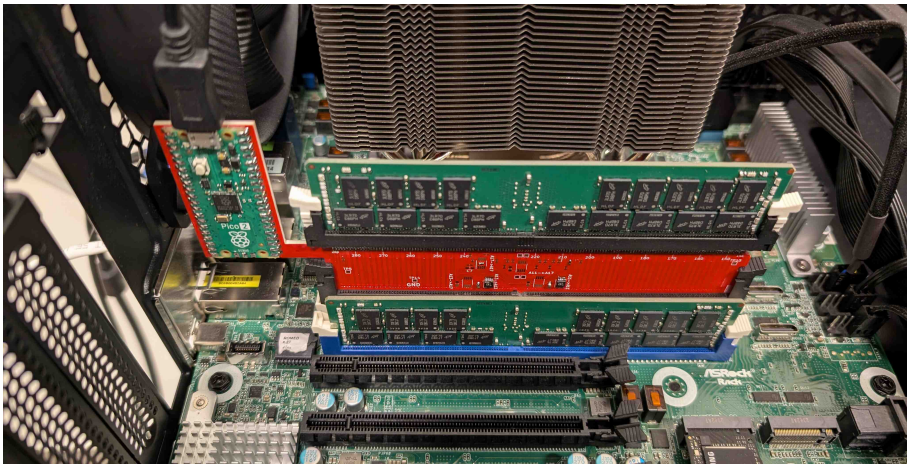
Trust No DIMM: Securing Memory Against Low-Cost Hardware Interposers



Modern computing systems rely on main memory as a fundamental component for storing and executing programs. Ensuring memory confidentiality and integrity is critical in scenarios where multiple tenants share the same physical hardware, such as in cloud computing. To provide these guarantees, modern CPUs enforce strict memory isolation to shield data from software-level compromises, and employ memory encryption to defend against physical attacks on external memory. However, recent research has demonstrated that these protections can be bypassed through memory aliasing, instantiated via either malicious DIMM configurations[1] or low-cost hardware interposers[2]. By undermining the expected memory topology, physical adversaries can completely break the security guarantees of modern Trusted Execution Environments (TEEs). This highlights the urgent need for robust countermeasures to secure encrypted memory against physical manipulation.

In this thesis, you will explore and develop novel defenses to make server memory architectures more resilient against physical adversaries. The project begins with a critical analysis of existing memory protections to identify their specific limitations against physical tampering. Following this, you will design and implement new memory protection mechanisms. Depending on your background and interests, potential research directions include: hardening the DRAM command bus, designing scalable and lightweight freshness protections, or integrating run-time aliasing detection. The proposed defenses will be validated by either implementing and evaluating the hardware modifications on a RISC-V softcore or software simulations. Because of the multiple possible research directions for this topic, it is strongly encouraged to contact us before making commitments.

Practicalities

Promotor:	Ingrid Verbauwhede Jo Van Bulck		
Daily supervisor:	Jesse De Meulemeester	jesse.demeulemeester@esat.kuleuven.be	office 01.21
Nature of the work:	30% literature, 20% theoretical work, 50% implementation		
Number of students:	1		

[1] J. De Meulemeester et al. 2025. BadRAM: Practical Memory Aliasing Attacks on Trusted Execution Environments. IEEE S&P'25. https://badram.eu/badram.pdf

[2] J. De Meulemeester et al. 2025. Battering RAM: Low-Cost Interposer Attacks on Confidential Computing via Dynamic Memory Aliasing. IEEE S&P'26. https://batteringram.eu/batteringram.pdf