ATTACKING AND SECURING LEAKY SYSTEMS AT THE HARDWARE-SOFTWARE BOUNDARY

JONAS JUFFINGER

ASSESSORS:
DANIEL GRUSS
ONUR MUTLU

7. JULY 2025

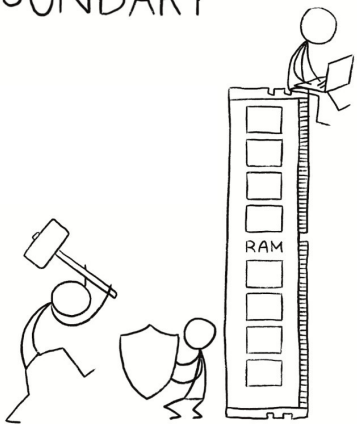
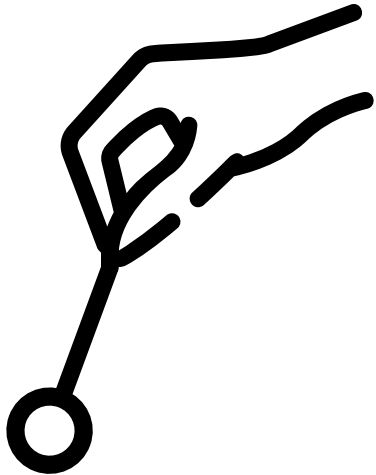
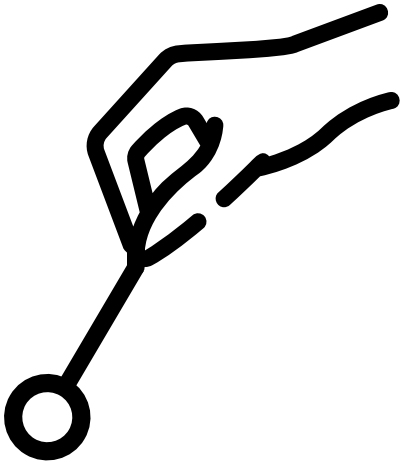
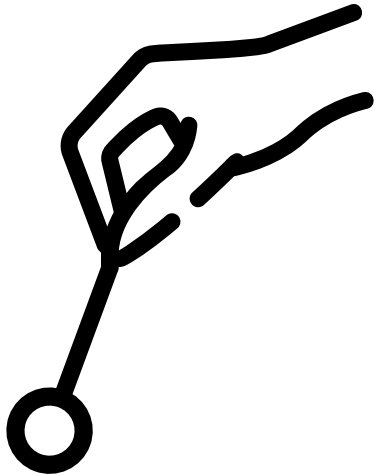
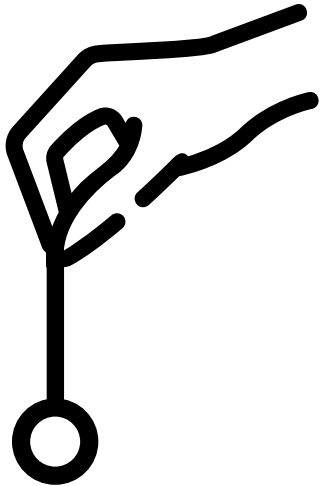


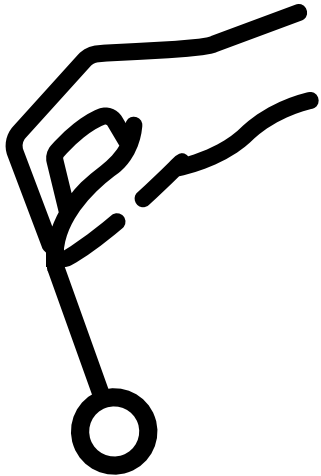
Image in a world **without** software vulnerabilities.

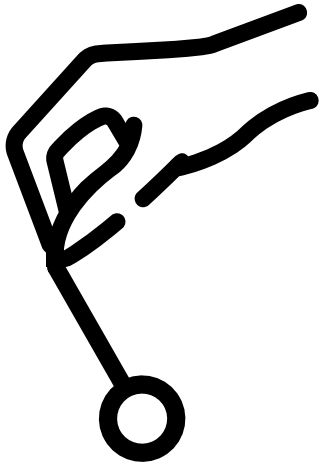












Critical vulnerability CVE-2025-32463 in sudo jeopardizes Linux systems

Posted on 2025-07-02 by guenni

[German]The sudo command in Linux allows local privilege escalation due to a vulnerability CVE-2025-32463 classified as critical. The background is an improper handling of /etc/nsswitch.conf, so that root privileges are obtained.

I came across the topic once through a comment by German blog reader Norddeutsch in my other IT blog, as well as through a tweet. I'm dragging the details here into the post, as I clean up the discussion area cyclically. Norddeutsch wrote;

> *Linux user expects urgent updates from the sudo package.* ***Priority high****, remote possible. This for various distributions and branches.*

Critical vulnerability CVE-2025-32463 in sudo jeopardizes Linux systems

Posted on 2025-07-02 by [illegible]

[German]The sudo command in Linux allows local privilege escalation due to a vulnerability CVE-2025-32463 classified as critical. The background is an improper handling of /etc/nsswitch.conf, so that root privileges are obtained.

I came across the topic once through a comment by German blog reader Norddeutsch in my other IT blog, as well as through a tweet. I'm dragging the details here into the post, as I clean up the discussion area cyclically. Norddeutsch wrote;

> *Linux [illegible] expects urgent updates from the sudo package.* ***Priority high****, remote [illegible] sible. This for various distributions and branches.*

Search Torrents | Browse Torrents | Recent Torrents | Top 100

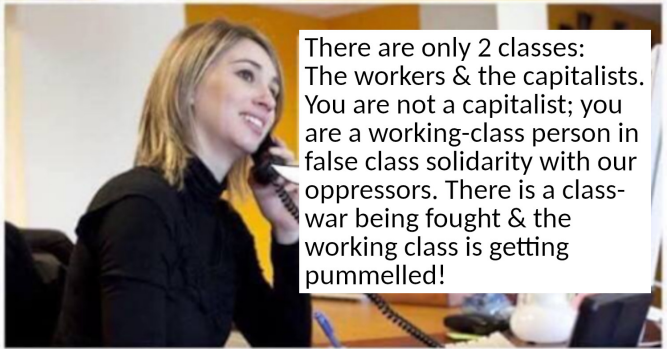
Pirate Search

All Audio Video Applications Games Porn Other

Pirate Search I'm Feeling Lucky

>pirate a game
>cmd.exe opens and closes in a blink of an eye


Hi!
I'd like a
wake up call.


There are only 2 classes:
The workers & the capitalists.
You are not a capitalist; you are a working-class person in false class solidarity with our oppressors. There is a class-war being fought & the working class is getting pummelled!

There are more issues still **unresolved**.

Phishing

Graham Smith | Mar 18, 2023 | 2 min read

How a CEO lost €42 million and his job after a cyber-attack

← Previous
Next →

Let's look at one of the most notorious cyber-attacks of all time. The 2016 phishing email was sent to aerospace manufacturer FACC. We'll explore how it all went down, the impact on the company, and what happened to the people involved.

The attack was a whale-phishing email scam known as a 'fake president' attack. In a phishing scam, hackers send numerous generic emails to random individuals hoping to trick them into

From: Stefan Mangard <gunthjerom01@gmail.com>
Sent: Tuesday, June 3, 2025 8:00 AM
To: Jonas Juffinger
Subject: Assistance Required

Good morning,

Are you familiar with gift cards? I need you to get some for me from any nearby store, there are some prospects I need to send them to but I'm currently out of town and few stores here don't stock them. Let me know if you can get them right now so I can tell you how many I would need and what amount. I'll refund you

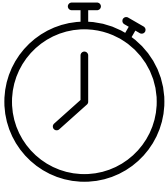
Software runs on **hardware**

Software runs on **hardware**

... which can be leaky.

Hardware can be leaky

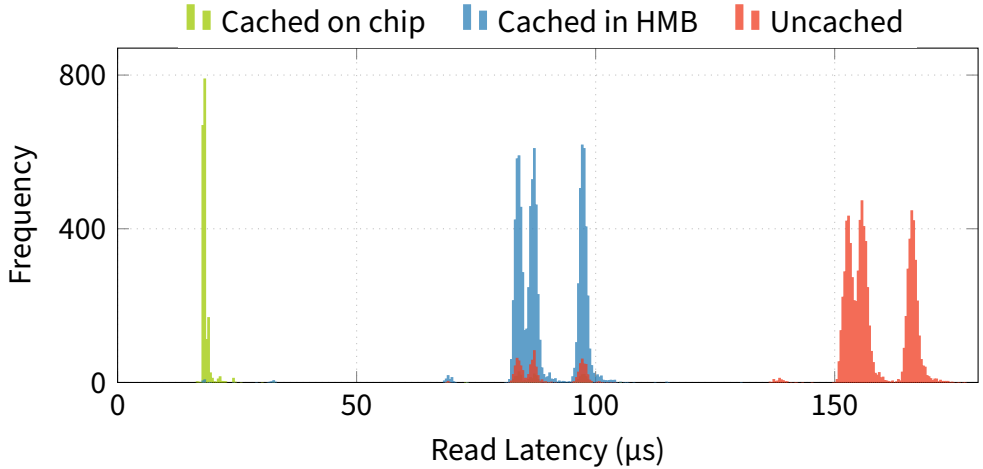
Hardware can be leaky



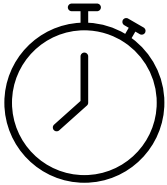
Side Channels


I WONDER WHAT THE CODE IS...

Side Channels

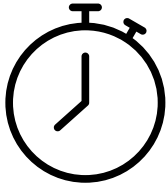


Hardware can be leaky



Side Channels

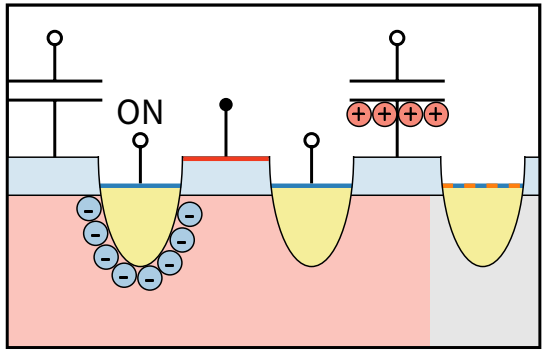
Hardware can be leaky



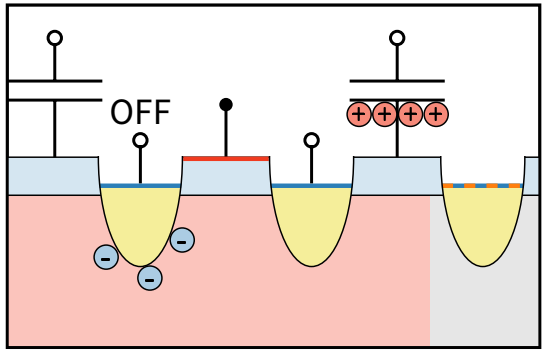
Side Channels

Rowhammer

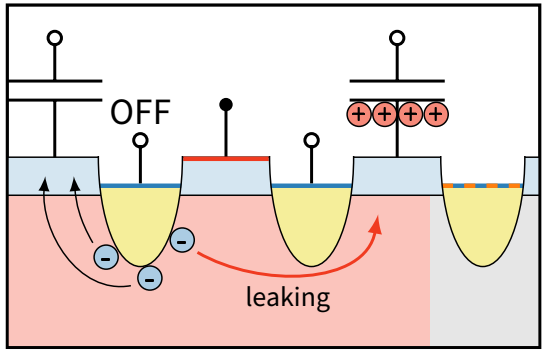
Rowhammer



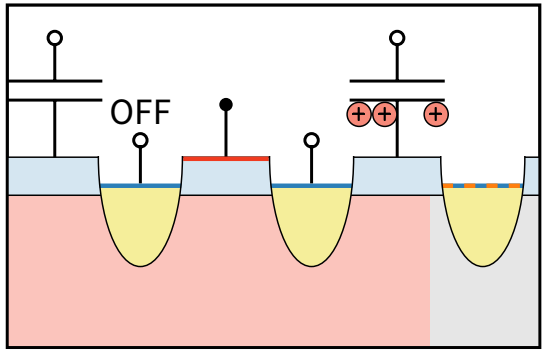
Rowhammer



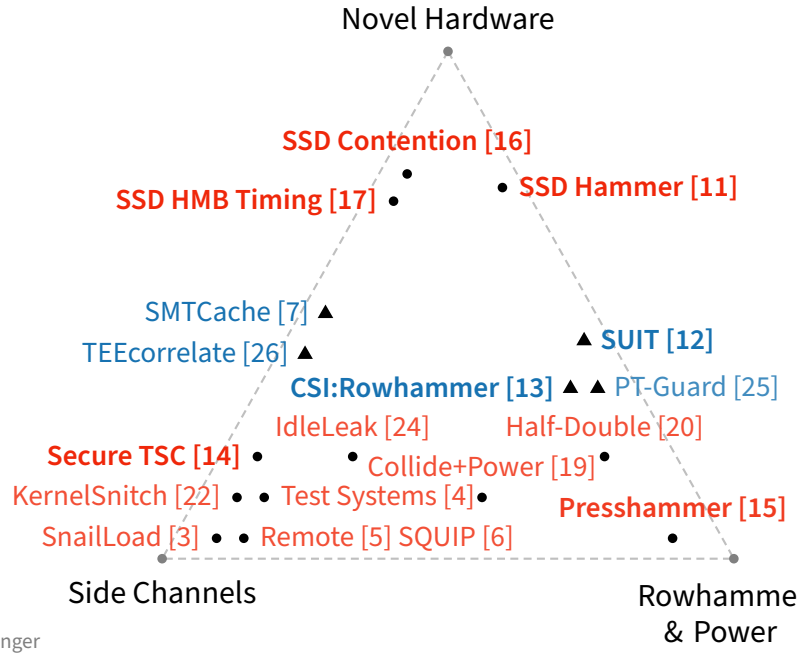
Rowhammer

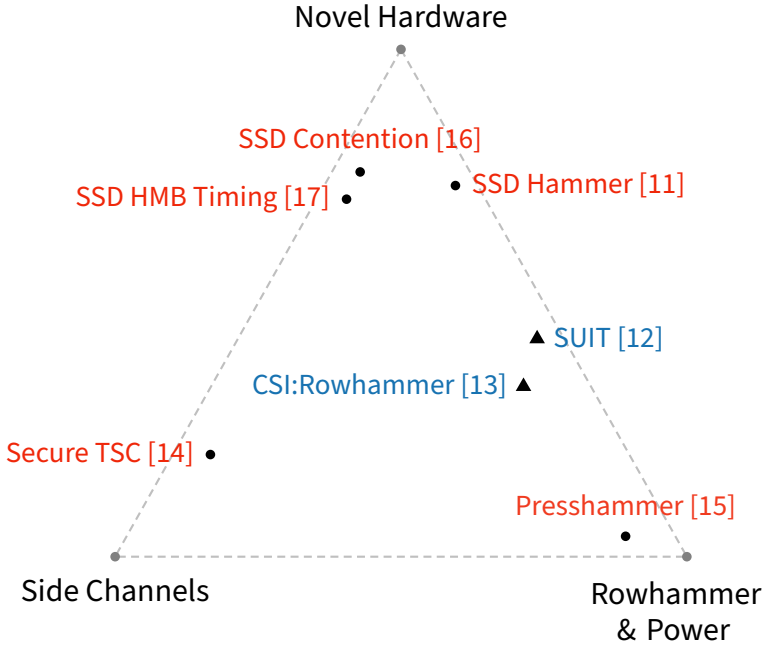


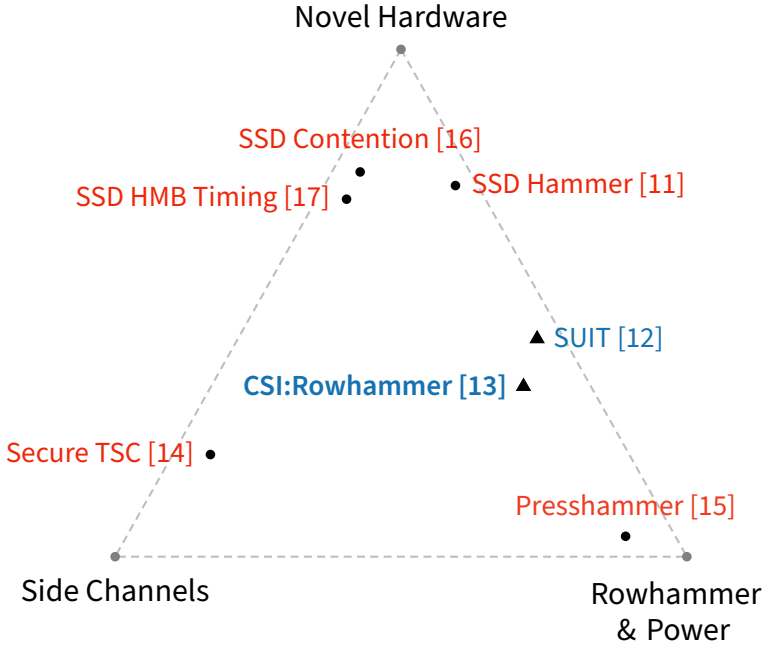
Rowhammer

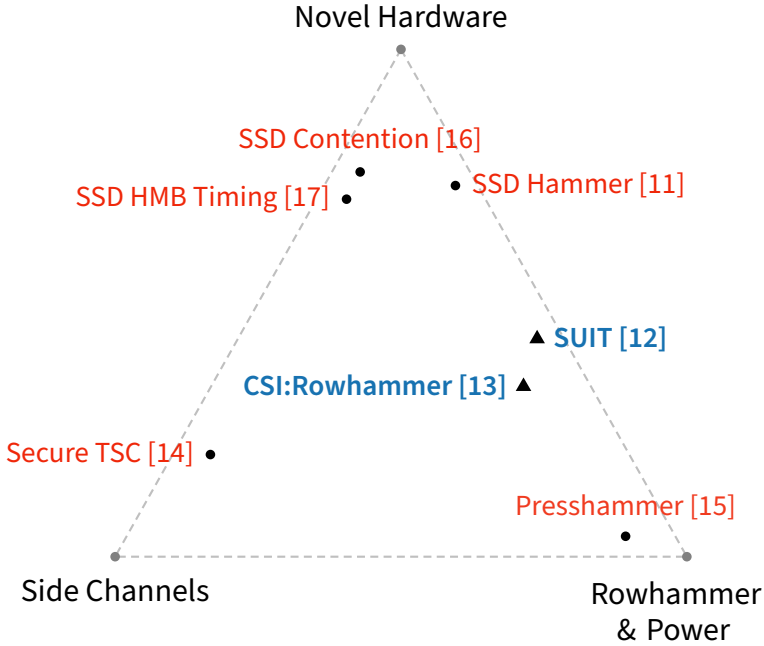


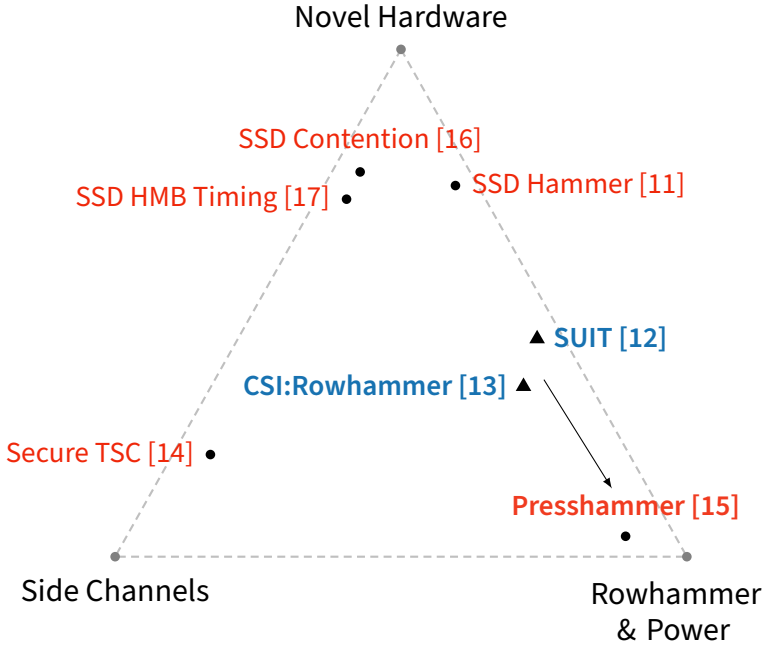
Contributions

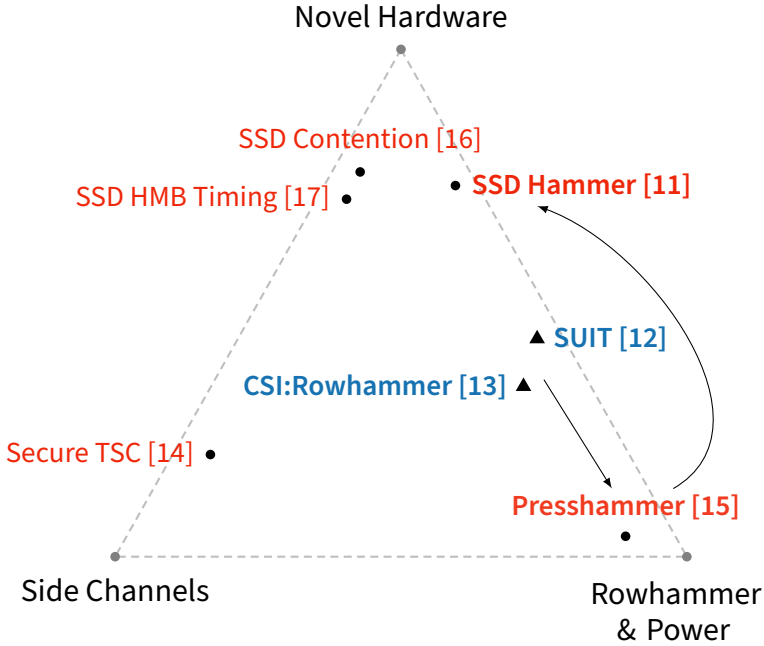

Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SMTCache [7]
TEEcorrelate [26]
SUIT [12]
CSI:Rowhammer [13]
PT-Guard [25]
IdleLeak [24]
Half-Double [20]
Secure TSC [14]
Collide+Power [19]
KernelSnitch [22]
Test Systems [4]
Presshammer [15]
SnailLoad [3]
Remote [5] SQUIP [6]
Side Channels
Rowhammer & Power

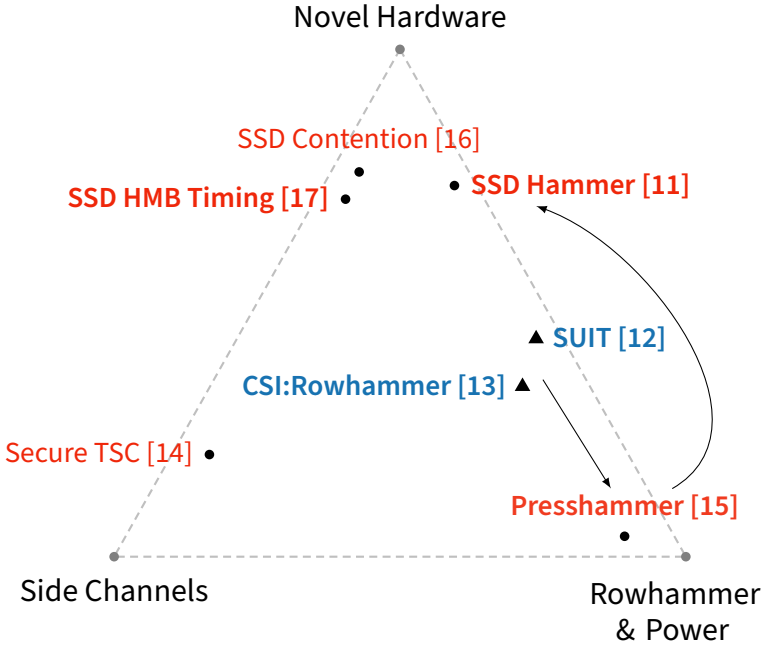

Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer
& Power

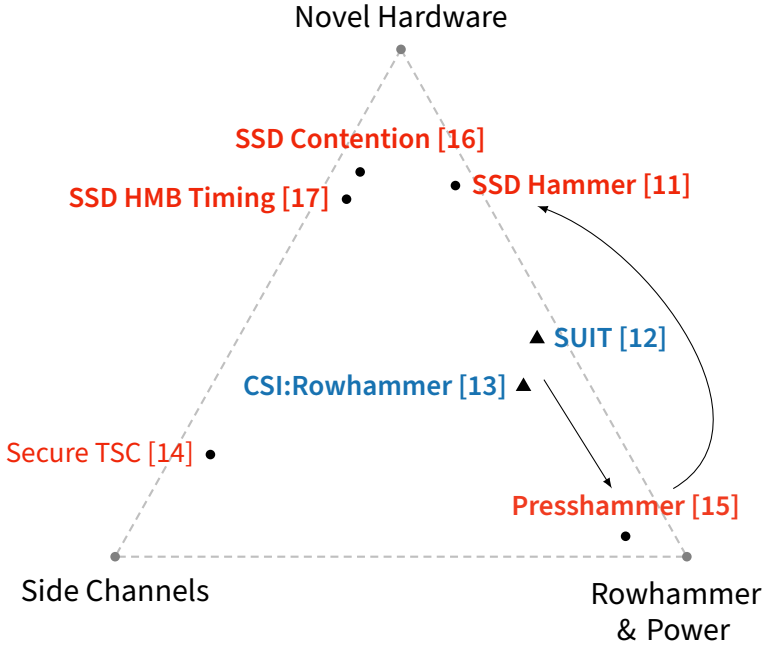

Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer
& Power

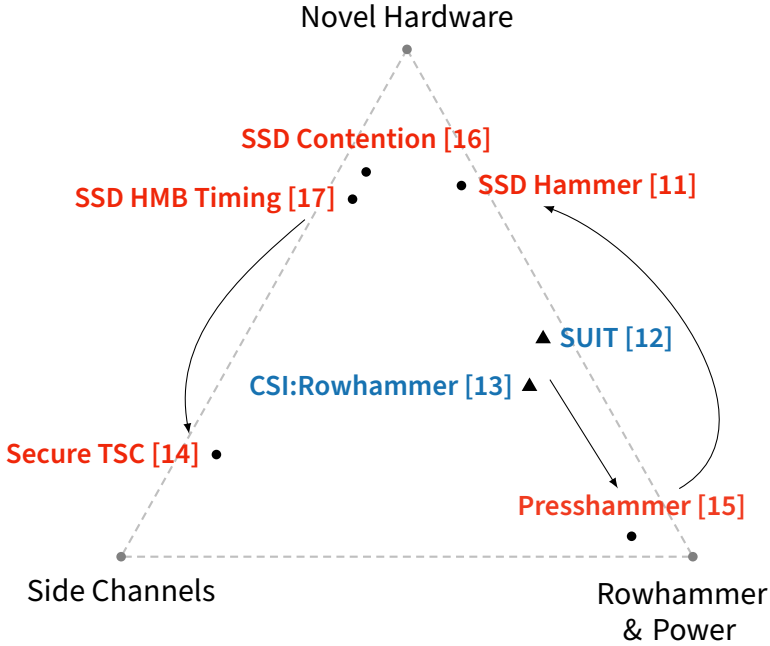

Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer & Power


Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer
& Power


Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer
& Power


Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer
& Power


Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer
& Power


Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer
& Power

CSI:Rowhammer

Cryptographic Security and Integrity against Rowhammer

Jonas Juffinger, Lukas Lamster, Andreas Kogler, Maria Eichlseder,
Moritz Lipp, and Daniel Gruss

S&P, 2023

The Problem with Rowhammer Defenses

The Problem with Rowhammer Defenses

- Focusing on **characteristics**

The Problem with Rowhammer Defenses

- Focusing on **characteristics**
- Which later turn out to be incomplete

The Problem with Rowhammer Defenses

- Focusing on **characteristics**
- Which later turn out to be incomplete
  - Bit flips are infrequent - ECC, Refresh Rate

The Problem with Rowhammer Defenses

- Focusing on **characteristics**
- Which later turn out to be incomplete
  - ~~Bit flips are infrequent - ECC, Refresh Rate~~ [18]

The Problem with Rowhammer Defenses

- Focusing on **characteristics**
- Which later turn out to be incomplete
  - ~~Bit flips are infrequent - ECC, Refresh Rate~~ [18]
  - Detectable with performance counters - ANVIL

The Problem with Rowhammer Defenses

- Focusing on **characteristics**
- Which later turn out to be incomplete
  - ~~Bit flips are infrequent - ECC, Refresh Rate~~ [18]
  - ~~Detectable with performance counters - ANVIL~~ [8]

The Problem with Rowhammer Defenses

- Focusing on **characteristics**
- Which later turn out to be incomplete
  - ~~Bit flips are infrequent - ECC, Refresh Rate~~ [18]
  - ~~Detectable with performance counters - ANVIL~~ [8]
  - Can simply be mitigated by detecting victims - TRR

The Problem with Rowhammer Defenses

- Focusing on **characteristics**
- Which later turn out to be incomplete
  - ~~Bit flips are infrequent - ECC, Refresh Rate~~ [18]
  - ~~Detectable with performance counters - ANVIL~~ [8]
  - ~~Can simply be mitigated by detecting victims - TRR~~ [2, 10, 9]

The Problem with Rowhammer Defenses

- Focusing on **characteristics**
- Which later turn out to be incomplete
  - ~~Bit flips are infrequent - ECC, Refresh Rate~~ [18]
  - ~~Detectable with performance counters - ANVIL~~ [8]
  - ~~Can simply be mitigated by detecting victims - TRR~~ [2, 10, 9]
  - Hammer distance is 1 - TRR, ZebRAM, B-CATT

The Problem with Rowhammer Defenses

- Focusing on **characteristics**
- Which later turn out to be incomplete
  - ~~Bit flips are infrequent - ECC, Refresh Rate~~ [18]
  - ~~Detectable with performance counters - ANVIL~~ [8]
  - ~~Can simply be mitigated by detecting victims - TRR~~ [2, 10, 9]
  - ~~Hammer distance is 1 - TRR, ZebRAM, B-CATT~~ [20]

The Solution

Detect all data integrity violations.

The Solution

Detect all data integrity violations.

The Solution

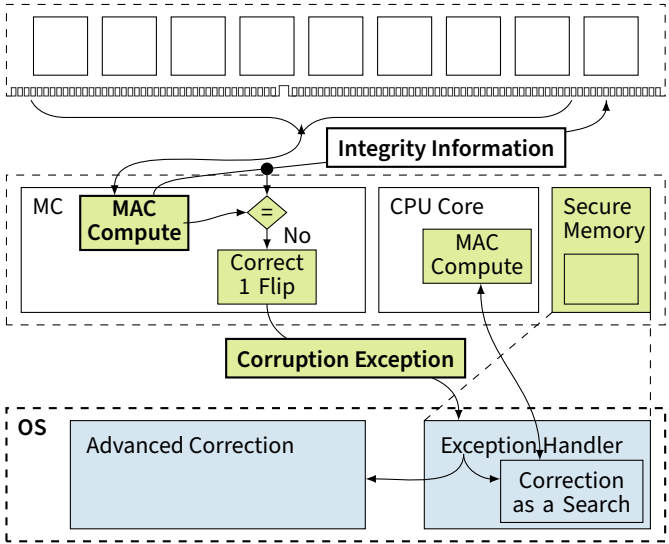
Best effort data correction.

The Solution

Best effort data correction.

Every attack becomes DoS in the worst case.

CSI:Rowhammer – Overview



CSI:Rowhammer – Data Correction

CSI:Rowhammer – Data Correction

MACs **cannot** correct bit flips.

CSI:Rowhammer – Data Correction

- Brute force search with **approximate equality**

CSI:Rowhammer – Data Correction

- Brute force search with **approximate equality**
- OS has some **knowledge** about the corrupted data

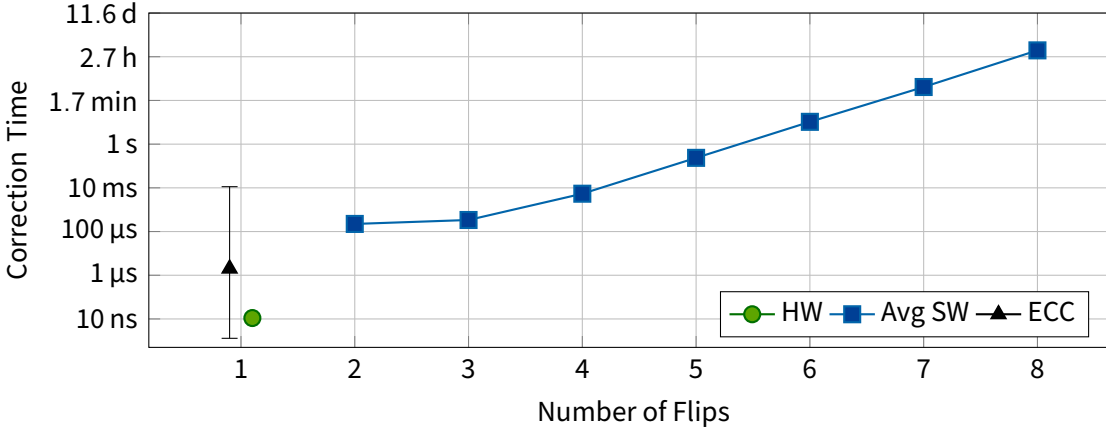
CSI:Rowhammer – Data Correction

- Brute force search with **approximate equality**
- OS has some **knowledge** about the corrupted data
- Reload disk backed data instead of correcting

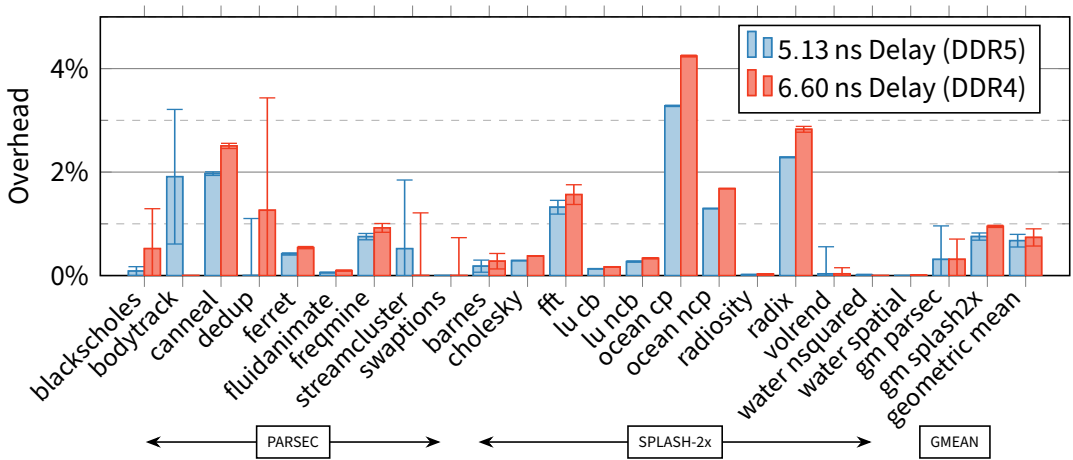
CSI:Rowhammer – Data Correction

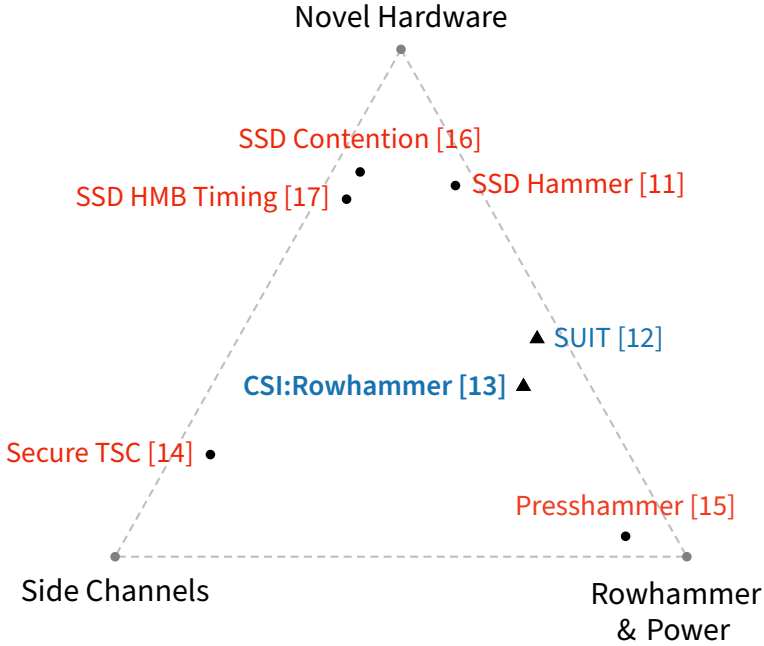
- Brute force search with **approximate equality**
- OS has some **knowledge** about the corrupted data
- Reload disk backed data instead of correcting
- Recompute data (page tables)

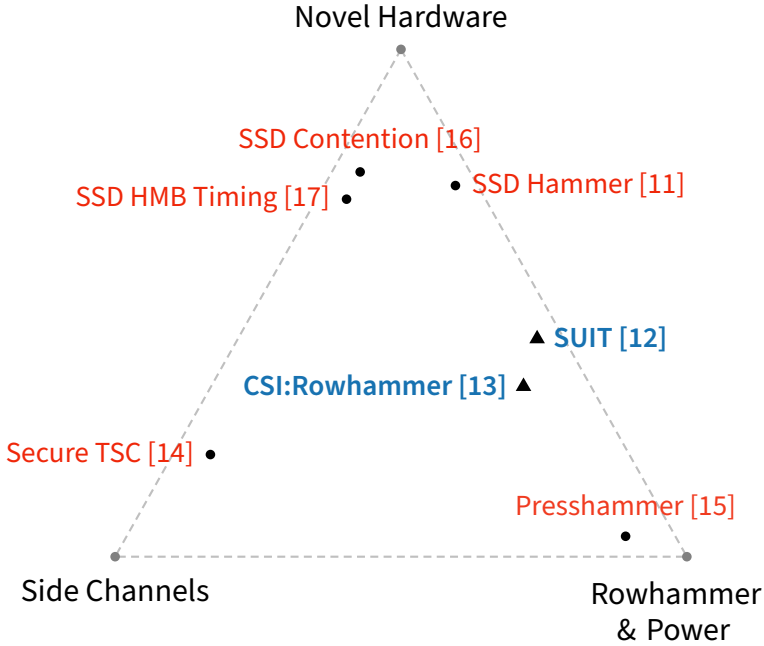
CSI:Rowhammer – Correction Time



CSI:Rowhammer – Performance Overhead




Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer & Power


Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer & Power

SUIT

Secure Undervolting with Instruction Traps

Jonas Juffinger, Stepan Kalinin, Daniel Gruss, Frank Mueller

ASPLOS, 2024

CPU Undervolting

Decreases Power Consumption

CPU Undervolting

Decreases Power Consumption

Increases Performance

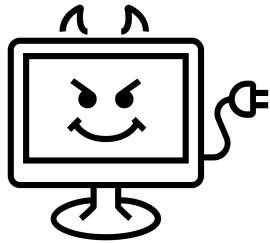
Performance Improvement and Power Savings

CPU	V_{off}	Performance	Power	Frequency	Efficiency
i5-1035G1	−70 mV	+6.0 %	−0.1 %	+8.5 %	+6.1 %
	−97 mV	+7.9 %	−0.5 %	+12 %	+8.4 %
i9-9900K	−70 mV	+2.2 %	−7.2 %	+2.6 %	+10 %
	−97 mV	+3.8 %	−16 %	+3.3 %	+23 %
7700X	−70 mV	+1.4 %	−9.8 %	+1.8 %	+12 %
	−97 mV	+1.9 %	−15 %	+1.8 %	+20 %

The Problem with CPU Undervolting

Cause Reliability Issues

The Problem with CPU Undervolting



Cause **Security** Issues

An infinite loop...

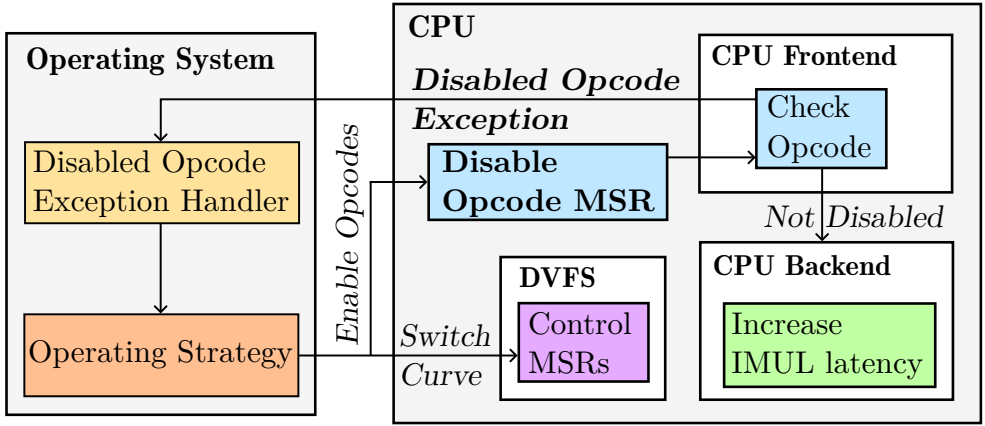

```
uint64_t multiplier = 0x1276af93a60d1cb7;
uint64_t var = 0x1313f7d45dd0339a * multiplier;

while (var == 0x1313f7d45dd0339a * multiplier)
{
  var  = 0x1313f7d45dd0339a;
  var *= multiplier;
}

printf("loop exited!\n");
```

[23]

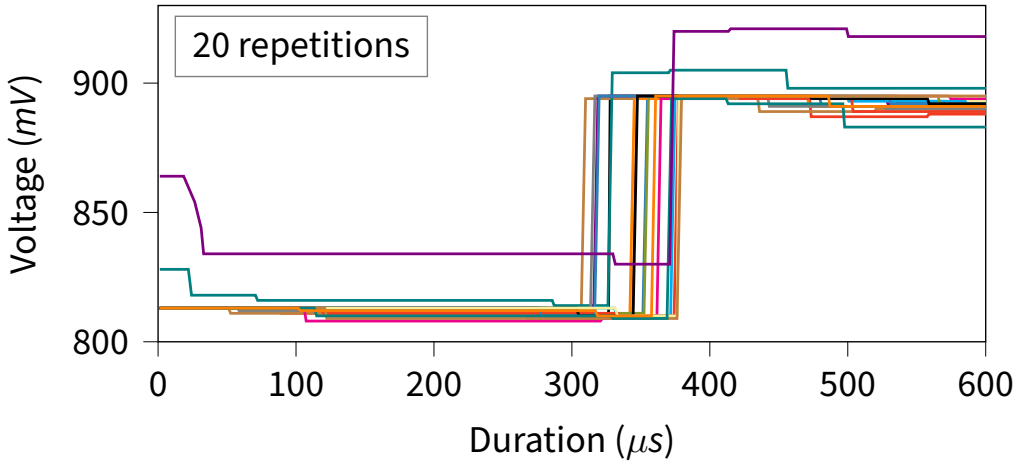
SUIT – Idea

Disable potentially faulting instruction while **undervolting**.

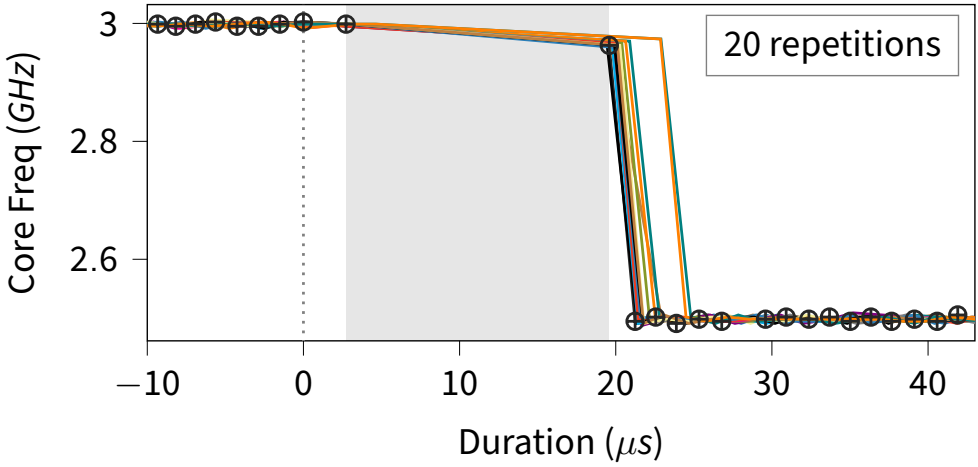
SUIT – Overview



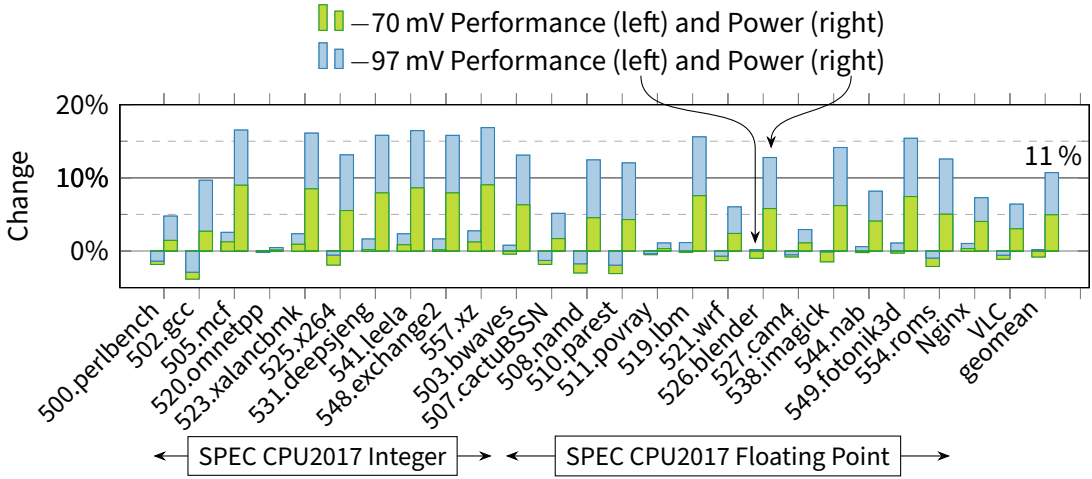
Voltage Change Delay

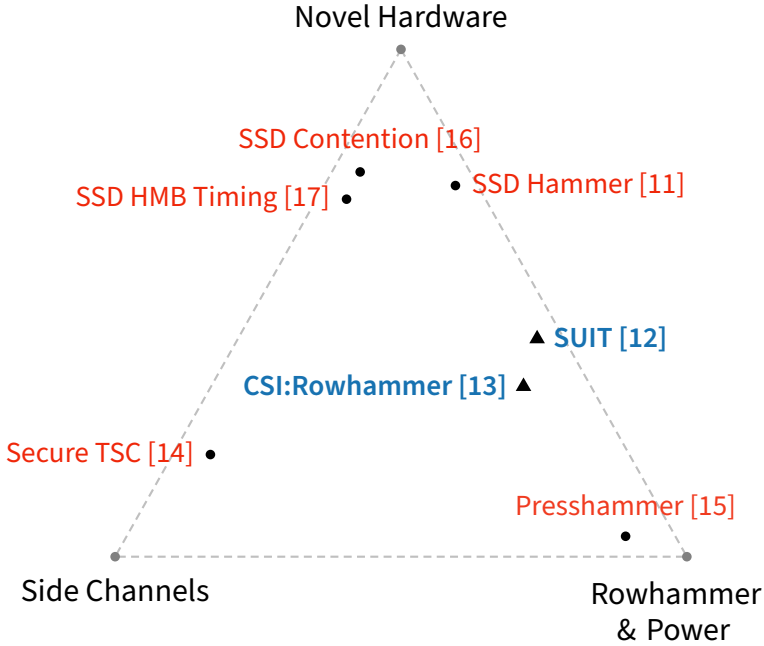


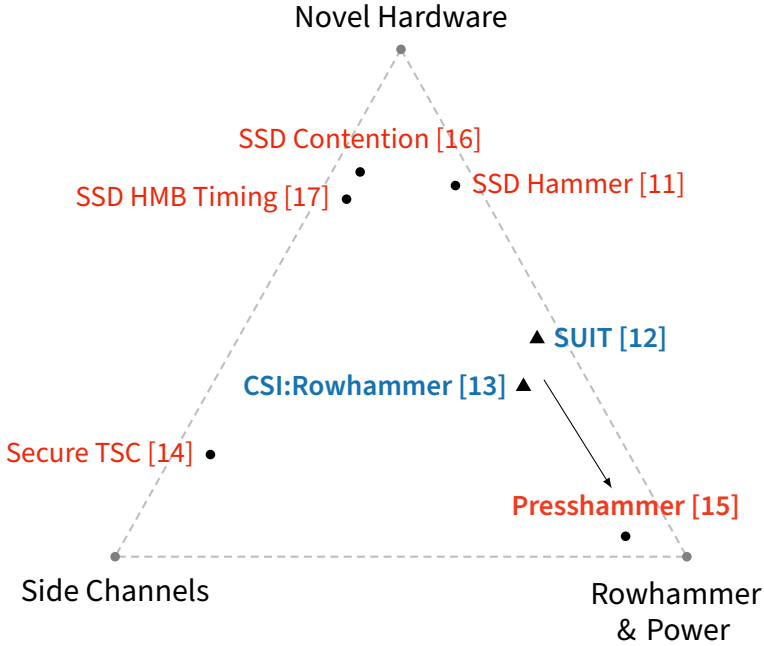
Frequency Change Delay



SUIT – Results




Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer & Power


Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer
& Power

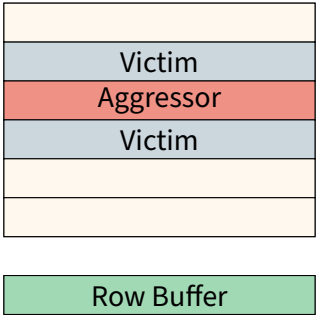
Presshammer

Rowhammer and Rowpress without Physical Address Information

Jonas Juffinger, Sudheendra Raghav Neela, Martin Heckel, Lukas Schwarz,
Florian Adamsky, Daniel Gruss

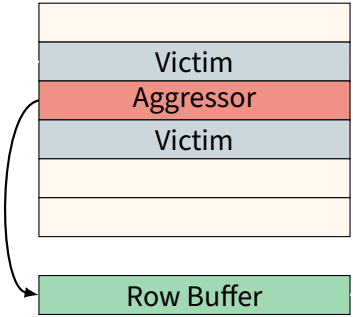
DIMVA, 2024

Single-Sided RowPress [21]



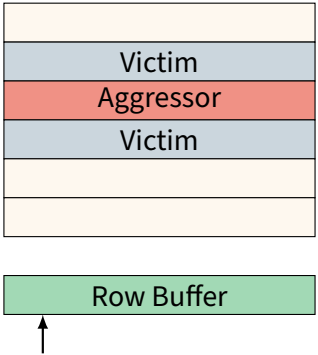
Keep one row open as long as possible.

Single-Sided RowPress [21]



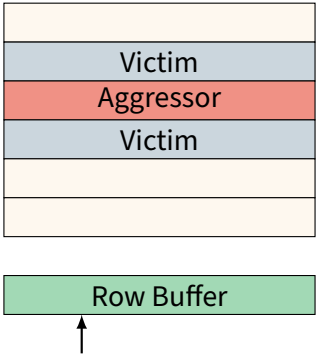
Keep one row open as long as possible.

Single-Sided RowPress [21]



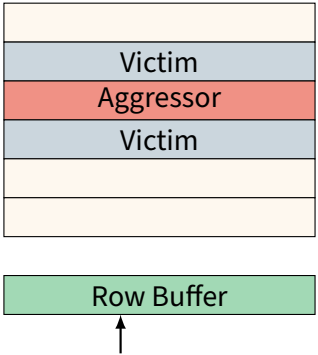
Keep one row open as long as possible.

Single-Sided RowPress [21]



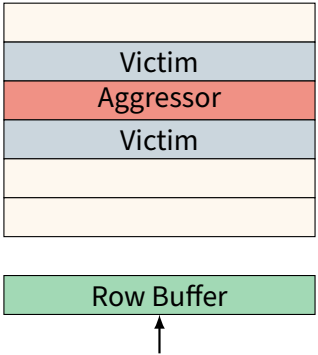
Keep one row open as long as possible.

Single-Sided RowPress [21]



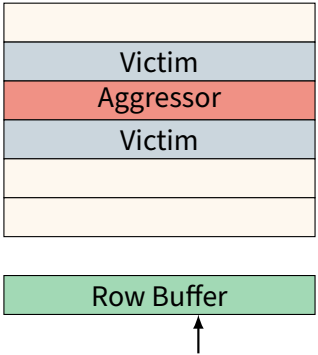
Keep one row open as long as possible.

Single-Sided RowPress [21]



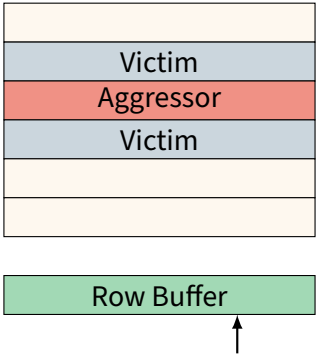
Keep one row open as long as possible.

Single-Sided RowPress [21]



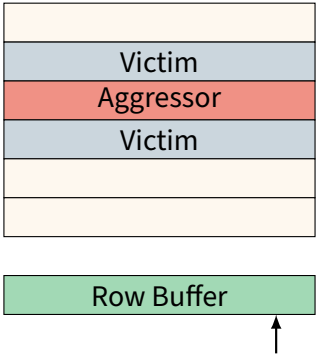
Keep one row open as long as possible.

Single-Sided RowPress [21]



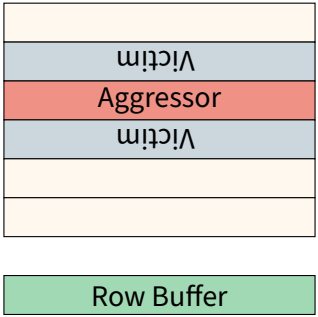
Keep one row open as long as possible.

Single-Sided RowPress [21]



Keep one row open as long as possible.

Single-Sided RowPress [21]



Keep one row open as long as possible.

Another Flip...

Wait...

Another Flip...

There is this paper from 2018...

Another Flip in the Wall of Rowhammer Defenses

Daniel Gruss[1], Moritz Lipp[1], Michael Schwarz[1], Daniel Genkin[2],
Jonas Juffinger[1], Sioli O'Connell[3], Wolfgang Schoechl[1], and Yuval Yarom[3,4]
[1] Graz University of Technology
[2] University of Pennsylvania and University of Maryland
[3] University of Adelaide
[4] Data61

***Abstract*—The Rowhammer bug allows unauthorized modification of bits in DRAM cells from unprivileged software, enabling powerful privilege-escalation attacks. Sophisticated Rowhammer countermeasures have been presented, aiming at mitigating the Rowhammer bug or its exploitation. However, the state of the art provides insufficient insight on the completeness of these defenses.**

In this paper, we present novel Rowhammer attack and exploitation primitives, showing that even a combination of all defenses is ineffective. Our new attack technique, *one-location hammering*, breaks previous assumptions on requirements for triggering the Rowhammer bug, i.e., we do not hammer multiple DRAM rows but only keep one DRAM row constantly open. Our new exploitation technique, *opcode flipping*, bypasses recent isolation mechanisms by flipping bits in a predictable and targeted way in userspace binaries. We replace conspicuous and memory-exhausting spraying and grooming techniques with a novel reliable technique called *memory waylaying*. Memory

Software-based mitigations, which can be implemented on commodity systems, have also been proposed. These include ad-hoc defense techniques such as doubling the RAM refresh rates [44], removing unprivileged access to the `pagemap` interface [45, 62, 65], and prohibiting the `clflush` instruction [65]. However, recent works have already bypassed these countermeasures [6, 24, 68]. Other ad-hoc attempts, such as disabling page deduplication by default [52, 60], only prevent specific Rowhammer attacks exploiting these features [11, 59], but not all Rowhammer attacks.

The research community proposed sophisticated defenses which seemingly have solved the Rowhammer problem. Based on the underlying primitives of these defenses, we introduce a new systematic categorization into five defense classes:

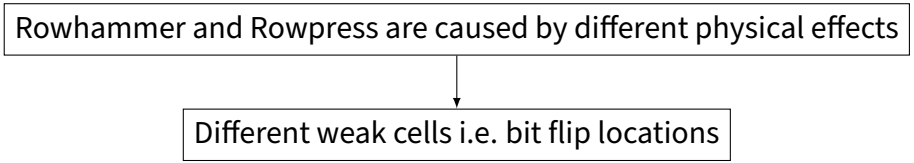
Is One-Location Rowhammer = RowPress?

Presshammer – Experiment

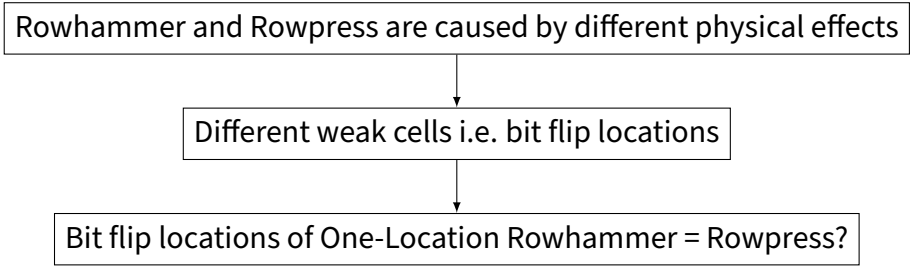
Presshammer – Experiment

Rowhammer and Rowpress are caused by different physical effects

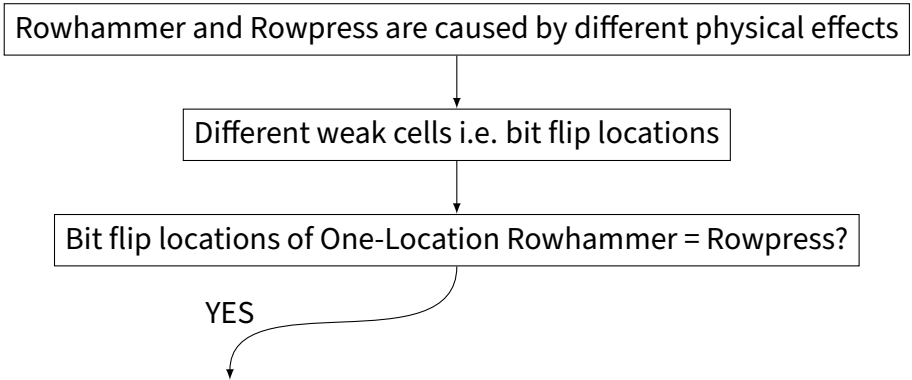
Presshammer – Experiment



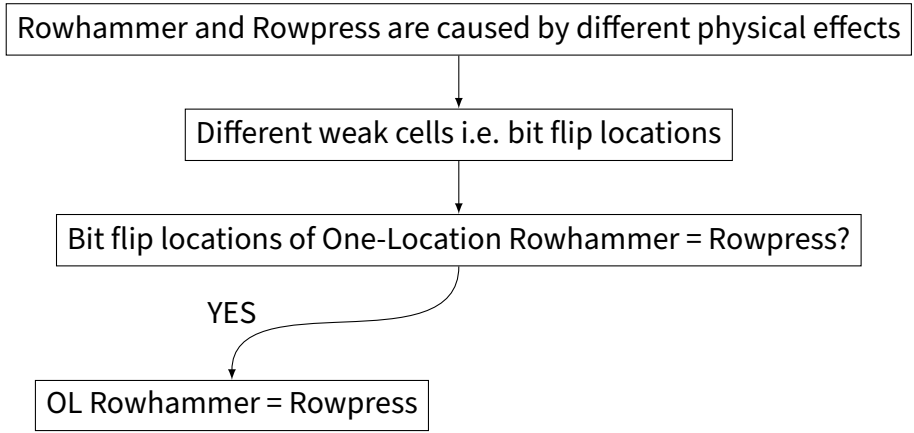
Presshammer – Experiment



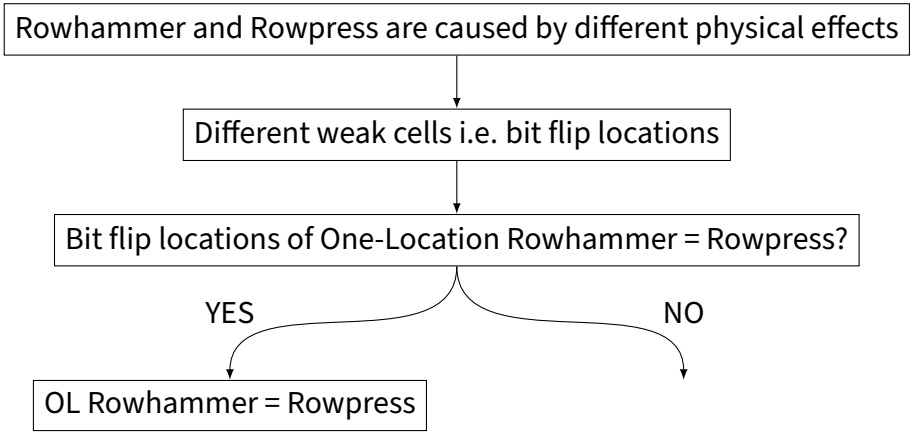
Presshammer – Experiment



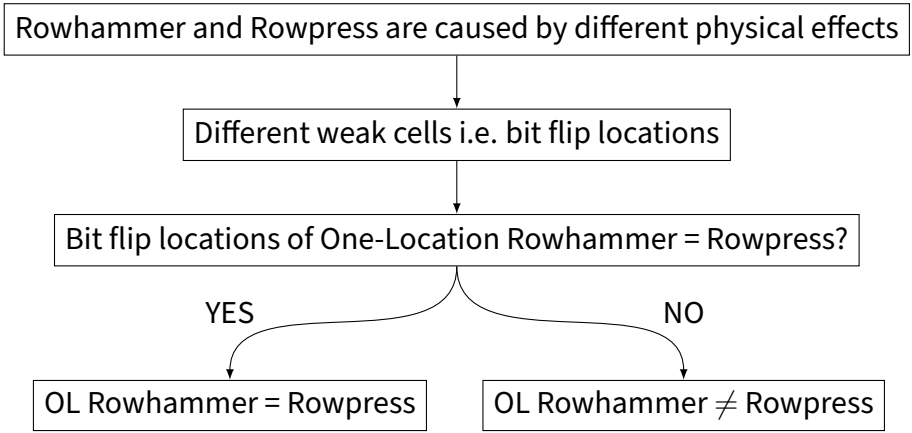
Presshammer – Experiment



Presshammer – Experiment



Presshammer – Experiment

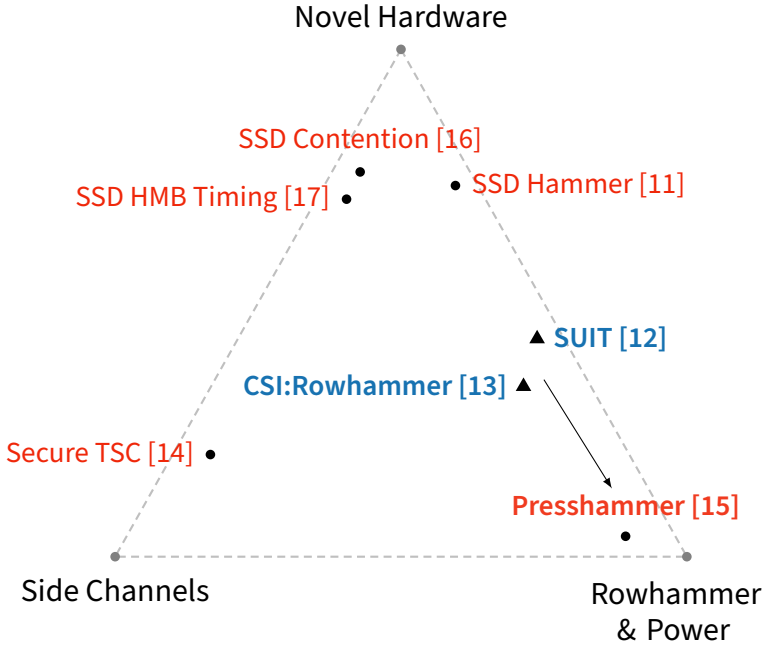


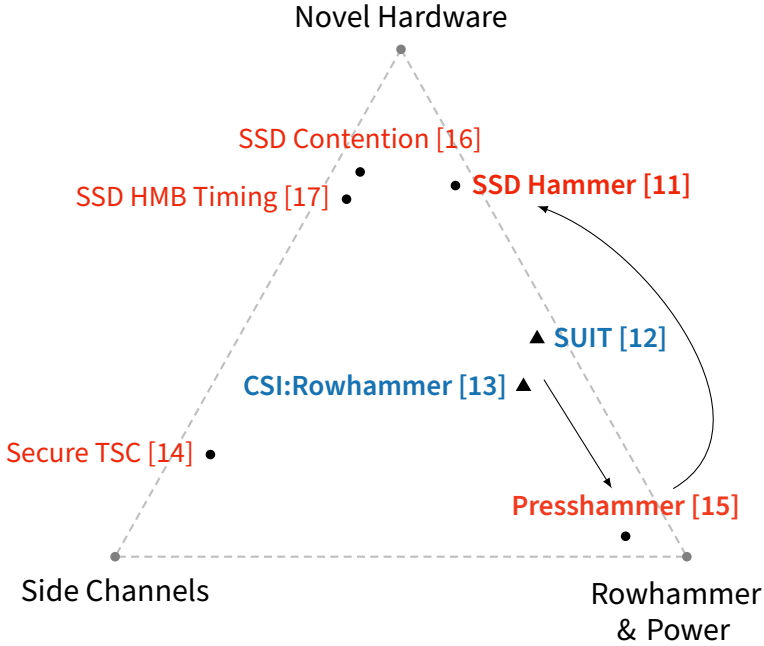
Presshammer – The Matrix

	RH		RP	
	DS	OL	DS	OL
Rowhammer (RH) double sided (DS)				
Rowhammer (RH) one location (OL)				
Rowpress (RP) double sided (DS)				
Rowpress (RP) one location (OL)				

Presshammer – The Matrix ... Is Inconclusive

		RH		RP	
		DS	OL	DS	OL
Rowhammer (RH)	double sided (DS)	100	56.5	13.7	1.0
	one location (OL)	61.8	100	14.5	1.1
Rowpress (RP)	double sided (DS)	98.1	95.3	100	1.0
	one location (OL)	96.3	98.8	81.4	100

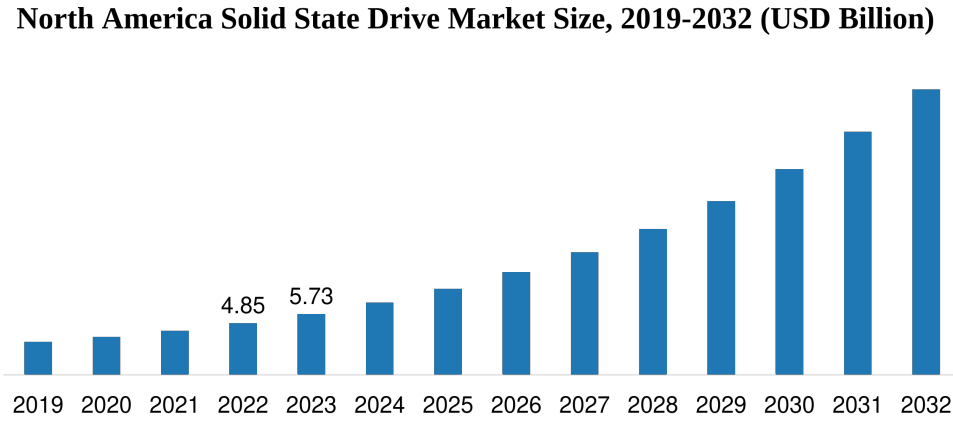

Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer
& Power


Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer
& Power

Solid State Drives

Research on solid state drives is **sparse**.

Solid State Drives



[1]

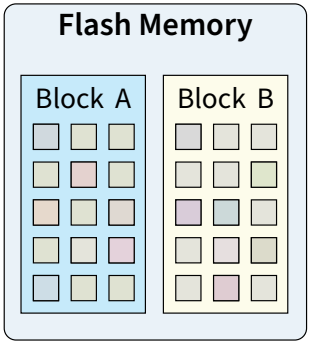
An Analysis of HMB-based SSD Rowhammer

Jonas Juffinger

uASC, 2025

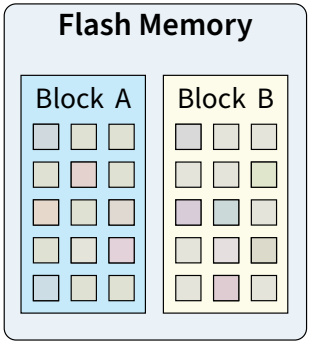
SSD Background

Flash Translation Layer (FTL)

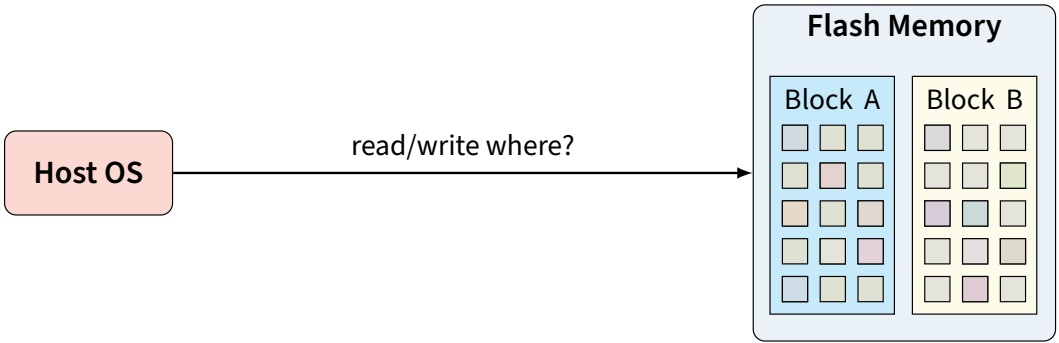


Flash Translation Layer (FTL)

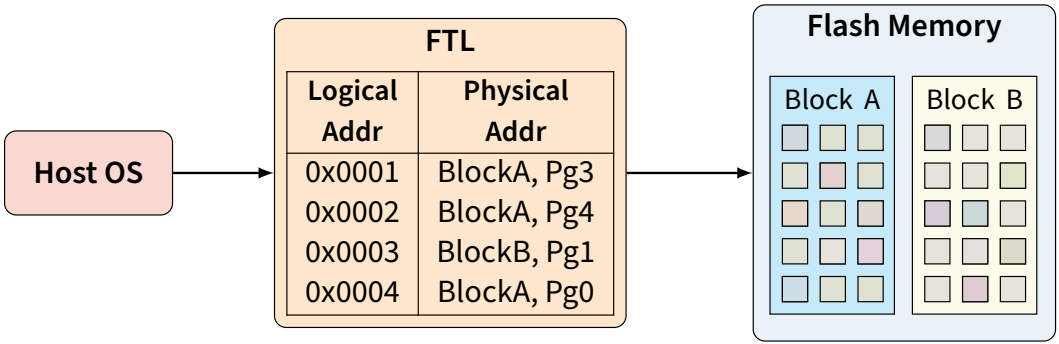
Host OS



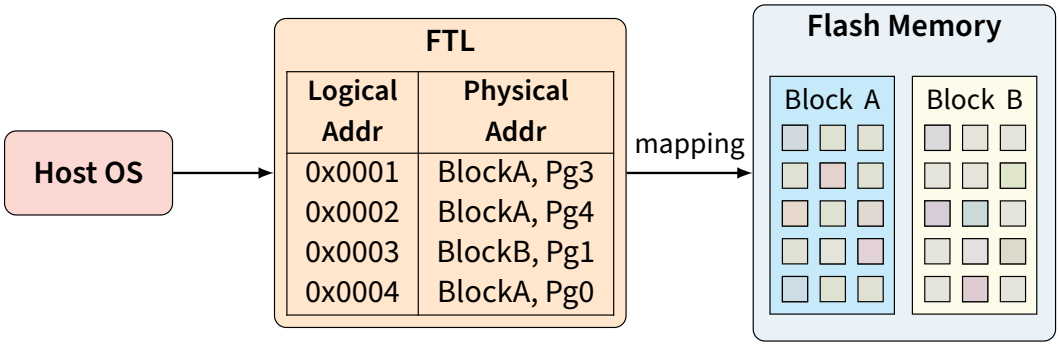
Flash Translation Layer (FTL)



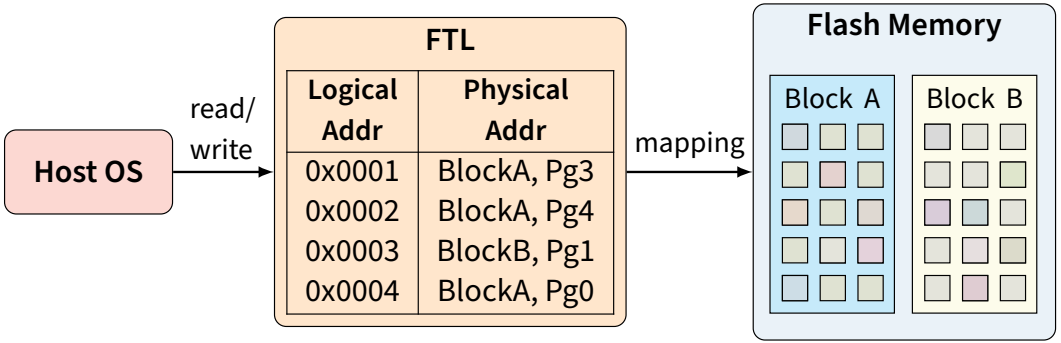
Flash Translation Layer (FTL)



Flash Translation Layer (FTL)



Flash Translation Layer (FTL)



Flash Translation Layer (FTL)

FTL

Logical Addr	Physical Addr
0x0001	BlockA, Pg3
0x0002	BlockA, Pg4
0x0003	BlockB, Pg1
0x0004	BlockA, Pg0

Flash Translation Layer (FTL)

FTL

Logical Addr	Physical Addr
0x0001	BlockA, Pg3
0x0002	BlockA, Pg4
0x0003	BlockB, Pg1
0x0004	BlockA, Pg0

- Required on each access

Flash Translation Layer (FTL)

FTL

Logical Addr	Physical Addr
0x0001	BlockA, Pg3
0x0002	BlockA, Pg4
0x0003	BlockB, Pg1
0x0004	BlockA, Pg0

- Required on each access
- Stored in flash memory

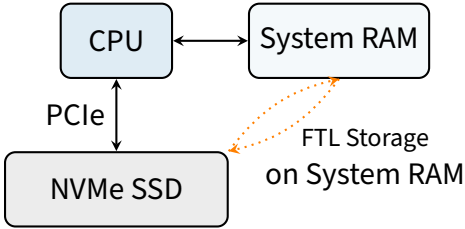
Flash Translation Layer (FTL)

FTL

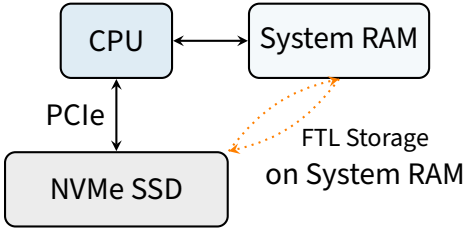
Logical Addr	Physical Addr
0x0001	BlockA, Pg3
0x0002	BlockA, Pg4
0x0003	BlockB, Pg1
0x0004	BlockA, Pg0

- Required on each access
- Stored in flash memory
- Cache

Host-Memory Buffer (HMB)

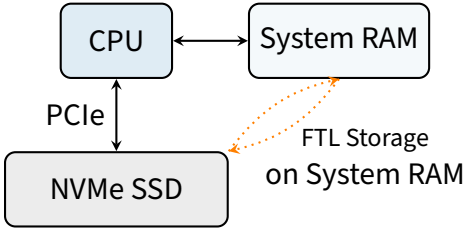


Host-Memory Buffer (HMB)



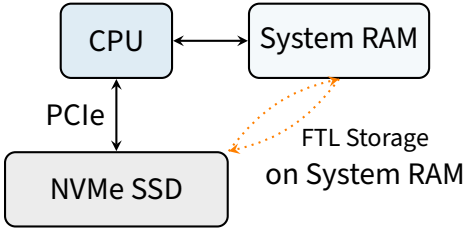
- Request memory from OS

Host-Memory Buffer (HMB)



- Request memory from OS
- Exclusive DMA access

Host-Memory Buffer (HMB)



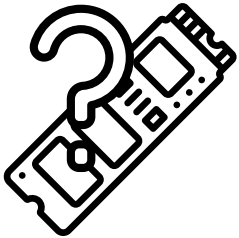
- Request memory from OS
- Exclusive DMA access
- Usage is undocumented

SSD Rowhammer?

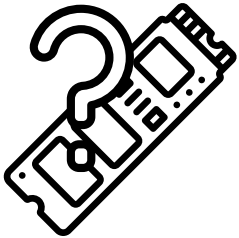
The SSD Uses the Main DRAM.

What About Rowhammer?

Research Questions

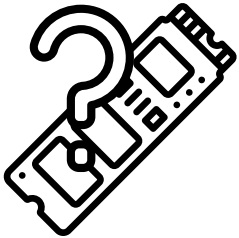


Research Questions



- What happens if bits flip in the HMB?

Research Questions



- What happens if bits flip in the HMB?
- Can we make the SSD hammer the HMB?

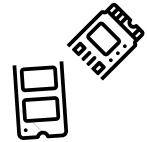
Bit Flips in The HMB

Bit Flips in The HMB

All SSDs Freeze

Bit Flips in The HMB

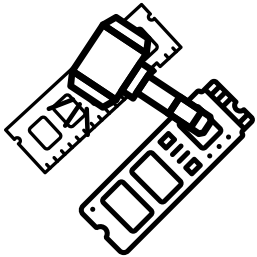
All SSDs Freeze



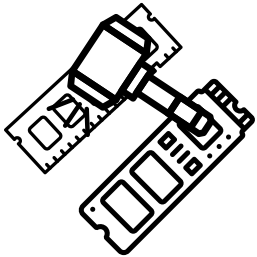
One SSD Broke

Can an SSD Hammer the Main Memory?

HMB Rowhammer

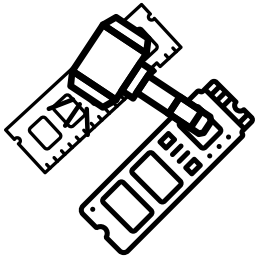


HMB Rowhammer



- Generate **high frequency** HMB accesses

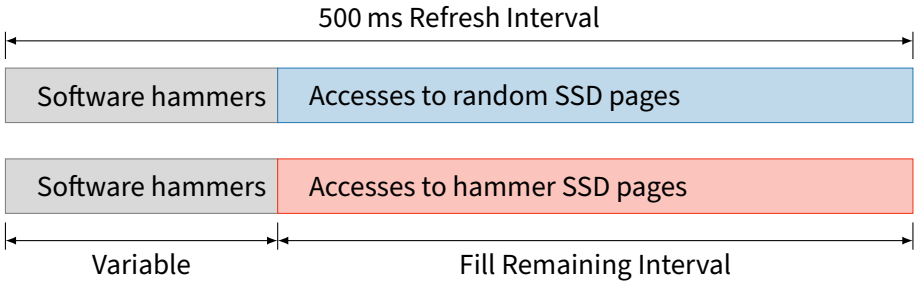
HMB Rowhammer



- Generate **high frequency** HMB accesses
- $78000\ \text{IOPS} \cdot 64\ \text{ms} = 4992$ Hammer Accesses

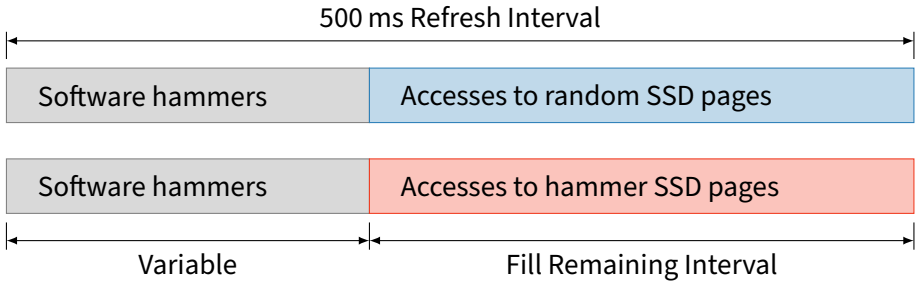
Combined Rowhammer

When combining them with DRAM access from software



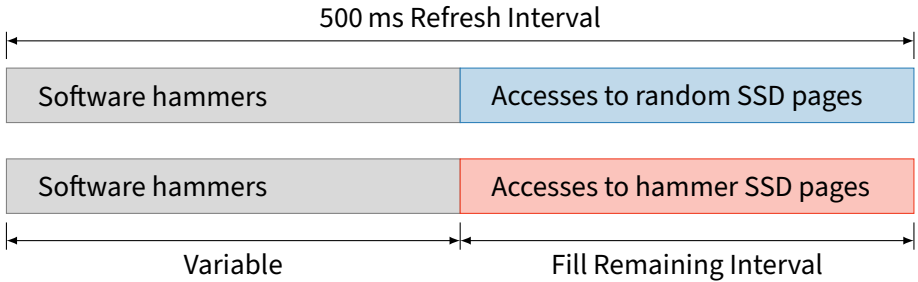
Combined Rowhammer

When combining them with DRAM access from software

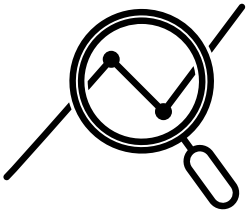


Combined Rowhammer

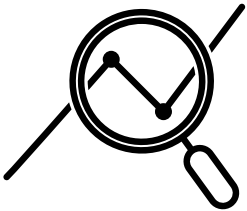
When combining them with DRAM access from software



Combined Rowhammer – Results

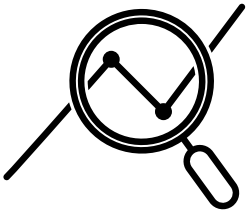


Combined Rowhammer – Results



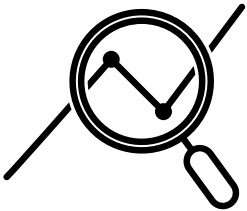
- 9 555 bit flips with random SSD accesses

Combined Rowhammer – Results

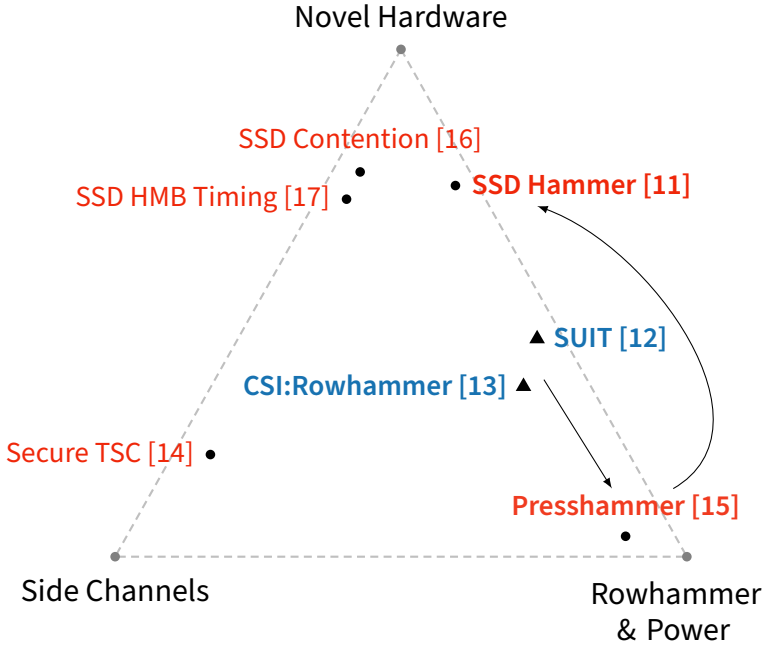


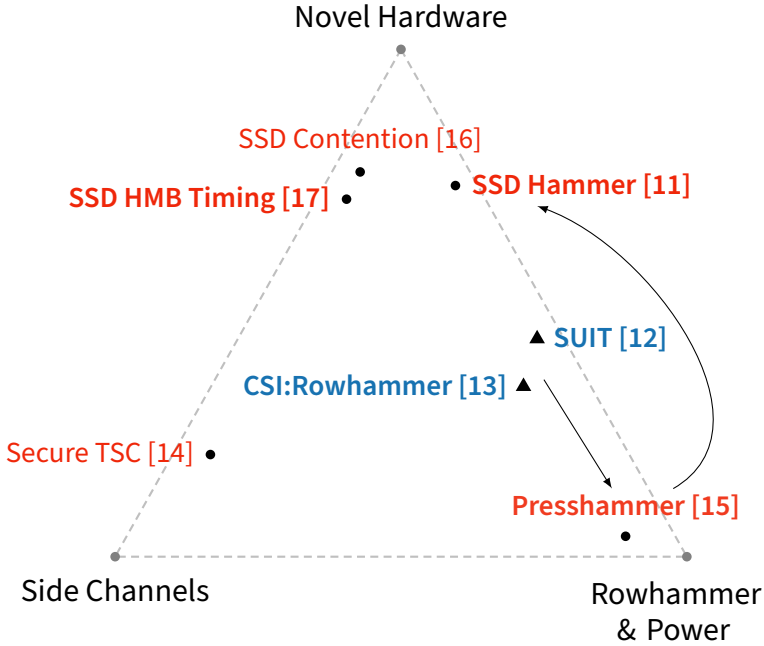
- 9 555 bit flips with random SSD accesses
- 9 877 bit flips with hammer SSD accesses

Combined Rowhammer – Results



- 9 555 bit flips with random SSD accesses
- 9 877 bit flips with hammer SSD accesses
- +3.4 %


Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer
& Power


Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer
& Power

The HMB Timing Side Channel:

Exploiting the SSD's Host Memory Buffer

Jonas Juffinger, Hannes Weissteiner, Thomas Steinbauer, Daniel Gruss

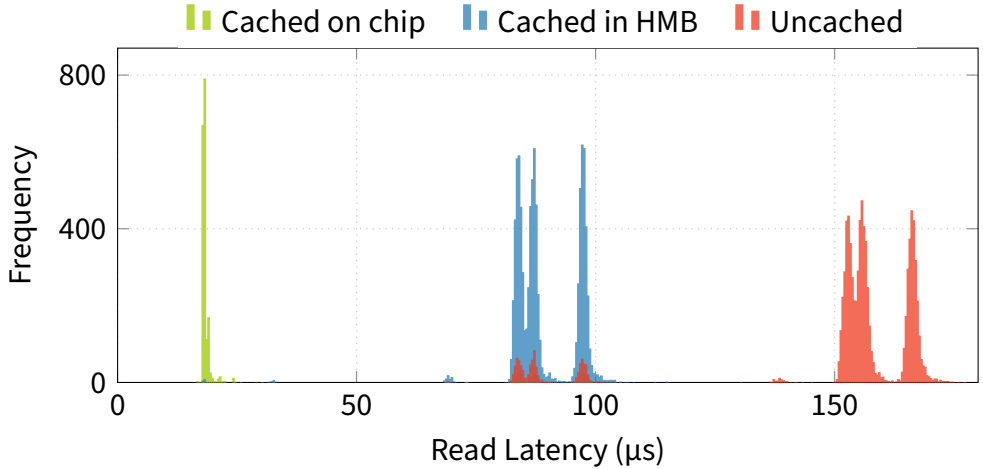
DIMVA, 2025

The HMB is a cache

The HMB is a cache $\rightarrow$ Is there a **timing side channel**?

Yes!

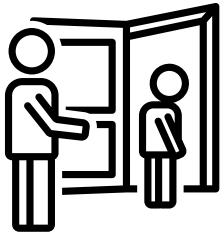
The HMB Timing Side Channel



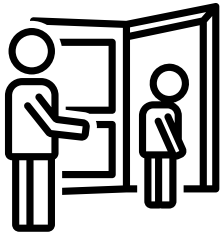
The HMB Timing Side Channel

Detect if an SSD page was recently accessed.

HMB Timing Side Channel – Cache Eviction

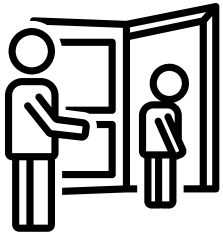


HMB Timing Side Channel – Cache Eviction



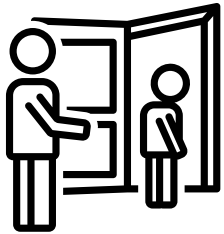
- $\approx$ 11 ms on the Lexar NM790

HMB Timing Side Channel – Cache Eviction



- $\approx$ 11 ms on the Lexar NM790
- $\approx$ 22 ms on the Samsung 990 EVO

HMB Timing Side Channel – Cache Eviction



- $\approx$ 11 ms on the Lexar NM790
- $\approx$ 22 ms on the Samsung 990 EVO
- Faster than page cache eviction (>150 ms)

HMB Timing Side Channel – Covert Channels

HMB Timing Side Channel – Covert Channels

- Up to 8.8 kbit/s between processes

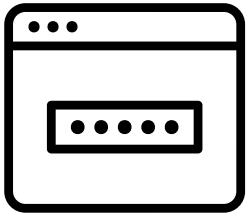
HMB Timing Side Channel – Covert Channels

- Up to 8.8 kbit/s between processes
- Between virtual machines

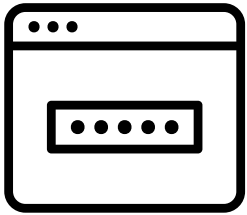
HMB Timing Side Channel – Covert Channels

- Up to 8.8 kbit/s between processes
- Between virtual machines
- Over the network by exploiting nginx as a confused deputy

HMB Timing Side Channel – UI Redress Attack

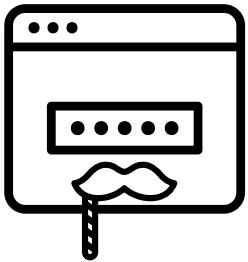


HMB Timing Side Channel – UI Redress Attack



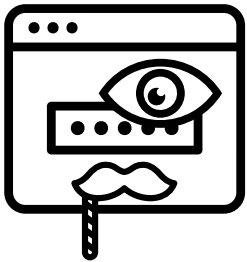
- Revive mitigated page cache attacks

HMB Timing Side Channel – UI Redress Attack



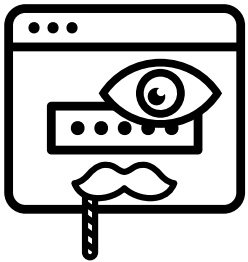
- Revive mitigated page cache attacks
- Detect when a program is started

HMB Timing Side Channel – UI Redress Attack

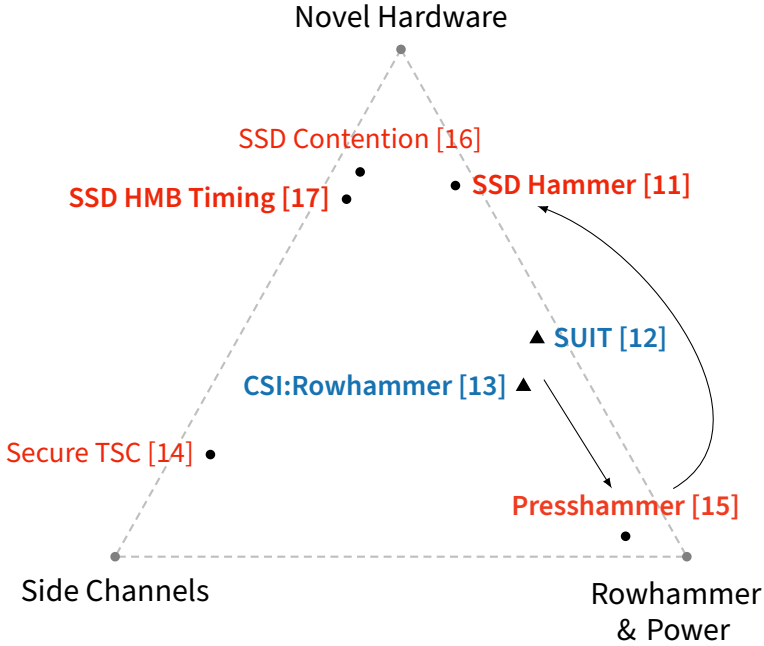


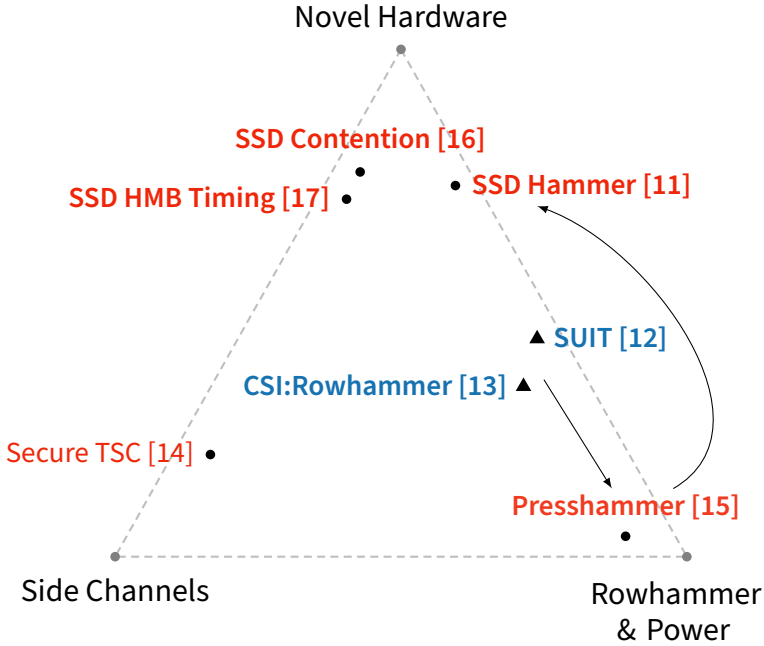
- Revive mitigated page cache attacks
- Detect when a program is started
- Draw fake window above

HMB Timing Side Channel – UI Redress Attack



- Revive mitigated page cache attacks
- Detect when a program is started
- Draw fake window above
- Steal password


Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer
& Power


Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer
& Power

Secret Spilling Drive:

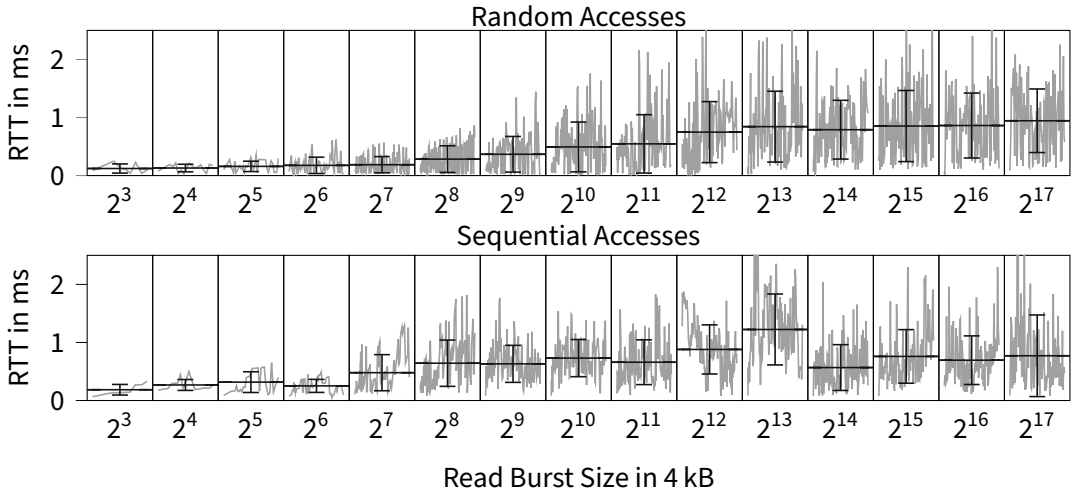
Leaking User Behavior through SSD Contention

Jonas Juffinger, Fabian Rauscher, Giuseppe La Manna, Daniel Gruss

NDSS, 2025

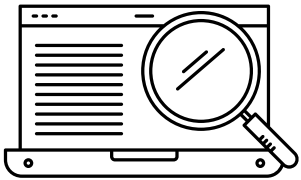
What about SSD contention?

SSD Contention



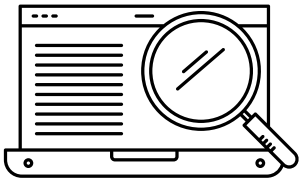
SSD	Model Name	Size	DRAM Cache	PCIe
$\mathcal{A}$	Samsung 980 Pro	256 GB	512 MB LPDDR4	4.0
$\mathcal{B}$	Samsung 980	1 TB	64 MB HMB	3.0
$\mathcal{C}$	Samsung 970 Evo	1 TB	–	3.0
$\mathcal{D}$	Samsung MZVL21T0HCLR-00BL7	1 TB	1 GB LPDDR4	4.0
$\mathcal{E}$	Samsung 970 Evo Plus	2 TB	–	3.0
$\mathcal{F}$	Crucial P5	1 TB	512 MB LPDDR4	4.0
$\mathcal{G}$	Crucial P5 Plus	500 GB	1 GB LPDDR4	4.0
$\mathcal{H}$	Kingston SA2000M81000G	1 TB	1 GB DDR3L	3.0
$\mathcal{I}$	Toshiba KXG6AZNV1T02	1 TB	–	3.0
$\mathcal{J}$	ADATA XPG Gammix S50 Lite	512 GB	512 MB DDR4	4.0
$\mathcal{K}$	Gigabyte Aorus Gen4	500 GB	512 MB DDR4	4.0
$\mathcal{L}$	Western Digital Blue SN550	1 TB	64 MB HMB	3.0

Website Fingerprinting



Identify websites currently opened on the same machine.

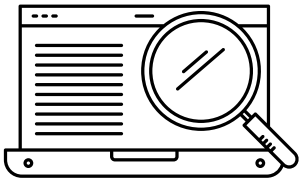
Website Fingerprinting



Identify websites currently opened on the same machine.

- Web browsers cache assets on the disk

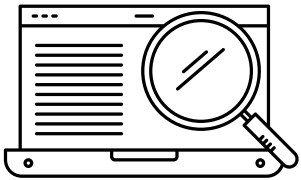
Website Fingerprinting



Identify websites currently opened on the same machine.

- Web browsers cache assets on the disk
- They are read from the disk on each load

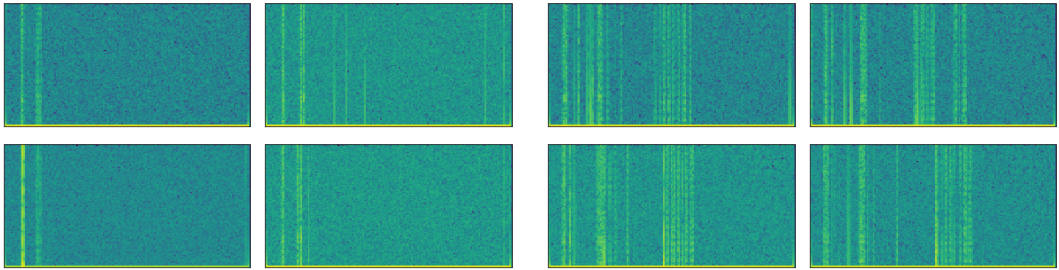
Website Fingerprinting



Identify websites currently opened on the same machine.

- Web browsers cache assets on the disk
- They are read from the disk on each load
- Create a unique fingerprint

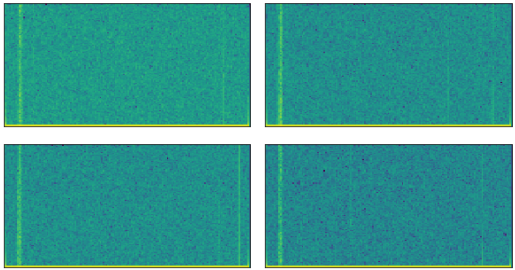
Website Spectrograms



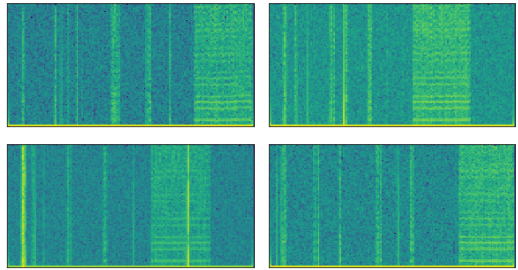
(a) google.com

(b) youtube.com

Website Spectrograms

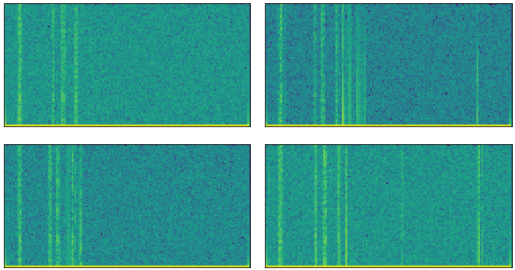


(c) facebook.com

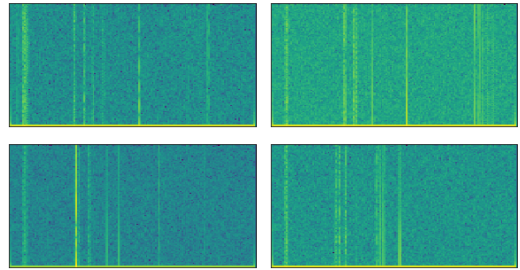


(d) qq.com

Website Spectrograms

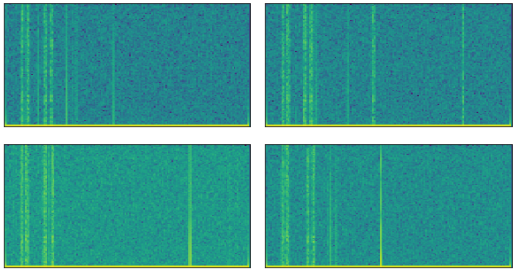


(e) xhamster.com

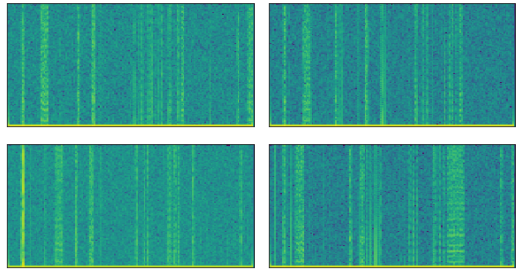


(f) imdb.com

Website Spectrograms

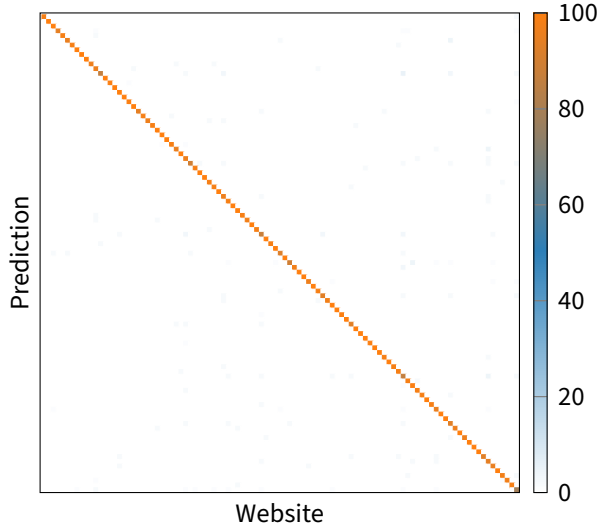


(g) force.com



(h) dropbox.com

Website Fingerprinting - Results

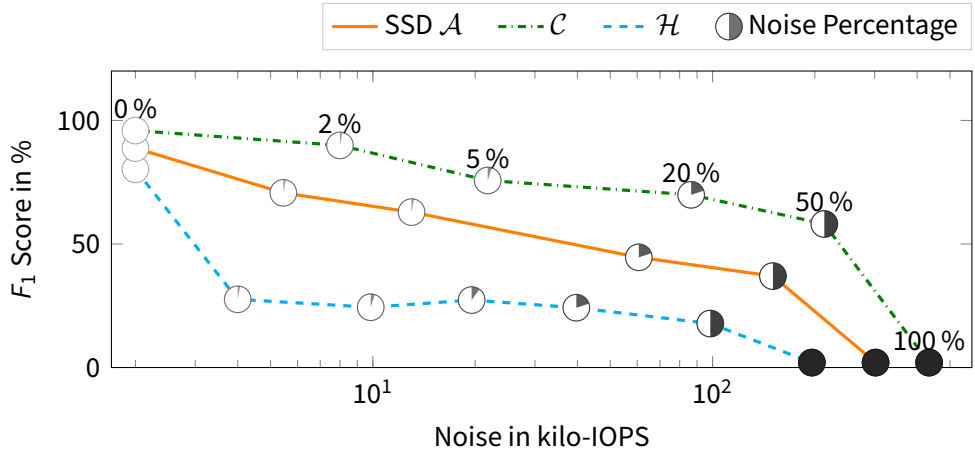


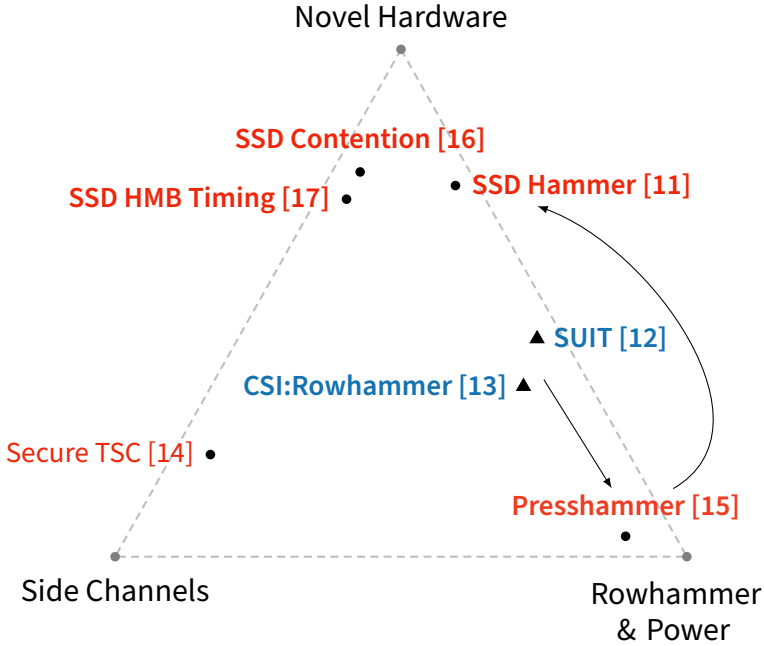
Website Fingerprinting - Results

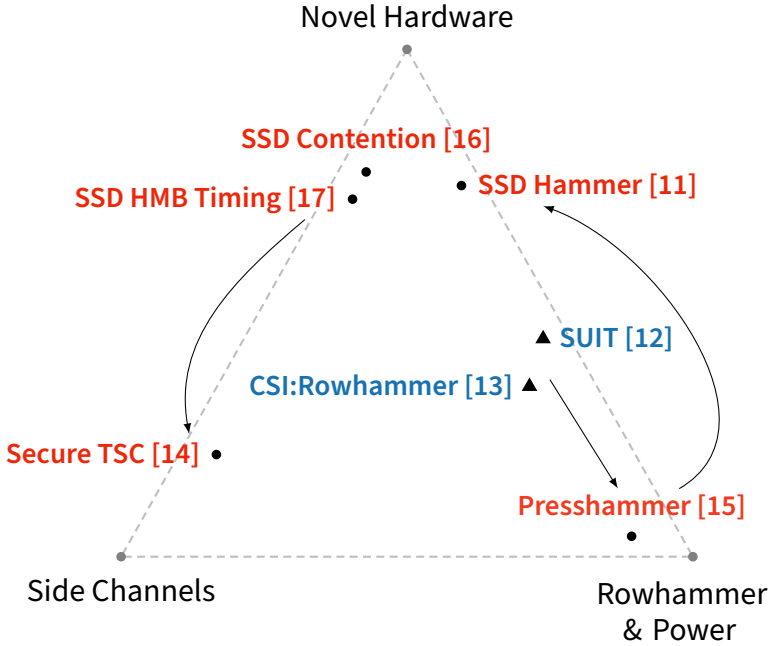
100 Websites + Open World Dataset

SSD	DRAM Cache	PCIe	Accuracy ↓
Crucial P5	✓	4.0	97.0 %
Gigabyte Aorus Gen4	✓	4.0	97.0 %
Samsung 970 Evo Plus	✗	3.0	96.6 %
	...		
ADATA XPG Gammix S50 Lite	✓	4.0	88.7 %
Kingston SA2000M81000G	✓	3.0	80.2 %

Noise Impact




Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer
& Power

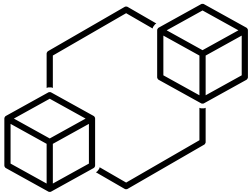

Novel Hardware
SSD Contention [16]
SSD HMB Timing [17]
SSD Hammer [11]
SUIT [12]
CSI:Rowhammer [13]
Secure TSC [14]
Presshammer [15]
Side Channels
Rowhammer
& Power

Not So Secure TSC

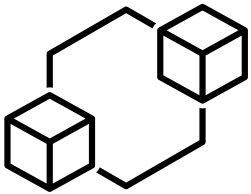
Jonas Juffinger, Sudheendra Raghav Neela, Daniel Gruss

ACNS, 2025

Virtual Machine Co-Location

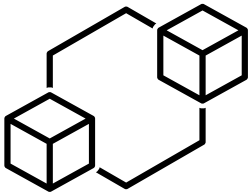


Virtual Machine Co-Location



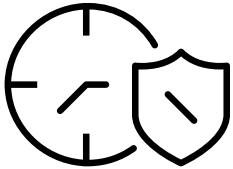
- Two virtual machines on same physical machine

Virtual Machine Co-Location

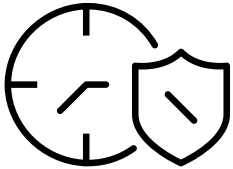


- Two virtual machines on same physical machine
- Required many for side-channel attacks

Secure TSC

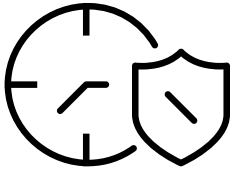


Secure TSC



- Trusted time stamp counter

Secure TSC

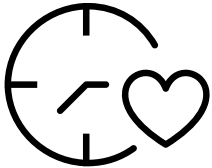


- Trusted time stamp counter
- Cannot be manipulate by host

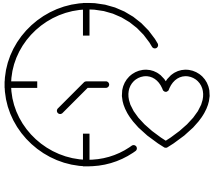
Secure TSC values leaks the boot time.

Same boot time $\rightarrow$ **Same** machine.

TsCupid

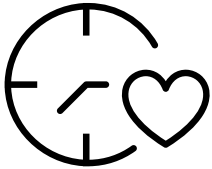


TsCupid



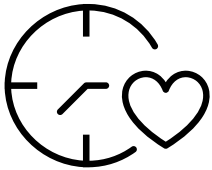
- Central service collects Secure TSC values

TsCupid



- Central service collects Secure TSC values
- Finds co-located virtual machines

TsCupid



- Central service collects Secure TSC values
- Finds co-located virtual machines
- **In less than** 130 **ms**

Conclusions

Rowhammer Needs **Principled** Mitigations.

Principled Mitigations Can Be **Inexpensive**

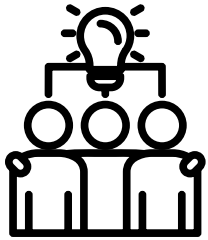
Principled Mitigations Can Be **Inexpensive**

... and even increase efficiency.

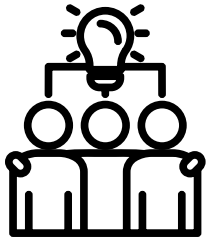
Not considering side channels in the design phase leaves new hardware vulnerable.

My PhD Journey

My PhD Journey

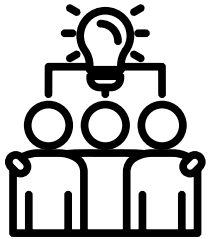


My PhD Journey



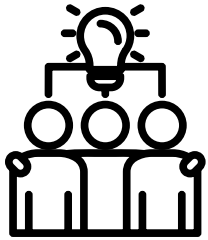
- Took almost exactly 4 years

My PhD Journey



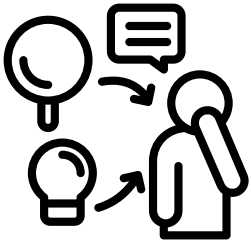
- Took almost exactly 4 years
- Traveled to 15 conferences in 7 countries

My PhD Journey

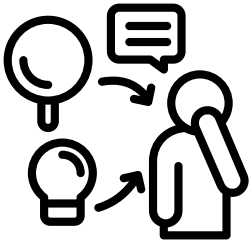


- Took almost exactly 4 years
- Traveled to 15 conferences in 7 countries
- Met many amazing people

Publications

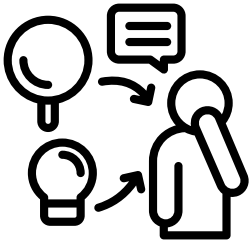


Publications



- 19 peer-reviewed publications

Publications



- 19 peer-reviewed publications
- 9 at A* conferences

Teaching & Talks

Teaching & Talks

- Information Security Practicals

Teaching & Talks

- Information Security Practicals
- Cloud Operating Systems

Teaching & Talks

- Information Security Practicals
- Cloud Operating Systems
- Side-Channel Security

Teaching & Talks

- Information Security Practicals
- Cloud Operating Systems
- Side-Channel Security

- 14 conference talks

Teaching & Talks

- Information Security Practicals
- Cloud Operating Systems
- Side-Channel Security

- 14 conference talks
- 1 sitcom

Any Questions?

Bibliography I

[1] Fortune Business Insights. **Solid State Drive Market Size, Share & Industry Trends Analysis**. 2025. URL: https://www.fortunebusinessinsights.com/solid-state-drive-market-109839.

[2] P. Frigo, E. Vannacci, H. Hassan, V. van der Veen, O. Mutlu, C. Giuffrida, H. Bos, and K. Razavi. **TRRespass: Exploiting the Many Sides of Target Row Refresh**. S&P. 2020.

[3] S. Gast, R. Czerny, J. Juffinger, F. Rauscher, S. Franza, and D. Gruss. **SnailLoad: Exploiting Remote Network Latency Measurements without JavaScript**. USENIX Security. 2024.

[4] S. Gast, S. D. Felix, A. Steinmaurer, J. **Juffinger**, and D. Gruss. **Real-World Study of the Security of Educational Test Systems**. Workshop on Operating Systems and Virtualization Security. 2025.

[5] S. Gast, J. Juffinger, L. Maar, C. Royer, A. Kogler, and D. Gruss. **Remote Scheduler Contention Attacks**. FC. 2024.

[6] S. Gast, J. Juffinger, M. Schwarzl, G. Saileshwar, A. Kogler, S. Franza, M. Köstl, and D. Gruss. **SQUIP: Exploiting the Scheduler Queue Contention Side Channel**. S&P. 2023.

Bibliography II

[7] L. Giner, R. Czerny, S. Lammer, A. Giner, P. Gollob, J. Juffiger, and D. Gruss. **Fast and Efficient Secure L1 Caches for SMT**. ARES. 2025.

[8] D. Gruss, M. Lipp, M. Schwarz, D. Genkin, J. Juffinger, S. O'Connell, W. Schoechl, and Y. Yarom. **Another Flip in the Wall of Rowhammer Defenses**. S&P. 2018.

[9] P. Jattke, M. Marazzi, F. Solt, M. Wipfli, and S. G. K. Razavi. **MCSEE: Evaluating Advanced Rowhammer Attacks and Defenses via Automated DRAM Traffic Analysis**. Usenix Security. 2025.

[10] P. Jattke, V. van der Veen, P. Frigo, S. Gunter, and K. Razavi. **BLACKSMITH: Rowhammering in the Frequency Domain**. S&P. 2021.

[11] J. Juffinger. **An Analysis of HMB-based SSD Rowhammer**. uASC. 2025.

[12] J. Juffinger, S. Kalinin, D. Gruss, and F. Mueller. **SUIT: Secure Undervolting with Instruction Traps**. ASPLOS. 2024.

[13] J. Juffinger, L. Lamster, A. Kogler, M. Eichlseder, M. Lipp, and D. Gruss. **CSI: Rowhammer - Cryptographic Security and Integrity against Rowhammer**. S&P. 2023.

Bibliography III

[14] J. Juffinger, S. R. Neela, and D. Gruss. **Not So Secure TSC**. ACNS. 2025.

[15] J. Juffinger, S. R. Neela, M. Heckel, L. Schwarz, F. Adamsky, and D. Gruss. **Presshammer: Rowhammer and Rowpress without Physical Address Information**. DIMVA. 2024.

[16] J. Juffinger, F. Rauscher, G. La Manna, and D. Gruss. **Secret Spilling Drive: Leaking User Behavior through SSD Contention**. NDSS. 2025.

[17] J. Juffinger, H. Weissteiner, T. Steinbauer, and D. Gruss. **The HMB Timing Side Channel: Exploiting the SSD's Host Memory Buffer**. DIMVA. 2025.

[18] Y. Kim, R. Daly, J. Kim, C. Fallin, J. H. Lee, D. Lee, C. Wilkerson, K. Lai, and O. Mutlu. **Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors**. ISCA. 2014.

[19] A. Kogler, J. Juffinger, L. Giner, L. Gerlach, M. Schwarzl, M. Schwarz, D. Gruss, and S. Mangard. **Collide+Power: Leaking Inaccessible Data with Software-based Power Side Channels**. USENIX Security. 2023.

Bibliography IV

[20] A. Kogler, J. Juffinger, S. Qazi, Y. Kim, M. Lipp, N. Boichat, E. Shiu, M. Nissler, and D. Gruss. **Half-Double: Hammering From the Next Row Over**. USENIX Security. 2022.

[21] H. Luo, A. Olgun, A. G. Yağlıkçı, Y. C. Tuğrul, S. Rhyner, M. B. Cavlak, J. Lindegger, M. Sadrosadati, and O. Mutlu. **RowPress: Amplifying Read Disturbance in Modern DRAM Chips**. ISCA. 2023.

[22] L. Maar, J. Juffinger, T. Steinbauer, D. Gruss, and S. Mangard. **KernelSnitch: Side-Channel Attacks on Kernel Data Structures**. NDSS. 2025.

[23] K. Murdock, D. Oswald, F. D. Garcia, J. Van Bulck, D. Gruss, and F. Piessens. **Plundervolt: Software-based Fault Injection Attacks against Intel SGX**. S&P. 2020.

[24] F. Rauscher, A. Kogler, J. Juffinger, and D. Gruss. **IdleLeak: Exploiting Idle State Side Effects for Information Leakage**. NDSS. 2024.

[25] A. Saxena, G. Saileshwar, J. Juffinger, A. Kogler, D. Gruss, and M. Qureshi. **PT-Guard: Integrity-Protected Page Tables to Defend Against Breakthrough Rowhammer Attacks**. DSN. 2023.

Bibliography V

[26] H. Weissteiner, F. Rauscher, R. L. Schröder, J. Juffinger, S. Gast, J. Wichelmann, T. Eisenbarth, and D. Gruss. **TEEcorrelate: An Information-Preserving Defense against Performance Counter Attacks on TEEs**. USENIX Security. 2025.