FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Review report of a final thesis

Student:	Bc. Jan Rubín
Reviewer:	Ing. Tomáš Zahradnický, Ph.D.
Thesis title:	Security Analysis of the Signal Protocol
Branch of the study:	Computer Security

Date: 2. 6. 2018

Evaluation criterion:	*The evaluation scale: 1 to 5.*
1. Difficulty and other comments on the assignment	*1 = extremely challenging assignment,* ***2 = rather difficult assignment,*** *3 = assignment of average difficulty,* *4 = easier, but still sufficient assignment,* *5 = insufficient assignment*

Criteria description:
Characterize this final thesis in detail and its relationships to previous or current projects. Comment what is difficult about this thesis (in case of a more difficult thesis, you may overlook some shortcomings that you would not in case of an easy assignment, and on the contrary, with an easy assignment those shortcomings should be evaluated more strictly.)

Comments:
I find the topic a rather difficult topic, as the student had to study a lot of materials and algorithms.

Evaluation criterion:	*The evaluation scale: 1 to 4.*
2. 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 thesis meets the assignment statement. In Comments indicate parts of the assignment that have not been fulfilled, completely or partially, or extensions of the thesis beyond the original assignment. If the assignment was not completely fulfilled, try to assess the importance, impact, and possibly also the reason of the insufficiencies.

Comments:
I consider the assignment fulfilled.

Evaluation criterion:	*The evaluation scale: 1 to 4.*
3. Size of the main written part	***1 = meets the criteria,*** *2 = meets the criteria with minor objections,* *3 = meets the criteria with major objections,* *4 = does not meet the criteria*

Criteria description:
Evaluate the adequacy of the extent of the final thesis, considering its content and the size of the written part, i.e. that all parts of the thesis are rich on information and the text does not contain unnecessary parts.

Comments:
Size of the thesis meets criteria for a diploma thesis.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
4. Factual and logical level of the thesis	*85 (B)*

Criteria description:
Assess whether the thesis is correct as to the facts or if there are factual errors and inaccuracies. Evaluate further the logical structure of the thesis, links among the chapters, and the comprehensibility of the text for a reader.

Comments:
In chapter 1 the student discusses IM protocols. He mentions IRC, OTR, Jabber, and MTProto, among others. Are these really the ones most widely used? In my opinion the student had to go from an application toward a protocol. On page 10, he mentions some applications but I find the list lacks widely used messaging platforms such as Slack or Apple iMessage.

Chapter 2, analysis, is missing a conclusion.

The student chose to analyse a java implementation of the Signal protocol. I am missing a discussion about key deletion. Though section 3.7 and its subsections touch this topic, I find it rather shallow. How do get keys really deleted when they are no longer necessary? Is deletion left on the garbage collector making the application vulnerable to memory grabbing attacks?

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
5. Formal level of the thesis	*85 (B)*

Criteria description:
Assess the correctness of formalisms used in the thesis, the typographical and linguistic aspect s, see Dean's Directive No. 26/2017, Article 3.

Comments:
Mathematical notation could be better. For instance, multiplicative inverse mod p is not very accurately described (section 2.2.1, page 14). Some equations are also missing (mod p) to express that the calculation occurs over a finite field.

The thesis could more often cite the source. For instance, chapter 1 cites only AOL Instant Messenger but the remaining protocols and applications are not cited until later in the thesis.

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

Criteria description:
Evaluate the student's activity in acquisition and use of studying materials in his thesis. Characterize the choice of the sources. Discuss whether the student used all relevant sources, or whether he tried to solve problems that were already solved. Verify that all elements taken from other sources are properly differentiated from his own results and contributions. Comment if there was a possible violation of the citation ethics and if the bibliographical references are complete and in compliance with citation standards.

Comments:
I find the amount of citations appropriate for a diploma thesis.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
7. Evaluation of results, publication outputs and awards	*95 (A)*

Criteria description:
Comment on the achieved level of major results of the thesis and indicate whether the main results of the thesis extend published state-of-the-art results and/or bring completely new findings. Assess the quality and functionality of hardware or software solutions. Alternatively, evaluate whether the software or source code that was not created by the student himself was used in accordance with the license terms and copyright. Comment on possible publication output or awards related to the thesis.

Comments:
The student described the protocol and analysed its java implementation. Though deletion of keys was not analysed thoroughly, the student was able to discover a minor problem within the application.

Evaluation criterion:	*No evaluation scale.*
8. Applicability of the results	

Criteria description:
Indicate the potential of using the results of the thesis in practice.

Comments:
The thesis presents an additional independent review of the Signal protocol confirming there are no problems in the protocol. Though the word "additional" might have a negative connotation with superfluousness, the more reviews there are, the less is the probability the application or the protocol contained a hidden functionality or a backdoor.

Evaluation criterion:	*No evaluation scale.*
9. Questions for the defence	

Criteria description:
Formulate any question(s) that the student should answer to the committee during the defence (use a bullet list).

Questions:
1. Which protocol is used by the Slack and Apple iMessage messaging?

2. How do really get keys deleted when they are no longer needed (elaborate section 3.7)?

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
10. The overall evaluation	*90 (A)*

Criteria description:
Summarize the parts of the thesis that had major impact on your evaluation. The overall evaluation **does not** have to be the arithmetic mean or any other formula with the values from the previous evaluation criteria 1 to 9.

Comments:
I do recommend the diploma thesis of Mr. Jan Rubin for defence and grade it with A (excellent).

Signature of the reviewer: