FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Review report of a final thesis

Reviewer:	Ing. Marina Shchavleva
Student:	Bc. Jan Havránek
Thesis title:	Leveraging Cache-Based Side-Channel Attacks for Coverage-Guided Fuzzing
Branch / specialization:	Computer Security
Created on:	23 August 2022

Evaluation criteria

1. Fulfillment of the assignment

[1] assignment fulfilled
▸ **[2] assignment fulfilled with minor objections**
[3] assignment fulfilled with major objections
[4] assignment not fulfilled

While author did not succeed in the ultimate goal of creating and evaluating the fuzzer, he definitely performed necessary steps to prove that such technique is feasible, even though it requires future work to bring it closer to a complete feedback component.

2. Main written part

65 / 100 (D)

The work is very concise and describes only topics relevant for the assignment, although some deserve a better coverage. For example, a more detailed description of coverage-guided fuzzing and feedback mechanisms specifically would be beneficial, as it would make it clearer how exactly should side-channel analysis aid the fuzzing. Figure 3.1. could have a better description of what exactly produces the noise: heat map pattern looks very regular. Overall text is shorter than it is expected from master's thesis.

Language and style are great, with occasional typos and other more significant mistakes. Page 19 right before listing has paragraph which contains word "The" and nothing else. On page 34 in the last paragraph there is missing reference, probably to a figure 5.7, and figure 5.8 is never referenced; both figures are not properly described in the text. Same problem is on page 35, where in description of figure 5.7 there is another missing reference, probably to figure 5.6. The same paragraph on page 34 ends with a comma, presumably because of a missing descriptions of multiple figures.

3. Non-written part, attachments 85 /100 (B)

Author implemented two utilities for future development of the fuzzer. Although those are seemingly not finished (judging by the amount of to-dos in the code), they performed well and could be a decent stepping stone for further analysis.

4. Evaluation of results, publication outputs and awards 90 /100 (A)

The work provides a solid base for future research into usage of cache side-channel analysis as fuzzing feedback component. It shows useful techniques for noise reduction, which are extremely important for successful signal extraction. It also provides a functioning flushing module, which might be later adapted for other techniques.

The overall evaluation 75 /100 (C)

The practical part, design of flusher and analysis of different noise reduction techniques, is well done, but theoretical part might benefit from deeper description of attacks and fuzzers. The goal is far reaching, and it is understandable that author was not able to fully achieve goals stated in the assignment. Still, entire work is marked by the lack of time and the written part suffered most from it. Therefore, I grade this work with C.

Questions for the defense

What produced vertical orange lines seen in heat maps showing cache usage?
Is there a possibility to improve attack on devices with different inclusiveness policies by using different approach such as Flush+Reload, Prime+Probe, etc?
For devices with the same inclusiveness policy, are there any advantages of Flush+Flush approach?

Instructions

Fulfillment of the assignment

Assess whether the submitted FT defines the objectives sufficiently and in line with the assignment; whether the objectives are formulated correctly and fulfilled sufficiently. In the comment, specify the points of the assignment that have not been met, assess the severity, impact, and, if appropriate, also the cause of the deficiencies. If the assignment differs substantially from the standards for the FT or if the student has developed the FT beyond the assignment, describe the way it got reflected on the quality of the assignment's fulfilment and the way it affected your final evaluation.

Main written part

Evaluate whether the extent of the FT is adequate to its content and scope: are all the parts of the FT contentful and necessary? Next, consider whether the submitted FT is actually correct – are there factual errors or inaccuracies?

Evaluate the logical structure of the FT, the thematic flow between chapters and whether the text is comprehensible to the reader. Assess whether the formal notations in the FT are used correctly. Assess the typographic and language aspects of the FT, follow the Dean's Directive No. 52/2021, Art. 3.

Evaluate whether the relevant sources are properly used, quoted and cited. Verify that all quotes are properly distinguished from the results achieved in the FT, thus, that the citation ethics has not been violated and that the citations are complete and in accordance with citation practices and standards. Finally, evaluate whether the software and other copyrighted works have been used in accordance with their license terms.

Non-written part, attachments

Depending on the nature of the FT, comment on the non-written part of the thesis. For example: SW work – the overall quality of the program. Is the technology used (from the development to deployment) suitable and adequate? HW – functional sample. Evaluate the technology and tools used. Research and experimental work – repeatability of the experiment.

Evaluation of results, publication outputs and awards

Depending on the nature of the thesis, estimate whether the thesis results could be deployed in practice; alternatively, evaluate whether the results of the FT extend the already published/known results or whether they bring in completely new findings.

The overall evaluation

Summarize which of the aspects of the FT affected your grading process the most. The overall grade does not need to be an arithmetic mean (or other value) calculated from the evaluation in the previous criteria. Generally, a well-fulfilled assignment is assessed by grade A.