Format inspired by NWO reviewer guidelines and templates.

Identification

Proposal title: Reverse Engineering of Memory Controllers

Overall assessment

Explain in one sentence or short paragraph how you see the entire project.

The proposal proposes a project about reverse engineering the memory mapping function of an MMU via performance counters, which has already been studied in the past.

Final score. How do you assess the entire application? Please give the final score for this proposal. Consider doing this after completing the rest of the application.

The final grade for this proposal is, in your view:

three (3)

Use the following scores in your grading:

Score	Meaning
10	Outstanding, must fund
9	Excellent, must fund
8	Very good, should fund
7	Good overall with one aspect very good, fund if room
6	Good, fund if room
5	Sufficient, fund if room
4	Insufficient, do not fund
3	Bad, do not fund
2	Very bad, do not fund
1	Does not meet academic level, do not fund

Please explain your answers. Try to exceed the length of 50-100 words per answer only when absolutely necessary.

Question 1. What is the scholarly, scientific or technological relevance of the problem? Is the problem original, timely, challenging? Is this a new line of research?

Answer:
The problem is timely because the Rowhammer problem is still not completely fixed. Understanding the memory controller can help in finding Rowhammer mitigations. The problem is not original however and several studies have studied this topic before [1,2].

Question 2. What are the innovative and original aspects of the proposal? Are the project objectives challenging and scientifically ground-breaking? Is the methodology credible?

Answer:
The innovative aspect of the proposal is the ability to control the physical address bit from virtual memory. The methodology is credible because reverse engineering DRAM mappings via performance counters has been proven before [1].

Question 3. Is the approach effective, including the practical work programme? How do you assess the program of work described in the proposal (realistic, feasible, ...)? Are the most important risks identified and effectively mitigated?

Answer:
The work programme is realistic yet a bit short for a four year project. The most important risks are identified.

Question 4. Is the proposal well-written and are the project's objectives clearly worded? Do you expect this project will lead to significant advancement of scholarship, science, or technology (academic impact)?

Answer:
The academic impact will be low as previous studies have done very similar work. Reverse engineering DRAM mappings is useful for security research, such as mitigating Rowhammer.

Question 5. What is your opinion on the societal impact of the proposed research? Are the expected results of the research relevant for solving a popular/economic/cultural/ technical or policy-related challenge?

Answer:
The societal impact of the proposed research are limited to helping security researchers and hardware vendors with trying to mitigate DRAM vulnerabilities such as Rowhammer.

Question 6. Are the main stakeholders of the problem clearly identified and addressed in the proposal? If any, what are the most important stakeholders the proposal does not address?

Answer:
The main stakeholders are addressed. Namely, security researchers and hardware vendors.

Question 7. Is the release of data and software artifacts clearly identified and addressed in the proposal?

Answer:
The proposal does not describe how it plans to release data and software artifacts.

Question 8. Are the main ethical concerns clearly identified and addressed in the proposal? If any, what are the most important ethical concerns the proposal does not address?

Answer:
The main ethical concern is the possible violation of intellectual property, which is addressed in the proposal.

Please identify at least 3 of the main strengths of the proposal:

Answer:
S1. The proposed methodology is sound and realistic.
S2. The proposed risk mitigation plan is good.
S3. The relevance of the problem is clearly explained by giving the example of multiple tenants sharing a server.

Please identify at least 3 of the main weaknesses of the proposal:

Answer:
W1. The proposed research is not original.
W2. The proposed research is not big enough for a four year project.
W3. It is not clear what artifacts are produced and in what form the results are going to be delivered.

[1] C. Helm, S. Akiyama and K. Taura, "Reliable Reverse Engineering of Intel DRAM Addressing Using Performance Counters," *2020 28th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, Nice, France, 2020, pp. 1-8, doi: 10.1109/MASCOTS50786.2020.9285962.
[2] Barenghi, A., Breveglieri, L., Izzo, N., & Pelosi, G. (2018, July). Software-only reverse engineering of physical DRAM mappings for RowHammer attacks. In *2018 IEEE 3rd International Verification and Security Workshop (IVSW)* (pp. 19-24). IEEE.