FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Supervisor's statement of a final thesis

Supervisor: Ing. Josef Kokeš, Ph.D.
Student: Bc. Viktor Dohnal
Thesis title: Protecting Sensitive Data in Memory in .NET
Branch / specialization: Computer Security
Created on: 13 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 is fairly complex, since the analysis necessarily depends on reverse engineering and covers multiple platforms. The student dealt with it well.

2. Main written part 90/100 (A)

As far as the factual content of the thesis, I have no complaints. The student described the state of the art, collated the known information and analyzed the unknown (or undocumented), and used his findings to assess the security of a real world application. The text is easy to read and the conclusions are well founded and clear. I would appreciate a less frequent use of commas, though.
I have some complaints regarding the formal aspects of the text. The introductory text is missing in chapter 1, there are ghost sections in chapters 2 and 3 (e.g section 3.0.0.1), incorrect characters are used throughout (e.g - in place of ---, "..." in place of ` ` ...''), some lines overflow into the margin.
The bibliography is inconsistent when dealing with company-produced materials For example, Microsoft's materials are attributed to author "Microsoft" (OK), but Intel's, Apple's, Elcomsoft's and others' are left authorless, even though some of them contain a clearly identifiable author (e.g. [19]).

3. Non-written part, attachments 90/100 (A)

The non-written part consists mostly of proof-of-concepts and demonstration codes, which is what the assignment asked for. The codes are easy to read and clearly demonstrate what they were supposed to demonstrate. My only issue is that some of the code that might be accepted by readers as a tutorial on "how to do it right", and even described that way in the text, are not entirely correct. For example, SimpleCrypt__WPF::FileCrypto::Encrypt purports to demonstrate the use of pinning byte arrays and clearing them before releasing, but due to the rather shoddy try-finally use it might lead to exposure of sensitive data - if the constructor for ciphertextGCHandle fails, key and plaintext fail to get overwritten. While it is very unlikely to happen in practice, it does deduct from the use-as-an-example value of the code somewhat.

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

I find the results extremely interesting and very useful. The reader will get a clear understanding of the issues inherent in handling sensitive data in .NET and will also receive information on how to do it right. A lot of the information provided is essentially new, in the sense that it hasn't been publicly documented and available in a compact form. The vulnerability discovered in KeePass is completely new and I think it's far more serious that the thesis takes a credit for - the vulnerability is such that it will manifest in a common use scenario and will reveal the master password even in cases where the user has been led to believe that the data is secure. For these reasons I consider it a major contribution to the application's security.

5. Activity of the student

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

The student's activity leaves a lot to be desired. For the most part, it occurred at irregular intervals with a lot of silence in between. The reasons have been communicated to me by the student and while I understand them, I must mention the fact.

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 95/100 (A)

Due to the problematic activity, I must admit to some worry about the student's ability to complete the thesis, but he did and the result exceeded expectations. I find the thesis well researched and executed and very interesting. The text is easy to read and full of new details on the subject area and the sample applications are very convincing. The work even led to a discovery of a major vulnerability in a widely-used application. I recommend the thesis for defense and grade 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.