FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Supervisor's statement of a final thesis

Student: Bc. Robert Husák
Supervisor: doc. Dipl.-Ing. Dr. techn. Stefan Ratschan
Thesis title: Handling heap data structures in backward symbolic execution
Branch of the study: Web and Software Engineering

Date: 23. 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:
For this thesis topic it is necessary to both master abstract formal machinery, and to translate this abstract machinery into an actual software implementation.

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 result fulfills 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 thesis fulfills the page requirements. The meat of the thesis are formalisms for symbolic modeling of heap data structures. The few pages describing these formalisms have more actual content than the content that one can find in an average full diploma thesis.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
4. Factual and logical level of the thesis	*90 (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 did not find any mistakes in the thesis, and it is well structured. More examples would have been useful, especially an example explaining backward symbolic execution and the corresponding heap model from Section 7.2.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
5. Formal level of the thesis	*98 (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:
The students fully masters the formal toolbox of computer science. Also, as far as I can judge, compared to the average Czech computer science student, his command of the English language is outstanding. The student deserves special praise for his mastery of the English articles. Up to now, I have only seen a handful texts written by Czech speakers that use them correctly. This is one of them.

A small recommendation: For better readability, try to make a difference between equality in the object and meta language. A common approach is to use the equality symbol = within first-order formulas (i.e., the object language), and the LaTeX symbol \equiv in running text (i.e., the meta language).

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 thesis works with the literature in a better way than some scientific articles. The chapter on related work might have profited from a little bit broader discussion, also taking into account work on formal modeling of the heap and data structures independent of symbolic execution. But this is really only minor criticism.

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 main results of the thesis are:
- a presentation of three symbolic heap representation methods under a unifying formal umbrella
- a modification of one of the three methods for backward symbolic execution
- an implementation of the result in an actual software tool

All three results represent a highly non-trivial effort, by far going beyond the achievements one finds in usual diploma thesis.

Personally, I would have found a slightly different approach that first maps heap data structures into a logical theory (see e.g., the chapter on pointer logic in the book on decision procedures by Kroening and Strichman), and then decides the logical theory, more elegant: Such an approach would keep a larger part of the formalization independent from symbolic execution and the direction of execution. However, this is far from my area of expertise and I might have overlooked some disadvantages of such an approach.

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:
Up to my knowledge, all three results described above extend the scientific state of the art. Symbolic execution is a technique of high practical relevance. For example, Microsoft claims to have saved millions of dollars based on symbolic execution:

Patrice Godefroid, Michael Y. Levin, and David Molnar. SAGE: whitebox fuzzing for security testing. Commun. ACM, 55(3):40–44, March 2012. doi: 10.1145/2093548.2093564.

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 came up with the thesis topic by himself and worked out the solution completely independently. He did most of the work under time-pressure with minimal consultation. With less time pressure the final result probably would have been even better.

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:
An outstanding thesis.

Apparently the student is already continuing with Ph.D. studies. For his further scientific growth I recommend to broaden the scope of research, to view tool development less as a goal in itself, and more as a means to come up with general scientific results.

Signature of the supervisor: