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: 6. 6. 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:

The assignment was, technically speaking, fulfilled, but at the minimum level possible. The text is very short which makes it difficult to decide whether specific assignment requirements were or were not completed, and if they were, were they done correctly? For example, in task 3, "evaluate these areas for threats", some evaluation was performed, but I find it vexing that the term "threat" was never used in doing so, no threat evaluation methodology was mentioned, etc. That tends to make the whole work unreliable.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
2. Main written part	*30 (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 text is by far the weakest part of the thesis. It suffers greatly from being extremely short, to the extent that it is often very shallow, frequently incorrect (or at least failing to cover various caveats, corner cases or possible extensions), and generally difficult to read due to its seemingly disorganized structure caused by too extensive cutting of "unnecessary details" which would hold the text together. For example, the UI analysis is covered in half a page of text. The source code analysis omits all detail about what was analyzed and how (and why), skipping directly to the conclusions, given in the briefest form possible. For example, I would love to know more about the way passwords remain in memory even after they are no longer needed!

The online materials are cited without the date of citation and sometimes without the date of creation as well - and in some cases are very old, making them barely relevant (e.g. [1], [5], [8] and [22]). I find it quite annoying that the two existing security analyses of Cryptomator are only mentioned in passing as a sidenote of the student's source code analysis.

What I do like very much are the figures, they are beautifully done and improve the readability of the text a lot. But they should have been used as an addition to the information in the text, not as its replacement!

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
3. Non-written part, attachments	*70 (C)*

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:

As a part of his analysis the student prepared his own reimplementation of the Cryptomator's cryptographic core. He failed to explain why he did it and what are the consequences of his findings (see the previous point of this evaluation), but despite that it is a very important result because 1) it shows that Cryptomator really is implemented according to its specification, and 2) it gives the users a way of accessing their data even if Cryptomator itself suddenly becomes unusable.

Regarding the code quality, I am not too impressed. While I am not familiar with either of the programming languages used (Swift and Objective-C), and in fact don't quite understand what made it necessary to use both, the coding style doesn't seem to be written with security in mind - e.g. sensitive information is not deleted after use, magic values are used without explanation, there are virtually no comments throughout the code, etc. While that in itself is not a problem for a code designed to verify Cryptomator's claims, it does somewhat detract from the user benefit #2 mentioned in the previous paragraph.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
4. Evaluation of results, publication outputs and awards	*60 (D)*

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 the results of this thesis *as submitted* can't be applied in practice. While some of them would be worthwhile (e.g. the reimplementation of Cryptomator's crypto core), the decision to use fairly uncommon programming languages and the lack of documentation limit their usefulness. The text itself is, unfortunately, of little value due to its extreme brevity and the student's failure to explain the concepts, the decisions, the reasoning and the results.

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:

I rather suspect the student kept his thesis on ice except when he accidentally bumped into me at school - that elicited some activity for a short while, but it quickly died off again. The weaker self-reliance may be a contributing factor here - the student completed what I told him to do, but apparently thought that's all that needs to be done while I considered it just the starting point.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
6. The overall evaluation	*49 (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:

I found it very difficult to decide whether to give this thesis a passing grade or not. The security analysis was performed, even though it is not clear how much of it was performed and how dependable the results are. The textual part is woefully insufficient. The code is OK, even though it does not really seem like a product of a semester of hard work, but considering its purpose, it is adequate - but I can't help but feel it could've been quite useful if more effort were put into it. Overall, I would prefer if this thesis failed at this time, giving the student time to improve on the textual part and realize his full potential, but if a good presentation and defense is given, it can be accepted for a passing grade.

Signature of the supervisor: