FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Supervisor's statement of a final thesis

Supervisor:	Ing. Josef Kokeš
Student:	Bc. Josef Hušek
Thesis title:	Security Analysis of OnlyKey
Branch / specialization:	Computer Security
Created on:	1 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 assignment was mostly completed. However, 1) this is not at all clear from the text, 2) frequently completely missing from it and left to the reader's inference, and 3) I am not sure point 3b of the assignment was even attempted, much less completed.

2. Main written part 60/100 (D)

The written part could use a lot of improvement. It desperately needs a revision, as the current version contains a great number of spelling errors, mistypes, incorrect typography, incorrect intra-document references and other errors. Its style doesn't quite reflect the academic standards, with a title "What I found" for a major chapter being the prime example. It is also quite unusual to place Conclusion as a second-to-last chapter and use it for other purposes than to summarize the methods and results.

Content-wise, I feel that too much space was used to describe the OnlyKey (chapter 2) and not enough on the methods used (not found). Despite this complaint, chapter 2 is certainly relevant and contains a lot of valuable information, but it is of a secondary importance to the description of methods. The actual findings are very nice and they do demonstrate that a lot of effort went into completing the work, but as a reader I need to know what was studied and in how much detail before I can rest contentedly knowing that no major vulnerabilities were found - I need some basis for belief that the reason they were not found is that they are not present, rather than because of an insufficient analysis.

3. Non-written part, attachments 60/100 (D)

The non-written part suffers from the same problem - it is there, it reflects the work done, but it is not described sufficiently to make it actually useful. Fortunately it is not particularly important in this type of work. But still, a lot of research went into it, it's unfortunate that it was largely left hidden among all the code without any easy way of even finding it, much less re-using it.

4. Evaluation of results, publication outputs and awards 80/100 (B)

Despite the rather sub-par realization of the previous points, the student's results are quite good. He spent a lot of time studying both the hardware and the software and the "What I found" chapter clearly shows that it was a time well spent - the student analyzed the code in detail and thought deep and hard about the possible implications of what he saw. The complaints about the written and non-written parts go towards the dependability and trustworthiness of the results, not towards their validity.

5. Activity of the student

[1] excellent activity
[2] very good activity
▸ **[3] average activity**
[4] weaker, but still sufficient activity
[5] insufficient activity

The student's activity was unbalanced. Sometimes he was quite active, consulting regularly, while other times weeks would go by without any contact. This was particularly unfortunate at the very end of the thesis work, because I never got a chance to see the full text before it was submitted.

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

I would say the student is quite self-reliant where the actual analysis work is concerned. Processing the results once they have been found presents a bit of a struggle for him.

The overall evaluation 70/100 (C)

The final thesis greatly suffers from its presentation which tends to focus on aspects that are not that important and skips over those that are, all the time distracting the reader with language and typography errors. The required work was done, the security analysis was performed and the discovered results are very good. If I were to base my evaluation on what I know about the thesis background, I could give it a much better grade. Unfortunately, I have to consider the work as submitted, and here the incorrect focus of the text, the lack of pre-print revision and the omission of methodology greatly detract from its value. Despite that, I think I can safely grade the thesis as Good.

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.