FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Supervisor's statement of a final thesis

Student: Jaroslav Chládek
Supervisor: Ing. Josef Kokeš
Thesis title: Feasibility of the Spectre attack in a security-focused language
Branch of the study: Computer Security and Information technology

Date: 3. 6. 2019

Evaluation criterion: *The evaluation scale: 1 to 4.*

1. Fulfilment of the assignment

[✓ 1 = assignment fulfilled,]
2 = assignment fulfilled with minor objections,
3 = assignment fulfilled with major objections,
4 = assignment not fulfilled

Criteria description:
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.

Comments:
The student researched the Spectre attack and applied his insight to implementing it in Rust. While he did not succeed in completely eliminating the need for unsafe language constructs, he did provide suggestions on doing so which seem reasonable.

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

2. Main written part

80 (B)

Criteria description:
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.

Comments:
The textual part of the work is quite detailed and full of information. Unfortunately, it may be a bit difficult to read and understand for a reader because the information is sometimes spread over multiple parts of the text (e.g. we get hints on the results as soon as in the Spectre description). Also, the student tends to skip over parts which are "clear" when one had followed the whole process of the work being created but may have been useful to those who hadn't been there.

I am not too convinced about the final chapter where the student analyzes his measured results. The actual data is very interesting, particularly the differences between the behavior of the attack on the three systems tested, but I am not at all sure about the assumption that it's specifically the location of the secret string in memory what is causing these differences. In particular I miss a verification that the OSes used don't already implement mitigations against Spectre.

The text is written in the traditional academic style more so than in most other theses, and the language and grammar, while not perfect, are very good. Quite a few unexpected page breaks may surprise and/or annoy the reader.

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

3. Non-written part, attachments

95 (A)

Criteria description:
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.

Comments:
The attachments consist of the actual demonstration of the Spectre attack in Rust and of the measurements of various program runs. While the size of these parts is comparatively tiny, they represent a huge amount of work, including a lot of effort put into getting it right.

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

4. Evaluation of results, publication outputs and awards

90 (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 student chose a very ambitious topic, taking a known attack and extending it to an environment which isn't suitable for it. However, he was able to execute the attack, even if he had to resort to unsafe code, and he was able to propose techniques for escaping from the unsafe code. The actual execution of that is yet to be seen, if it is even possible - it seems that even without specific countermeasures Rust is quite resistant to Spectre.

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:

I have nothing but praise for the student here. He was one of the most active and self-reliant students I've ever had.

Evaluation criterion:

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

6. The overall evaluation

90 (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:

Overall, I consider this an excellent bachelor thesis. The student took a rather new vulnerability, researched how it works and then applied it to an environment which one might expect to be resistant to it. While he had to reduce the security sureties somewhat to make this happen, that was to be expected, and I highly value to proposals on executing the attack even in a fully secure variant of the language. Despite the doubts expressed in the evaluation of the text I grade the work A-excellent.

Signature of the supervisor: