FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Supervisor's statement of a final thesis

Student:	Tomáš Stefan
Supervisor:	Ing. Josef Kokeš
Thesis title:	Digital Signature Verification in PDF
Branch of the study:	Computer Security and Information technology

Date: 21. 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 result of the thesis was to be a library for verification of digital signatures in PDF documents. That is itself is well documented and should not present too much of a challenge, but one must not forget that we are dealing with cryptography here and even minor misunderstandings or deviations can have disastrous consequences. Furthermore, writing a library is significantly more difficult than writing an application, because a library should be easy to use while allowing enough variability to suit all possible situations. Both aspects increase the difficulty to an above-average level.

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 fulfilled to my satisfactions. It was expected that signature verification in its entirety is beyond the scope of a thesis.

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 and information content of the text meet the standard requirements.

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

4. Factual and logical level of the thesis

95 (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:
The work's content is of a very high quality. The descriptions are deep enough to be accurate and convey the necessary information without confusing the reader.

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

5. Formal level of the thesis

90 (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:
Formal notations adhere to the standard requirements. There are also very few grammatical or other errors in the text. I do have two minor complaints, though: The comments in the printed listings are too light to be easily readable, and in places the language used leans towards storytelling rather than to a scientific text.

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

6. Bibliography *90 (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 work refers to an above average number of sources in the proper manner. While about a half of the references simply link to the descriptions of available applications dealing with PDFs and signatures within, the remaining sources are still rich enough and very relevant.

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

7. Evaluation of results, publication outputs and awards *96 (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 main output of the thesis is the libpdfsigil library, which provides exactly what we set to achieve: an easy to use PDF-signature handling library written in pure C, with few external dependencies. The fact that some aspects of PDF signing were left out due to the time constraints was not unexpected and does not diminish the value of the work. Both PKCS7 and certificate revocations can be easily added later thanks to the simple structure of the library. Even in its current state the library provides functions which were sorely missing on Linux operating systems.

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 library provides a functionality which has been in low supply in the Linux world until now - a simple PDF-signature verification without prohibitive external dependencies (e.g. Java). That in itself is a worthwhile contribution.

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 very active in the early phases of writing the thesis. Later on his activity somewhat decreased, due in part to the implementation challenges. Still, the overall activity was sufficient, and I appreciate that the student was able to solve the encountered issues on his own.

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

10. The overall evaluation *95 (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:
Overall, this is an excellent work. The text is deep but easy to understand, and the developed library is an excellent contribution as it provides a functionality which has heretofore been missing. It should also be easy enough to maintain and enhance, even for a third party. I believe this thesis to be a prime example of what we expect from a bachelor's thesis.

Signature of the supervisor: