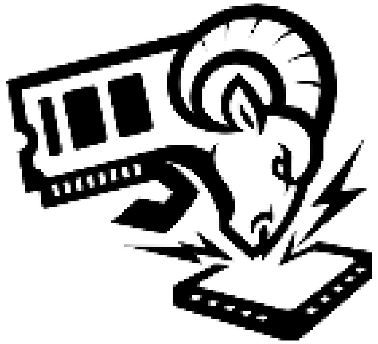
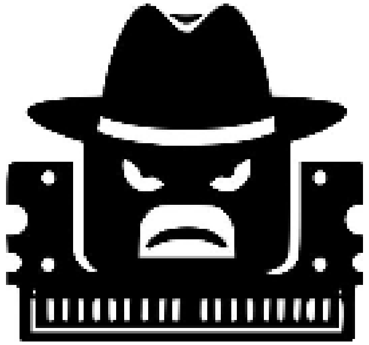




RAM Raids: Low-Cost Attacks on Encrypted Memory for Confidential Computing

Jo Van Bulck *(joint work with COSIC, Durham, Lubeck)*

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

DistriNet Reunion, Feb 5, 2026

The Big Picture: Protecting Private Data

Data in transit

Data in use

Data at rest

The Big Picture: Protecting Private Data

Data in transit

- ✓ SSL/TLS etc.

Data in use

Data at rest

- ✓ Full disk encryption

The Big Picture: Protecting Private Data

Data in transit

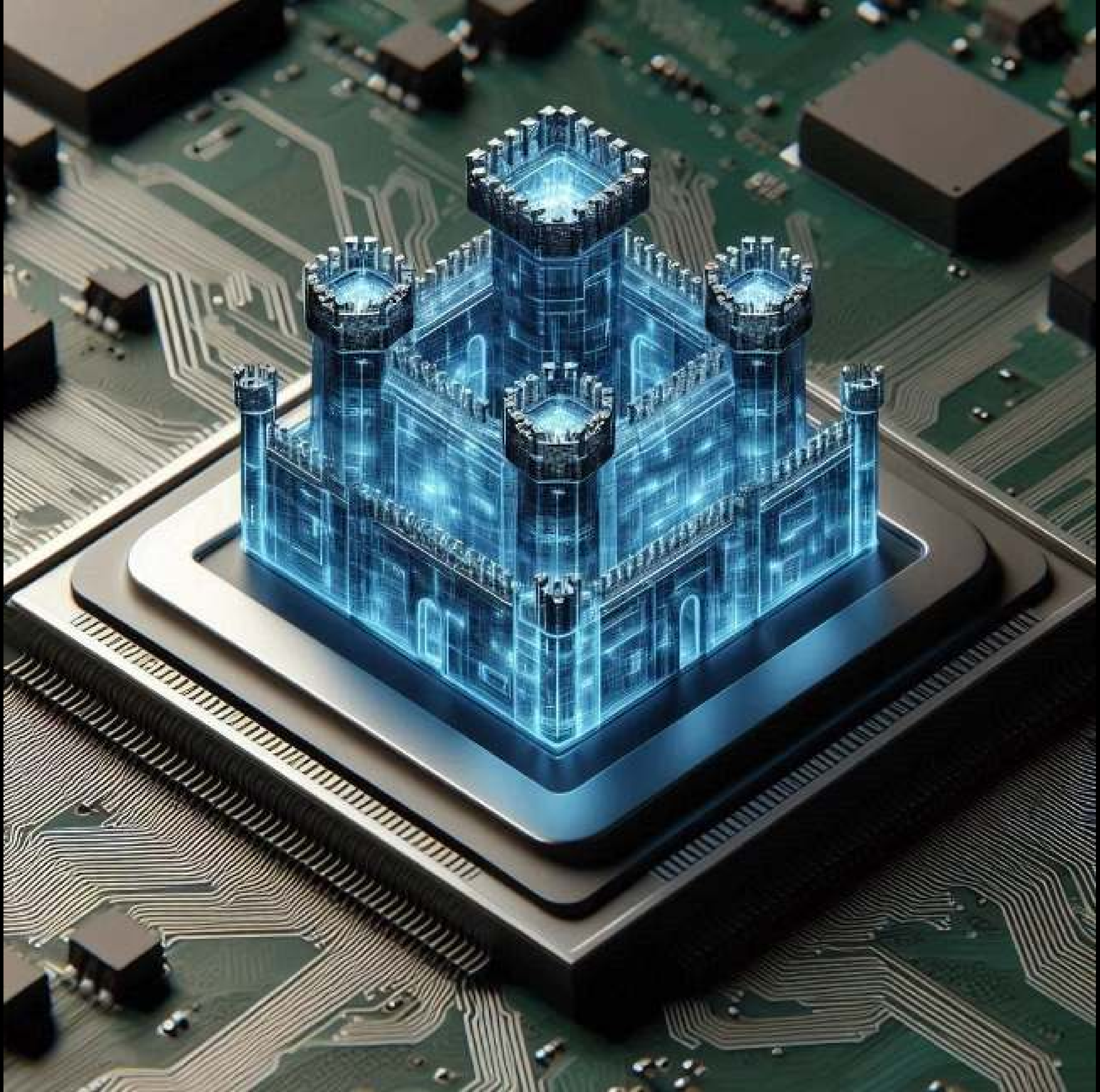
- ✓ SSL/TLS etc.

Data in use

- ? **Homomorphic encryption?**
- ? **Trusted Execution?**
  - = *Confidential Computing*
  - = *Hardware Enclaves*

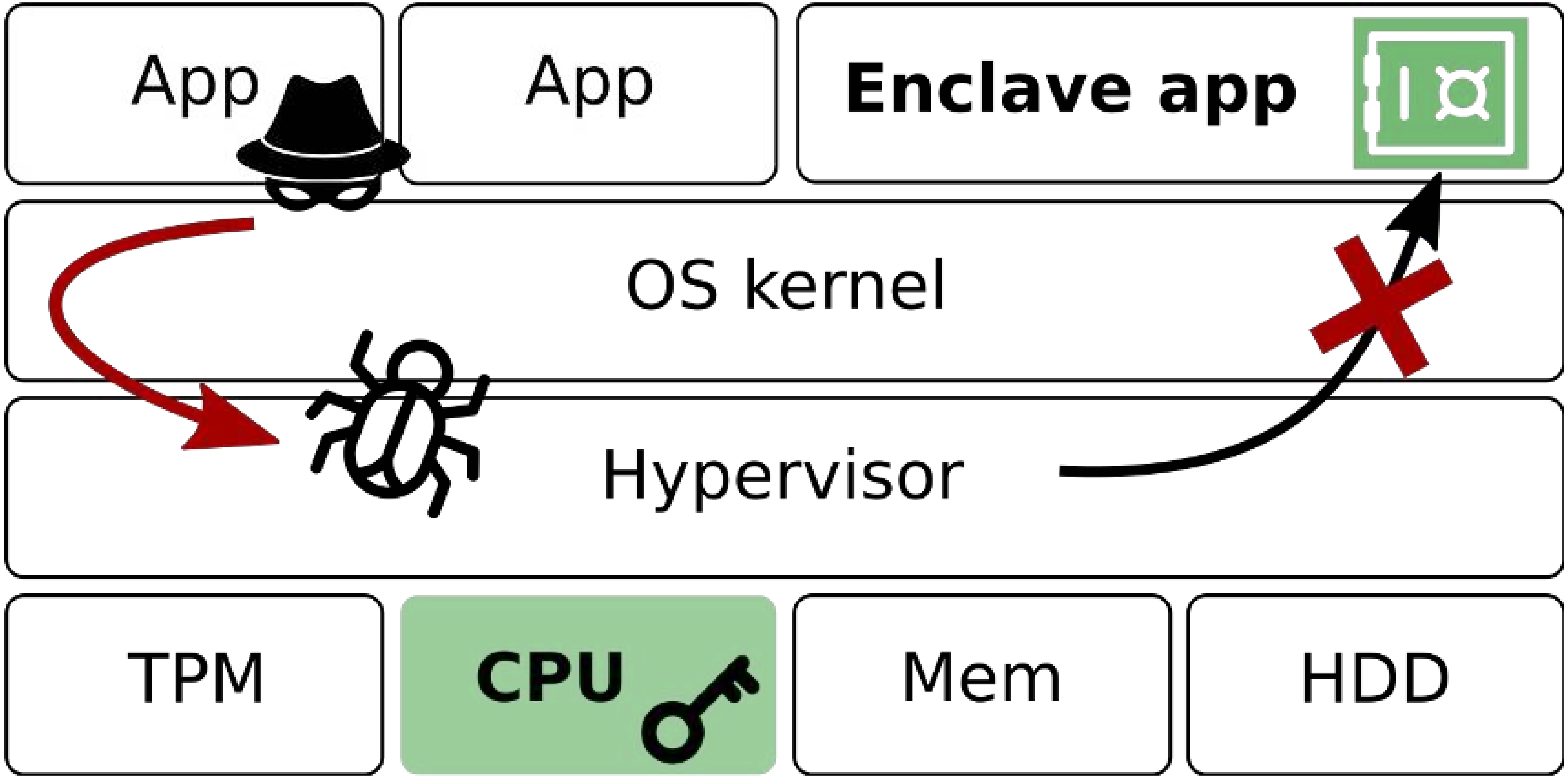
Data at rest

- ✓ Full disk encryption



DALL·E 3

Confidential Computing: Reducing Attack Surface



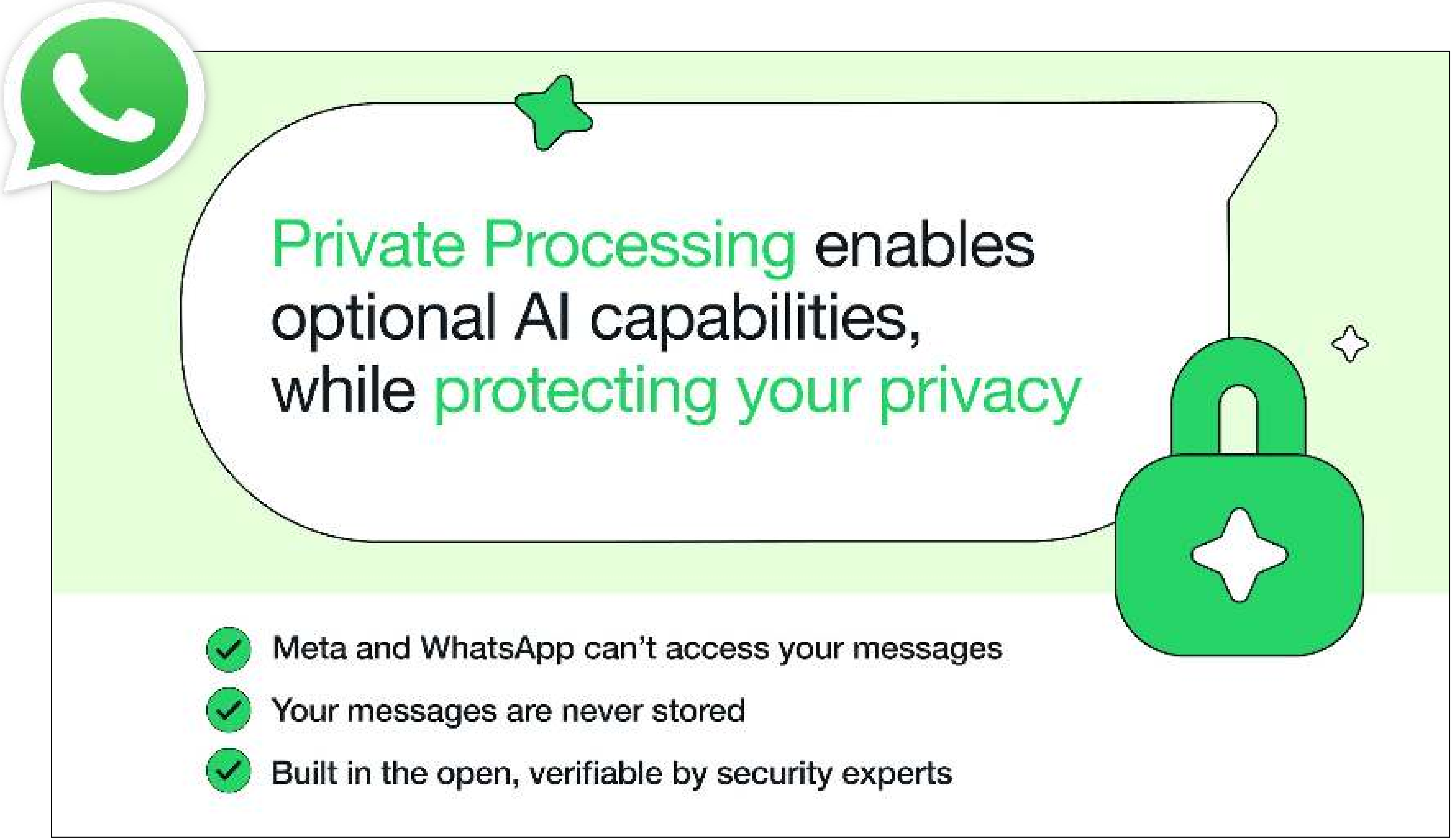
Trusted execution: Hardware-level isolation and attestation

The Rise of Confidential Computing CPU Technology

- 2004: ARM TrustZone
- 2015: **Intel Software Guard Extensions (SGX)**
- 2016: AMD Secure Encrypted Virtualization (SEV)
- 2018: IBM Protected Execution Facility (PEF)
- 2020: AMD SEV with Secure Nested Paging (SEV-SNP)
- 2022: Intel Trust Domain Extensions (TDX)
- 2023: ARM Confidential Compute Architecture (CCA)
- 2024: NVIDIA Confidential Computing

🔔 **TEEs are here to stay. . .**

Example: WhatsApp Private Processing Confidential AI

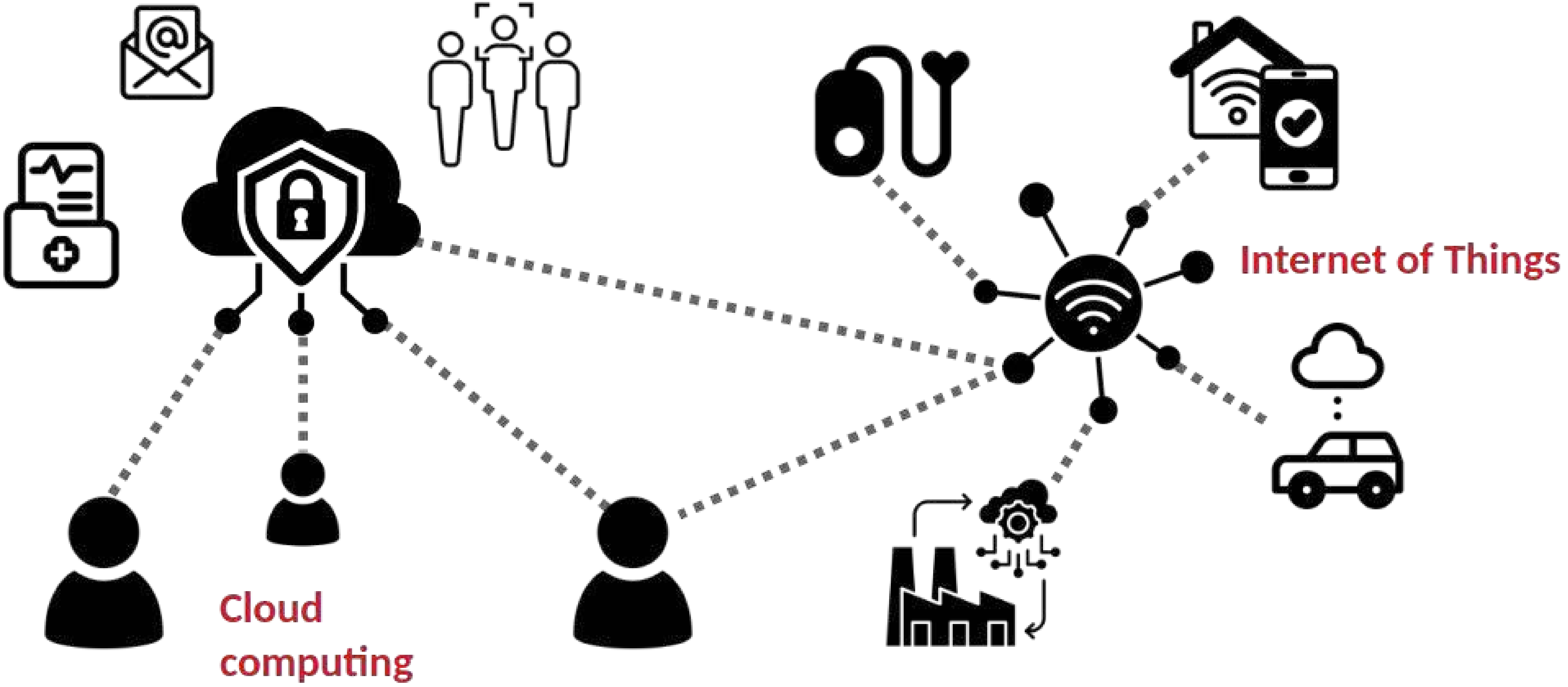


Private Processing enables optional AI capabilities, while protecting your privacy

- ✓ Meta and WhatsApp can't access your messages
- ✓ Your messages are never stored
- ✓ Built in the open, verifiable by security experts

https://engineering.fb.com/2025/04/29/security/whatsapp-private-processing-ai-tools/

“Confidential Computing Today, Just Computing Tomorrow” *

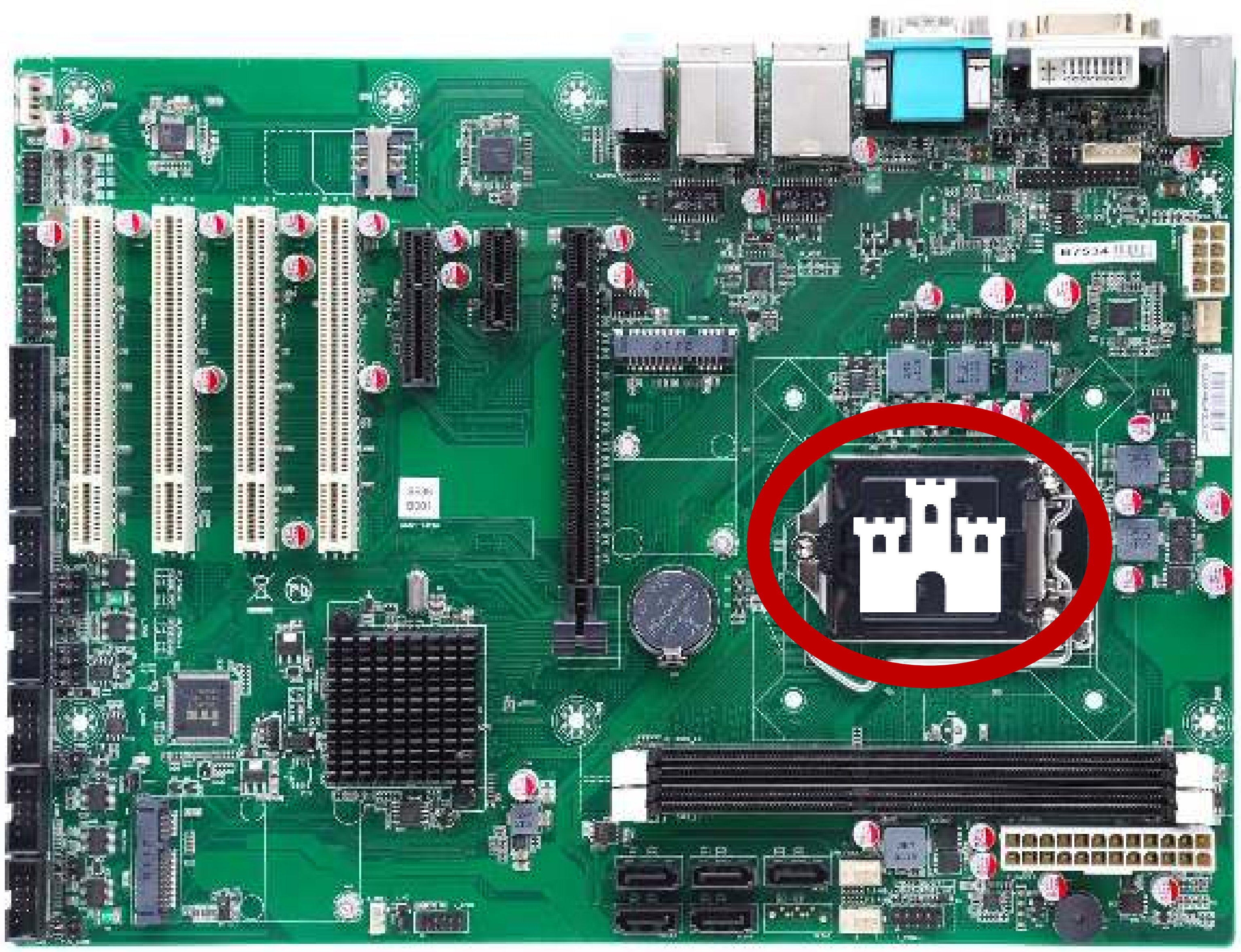


* *Mark Russinovich, CTO Microsoft Azure*

Confidential Computing: The Weakest Link?

Confidential Computing: Trust Boundary

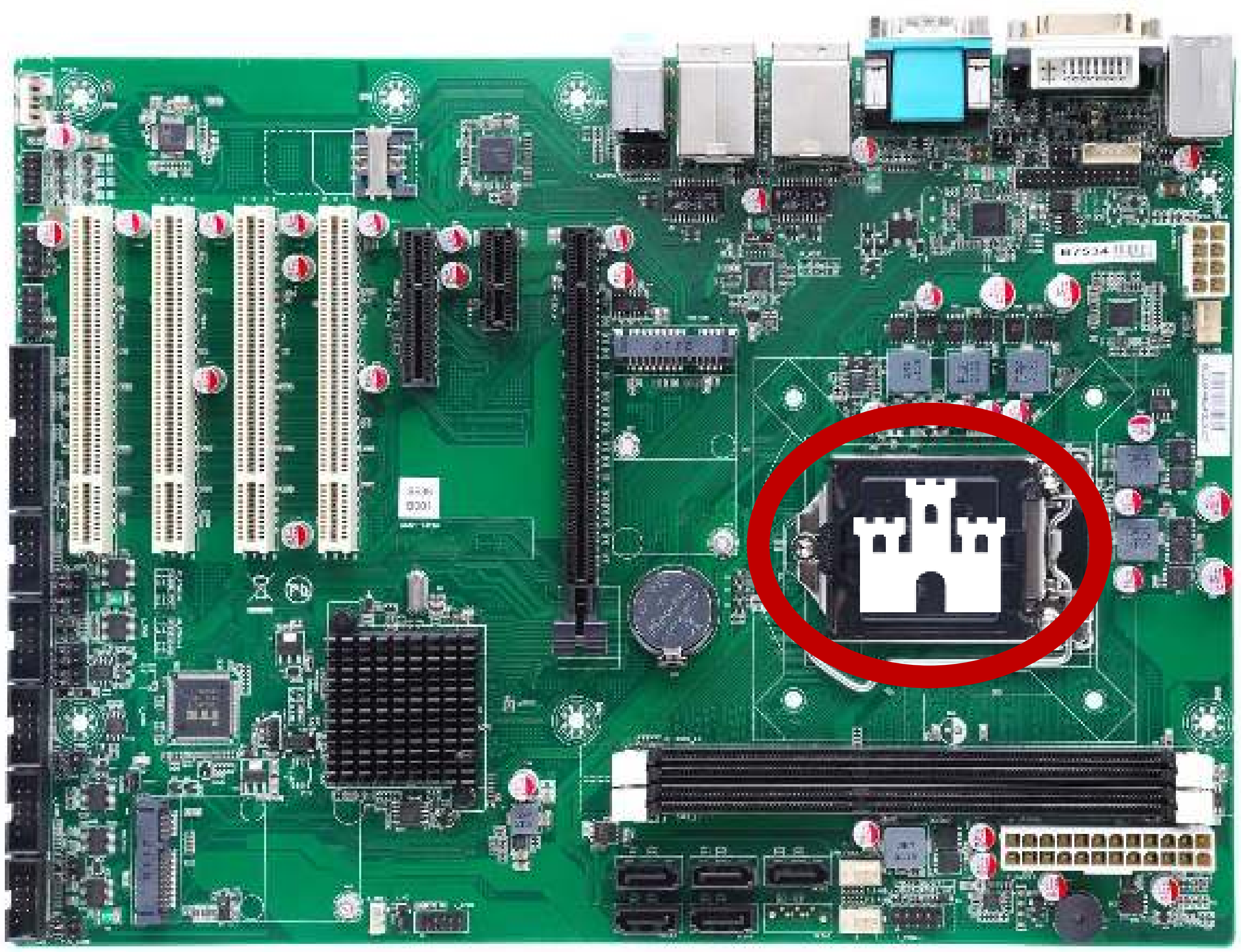
- **CPU package** = trust boundary



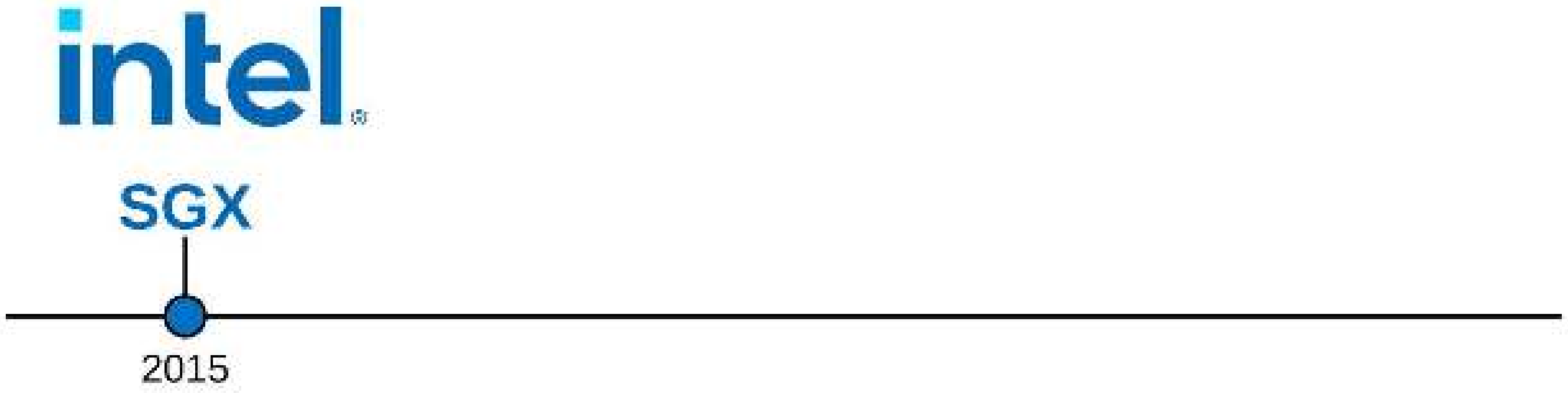
Confidential Computing: Trust Boundary

- **CPU package** = trust boundary
- **Memory encryption** to protect against physical access:

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



A Brief History of Commercial Memory Encryption

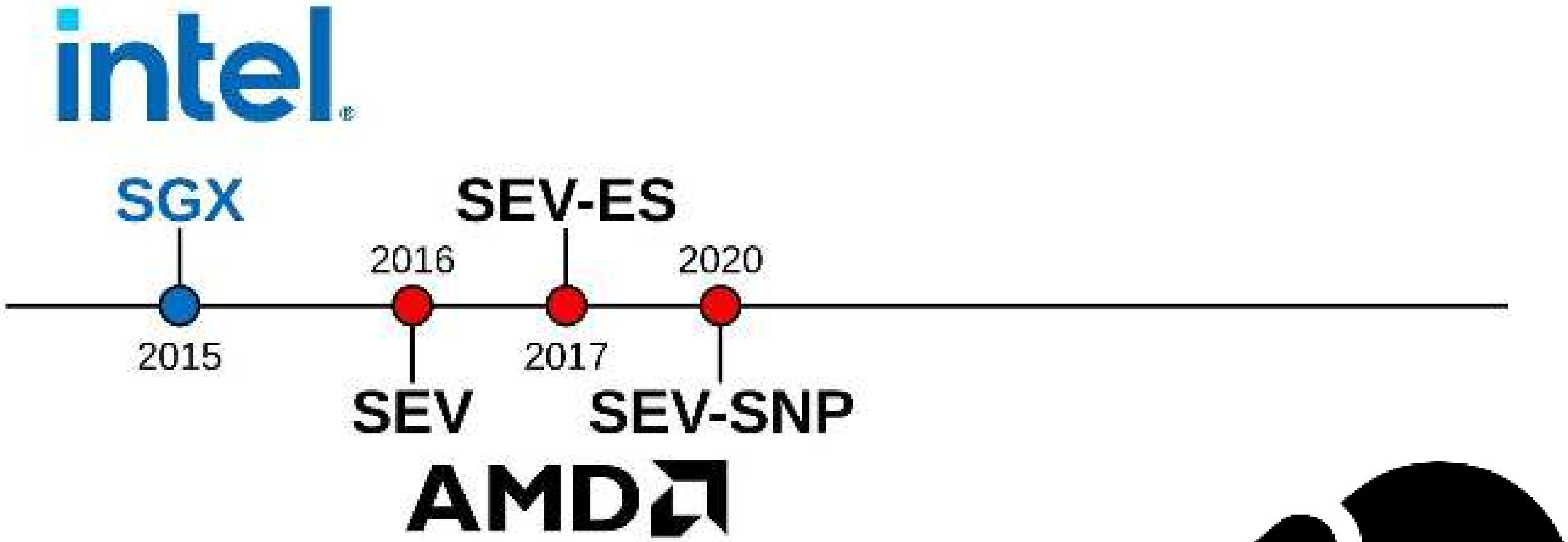


Confidentiality	🔒
Integrity	✓
Freshness	↻
Scalable	✗

🤩

👍

A Brief History of Commercial Memory Encryption



intel

SGX
2015

SEV
2016

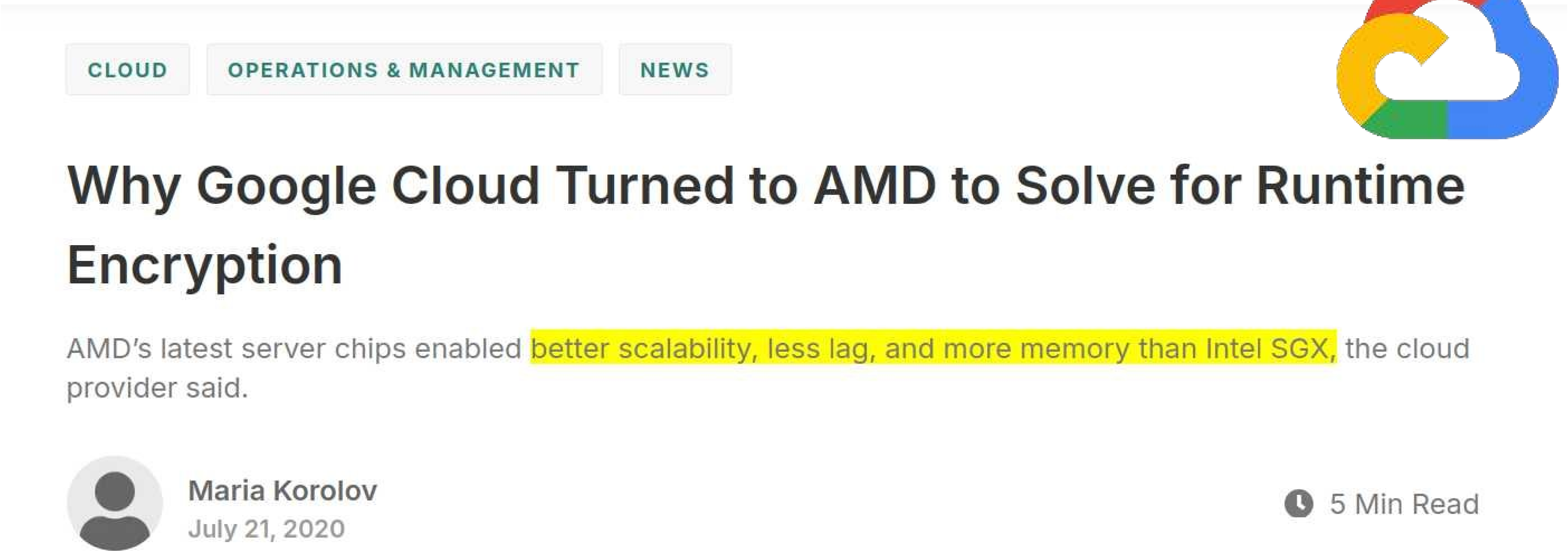
SEV-ES
2017

SEV-SNP
2020

AMD

	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

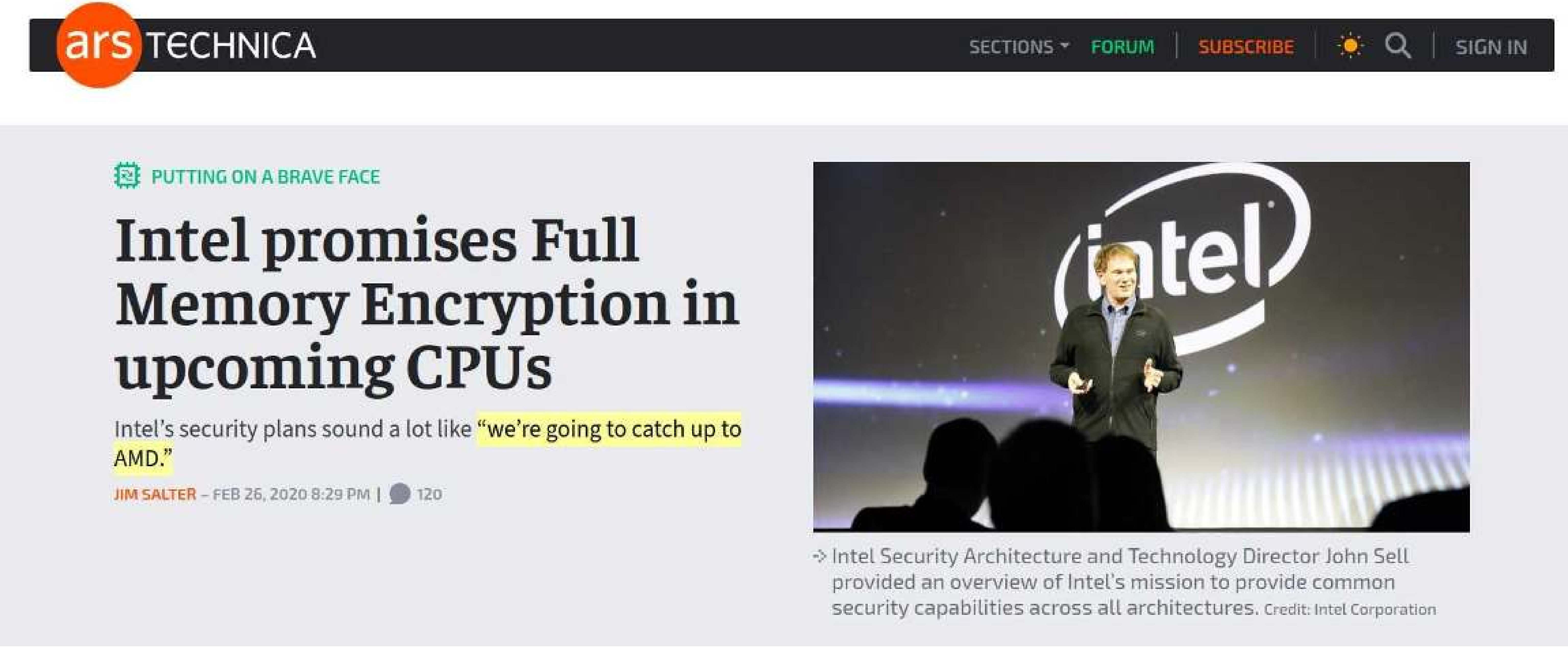
AMD's latest server chips enabled better scalability, less lag, and more memory than Intel SGX, the cloud provider said.

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



PUTTING ON A BRAVE FACE

Intel promises Full Memory Encryption in upcoming CPUs

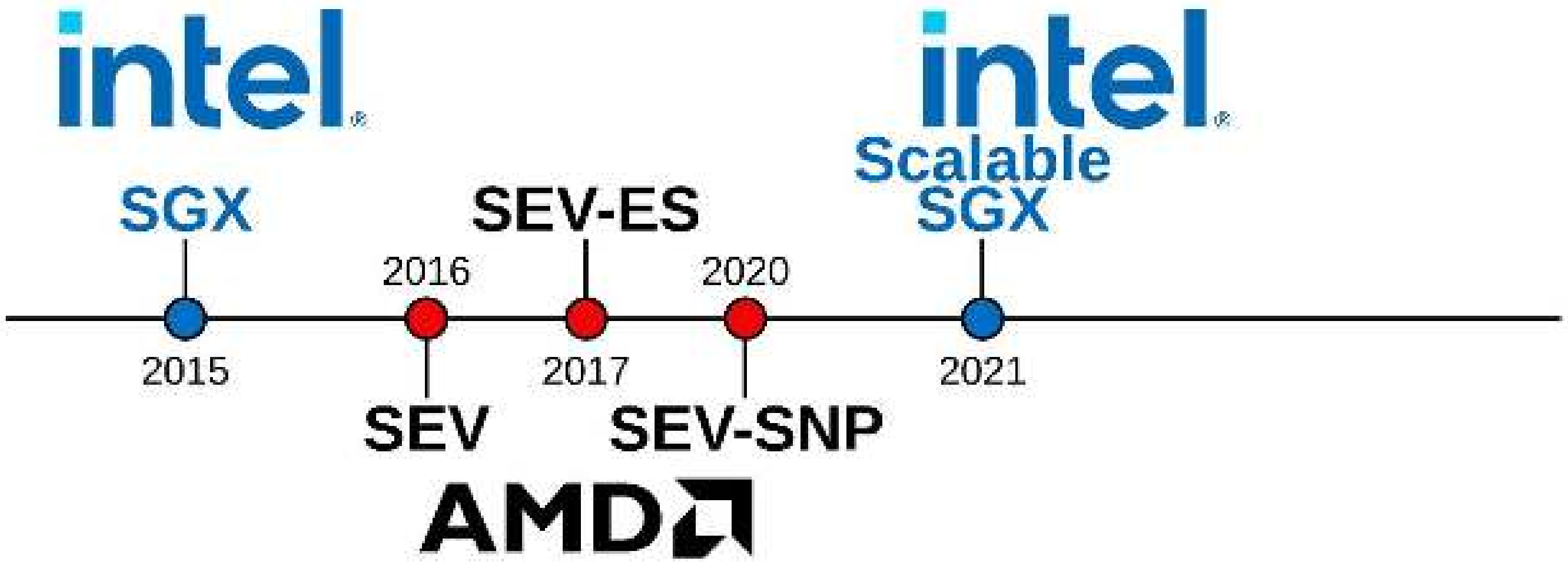
Intel's security plans sound a lot like "we're going to catch up to AMD."

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

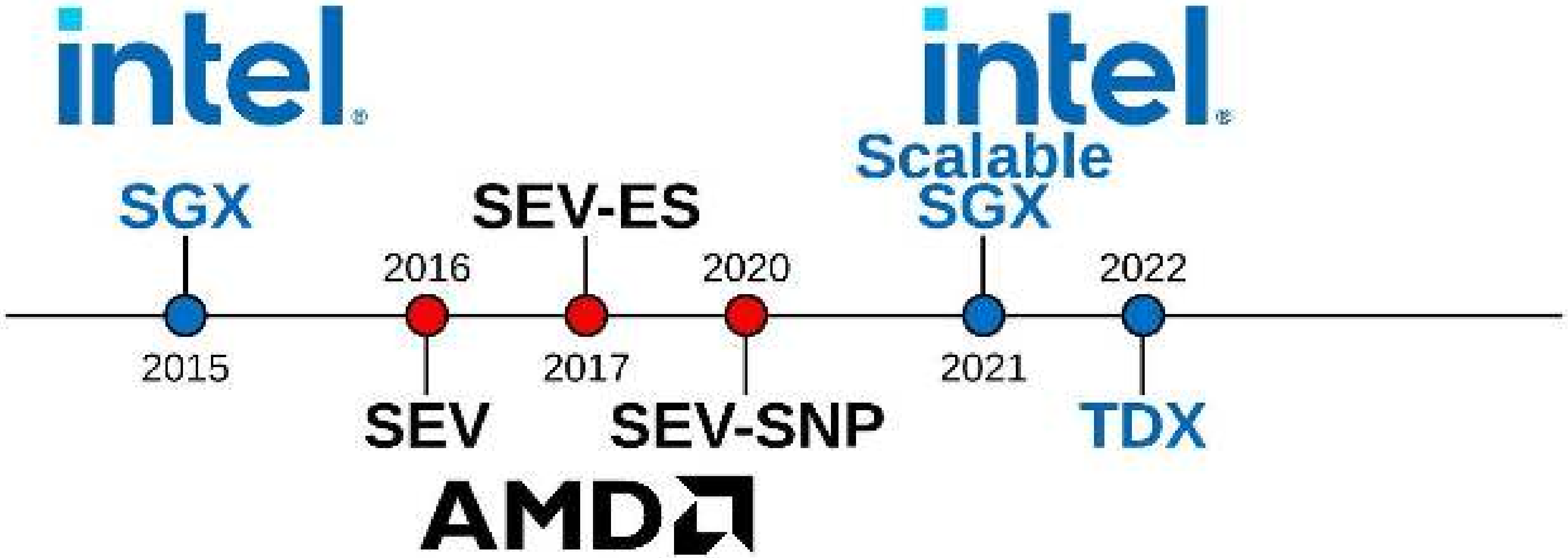
https://arstechnica.com/gadgets/2020/02/intel-promises-full-memory-encryption-in-upcoming-cpus/

A Brief History of Commercial Memory Encryption



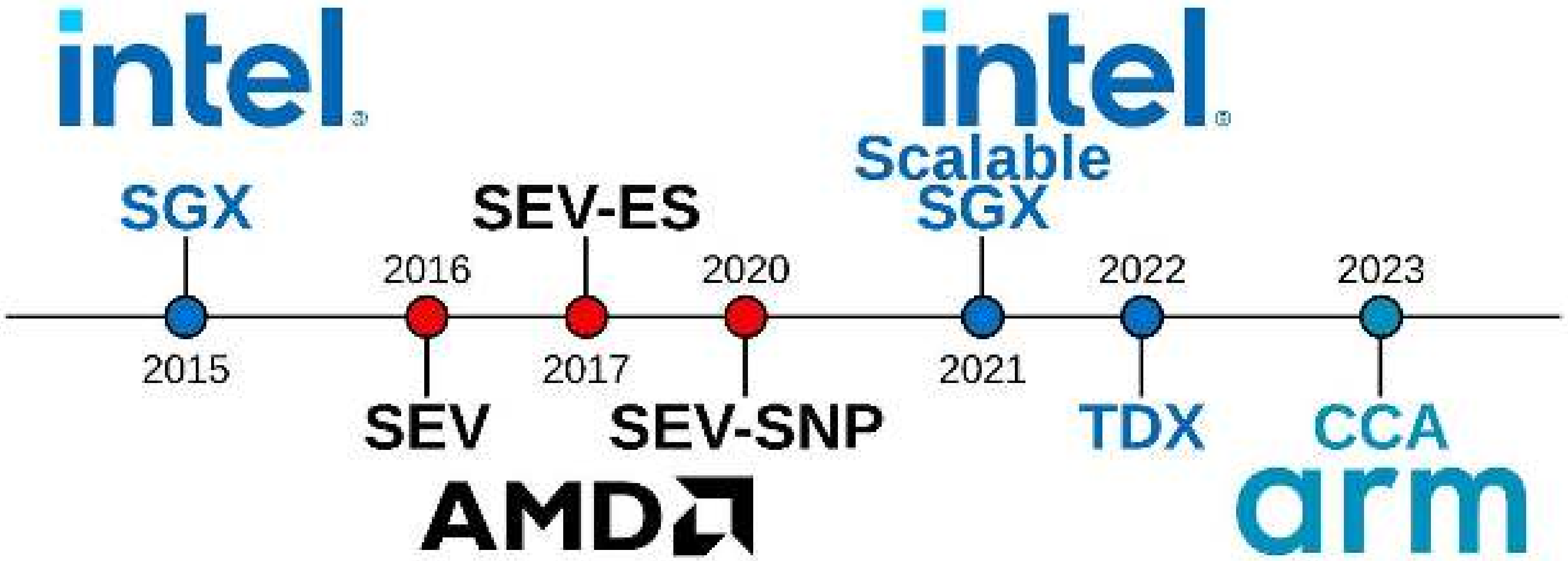
Confidentiality	🔒	🔒	🔒	🔒	🔒
Integrity	✓	✗	✗	✗	✗
Freshness	↻	✗	✗	✗	✗
Scalable	✗	↗	↗	↗	↗
	🤩	🤔	🤔	🤔	🤔

A Brief History of Commercial Memory Encryption



Confidentiality	🔒	🔒	🔒	🔒	🔒	🔒
Integrity	✓	✗	✗	✗	✗	✓
Freshness	↻	✗	✗	✗	✗	✗
Scalable	✗	⤢	⤢	⤢	⤢	⤢
	🤩	🤔	🤔	🤔	🤔	🤔

A Brief History of Commercial Memory Encryption



intel

SGX 2015

SEV 2016

SEV-ES 2017

SEV-SNP 2020

AMD

intel

Scalable SGX 2021

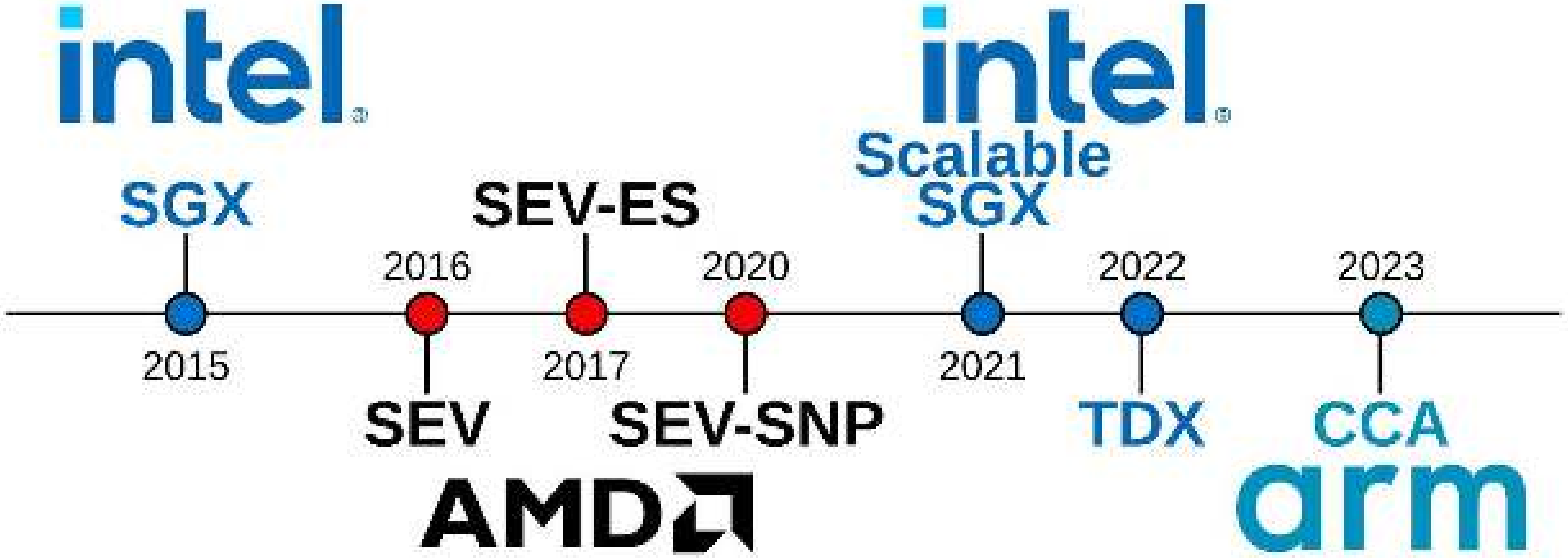
TDX 2022

CCA 2023

arm

Confidentiality	🔒	🔒	🔒	🔒	🔒	🔒	🔒
Integrity	✓	✗	✗	✗	✗	✓	✗
Freshness	↻	✗	✗	✗	✗	✗	✗
Scalable	✗	⤢	⤢	⤢	⤢	⤢	⤢
	🤩	🤔	🤔	🤔	🤔	🤔	🤔

A Brief History of Commercial Memory Encryption



intel

2015 SGX

2016 SEV

2017 SEV-ES

2020 SEV-SNP

AMD

intel

2021 Scalable SGX

2022 TDX

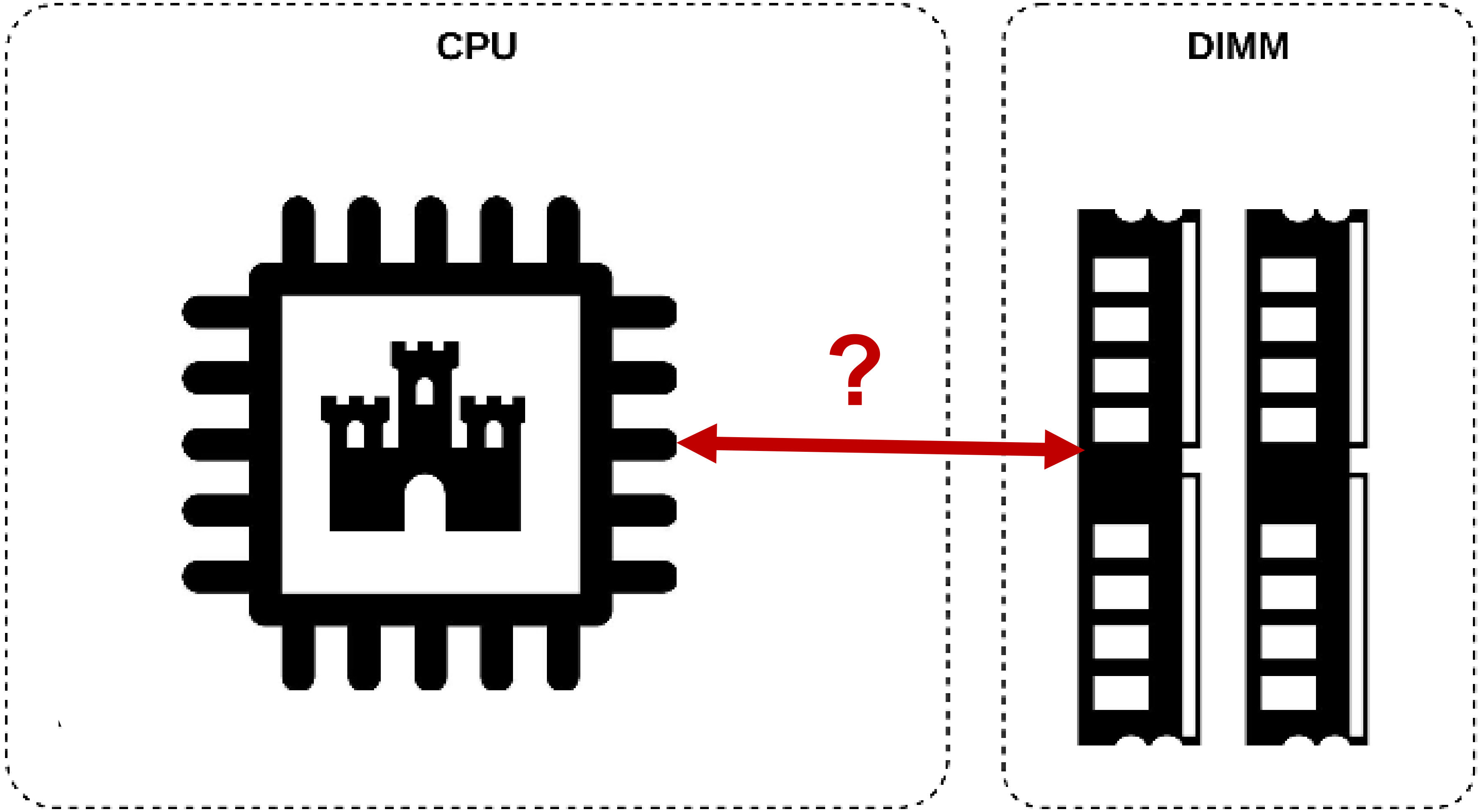
2023 CCA

arm

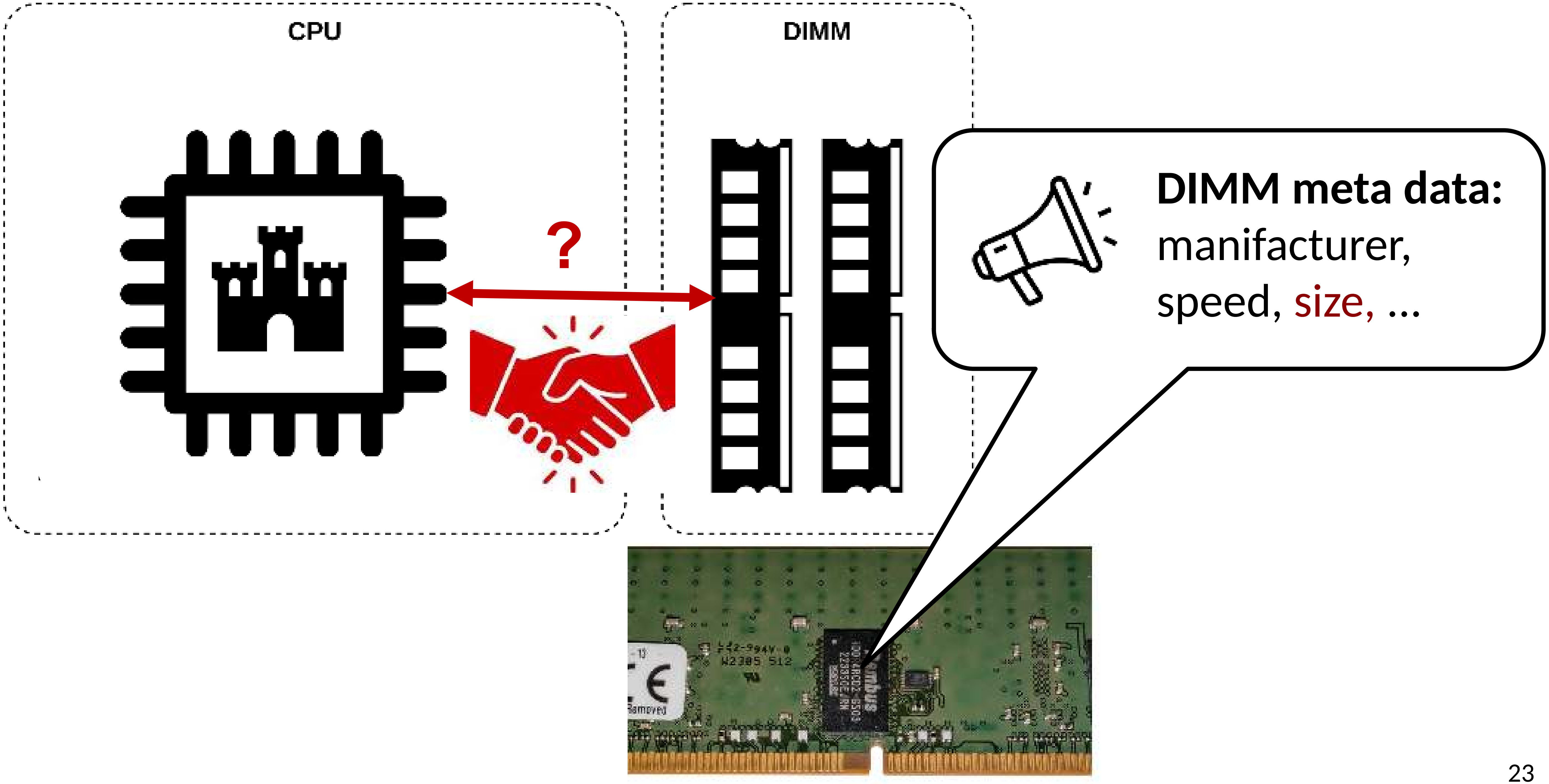
	SGX	SEV	SEV-ES	SEV-SNP	Scalable SGX	TDX	CCA
Confidentiality	🔒	🔒	🔒	🔒	🔒	🔒	🔒
Integrity	✓	✗	✗	✗	✗	✓	✗
Freshness	↻	✗	✗	✗	✗	✗	✗
Scalable	✗	↗	↗	↗	↗	↗	↗
	🤩	🤔	🤔	🤔	🤔	🤔	🤔

AW, MAN, WHERE DO I BEGIN?

Background: Memory Initialization

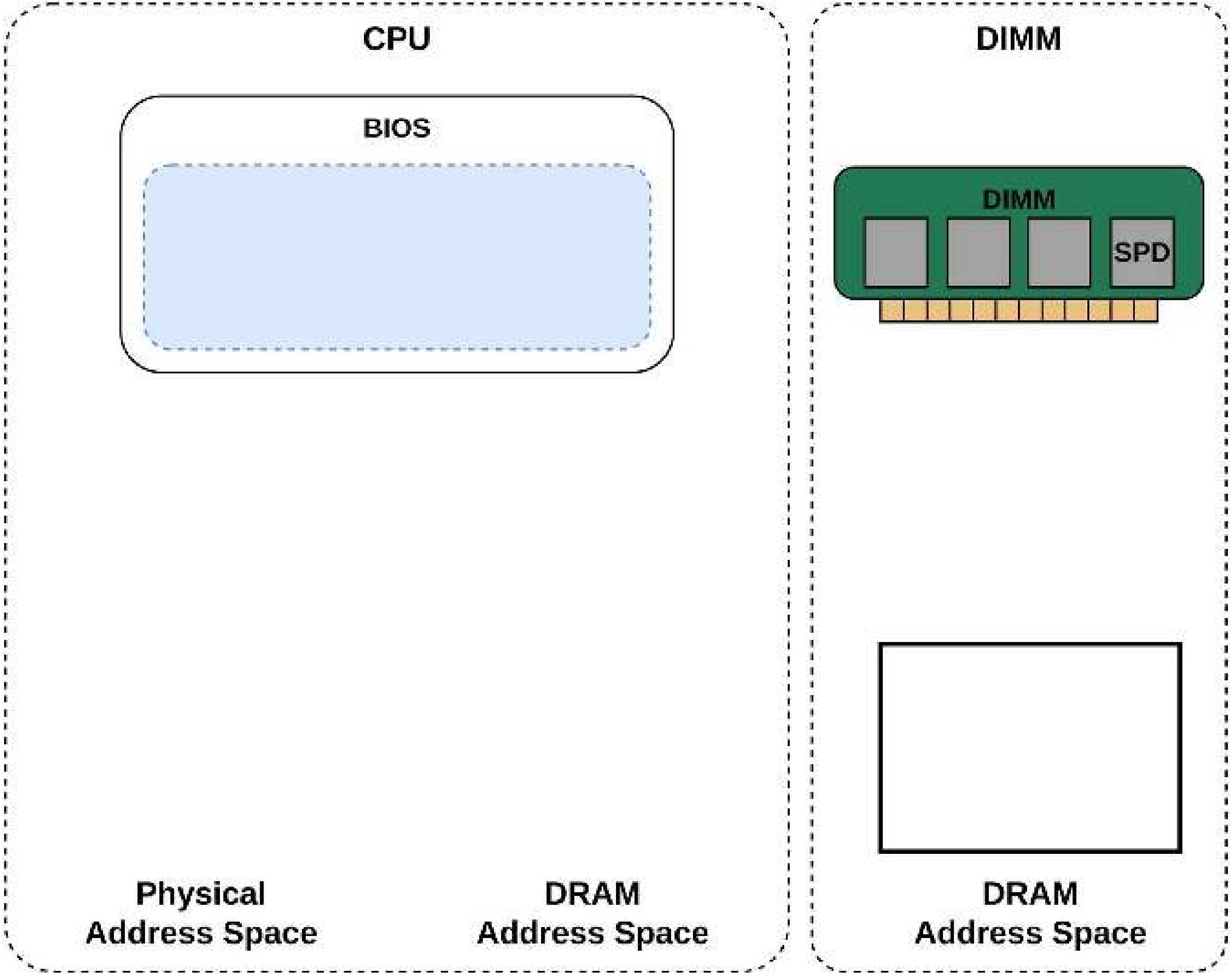


Background: Memory Initialization - Serial Presence Detect (SPD)

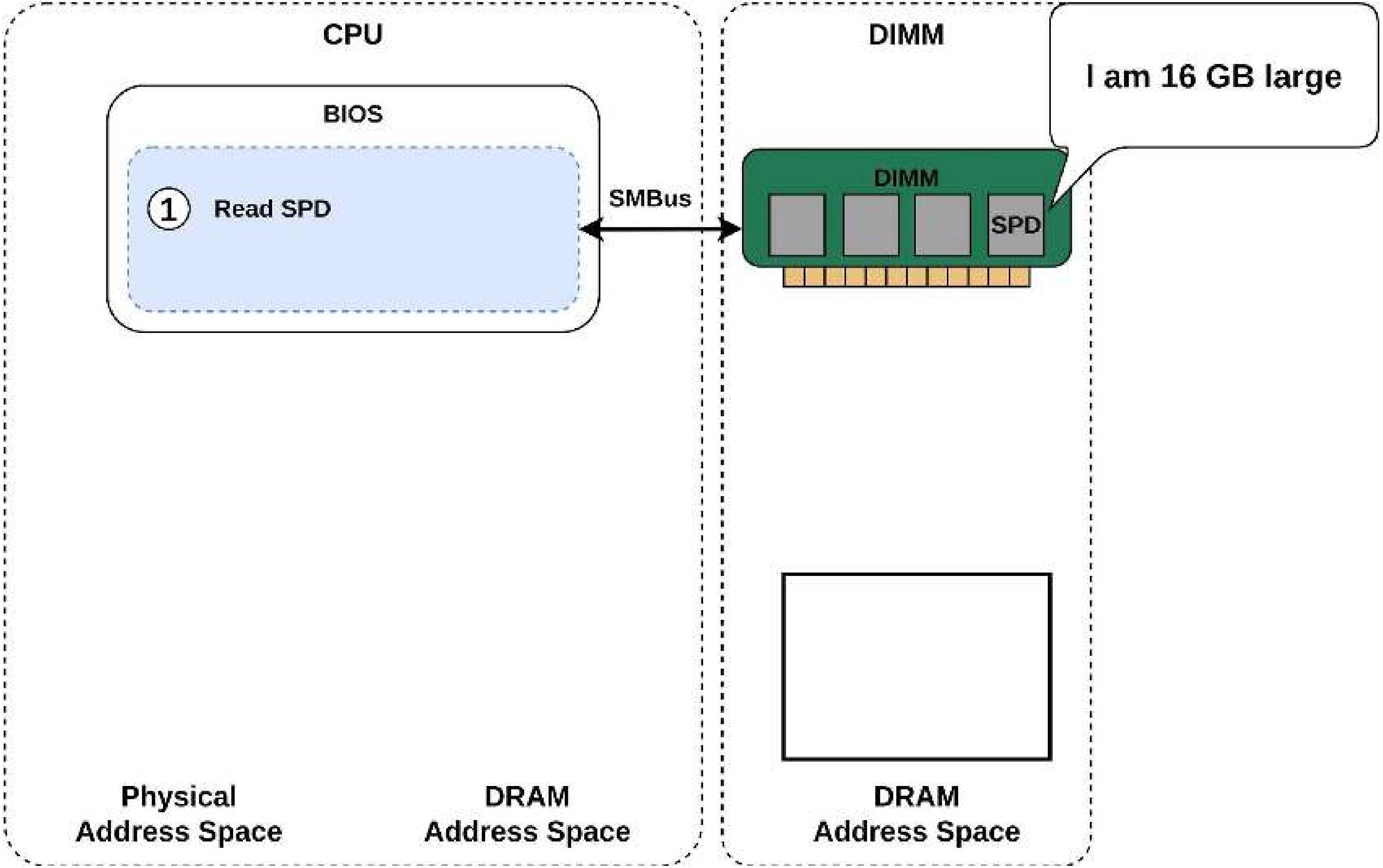


DIMM meta data: manifacturer, speed, size, ...

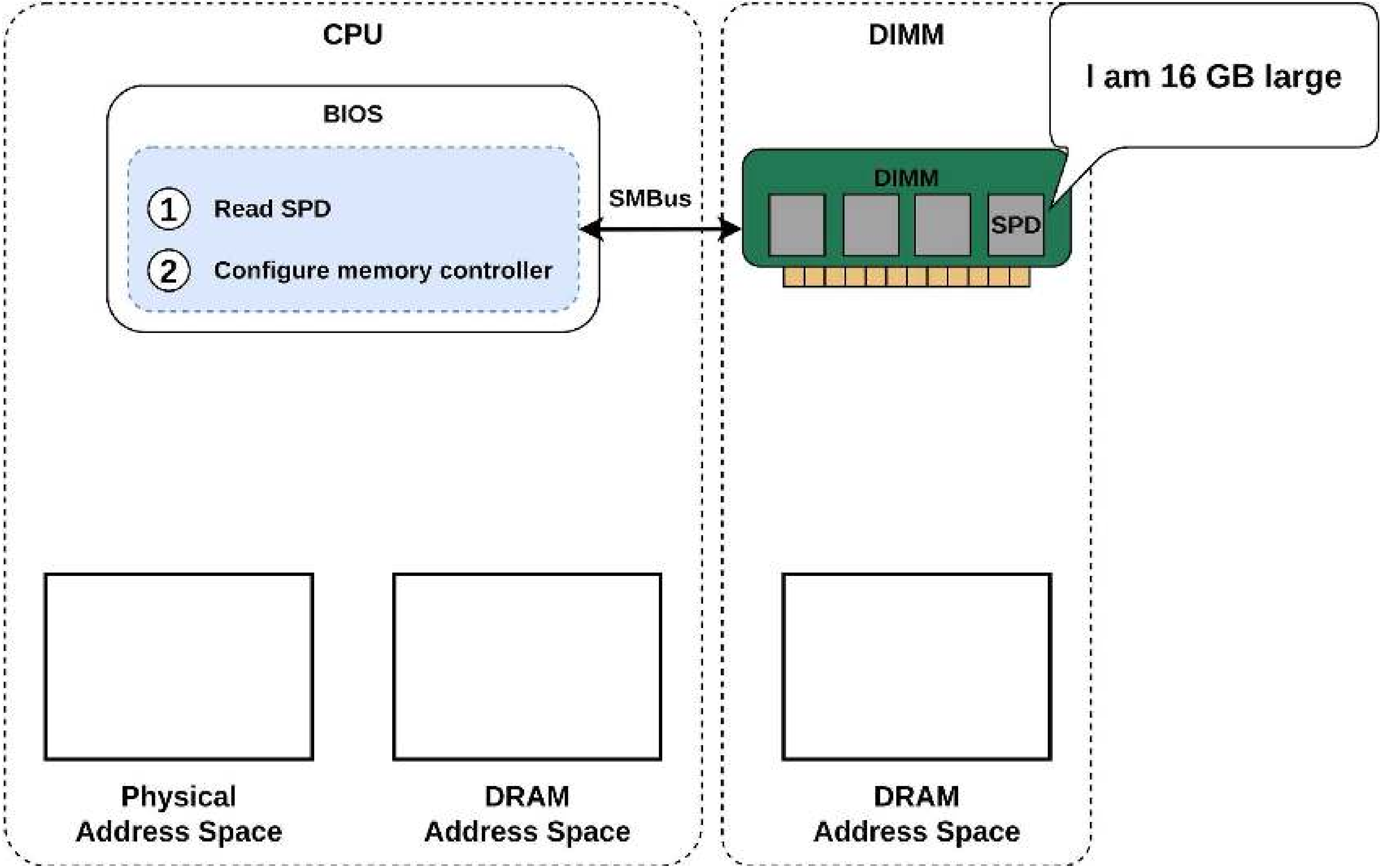
BadRAM: What if Your DRAM Lies to You?



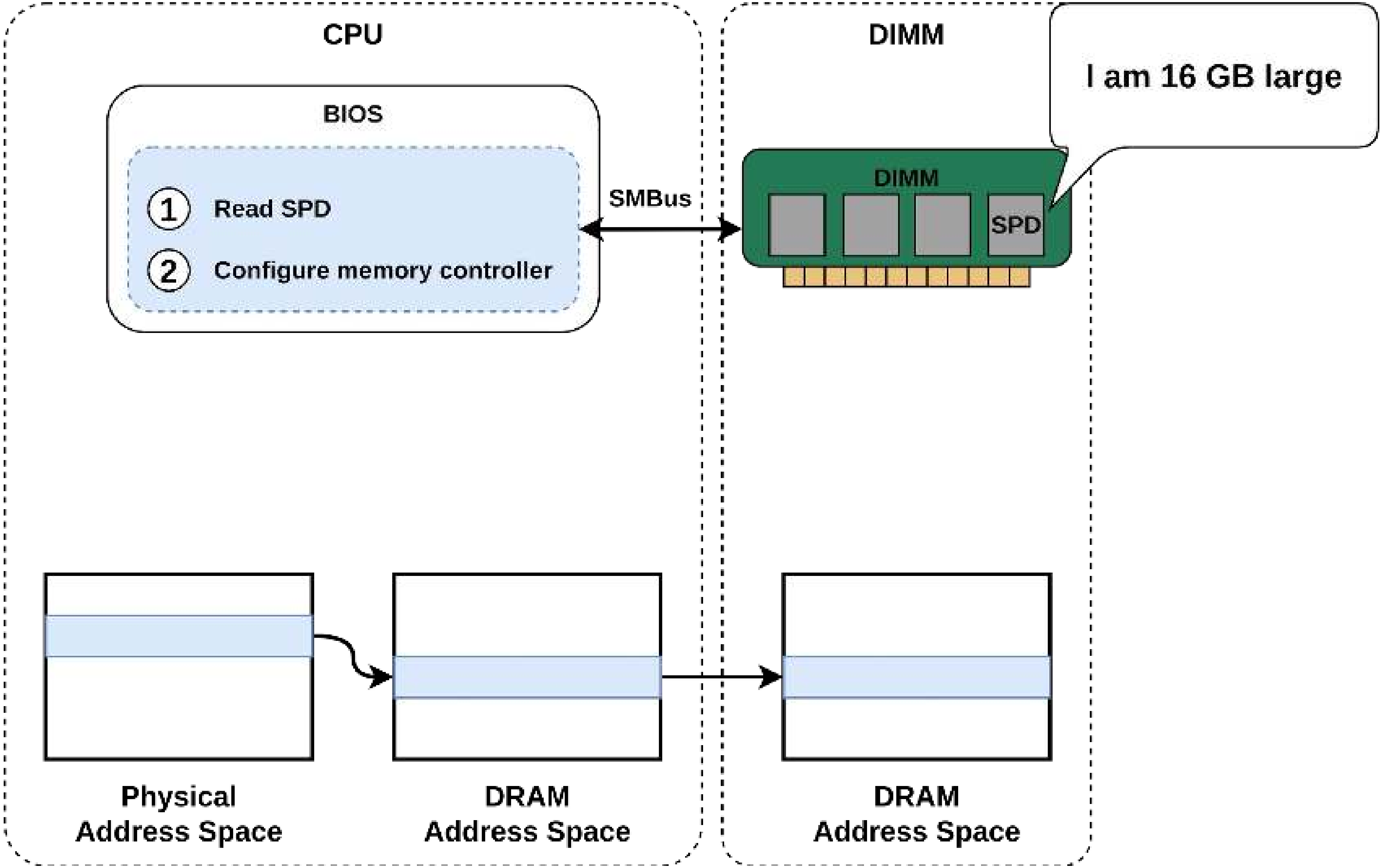
BadRAM: What if Your DRAM Lies to You?



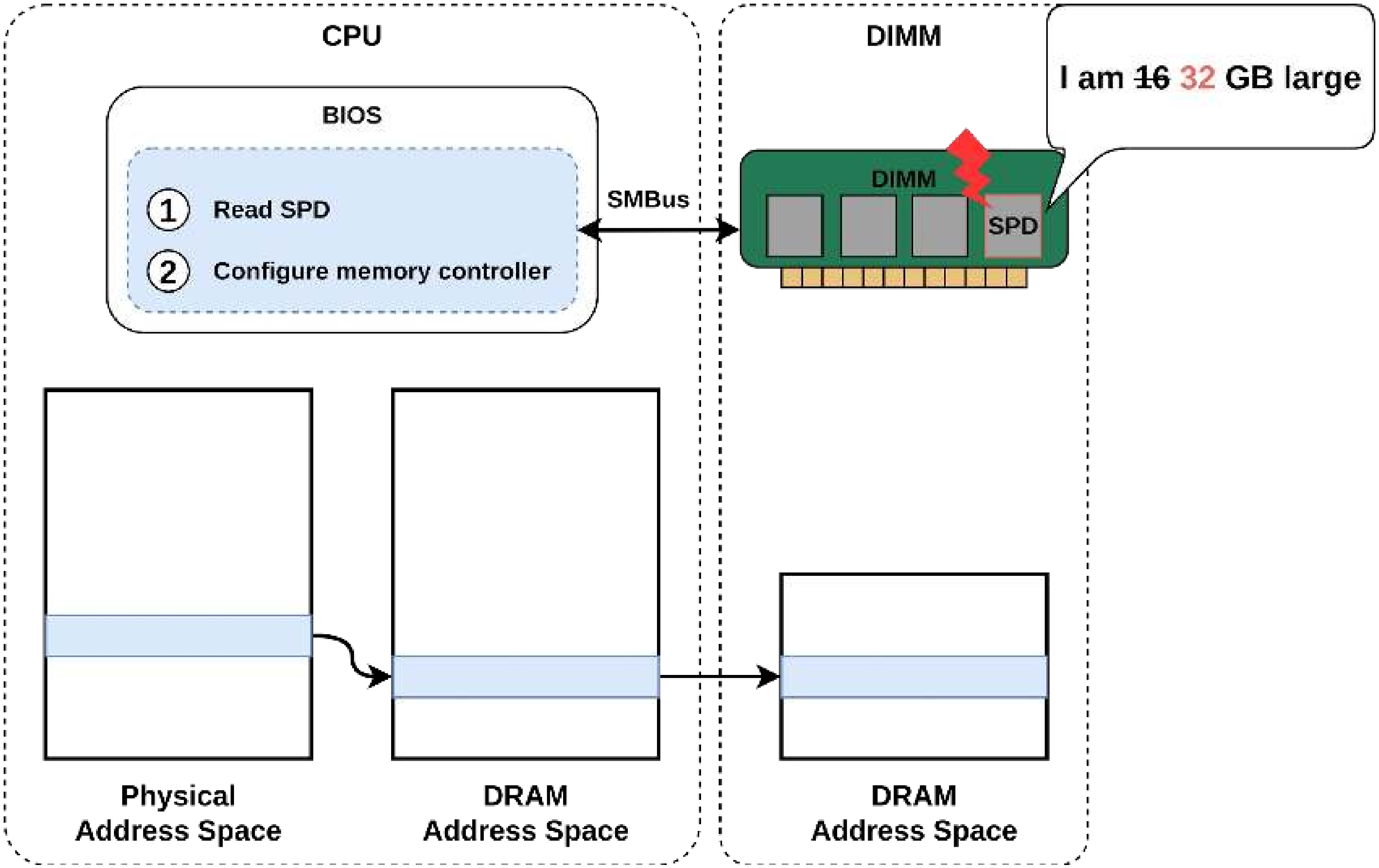
BadRAM: What if Your DRAM Lies to You?



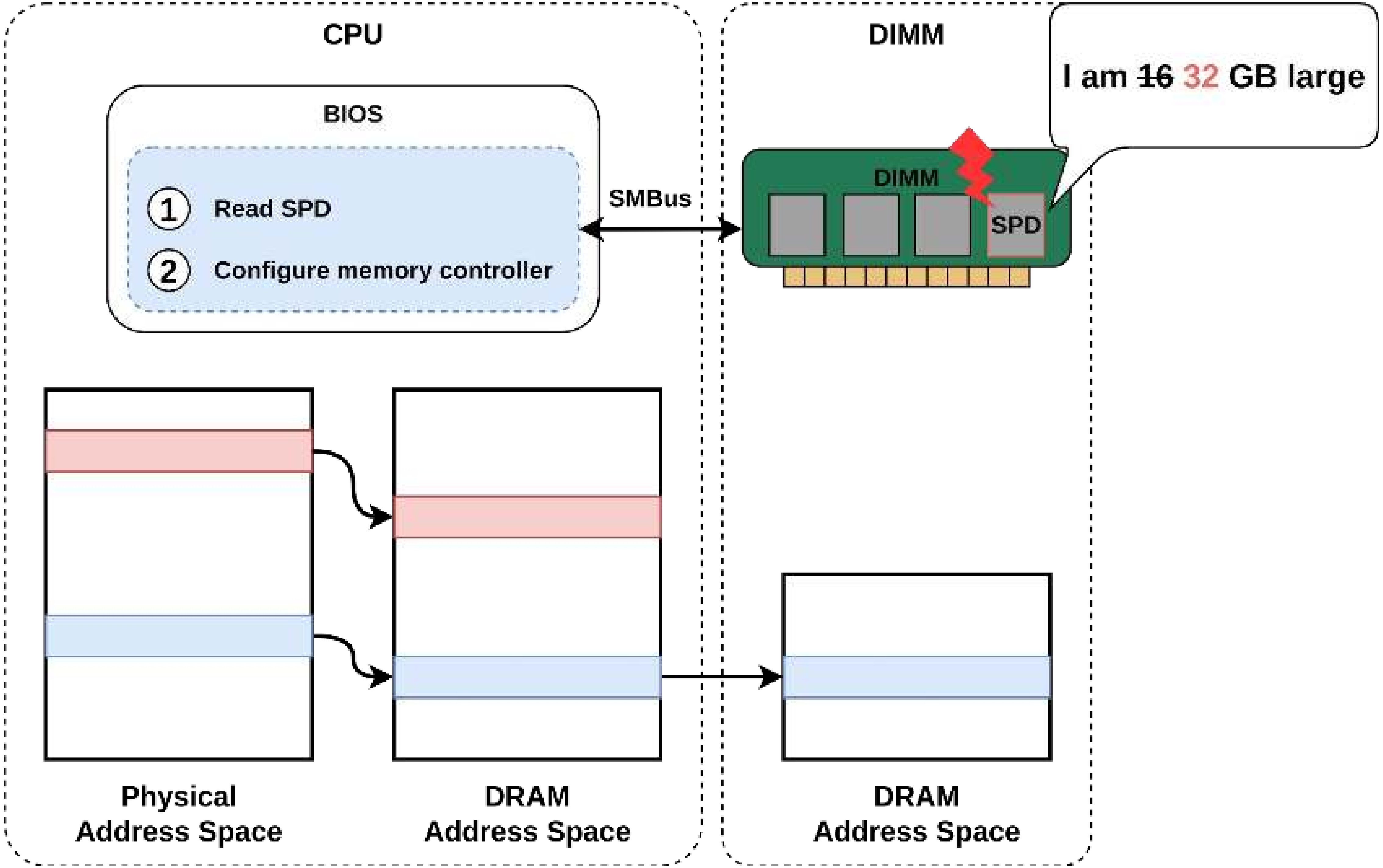
BadRAM: What if Your DRAM Lies to You?



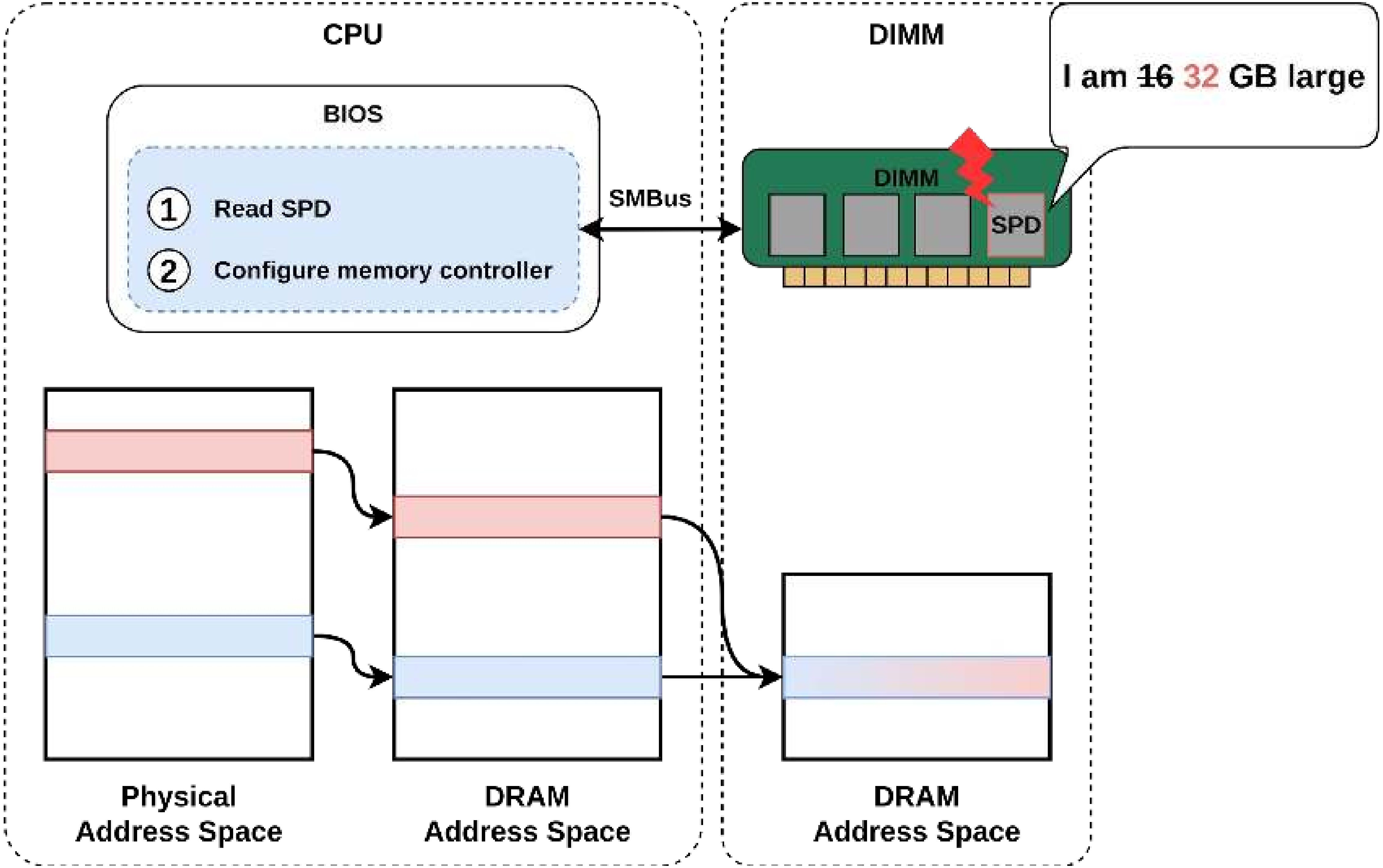
BadRAM: What if Your DRAM Lies to You?



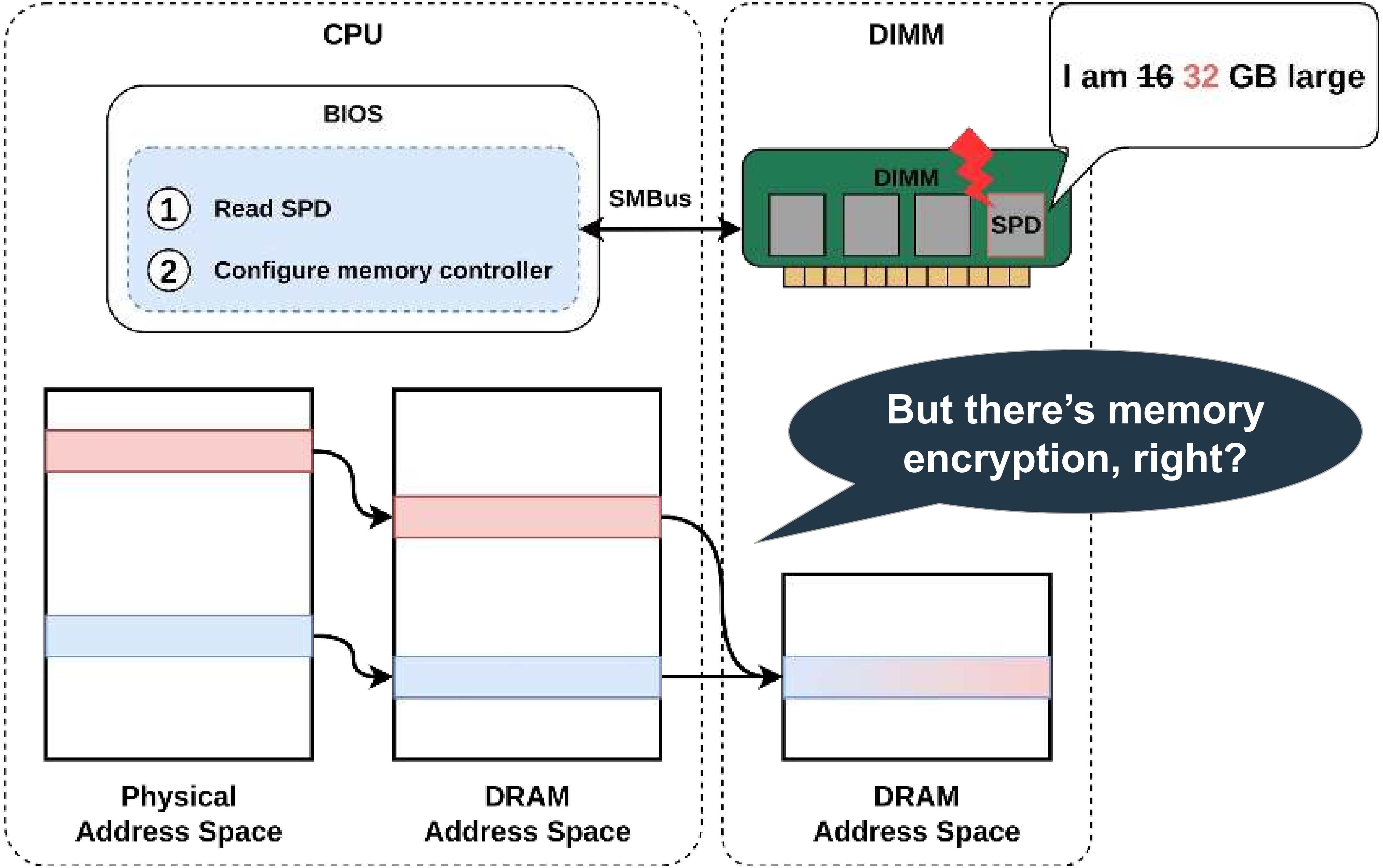
BadRAM: What if Your DRAM Lies to You?



BadRAM: What if Your DRAM Lies to You?

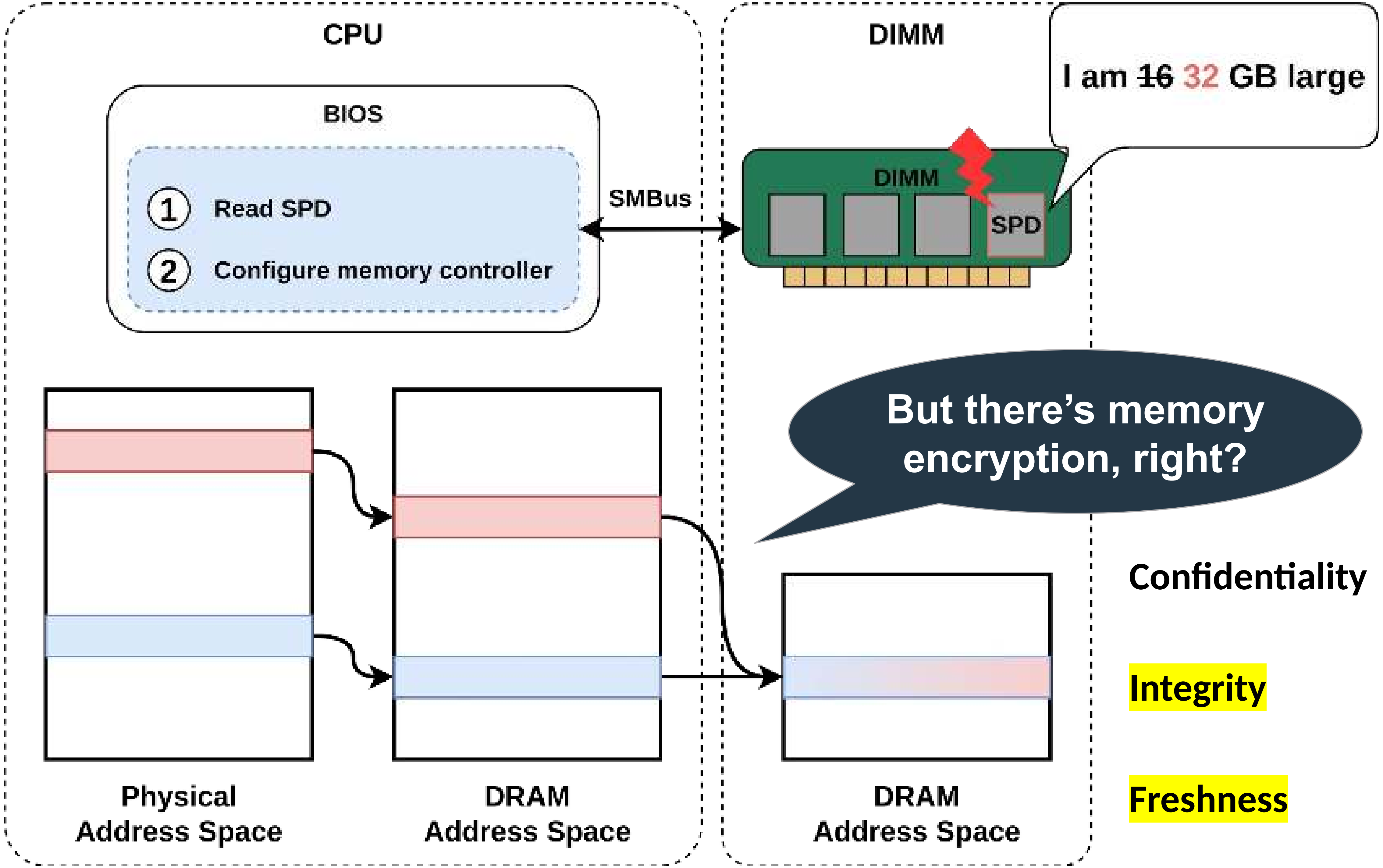


BadRAM: What if Your DRAM Lies to You?



But there’s memory encryption, right?

BadRAM: What if Your DRAM Lies to You?



But there’s memory encryption, right?

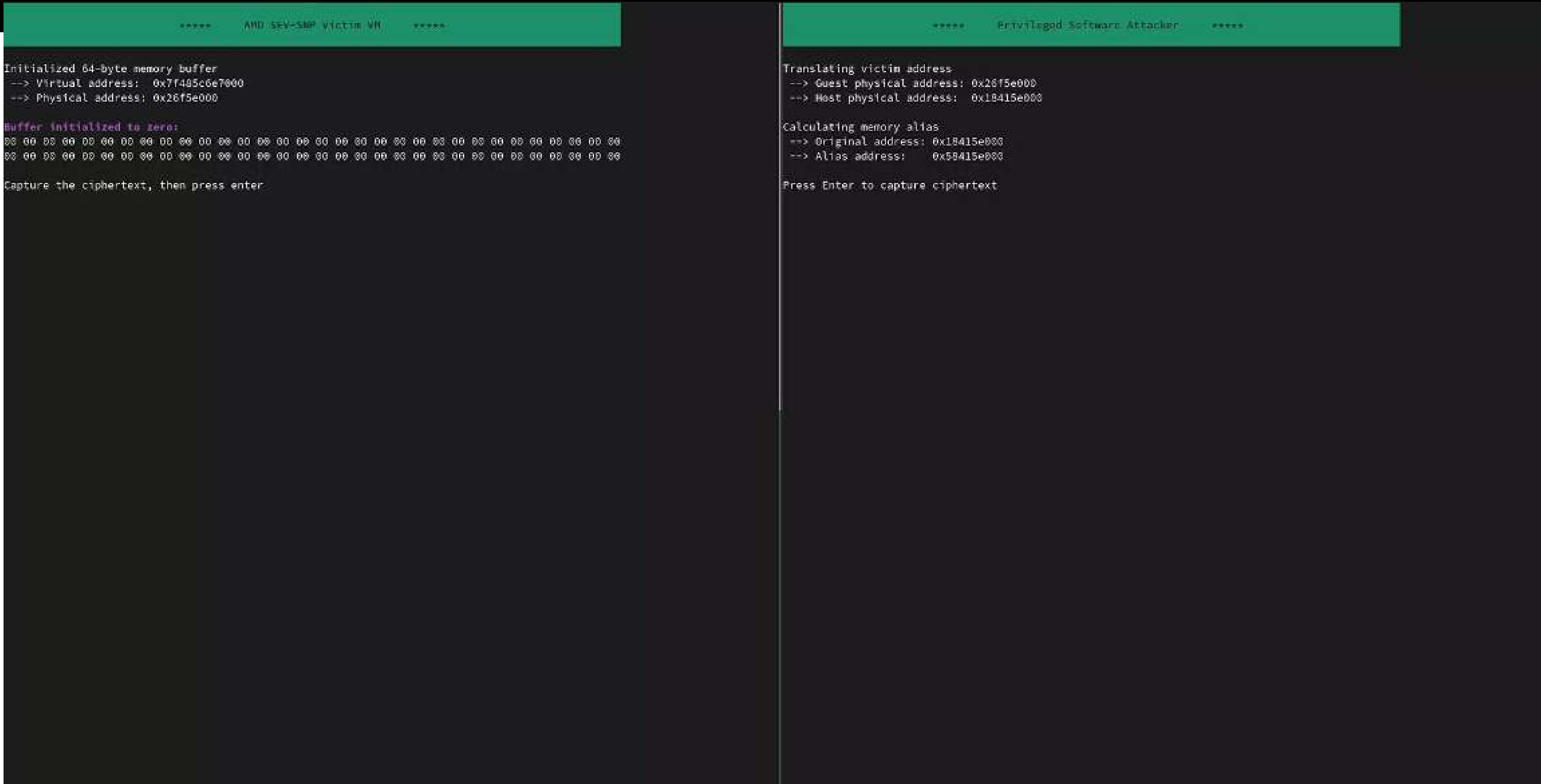
Confidentiality 🔒

Integrity ✗

Freshness ✗

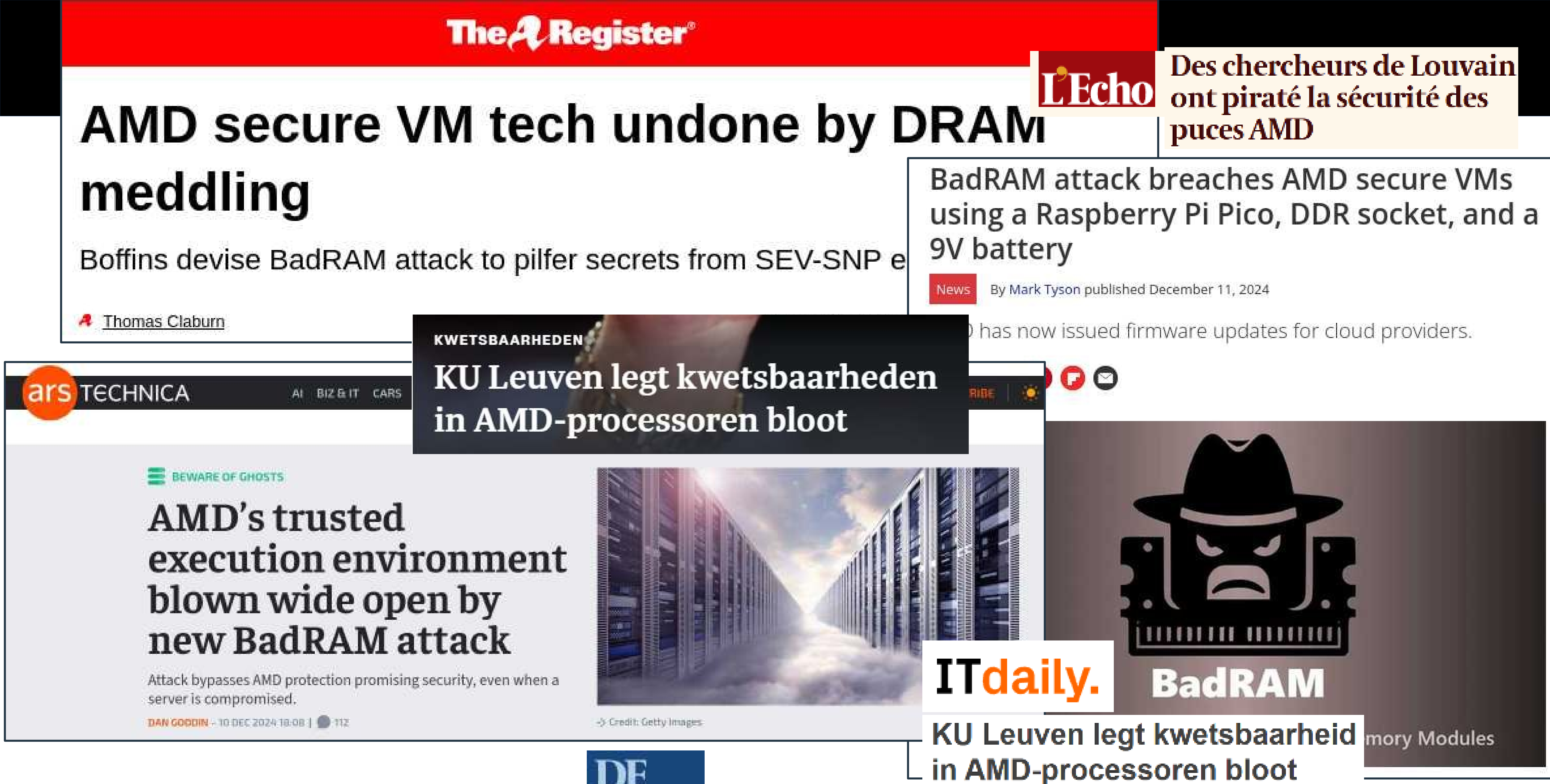
Demo

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
```

```
*****     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
```



The Register®

AMD secure VM tech undone by DRAM meddling

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

Thomas Claburn

L'Echo

Des chercheurs de Louvain ont piraté la sécurité des puces AMD

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

) has now issued firmware updates for cloud providers.

KWETSBAARHEDEN

KU Leuven legt kwetsbaarheden in AMD-processoren bloot

ars TECHNICA AI BIZ & IT CARS RIBE

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

ITdaily.

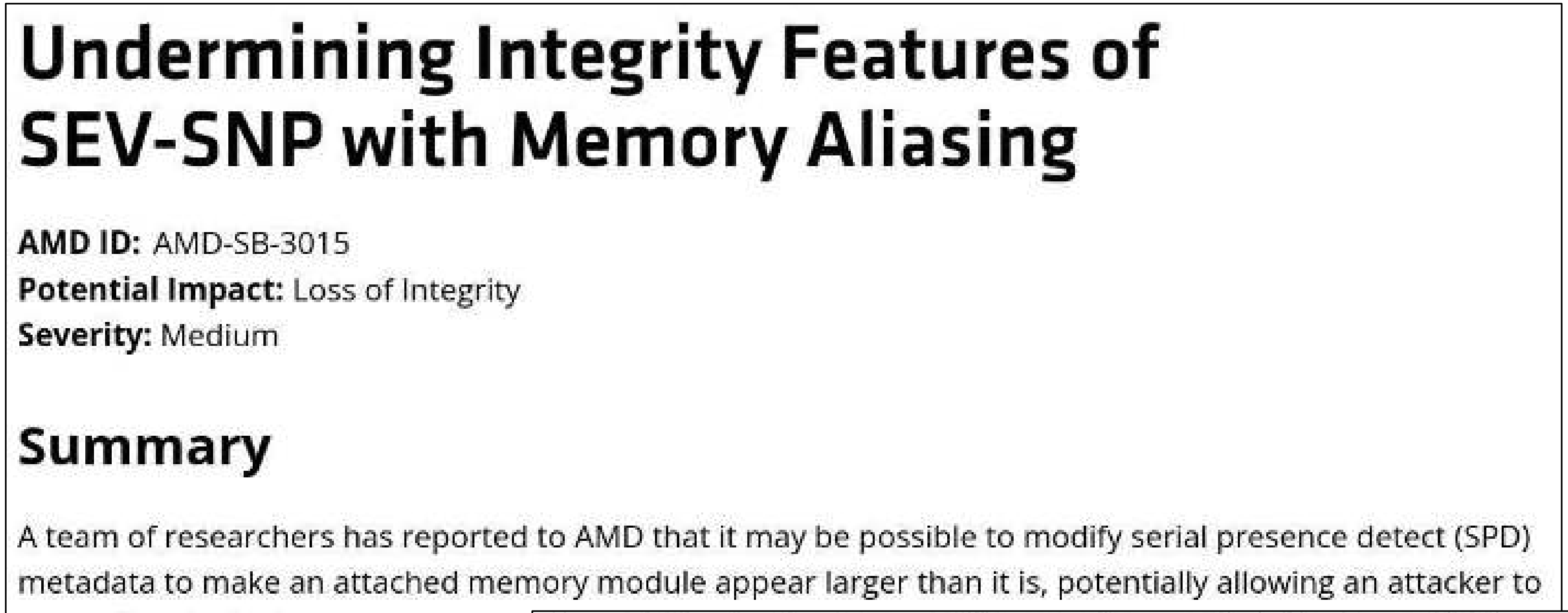
KU Leuven legt kwetsbaarheid in AMD-processoren bloot

DE TIJD

Leuvense onderzoekers kraken beveiliging AMD-chips

🌍 https://badram.eu/

Vendor Response: Boot-Time Firmware Mitigations

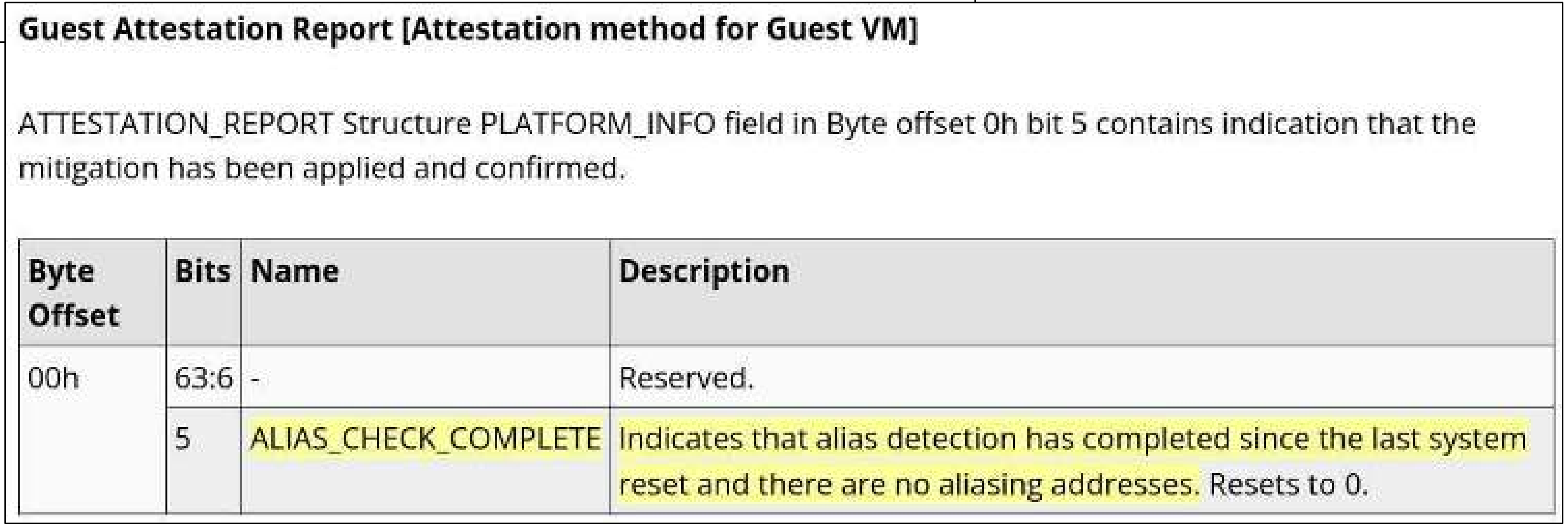


Undermining Integrity Features of SEV-SNP with Memory Aliasing

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.



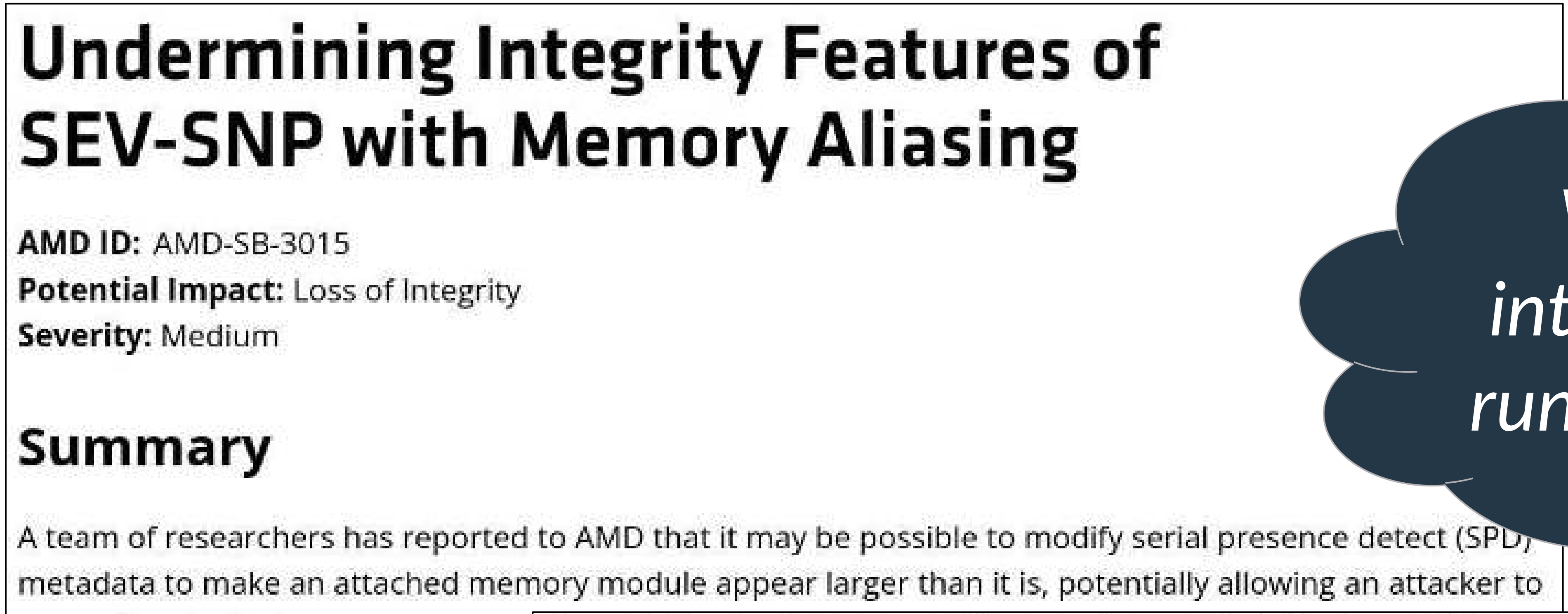
Guest Attestation Report [Attestation method for Guest VM]

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



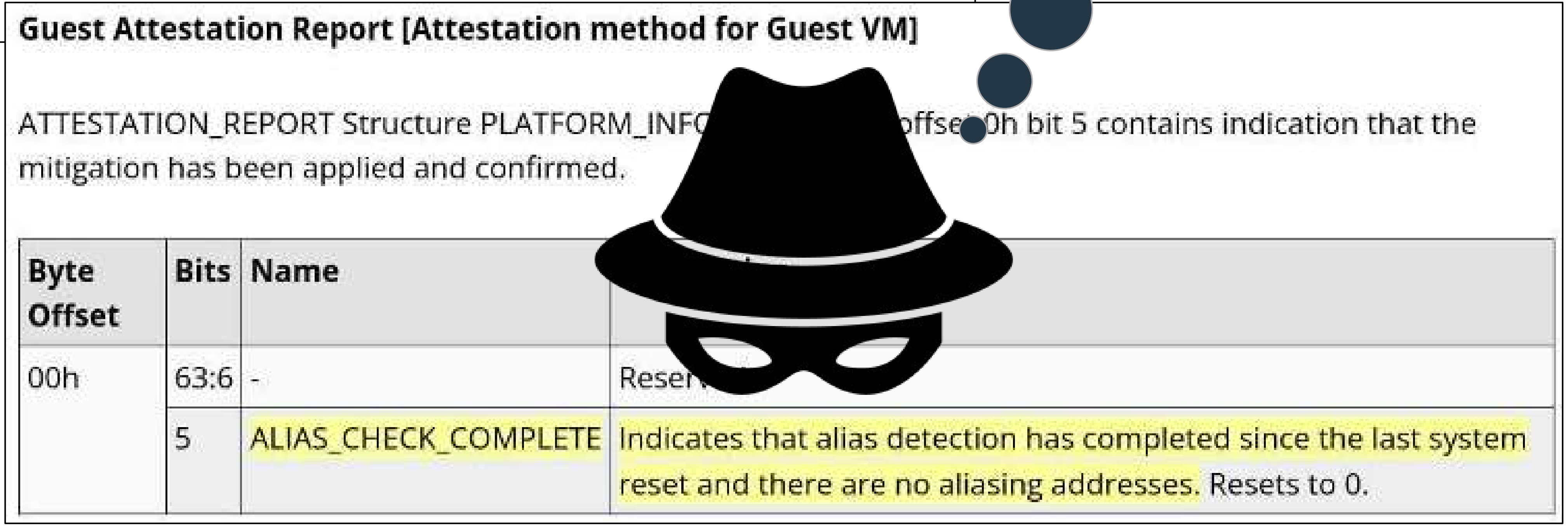
Undermining Integrity Features of SEV-SNP with Memory Aliasing

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]

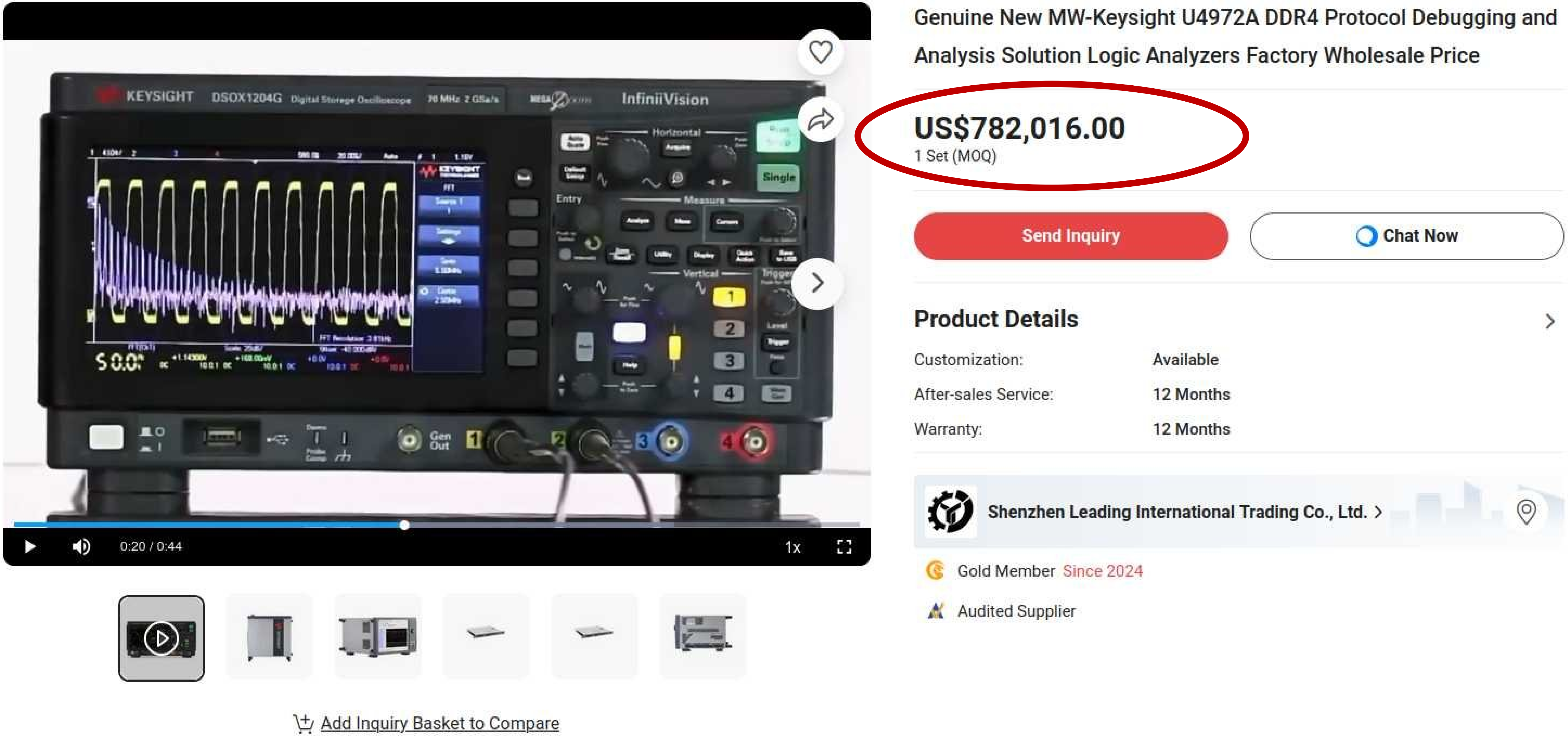
ATTESTATION_REPORT Structure PLATFORM_INF offse 0h bit 5 contains indication that the mitigation has been applied and confirmed.

Byte Offset	Bits	Name	
00h	63:6	-	Reser
	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?



KEYSIGHT
DSOX1204G Digital Storage Oscilloscope
InfiniiVision
Single
Gen Out
0:20 / 0:44
1x
Send Inquiry
Chat Now
Add Inquiry Basket to Compare

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

US$782,016.00

1 Set (MOQ)

Product Details

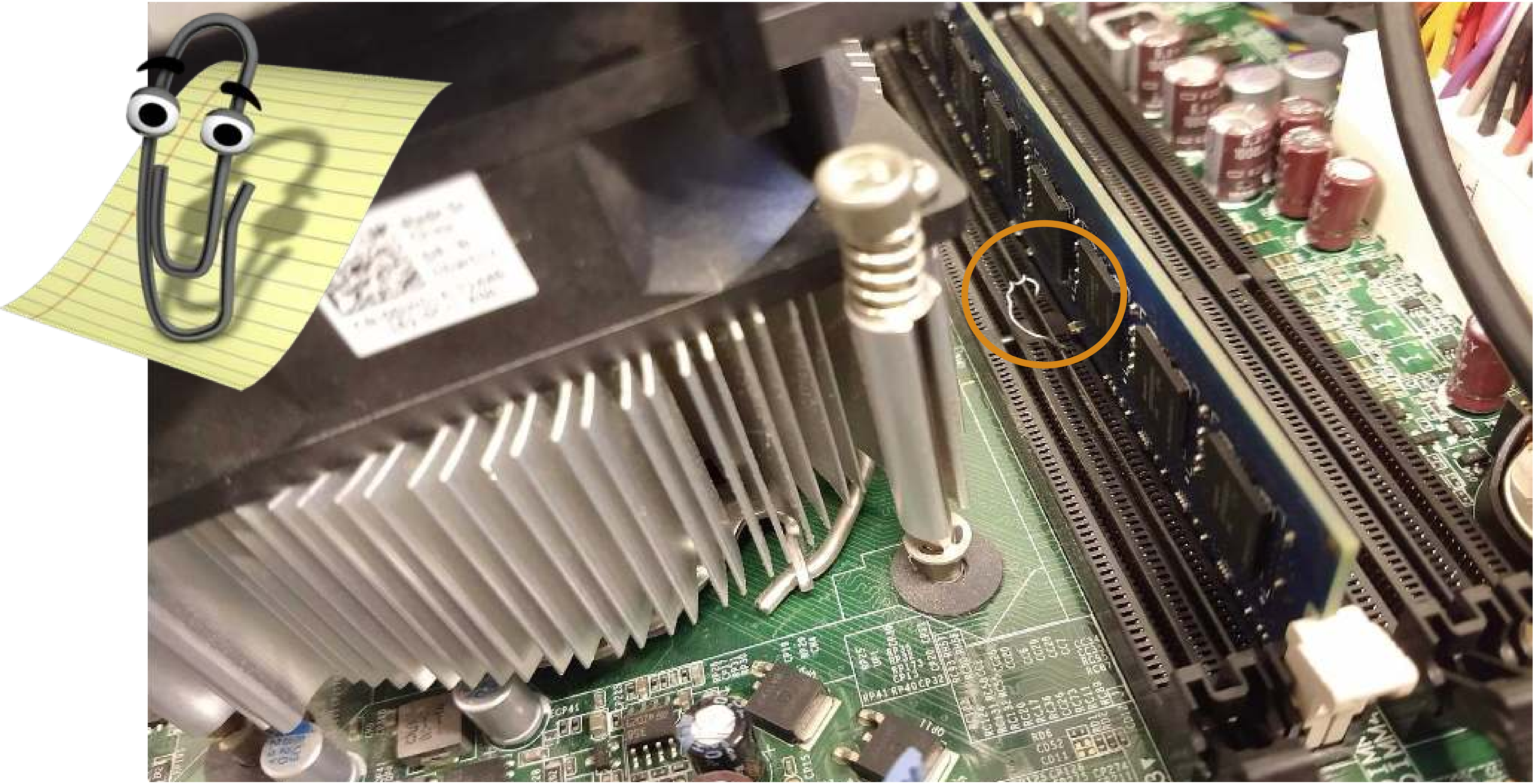
Customization:	Available
After-sales Service:	12 Months
Warranty:	12 Months

Shenzhen Leading International Trading Co., Ltd.

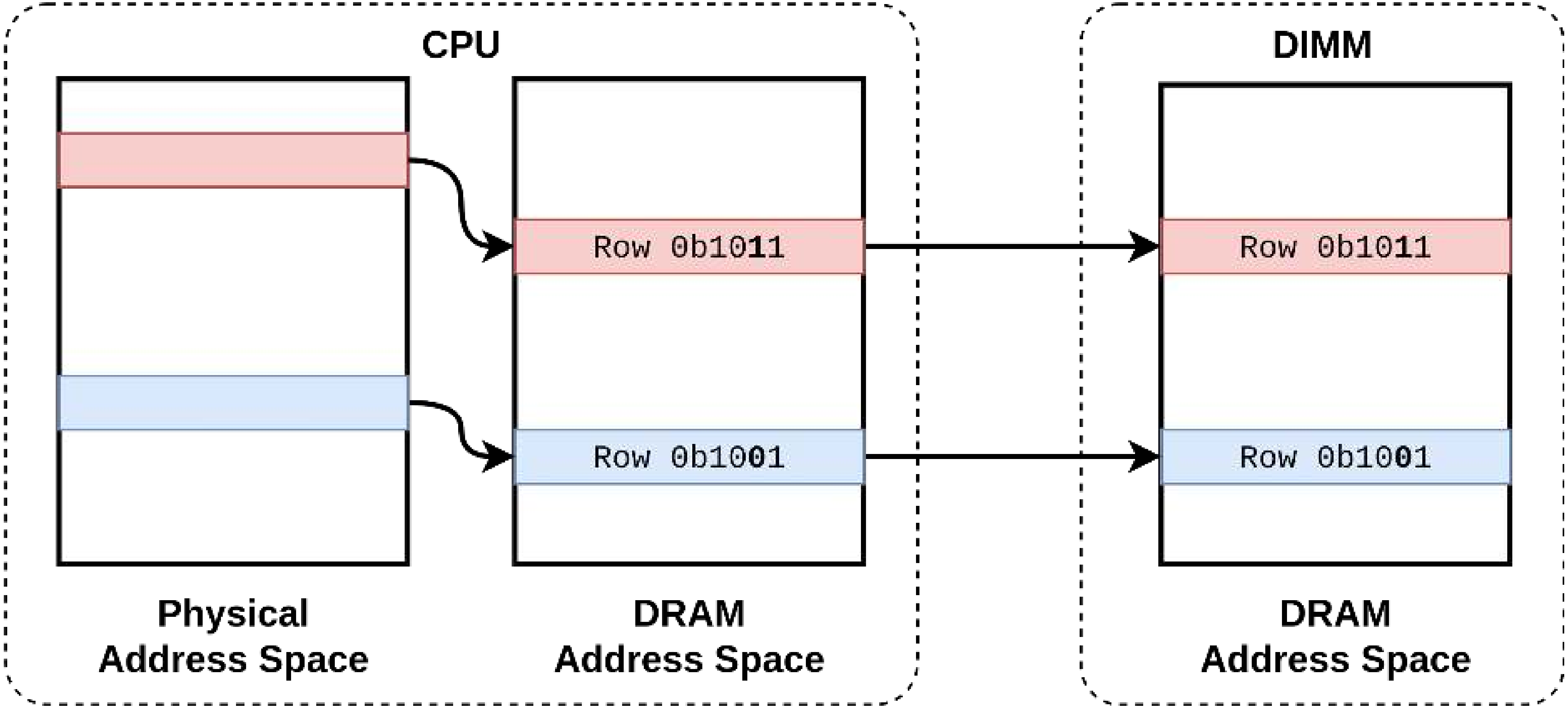
Gold Member Since 2024

Audited Supplier

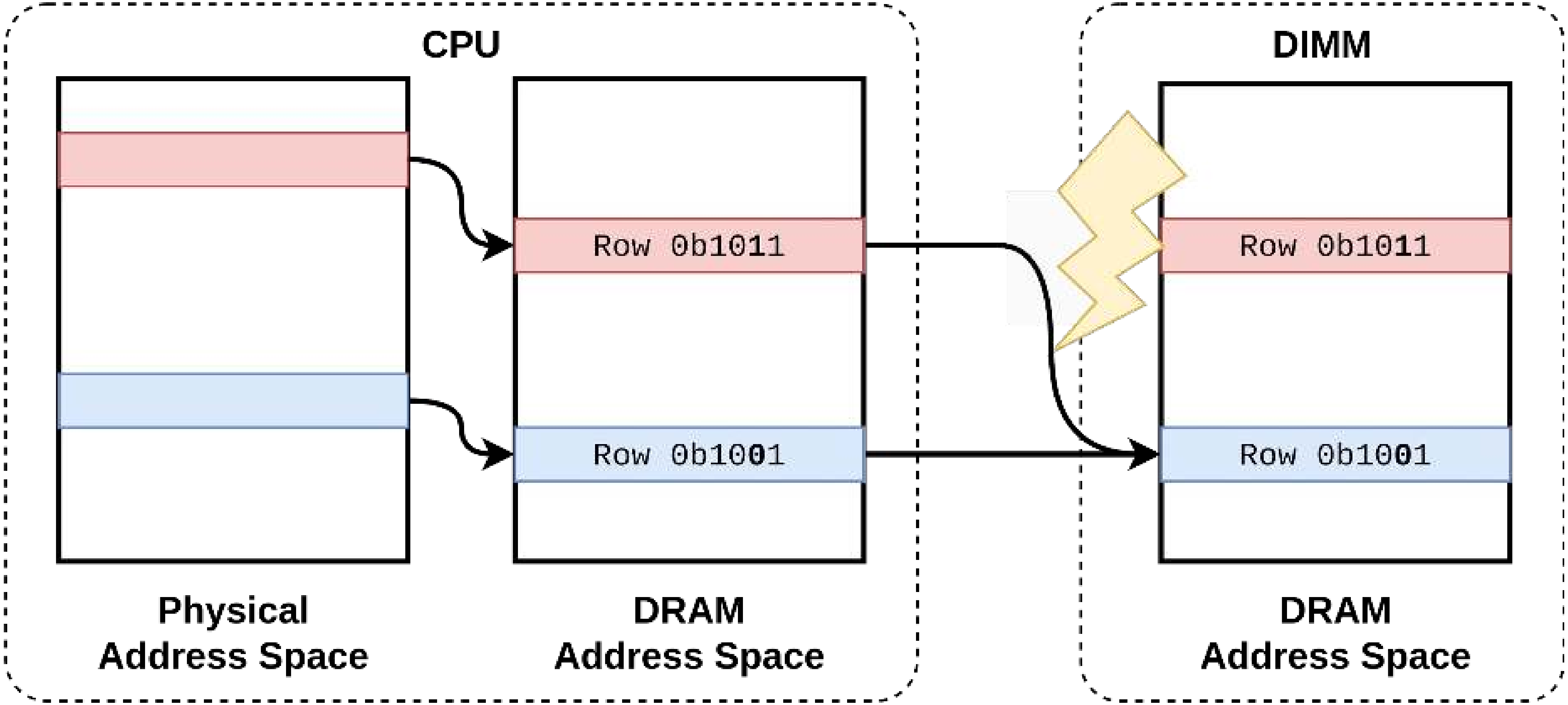
Tampering with Addressing at Runtime



Battering RAM: Tampering with Addressing at Runtime



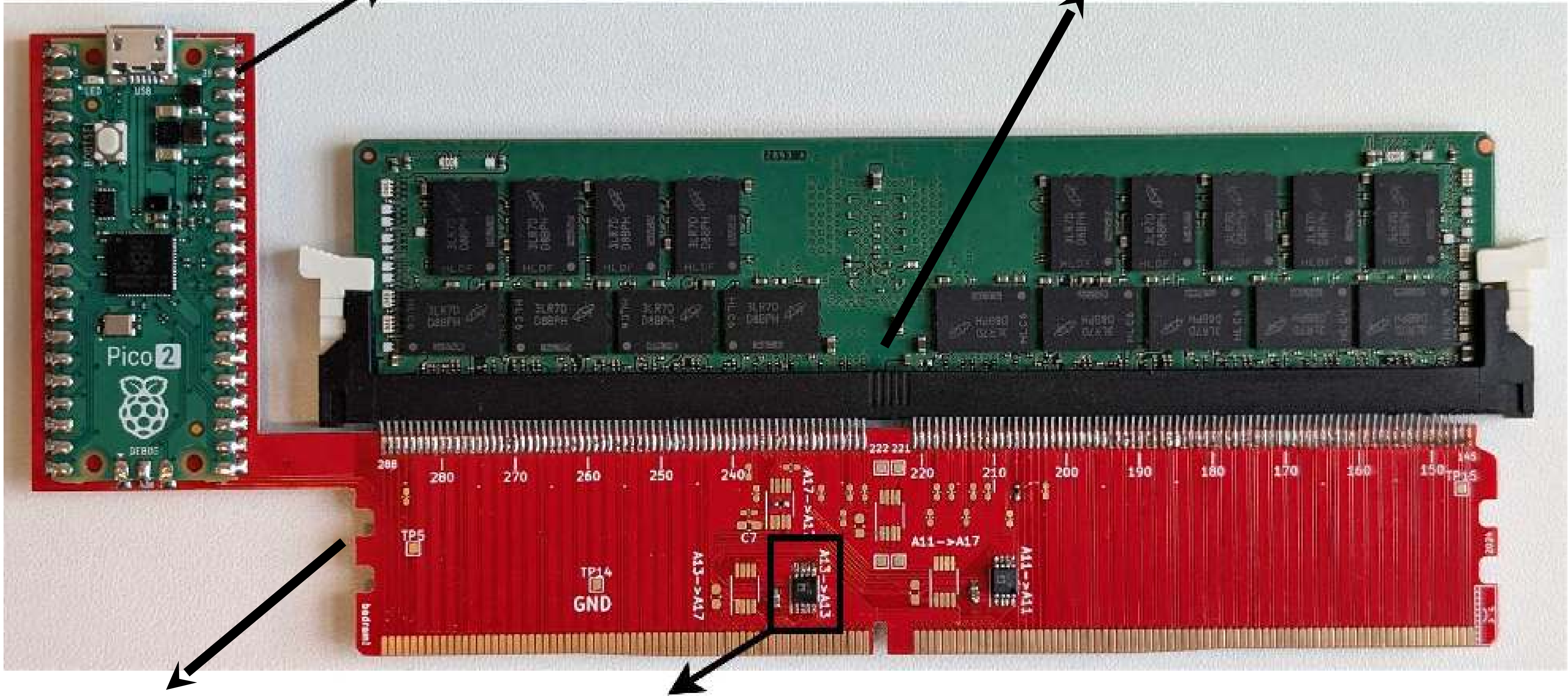
Battering RAM: Tampering with Addressing at Runtime



Battering RAM: Tampering with Addressing at Runtime

Microcontroller (RPi Pico) $4

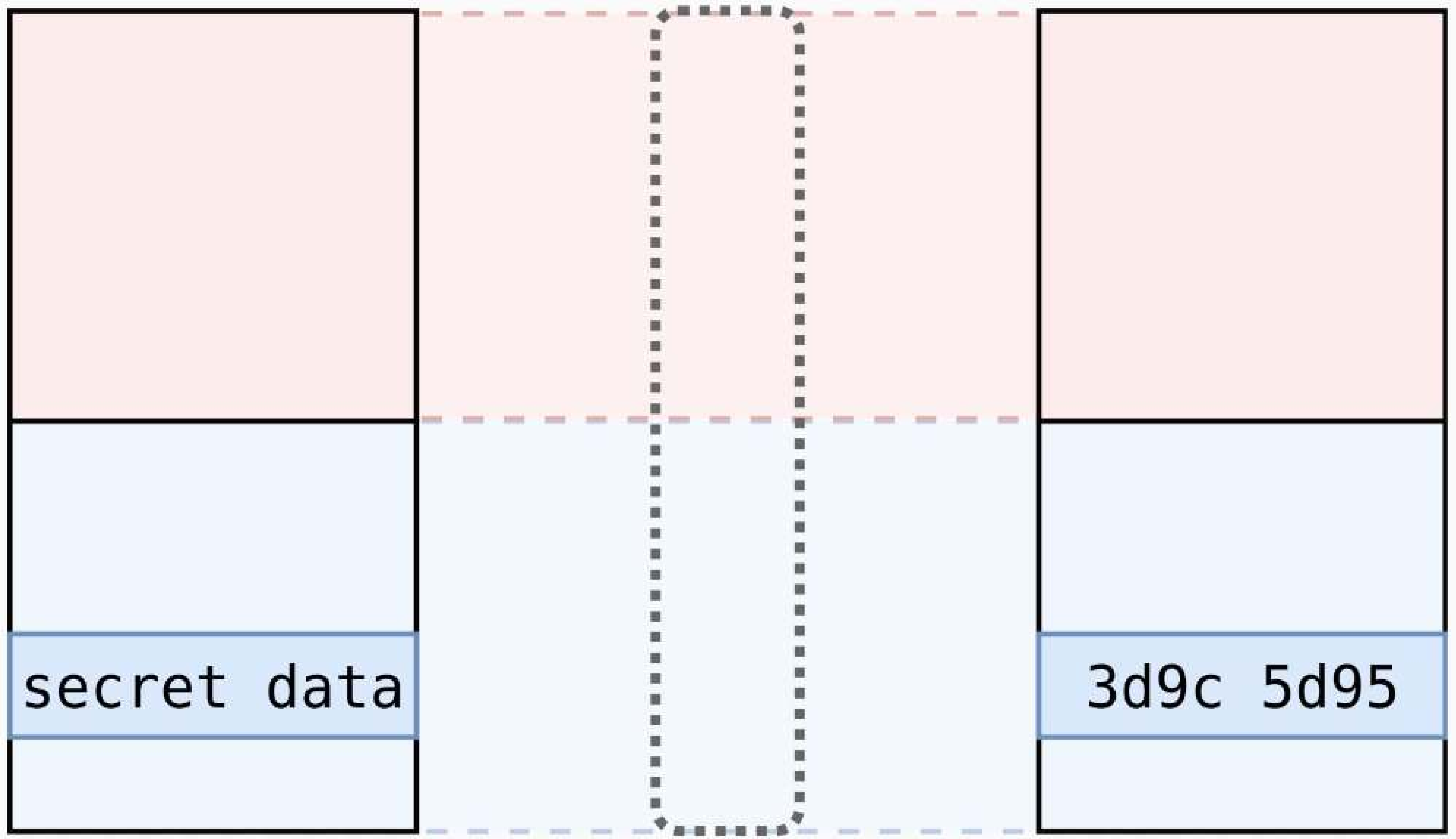
DDR4 connector: $16



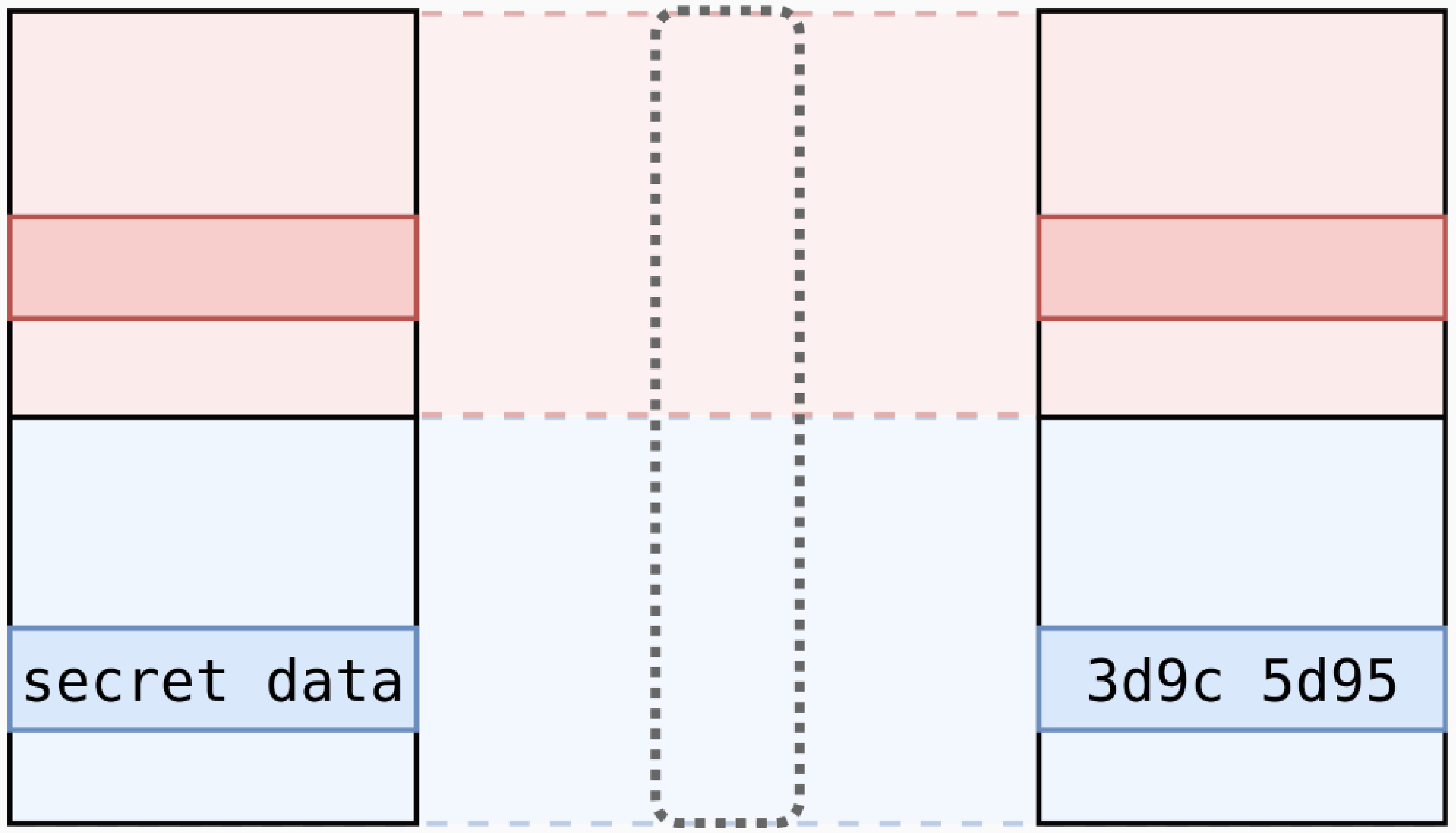
Custom PCB: $18

Analog Switch (ADG902) $4

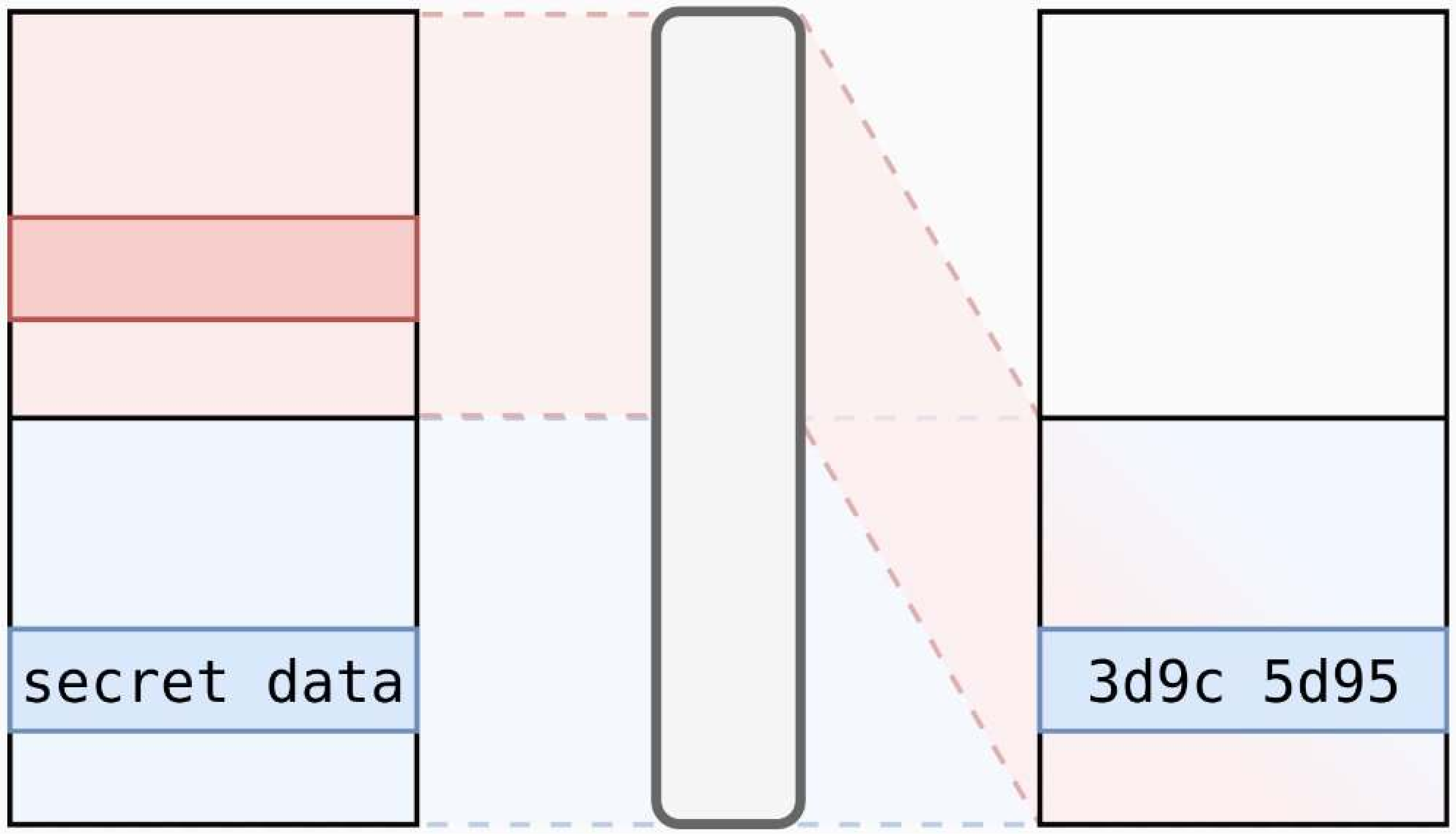
Battering RAM: Breaking Intel Scalable SGX Memory Encryption



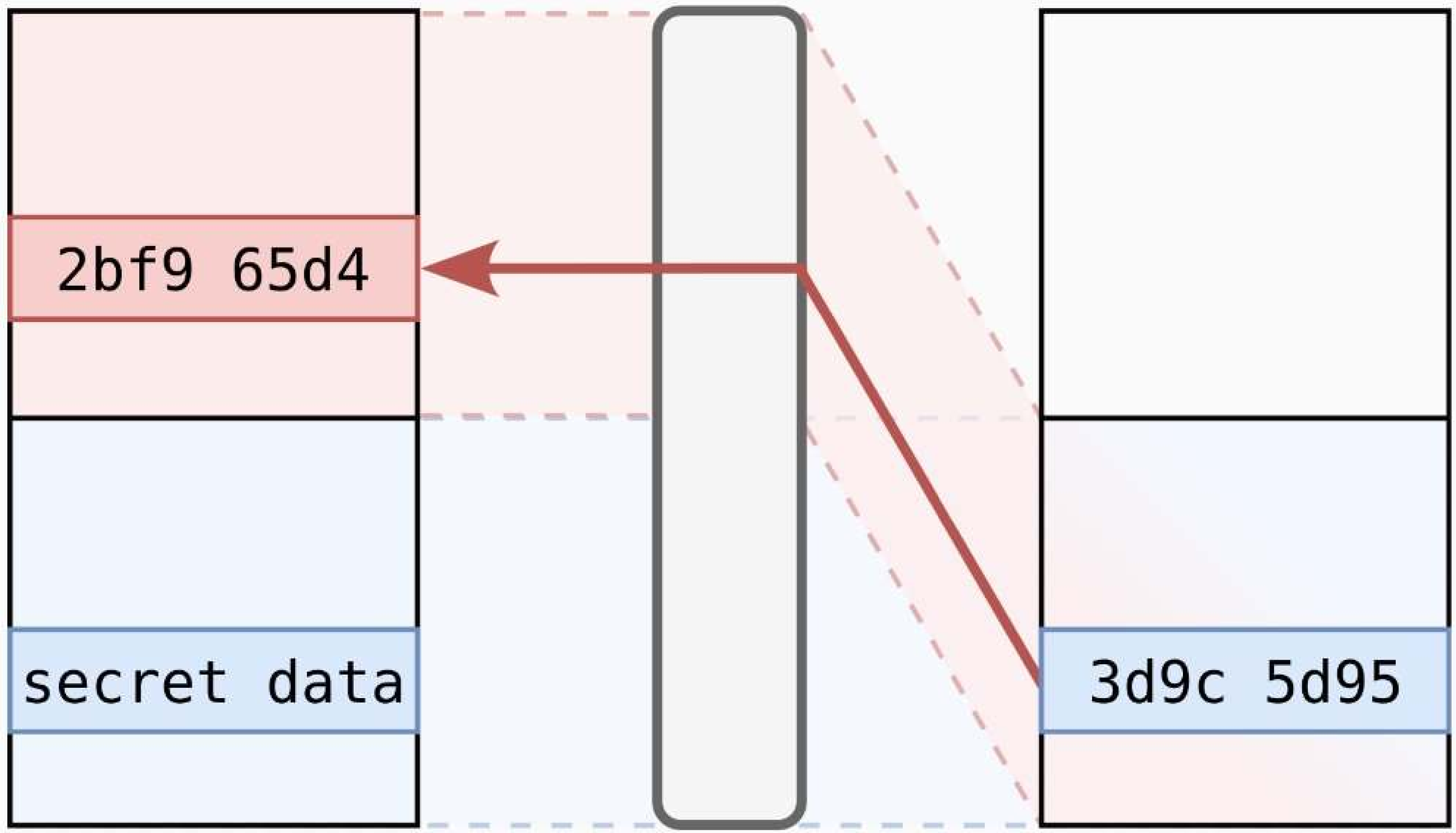
Battering RAM: Breaking Intel Scalable SGX Memory Encryption



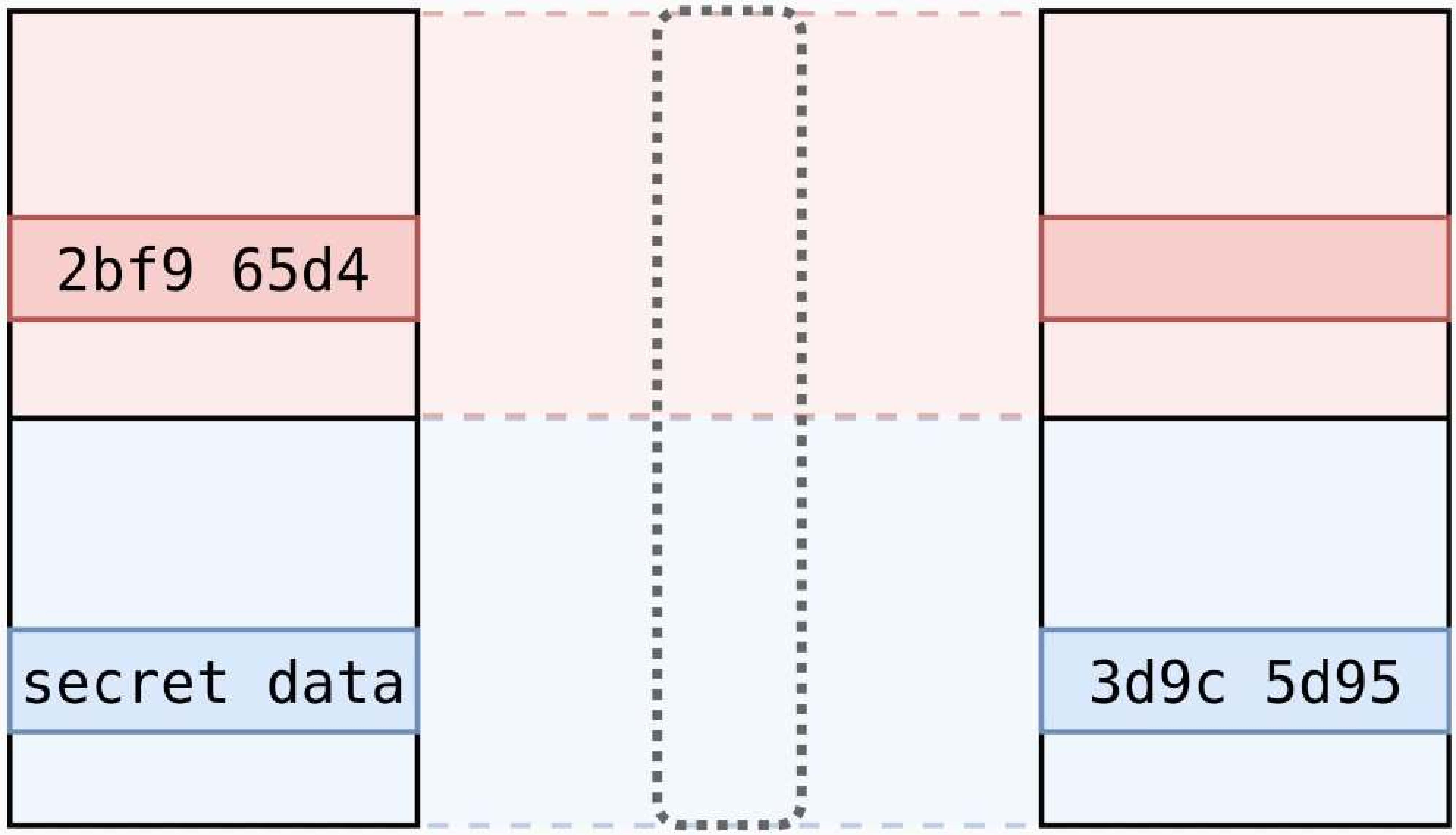
Battering RAM: Breaking Intel Scalable SGX Memory Encryption



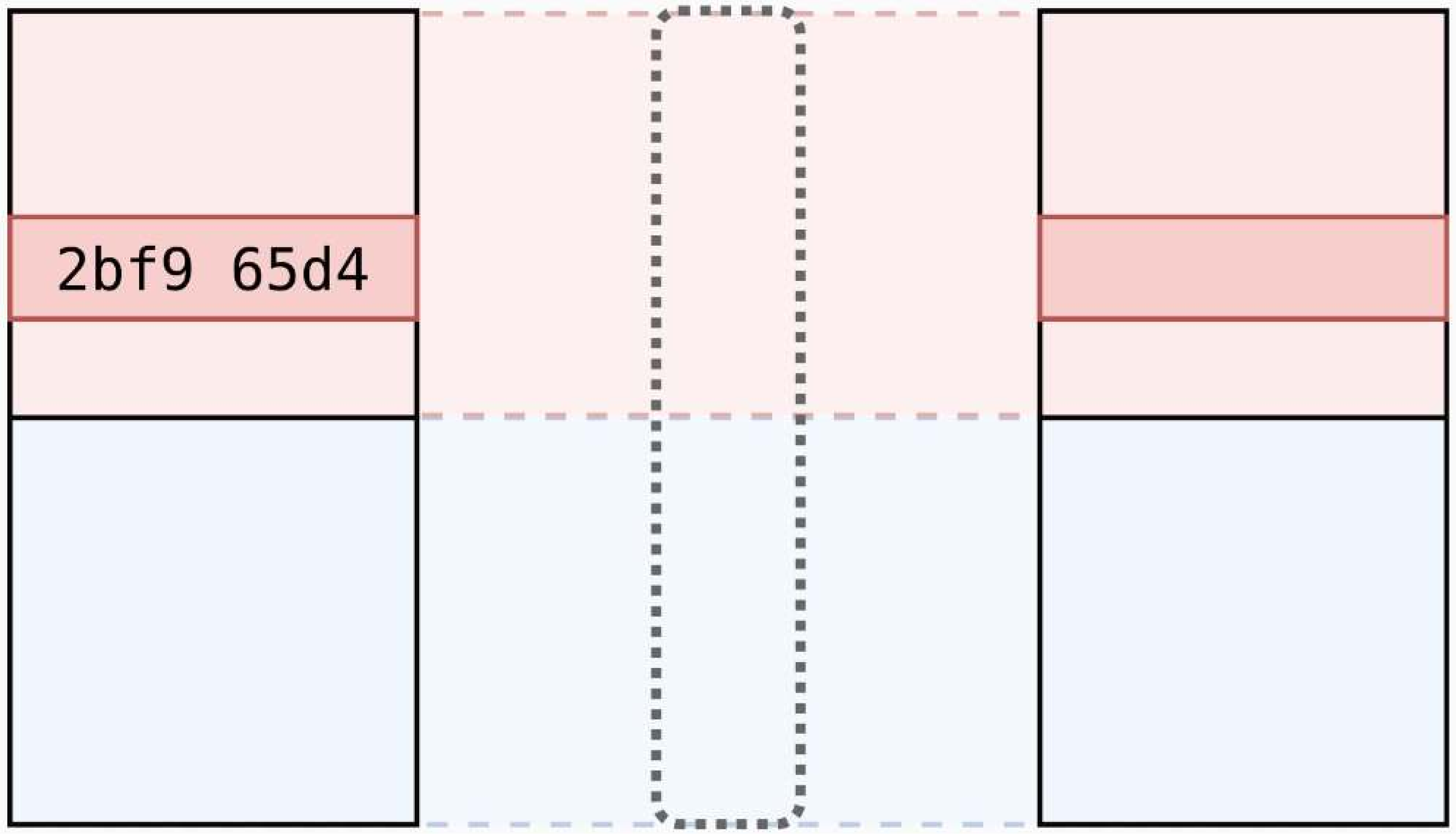
Battering RAM: Breaking Intel Scalable SGX Memory Encryption



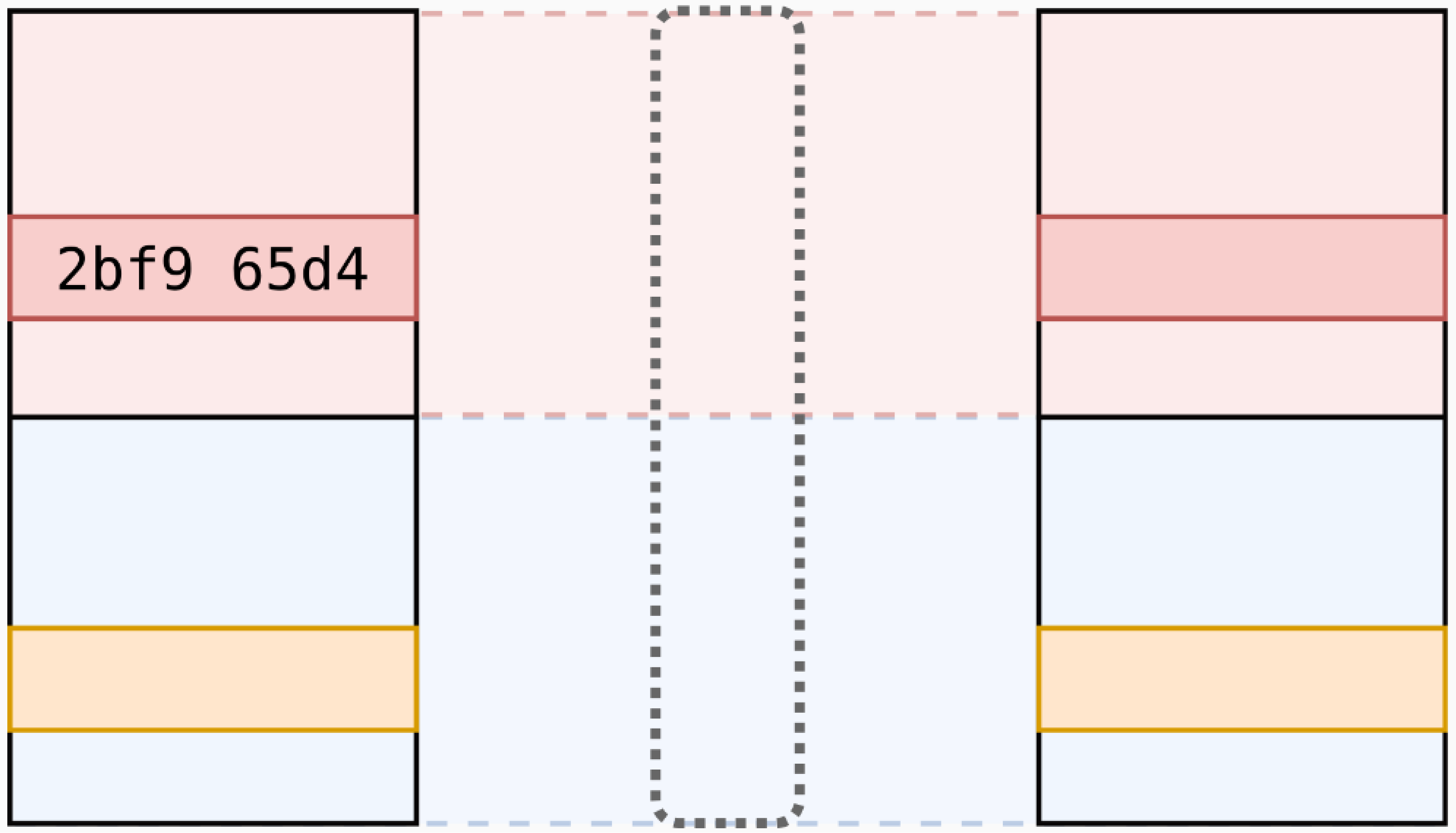
Battering RAM: Breaking Intel Scalable SGX Memory Encryption



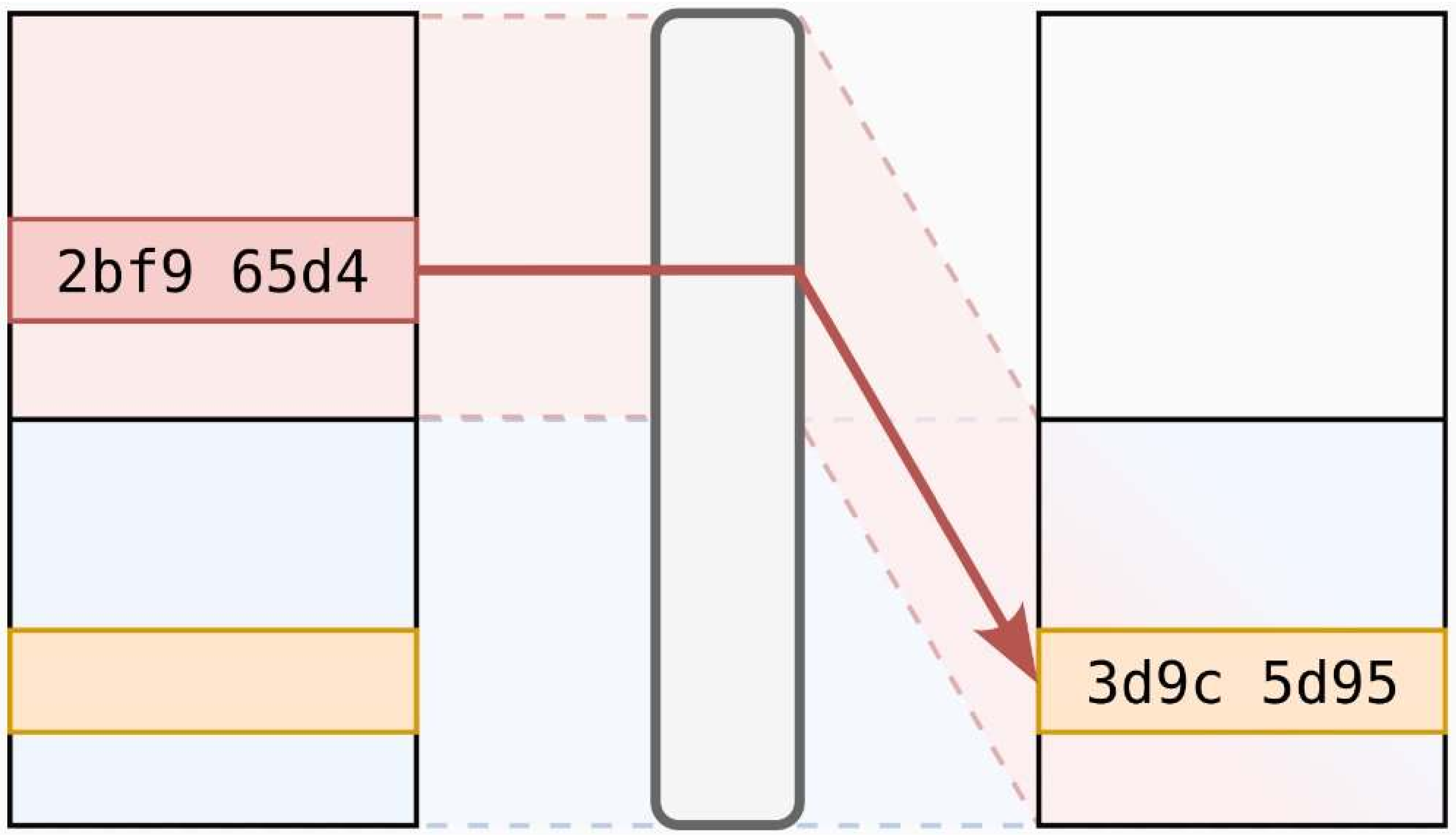
Battering RAM: Breaking Intel Scalable SGX Memory Encryption



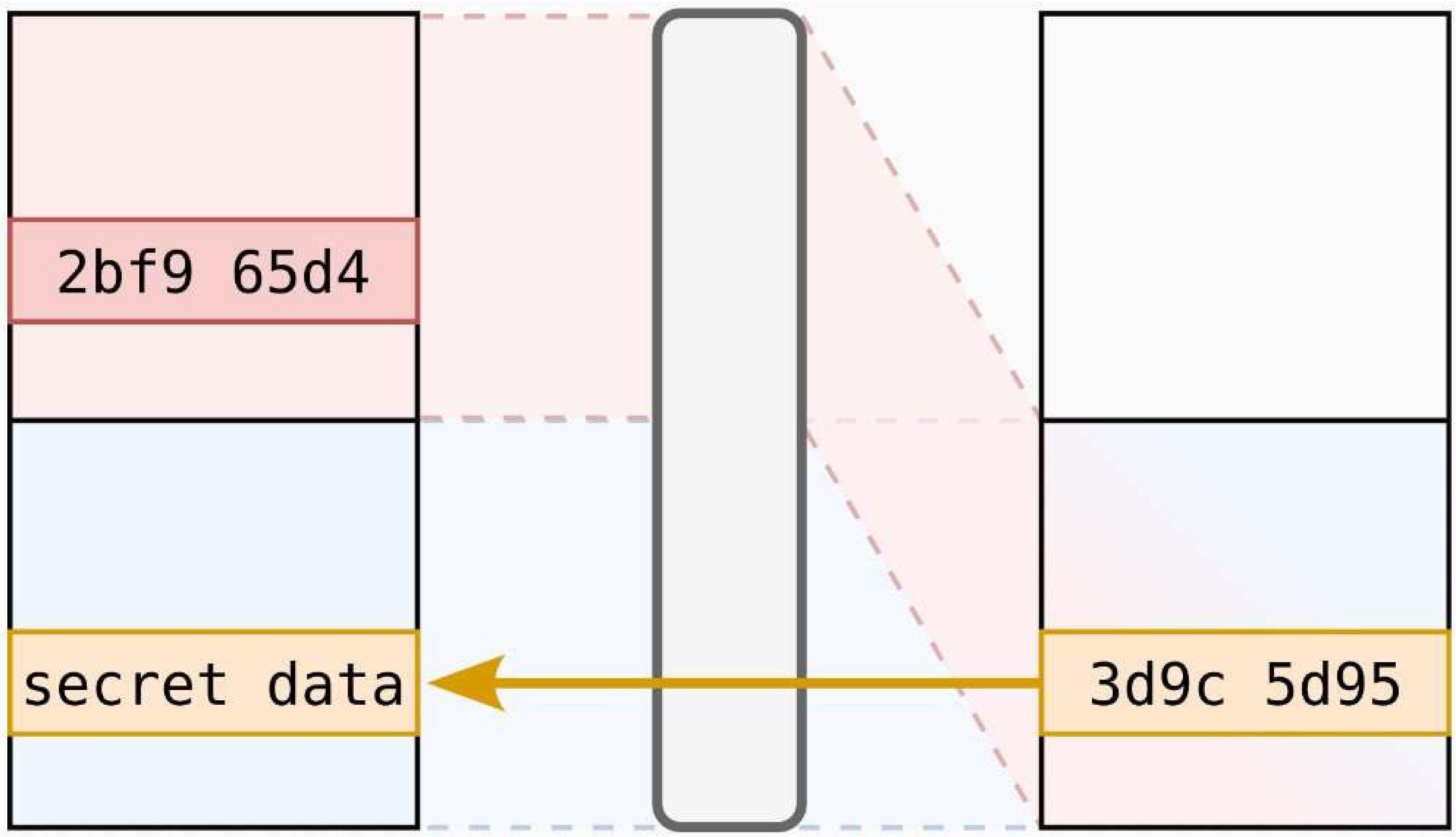
Battering RAM: Breaking Intel Scalable SGX Memory Encryption



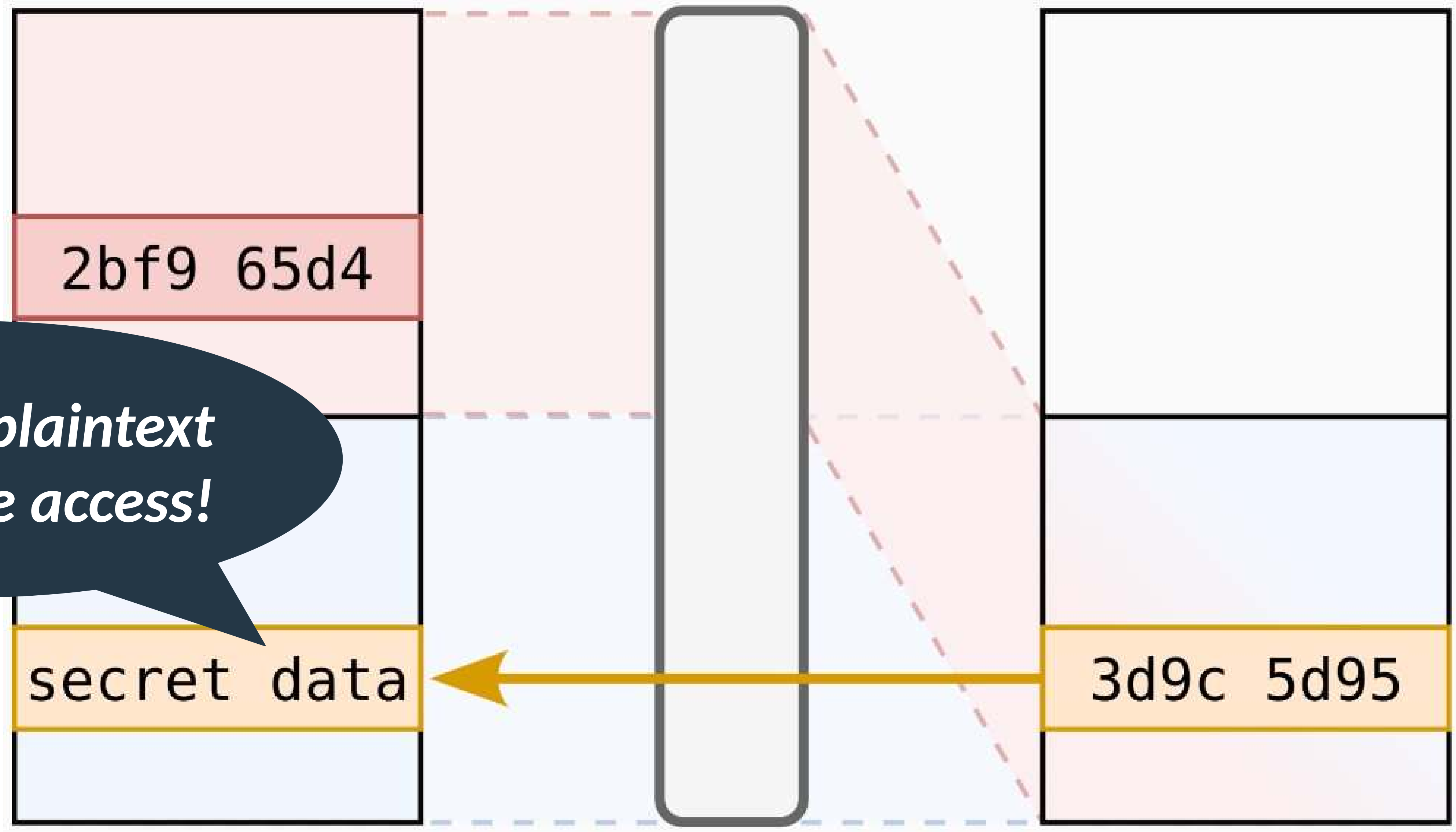
Battering RAM: Breaking Intel Scalable SGX Memory Encryption



Battering RAM: Breaking Intel Scalable SGX Memory Encryption



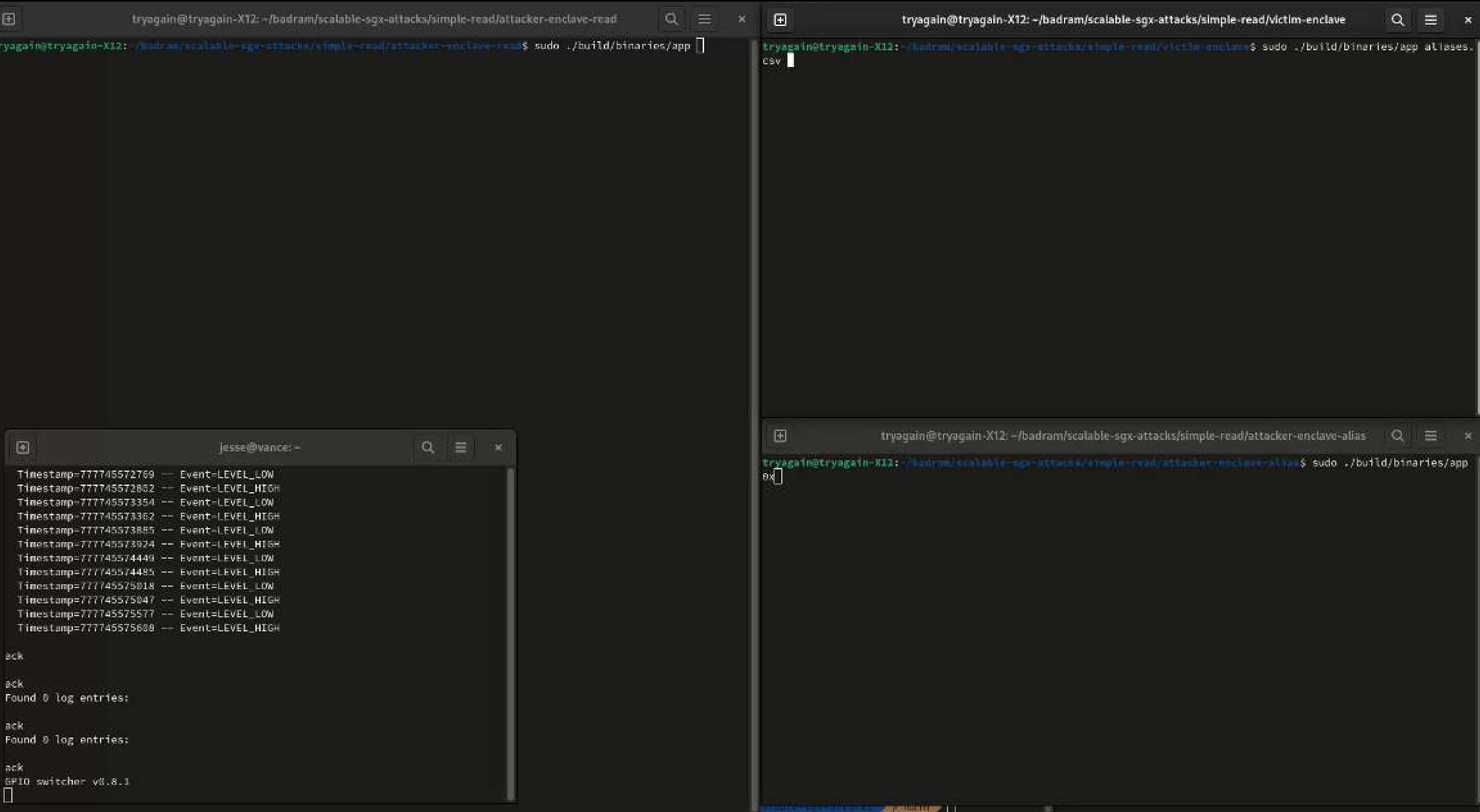
Battering RAM: Breaking Intel Scalable SGX Memory Encryption



Arbitrary plaintext read/write access!

Demo

Arbitrary plaintext access on Intel Scalable SGX

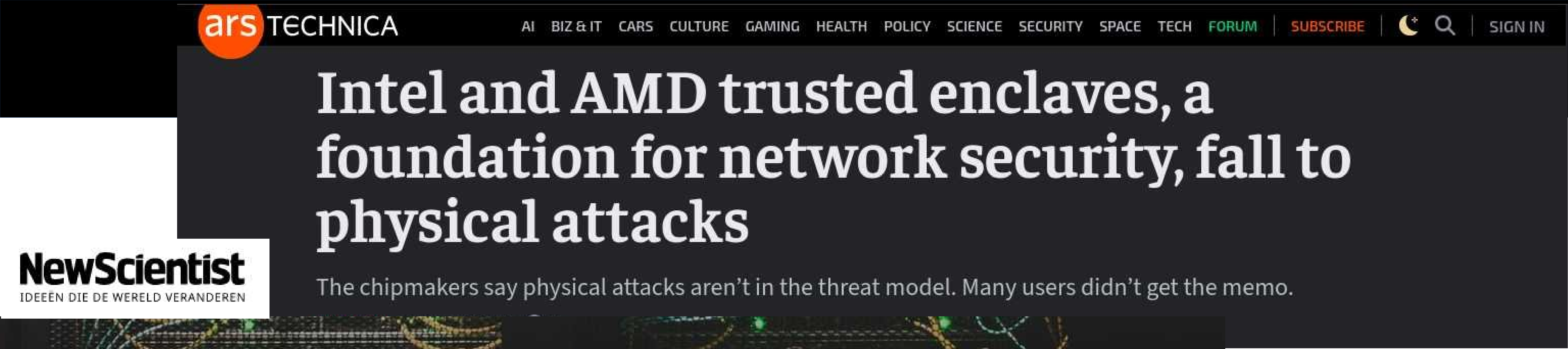

tryagain@tryagain-X12: ~/badram/scalable-sgx-attacks/simple-read/attacker-enclave-read
tryagain@tryagain-X12: ~/badram/scalable-sgx-attacks/simple-read/victim-enclave
jesse@vance: ~
tryagain@tryagain-X12: ~/badram/scalable-sgx-attacks/simple-read/attacker-enclave-alias

```
yagain@tryagain-X12:~/badram/scalable-sgx-attacks/simple-read/attacker-enclave-read$ sudo ./build/binaries/app
```

```
tryagain@tryagain-X12:~/badram/scalable-sgx-attacks/simple-read/victim-enclave$ sudo ./build/binaries/app aliases.
csv
```

```
  Timestamp=777745572769 -- Event=LEVEL_LOW
  Timestamp=777745572832 -- Event=LEVEL_HIGH
  Timestamp=777745573354 -- Event=LEVEL_LOW
  Timestamp=777745573362 -- Event=LEVEL_HIGH
  Timestamp=777745573885 -- Event=LEVEL_LOW
  Timestamp=777745573924 -- Event=LEVEL_HIGH
  Timestamp=777745574449 -- Event=LEVEL_LOW
  Timestamp=777745574485 -- Event=LEVEL_HIGH
  Timestamp=777745575018 -- Event=LEVEL_LOW
  Timestamp=777745575047 -- Event=LEVEL_HIGH
  Timestamp=777745575577 -- Event=LEVEL_LOW
  Timestamp=777745575608 -- Event=LEVEL_HIGH

ack

ack
Found 0 log entries:

ack
Found 0 log entries:

ack
GPIO switcher v0.8.1
```

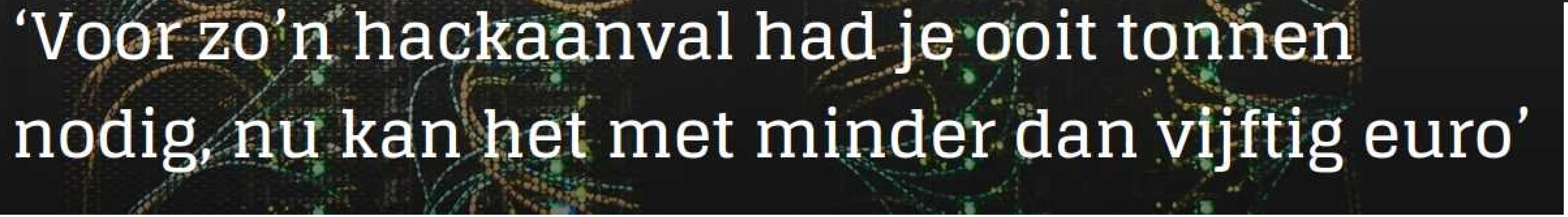
```
tryagain@tryagain-X12:~/badram/scalable-sgx-attacks/simple-read/attacker-enclave-alias$ sudo ./build/binaries/app
0x
```


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

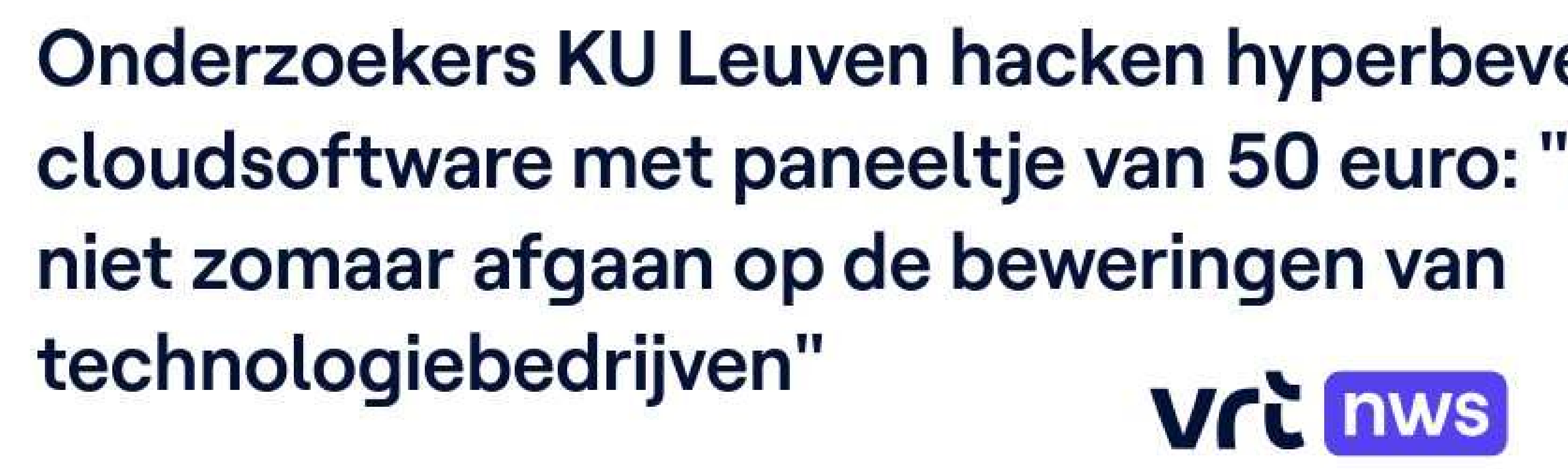
Intel and AMD trusted enclaves, a foundation for network security, fall to physical attacks

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

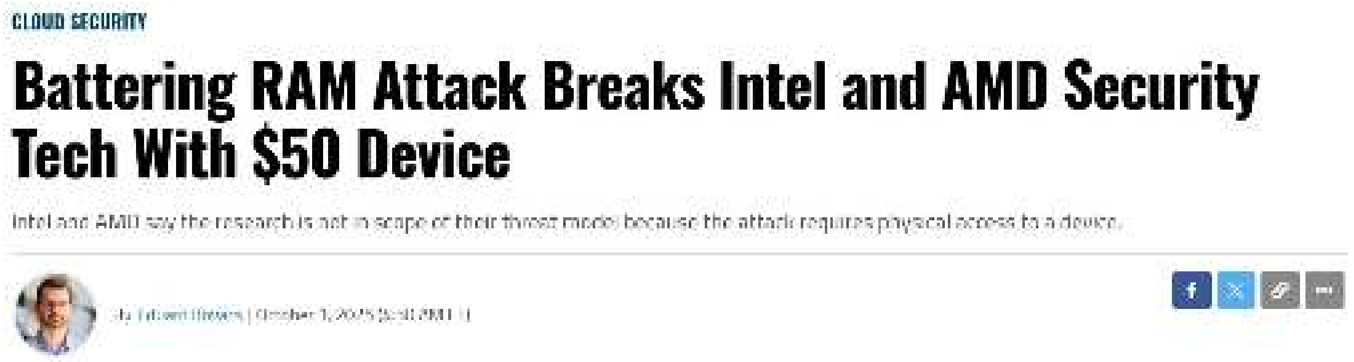
NewScientist
IDEEEN DIE DE WERELD VERANDEREN



‘Voor zo’n hackaanval had je ooit tonnen nodig, nu kan het met minder dan vijftig euro’



Onderzoekers KU Leuven hacken hyperbeveiligde cloudsoftware met paneeltje van 50 euro: "Zeker niet zomaar afgaan op de beweringen van technologiebedrijven"



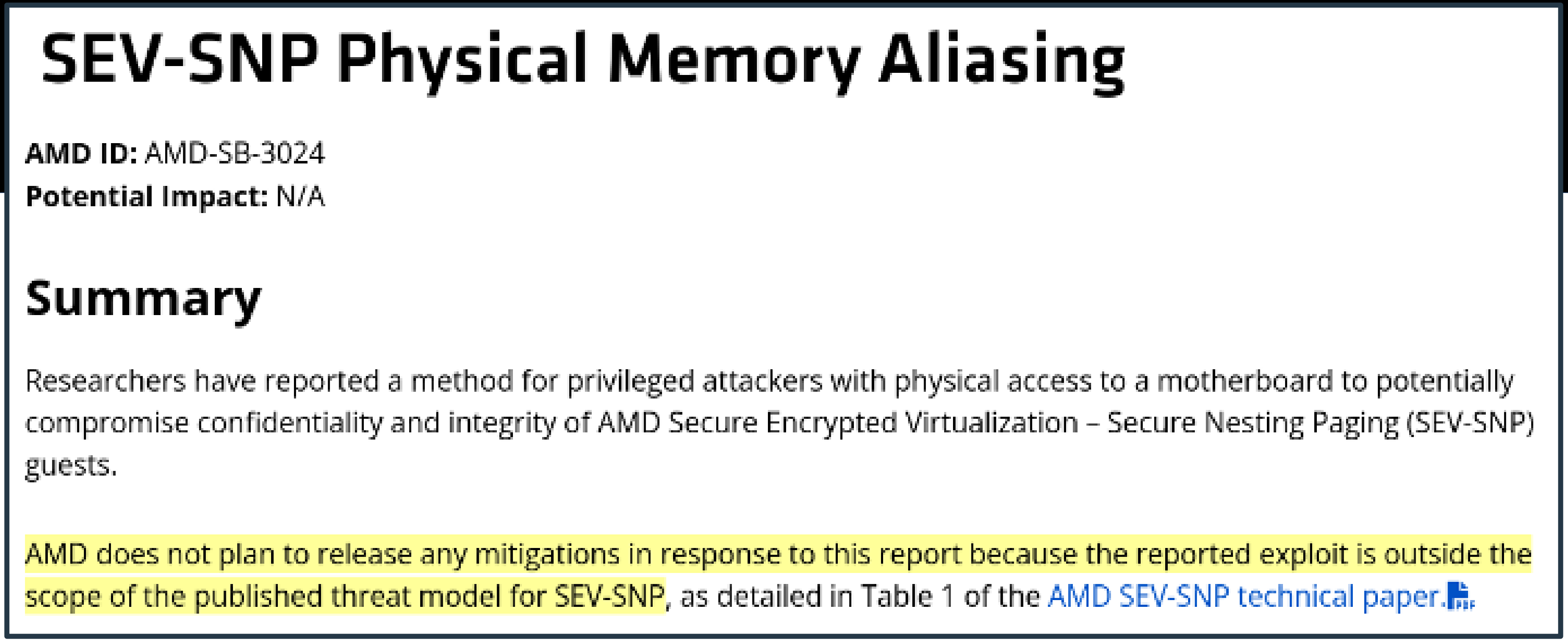
CLOUD SECURITY

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

🌍 https://batteringram.eu/



SEV-SNP Physical Memory Aliasing

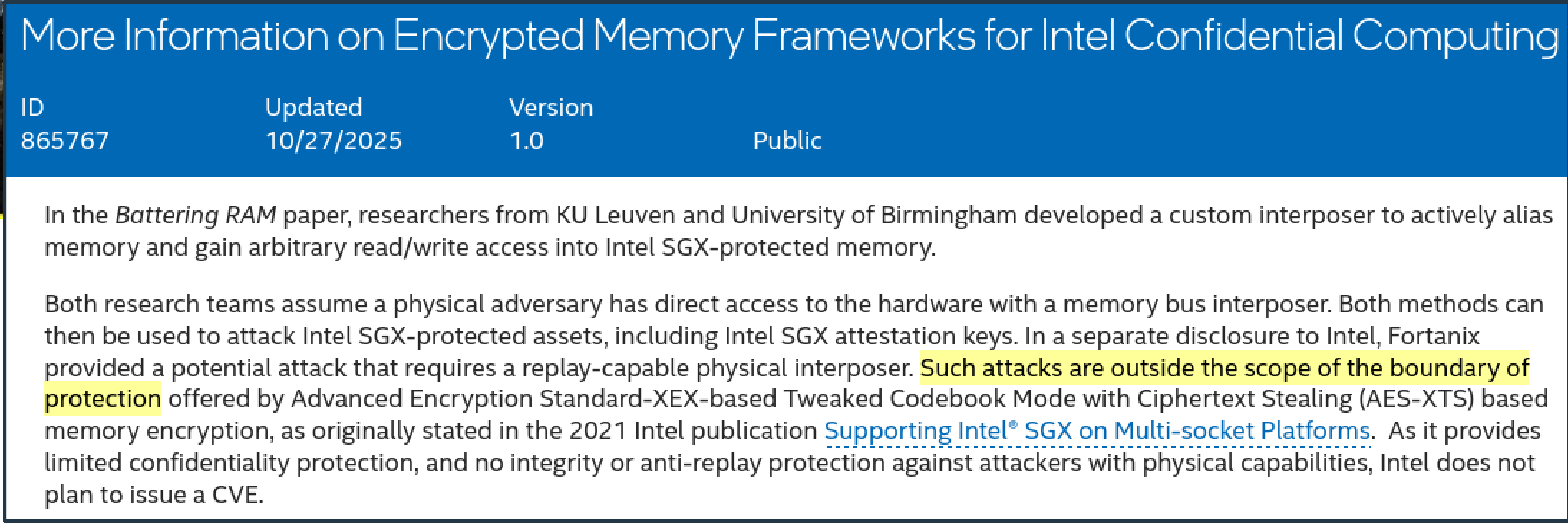
AMD ID: AMD-SB-3024
Potential Impact: N/A

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



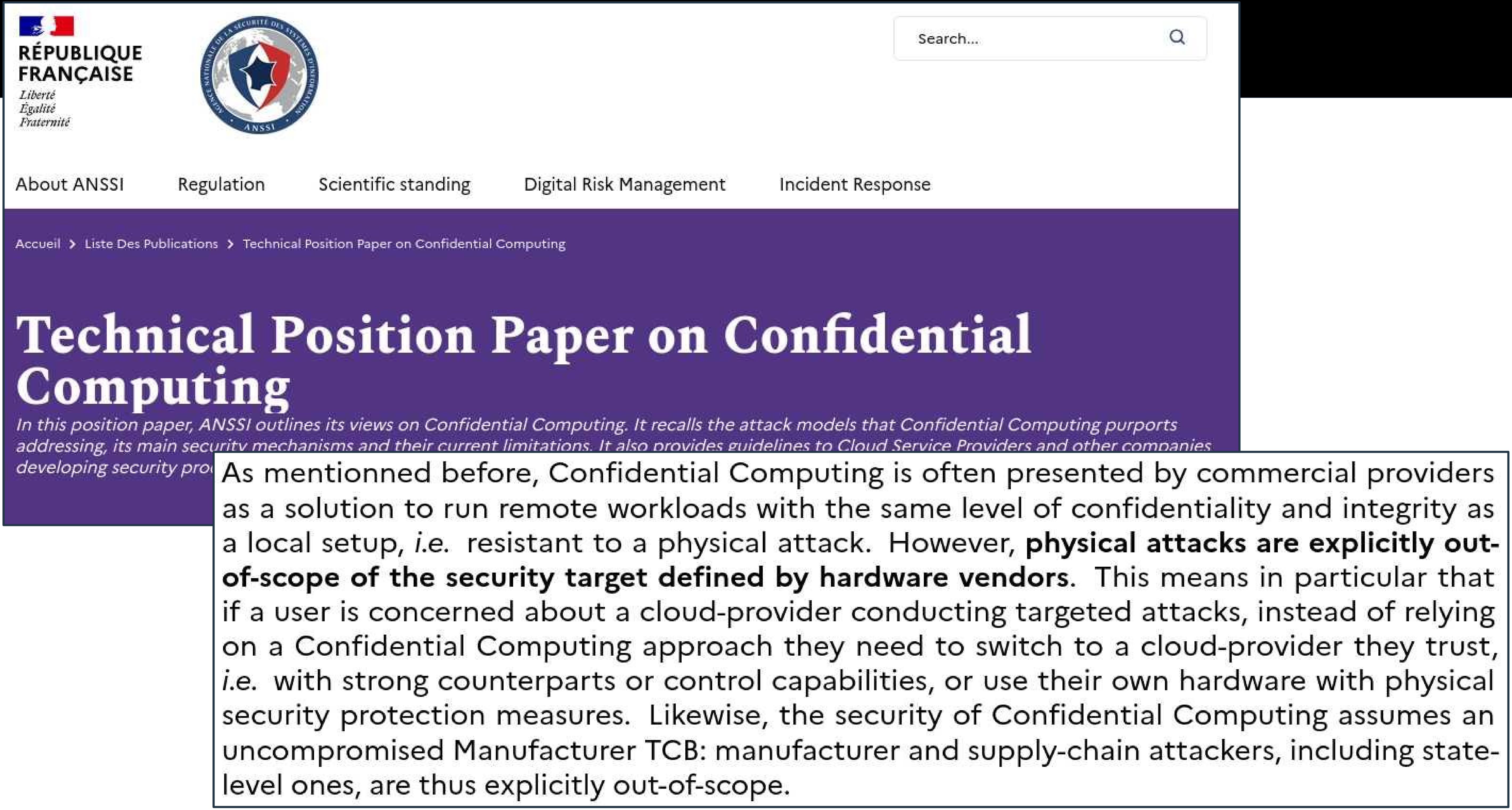
More Information on Encrypted Memory Frameworks for Intel Confidential Computing

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



RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

Search...

About ANSSI Regulation Scientific standing Digital Risk Management Incident Response

Accueil > Liste Des Publications > Technical Position Paper on Confidential Computing

Technical Position Paper on Confidential Computing

In this position paper, ANSSI outlines its views on Confidential Computing. It recalls the attack models that Confidential Computing purports addressing, its main security mechanisms and their current limitations. It also provides guidelines to Cloud Service Providers and other companies developing security pro

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

Lessons Learned

1. **Confidential computing** is here to stay
2. Challenge your **attacker models**
3. **Hardware attacks** are practical

Thank you! Questions?