



Supervisor's statement of a final thesis

Student: Tomáš Zvara
Supervisor: Ing. Josef Kokeš
Thesis title: Analysis of the Meltdown attack
Branch of the study: Computer Security and Information technology

Date: 19. 5. 2019

| | |
|--|--|
| <i>Evaluation criterion:</i> | <i>The evaluation scale: 1 to 4.</i> |
| 1. Fulfilment of the assignment | <u>1 = assignment fulfilled,</u> 2 = assignment fulfilled with minor objections, 3 = assignment fulfilled with major objections, 4 = assignment not fulfilled |
| <i>Criteria description:</i> 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. | |
| <i>Comments:</i> The assignment focuses on the Meltdown attacks against modern CPUs. The student was tasked to research the attack and the conditions for its successful execution, then implement the attack for both Linux and Windows, and finally evaluate his results and the effectiveness of available defenses against the attack. This is quite a complex and difficult task, despite the fact that all the necessary theory has already been published. The student managed to fulfill it admirably well. | |
| <i>Evaluation criterion:</i> | <i>The evaluation scale: 0 to 100 points (grade A to F).</i> |
| 2. Main written part | 95 (A) |
| <i>Criteria description:</i> 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. 26/2017, 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. | |
| <i>Comments:</i> The textual part of the thesis is very logically structured. It starts with the description of the CPU components crucial to the execution of the attack and explains the necessary background to the kernel address space layout in both Linux and Windows. The key building blocks of the attack are explained and then used to prepare and execute the attack on both platforms, starting with a simple test case to showcase the cache covert channel and then expanding to the full-blown attack on the kernel memory. The text is easy to read and understand and contains very few errors (mostly incorrect articles or prepositions, sometimes mistypes). The technical aspect of the thesis is fine, only in the bibliography the text overflows the page box in a few cases. Speaking of bibliography, it's rich, used well and in accordance with standard practice. | |
| <i>Evaluation criterion:</i> | <i>The evaluation scale: 0 to 100 points (grade A to F).</i> |
| 3. Non-written part, attachments | 90 (A) |
| <i>Criteria description:</i> 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. | |
| <i>Comments:</i> The non-written part consists of a suite of test applications and the results of the measurements. None of these form a standalone application, but that wasn't requested - or necessary. Their main purpose is to provide a solid basis for the text, and this purpose is served well even in their current form. | |
| <i>Evaluation criterion:</i> | <i>The evaluation scale: 0 to 100 points (grade A to F).</i> |
| 4. Evaluation of results, publication outputs and awards | 95 (A) |

Criteria description:
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.

Comments:

The main result of the work is its clear explanation of the Meltdown attack, its prerequisites and effects, along with the demonstration code. An unforeseen development was the fact that even though Meltdown is a hardware attack, it apparently behaves very differently on different operating systems due to their different memory layouts: while the attack on the Linux kernel was highly successful, at least when the system was mostly idle, Windows proved much more of a challenge due to their more complex physical-to-virtual memory mapping. That is quite interesting on its own, and thanks to the use of English, available to readers worldwide.

Evaluation criterion:

The evaluation scale: 1 to 5.

5. Activity and self-reliance of the student

5a:

1 = excellent activity,
2 = very good activity,
3 = average activity,
4 = weaker, but still sufficient activity,
5 = insufficient activity

5b:

1 = excellent self-reliance,
2 = very good self-reliance,
3 = average self-reliance,
4 = weaker, but still sufficient self-reliance,
5 = insufficient self-reliance.

Criteria description:

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 (5a). Assess the student's ability to develop independent creative work (5b).

Comments:

The student was exceptionally active. He frequently attended the consultation sessions, and every single time was well prepared. He was also highly self-reliant, mostly it was he who came up with new ideas and proposals.

Evaluation criterion:

The evaluation scale: 0 to 100 points (grade A to F).

6. The overall evaluation

95 (A)

Criteria description:

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.

Comments:

The student handled his challenging topic exceptionally well. He understood the Meltdown attacks well enough to be able to explain their prerequisites, their inner workings and their effects, and was able to prepare proofs of code to demonstrate the attacks on live systems. He has shown that seemingly minor differences in the OS's memory organization can cause a significant difference in the actual execution of the attack, even though theoretically the attack should affect all systems equally. I find that quite impressive. For these reasons, I recommend the thesis to the defense and grade it A-excellent.

Signature of the supervisor: