FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Supervisor's statement of a final thesis

Supervisor:	Ing. Josef Kokeš
Student:	Petr Adámek
Thesis title:	Security of the Lua Sandbox
Branch / specialization:	Computer Security and Information technology
Created on:	19 May 2022

Evaluation criteria

1. Fulfillment of the assignment

- ▸ [1] **assignment fulfilled**
  [2] assignment fulfilled with minor objections
  [3] assignment fulfilled with major objections
  [4] assignment not fulfilled

2. Main written part

85 /100 (B)

The written part of the thesis presents a very detailed and in-depth study of the issues of implementing a sandbox for Lua scripts. Certainly, the student performed a thorough analysis of the language and its implementations as well as a review of past vulnerabilities in this area.

Unfortunately, it is somewhat hard on the reader, expecting a fairly deep knowledge of the language as a prerequisite. This is particularly obvious in sections 3.2-3.4 where the reader is assumed to already be familiar with the known bugs before they started to read, so that only the parts relevant to the sandbox issues need to be discussed. I don't think these expectations are necessarily justified and feel that with a brief explanation of the language itself or with an addition of small code examples to the discussed topics, the thesis could become accessible to many more readers.

The typography and language of the thesis present are very good. I did notice a few minor errors, but nothing that would cause the reader any more trouble than the above-mentioned expectations.

3. Non-written part, attachments

95 /100 (A)

The non-written part consists of a Lua environment analyzer and a demonstration of sandbox violation in OpenMW. While the demonstration was one of the major tasks of the assignment, and it certainly delivers what was asked, I am actually more impressed with

the analyzer as it can be much more widely used. I did successfully use it in FAR Manager to explore its environment, for example.

4. Evaluation of results, publication outputs and awards 85 /100 (B)

The Lua environment analyzer can be used straight "out of the box" to evaluate the potential attack surfaces of any application that provides Lua scripting.

The analysis performed while researching and writing the thesis also resulted in a number of reports to the related projects (e.g. OpenMW) that were incorporated to improve the security of these projects.

I am not certain about the direct usability of the thesis text itself, though, as its high prerequisites tend to make it less accessible to a casual reader. A chapter on "Lua best sandboxing practices" would be a welcome addition here, although I appreciate the thesis is already long enough.

5. Activity of the student

[1] excellent activity
▸ **[2] very good activity**
[3] average activity
[4] weaker, but still sufficient activity
[5] insufficient activity

6. Self-reliance of the student

▸ **[1] excellent self-reliance**
[2] very good self-reliance
[3] average self-reliance
[4] weaker, but still sufficient self-reliance
[5] insufficient self-reliance

The overall evaluation 90 /100 (A)

Overall, I consider this thesis of a very high quality as far as the actual content is concerned, albeit somewhat hampered by its high (and in my case, unwarranted) expectations on the reader's knowledge. A little more reader-friendly approach would be beneficial here. Still, that is mostly the fault of the reader, not the author. I recommend the thesis for defense and grade it A=excellent.

Instructions

Fulfillment of the assignment

Assess whether the submitted FT defines the objectives sufficiently and in line with the assignment; whether the objectives are formulated correctly and fulfilled sufficiently. In the comment, specify the points of the assignment that have not been met, assess the severity, impact, and, if appropriate, also the cause of the deficiencies. If the assignment differs substantially from the standards for the FT or if the student has developed the FT beyond the assignment, describe the way it got reflected on the quality of the assignment's fulfilment and the way it affected your final evaluation.

Main written part

Evaluate whether the extent of the FT is adequate to its content and scope: are all the parts of the FT contentful and necessary? Next, consider whether the submitted FT is actually correct – are there factual errors or inaccuracies?

Evaluate the logical structure of the FT, the thematic flow between chapters and whether the text is comprehensible to the reader. Assess whether the formal notations in the FT are used correctly. Assess the typographic and language aspects of the FT, follow the Dean's Directive No. 52/2021, Art. 3.

Evaluate whether the relevant sources are properly used, quoted and cited. Verify that all quotes are properly distinguished from the results achieved in the FT, thus, that the citation ethics has not been violated and that the citations are complete and in accordance with citation practices and standards. Finally, evaluate whether the software and other copyrighted works have been used in accordance with their license terms.

Non-written part, attachments

Depending on the nature of the FT, comment on the non-written part of the thesis. For example: SW work – the overall quality of the program. Is the technology used (from the development to deployment) suitable and adequate? HW – functional sample. Evaluate the technology and tools used. Research and experimental work – repeatability of the experiment.

Evaluation of results, publication outputs and awards

Depending on the nature of the thesis, estimate whether the thesis results could be deployed in practice; alternatively, evaluate whether the results of the FT extend the already published/known results or whether they bring in completely new findings.

Activity of the student

From your experience with the course of the work on the thesis and its outcome, review the student's activity while working on the thesis, his/her punctuality when meeting the deadlines and whether he/she consulted you as he/she went along and also, whether he/she was well prepared for these consultations.

Self-reliance of the student

From your experience with the course of the work on the thesis and its outcome, assess the student's ability to develop independent creative work.

The overall evaluation

Summarize which of the aspects of the FT affected your grading process the most. The overall grade does not need to be an arithmetic mean (or other value) calculated from the evaluation in the previous criteria. Generally, a well-fulfilled assignment is assessed by grade A.