FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Supervisor's statement of a final thesis

Supervisor:	Ing. Josef Kokeš, Ph.D.
Student:	Bc. Michal Žůrek
Thesis title:	Memory Explorer for .NET
Branch / specialization:	Computer Security
Created on:	27 May 2023

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

The assignment was completed, but there is a significant variance in the quality of the components of the thesis. Clearly, the student found the implementation much more interesting than the text, which caused him to allocate most of his time to the former at the cost to the latter.

2. Main written part 60/100 (D)

The written part of the thesis covers most of the aspects that one would expect from a work of this type, but the quality is not too high. Apparently not enough resources were dedicated to it and as a result, it was created in a hurry without sufficient time for even basic proofreading. Chapters directly related to the .NET Memory Explorer application (3 and 5) are generally well described and contain most of the necessary information but the other chapters suffer from a rather disorganized approach and sometimes feel almost as filler text (e.g. chapter 4 makes little sense where it is, but becomes more relevant once the reader finishes with chapter 6). Reordering some sections and applying a more hierarchical structure would help the reader a lot, I think.
Uniformly, the text suffers from many mistypes, missing words, misspelled words, etc. Articles and prepositions are incorrectly used and often the meaning needs to be deduced by performing a literal translation of the term concerned to Czech (e.g. the very frequent "in opposition" phrase). Additionally, some incorrect references can be found, especially in chapter 4.
The bibliography is relevant for the most part and covers the subject area well, but could be improved. In particular, we often see the name of the project in place of author names. [34] is apparently a modified copy&paste of [33], although it should relate to [30].

3. Non-written part, attachments

95/100 (A)

The non-written part is represented by an application that can explore the memory space of a .NET process, built along the principles explained in the text, and a suite of test applications. These clearly demonstrate that the student's approach at extracting the memory works. The UI might not be pretty, but it gets the job done, and most importantly, it supports all the most important functionalities - listing allocated memory blocks of an application, searching for objects by data, following cross-references to find the objects from which the data is referenced, allowing modifications of the contents of the objects. That's exactly what's needed if one needs to explore a .NET application at runtime. There are some obvious limitations, but these are clearly explained in the text and quite understandable.

4. Evaluation of results, publication outputs and awards

95/100 (A)

The main result is a completely new algorithm as well as its practical implementation that allow an analyst to explore the memory space of a running .NET application. I believe represents a very useful addition to the arsenal of a reverse engineer which complements the existing tools such as DnSpy nicely - once can, for example, locate an interesting value in memory and then by following cross-references find the object(s) responsible for managing that value, which can then be explored and/or debugged, combining the strengths of the respective tools.

5. Activity of the student

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

I am afraid the student's activity was all "behind the scenes". Basically, we had some contact regarding the topic at the beginning of the Project, then some more when the Assignment was to be created, and then just before the submission deadline. I understand that some people work better on their own, but one of the reasons for having a supervisor is to help directing the efforts towards completing the thesis. The disadvantages of the lack of contact are made painfully obvious in the written part.

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

Certainly, the student can work on his own. The end result might have been better if he didn't.

The overall evaluation 90 /100 (A)

While the text itself is very much in need of revising and rearranging, the practical aspects of the thesis are great. The student came up with a new method for exploring .NET applications and by implementing it demonstrated that it works really well. While the tool may not be fully polished just yet, it already contains the most important functionalities and I am quite confident it will eventually become one of the main tools in a reverse engineer's arsenal, along the likes of DnSpy. That alone is sufficient to offset any deficiencies in the text. 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.