FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Supervisor's statement of a final thesis

Student: Bc. Jan Rubín
Supervisor: Ing. Josef Kokeš
Thesis title: Security Analysis of the Signal Protocol
Branch of the study: Computer Security

Date: 13. 5. 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:
The thesis discusses the security aspects of the Signal protocol. That's generally quite a challenging task as cryptographic protocols tend to be complicated and at the same time a seemingly tiny error can have vast consequences to the confidentiality or integrity of the payload. On the other hand, the protocol itself is well documented and the applications built around it are open-source. For these reasons I rate the difficulty as above average rather than extreme.

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:
The assignment has been fulfilled. It may appear that a more detailed study of the Signal application should be provided, but due to the complexity of the matter that can not be reasonably expected.

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:
The length of the thesis is adequate. The text itself is very information-rich and yet easy to understand.

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

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:
I am very happy about the factual level of the thesis. As far as I can tell, it is perfect. The work is also logically structured and easy to follow, which is quite an achievement considering the level of complexity of the topic matter.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
5. Formal level of the thesis	*95 (A)*

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:
I did find some minor issues in the work's grammar (a few missing articles, a neither in a negative sentence etc.), but these are rare and far between. Overall, the formal level of the thesis is excellent.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
6. Bibliography	*95 (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:
The bibliography used in the thesis is excellent. The student had to study a wide selection of complex papers and he completed that task exceptionally well.

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 analyzed a complex protocol and an application using it in detail and performed a security analysis he can be proud of. That he did not find a serious security issue is no fault of his, and in the end is not a bad thing at all - it shows that both the protocol and the application are well designed and secure.

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 serves as an independent security review of a widely used protocol. The fact that no serious issues were found helps the users of the applications built upon that protocol, e.g. WhatsApp, to increase their confidence in the security of their messaging.

Evaluation criterion:	*The evaluation scale: 1 to 5.*
9. Activity and self-reliance of the student	*9a:* ***1 = excellent activity,*** *2 = very good activity,* *3 = average activity,* *4 = weaker, but still sufficient activity,* *5 = insufficient activity* *9b:* ***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:
Review student's activity while working on this final thesis, student's punctuality when meeting the deadlines and consulting continuously and also, student's preparedness for these consultations. Furthermore, review student's independency.

Comments:
This was probably the best co-operation on a thesis that I ever had.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
10. The overall evaluation	*98 (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:
The student handled a complex assignment exceptionally well. He performed an excellent security analysis of a widely used protocol and concluded that the protocol is very well designed. A few minor issues were found, mostly in the documentation department, not in the security of the messaging itself. That helps users built confidence about the protocol and the applications using it. Overall, I am very happy with the result. I recommend the thesis for a defense and suggest it be graded as excellent. A recommendation for the Dean's Reward should be considered.

Signature of the supervisor: