Let's Get Physical:

Low-Cost Memory Interposer Attacks and the Future of Confidential Computing

Jo Van Bulck

DistriNet, KU Leuven, Belgium jo.vanbulck@cs.kuleuven.be vanbulck.net

9th Workshop on System Software for Trusted Execution

(SysTEX 2026) - April 27, 2026

DistriNet

KU LEUVEN

The Future of Confidential Computing?

*"Confidential Computing is the **protection of data in use** by performing computation in a hardware-based, attested Trusted Execution Environment."*

*"Confidential computing enables **new public cloud scenarios** (e.g., migrating extremely sensitive data to the cloud [...]"*

CONFIDENTIAL COMPUTING CONSORTIUM

https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC_Overview.pdf

The Rise of Confidential Cloud Computing

DARKREADING

Cloud Providers Throw Their Weight Behind Confidential Computing

New technologies designed into processors allow enterprises to leverage cloud advantages while meeting privacy regulations.

https://www.darkreading.com/cloud-security/cloud-providers-are-putting-more-weight-in-confidential-computing

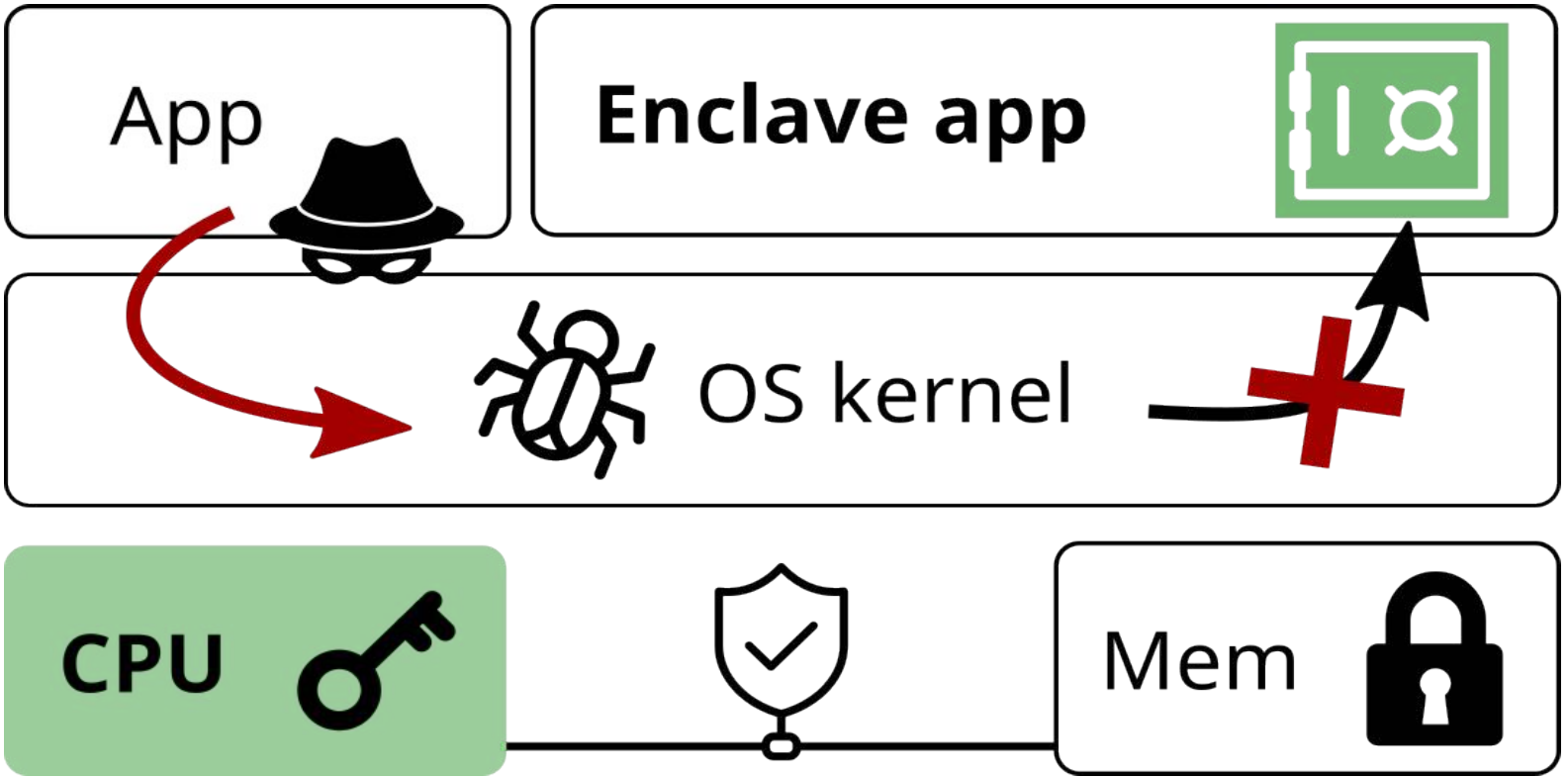
Confidential Computing Today, Computing Tomorrow

*In the near future, "confidential computing" will just be "computing." **

* Mark Russinovich, CTO
Microsoft Azure

Confidential Computing: The Weakest Link?

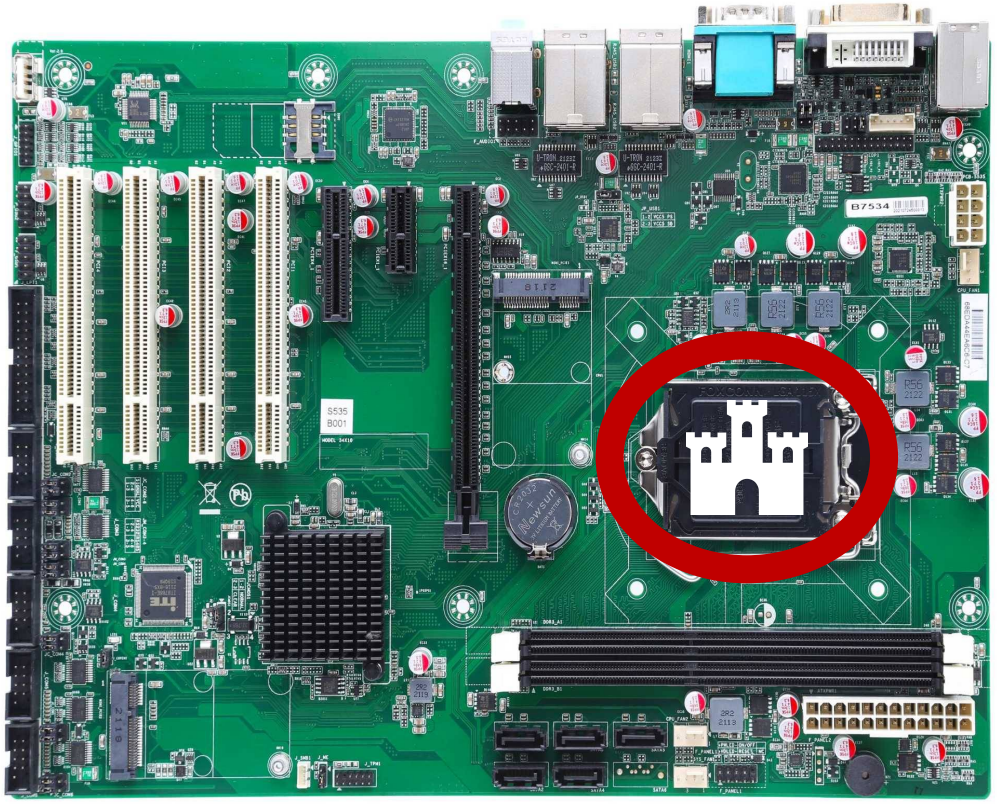
Confidential Computing: Reducing Attack Surface



Trusted execution: CPU-level isolation + memory encryption

Confidential Computing: Trust Boundary

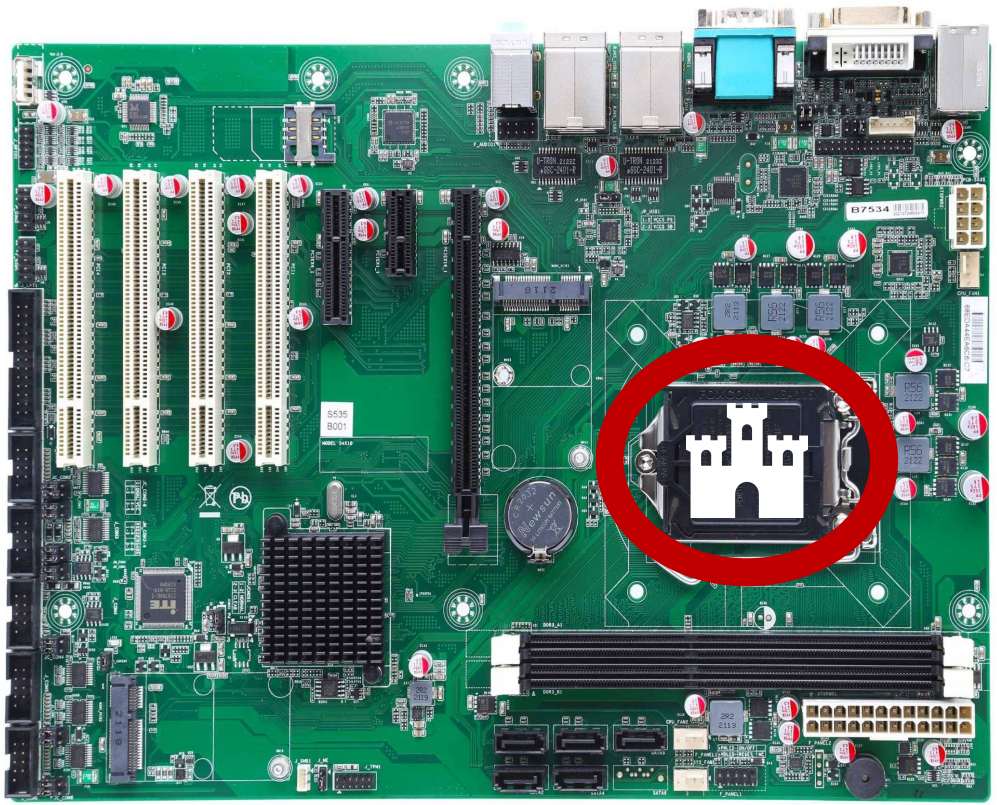
- **CPU package** = trust boundary



Confidential Computing: Trust Boundary

- **CPU package** = trust boundary
- **Memory encryption** to protect against <u>physical access:</u>

1. Rogue cloud provider employees
2. Supply-chain adversaries
3. Local law enforcement



A Brief History of Commercial Memory Encryption

intel

SGX

2015

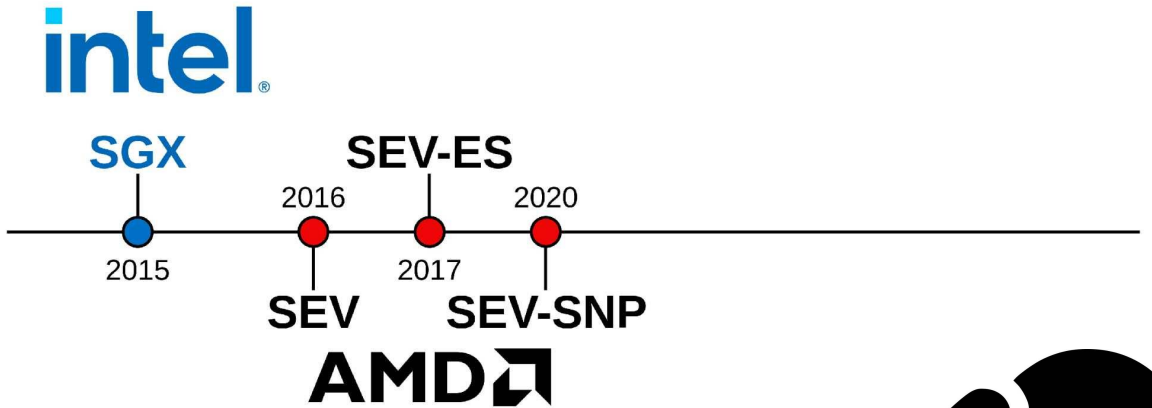
Confidentiality

Integrity

Freshness

Scalable

A Brief History of Commercial Memory Encryption



	SGX	SEV	SEV-ES	SEV-SNP
Confidentiality	🔒	🔒	🔒	🔒
Integrity	🛡	✗	✗	✗
Freshness	↻	✗	✗	✗
Scalable	✗	⤢	⤢	⤢
	🤩	🤔	🤔	🤔

A Brief History of Commercial Memory Encryption

CLOUD | OPERATIONS & MANAGEMENT | NEWS

Why Google Cloud Turned to AMD to Solve for Runtime Encryption

AMD's latest server chips enabled better scalability, less lag, and more memory than Intel SGX, the cloud provider said.

Maria Korolov
July 21, 2020

5 Min Read

https://www.datacenterknowledge.com/cloud/why-google-cloud-turned-to-amd-to-solve-for-runtime-encryption

A Brief History of Commercial Memory Encryption

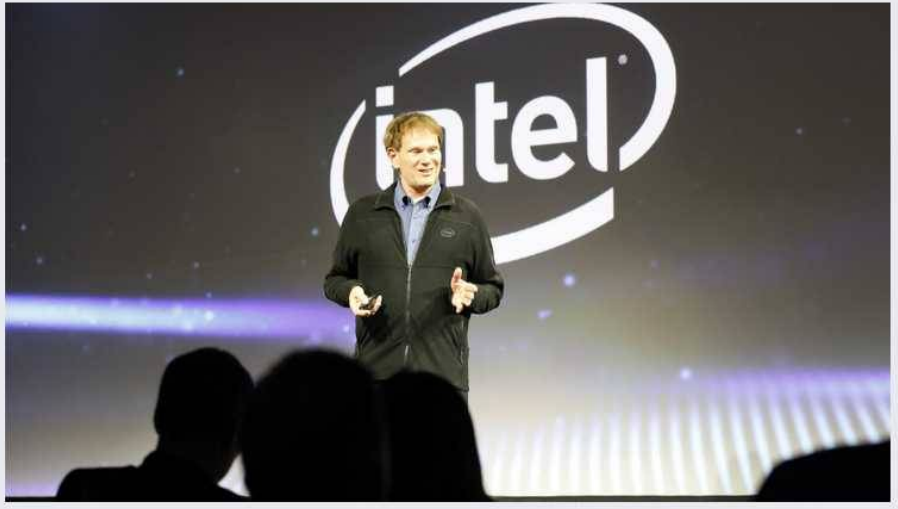
ars TECHNICA SECTIONS FORUM SUBSCRIBE SIGN IN

PUTTING ON A BRAVE FACE

Intel promises Full Memory Encryption in upcoming CPUs

Intel's security plans sound a lot like "we're going to catch up to AMD."

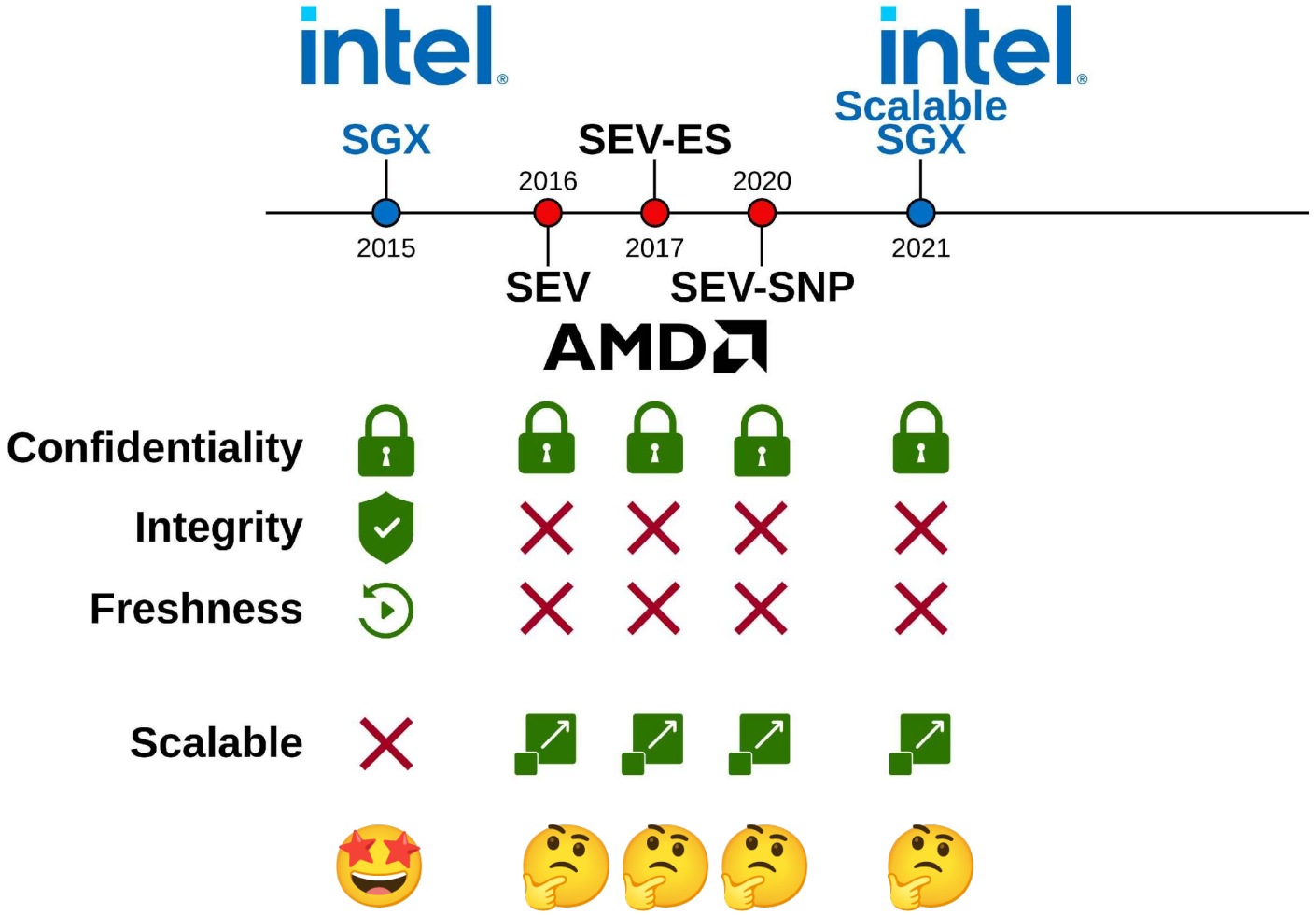
JIM SALTER – FEB 26, 2020 8:29 PM | 120



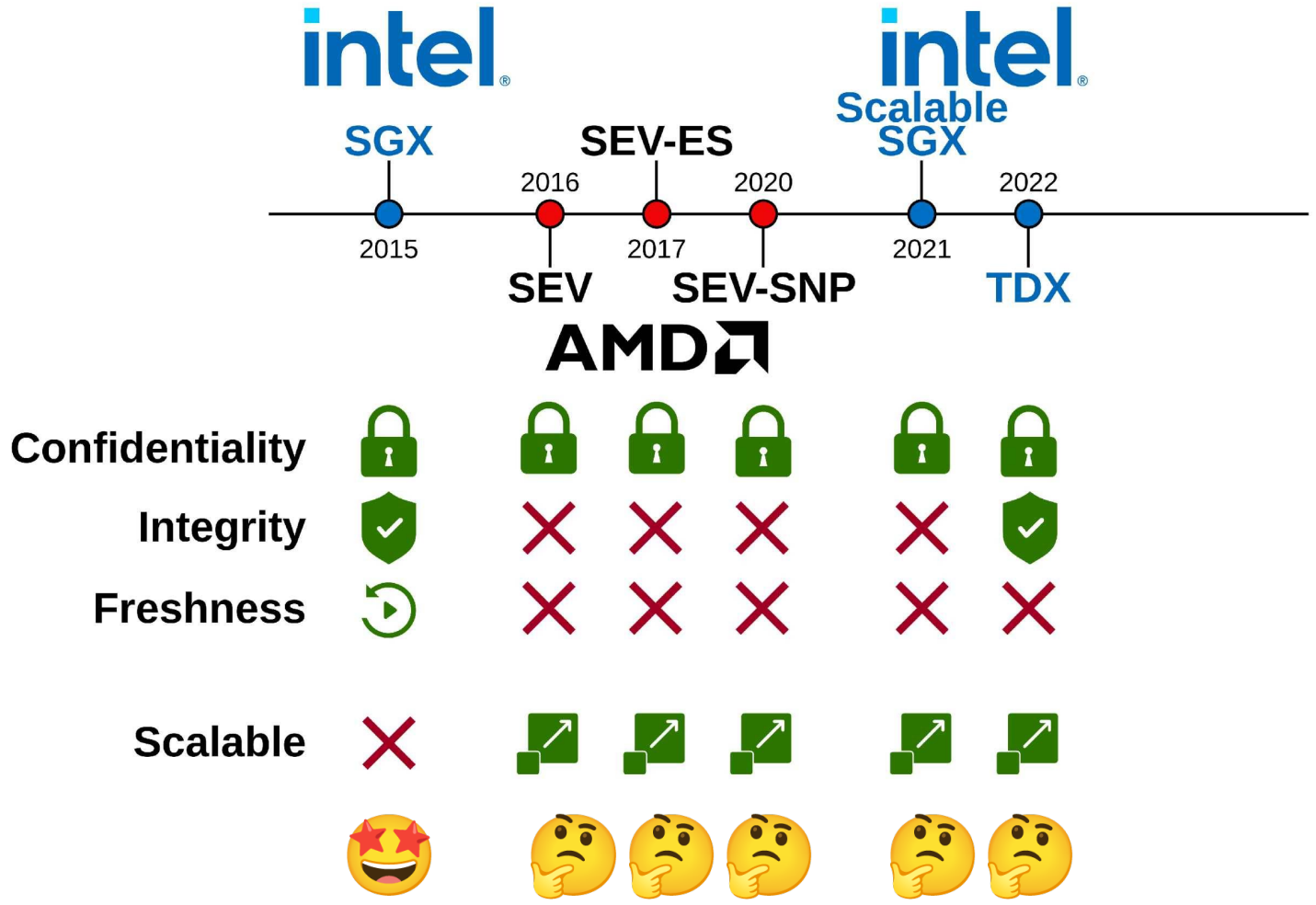
Intel Security Architecture and Technology Director John Sell provided an overview of Intel's mission to provide common security capabilities across all architectures. Credit: Intel Corporation

https://arstechnica.com/gadgets/2020/02/intel-promises-full-memory-encryption-in-upcoming-cpus/

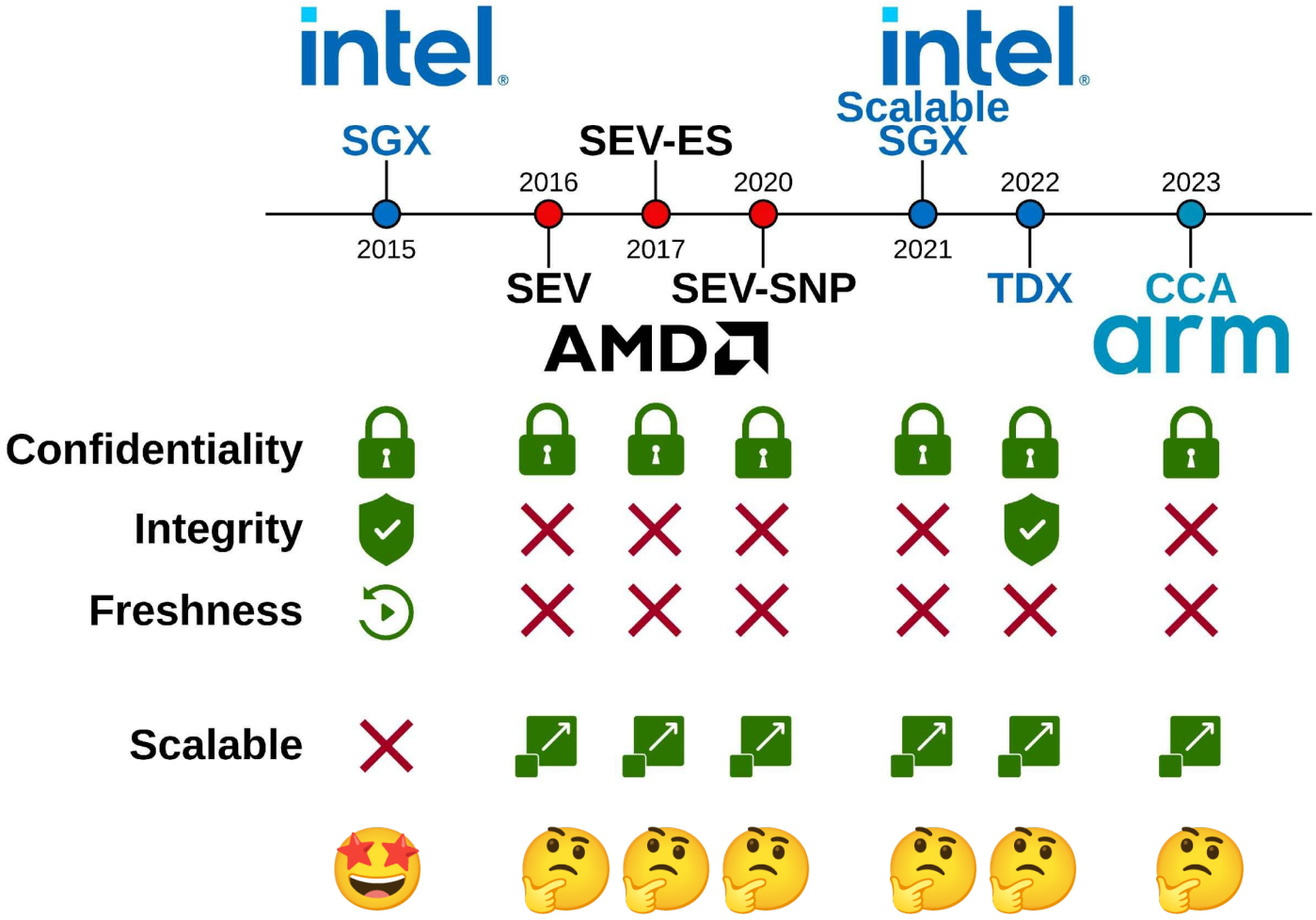
A Brief History of Commercial Memory Encryption



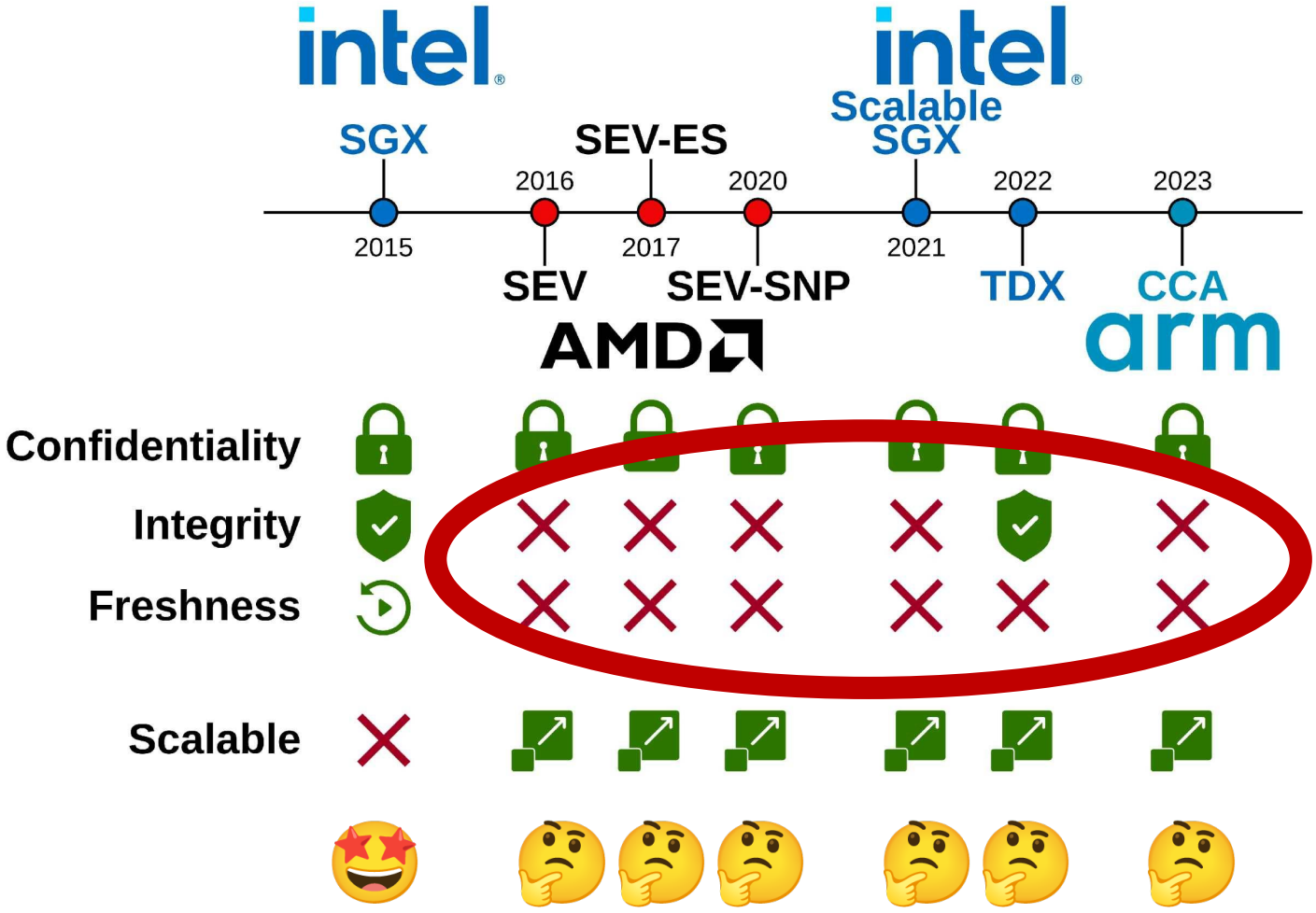
A Brief History of Commercial Memory Encryption

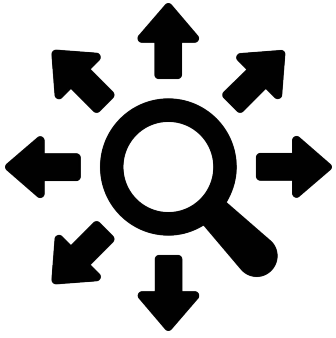


A Brief History of Commercial Memory Encryption



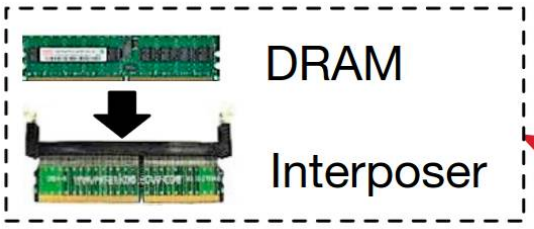
A Brief History of Commercial Memory Encryption

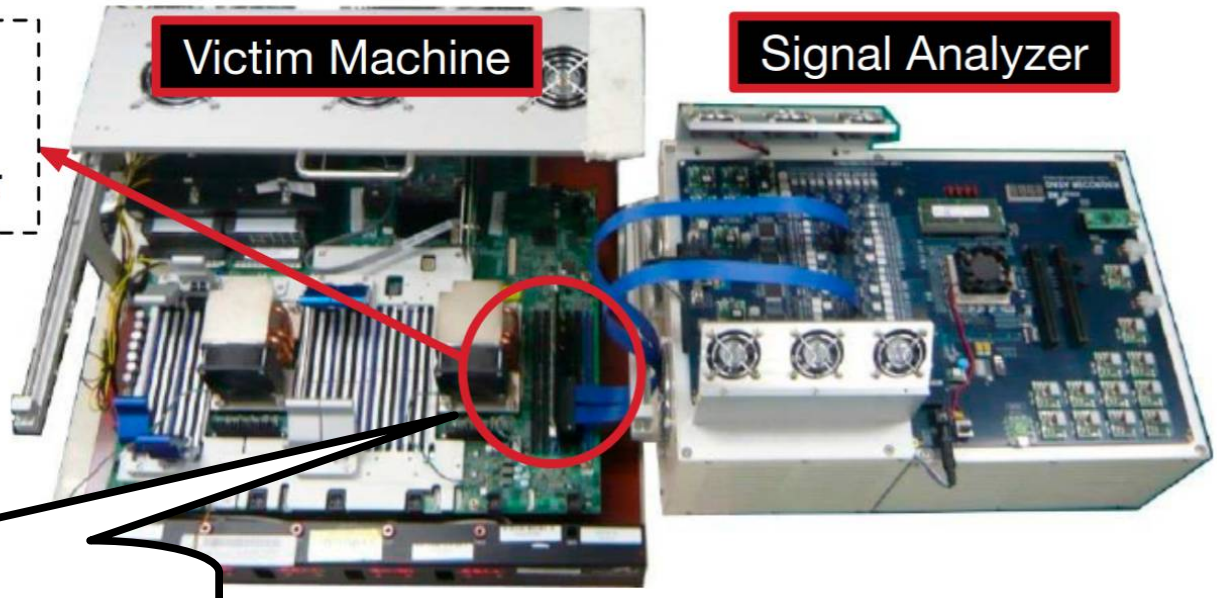




1. Passive Memory Interposers?

MemBuster: Address Side-Channel Analysis for “Classic” SGX



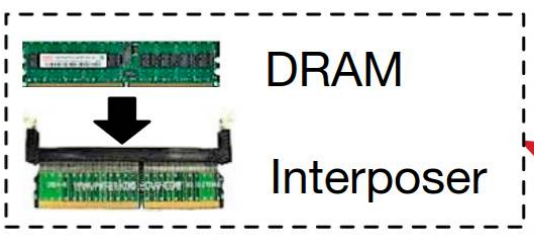


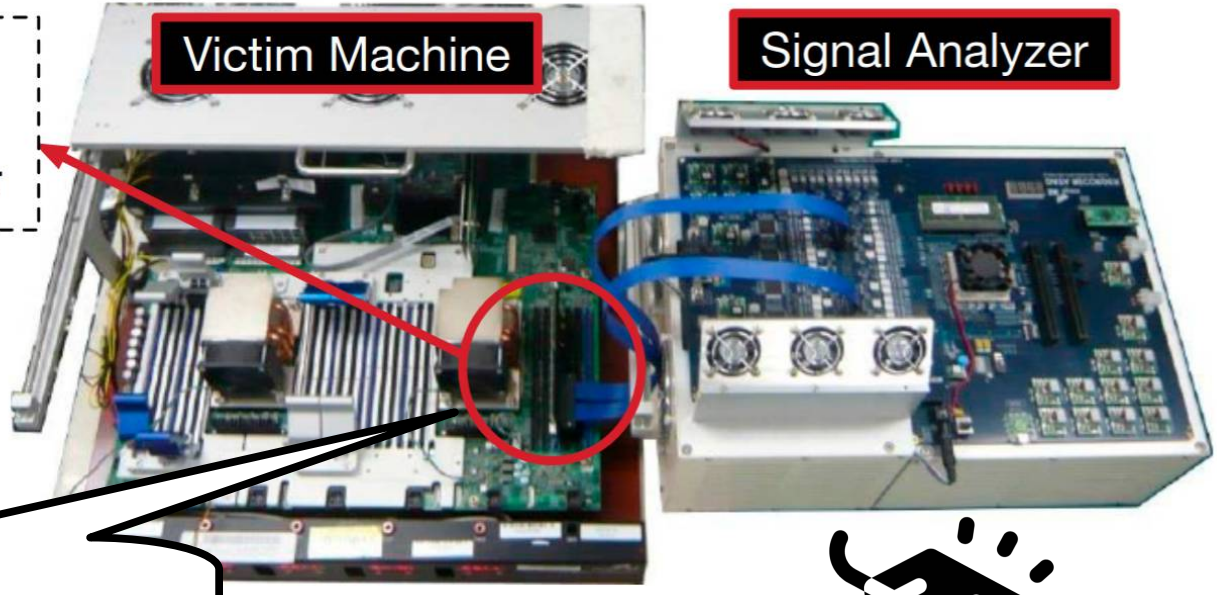
Metadata leaks via
unencrypted address bus

```
if (secret) access(&A);
else access(&B);
```

Lee et al. “An Off-Chip Attack on Hardware Enclaves via the Memory Bus”, USENIX Security 2020.

MemBuster: Address Side-Channel Analysis for “Classic” SGX



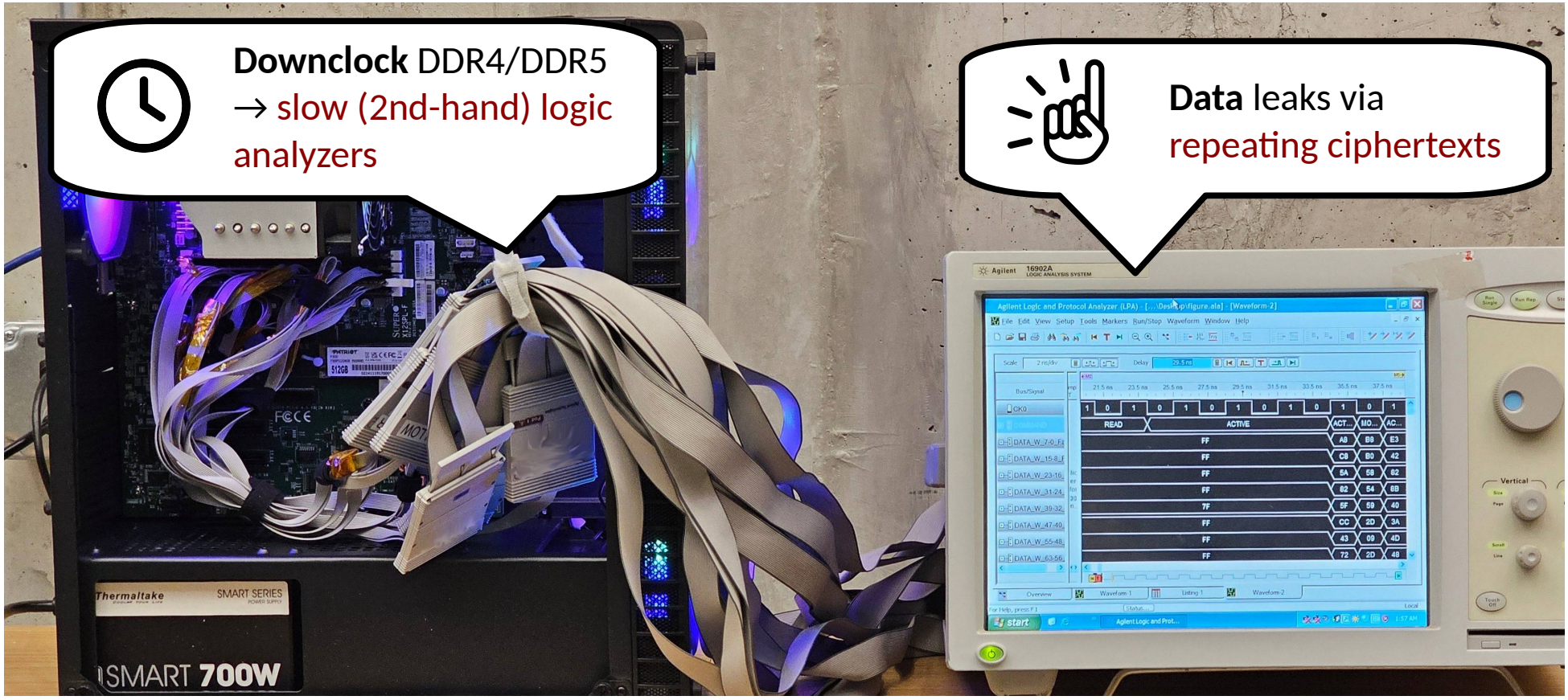


Metadata leaks via
unencrypted address bus

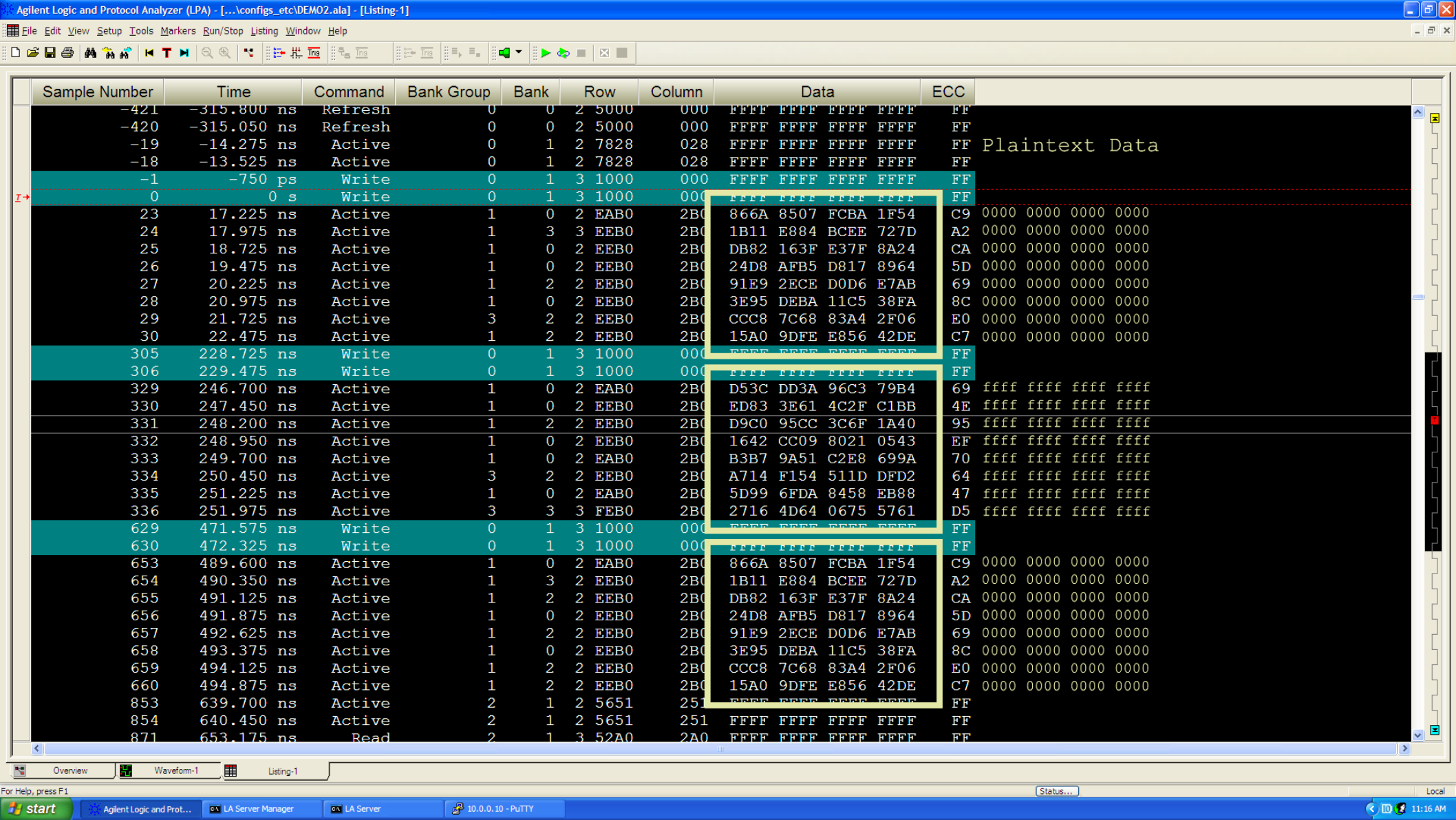
~$170,000(!)

Lee et al. “An Off-Chip Attack on Hardware Enclaves via the Memory Bus”, USENIX Security 2020.

WireTap: Low-Cost Ciphertext Side-Channel Analysis

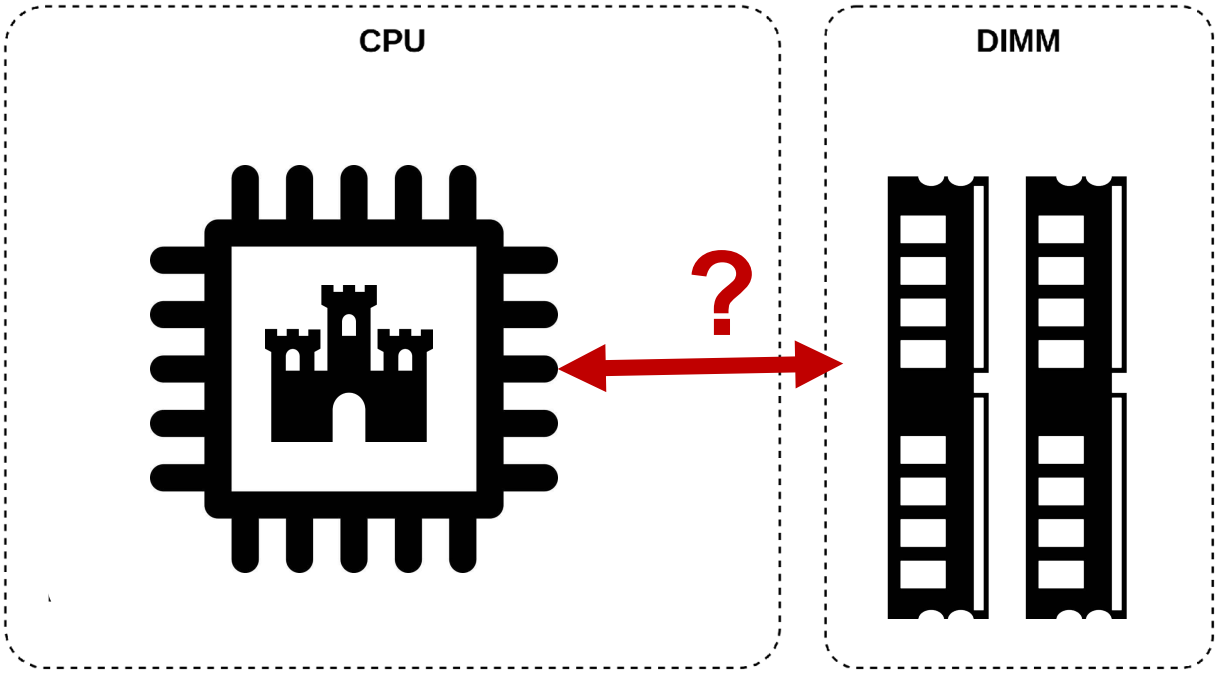


Seto et al. “WireTap: Breaking Server SGX via DRAM Bus Interposition”, CCS 2025.
Chuang et al. “TEE.fail: Breaking Trusted Execution Environments via DDR5 Memory Bus Interposition”, S&P 2026.

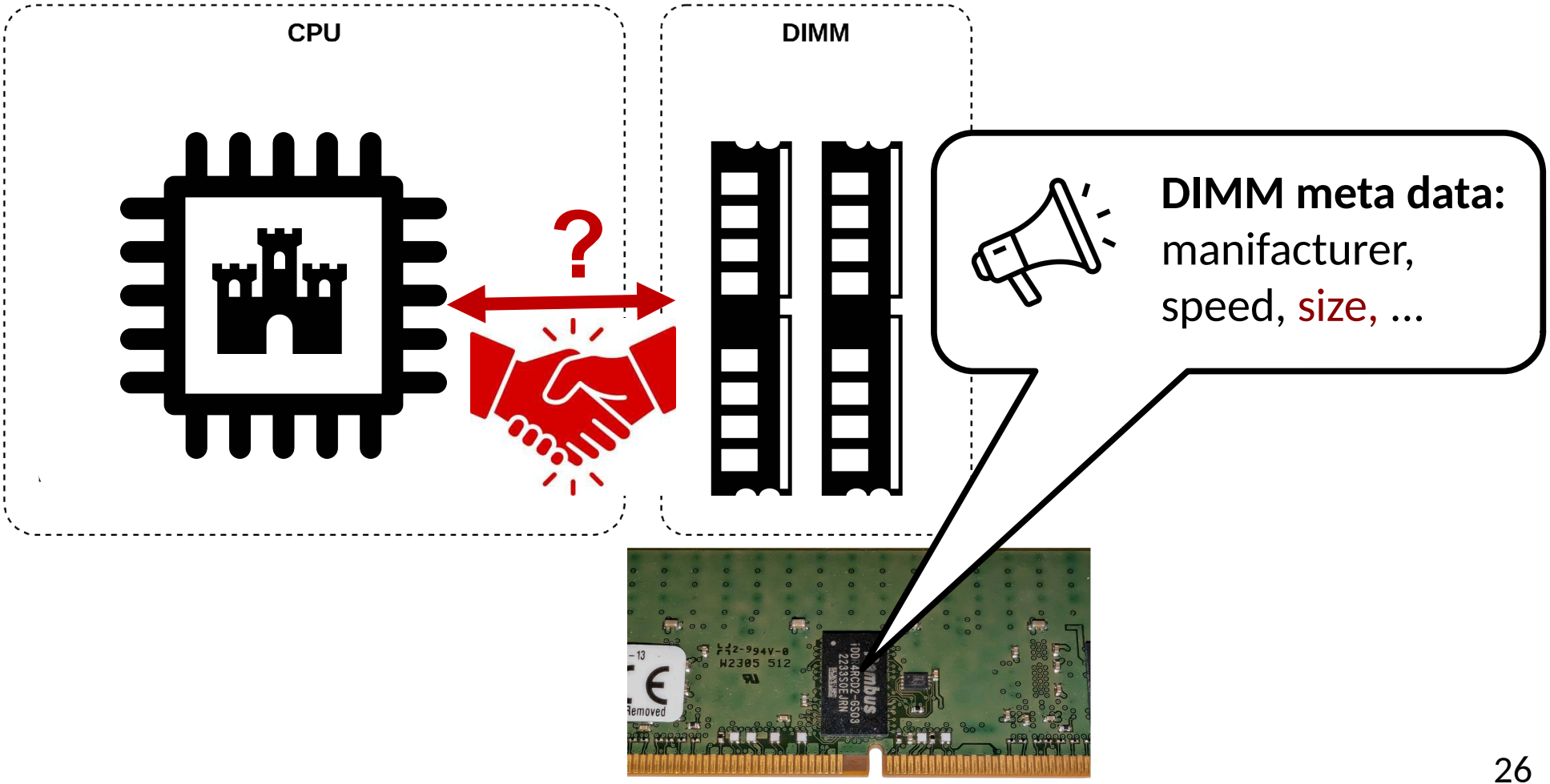

Agilent Logic and Protocol Analyzer (LPA) - [...\configs_etc\DEMO2.ala] - [Listing-1]
File Edit View Setup Tools Markers Run/Stop Listing Window Help
Sample Number | Time | Command | Bank Group | Bank | Row | Column | Data | ECC
-421 -315.800 ns Refresh 0 0 2 5000 000 FFFF FFFF FFFF FFFF FF
-420 -315.050 ns Refresh 0 0 2 5000 000 FFFF FFFF FFFF FFFF FF
-19 -14.275 ns Active 0 1 2 7828 028 FFFF FFFF FFFF FFFF FF Plaintext Data
-18 -13.525 ns Active 0 1 2 7828 028 FFFF FFFF FFFF FFFF FF
-1 -750 ps Write 0 1 3 1000 000 FFFF FFFF FFFF FFFF FF
0 0 s Write 0 1 3 1000 000 FFFF FFFF FFFF FFFF FF
23 17.225 ns Active 1 0 2 EAB0 2B0 866A 8507 FCBA 1F54 C9 0000 0000 0000 0000
24 17.975 ns Active 1 3 3 EEB0 2B0 1B11 E884 BCEE 727D A2 0000 0000 0000 0000
25 18.725 ns Active 1 0 2 EEB0 2B0 DB82 163F E37F 8A24 CA 0000 0000 0000 0000
26 19.475 ns Active 1 0 2 EEB0 2B0 24D8 AFB5 D817 8964 5D 0000 0000 0000 0000
27 20.225 ns Active 1 2 2 EEB0 2B0 91E9 2ECE D0D6 E7AB 69 0000 0000 0000 0000
28 20.975 ns Active 1 0 2 EEB0 2B0 3E95 DEBA 11C5 38FA 8C 0000 0000 0000 0000
29 21.725 ns Active 3 2 2 EEB0 2B0 CCC8 7C68 83A4 2F06 E0 0000 0000 0000 0000
30 22.475 ns Active 1 2 2 EEB0 2B0 15A0 9DFE E856 42DE C7 0000 0000 0000 0000
305 228.725 ns Write 0 1 3 1000 000 FFFF FFFF FFFF FFFF FF
306 229.475 ns Write 0 1 3 1000 000 FFFF FFFF FFFF FFFF FF
329 246.700 ns Active 1 0 2 EAB0 2B0 D53C DD3A 96C3 79B4 69 ffff ffff ffff ffff
330 247.450 ns Active 1 0 2 EEB0 2B0 ED83 3E61 4C2F C1BB 4E ffff ffff ffff ffff
331 248.200 ns Active 1 2 2 EEB0 2B0 D9C0 95CC 3C6F 1A40 95 ffff ffff ffff ffff
332 248.950 ns Active 1 0 2 EEB0 2B0 1642 CC09 8021 0543 EF ffff ffff ffff ffff
333 249.700 ns Active 1 0 2 EAB0 2B0 B3B7 9A51 C2E8 699A 70 ffff ffff ffff ffff
334 250.450 ns Active 3 2 2 EEB0 2B0 A714 F154 511D DFD2 64 ffff ffff ffff ffff
335 251.225 ns Active 1 0 2 EAB0 2B0 5D99 6FDA 8458 EB88 47 ffff ffff ffff ffff
336 251.975 ns Active 3 3 3 FEB0 2B0 2716 4D64 0675 5761 D5 ffff ffff ffff ffff
629 471.575 ns Write 0 1 3 1000 000 FFFF FFFF FFFF FFFF FF
630 472.325 ns Write 0 1 3 1000 000 FFFF FFFF FFFF FFFF FF
653 489.600 ns Active 1 0 2 EAB0 2B0 866A 8507 FCBA 1F54 C9 0000 0000 0000 0000
654 490.350 ns Active 1 3 3 EEB0 2B0 1B11 E884 BCEE 727D A2 0000 0000 0000 0000
655 491.125 ns Active 1 2 2 EEB0 2B0 DB82 163F E37F 8A24 CA 0000 0000 0000 0000
656 491.875 ns Active 1 0 2 EEB0 2B0 24D8 AFB5 D817 8964 5D 0000 0000 0000 0000
657 492.625 ns Active 1 2 2 EEB0 2B0 91E9 2ECE D0D6 E7AB 69 0000 0000 0000 0000
658 493.375 ns Active 1 0 2 EEB0 2B0 3E95 DEBA 11C5 38FA 8C 0000 0000 0000 0000
659 494.125 ns Active 1 2 2 EEB0 2B0 CCC8 7C68 83A4 2F06 E0 0000 0000 0000 0000
660 494.875 ns Active 1 2 2 EEB0 2B0 15A0 9DFE E856 42DE C7 0000 0000 0000 0000
853 639.700 ns Active 2 1 2 5651 251 FFFF FFFF FFFF FFFF FF
854 640.450 ns Active 2 1 2 5651 251 FFFF FFFF FFFF FFFF FF
871 653.175 ns Read 2 1 3 52A0 2A0 FFFF FFFF FFFF FFFF FF
Overview Waveform-1 Listing-1
For Help, press F1
Status...
Local
start
Agilent Logic and Prot...
LA Server Manager
LA Server
10.0.0.10 - PuTTY
11:16 AM

2. Active Memory Interposers?

Background: Memory Initialization

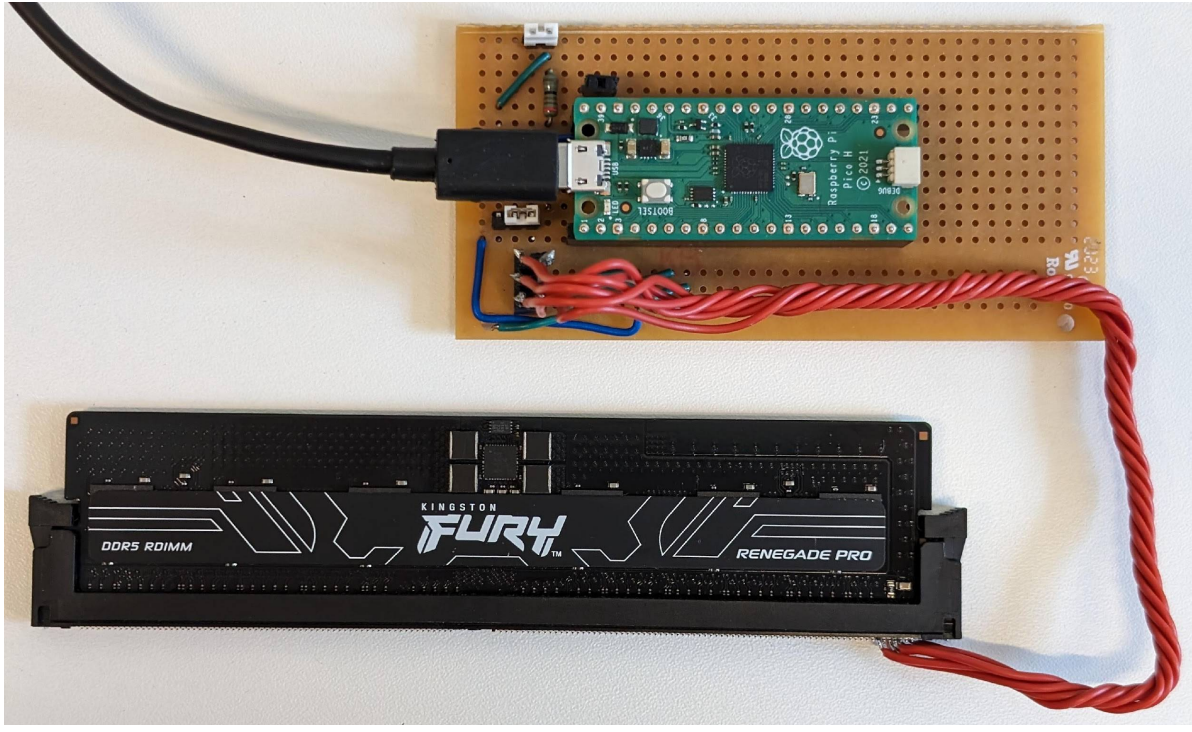


Background: Memory Initialization - Serial Presence Detect (SPD)

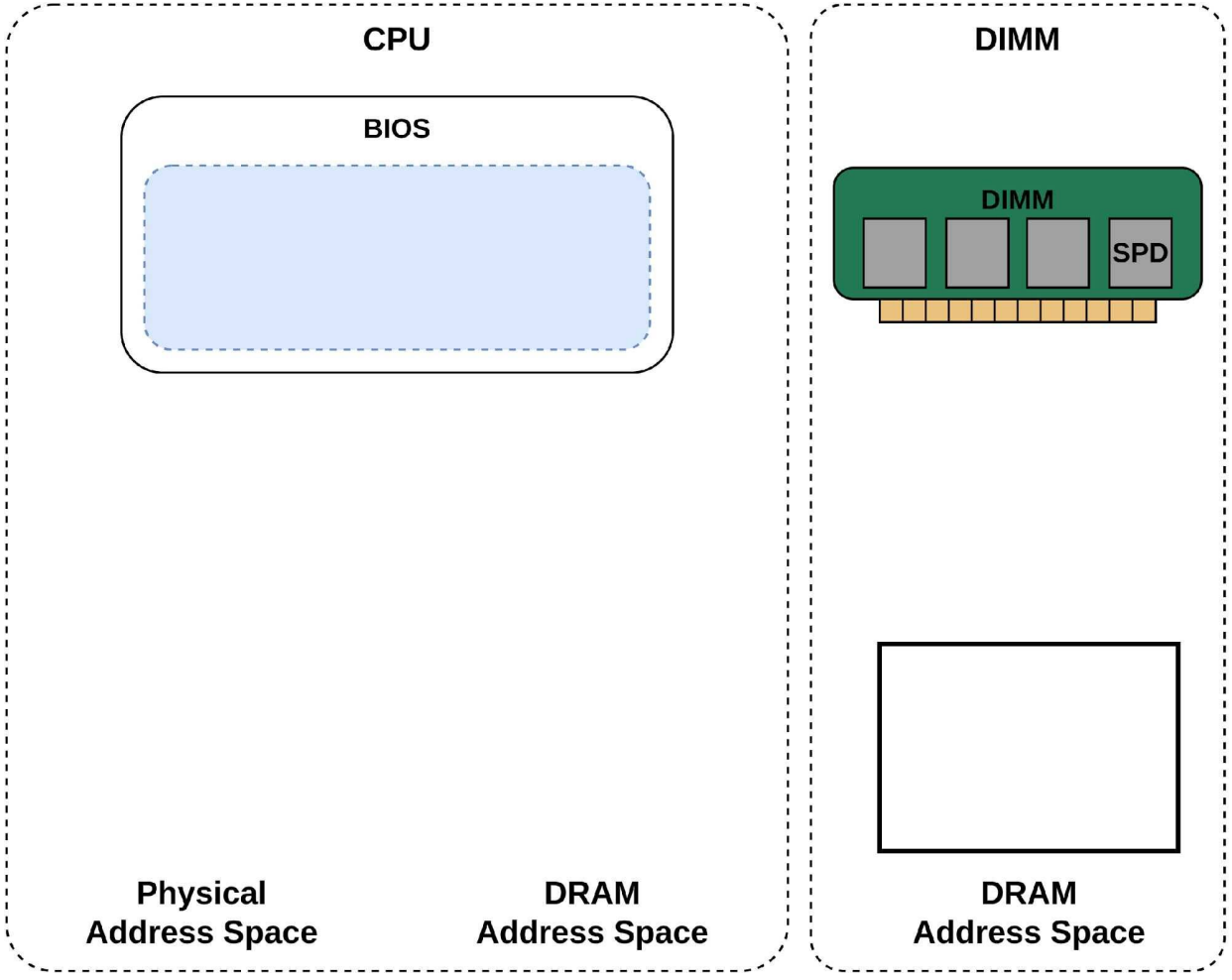


BadRAM: Overwriting the on-DIMM SPD Chip

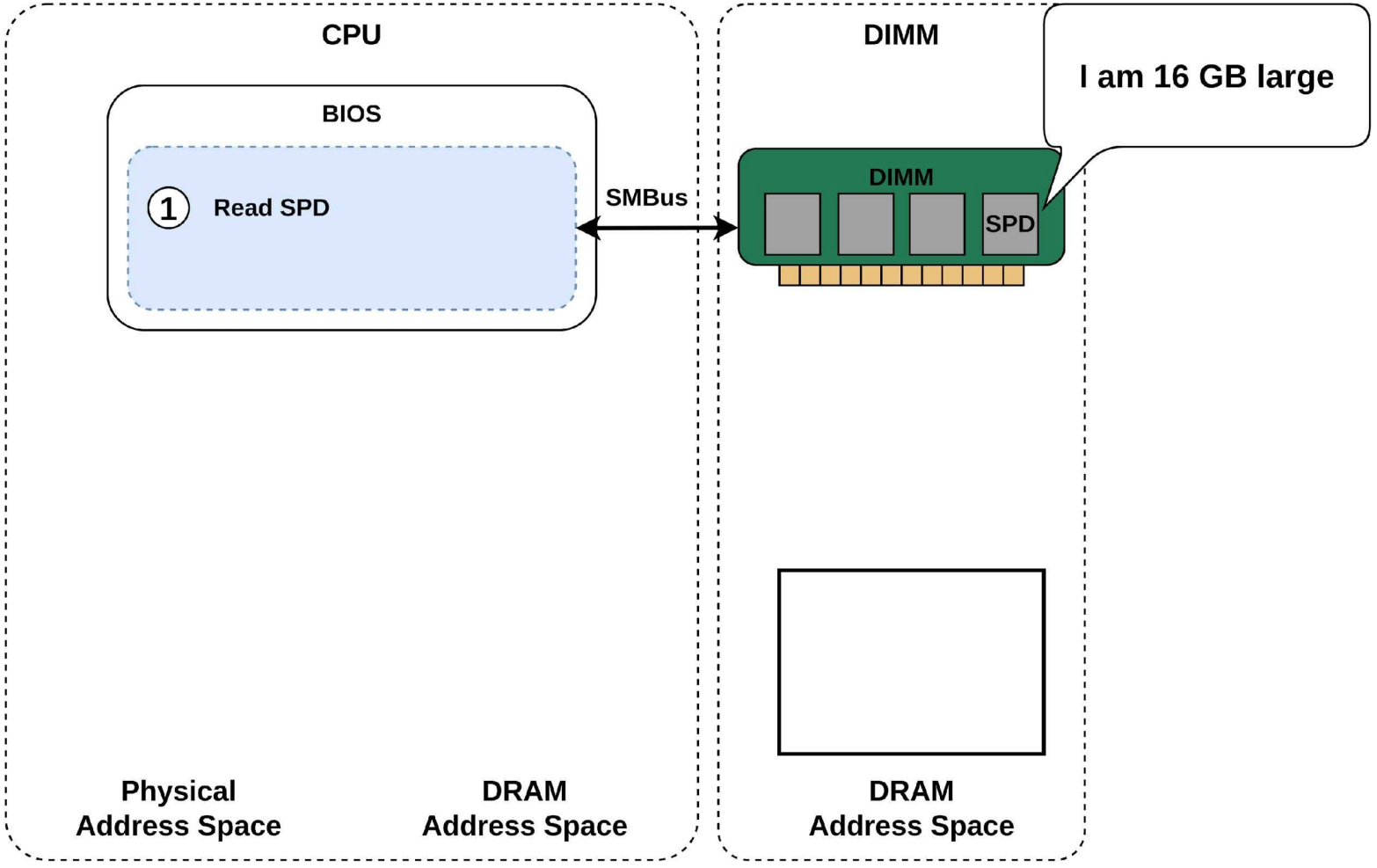
- I^2C pins exposed on DIMM
- Trivial to unlock and overwrite
- **Total cost: ~10$**



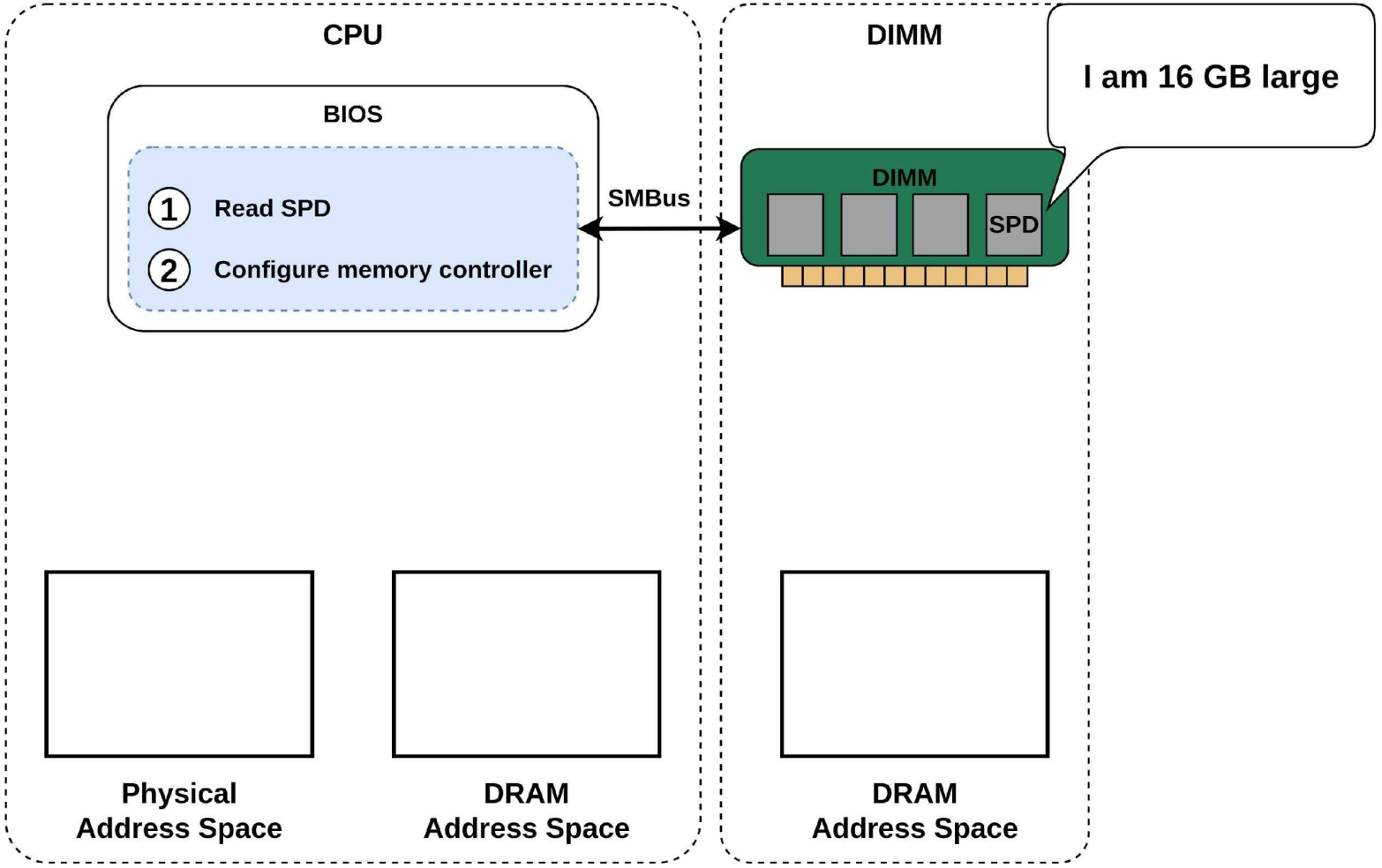
BadRAM: What if Your DRAM Lies to You?



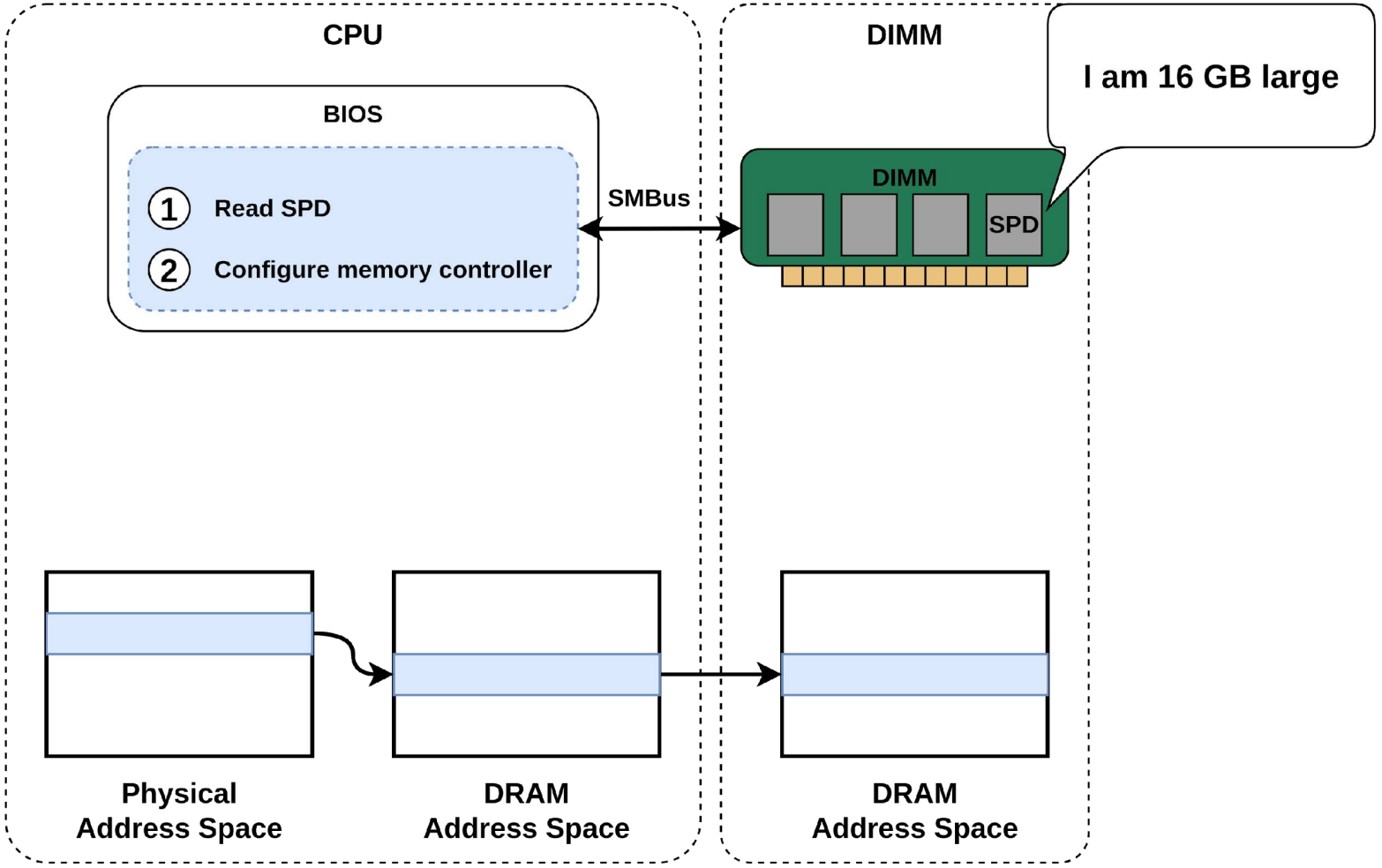
BadRAM: What if Your DRAM Lies to You?



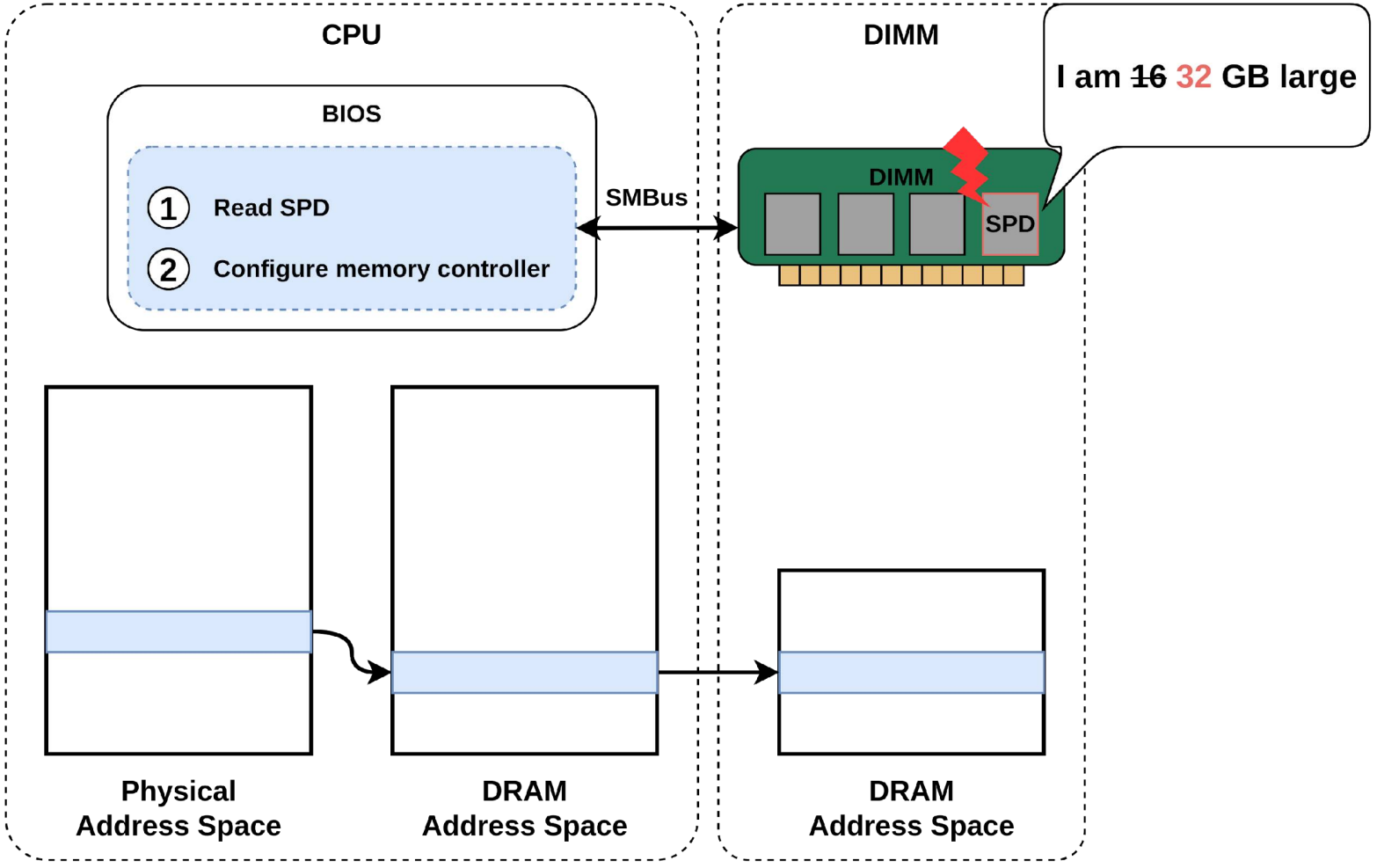
BadRAM: What if Your DRAM Lies to You?



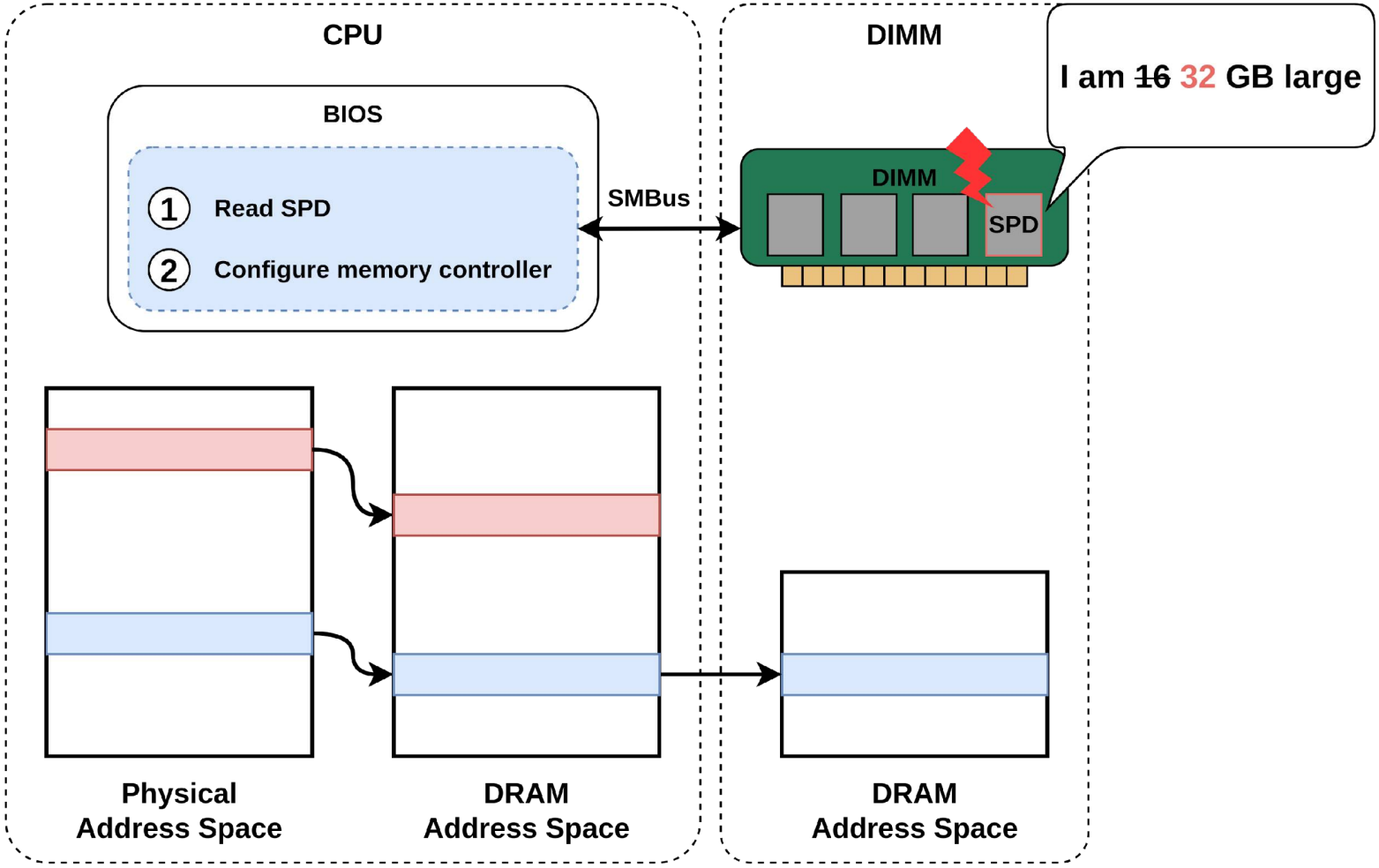
BadRAM: What if Your DRAM Lies to You?



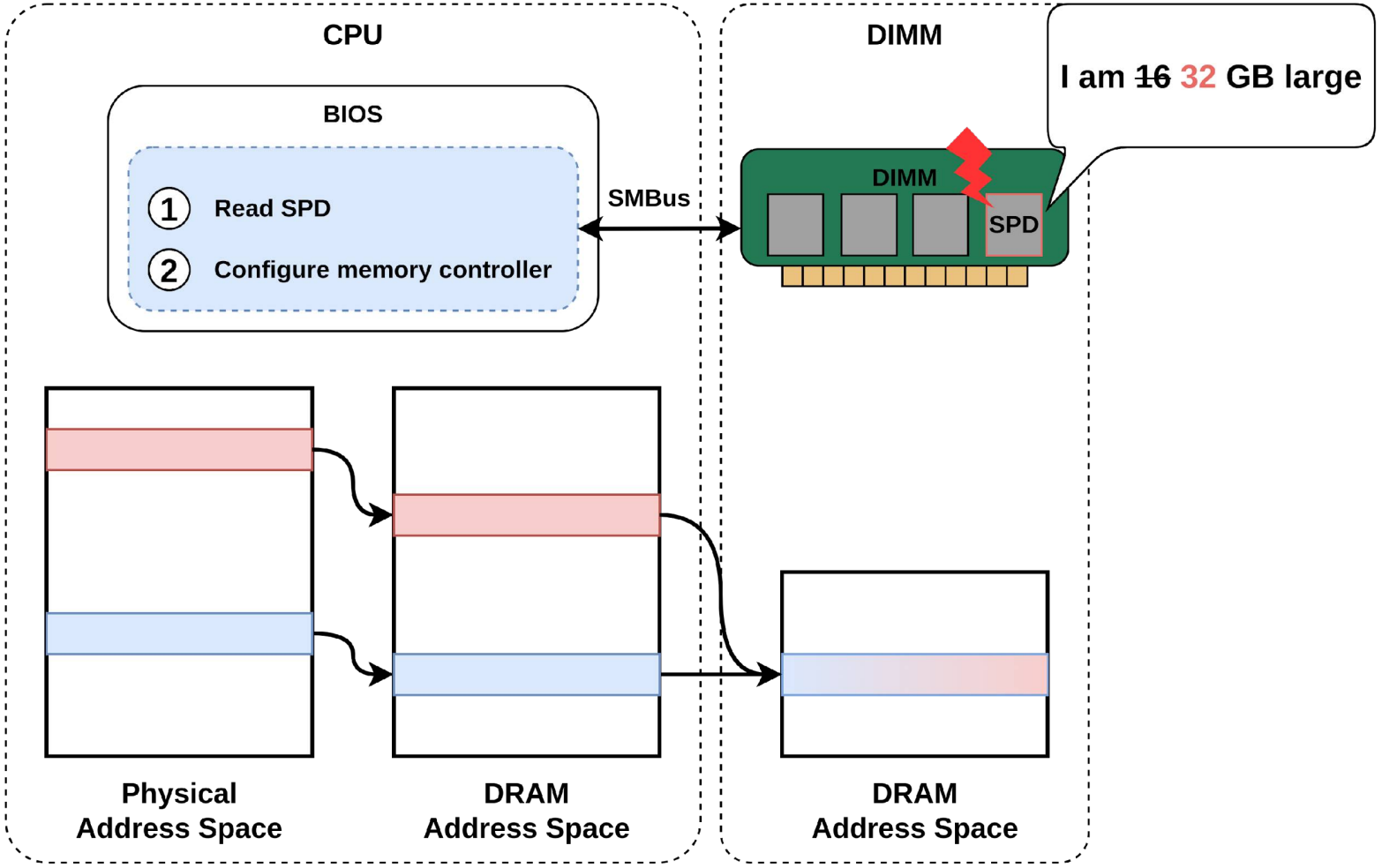
BadRAM: What if Your DRAM Lies to You?



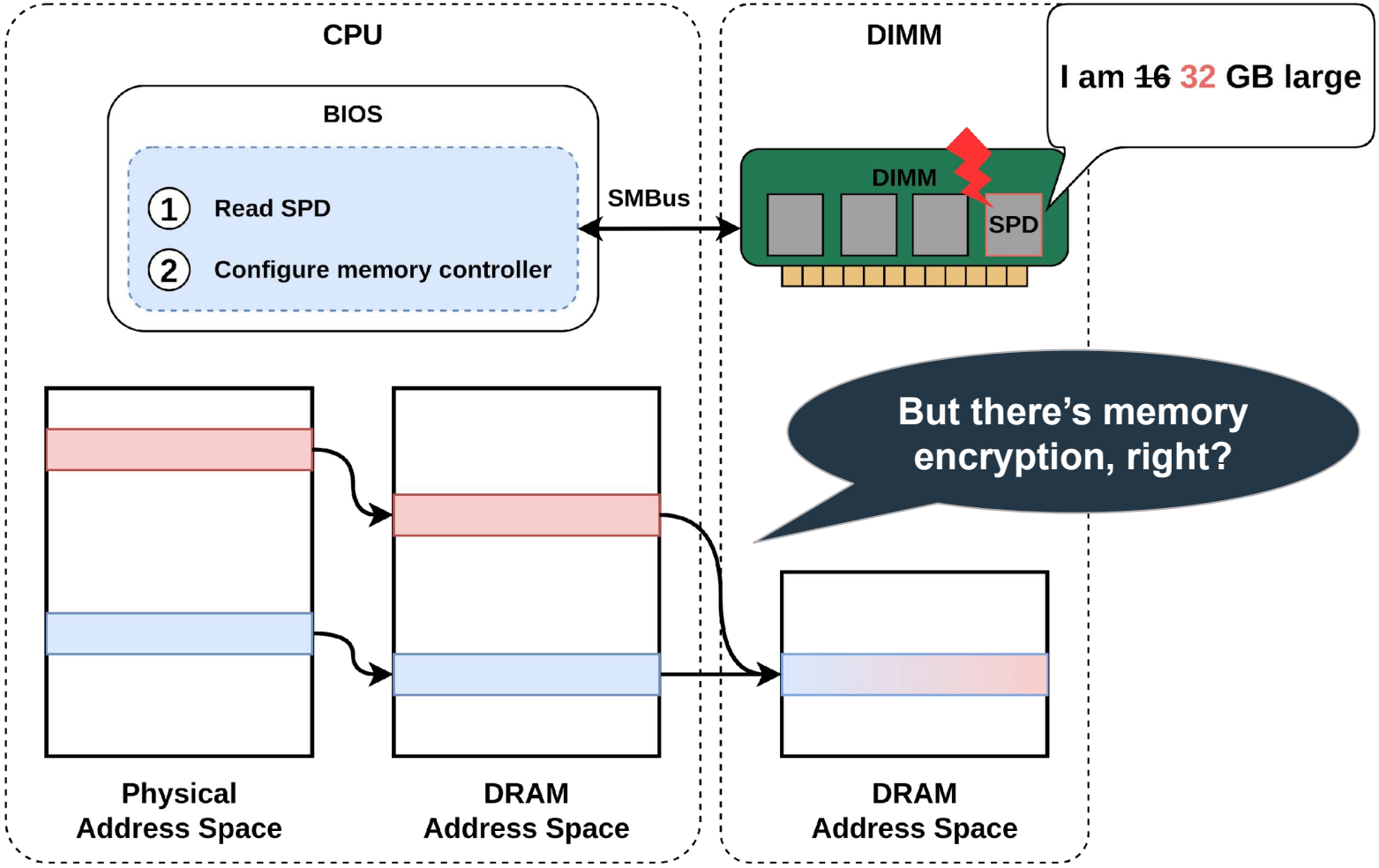
BadRAM: What if Your DRAM Lies to You?



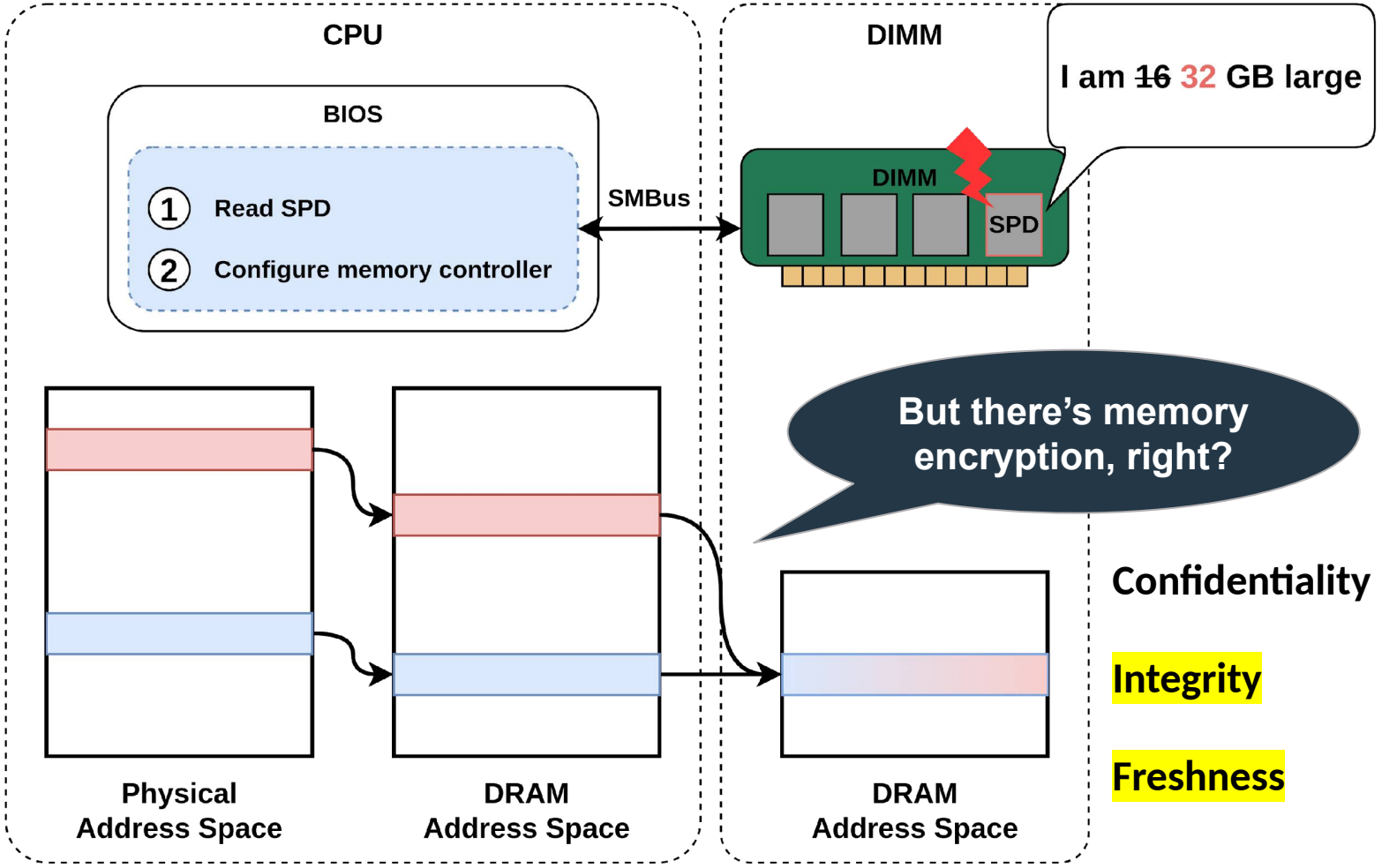
BadRAM: What if Your DRAM Lies to You?



BadRAM: What if Your DRAM Lies to You?



BadRAM: What if Your DRAM Lies to You?



Demo

Replaying encrypted memory

```
*****     AMD SEV-SNP Victim VM     *****

Initialized 64-byte memory buffer
 --> Virtual address:  0x7f485c6e7000
 --> Physical address: 0x26f5e000

Buffer initialized to zero:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Capture the ciphertext, then press enter

Setting buffer to 0xff
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

Replay the old ciphertext, then press enter

Printing memory buffer
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
jesse@jesse-test:~$
```

```
*****     Privileged Software Attacker     *****

Translating victim address
 --> Guest physical address: 0x26f5e000
 --> Host physical address:  0x18415e000

Calculating memory alias
 --> Original address: 0x18415e000
 --> Alias address:    0x58415e000

Press Enter to capture ciphertext

Successfully captured victim ciphertext:
0d 52 96 9c b1 b3 0a e9 b5 f0 7e d9 06 e7 2f 5c fa 17 cf aa 88 c8 4e 8b c5 26 f7 28 5e 57 1f c4
e8 b5 09 44 00 a3 af 6f b9 12 61 aa 27 b7 e4 df 65 6f 39 ec a7 ee c5 50 f3 c9 56 51 dc 84 ee b3


Press enter to start replay

Replayed victim ciphertext
jesse@horus:~/badram/sev-attacks/simple-replay$
```

The Register

AMD secure VM tech undone by DRAM meddling

Boffins devise BadRAM attack to pilfer secrets from SEV-SNP e

Thomas Claburn

Tue 10 Dec 2024

BadRAM attack breaches AMD secure VMs using a Raspberry Pi Pico, DDR socket, and a 9V battery

News By Mark Tyson published December 11, 2024

AMD has now issued firmware updates for cloud providers.

ars TECHNICA AI BIZ & IT CARS CULTURE GAMING HEALTH POLICY SCIENCE SECURITY SPACE TECH FORUM SUBSCRIBE

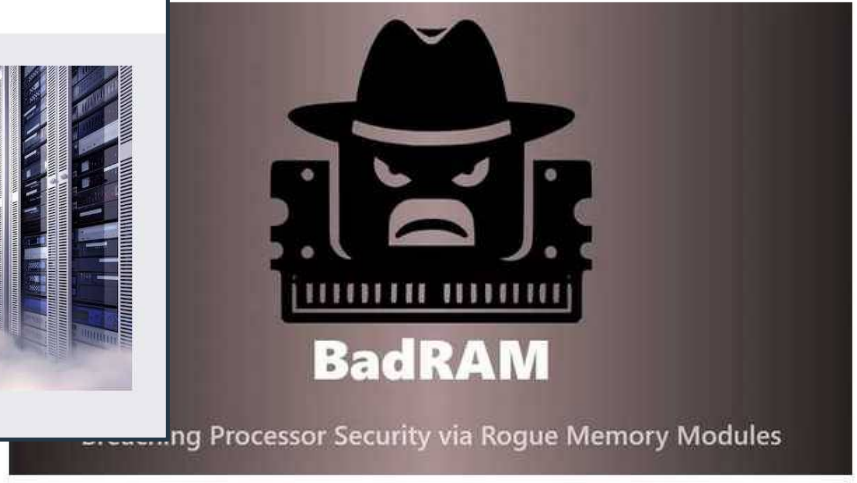
BEWARE OF GHOSTS

AMD's trusted execution environment blown wide open by new BadRAM attack

Attack bypasses AMD protection promising security, even when a server is compromised.

DAN GOODIN – 10 DEC 2024 18:08 | 112

Credit: Getty Images



🌍 https://badram.eu/

Vendor Response: Boot-Time Firmware Mitigations

Undermining Integrity Features of SEV-SNP with Memory Aliasing

AMD ID: AMD-SB-3015
Potential Impact: Loss of Integrity
Severity: Medium

Summary

A team of researchers has reported to AMD that it may be possible to modify serial presence detect (SPD) metadata to make an attached memory module appear larger than it is, potentially allowing an attacker to overwrite physical memory.

Guest Attestation Report [Attestation method for Guest VM]

ATTESTATION_REPORT Structure PLATFORM_INFO field in Byte offset 0h bit 5 contains indication that the mitigation has been applied and confirmed.

Byte Offset	Bits	Name	Description
00h	63:6	-	Reserved.
	5	ALIAS_CHECK_COMPLETE	Indicates that alias detection has completed since the last system reset and there are no aliasing addresses. Resets to 0.

https://www.amd.com/en/resources/product-security/bulletin/amd-sb-3015.html

Vendor Response: Boot-Time Firmware Mitigations

Undermining Integrity Features of SEV-SNP with Memory Aliasing

AMD ID: AMD-SB-3015
Potential Impact: Loss of Integrity
Severity: Medium

Summary

A team of researchers has reported to AMD that it may be possible to modify serial presence detect (SPD) metadata to make an attached memory module appear larger than it is, potentially allowing an attacker to overwrite physical memory.

What if we can introduce aliases at runtime (post-boot)?

Guest Attestation Report [Attestation method for Guest VM]

ATTESTATION_REPORT Structure PLATFORM_INFO[illegible] offset 0h bit 5 contains indication that the mitigation has been applied and confirmed.

Byte Offset	Bits	Name	
00h	63:6	-	Reser[illegible]
	5	ALIAS_CHECK_COMPLETE	Indicates that alias detection has completed since the last system reset and there are no aliasing addresses. Resets to 0.

https://www.amd.com/en/resources/product-security/bulletin/amd-sb-3015.html


I HAVE...
AN EVIL PLAN
quickmeme.com

Interfering at Runtime: Commercial DRAM Interposers?

Genuine New MW-Keysight U4972A DDR4 Protocol Debugging and Analysis Solution Logic Analyzers Factory Wholesale Price

US$782,016.00
1 Set (MOQ)

Send Inquiry | Chat Now

Product Details

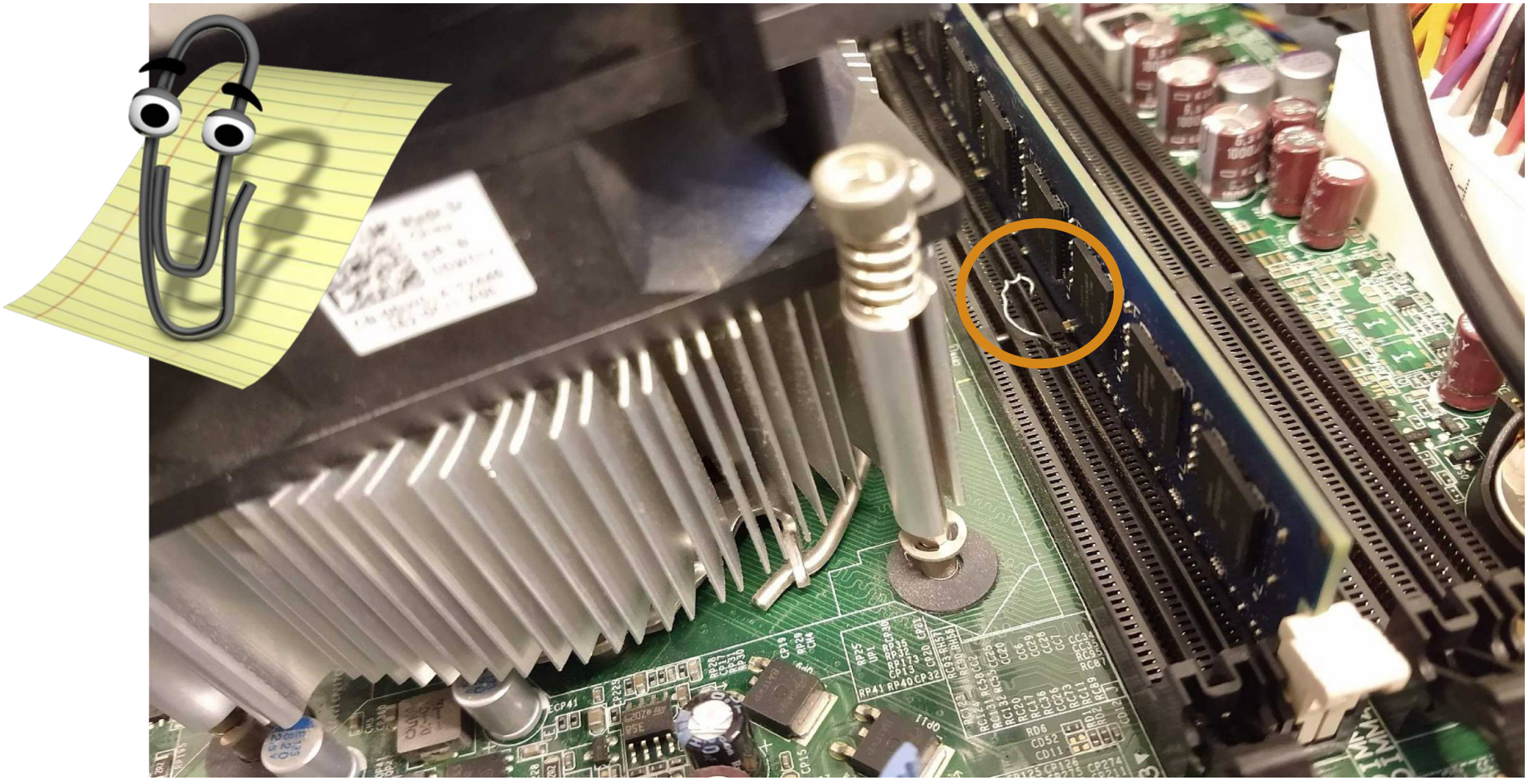
Customization:	Available
After-sales Service:	12 Months
Warranty:	12 Months

Shenzhen Leading International Trading Co., Ltd. >

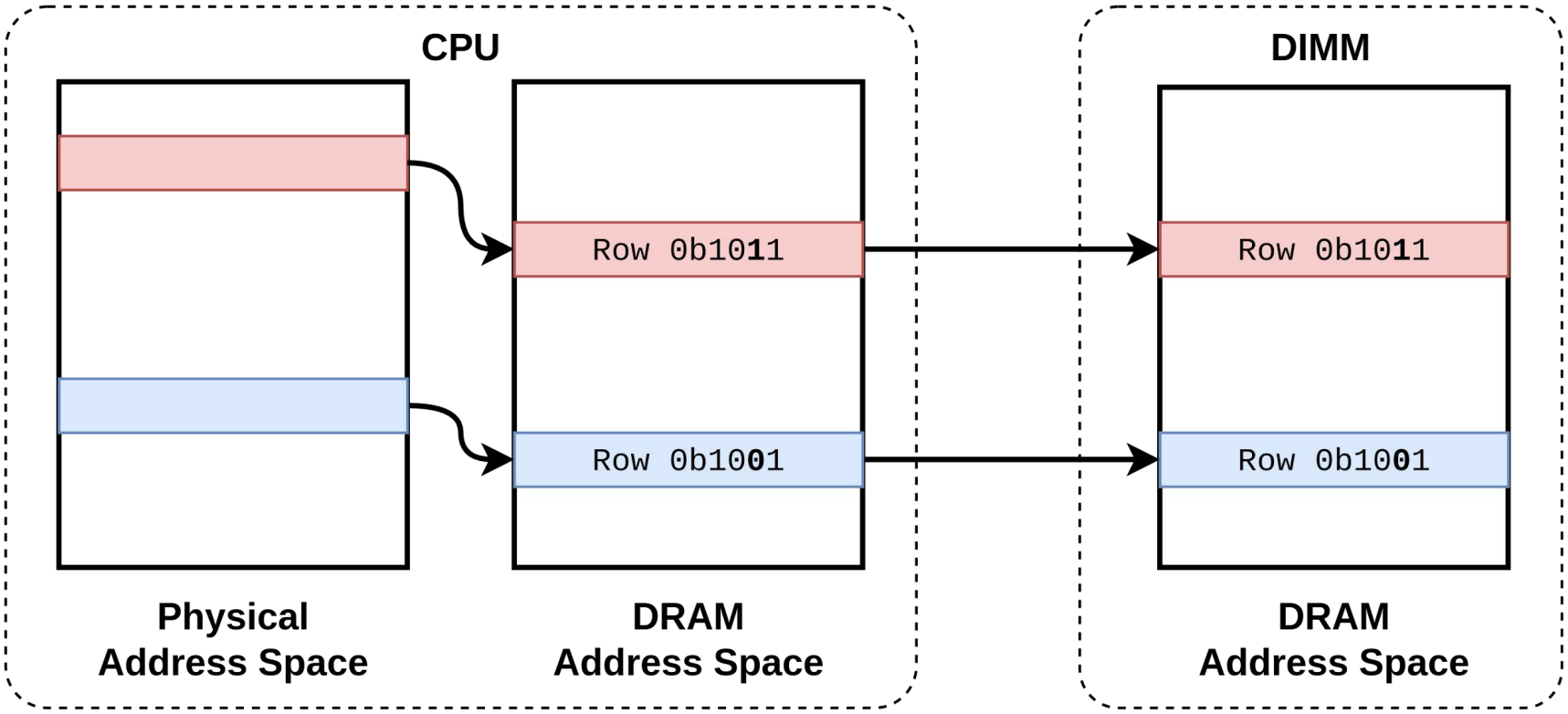
Gold Member Since 2024

Audited Supplier

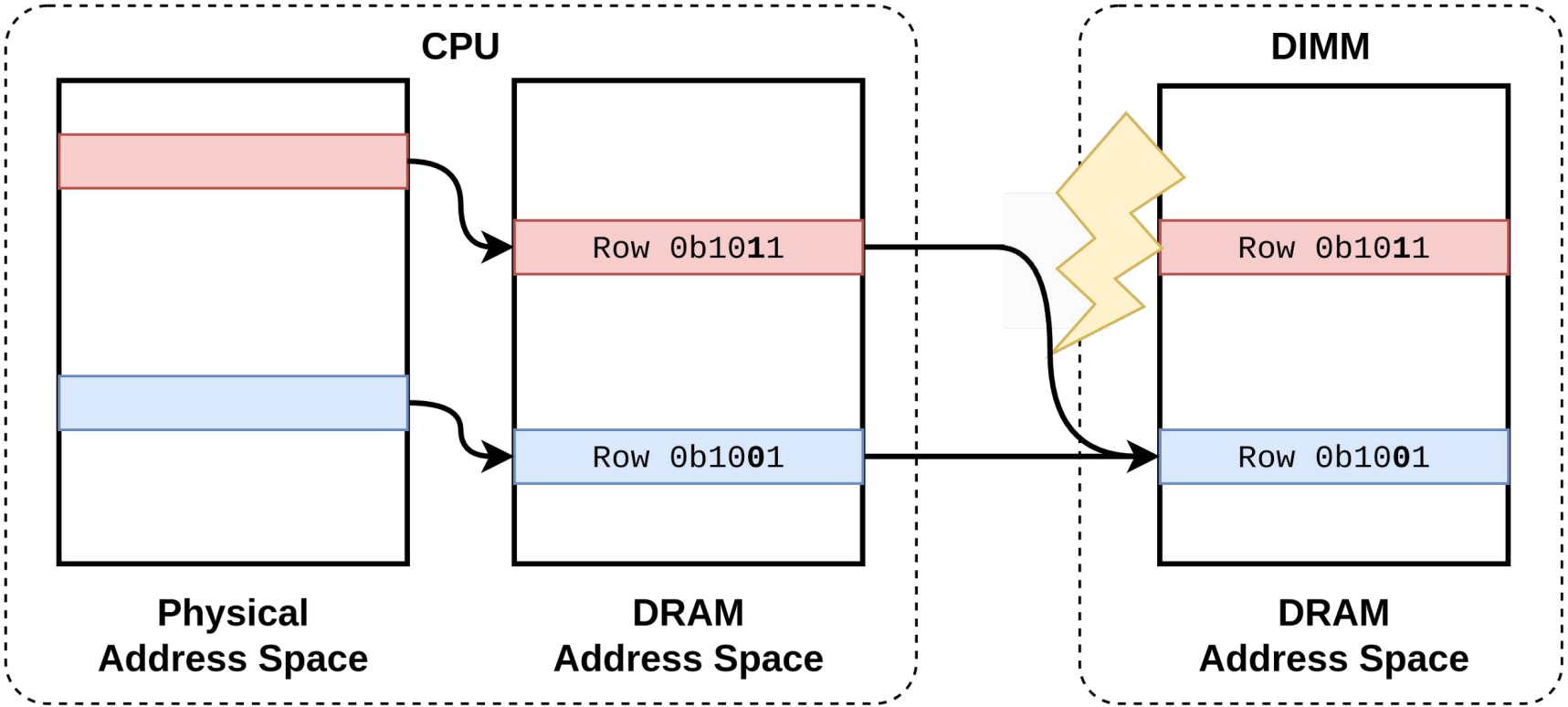
Tampering with Addressing at Runtime



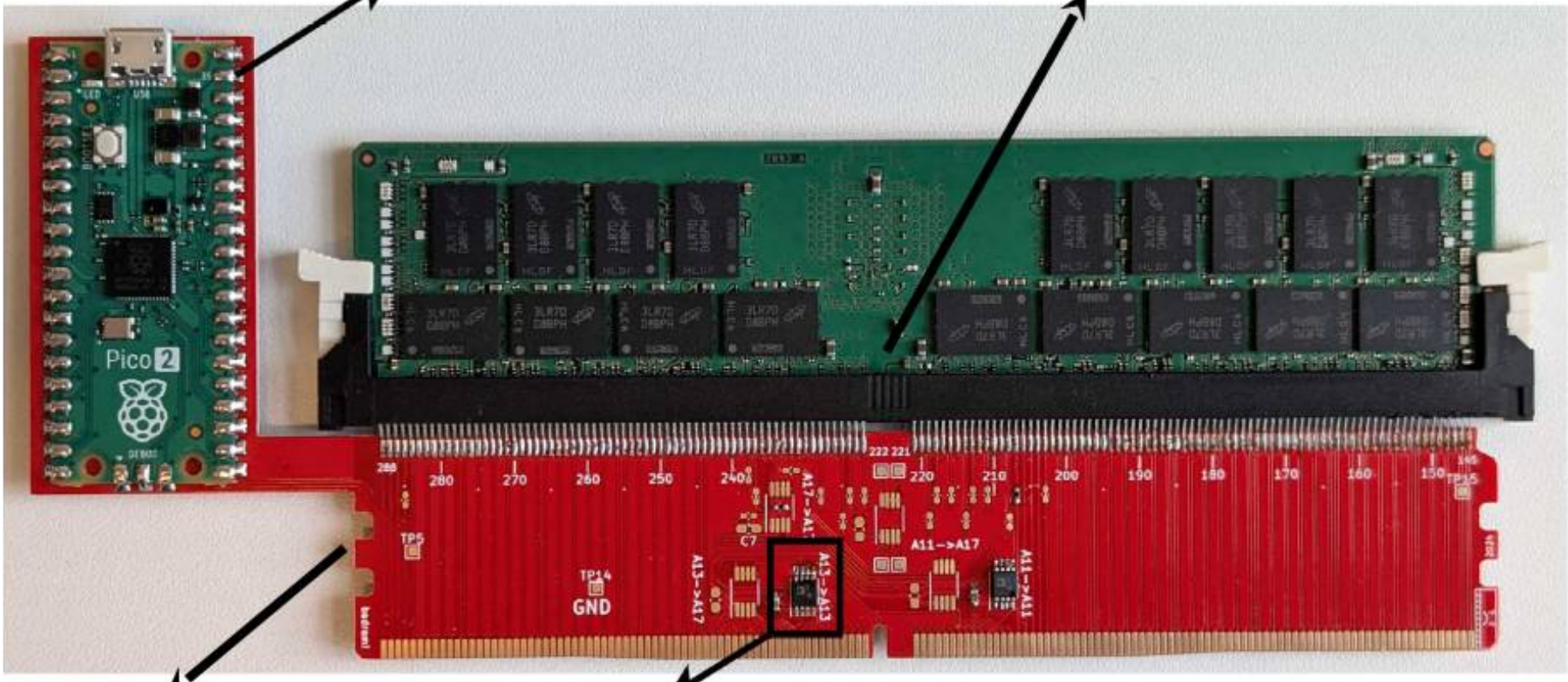
Battering RAM: Tampering with Addressing at Runtime



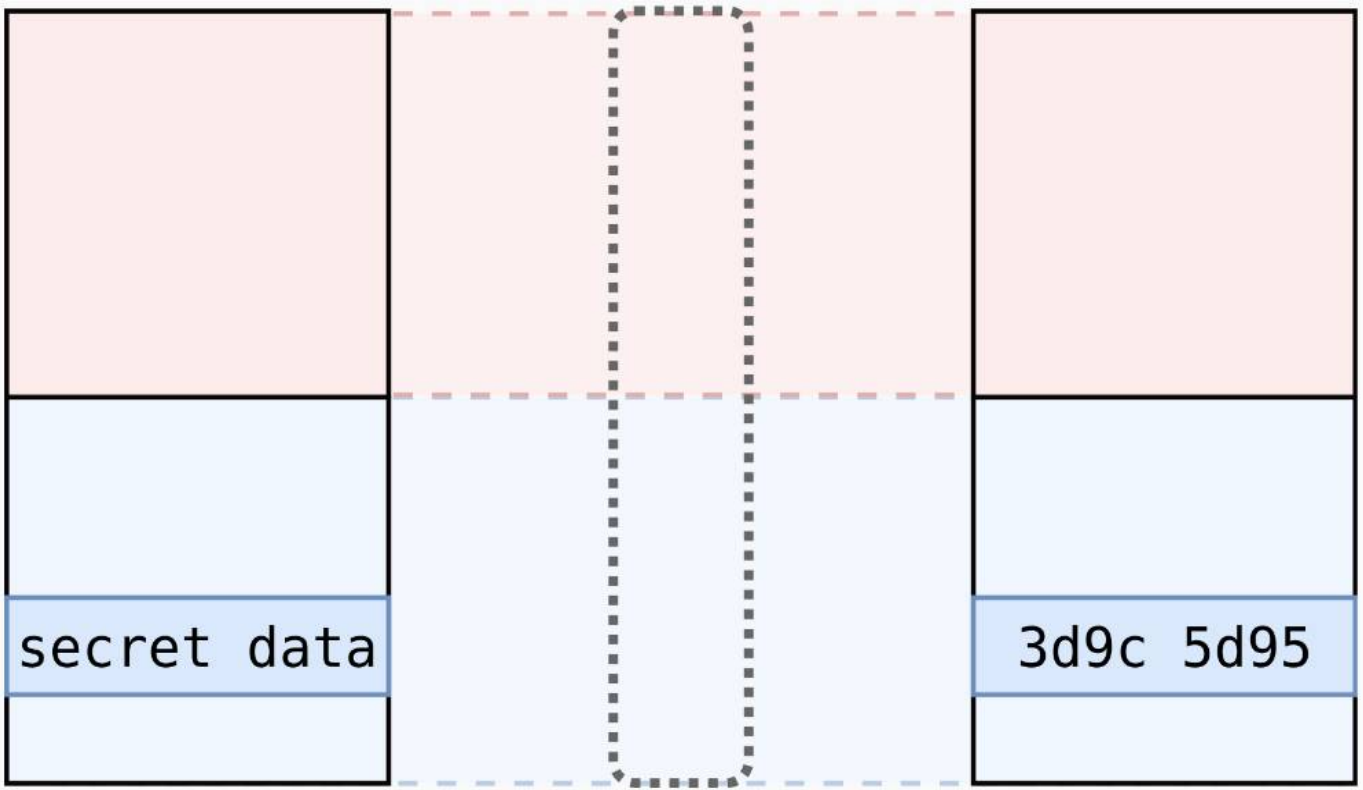
Battering RAM: Tampering with Addressing at Runtime



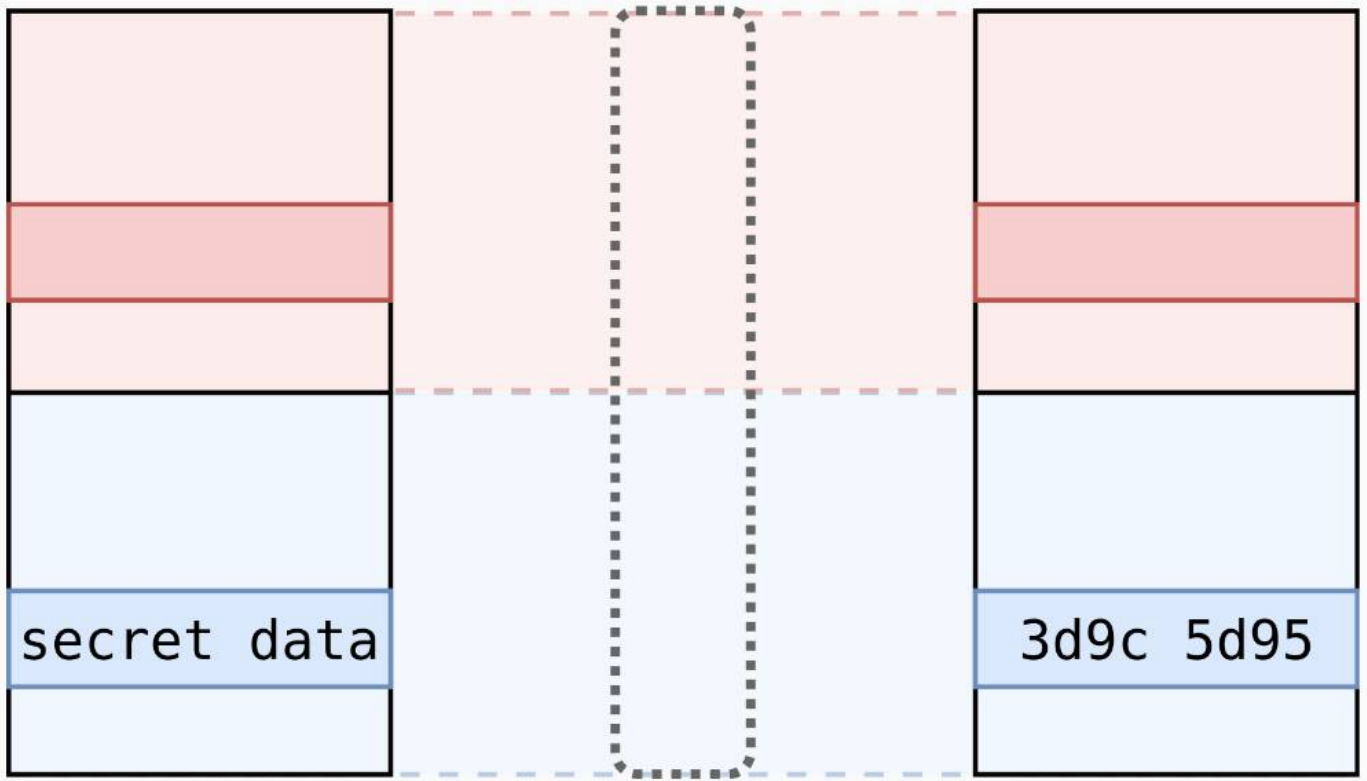
Battering RAM: Tampering with Addressing at Runtime



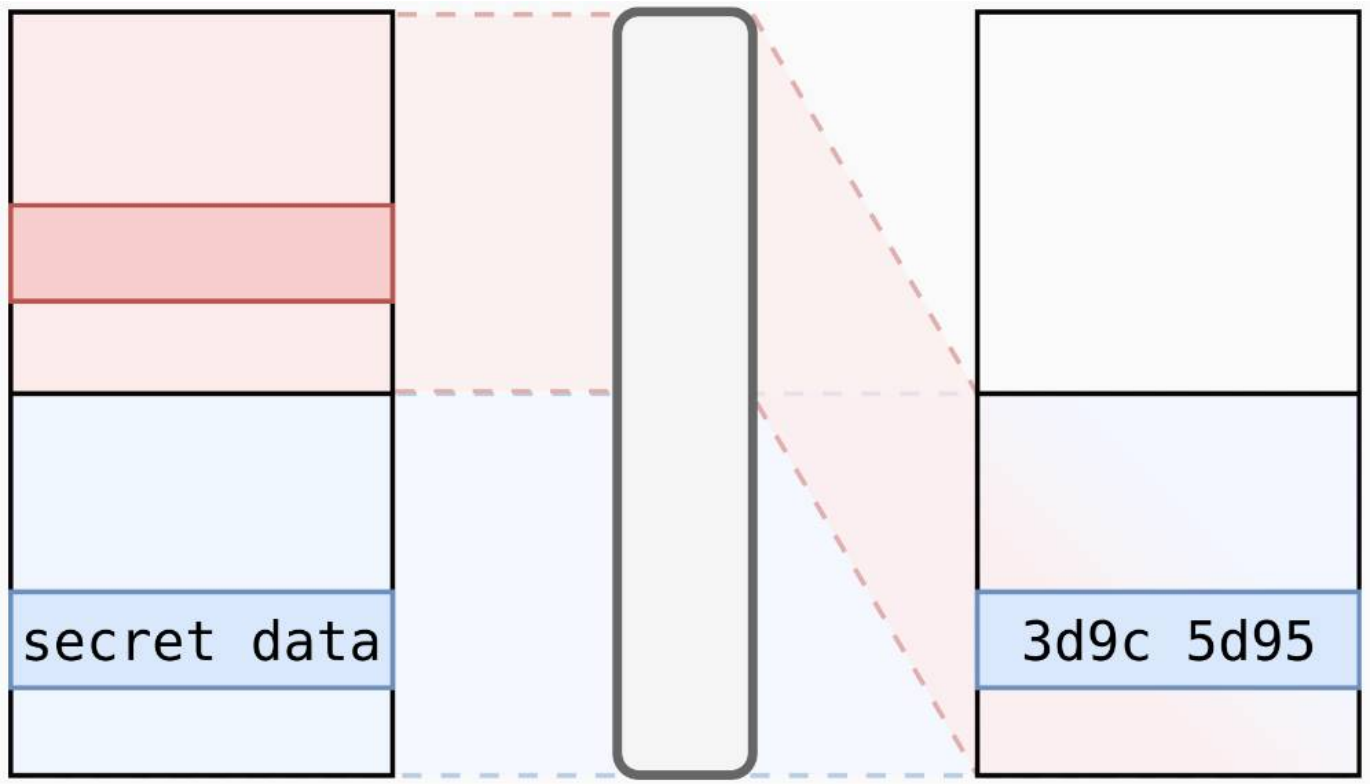
Battering RAM: Breaking Intel Scalable SGX Memory Encryption



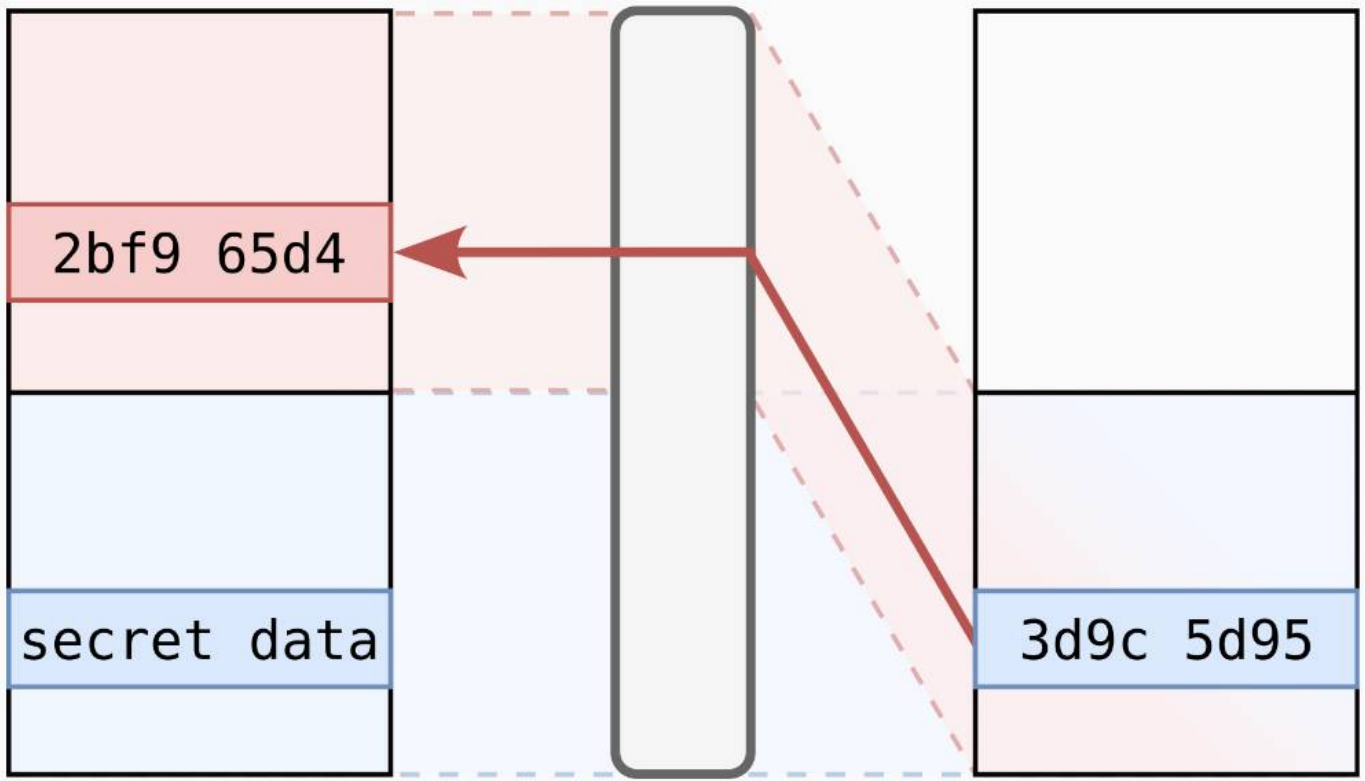
Battering RAM: Breaking Intel Scalable SGX Memory Encryption



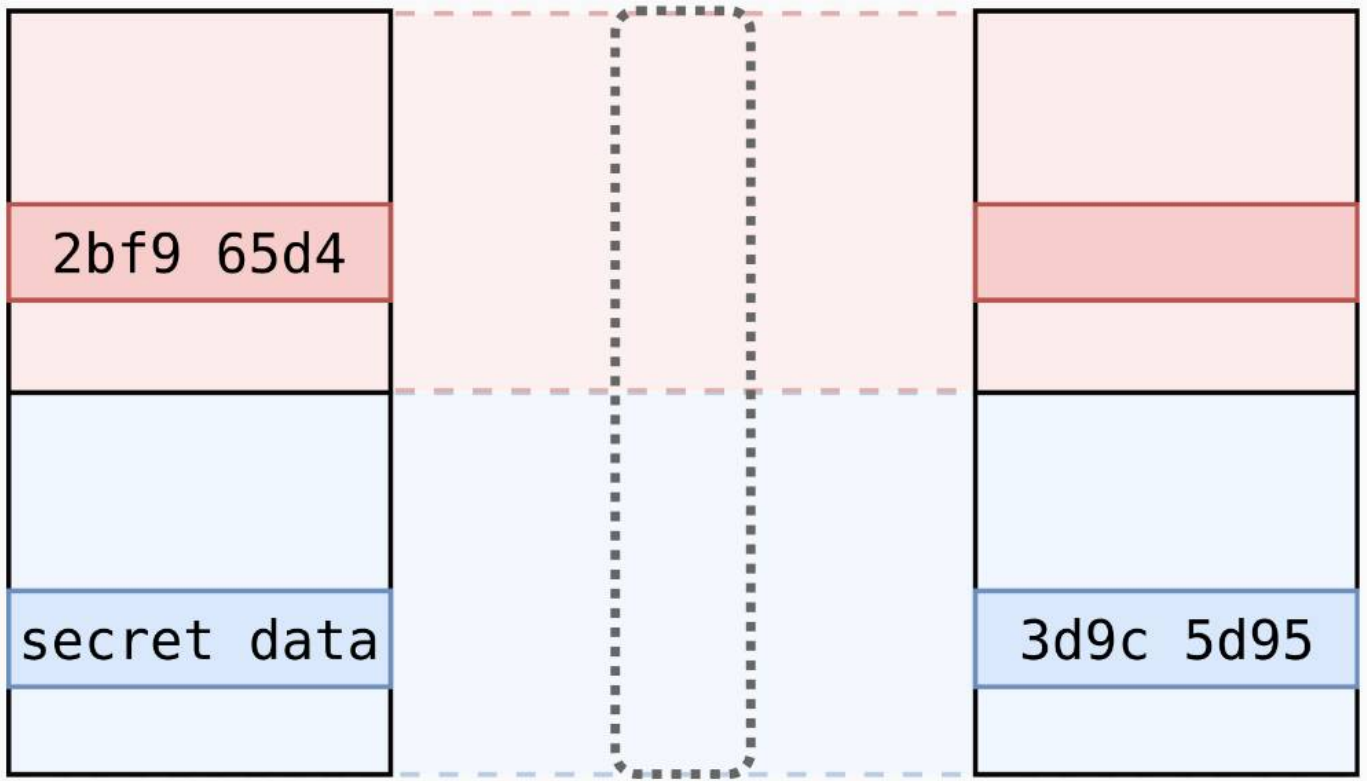
Battering RAM: Breaking Intel Scalable SGX Memory Encryption



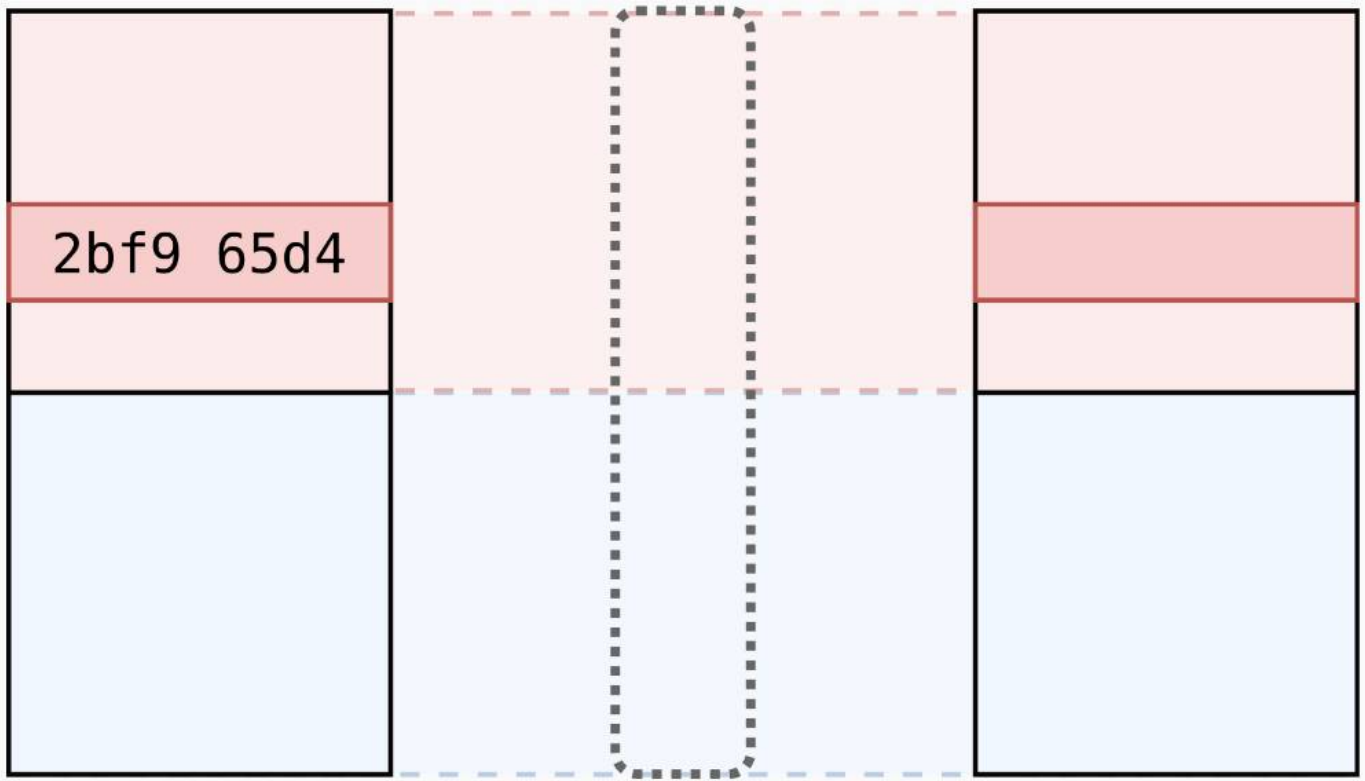
Battering RAM: Breaking Intel Scalable SGX Memory Encryption



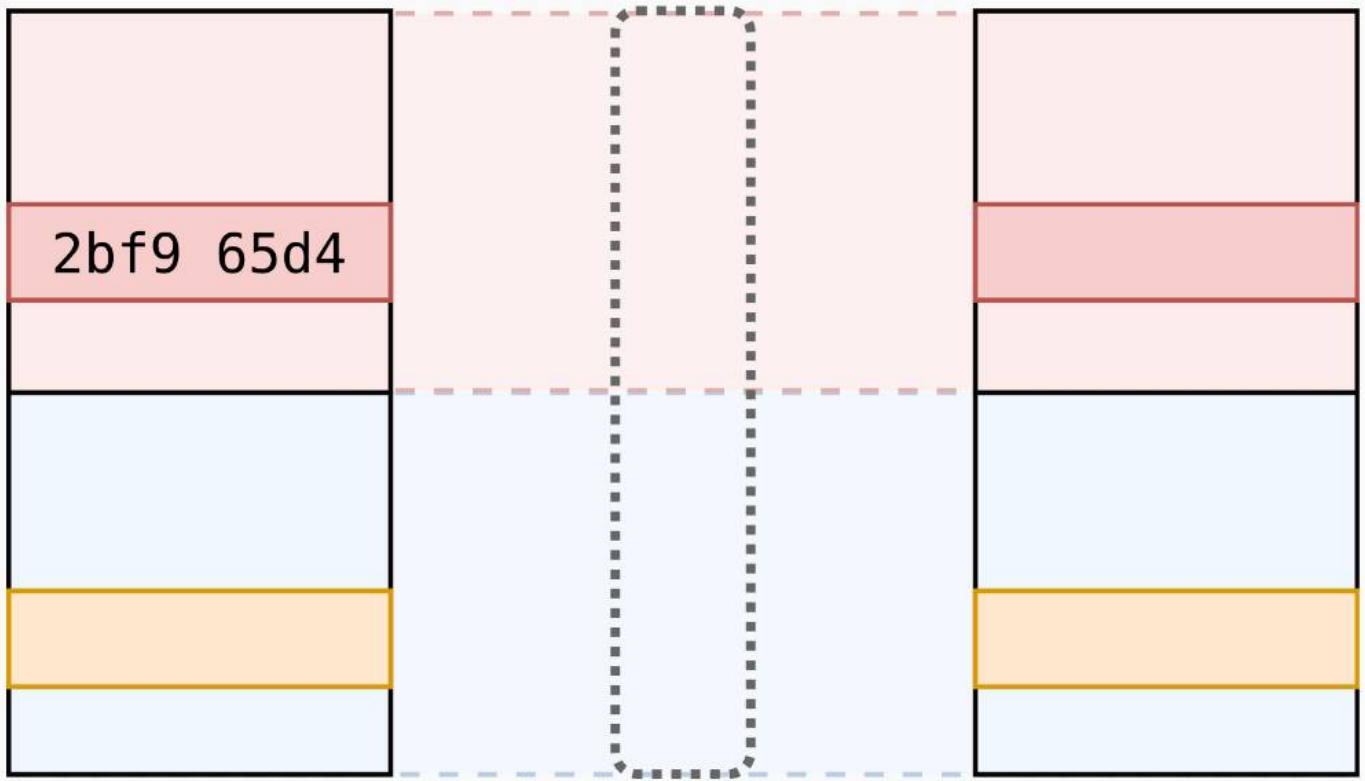
Battering RAM: Breaking Intel Scalable SGX Memory Encryption



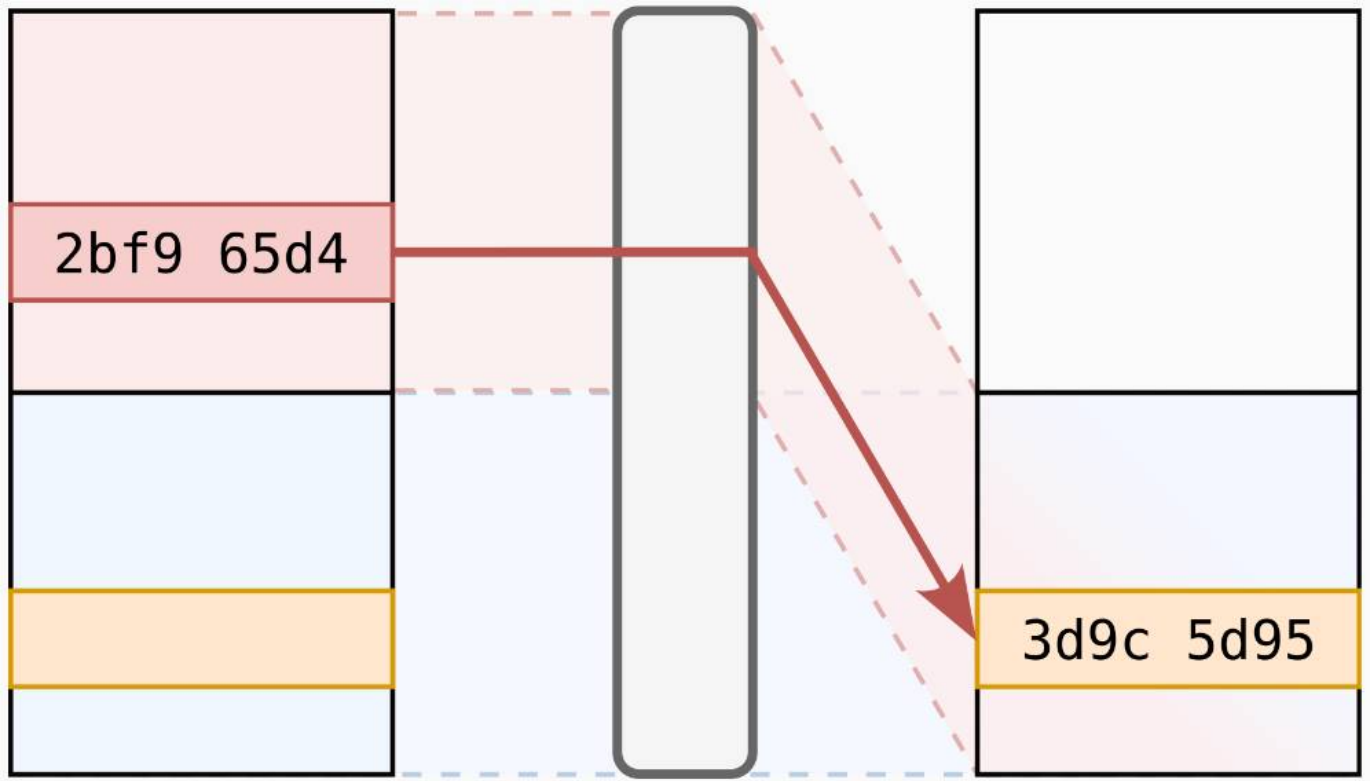
Battering RAM: Breaking Intel Scalable SGX Memory Encryption



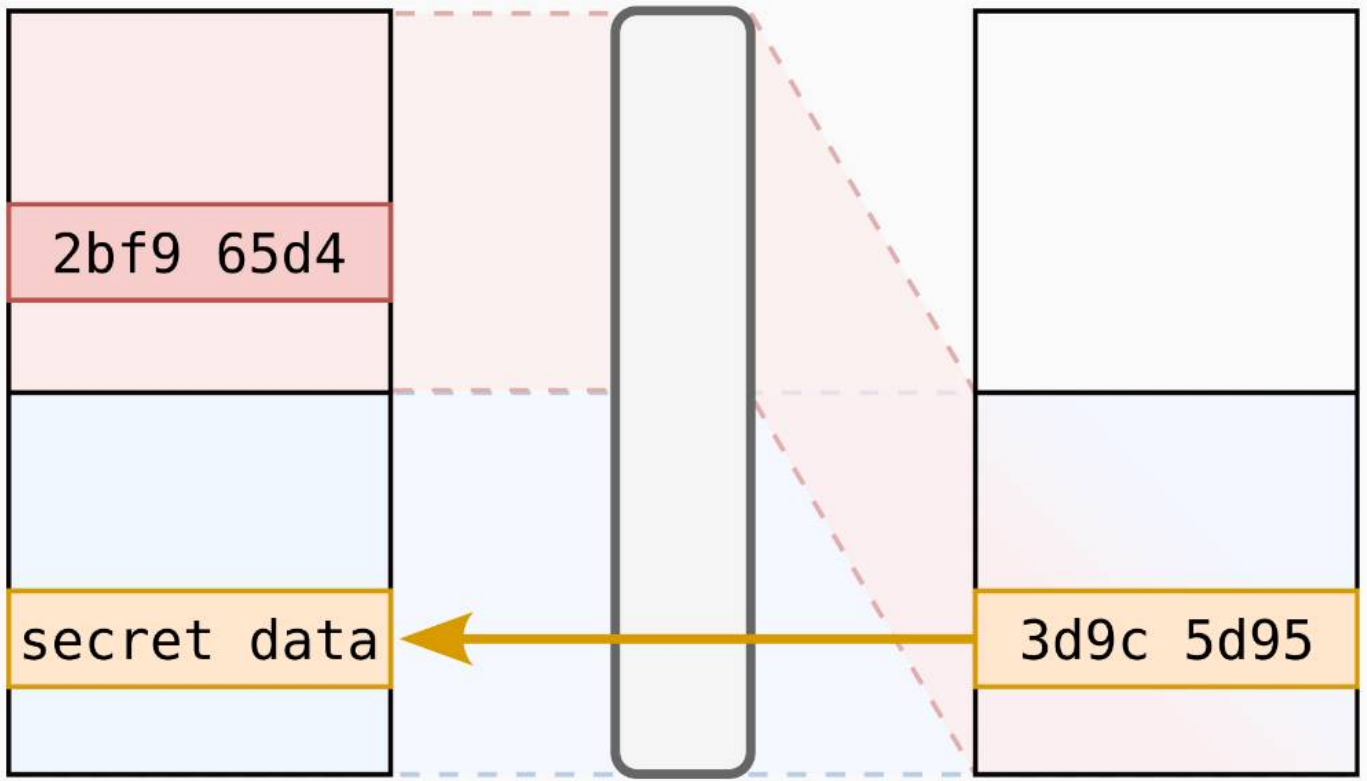
Battering RAM: Breaking Intel Scalable SGX Memory Encryption



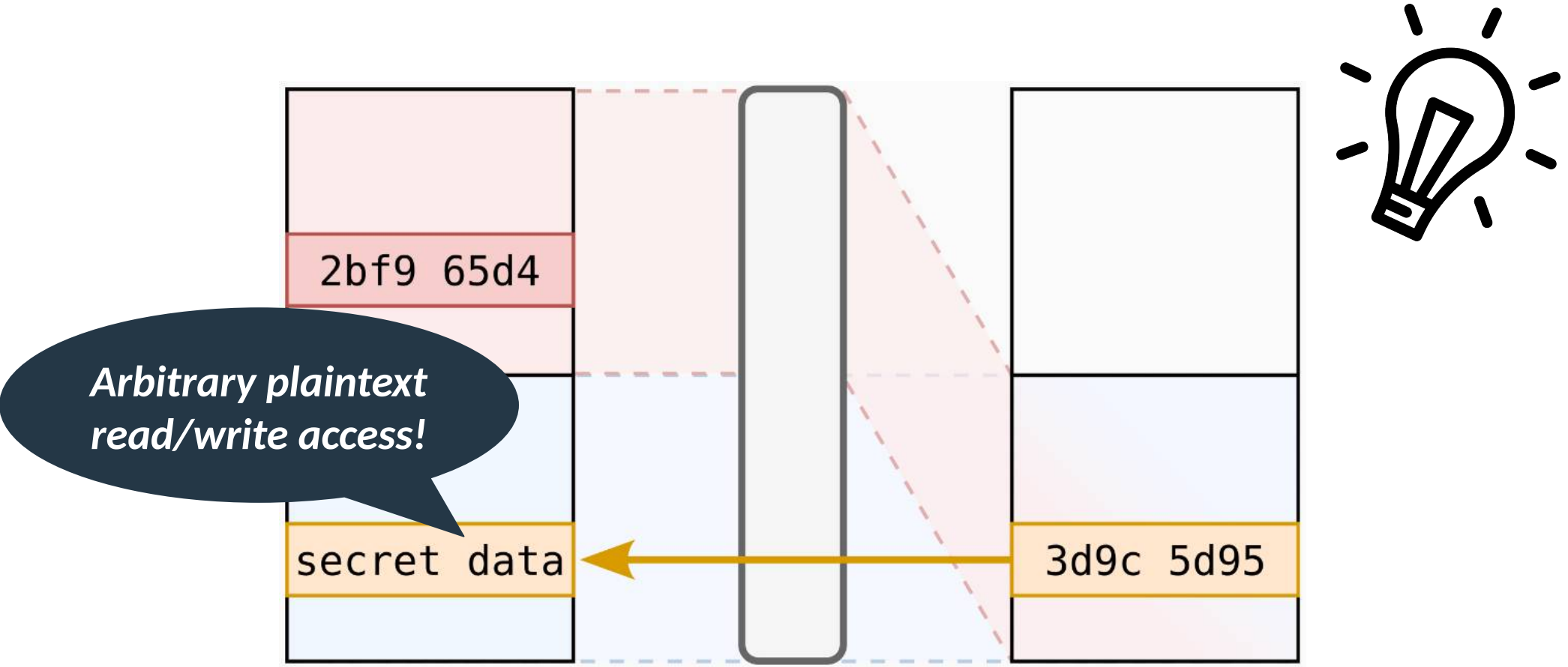
Battering RAM: Breaking Intel Scalable SGX Memory Encryption



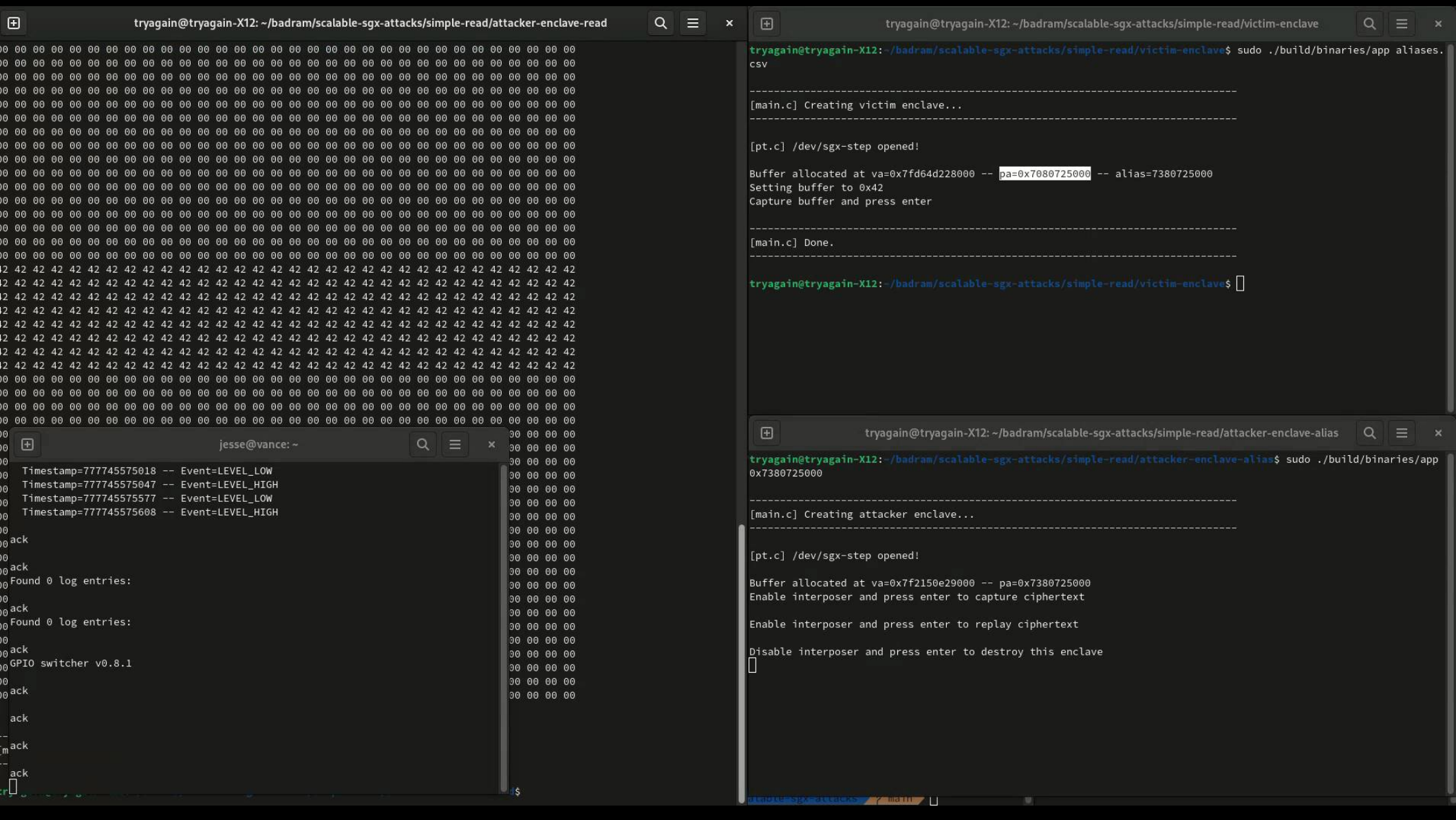
Battering RAM: Breaking Intel Scalable SGX Memory Encryption



Battering RAM: Breaking Intel Scalable SGX Memory Encryption




Demo
Arbitrary plaintext access on Intel Scalable SGX


tryagain@tryagain-X12: ~/badram/scalable-sgx-attacks/simple-read/attacker-enclave-read
tryagain@tryagain-X12: ~/badram/scalable-sgx-attacks/simple-read/victim-enclave
tryagain@tryagain-X12:~/badram/scalable-sgx-attacks/simple-read/victim-enclave$ sudo ./build/binaries/app aliases.csv
[main.c] Creating victim enclave...
[pt.c] /dev/sgx-step opened!
Buffer allocated at va=0x7fd64d228000 -- pa=0x7080725000 -- alias=7380725000
Setting buffer to 0x42
Capture buffer and press enter
[main.c] Done.
tryagain@tryagain-X12:~/badram/scalable-sgx-attacks/simple-read/victim-enclave$
jesse@vance: ~
Timestamp=777745575018 -- Event=LEVEL_LOW
Timestamp=777745575047 -- Event=LEVEL_HIGH
Timestamp=777745575577 -- Event=LEVEL_LOW
Timestamp=777745575608 -- Event=LEVEL_HIGH
Found 0 log entries:
Found 0 log entries:
GPIO switcher v0.8.1
tryagain@tryagain-X12: ~/badram/scalable-sgx-attacks/simple-read/attacker-enclave-alias
tryagain@tryagain-X12:~/badram/scalable-sgx-attacks/simple-read/attacker-enclave-alias$ sudo ./build/binaries/app 0x7380725000
[main.c] Creating attacker enclave...
[pt.c] /dev/sgx-step opened!
Buffer allocated at va=0x7f2150e29000 -- pa=0x7380725000
Enable interposer and press enter to capture ciphertext
Enable interposer and press enter to replay ciphertext
Disable interposer and press enter to destroy this enclave

ars TECHNICA AI BIZ & IT CARS CULTURE GAMING HEALTH POLICY SCIENCE SECURITY SPACE TECH FORUM SUBSCRIBE SIGN IN

Intel and AMD trusted enclaves, a foundation for network security, fall to physical attacks

The chipmakers say physical attacks aren't in the threat model. Many users didn't get the memo.

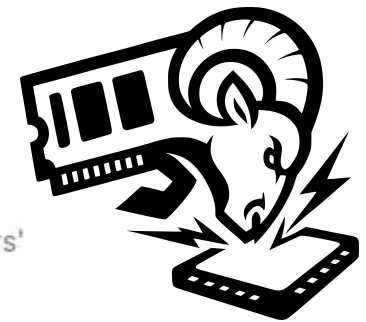
DAN GOODIN – 30 SEPT 2025 22:25 67

The Hacker News

Home Newsletter

Cheap Hardware Module Bypasses AMD, Intel Memory Encryption

Researchers built an inexpensive device that circumvents chipmakers' confidential computing protections and reveals weaknesses in scalable memory encryption.



New $50 Battering RAM Attack Breaks Intel and AMD Cloud Security Protections

CLOUD SECURITY

Battering RAM Attack Breaks Intel and AMD Security Tech With $50 Device

Intel and AMD say the research is not in scope of their threat model because the attack requires physical access to a device.

By Eduard Kovacs | October 1, 2025 (4:50 AM ET)

🌍 https://batteringram.eu/

SEV-SNP Physical Memory Aliasing

AMD ID: AMD-SB-3024
Potential Impact: N/A

Summary

Researchers have reported a method for privileged attackers with physical access to a motherboard to potentially compromise confidentiality and integrity of AMD Secure Encrypted Virtualization – Secure Nesting Paging (SEV-SNP) guests.

AMD does not plan to release any mitigations in response to this report because the reported exploit is outside the scope of the published threat model for SEV-SNP, as detailed in Table 1 of the AMD SEV-SNP technical paper.

https://www.amd.com/en/resources/product-security/bulletin/amd-sb-3024.html

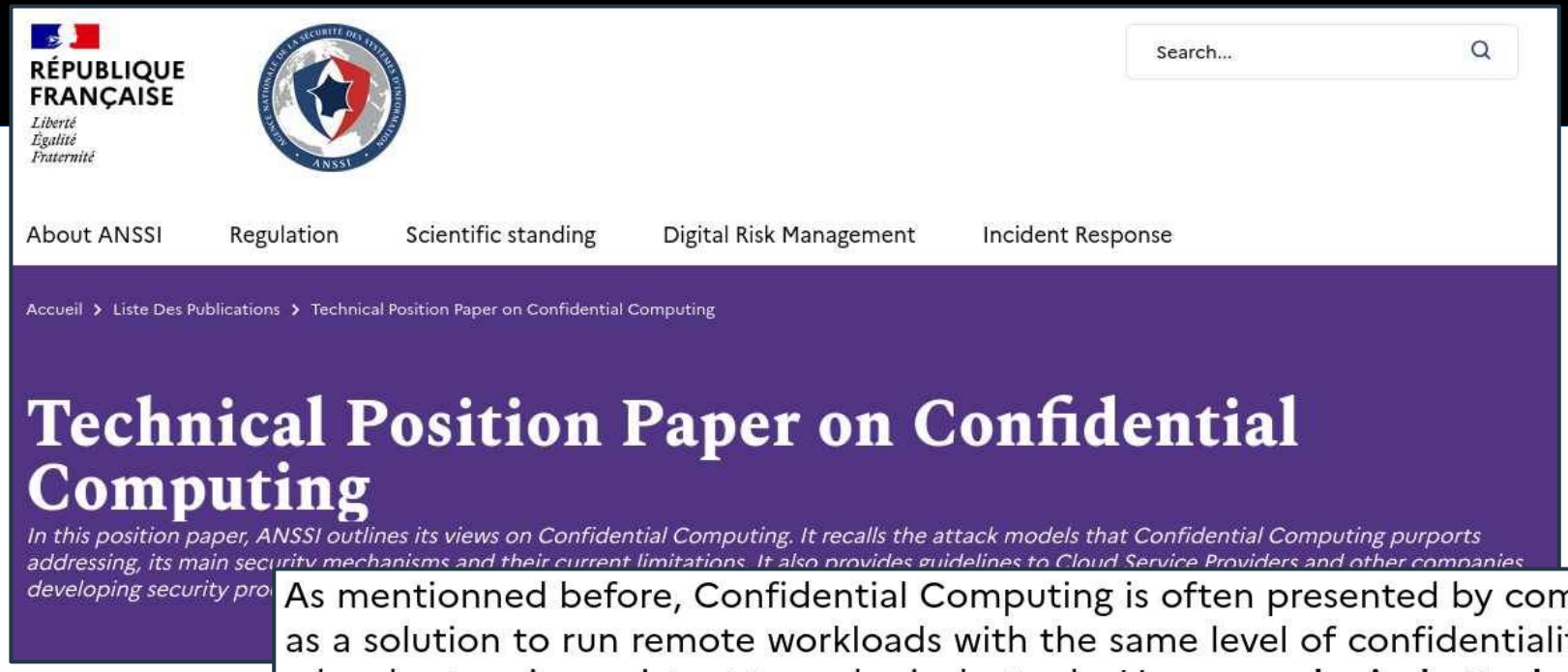
More Information on Encrypted Memory Frameworks for Intel Confidential Computing

ID	Updated	Version	
865767	10/27/2025	1.0	Public

In the *Battering RAM* paper, researchers from KU Leuven and University of Birmingham developed a custom interposer to actively alias memory and gain arbitrary read/write access into Intel SGX-protected memory.

Both research teams assume a physical adversary has direct access to the hardware with a memory bus interposer. Both methods can then be used to attack Intel SGX-protected assets, including Intel SGX attestation keys. In a separate disclosure to Intel, Fortanix provided a potential attack that requires a replay-capable physical interposer. Such attacks are outside the scope of the boundary of protection offered by Advanced Encryption Standard-XEX-based Tweaked Codebook Mode with Ciphertext Stealing (AES-XTS) based memory encryption, as originally stated in the 2021 Intel publication Supporting Intel® SGX on Multi-socket Platforms. As it provides limited confidentiality protection, and no integrity or anti-replay protection against attackers with physical capabilities, Intel does not plan to issue a CVE.

https://www.intel.com/content/www/us/en/developer/articles/news/more-information-encrypted-memory-frameworks.html



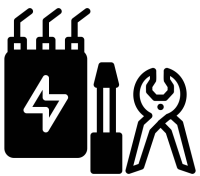
As mentionned before, Confidential Computing is often presented by commercial providers as a solution to run remote workloads with the same level of confidentiality and integrity as a local setup, *i.e.* resistant to a physical attack. However, **physical attacks are explicitly out-of-scope of the security target defined by hardware vendors**. This means in particular that if a user is concerned about a cloud-provider conducting targeted attacks, instead of relying on a Confidential Computing approach they need to switch to a cloud-provider they trust, *i.e.* with strong counterparts or control capabilities, or use their own hardware with physical security protection measures. Likewise, the security of Confidential Computing assumes an uncompromised Manufacturer TCB: manufacturer and supply-chain attackers, including state-level ones, are thus explicitly out-of-scope.

https://cyber.gouv.fr/en/publications/technical-position-paper-confidential-computing

Conclusions and Take-Away

1. **Confidential computing** is here to stay…

2. Challenge your **attacker models**



3. **Hardware attacks** are practical