Review report of a final thesis

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

Student:	Bc. Tomáš Kvasnička
Reviewer:	Ing. Josef Kokeš
Thesis title:	Application Security Analysis
Branch of the study:	Computer Security

Date: 20. 1. 2018

Evaluation criterion:

1. Difficulty and other comments on the assignment

The evaluation scale: 1 to 5.

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 difficulty of the topic is average, bordering on above-average.

Evaluation criterion:

2. Fulfilment of the assignment

The evaluation scale: 1 to 4.

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.

Evaluation criterion:

3. Size of the main written part

The evaluation scale: 1 to 4.

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:

Even considering that some parts of the text are repeated multiple times and that section 2.3 should either be expanded or moved to the appendices, the size of the actual relevant text meets the criteria.

Evaluation criterion:

4. Factual and logical level of the thesis

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

75 (C)

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 thesis is, for the most part, factually correct. There are, however, three aspects which I find problematic:

1) No formal vulnerability assessment methodology (e.g. CVSS, CWSS) was used for the vulnerabilities discovered. As a result, the discussion of the seriousness of the vulnerabilities is highly subjective.

2) Also as a result of #1, the recommendations of the student are suspect. While I would agree with the switch to HTTPS, I do not believe the checksum publication would help significantly and I disagree with the recommendations for the buffer overflow vulnerability.

3) The author claims to have studied all of the executable components of the application. That is not true: Beside the 4 EXEs and 4 DLLs, two other executable components exist which haven't been studied (or even noticed!!!) at all. These two components do not carry authenticode and as a result can be modified or replaced by the attacker rather easily. Furthermore, it should be noted that in a previous version of the application, a remote code execution vulnerability existed in these components.

There are also some minor mistakes in the text, e.g. the application's "JS engine" (page 35) apparently does not even exist since the web content display is done by the Internet Explorer core components.

The structure of the thesis needs some reordering. As it is now, it leads to a significant duplication of explanations while at the same time spreading related information all over the text. Particularly the separation of chapters 3 and 4 seems to be adverse to the work's logical flow.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
5. Formal level of the thesis	*60 (D)*

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:
The thesis is written in English, which is great for the work's accessibility to readers. Unfortunately, the language is not used correctly - I note *many* grammatical errors (missing articles, incorrect prepositions, unsuitable pronouns) and the structure of the sentences is that of the Czech language, not English. Quite often a term is used which is incorrect in English but which translates to a correct Czech counterpart. As a result, knowledge of both Czech and English is necessary to fully understand the text, which detracts from the accessibility mentioned earlier.

The keywords in the abstract need reworking, they are useless now.

Typographical errors appear throughout the text, the use of a minus in place of a dash being the most prominent. We can also encounter quite a few ampersands where an "and" would be more appropriate.

The list of acronyms (3 pages long) is unsorted.

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 bibliography is sizeable, current, and relevant, except for items 3, 4 and particularly 1. Its use is not perfect in all cases, though - many references should appear in a footnote as a "for more information regarding this topic, read X" note rather than as straight citations supporting the author's claim. The ordering of the citations is unclear - it seems to follow the order in which the references appear in the text, but it's not always the case.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
7. Evaluation of results, publication outputs and awards	*85 (B)*

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 presented in this thesis are new and useful. The errors mentioned above detract from them somewhat, but the results are still respectable. The recommendations provided are not sufficiently supported by objective data, though.

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 applicability of the results is good. While the decision on the part of the author to hide the name of the studied application would seem to detract from the applicability of the results, the findings were communicated to the developer, so the users should get a better product even if they don't know its name. On the other hand, it should be noted that 1) I was able to discern the application concerned within minutes of starting to read chapter 3, 2) the seriousness of the discovered vulnerabilities seems to be rather low, and 3) at least some of the vulnerabilities have been fixed 4 months before the thesis was submitted. With that in mind, the decision to hide the name of the application seems to be rather pointless.

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:

- Can you provide an objective vulnerability assessment of the vulnerabilities you found according to a common methodology?

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

10. The overall evaluation

80 (B)

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 successfully demonstrated his ability to perform a master-level work. He successfully performed a security study of a major closed-source application, and done that above the level required by the assignment. His findings have been reported to the developer and the users will benefit as a result. Unfortunately, the mistakes mentioned in #4 and particularly the poor language level mentioned in #5 prevent me from recommending the top grade.

Signature of the reviewer: