FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Supervisor's statement of a final thesis

Student:	Anton Titkov
Supervisor:	Ing. Josef Kokeš
Thesis title:	Security analysis of Cryptomator
Branch of the study:	Computer Security and Information technology

Date: 15. 8. 2020

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:
In this second iteration the assignment was fulfilled. The level of detail is still somewhat low, but all required parts are there now.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
2. Main written part	*65 (D)*

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 text was significantly expanded over the original version, fixing many of my complaints. The two prior analyses of Cryptomator are now presented in more detail, the discovered vulnerabilities are now better explained and evaluated using CVSS, etc. Despite that, the work comes across as rather thin, in many cases I felt that a more detailed explanation of the student's reasoning would be beneficial. The first chapter was unfortunately left unchanged and as such its short length and lack of detail make it still very shallow and frequently either incorrect in misleading (e.g. the discussion of the advantages and disadvantages of different types of encryption is very problematic, with comments about a particular type often applying to all other types as well). I attribute this problem to the student's heavy reliance on one source of information.

I would not agree with all of the student's reasoning in the CVSS evaluation of the vulnerabilities, but I feel this falls within the bounds of reasonable differences in subjective points of view.

I noticed several grammatical or typographical errors such as missing periods at the end of sentences in bullet lists, incorrect quotes, some misspellings, an incorrect reference to figure 5.1, etc. I still like the figures very much.

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 application succeeds in reimplementing Cryptomator using alternative cryptographic libraries. All major functionalities have been implemented: It's possible to create a new encrypted vault as well as read and modify its contents. That gives us high assurance that the application was written according to its specifications while at the same time providing the users with an alternative way of accessing their vaults in case Cryptomator itself stops functioning.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
4. Evaluation of results, publication outputs and awards	*75 (C)*

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 results of this thesis are of mixed practical usefulness. The analysis itself would be useful for end users, except for the fact that a new version of Cryptomator, which fixes most of the discovered vulnerabilities, was published just before the thesis was completed; that's not a fault of the student, though. The supplied application may be useful for data recovery purposes as it provides an alternate way of accessing the encrypted vault's data; care should be taken, though, because that was not the application's primary purpose and as a result it doesn't really focus on accessing the vault securely. That's not helped by the lack of documentation.

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:

In this iteration, the student was much more active that in the previous one. The self-reliance was about the same - the student still depended on my input more than his own knowledge and abilities.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
6. The overall evaluation	*75 (C)*

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:

The improvements made to the thesis certainly qualify it for a successful defense. It now represents a reasonable security analysis of the Cryptomator that can stand on its own, and it does show that the student achieved some insight into the issues related to the security analyses. I still consider the text way too brief, though, and the first chapter too shallow - it might be OK for a student of a non-IT field, but not for a computer security student. For that reason I am grading the thesis C-good.

Signature of the supervisor: