FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Supervisor's statement of a final thesis

Supervisor:	Dr. Marcel Busch
Student:	Bc. Jan Havránek
Thesis title:	Leveraging Cache-Based Side-Channel Attacks for Coverage-Guided Fuzzing
Branch / specialization:	Computer Security
Created on:	24 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

The initial goal of this thesis was to investigate cache-based timing
side-channels to aid coverage-guided fuzzers exploring a given target. The student managed to recreate and extend existing research from 2016 in his thesis but did not advance the research in the direction initially planned. The student's work can measure data accesses in cross-core scenarios (one core controlled by the attacker, the other controlled by the victim) and significantly reduces the noise of experimental measurements. Still, it does not demonstrate any usability to measure the victim's core code access. The latter is the side channel this project was concerned with. Reproducing the research from 2016 (ARMageddon) is an important step for this project, and the conducted engineering is solid. Still, for the amount of time that was available for this project, the results are sparse.

2. Main written part 69/100 (D)

Writing takes time. The student underestimated how long it takes to present concepts and thoughts in written form. The document seems unfinished and lacks polishing. However, the primary concepts of this work are present, and the core parts are well-written. Due to the lack of time, the document does not explain why all of the conducted experiments are insufficient to aid coverage-guided fuzzers and an outlook of research directions that could advance the current system in the originally intended direction.

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

All the software components implemented are well-engineered and functional. The components are a solid basis for future research on the topic.

4. Evaluation of results, publication outputs and awards 75/100 (C)

Especially the noise reduction techniques are well-engineered and will serve future research. A proof of concept demonstrating a cache-based timing side-channel for code coverage in cross-core scenarios is missing. Thus, the original question of whether these side channels can be used for coverage-guided fuzzing remains unanswered.

5. Activity of the student

[1] excellent activity

[2] very good activity

[3] average activity

▸ **[4] weaker, but still sufficient activity**

[5] insufficient activity

Jan is a great engineer and likes to tinker with technical challenges. Jan and I had many discussions about technical challenges, and we came up with satisfying solutions. I am confident that Jan understood the goal of this project. During this project, he made only minor steps towards this goal. In the given amount of time, I would have expected more progress.

6. Self-reliance of the student

[1] excellent self-reliance

[2] very good self-reliance

▸ **[3] average self-reliance**

[4] weaker, but still sufficient self-reliance

[5] insufficient self-reliance

Given an orally specified/whiteboard-discussed design, Jan is capable of engineering a solid solution. Given a more abstract idea or presented with a distant goal that requires some groundwork and experimentation, he requires a lot of guidance.

The overall evaluation 79/100 (C)

It was great to work with Jan, although the initial goal was not met in his thesis. The challenges he touched are solved to my fullest satisfaction. He sometimes lacks the ability to see the bigger picture and act/prioritize his tasks in a goal-oriented way (his biggest challenge during this work). Overall, future research will benefit from his research, which is a great contribution for a master's thesis.

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.

Activity of the student

From your experience with the course of the work on the thesis and its outcome, review the student's activity while working on the thesis, his/her punctuality when meeting the deadlines and whether he/she consulted you as he/she went along and also, whether he/she was well prepared for these consultations.

Self-reliance of the student

From your experience with the course of the work on the thesis and its outcome, assess the student's ability to develop independent creative work.

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.