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: 14. 1. 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 assignment asked for a security analysis of the Kingston DataTraveler Vault Privacy encrypted flash drive, with a particular focus at extracting the data without knowing the password. The thesis fulfills this requirement: The component parts of the drive were analyzed and their security implications evaluated, both the hardware and the software, which I consider quite admirable - each of these aspects requires a radically different approach and it's not at all easy to handle them both.

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

2. Main written part

75 (C)

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 of the thesis was the major cause of its failure last year. This year's version written part is much improved, although still some issues remain. The work now covers the necessary aspects of the thesis and the citations are much more satisfactory, although the first chapter would still benefit from better references - particularly, if a reference can't be found, perhaps that claim should be removed rather than kept without a note (e.g. the claim that archive managers are among the most commonly used tools for protecting data, chapter 1.1.1.1). The grammar of the work has been improved, though some issues remain (e.g. the work with articles); despite these issues, the ideas are related clearly, even if the flow of the information is not as natural as I would like. In chapter 6, two incorrectly bound references appear (on page 36 and 37). My major objection to the written part is that in several places it is more of a story than a technical report, which tended to annoy me while reading (e.g. page 41). It also led to the work being less information rich than would be desirable. Still, this does not prevent the work from being successfully defended.

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

3. Non-written part, attachments

90 (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 attached materials are suitable for their purpose - to demonstrate the analyses performed while writing the thesis. I wasn't able to actually make use of the .idb file because it was created with a newer version IDA Pro than I have, but I saw the generated files and they contain what I would expect.

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

4. Evaluation of results, publication outputs and awards

85 (B)

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 find the results quite interesting, and I am certain they would be of interest to other users of encrypted flash drives as well. It seems that the drive's manufacturer has fixed the issues of the previous generation of drives, e.g. the ability to easily access the data without knowing the password. The behavior of the drive when changing the password and resetting the drive is encouraging. The fact that the student did not find any major weakness is not a problem at all - quite the opposite, in fact, with a well-designed solution we expect to find just that. But there is a caveat, embodied in the first question for the defense.

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:

1) How do you explain the appearance of decrypted empty data (figure 6.1, data files in the re/ha_dump directory) in respect to AES/CBC presumably used for encryption?

2) In the conclusion, you note that you consider the RSA-512 key hard-coded inside the application inadequate and recommend a different authentication scheme. What kind of a scheme would you consider adequate, particularly considering an attacker able to reverse-engineer the application?

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

6. The overall evaluation

82 (B)

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 think the revised thesis is a worthy addition to the student's resume. The work now much more clearly explains why the Kingston DataTraveler Vault Privacy flashdrive can be considered secure, although I find the state of the decrypted empty data disturbing. I highly value the student's ability to work meaningfully with both hardware and software, which I consider quite difficult. Despite the somewhat weaker text part, I recommend the thesis for the defense and suggest a grade B - very good.

Signature of the reviewer: