Success Rate (200 VMs)



All done?

Consistent audience question: what about ECC memory?

ECC DRAM



Cores

DRAM Controller

DRAM

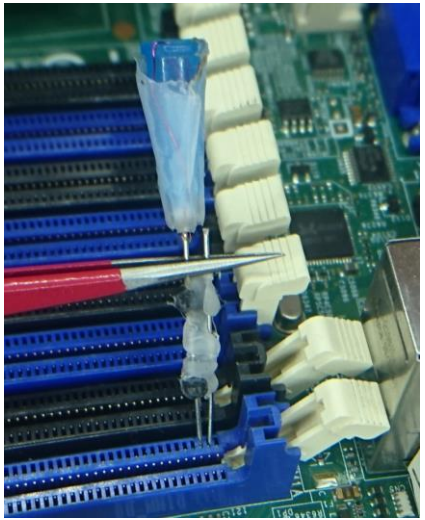
Error-correction Codes (SECDED)

- Original paper demonstrated SECDED not to be enough
- … but exploitation turned out to be difficult
  - ECC implementation is closed (guarantees unknown)
  - 1 bit flips not visible, 2 bit flips crash the system

ECC DRAM as a practical secure defense.

Recovering ECC Functions

- Observing signals are not easy at 1Ghz+
  - Need custom interposer
  - Expensive logic analyzer
- Fault injection with syringe needles!
- Short-circuit data lines with Vss
  - High-to-low voltage flips
- With some math, error reports allows for ECC recovery



Cojocar et al., “Exploiting Correcting Codes: On the Effectiveness of ECC Memory Against Rowhammer Attacks,” S&P’19

Results

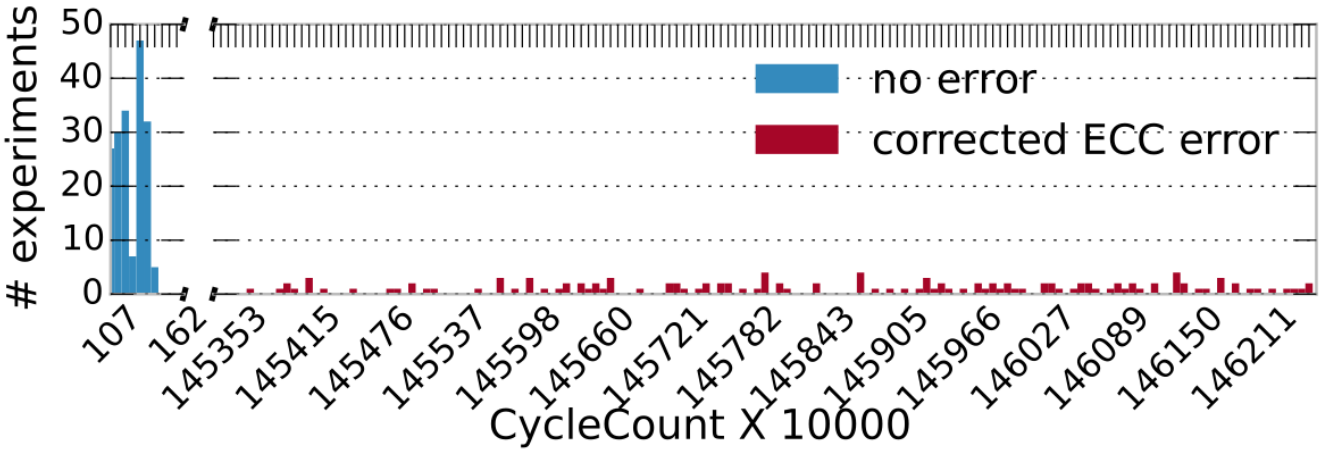
TABLE V: Error patterns that can circumvent ECC.

ID	Pattern	Config.	# flips	Flips location
AMD-1	$[\mathcal{P}_1]$	Ideal	3-BF-16	3 symbols, 1 in control bits
AMD-1	$[\mathcal{P}_2]$	Ideal	4-BF-16	Min. 2 symbols
Intel-1	$[\mathcal{P}_3]$	Ideal	4-BF-8	Min. 2 symbols
Intel-1	$[\mathcal{P}_4]$	Default	2-BF-8	Min. 2 symbols

TABLE VI: Percentages of rows with corruptions in an ECC DIMM.

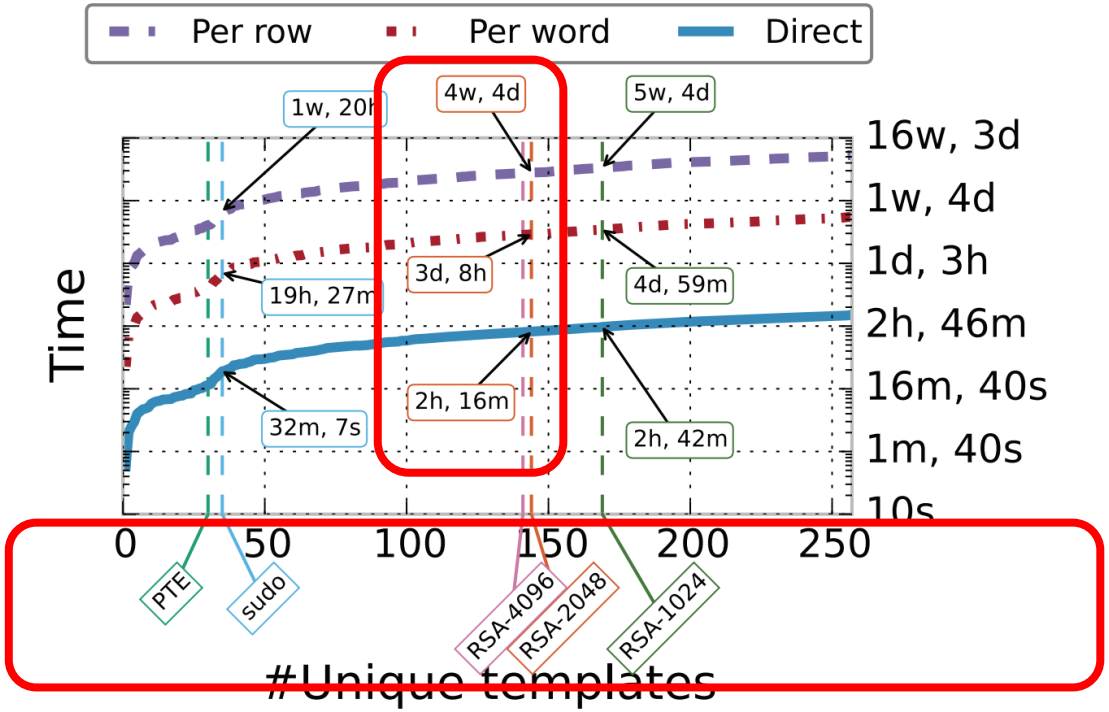
$[\mathcal{P}_1]$	$[\mathcal{P}_2]$	$[\mathcal{P}_3]$	$[\mathcal{P}_4]$
0.12%	0.12%	0.06%	0.60%

Avoiding Crashes

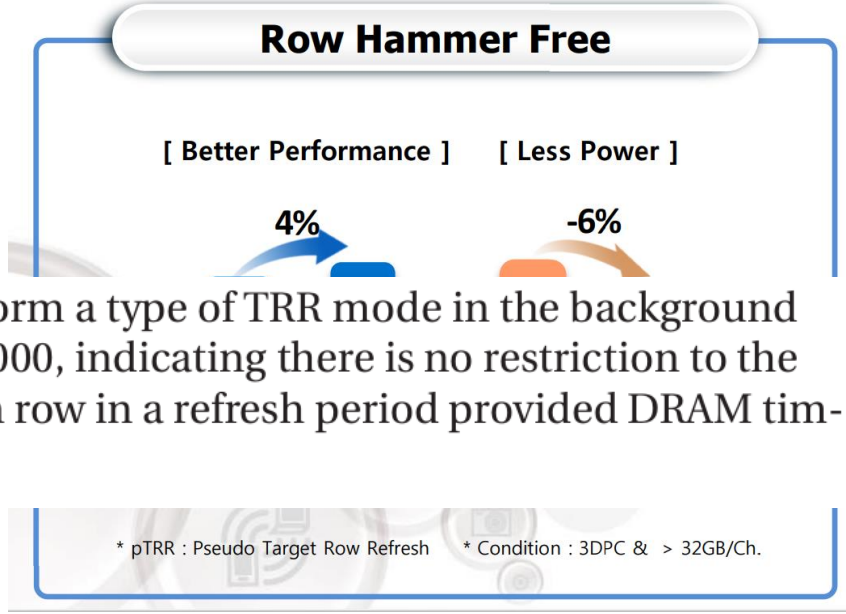


Detect single flips and merge them for silent corruptions.

Exploitation with ECC Memory

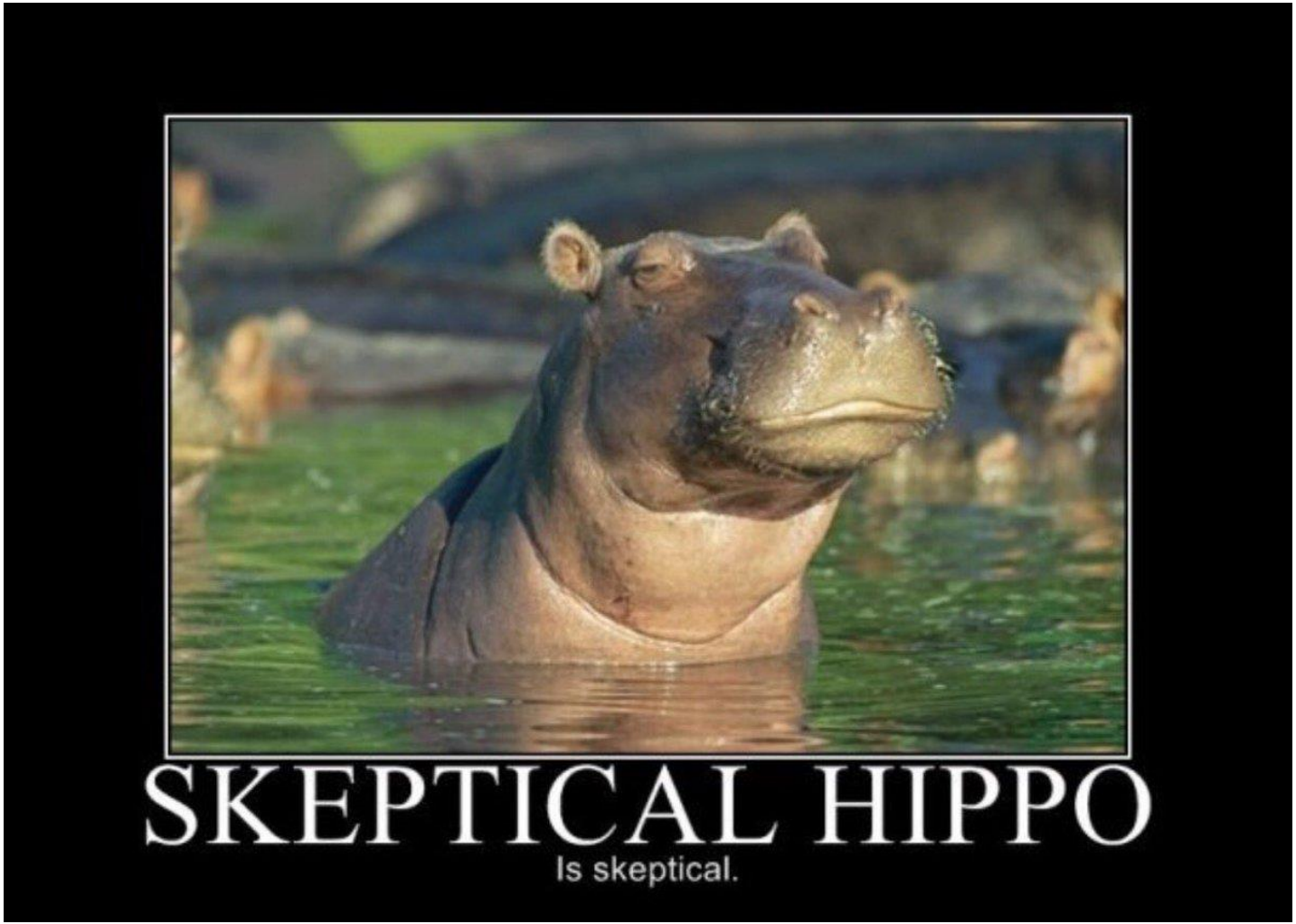


DRAM Vendors: We Fixed Rowhammer in DDR4



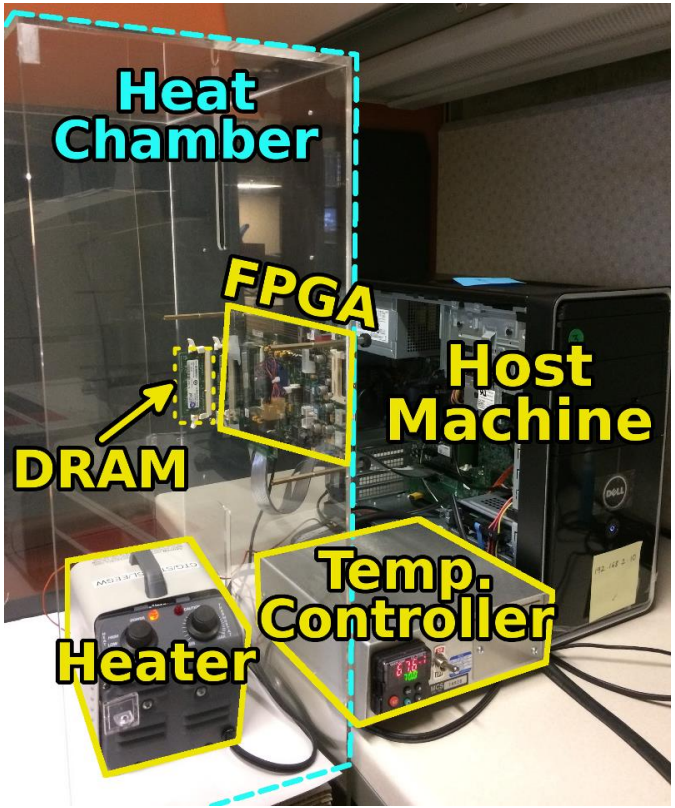
Micron's DDR4 devices automatically perform a type of TRR mode in the background and provide an MPR Page 3 MPR3[3:0] of 1000, indicating there is no restriction to the number of ACTIVATE commands to a given row in a refresh period provided DRAM timing specifications are not violated.

Target Row Refresh (TRR): keep track of intensely activated rows and refresh their neighbors.


SKEPTICAL HIPPO
Is skeptical.

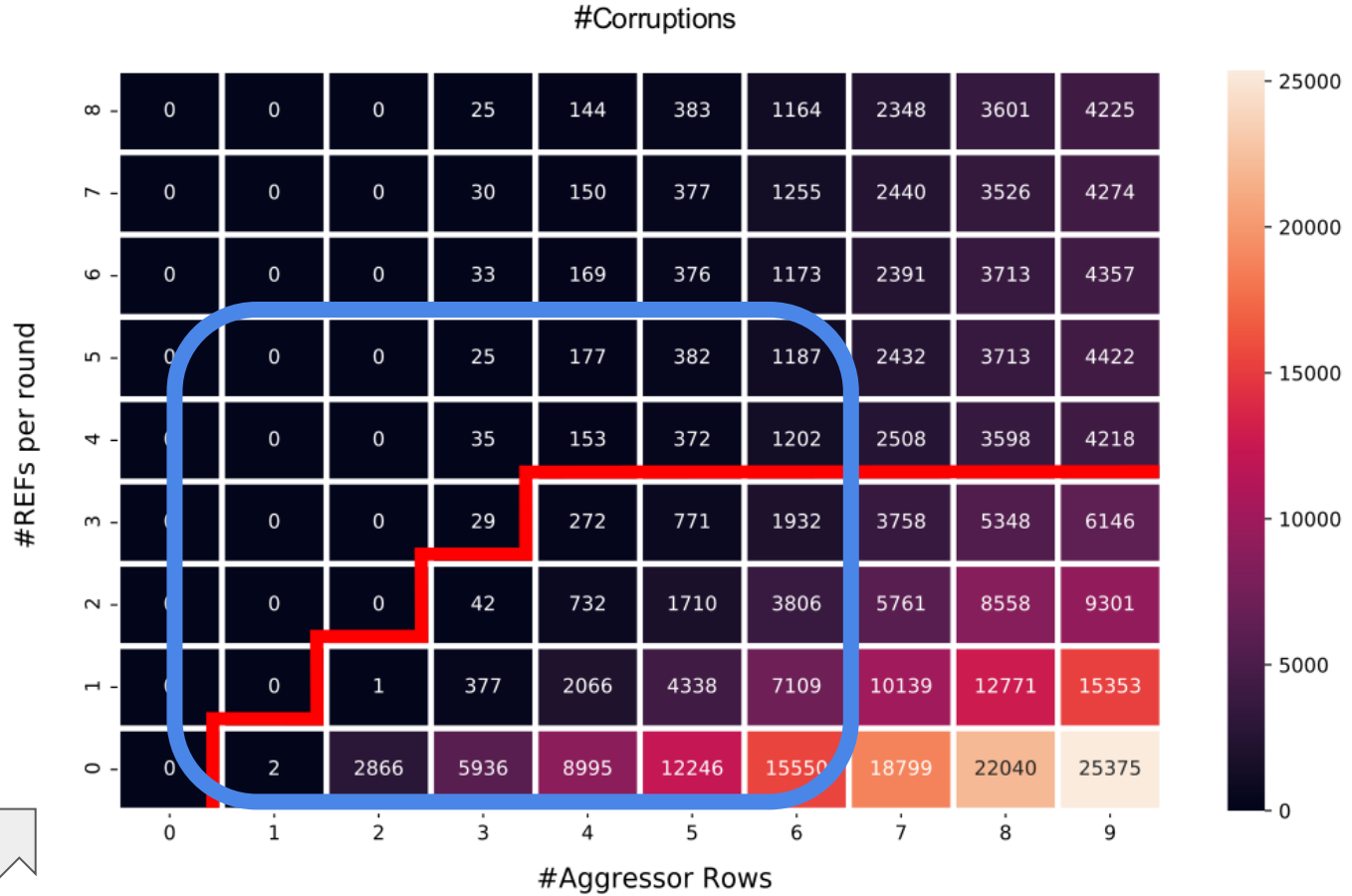
Looking into in-DRAM TRR

- SoftMC: platform for DRAM studies
- Support for DDR4
- Precise control over DRAM commands
  - ACTIVATE, READ/WRITE, PRECHARGE, REFRESH
- Run DRAM out of spec



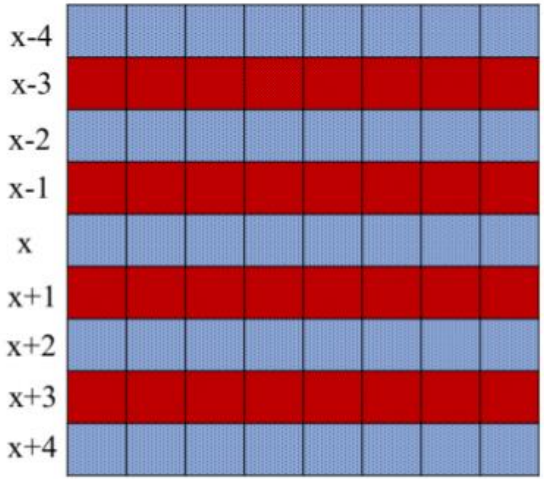
Frigo et al., “TRRespass: Exploiting the Many Sides of Target Row Refresh,” S&P’20

Results

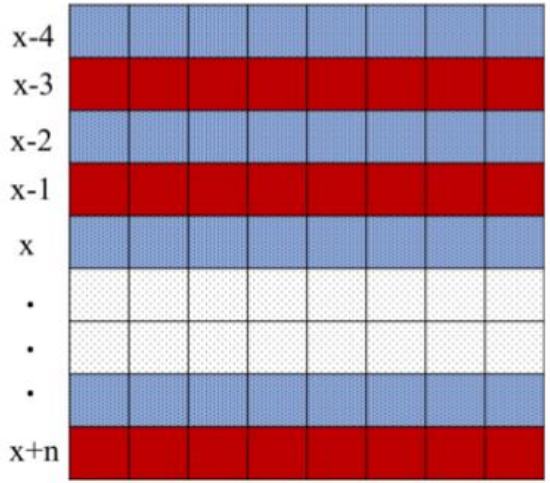


1 year of reverse engineering

Successful patterns: many-sided Rowhammer



4-sided

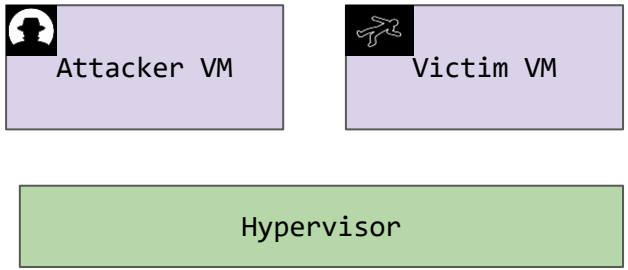


Assisted double-sided

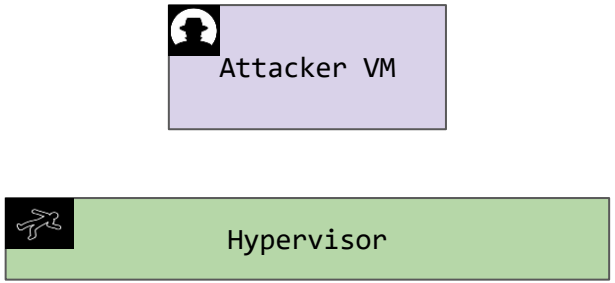
Results

Module	Date (yy-ww)	Freq. (MHz)	Size (GB)	Organization			MAC	Found Patterns	Best Pattern	Corruptions			Double Refresh
				Ranks	Banks	Pins				Total	$1 \to 0$	$0 \to 1$	
$\mathcal{A}_{0,1,2,3}$	16-37	2132	4	1	16	×8	UL	—	—	—	—	—	—
$\mathcal{A}_4$	16-51	2132	4	1	16	×8	UL	4	9-sided	7956	4008	3948	—
$\mathcal{A}_5$	18-51	2400	4	1	8	×16	UL	—	—	—	—	—	—
$\mathcal{A}_{6,7}$	18-15	2666	4	1	8	×16	UL	—	—	—	—	—	—
$\mathcal{A}_8$	17-09	2400	8	1	16	×8	UL	33	19-sided	20808	10289	10519	—
$\mathcal{A}_9$	17-31	2400	8	1	16	×8	UL	33	19-sided	24854	12580	12274	—
$\mathcal{A}_{10}$	19-02	2400	16	2	16	×8	UL	488	10-sided	11342	1809	11533	✓
$\mathcal{A}_{11}$	19-02	2400	16	2	16	×8	UL	523	10-sided	12830	1682	11148	✓
$\mathcal{A}_{12,13}$	18-50	2666	8	1	16	×8	UL	—	—	—	—	—	—
$\mathcal{A}_{14}$	19-08†	3200	16	2	16	×8	UL	120	14-sided	32723	16490	16233	—
$\mathcal{A}_{15}$‡	17-08	2132	4	1	16	×8	UL	2	9-sided	22397	12351	10046	—
$\mathcal{B}_0$	18-11	2666	16	2	16	×8	UL	2	3-sided	17	10	7	—
$\mathcal{B}_1$	18-11	2666	16	2	16	×8	UL	2	3-sided	22	16	6	—
$\mathcal{B}_2$	18-49	3000	16	2	16	×8	UL	2	3-sided	5	2	3	—
$\mathcal{B}_3$	19-08†	3000	8	1	16	×8	UL	—	—	—	—	—	—
$\mathcal{B}_{4,5}$	19-08†	2666	8	2	16	×8	UL	—	—	—	—	—	—
$\mathcal{B}_{6,7}$	19-08†	2400	4	1	16	×8	UL	—	—	—	—	—	—
$\mathcal{B}_8$◇	19-08†	2400	8	1	16	×8	UL	—	—	—	—	—	—
$\mathcal{B}_9$◇	19-08†	2400	8	1	16	×8	UL	2	3-sided	12	—	12	✓
$\mathcal{B}_{10,11}$	16-13†	2132	8	2	16	×8	UL	—	—	—	—	—	—
$\mathcal{C}_{0,1}$	18-46	2666	16	2	16	×8	UL	—	—	—	—	—	—
$\mathcal{C}_{2,3}$	19-08†	2800	4	1	16	×8	UL	—	—	—	—	—	—
$\mathcal{C}_{4,5}$	19-08†	3000	8	1	16	×8	UL	—	—	—	—	—	—
$\mathcal{C}_{6,7}$	19-08†	3000	16	2	16	×8	UL	—	—	—	—	—	—
$\mathcal{C}_8$	19-08†	3200	16	2	16	×8	UL	—	—	—	—	—	—
$\mathcal{C}_9$	18-47	2666	16	2	16	×8	UL	—	—	—	—	—	—
$\mathcal{C}_{10,11}$	19-04	2933	8	1	16	×8	UL	—	—	—	—	—	—
$\mathcal{C}_{12}$‡	15-01†	2132	4	1	16	×8	UT	25	10-sided	190037	63904	126133	✓
$\mathcal{C}_{13}$‡	18-49	2132	4	1	16	×8	UT	3	9-sided	694	239	455	—

Cloud Threat Models under Rowhammer



Possible today under **certain conditions** with **Rowhammer** bit flips



Needs more research

Conclusions

- Possible to compromise cloud VMs with Rowhammer
- Rowhammer is not going away
- Getting harder ← things are improving

Ben Gras, Erik Bosman, Victor van der Veen, Lucian Cojocar,
Pietro Frigo, Emanuele Vannacci, Hasan Hassan,
Onur Mutlu, Cristiano Giuffrida, Herbert Bos