Supervisor's statement of a final thesis

Czech Technical University in Prague **Faculty of Information Technology**

Student:	Bc. Tomáš Sušánka
Supervisor:	Ing. Josef Kokeš
Thesis title:	Security Analysis of the Telegram IM
Branch of the study:	Computer Security

Date: 9. 1. 2017

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:
While the fact that Telegram is open-source seems to make the assignment of average difficulty, it should be noted that the student was required to perform a security evaluation of the code, and that is always a complex and difficult task as it's not enough to understand the code, but to understand space- and time-separated interrelations of various parts of the code. The fact that the mobile-phone version of the application was analyzed made things yet more complicated for the student and the work borders on the "exceptionally difficult" rating of the scale.

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 was successfully completed, as demonstrated by the fact an actual security issue eligible for bug bounty was found.

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 text of the diploma thesis falls slightly below the recommended minimum, but there are is no filler to be found in it and no significant missing content either. Also, the majority of the student's work is necessarily hidden "below the surface", in his study of the principles and particulars of Telegram and the specifics of tools needed to complete the task.

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 can't find any fault in the factual part of the thesis. The student completed his assigned tasks exceptionally well, performed the required analysis and found a security issue which was acknowledged by the developers of Telegram.

The logical structure of the work is exceptional, very easy to follow and certainly a great basis for future works.

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. 12/2014, Article 3.

Comments:

The thesis is written in English, and even though there is a not insignificant number of errors (esp. missing articles, some misspellings), the overall quality is very high. The text is very easy to follow and feels almost as if it were written by a native speaker.

I can't fault the typography, the images, the formal expressions at all.

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:

The bibliography is exceptional - numerous and at the same time highly relevant. The citations are used appropriately.

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 results are also quite exceptional. The student performed the required analysis and discovered several new and relevant issues in the Telegram's communication protocol - some of which were acknowledged by the developers, some of which weren't (in my opinion, the developers took a somewhat blase attitude to the complaints about the undocumented obfuscation and the implications of it). It may not be possible to break Telegram's encryption, as yet anyway, but the student made some quite interesting inroads into the application and I feel a major work on the part of developers is in order to dismiss the doubts cast on 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:

No major break was found in the application, but that was to be expected. I value the description of so-far-undocumented obfuscation scheme quite highly, and think that the users got a major food for thought from that - is the supposedly better performance really worth the potential privacy violations and censorship opportunities? The proposed replay attack scenario was acknowledged by the developers and should be fixed shortly.

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:

The student was extremely active and worked out most of his results on his own, with only a minor guidance on my part.

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

10. The overall evaluation

97 (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 the assigned task exceptionally well. He performed an excellent security analysis of a commonly used software and discovered several potential issues in its currently available version, some of which are being fixed by the developers at the moment. That will benefit the users. The fact that the thesis is written in a very good English, which makes it accessible to people worldwide, doesn't hurt at all, either.

Signature of the supervisor: