Format inspired by NWO reviewer guidelines and templates.

Identification

Proposal title: Selective Cache Flushing for Spectre

Overall assessment

Explain in one sentence or short paragraph how you see the entire project.
The proposed project has the potential to solve Spectre in hardware but contains several pitfalls.

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:

four (4)

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:
This is not a new line of research, several studies on this topic have been conducted. It is however both timely and challenging because several processors are still vulnerable for Spectre and it is a difficult problem to solve without degrading performance too much.

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 online detection of Spectre attacks in hardware is innovative and challenging. It will be challenging to keep the detector small enough to not impact performance too much. It will also be challenging to make the detector accurate, especially if generalized over all processors and workloads. The methodology is credible because the Spectre attack consists of two phases with distinct characteristics.

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 proposal seems small for a four year project. Reverse engineering the branch predictor of one CPU is feasible, but I have doubts about the feasibility of generalizing over all possible workloads and generalizing potentially over the behavior of several branch predictors. Flushing the targeted address as a mitigation is an observable side-effect, which could introduce a new vulnerability. The risk of not being able to accurately detect the attack is missing. Additionally, making the proposed predictor performant and not take up too much valuable chip space will be challenging.

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 proposal is very well-written and the objectives are clearly worded. If successful, the project could lead to a new way to mitigate Spectre attacks which is a from of technological advancement.

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 results from the proposed research are relevant for the security of hardware designs, which has an impact on data confidentiality and overall societal stability.

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:
Hardware vendors are implicitly named as a main stakeholder of the problem. However, any user of a CPU is also an important stakeholder of the problem: from consumers to businesses.

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

Answer:
It is not described how the results from reverse engineering a branch predictor are going to be released and it is insufficiently clear if and if so how the chip design is going to be published.

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 most important ethical concern that is not addressed is the potential violation of protected intellectual property by reverse engineering a branch predictor.

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

Answer:
S1. Solves the Spectre problem completely in hardware with no need for software mitigations, in contrary to many related studies.
S2. The project has potential for a big impact.
S3. The methodology is credible but with enough open questions for research.

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

Answer:
W1. No comparison with state-of-the-art.
W2. Small project for four years of work.
W3. Limited knowledge utilisation or valorisation.
W4. Flushing the targeted address on Spectre detection opens the possibility of a new side-channel.