Ten Years of Rowhammer

A Retrospect (and Path to the Future)

Martin Heckel[1,2] **(@lunkw1ll)**
Daniel Gruss[1] **(@lavados)**
Florian Adamsky[2] **(@c1t)**

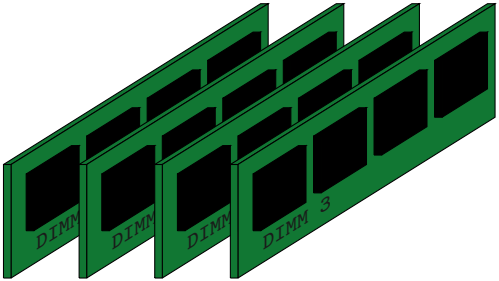
[1] Graz University of Technology
[2] Hof University of Applied Sciences

NeRAM
FWF Der Wissenschaftsfonds.
DFG Deutsche Forschungsgemeinschaft

Origins and Root Cause

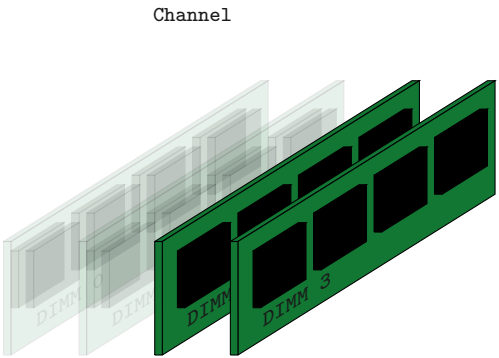
Overview DRAM

System DRAM



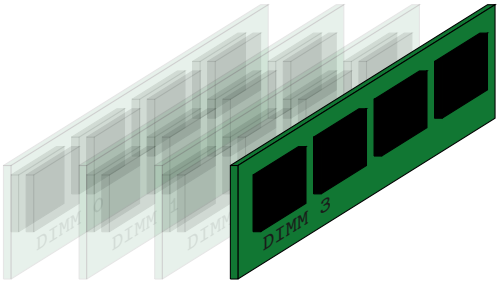
Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

Overview DRAM



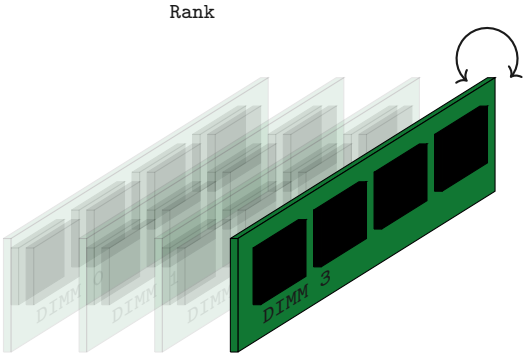
Overview DRAM

DIMM

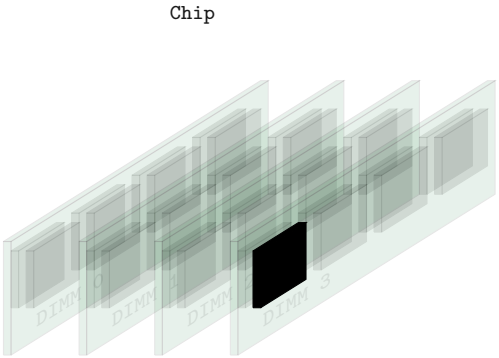


Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

Overview DRAM

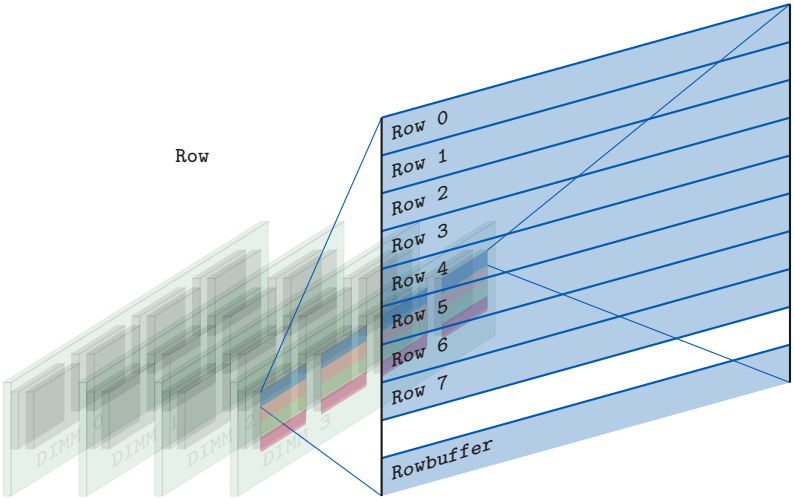


Overview DRAM



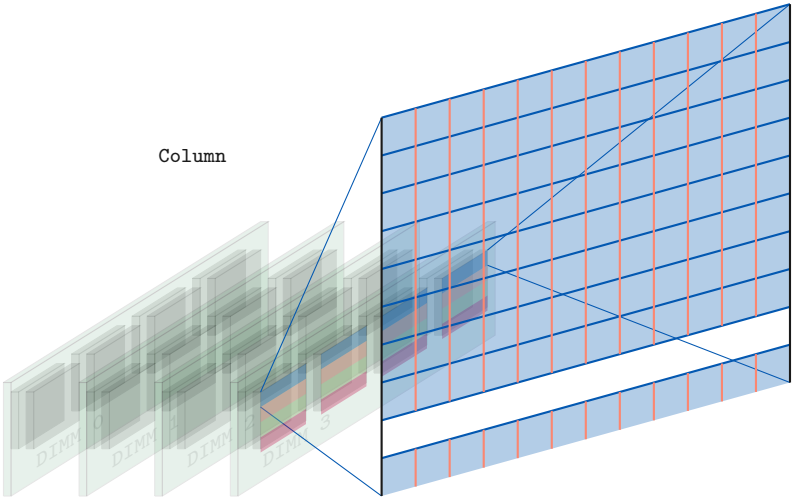
Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

Overview DRAM



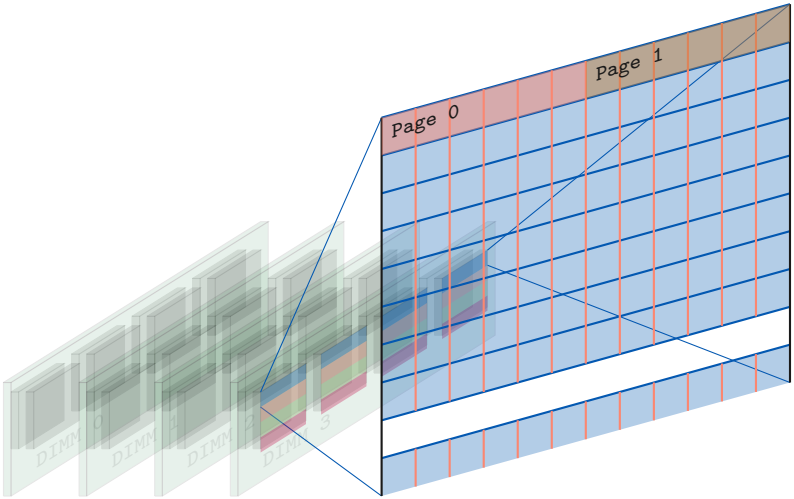
Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

Overview DRAM



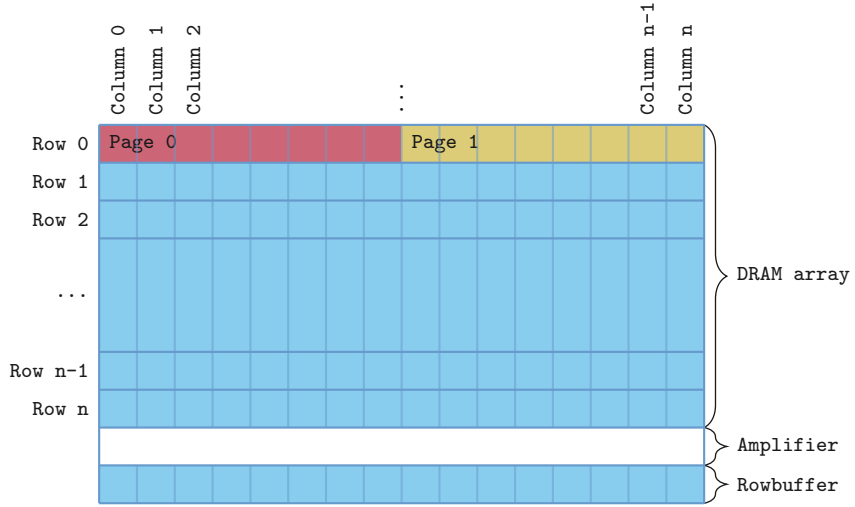
Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

Overview DRAM



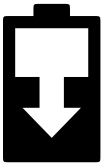
Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

Structure within a DRAM bank

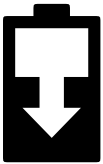


Problems with DRAM

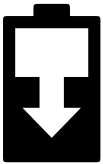
Problems with DRAM



Problems with DRAM



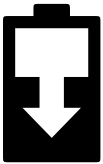
Problems with DRAM



1. Capacitor loses its voltage over time

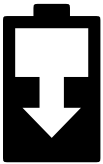
Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

Problems with DRAM



1. Capacitor loses its voltage over time
   - Cells must be refreshed regularly (refresh rate)

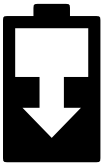
Problems with DRAM



1. Capacitor loses its voltage over time
   - Cells must be refreshed regularly (refresh rate)
   - Cells are normally refreshed every 64 ms

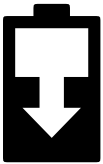
Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

Problems with DRAM



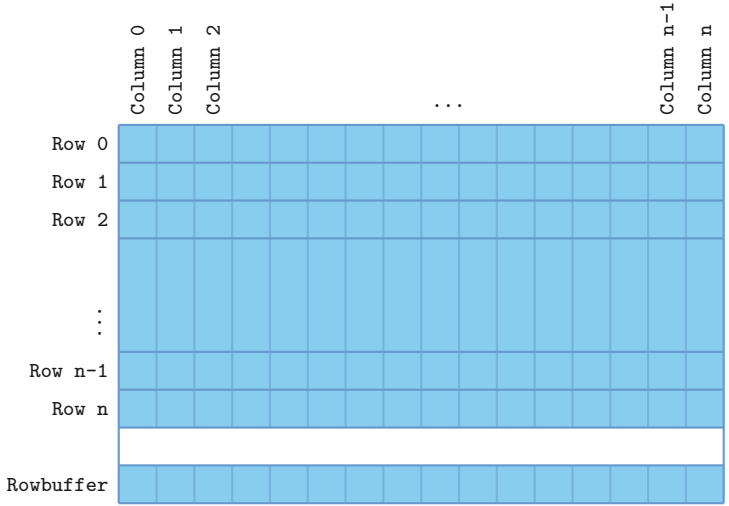
1. Capacitor loses its voltage over time
   - Cells must be refreshed regularly (refresh rate)
   - Cells are normally refreshed every 64 ms
2. When reading a row, we destroy the data in this row

Problems with DRAM



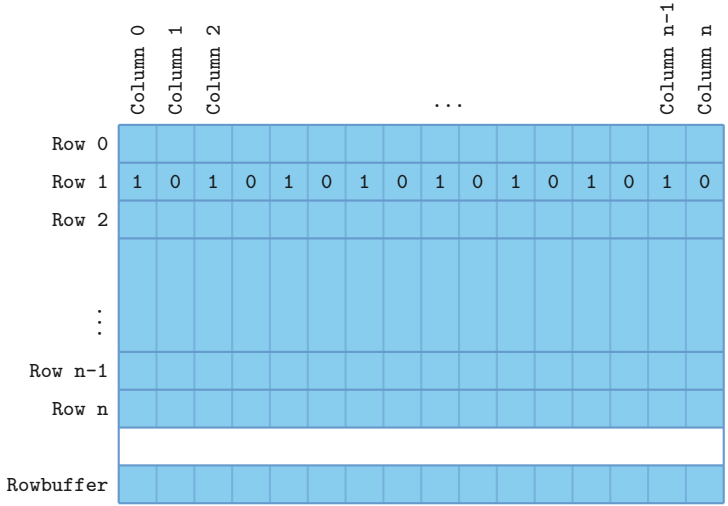
1. Capacitor loses its voltage over time
   - Cells must be refreshed regularly (refresh rate)
   - Cells are normally refreshed every 64 ms
2. When reading a row, we destroy the data in this row
   - Intermediate memory in the row buffer

Row Buffer

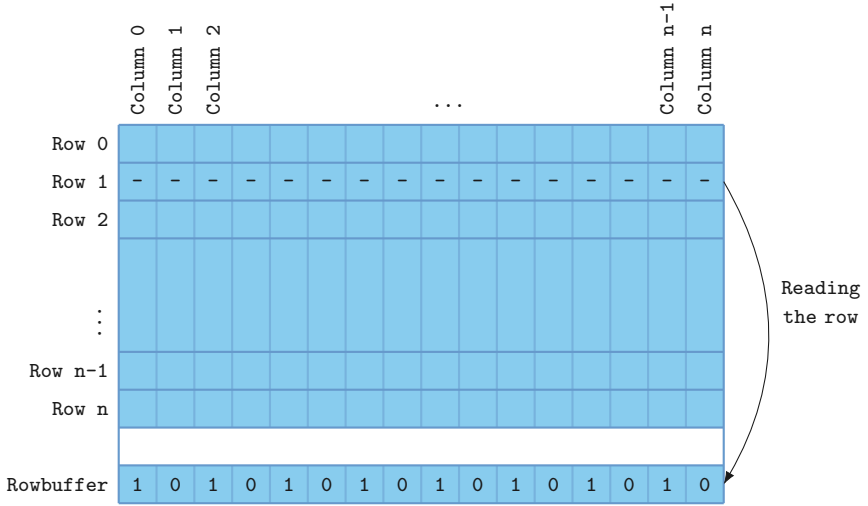


Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

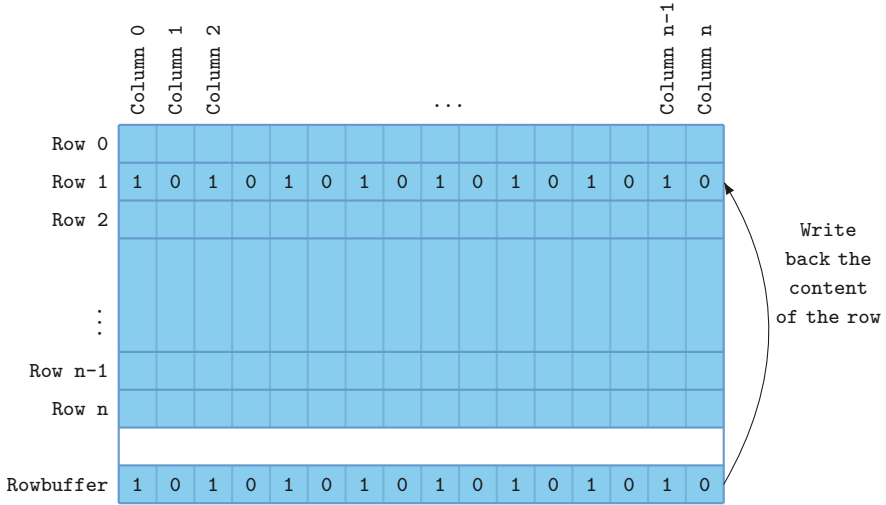
Row Buffer


Column 0
Column 1
Column 2
...
Column n-1
Column n
Row 0
Row 1
1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
Row 2
Row n-1
Row n
Rowbuffer

Row Buffer

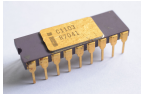

Column 0
Column 1
Column 2
...
Column n-1
Column n
Row 0
Row 1
Row 2
Row n-1
Row n
Rowbuffer
1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
Reading
the row

Row Buffer


Column 0
Column 1
Column 2
...
Column n-1
Column n
Row 0
Row 1
Row 2
Row n-1
Row n
Rowbuffer
1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
Write back the content of the row

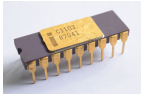
Historical Overview

Historical Overview

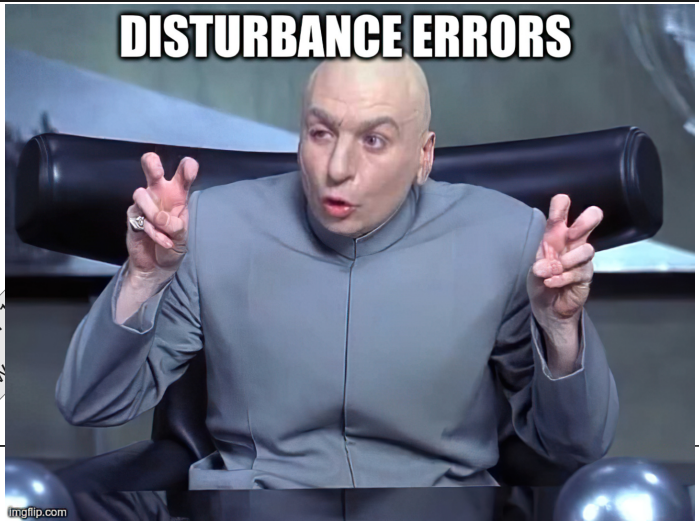


Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

Historical Overview



Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)



1971

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

How Rowhammer Works

How Rowhammer Works

How Rowhammer Works

How Rowhammer Works

- Memory rows are disturbed by frequent accesses

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

How Rowhammer Works

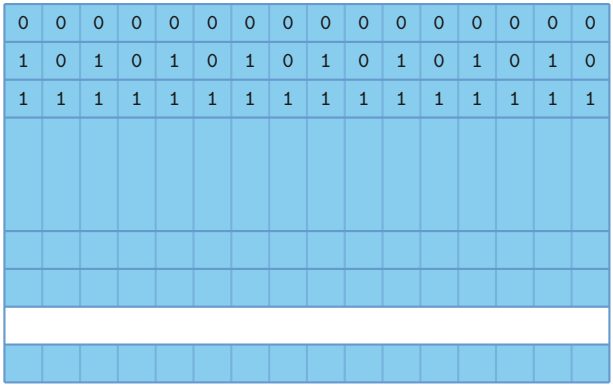
- Memory rows are disturbed by frequent accesses
- Results in bit flips in adjacent rows

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

How Rowhammer Works

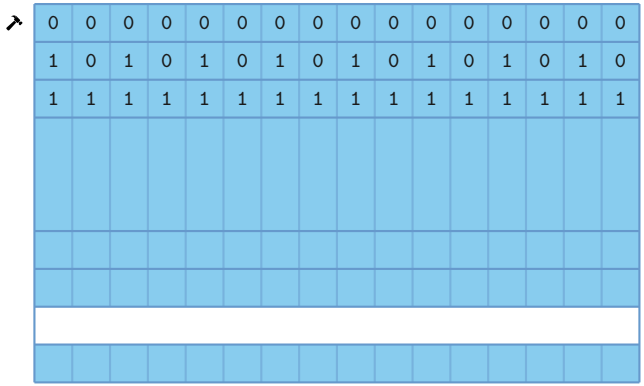
- Memory rows are disturbed by frequent accesses
- Results in bit flips in adjacent rows
- Exploited through clever hammering techniques

Simple Example of Rowhammer



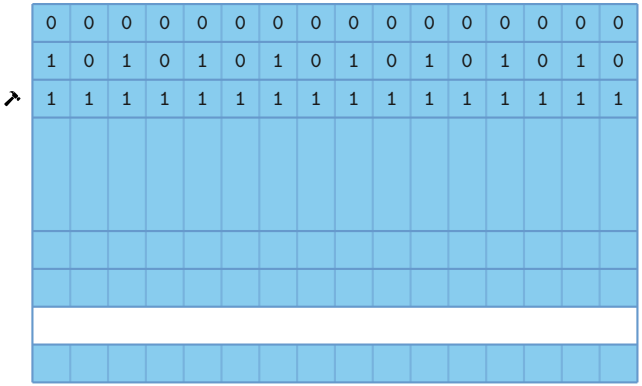

```
hammertime:
  mov (Row 0), %eax
  mov (Row 2), %ebx
  clflush (Row 0)
  clflush (Row 2)
  jmp hammertime
```

Simple Example of Rowhammer



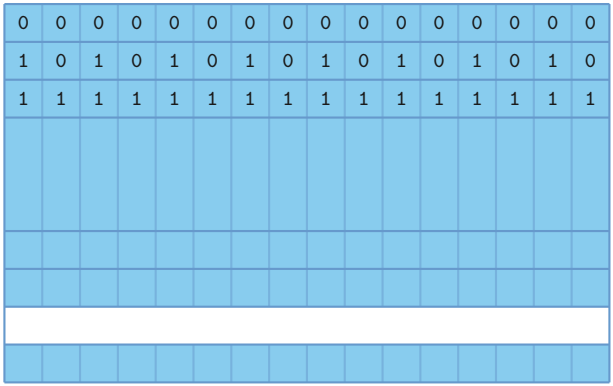

```
hammertime:
    mov (Row 0), %eax
    mov (Row 2), %ebx
    clflush (Row 0)
    clflush (Row 2)
    jmp hammertime
```

Simple Example of Rowhammer



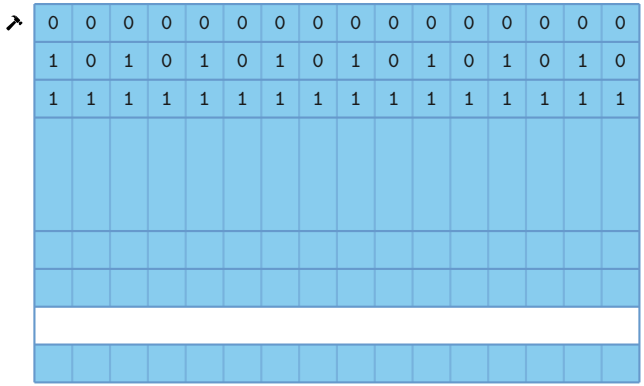

```
hammertime:
  mov (Row 0), %eax
  mov (Row 2), %ebx
  clflush (Row 0)
  clflush (Row 2)
  jmp hammertime
```

Simple Example of Rowhammer



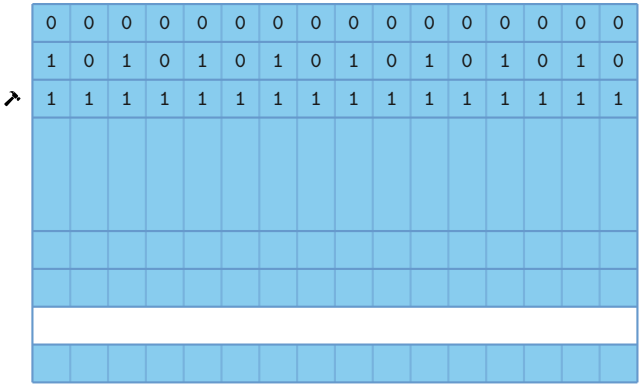

```
hammertime:
  mov (Row 0), %eax
  mov (Row 2), %ebx
  clflush (Row 0)
  clflush (Row 2)
  jmp hammertime
```

Simple Example of Rowhammer




```
hammertime:
    mov (Row 0), %eax
    mov (Row 2), %ebx
    clflush (Row 0)
    clflush (Row 2)
    jmp hammertime
```

Simple Example of Rowhammer




```
hammertime:
  mov (Row 0), %eax
  mov (Row 2), %ebx
  clflush (Row 0)
  clflush (Row 2)
  jmp hammertime
```

Simple Example of Rowhammer

We can touch this!

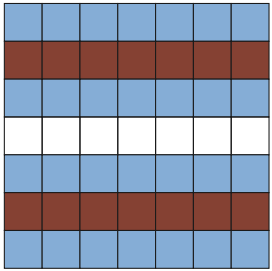
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	0	1	0	1	0	1	0	1	0	1	0	1	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

```
hammertime:
  mov (Row 0), %eax
  mov (Row 2), %ebx
  clflush (Row 0)
  clflush (Row 2)
  jmp hammertime
```


Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

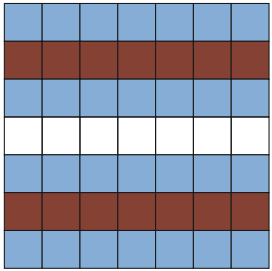
Various Hammering Patterns

Single-Sided

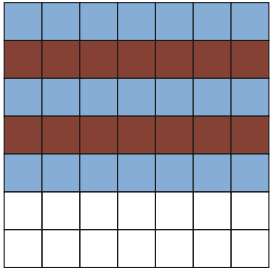


Various Hammering Patterns

Single-Sided

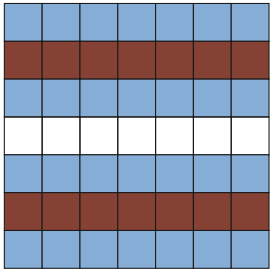


Double-Sided

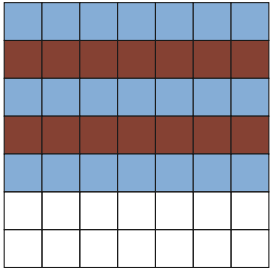


Various Hammering Patterns

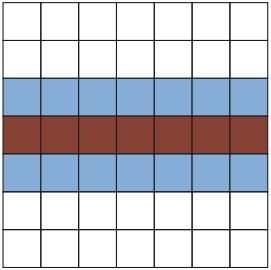
Single-Sided



Double-Sided

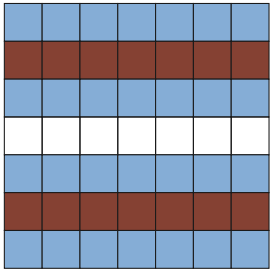


One-Location

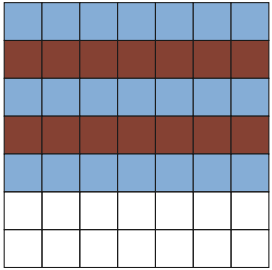


Various Hammering Patterns

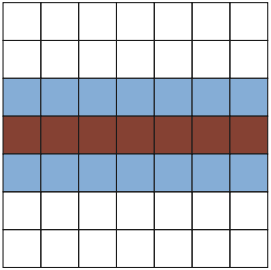
Single-Sided



Double-Sided

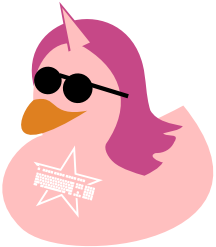


One-Location



... and several more (e.g., many-sided hammering)

Wait a Minute!

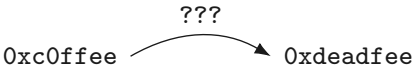


Wait a Minute!

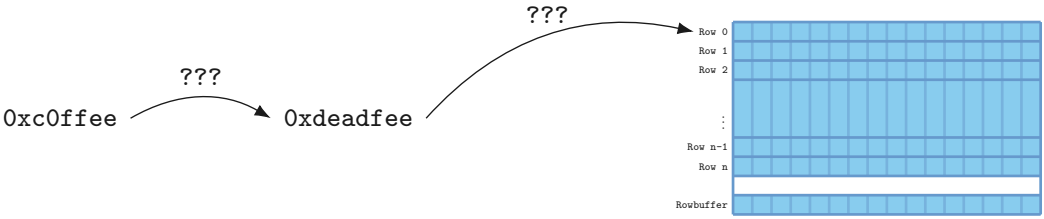
Addressing Functions

```
0xc0ffee
```

Addressing Functions

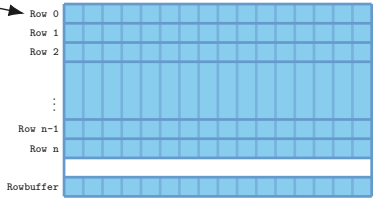


Addressing Functions



Addressing Functions

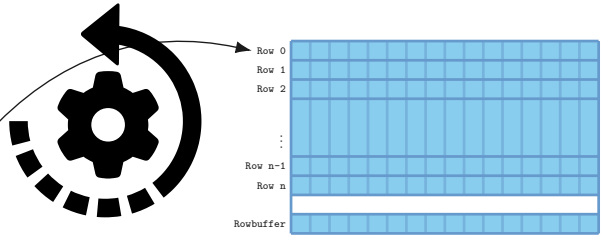
0xc0ffee → 0xdeadfee ???



Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

Addressing Functions

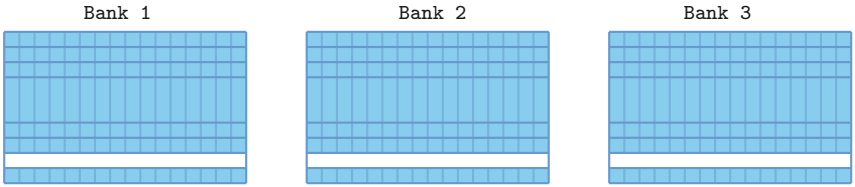
0xc0ffee → 0xdeadfee



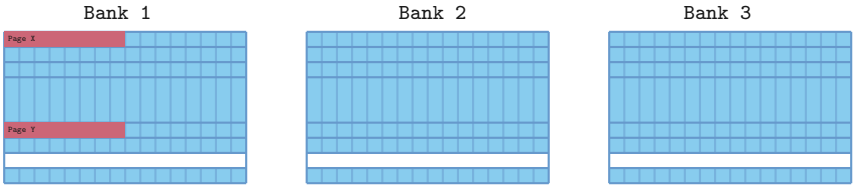
Reverse Engineering
to the Rescue!

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

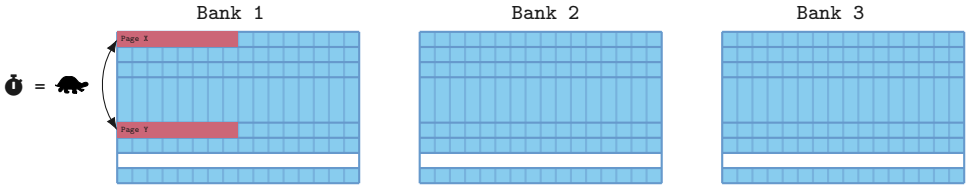
Reverse Engineering DRAM Addressing Functions



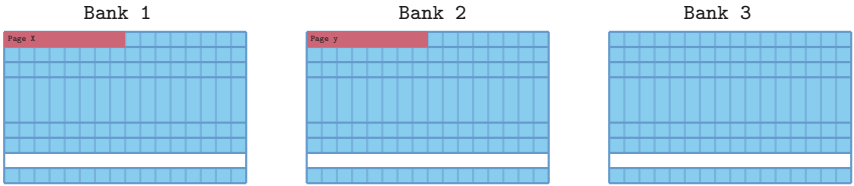
Reverse Engineering DRAM Addressing Functions



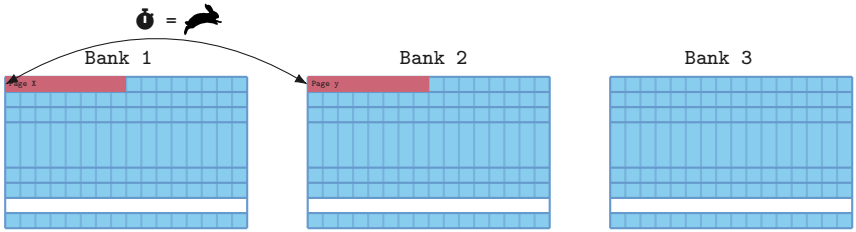
Reverse Engineering DRAM Addressing Functions



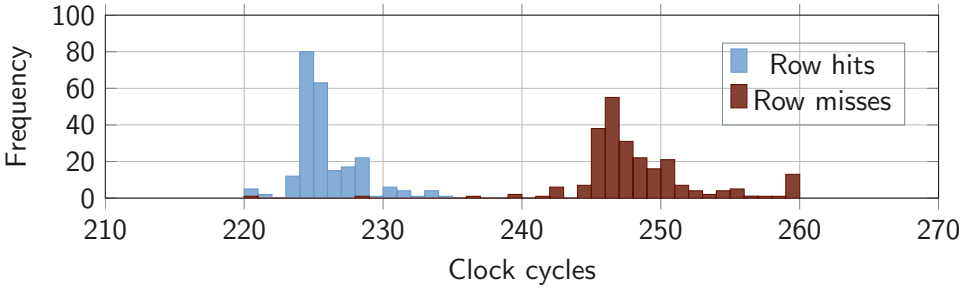
Reverse Engineering DRAM Addressing Functions



Reverse Engineering DRAM Addressing Functions



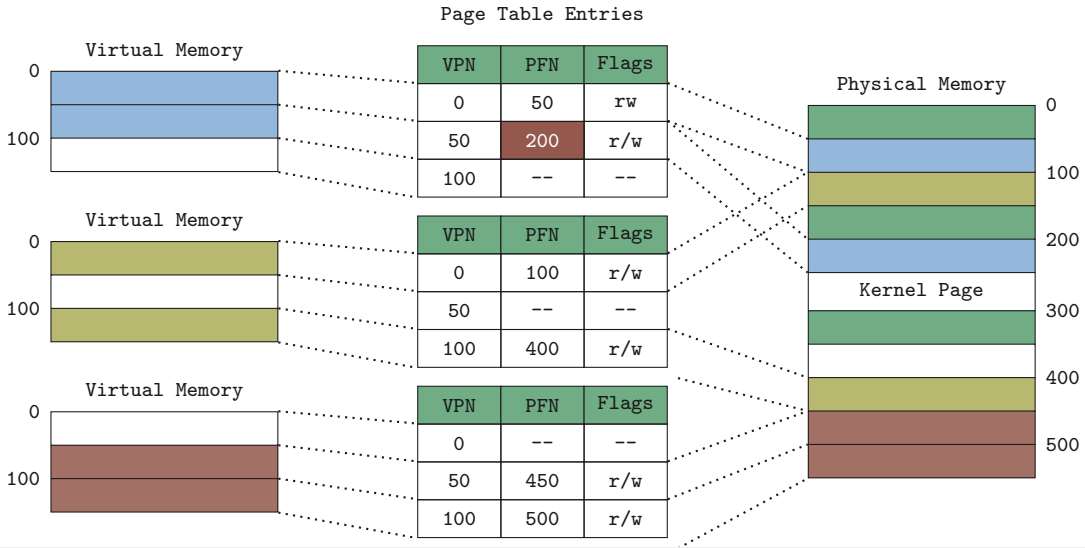
Row-Conflict Side Channel



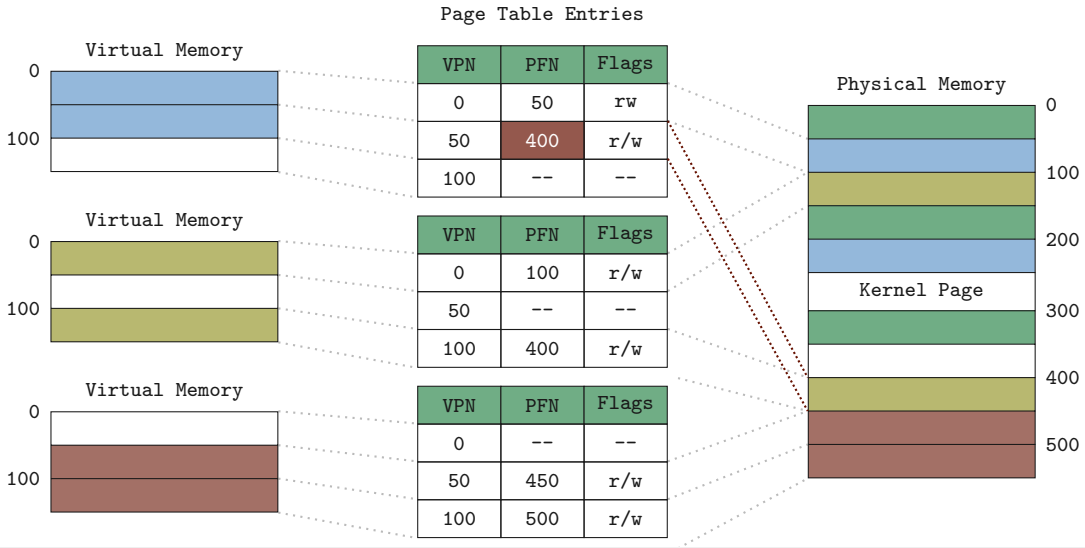
Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

But how can we exploit it?

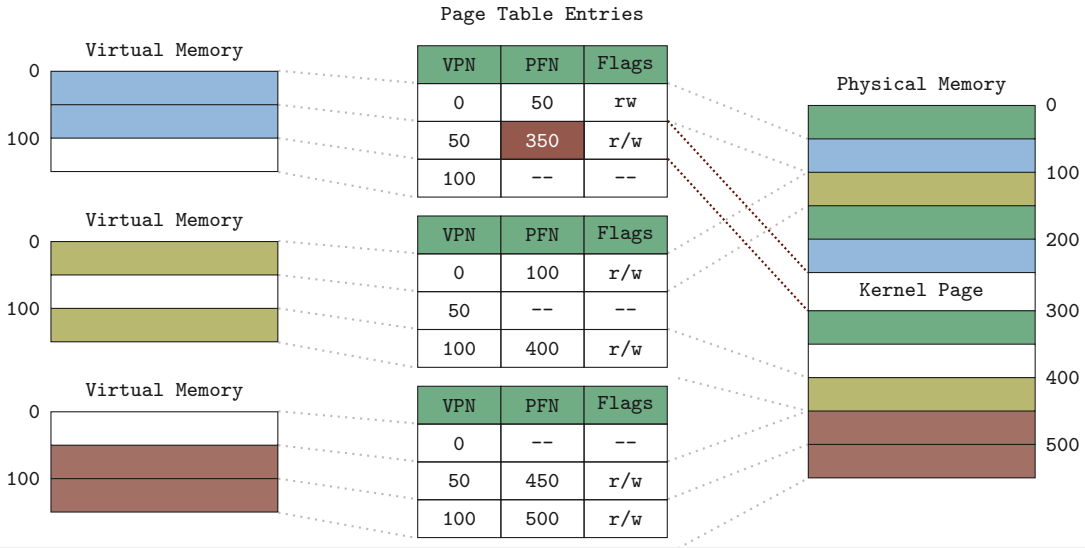
Reminder: Page Table Entries (simplified)



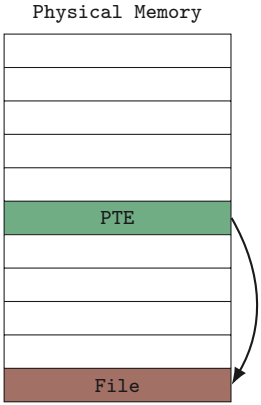
Reminder: Page Table Entries (simplified)



Reminder: Page Table Entries (simplified)

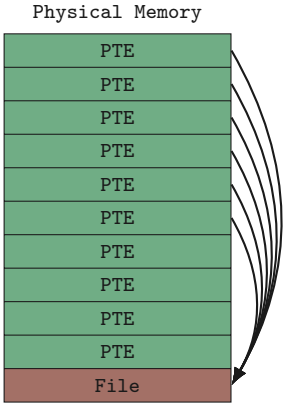


Increasing our chances with PTE Spraying




```
for (int i = 0; i < N; i++)
  mmap(NULL, FSIZE, PROT_READ | PROT_WRITE,
       MAP_SHARED, fd, 0);
```

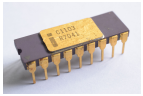
Increasing our chances with PTE Spraying

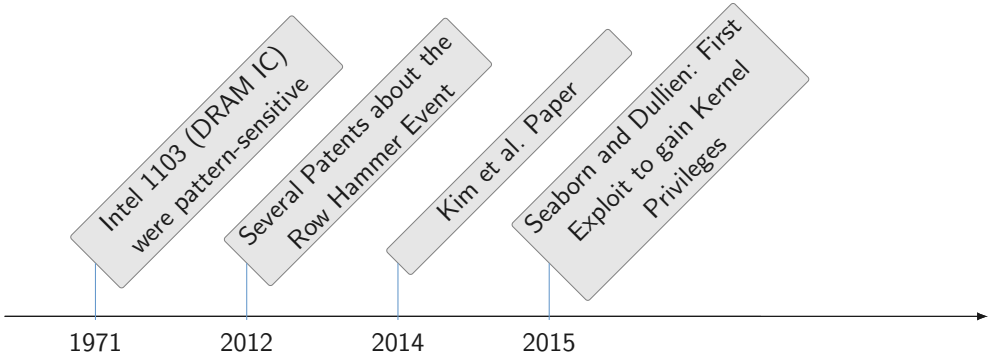



```
for (int i = 0; i < N; i++)
  mmap(NULL, FSIZE, PROT_READ | PROT_WRITE,
       MAP_SHARED, fd, 0);
```

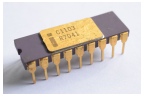

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

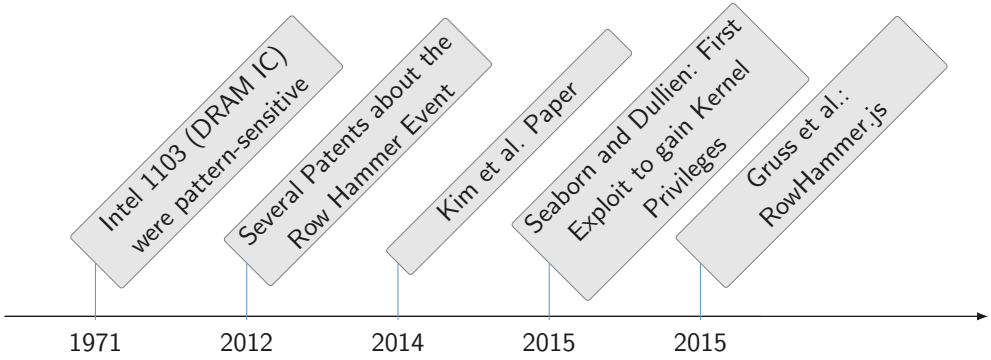
Historical Overview





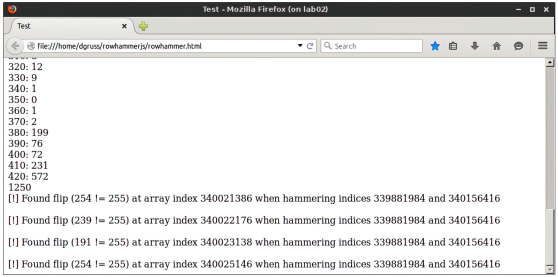
Historical Overview



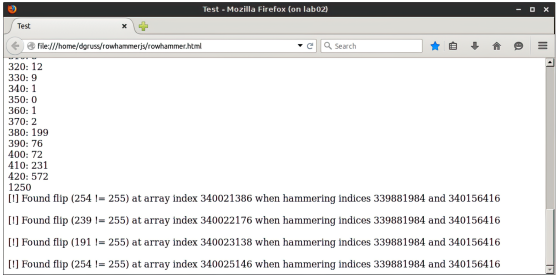


2015: Rowhammer.js

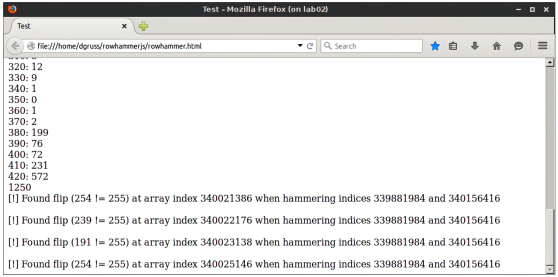
2015: Rowhammer.js



2015: Rowhammer.js

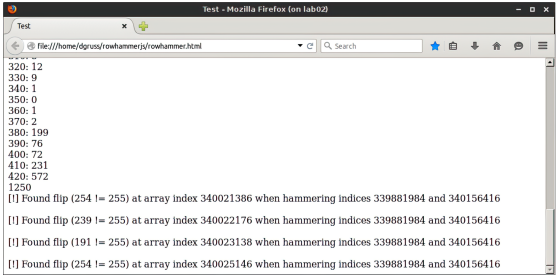


2015: Rowhammer.js



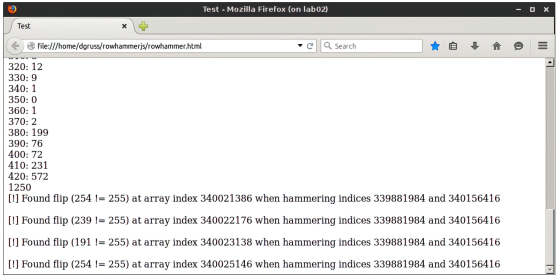
- double-sided hammer

2015: Rowhammer.js



- double-sided hammer
- via JavaScript

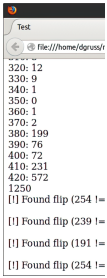
2015: Rowhammer.js



- double-sided hammer
- via JavaScript
- without `clflush`

2015: Rowhammer.js

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)



ROWHAMMERJS

ROOT privileges for web apps!

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

heise online heise+ gratis testen Anmelden Suchen

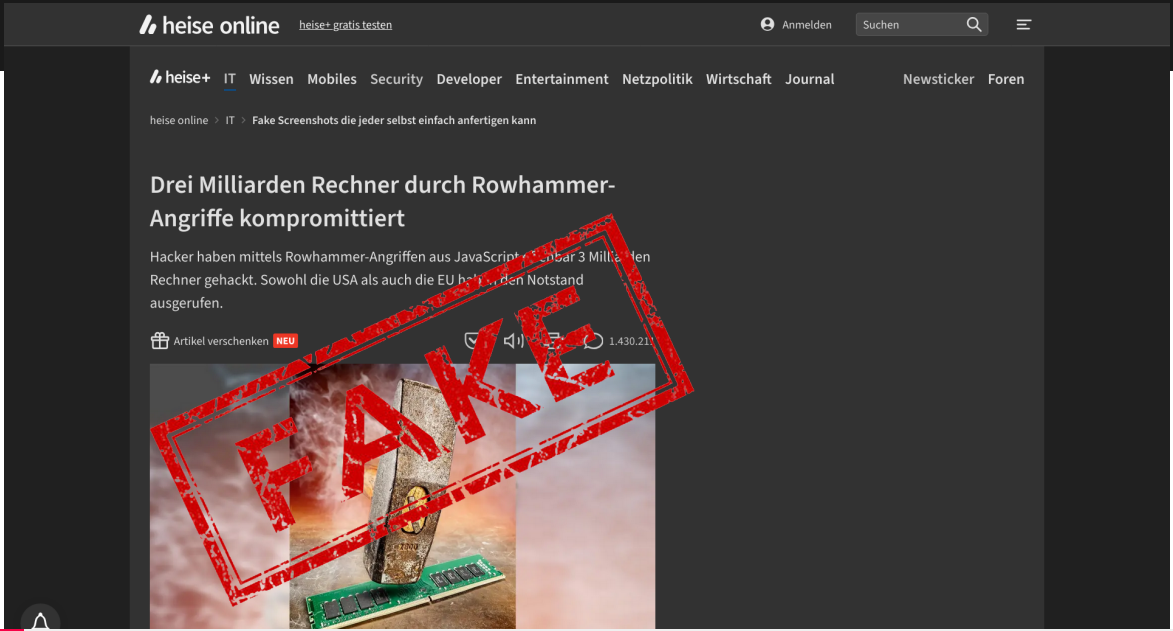
heise+ IT Wissen Mobiles Security Developer Entertainment Netzpolitik Wirtschaft Journal Newsticker Foren

heise online › IT › Fake Screenshots die jeder selbst einfach anfertigen kann

Drei Milliarden Rechner durch Rowhammer-Angriffe kompromittiert

Hacker haben mittels Rowhammer-Angriffen aus JavaScript offenbar 3 Milliarden Rechner gehackt. Sowohl die USA als auch die EU haben den Notstand ausgerufen.

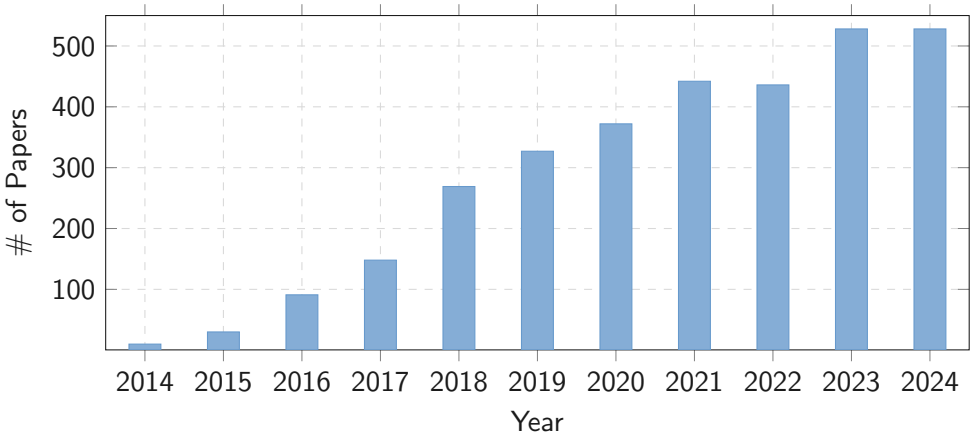
Artikel verschenken NEU 1.430.211



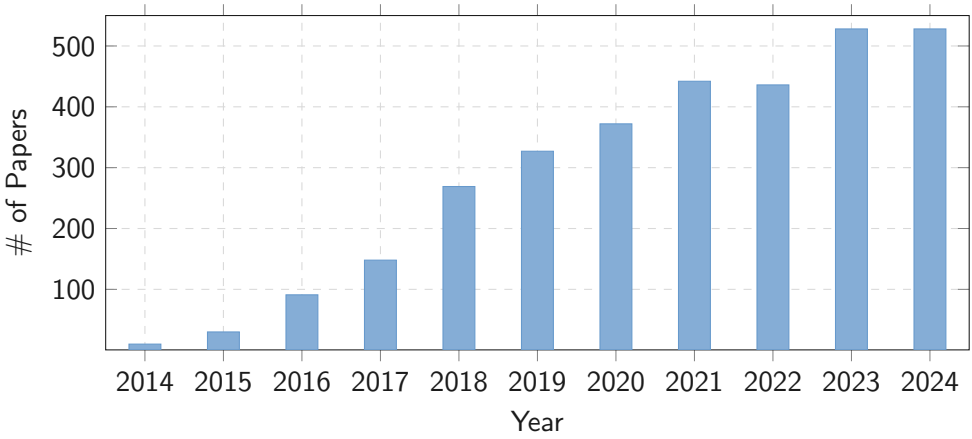
Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)


ROWHAMMER ATTACKS IN THE REAL WORLD?
STILL NOTHING?
imgflip.com

Scientific Papers about Rowhammer per Year



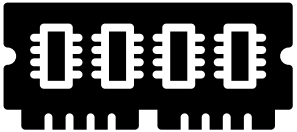
Scientific Papers about Rowhammer per Year



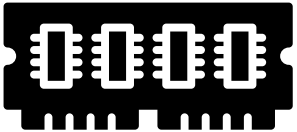
Too many works to discuss...

Why does Rowhammer even matter?

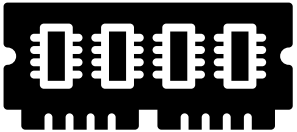
Why does Rowhammer even matter?



Why does Rowhammer even matter?

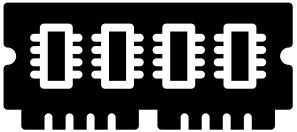


Why does Rowhammer even matter?



- Reliability

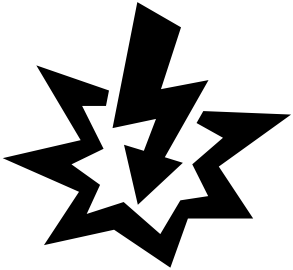
Why does Rowhammer even matter?



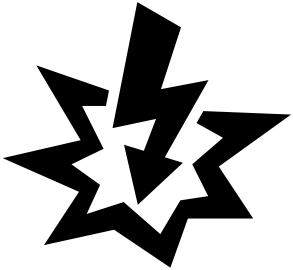
- Reliability
- Exploits

Exploitation Potential

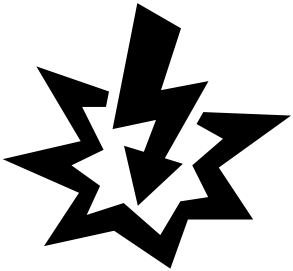
Exploitation Potential



Exploitation Potential

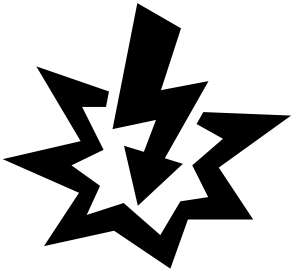


Exploitation Potential



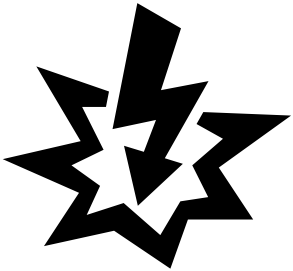
- Rowhammer enables privilege escalation attacks

Exploitation Potential



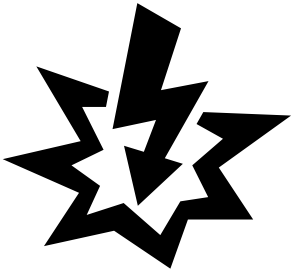
- Rowhammer enables privilege escalation attacks
- Bypassing memory isolation barriers

Exploitation Potential



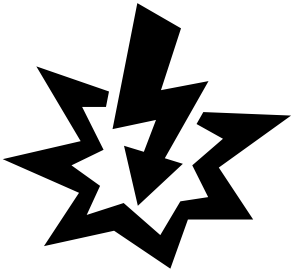
- Rowhammer enables privilege escalation attacks
- Bypassing memory isolation barriers
- Challenges:

Exploitation Potential



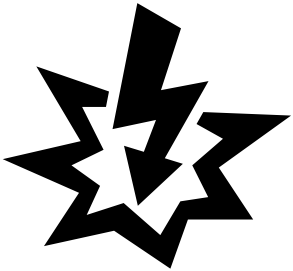
- Rowhammer enables privilege escalation attacks
- Bypassing memory isolation barriers
- Challenges:

Exploitation Potential



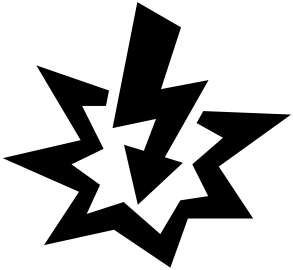
- Rowhammer enables privilege escalation attacks
- Bypassing memory isolation barriers
- Challenges:
  - High-Resolution Timers (for the side channel / reverse-engineering)

Exploitation Potential



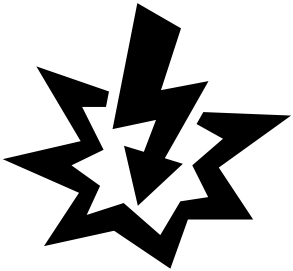
- Rowhammer enables privilege escalation attacks
- Bypassing memory isolation barriers
- Challenges:
  - High-Resolution Timers (for the side channel / reverse-engineering)
  - Differences between environments

Exploitation Potential



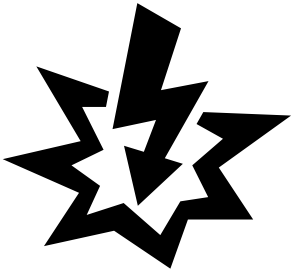
- Rowhammer enables privilege escalation attacks
- Bypassing memory isolation barriers
- Challenges:
  - High-Resolution Timers (for the side channel / reverse-engineering)
  - Differences between environments
  - **Right amount of bit flips in the right locations!**

Exploitation Potential



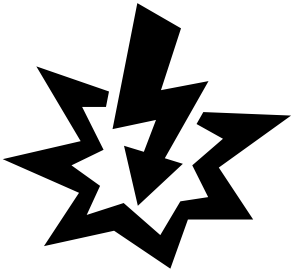
- Rowhammer enables privilege escalation attacks
- Bypassing memory isolation barriers
- Challenges:
  - High-Resolution Timers (for the side channel / reverse-engineering)
  - Differences between environments
  - **Right amount of bit flips in the right locations!**
  - Flips reproducible (!?) $\rightarrow$ great for attacks

Exploitation Potential



- Rowhammer enables privilege escalation attacks
- Bypassing memory isolation barriers
- Challenges:
  - High-Resolution Timers (for the side channel / reverse-engineering)
  - Differences between environments
  - **Right amount of bit flips in the right locations!**
  - Flips reproducible (!?) $\rightarrow$ great for attacks

Exploitation Potential



- Rowhammer enables privilege escalation attacks
- Bypassing memory isolation barriers
- Challenges:
  - High-Resolution Timers (for the side channel / reverse-engineering)
  - Differences between environments
  - **Right amount of bit flips in the right locations!**
  - Flips reproducible (!?) $\rightarrow$ great for attacks (and PUFs...)

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

A Cat and Mouse Game

Early Mitigation: Increasing Refresh Rate

Early Mitigation: Increasing Refresh Rate

Early Mitigation: Increasing Refresh Rate

Early Mitigation: Increasing Refresh Rate

- Usually systems have a refresh rate of 64 ms

Early Mitigation: Increasing Refresh Rate

- Usually systems have a refresh rate of 64 ms

Early Mitigation: Increasing Refresh Rate

- Usually systems have a refresh rate of 64 ms
  - Can be increased by 2–4 times

Early Mitigation: Increasing Refresh Rate

- Usually systems have a refresh rate of 64 ms
  - Can be increased by 2–4 times
- More power is used

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

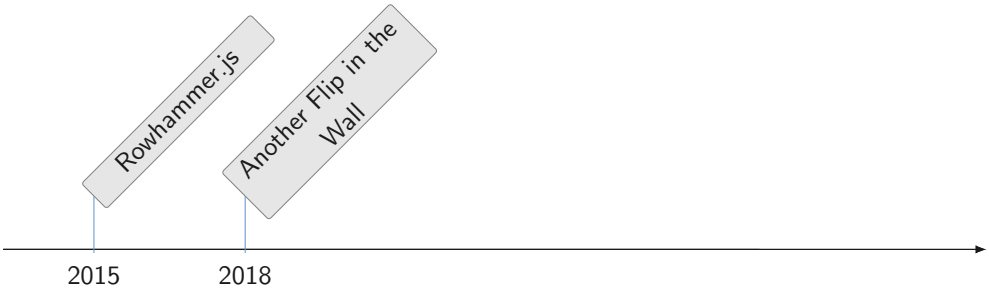
Early Mitigation: Increasing Refresh Rate

- Usually systems have a refresh rate of 64 ms
  - Can be increased by 2–4 times
- More power is used
- Will delay the requested data → less performance

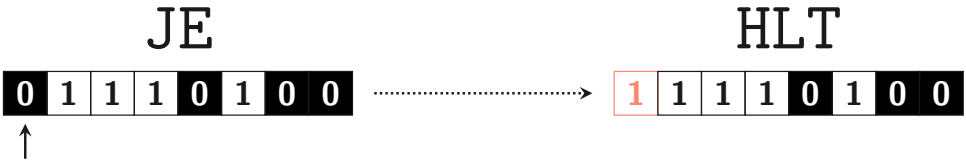
Early Mitigation: Increasing Refresh Rate

- Usually systems have a refresh rate of 64 ms
  - Can be increased by 2–4 times
- More power is used
- Will delay the requested data → less performance
- Will not prevent Rowhammer

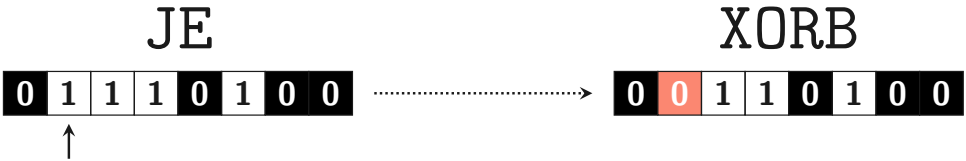
Cat and Mouse Game



2018: Opcode Flipping



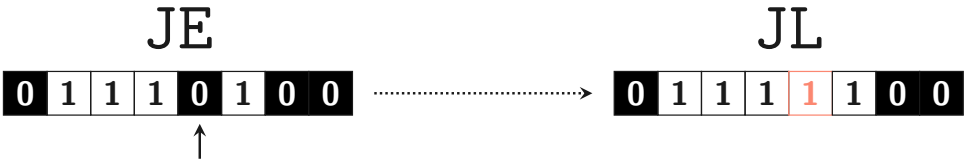
2018: Opcode Flipping



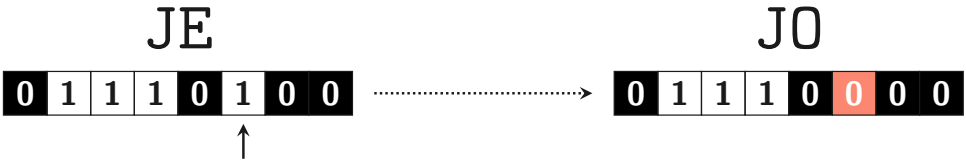
2018: Opcode Flipping

2018: Opcode Flipping

2018: Opcode Flipping

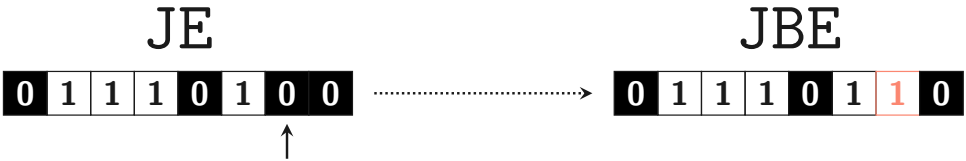


2018: Opcode Flipping

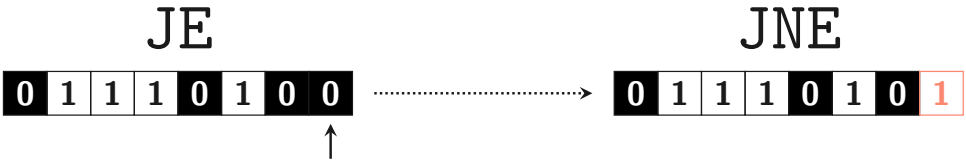


Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

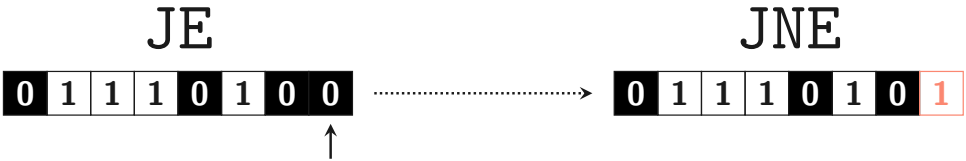
2018: Opcode Flipping



2018: Opcode Flipping



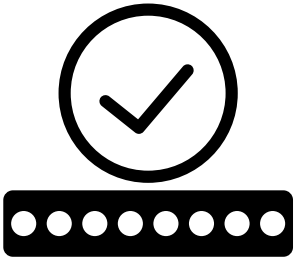
2018: Opcode Flipping



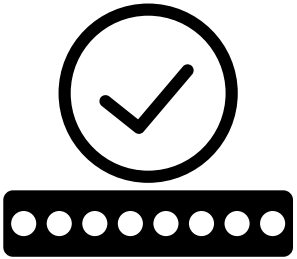
Not just opcodes → 29 exploitable bit flips in `sudo`

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

Error-Correcting Code (ECC) Memory

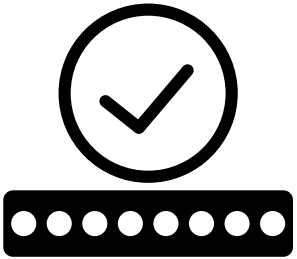


Error-Correcting Code (ECC) Memory



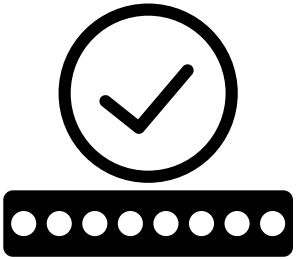
- ECC stores extra parity bits next to the data

Error-Correcting Code (ECC) Memory



- ECC stores extra parity bits next to the data
- but it can be bypassed

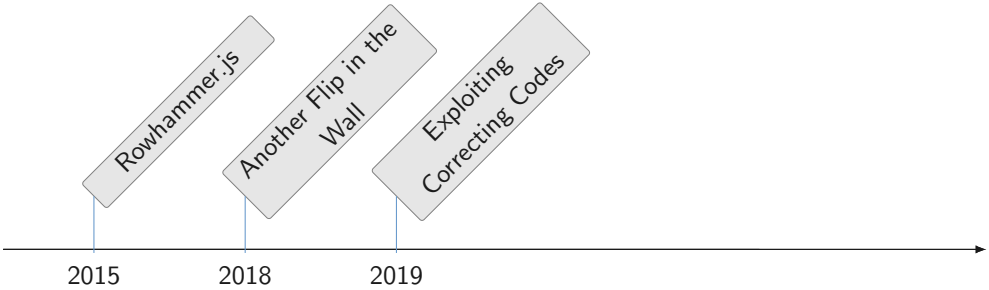
Error-Correcting Code (ECC) Memory



- ECC stores extra parity bits next to the data
- but it can be bypassed
- reverse-engineering + multiple bit flips in the right locations → ECC bypassed

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

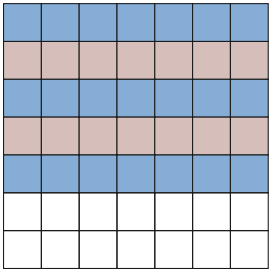
Cat and Mouse Game



Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

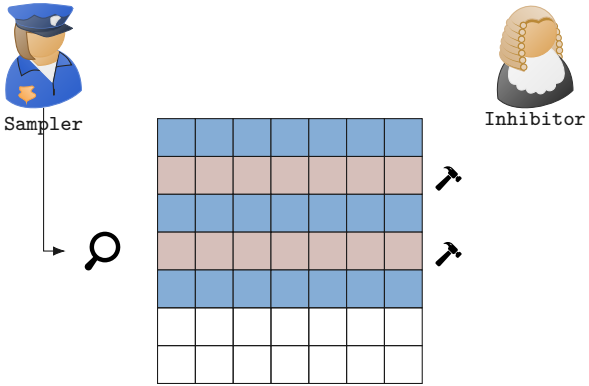
Target Row Refresh (TRR)

Sampler



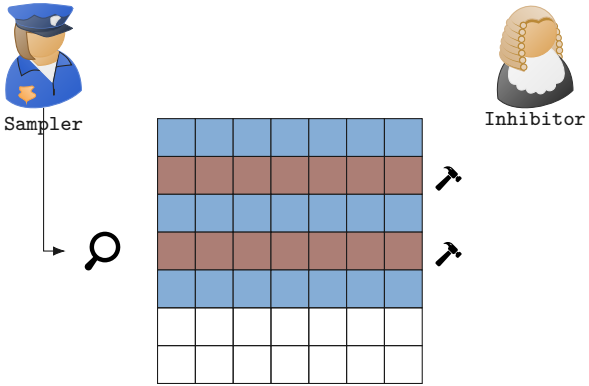
Inhibitor

Target Row Refresh (TRR)

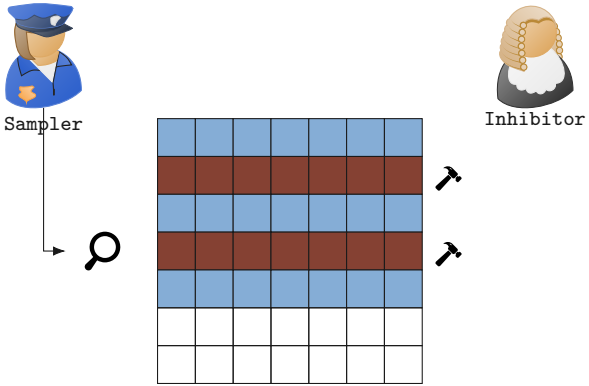


Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

Target Row Refresh (TRR)

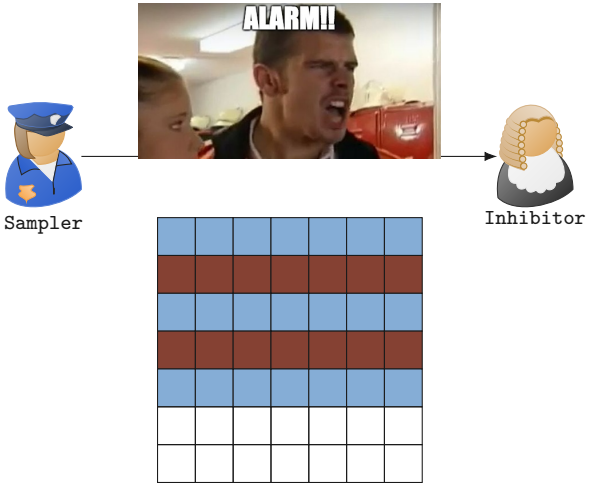


Target Row Refresh (TRR)



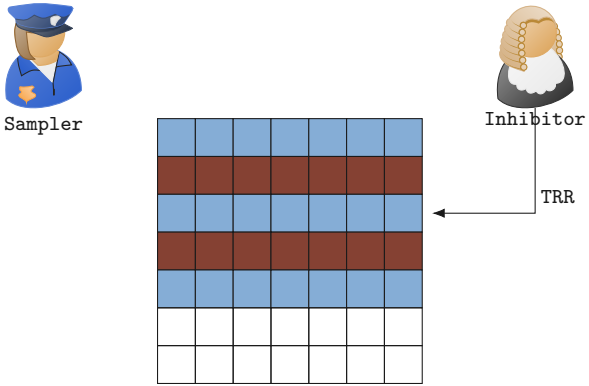
Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

Target Row Refresh (TRR)

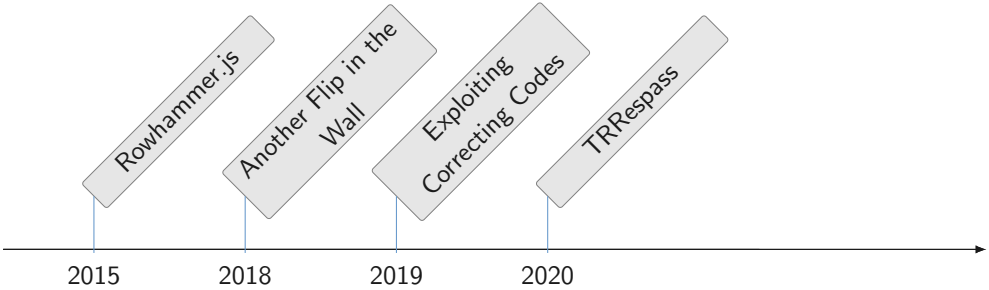


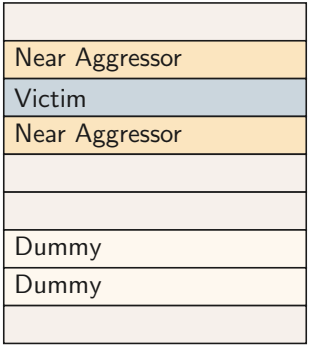
Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

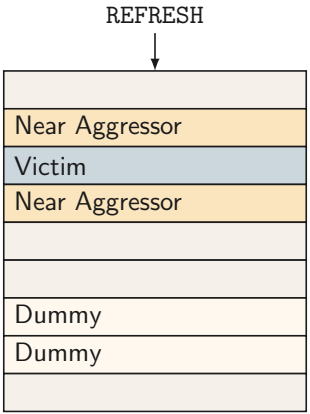
Target Row Refresh (TRR)

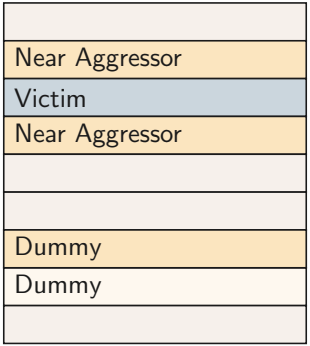


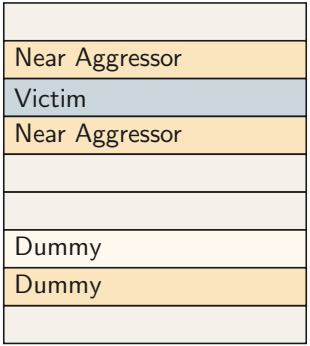
Cat and Mouse Game

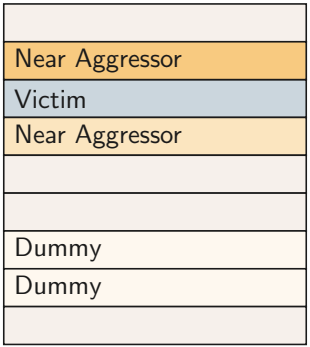


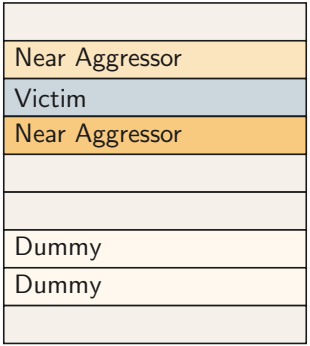

Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

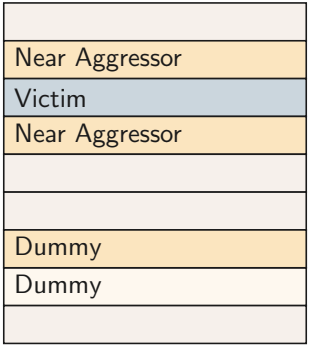

REFRESH
Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

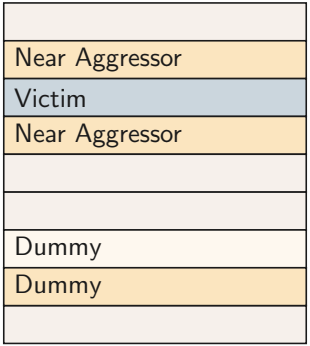

Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

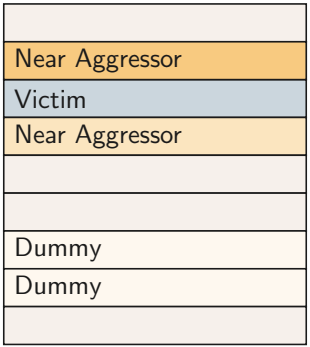

Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

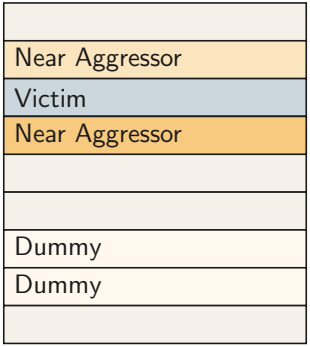

Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

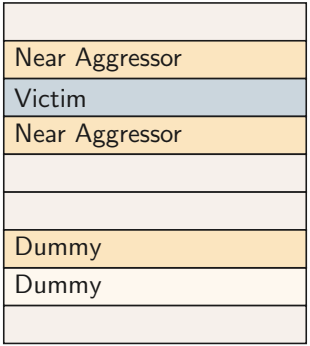

Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

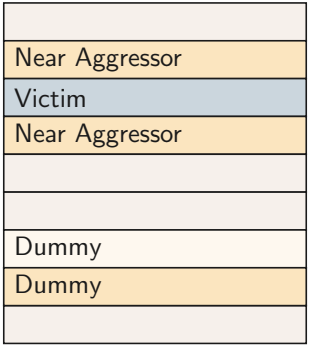

Near Aggressor
Victim
Near Aggressor
Dummy
Dummy


Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

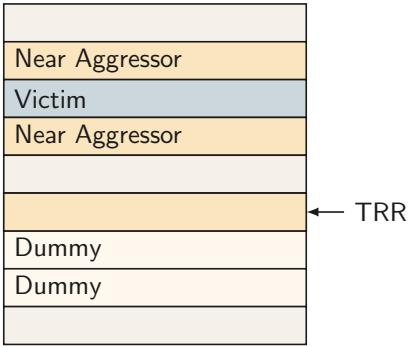

Near Aggressor
Victim
Near Aggressor
Dummy
Dummy


Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

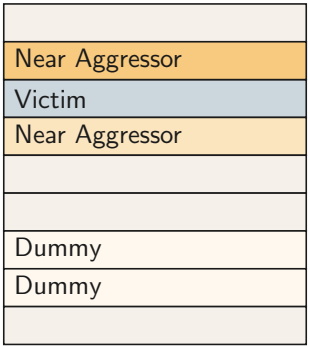

Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

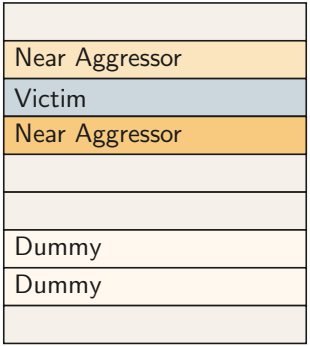

Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

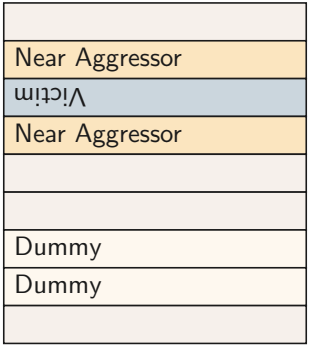
TRRespass



Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

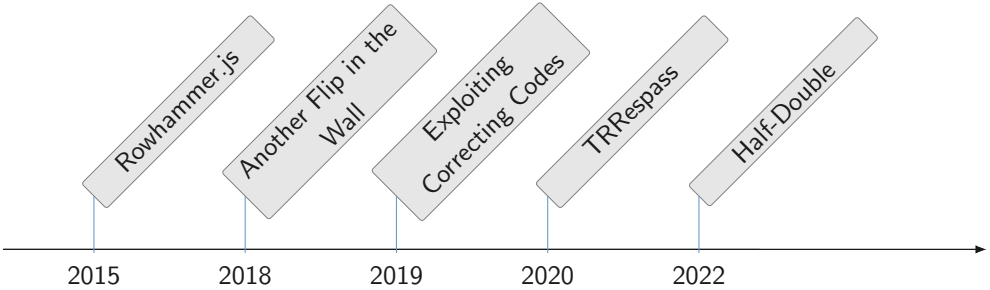

Near Aggressor
Victim
Near Aggressor
Dummy
Dummy


Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

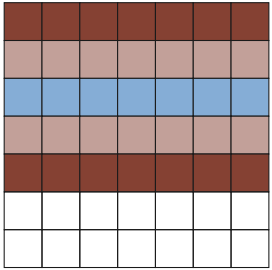


Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

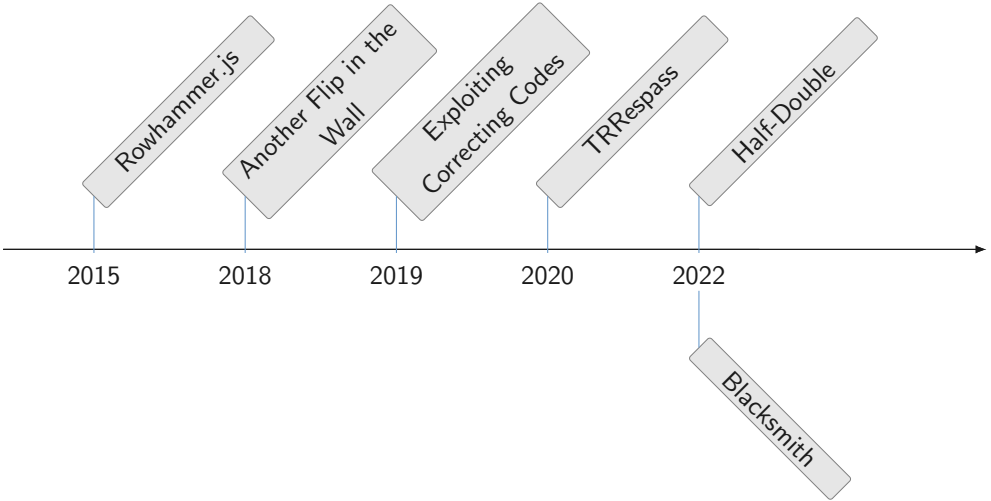
Cat and Mouse Game



Attacking with TRR: Half-Double



Cat and Mouse Game



Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

2022: Blacksmith

2022: Blacksmith

2022: Blacksmith

2022: Blacksmith

- Non-uniform Rowhammer Fuzzer

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

2022: Blacksmith

- Non-uniform Rowhammer Fuzzer
- Randomizes three characteristics:

2022: Blacksmith

- Non-uniform Rowhammer Fuzzer
- Randomizes three characteristics:

Frequency: How often the aggressor row is accessed

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

2022: Blacksmith

- Non-uniform Rowhammer Fuzzer
- Randomizes three characteristics:

Frequency: How often the aggressor row is accessed

Phase: First hammer after start of a pattern

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

2022: Blacksmith

- Non-uniform Rowhammer Fuzzer
- Randomizes three characteristics:

Frequency: How often the aggressor row is accessed
Phase: First hammer after start of a pattern
Amplitude: How many consecutive hammers

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

2022: Blacksmith

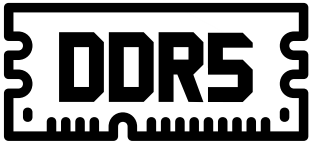
- Non-uniform Rowhammer Fuzzer
- Randomizes three characteristics:

Frequency: How often the aggressor row is accessed
Phase: First hammer after start of a pattern
Amplitude: How many consecutive hammers

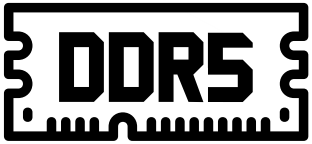
- Found bit flips in all 41 DIMMs tested

DDR5: Per Row Activation Counting (PRAC)

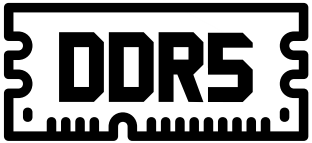
DDR5: Per Row Activation Counting (PRAC)



DDR5: Per Row Activation Counting (PRAC)

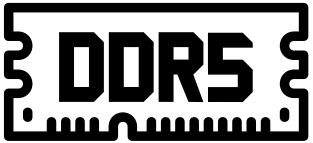


DDR5: Per Row Activation Counting (PRAC)



- Each row has its own activation counter

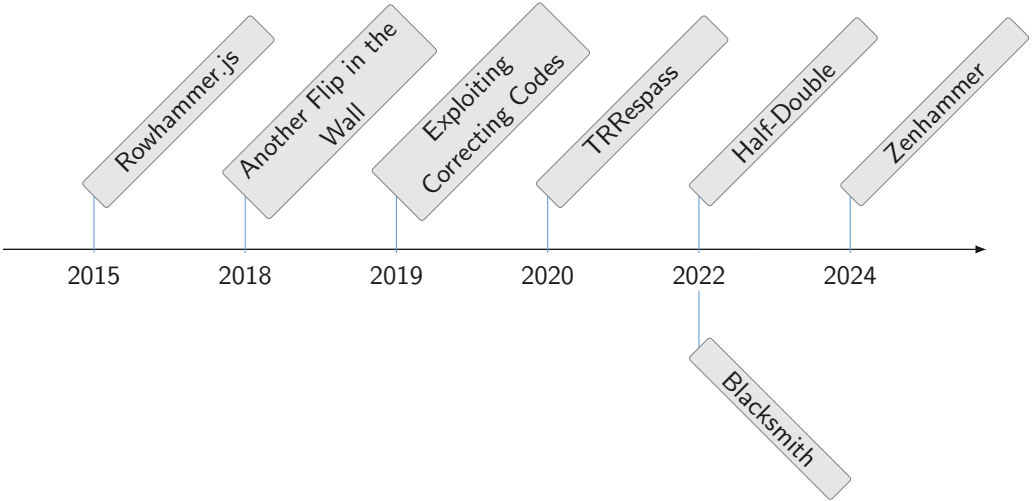
DDR5: Per Row Activation Counting (PRAC)



- Each row has its own activation counter
- Guarantee that every victim row is refreshed in a specific time frame

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

Cat and Mouse Game



2024: ZenHammer

- First Rowhammer bit flips on AMD

2024: ZenHammer

- First Rowhammer bit flips on AMD
- Different DRAM mapping, better refresh alignment

2024: ZenHammer

- First Rowhammer bit flips on AMD
- Different DRAM mapping, better refresh alignment
- First bit flips on DDR5

2024: ZenHammer

- First Rowhammer bit flips on AMD
- Different DRAM mapping, better refresh alignment
- First bit flips on DDR5 on 1 DIMM

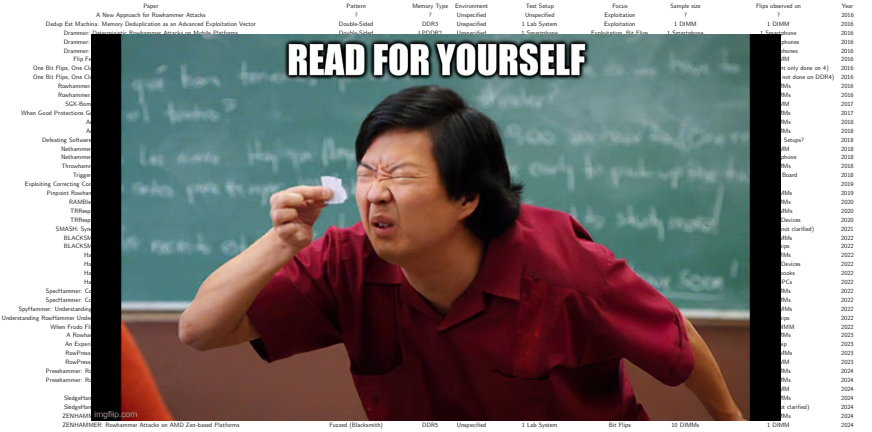
Comprehensive Review of Rowhammer Papers

Comprehensive Review of Rowhammer Papers

Paper	Pattern	Memory Type	Environment	Test Setup	Focus	Sample size	Flips observed on	Year
A New Approach for Rowhammer Attacks	?	?	Unspecified	Unspecified	Exploitation	?	?	2016
Dedup Est Machina: Memory Deduplication as an Advanced Exploitation Vector	Double-Sided	DDR3	Unspecified	1 Lab System	Exploitation	1 DIMM	1 DIMM	2016
Drammer: Deterministic Rowhammer Attacks on Mobile Platforms	Double-Sided	LPDDR2	Unspecified	1 Smartphone	Exploitation, Bit Flips	1 Smartphone	1 Smartphone	2016
Drammer: Deterministic Rowhammer Attacks on Mobile Platforms	Double-Sided	LPDDR3	Unspecified	26 Smartphones	Exploitation, Bit Flips	26 Smartphones	17 Smartphones	2016
Drammer: Deterministic Rowhammer Attacks on Mobile Platforms	Double-Sided	LPDDR4	Unspecified	1 Smartphone	Exploitation, Bit Flips	1 Smartphone	0 Smartphones	2016
Flip Feng Shui: Hammering a Needle in the Software Stack	Double-Sided	DDR3	Unspecified	1 Lab System	Exploitation	1 DIMM	1 DIMM	2016
One Bit Flips, One Cloud Flops: Cross-VM Row Hammer Attacks and Privilege Escalation	Single-Sided, Double-Sided	DDR3	Unspecified	5 Lab Systems	Exploitation, Bit Flips	5 DIMMs	4 DIMMs (experiment only done on 4)	2016
One Bit Flips, One Cloud Flops: Cross-VM Row Hammer Attacks and Privilege Escalation	Single-Sided, Double-Sided	DDR4	Unspecified	1 Lab System	Exploitation, Bit Flips	1 DIMM	0 DIMMs (experiment not done on DDR4)	2016
Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript	Double-Sided	DDR3	Unspecified	2 Lab Systems	Bit Flips	6 DIMMs	5 DIMMs	2016
Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript	Double-Sided	DDR4	Unspecified	1REFI	Bit Flips	4 DIMMs	2 DIMMs	2016
SGX-Bomb: Locking Down the Processor via Rowhammer Attack	Double-Sided	DDR4	Unspecified	1 Lab System	Exploitation, Bit Flips	1 DIMM	1 DIMM	2017
When Good Protections Go Bad: Exploiting Anti-DoS Measures to Accelerate Rowhammer Attacks	Single-Sided, Double-Sided	DDR4	Unspecified	1 Lab System	Bit Flips	4 DIMMs	3 DIMMs	2017
Another Flip in the Wall of Rowhammer Defenses	One-Location	DDR3	Unspecified	2 Lab Systems	Exploitation, Bit Flips	4 DIMMs	4 DIMMs	2018
Another Flip in the Wall of Rowhammer Defenses	One-Location	DDR4	Unspecified	1 Lab System	Exploitation, Bit Flips	2 DIMMs	2 DIMMs	2018
Defeating Software Mitigations Against Rowhammer: A Surgical Precision Hammer	Single-Sided, Double-Sided, Amplified	DDR3	Unspecified	2 Lab Systems	Exploitation	33 Memory Setups?	14 Memory Setups?	2018
Nethammer: Inducing Rowhammer Faults through Network Requests	Double-Sided	DDR4	Unspecified	3 Lab Systems	Exploitation, Bit Flips	1 DIMM	1 DIMM	2018
Nethammer: Inducing Rowhammer Faults through Network Requests	One-Location	LPDDR2	Unspecified	1 Smartphone	Exploitation, Bit Flips	1 Smartphone	1 Smartphone	2018
Throwhammer: Rowhammer Attacks over the Network and Defenses	Double-Sided	DDR3	Unspecified	2 Lab Systems	Bit Flips	4 DIMMs	4 DIMMs	2018
Triggering Rowhammer Hardware Faults on ARM: A Revisit	Double-Sided	LPDDR3	Unspecified	1 Single Board Computer	Bit Flips	1 Single Board	1 Single Board	2018
Exploiting Correcting Codes: On the Effectiveness of ECC Memory Against Rowhammer Attacks	Double-Sided	?	Unspecified	?	Exploitation	?	?	2019
Pinpoint Rowhammer: Suppressing Unwanted Bit Flips on Rowhammer Attacks	Double-Sided	DDR3	Unspecified	1 Lab System	Bit Flips	16 DIMMs	12 DIMMs	2019
RAMBleed: Reading Bits in Memory Without Accessing Them	Single-Sided, Double-Sided	DDR3	Unspecified	1 Lab System	Bit Flips	2 DIMMs	2 DIMMs	2020
TRRespass: Exploiting the Many Sides of Target Row Refresh	Many-Sided	DDR4	Unspecified	1 Lab System	Bit Flips	42 DIMMs	13 DIMMs	2020
TRRespass: Exploiting the Many Sides of Target Row Refresh	Many-Sided	LPDDR4X	Unspecified	13 Mobile Devices	Bit Flips	13 Mobile Devices	5 Mobile Devices	2020
SMASH: Synchronized Many-sided Rowhammer Attacks from JavaScript	Many-Sided	DDR4	Unspecified	3 Lab Systems	Bit Flips	5 DIMMs	3 - 5 DIMMs (not clarified)	2021
BLACKSMITH: Scalable Rowhammering in the Frequency Domain	Fuzzed (Blacksmith)	DDR4	Unspecified	10 Lab Systems	Bit Flips	40 DIMMs	40 DIMMs	2022
BLACKSMITH: Scalable Rowhammering in the Frequency Domain	Fuzzed (Blacksmith)	LPDDR4X	Unspecified	JEDEC-compliant developer board	Bit flips	19 Chips	16 Chips	2022
Half-Double: Hammering From the Next Row Over	Half-Double	DDR4	Unspecified	FPGA	Bit Flips	3 DIMMs	2 DIMMs	2022
Half-Double: Hammering From the Next Row Over	Half-Double	LPDDR4X	Unspecified	7 Mobile Devies	Bit Flips	7 Mobile Devices	5 Mobile Devices	2022
Half-Double: Hammering From the Next Row Over	Half-Double	DDR4	Unspecified	1 Notebook	Bit Flips	1 Notebook	0 Notebooks	2022
Half-Double: Hammering From the Next Row Over	Half-Double	LPDDR4	Unspecified	2 MiniPCs	Bit Flips	2 MiniPCs	0 MiniPCs	2022
SpecHammer: Combining Spectre and Rowhammer for New Speculative Attacks	Double-Sided	DDR3	Unspecified	1 Lab System	Exploitation, Bit Flips	3 DIMMs	3 DIMMs	2022
SpecHammer: Combining Spectre and Rowhammer for New Speculative Attacks	Many-Sided	DDR4	Unspecified	3 Lab Systems	Exploitation, Bit Flips	3 DIMMs	3 DIMMs	2022
SpyHammer: Understanding and Exploiting RowHammer Under Fine-Grained Temperature Variations	Single-Sided	DDR4	Temperature	FPGA	Bit Flips	12 DIMMs	12 DIMMs	2022
Understanding RowHammer Under Reduced Wordline Voltage: An Experimental Study Using Real DRAM Devices	Double-Sided	DDR4	?	SiC	FPGA	Bit Flips	30 DIMMs (272 Chips)	64 Chips	2022
When Frodo Flips: End-to-End Key Recovery on FrodoKEM via Rowhammer	Double-Sided	DDR3	Unspecified	1 Lab System	Exploitation	2 DIMMs	¿= 1 DIMM	2022
A Rowhammer Reproduction Study Using the Blacksmith Fuzzer	Fuzzed (Blacksmith)	DDR4	Unspecified	4 Lab Systems	Bit Flips	10 DIMMs	8 DIMMs	2023
An Experimental Analysis of RowHammer in HBM2 DRAM Chips	Double-Sided	HBM2	Unspecified	FPGA	Bit Flips	1 Chip	1 Chip	2023
RowPress: Amplifying Read Disturbance in Modern DRAM Chips	Single-Sided	DDR4	Temperature	FPGA	Bit Flips	21 DIMMs	21 DIMMs	2023
RowPress: Amplifying Read Disturbance in Modern DRAM Chips	Single-Sided	DDR4	Unspecified	1 Lab System	Bit Flips	1 DIMM	1 DIMM	2023
Preshammer: Rowhammer and Rowpress Without Physical Address Information	Fuzzed (Blacksmith)	DDR4	Unspecified	Lab Systems	Bit Flips	12 DIMMs	6 DIMMs	2024
Preshammer: Rowhammer and Rowpress Without Physical Address Information	Single-Sided	DDR4	Unspecified	Lab Systems	Bit Flips	12 DIMMs	2 DIMMs	2024
RISC-H: Rowhammer Attacks on RISC-V	Double-Sided	DDR4	?	1 Lab System (RISC-V)	Bit Flips	1 DIMM	1 DIMM	2024
SledgeHammer: Amplifying Rowhammer via Bank-level Parallelism	Many-Sided	DDR3	Unspecified	1 Lab System	Bit Flips	1 DIMM	? DIMMs	2024
SledgeHammer: Amplifying Rowhammer via Bank-level Parallelism	Many-Sided	DDR4	Unspecified	1 Lab System	Bit Flips	2 DIMMs	2 DIMMs (not clarified)	2024
ZENHAMMER: Rowhammer Attacks on AMD Zen-based Platforms	Fuzzed (Blacksmith)	DDR4	Unspecified	3 Lab Systems	Bit Flips	10 DIMMs	8 DIMMs	2024
ZENHAMMER: Rowhammer Attacks on AMD Zen-based Platforms	Fuzzed (Blacksmith)	DDR5	Unspecified	1 Lab System	Bit Flips	10 DIMMs	1 DIMM	2024

Table 1: Overview of Rowhammer Studies

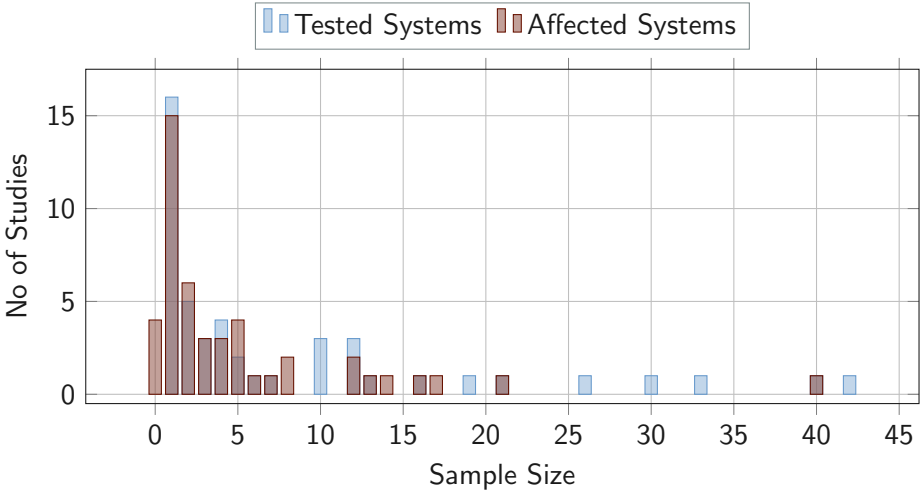
Comprehensive Review of Rowhammer Papers



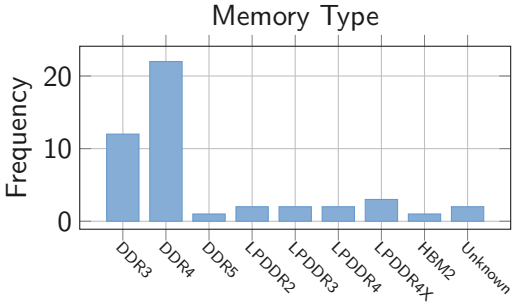
Paper	Pattern	Memory Type	Environment	Test Setup	Focus	Sample size	Flips observed on	Year
A New Approach for Rowhammer Attacks	?	?	Unspecified	Unspecified	Exploitation	?	?	2016
Dedup Est Machina: Memory Deduplication as an Advanced Exploitation Vector	Double-Sided	DDR3	Unspecified	1 Lab System	Exploitation	1 DIMM	1 DIMM	2016
Drammer: Deterministic Rowhammer Attacks on Mobile Platforms	Double-Sided	LPDDR3	Unspecified	1 Smartphone	Exploitation, Bit Flips	1 Smartphone	1 Smartphone	2016
Drammer:							phones	2016
Drammer:							phones	2016
Flip Fe							IM	2016
One Bit Flips, One Cu							t only done on 4)	2016
One Bit Flips, One Cu							not done on DDR4)	2016
Rowhammer							Ms	2016
Rowhammer							Ms	2016
SGX-Bom							IM	2017
When Good Protections Go							Ms	2017
A							Ms	2018
Ad							Ms	2018
Defeating Software							Setups?	2018
Nethammer							IM	2018
Nethammer							phone	2018
Throwhamm							Ms	2018
Trigger							Board	2018
Exploiting Correcting Cod								2019
Pinpoint Rowhar							Ms	2019
RAMBlu							Ms	2020
TRResp							Ms	2020
TRResp							Devices	2020
SMASH: Syn							not clarified)	2021
BLACKSM							Ms	2022
BLACKSM							ips	2022
Ha							Ms	2022
Ru							Devices	2022
Ha							ooks	2022
Ha							PCs	2022
SpecHammer: Co							Ms	2022
SpecHammer: Co							Ms	2022
SpyHammer: Understanding							Ms	2022
Understanding RowHammer Unde							ips	2022
When Frodo Flip							HMM	2022
A Rowha							Ms	2023
An Experi							p	2023
RowPress							Ms	2023
RowPress							IM	2023
Preshammer: Ro							Ms	2024
Preshammer: Ro							Ms	2024
							IM	2024
SledgeHam							Ms	2024
SledgeHam							t clarified)	2024
ZENHAMMER: Rowhammer Attacks on AMD Zen-based Platforms	Fuzzed (Blacksmith)	DDR5	Unspecified	1 Lab System	Bit Flips	10 DIMMs	1 DIMM	2024

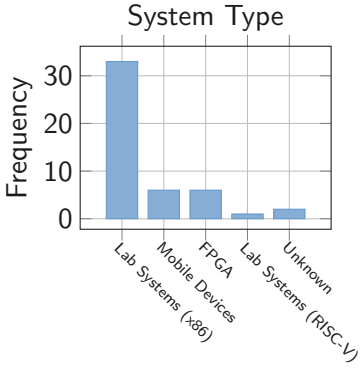
Table 1: Overview of Rowhammer Studies

Rowhammer Papers: Sample Sizes



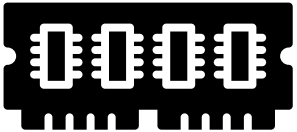
Rowhammer Papers: Experimental Setup



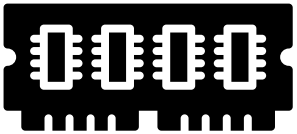


So, does it really matter?

Is Rowhammer relevant?

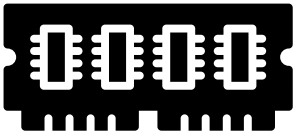


Is Rowhammer relevant?



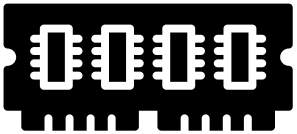
- Reliability? Yes, but...

Is Rowhammer relevant?



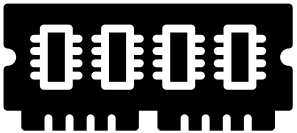
- Reliability? Yes, but...
- Exploits? Yes, but..

Is Rowhammer relevant?



- Reliability? Yes, but...
- Exploits? Yes, but..
- Prevalence? Are even that many system affected?

Is Rowhammer relevant?

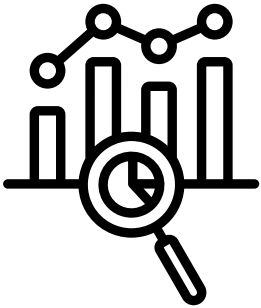


- Reliability? Yes, but...
- Exploits? Yes, but..
- Prevalence? Are even that many system affected?

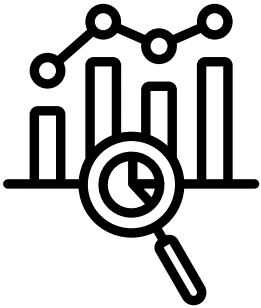
→ **We don't know!**

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

Rowhammer Prevalence - What We Know

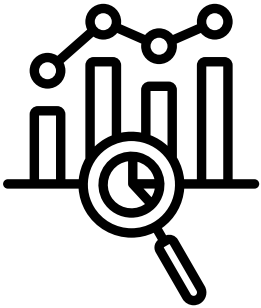


Rowhammer Prevalence - What We Know

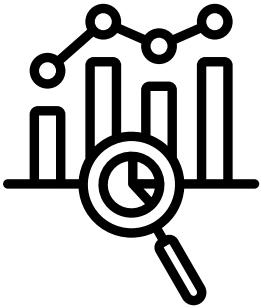


- Overall 378 DIMMs tested

Rowhammer Prevalence - What We Know



- Overall 378 DIMMs tested
- Overall 296 DIMMs (78.3 %) affected




IS 400 A LOT?
DEPENDS.
mg MDMA? YES.
DIMMs? NO.

What do we need?

A Large-Scale Prevalence Study

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

Goal of our Study

Goal of our Study

- Real-world conditions on real systems

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

Goal of our Study

- Real-world conditions on real systems
- Large-scale prevalence observations

Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

Goal of our Study

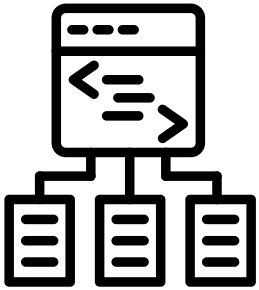
- Real-world conditions on real systems
- Large-scale prevalence observations
- Reproducibility of bit flips

Goal of our Study

- Real-world conditions on real systems
- Large-scale prevalence observations
- Reproducibility of bit flips ($\rightarrow$ are Rowhammer PUFs even practical?)

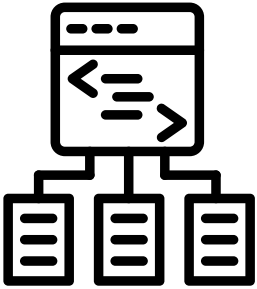
Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

Our Framework and Study: FlippyR.am



Linux bundled with a set of tools to

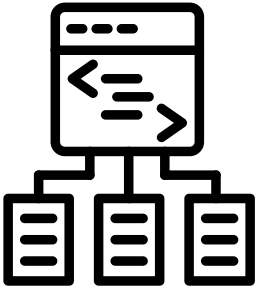
Our Framework and Study: FlippyR.am



Linux bundled with a set of tools to

- Test and identify DRAM address functions

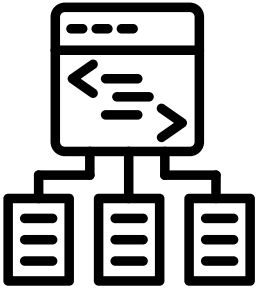
Our Framework and Study: FlippyR.am



Linux bundled with a set of tools to

- Test and identify DRAM address functions
  - Drama, DRAMDig, TRRespass RE, Dare (Zenhammer), AMDRE

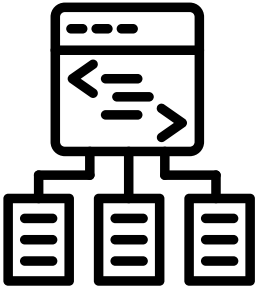
Our Framework and Study: FlippyR.am



Linux bundled with a set of tools to

- Test and identify DRAM address functions
  - Drama, DRAMDig, TRRespass RE, Dare (Zenhammer), AMDRE
- Test Rowhammer patterns and document bit flips

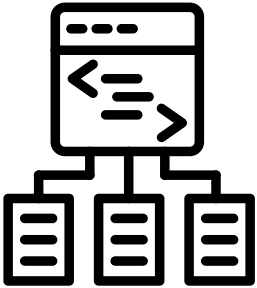
Our Framework and Study: FlippyR.am



Linux bundled with a set of tools to

- Test and identify DRAM address functions
  - Drama, DRAMDig, TRRespass RE, Dare (Zenhammer), AMDRE
- Test Rowhammer patterns and document bit flips
  - Blacksmith, TRRespass, RowhammerJs, Rowhammer-Test, FlipFloyd, RowPress, HammerTool

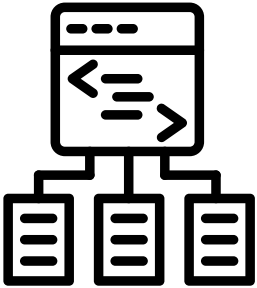
Our Framework and Study: FlippyR.am



Linux bundled with a set of tools to

- Test and identify DRAM address functions
  - Drama, DRAMDig, TRRespass RE, Dare (Zenhammer), AMDRE
- Test Rowhammer patterns and document bit flips
  - Blacksmith, TRRespass, RowhammerJs, Rowhammer-Test, FlipFloyd, RowPress, HammerTool
- **No** attacks/exploits

Our Framework and Study: FlippyR.am



Linux bundled with a set of tools to

- Test and identify DRAM address functions
  - Drama, DRAMDig, TRRespass RE, Dare (Zenhammer), AMDRE
- Test Rowhammer patterns and document bit flips
  - Blacksmith, TRRespass, RowhammerJs, Rowhammer-Test, FlipFloyd, RowPress, HammerTool
- **No** attacks/exploits
  - No advantage in testing them on real-world systems

How can I participate?

How can I participate?

- Get a free bootable USB stick from us

How can I participate?

- 

How can I participate?

- Get a free bootable USB stick from us
- or download bootable ISO from `https://FlippyR.am`

How can I participate?

- Get a free bootable USB stick from us
- or download bootable ISO from `https://FlippyR.am`

→ Run our tests while you don't need the system (e.g., while sleeping/at work)

How can I participate?

- Get a free bootable USB stick from us
- or download bootable ISO from `https://FlippyR.am`

→ Run our tests while you don't need the system (e.g., while sleeping/at work)

→ Upload your results → then they contribute to our study

- Everything is open source: `https://FlippyR.am`

- Everything is open source: `https://FlippyR.am`
- Build the ISO and flash it yourself

Trusting Trust

- Everything is open source: `https://FlippyR.am`
- Build the ISO and flash it yourself
- Docker-Image is available as well

Trusting Trust

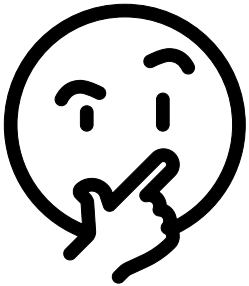
- Everything is open source: `https://FlippyR.am`
- Build the ISO and flash it yourself
- Docker-Image is available as well
- ISO-Image booted via USB is best

Trusting Trust

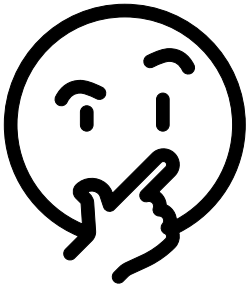
- Everything is open source: `https://FlippyR.am`
- Build the ISO and flash it yourself
- Docker-Image is available as well
- ISO-Image booted via USB is best
  - (your own or ours, doesn't matter for us)

More ideas to address concerns...

More ideas to address concerns...

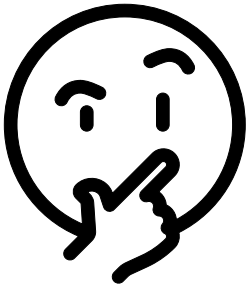


More ideas to address concerns...



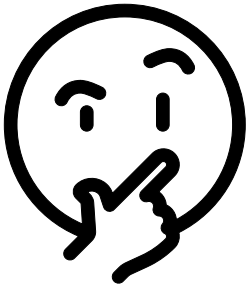
More ideas to address concerns...

- Got the USB stick from us?



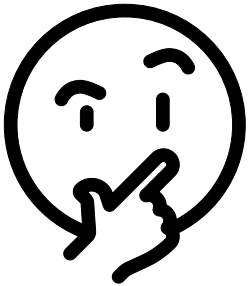
More ideas to address concerns...

- Got the USB stick from us?

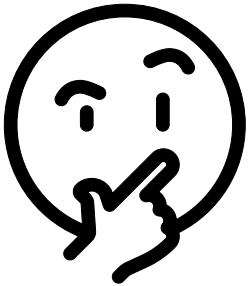


More ideas to address concerns...

- Got the USB stick from us?
  - You know who we are

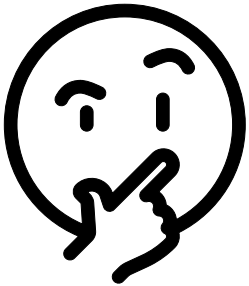


More ideas to address concerns...



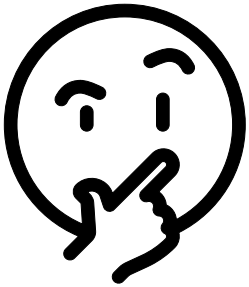
- Got the USB stick from us?
  - You know who we are
  - This is a DFG-FWF research project

More ideas to address concerns...



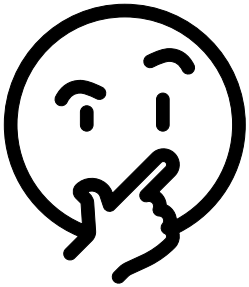
- Got the USB stick from us?
  - You know who we are
  - This is a DFG-FWF research project
  - We don't spread malware $\rightarrow$ We would run into bigger problems if we would

More ideas to address concerns...



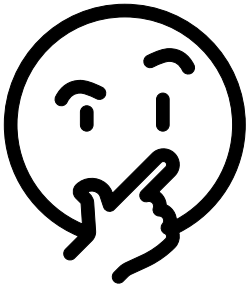
- Got the USB stick from us?
  - You know who we are
  - This is a DFG-FWF research project
  - We don't spread malware → We would run into bigger problems if we would
- Should I disconnect all disks and peripherals? If you feel like it...

More ideas to address concerns...



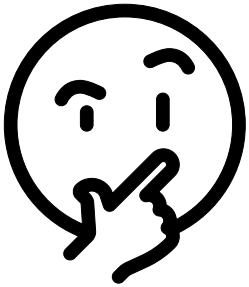
- Got the USB stick from us?
  - You know who we are
  - This is a DFG-FWF research project
  - We don't spread malware → We would run into bigger problems if we would
- Should I disconnect all disks and peripherals? If you feel like it...
- Science is important but I still have concerns

More ideas to address concerns...



- Got the USB stick from us?
  - You know who we are
  - This is a DFG-FWF research project
  - We don't spread malware → We would run into bigger problems if we would
- Should I disconnect all disks and peripherals? If you feel like it...
- Science is important but I still have concerns
  - Don't participate if you have concerns

More ideas to address concerns...



- Got the USB stick from us?
  - You know who we are
  - This is a DFG-FWF research project
  - We don't spread malware → We would run into bigger problems if we would
- Should I disconnect all disks and peripherals? If you feel like it...
- Science is important but I still have concerns
  - Don't participate if you have concerns
  - Otherwise: please help us answering a question that we can't answer without you

Why should I participate?

Why should I participate?

Why should I participate?

Why should I participate?

- **How relevant is Rowhammer on real systems?**

Why should I participate?

- **How relevant is Rowhammer on real systems?**
- Academics cannot answer this alone

Why should I participate?

- **How relevant is Rowhammer on real systems?**
- Academics cannot answer this alone
  - we need real users to know

Why should I participate?

- **How relevant is Rowhammer on real systems?**
- Academics cannot answer this alone
  - we need real users to know
- Other perks, if you want to:

Why should I participate?

- **How relevant is Rowhammer on real systems?**
- Academics cannot answer this alone
  - we need real users to know
- Other perks, if you want to:
  - Keep your flippyr.am USB stick

Why should I participate?

- **How relevant is Rowhammer on real systems?**
- Academics cannot answer this alone
  - we need real users to know
- Other perks, if you want to:
  - Keep your flippyr.am USB stick
  - Get a flippyr.am t-shirt if you test at least 10 systems (limited stock)

Why should I participate?

- **How relevant is Rowhammer on real systems?**
- Academics cannot answer this alone
  - we need real users to know
- Other perks, if you want to:
  - Keep your flippyr.am USB stick
  - Get a flippyr.am t-shirt if you test at least 10 systems (limited stock)
  - You can win a gift card (see website)

Why should I participate?

- **How relevant is Rowhammer on real systems?**
- Academics cannot answer this alone
  - we need real users to know
- Other perks, if you want to:
  - Keep your flippyr.am USB stick
  - Get a flippyr.am t-shirt if you test at least 10 systems (limited stock)
  - You can win a gift card (see website)
  - Get your name in the acknowledgements of our study

Why should I participate?

- **How relevant is Rowhammer on real systems?**
- Academics cannot answer this alone
  - we need real users to know
- Other perks, if you want to:
  - Keep your flippyr.am USB stick
  - Get a flippyr.am t-shirt if you test at least 10 systems (limited stock)
  - You can win a gift card (see website)
  - Get your name in the acknowledgements of our study
  - Learn if your own hardware is affected

Conclusion and Call to Action

Conclusion and Call to Action

Conclusion and Call to Action

Conclusion and Call to Action

- Rowhammer: reliability issue + exploitable

Conclusion and Call to Action

- Rowhammer: reliability issue + exploitable
- Real-world prevalence still unclear

Conclusion and Call to Action

- Rowhammer: reliability issue + exploitable
- Real-world prevalence still unclear
- Join us: Contribute to the large-scale flippyr.am study!

Ten Years of Rowhammer

A Retrospect (and Path to the Future)

Martin Heckel[1,2] **(@lunkw1ll)**
Daniel Gruss[1] **(@lavados)**
Florian Adamsky[2] **(@c1t)**

[1] Graz University of Technology
[2] Hof University of Applied Sciences

NeRAM
FWF Der Wissenschaftsfonds.
DFG Deutsche Forschungsgemeinschaft