FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Supervisor's statement of a final thesis

Student:	Josef Hušek
Supervisor:	Ing. Josef Kokeš
Thesis title:	The use of cryptography in 7-zip
Branch of the study:	Computer Security and Information technology

Date: 29. 5. 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 an analysis of the 7-zip application with a particular focus on the tool's security. While most of the required aspects have actually been covered during the research, the thesis as submitted provides only a very limited indication of that. The description of the application's structure, components and relationships between them is extremely sketchy. The security analysis focuses mostly on the key generation and somewhat on the key management, but there is very little discussion of the secure coding and almost no mention of the security properties of the algorithms used.

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 was created literally at the last minute. As a result, the student had to complete it on his own, without any real input from me. That led to mistakes which could be easily fixed but unfortunately remain in the final version, among others numerous typos, grammatical errors, incorrect structure of sentences, rather informal language and a confusing logical structure. Most importantly, the work covers non-essential aspects, such as the logger component or the compilation processes, in great detail while omitting critical information - for example, the results of the password-cracking attempts are only shown in the files on the attached SD card, not in a table in the thesis! I am afraid in this form the text is unacceptable.

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:
There are three non-textual components provided:

The files used in the password-breaking attempts and the results thereof contain some of the required information, but sorely miss a detailed discussion. For example, an explanation of the huge variation in the cracking speed for files differing only in the password (e.g. large file with 2^19 of password repetitions) should be attempted. Not to mention that there's no mention of the hardware used, preventing the user from even estimating the number of checks they may expect with their (or their attacker's) hardware.

The logger component is functional but very very trivial.

The AES and buffer overflow testing application works and fulfills its purpose, but it is also very simple.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
4. Evaluation of results, publication outputs and awards	*80 (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:
Despite the complaints in the previous sections, I think the thesis actually provides some new and useful results.

First, I find the discoveries regarding the key derivation function, such as the lack of salt or the support for a seriously weakened KDF, very interesting - and disturbing. Unfortunately, the results are poorly presented in the text and more effort should have been put into the proposal of a real-world attack scenario which would demonstrate the need for a change in this area, but I am convinced the danger is real and it's important that the student discovered it.

Second, I consider the proposals on the characteristics of particularly vulnerable archives and the suggestions on how to create these archives without the user's knowledge valid and fairly important if one is to use 7-zip securely - it gives an implicit recommendation of how to build a difficult-to-attack archive. Still, that recommendation should have been explicit!

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:
While I appreciate the student's attempt to reduce demands on my time, this was apparently far too much of a concern, especially when considered along with the fact that the student often found it difficult to figure out a course of action. He did perform the work himself, but my overall impression is that he mostly did only what I told him to do.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
6. The overall evaluation	*50 (E)*

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:
I am afraid the thesis can barely be accepted. Both the textual and non-textual parts are very weak and would benefit significantly from more time spent on them. However, most of the required work was actually done, even if not described, and I think the discoveries mentioned in the "evaluation of results" justify the grade E-sufficient.

Signature of the supervisor: