FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Supervisor's statement of a final thesis

Student: Petr Heřmánek
Supervisor: Ing. Josef Kokeš
Thesis title: The Stack Clash Attack
Branch of the study: Information Technology

Date: 16. 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 and demonstrates the issues inherent in the recently published Stack Clash attack. Unfortunately, the original paper does not provide sufficient information to replicate the attack. The student had to research the internals of the memory management mechanisms on Linux and perform extensive experiments in order to succeed in the attack's execution. For this reason I rate the assignment as rather difficult.

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 student was able to execute the attack, demonstrating the fulfillment of the assignment.

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 is adequate.

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 factual level of the work is excellent. As for the logical structure, the work is well organized and generally easy to follow, although a more detailed discussion of some key issues (e.g. skipping over the guard page) may have been helpful for an average reader.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
5. Formal level of the thesis	*89 (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:
The formal level of the work is very good, bordering on excellent. My only complaint is that quite a few articles are still missing, and incorrect single-quotes are used in several places in the text.

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 sources are rich and cited properly. However, some internet-based articles lack the "date accessed" information.

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 successfully replicated the attack, using his own code and environment. He prepared a virtual image for demonstrations of the attack. While the code does not represent an actual exploit (the attacker needs a lot of "magic" information about the system), it is one of the first, if not the first, published proof-of-concept code.

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 virtual image has already been successfully used in the Secure Code class to explain the issues of the Stack Clash.

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:
I was very satisfied with the co-operation inherent in composing this thesis.

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:
The student successfully researched a difficult topic and created a proof-of-concept code to demonstrate it. Although all necessary information has been published previously, none of it was complete enough to allow for an easy, straightforward re-use; rather, the student had to piece it together from multiple unrelated sources and perform significant experiments to gain the missing links. It is easy enough to imagine this work succeeding even as a Master's Thesis.

Signature of the supervisor: