FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Review report of a final thesis

Student:	Bc. David Jagoš
Reviewer:	Ing. Josef Kokeš
Thesis title:	Security analysis of USB drive
Branch of the study:	Design and Programming of Embedded Systems

Date: 30. 5. 2018

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:

It is quite possible that most of the assignment was actually fulfilled. However, that is not apparent from the supplied materials (either the text or the data on the CD) - the thesis tends to skip all the details and jumps directly to conclusions. That makes the results unverifiable and in the end, unreliable.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
2. Main written part	*40 (F)*

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 written part is extremely short - 33 pages. Out of that, 6 pages are blank and at least two more are filled with unnecessary images (e.g. photos of other flash drives). As a result, the text does not contain all the information it should contain. In particular, there is almost no objective support for the student's claims - starting with the ubiquitous assumption that the AES key is stored in the secure hidden area, without other considerations - e.g. a key derived purely from the user's password or a fixed key released when the right password is provided. This has been subsequently explained to me and I agree with the reasoning, but the fact remains that it should have been written in the work. I would like to state, though, that the research chapters 2-4 are very well done and the text in chapter 5 suggests that the student did far more work than he actually wrote about; the additional materials I received agree with this impression.

The factual correctness of the work is uncertain. The OSX version of the software is not written in Java (page 17), but if it was, it would be an extremely useful source of information for RE and worthy of exploration even without a machine to run it on (page 26). The methods used to analyze the program are described in a sketchy manner, and it's only through the additional materials that I can get a good idea of their correctness.

Grammatically, the work needs a lot more work. The incorrect articles are a pain but understandable, but missing words should not be present in the final version of the text. The same is true for typography, I noticed incorrect quotes (figure 1.2), dashes (page 9), overflowing text, forgotten function arguments (page 28), unsorted list of acronyms...

The thesis cites 13 sources, two of them being photos of other flash drives. 4 items in the bibliography show an incorrect author name (company name displayed as if it was a person's name). The first chapter (introduction to flash drives with hardware encryption) does not cite *any* sources because it doesn't rely on any, chapter 4 (Phison flash drive controllers) cites only one source at the very end of the chapter, even when other sources have apparently been used (e.g. figure 4.1).

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
3. Non-written part, attachments	*50 (E)*

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 short length and the lack of verifiable data applies to the attachments, too. The CD does not contain *any* student's work except for the actual thesis text. I received extra materials after asking for them, but once again they are not verifiable; the only place which exhibits the student's contribution is the re_notes.txt file (missing on the CD) which contains some 7 KB of bits and pieces discovered during the reverse engineering. That would be a worthwhile portion of the thesis if it was included on the CD and preferably explained in the text in more detail.
What is on the CD, and probably shouldn't be, are the different versions of Phison MPALL application (in the absence of any file detailing the license, we have to assume that the application may not be distributed) and particularly the datasheets (marked as "Micron confidential and proprietary", "Any portion of this paper shall not be reproduced..." etc.). I can appreciate that they are highly relevant to the work, but they should have been cited properly rather than placed on the CD.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
4. Evaluation of results, publication outputs and awards	*30 (F)*

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:

I am afraid that the thesis as-is does not contain many results to evaluate. The thesis presents ideas and hypotheses which are neither supported nor disproved by the data provided within and no important question has been answered. I understand that without extra devices to experiment on the student was disinclined to perform risky actions which might destroy the flash disk, but there were other options. It turns out that these options have in fact been exercised, but again there's no mention of that in the supplied materials.
Personally, I am convinced that after all else had failed, even the potentially destructive action should have been attempted. That would be more in-line with the student's branch of study than reverse-engineering applications, anyway.

Evaluation criterion:	*No evaluation scale.*
5. Questions for the defence	

Criteria description:
Formulate questions that the student should answer during the Presentation and defence of the FT in front of the SFE Committee (use a bullet list).

Questions:

Can you give a brief summary of the work you did in addition to what you described in the text?

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
6. The overall evaluation	*40 (F)*

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:

In its current version, the thesis can't be successfully defended, for the following reasons:
1) The text is way too short and incomplete. Due to that, the results within are largely unfounded. This is my major objection.
2) The work with external sources needs to be much more precise. Chapter 1 requires references to show that it is founded on facts, chapter 4 must clearly specify which sources it is based on.
3) The potentially illegal content of the attached CD must be clarified.
Note that I am evaluating the thesis as it appears in its printed form and on the official CD. After going over the additional materials I requested and after consulting the matters with the student, I am now convinced he actually did perform a majority of the work that I require in my review. But I can't recommend the submitted version of the thesis for defense.

Signature of the reviewer: