FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Supervisor's statement of a final thesis

Student:	Ali Mammadov
Supervisor:	Ing. Josef Kokeš
Thesis title:	Improvements to the Off-The-Record Protocol
Branch of the study:	Computer Science

Date: 27. 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:
The assignment was fulfilled for the most part. However, the discussion of the practical feasibility of a computational attack should be discussed in more detail - while the thesis quite correctly focuses on the documented standards and best practices, a discussion of the current real-world successful computational attacks should also be present.

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 is rather short and densely packed, which causes parts of the text to be difficult to understand; also, some relevant topics are not discussed in as much detail as they would deserve. In particular, I think that the Authenticated Key Exchange is very hard on the reader. The Ciphersuite Agreement algorithm needs to be evaluated in more detail as it is a crucial part of any cryptographic protocol. Chapter 3 ends too abruptly - I would expect to see 1) a discussion of how the structure of the library and the pre-implemented classes adhere to the improvements proposed in chapter 2, 2) a set of recommendations for future developers, and 3) the results of the testing. On the other hand, the core of the work is solid.
The language of the work is acceptable, although there are quite a few missing articles. Also, a thesis should not turn to the reader ("you").
As for typography, the hard page-break at page 4 was a nasty shock.
Two of the citations (1, 3) lack any details except for the list of the authors and the work's name.

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 developed library, pyotr, does what it is supposed to do, and does it correctly. Python was definitely a good choice here. However, I would expect a discussion of the proper destruction of sensitive data - this is not handled in either the text or the library at all. If the student believes this does not need to be done (and there admittedly are objective grounds for that belief!), that reasoning should be provided to the reader.

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 believe the produced library could well be deployed in practice, despite new well-secured protocols such as Signal being available - OTR provides malleability which can significantly help in plausible deniability for the parties of the conversation. The biggest obstacle to an immediate applicability is the sketchy Ciphersuite Agreement mechanism which needs a serious discussion regarding its security (e.g. assuming an attacker who intentionally modifies the ciphersuite by giving huge positive values to ciphersuites she can break and huge negative values to those she can't).

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:

The student's activity was rather unbalanced - exceptional during the Project part, average during the Thesis part. He was highly self-reliant throughout and from the discussions I had with him, I am confident he is on the right track when it comes to security in his further studies or work.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
6. The overall evaluation	*85 (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:

The presented thesis proposes important security improvements to a actively-used cryptographic protocol with significant real-world implications. The implementation of these improvements solves the observed weak points in the current version of the protocol and provides plenty of room for future evolution. The written part of the thesis is, unfortunately, too short to cover all the aspects it should cover. For that reason I recommend that the thesis be graded as very good - B.

Signature of the supervisor: