FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Review report of a final thesis

Student:	Martin Kolárik
Reviewer:	Ing. Josef Kokeš
Thesis title:	FIDO2 KeePass Plugin
Branch of the study:	Web and Software Engineering

Date: 6. 6. 2020

Evaluation criterion: *The evaluation scale: 1 to 4.*

1. 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 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.

Comments:

The assignment has been fulfilled. The student managed to overcome unforeseen setbacks and implemented a plugin which would allow decryption of the KeePass database using a FIDO2-compatible authenticator. It should be noted, though, that the developed plugin is not of a production-quality - partially due to minor issues in the application and partially due to the FIDO2 standard not being entirely suitable for the task.

Evaluation criterion: *The evaluation scale: 0 to 100 points (grade A to F).*

2. Main written part

85 (B)

Criteria description:
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. 26/2017, 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.

Comments:

The text explores the necessary prerequisites to completing the task at hand. The first chapter is clear and well presented, as is the majority of the second one. I think, however, that section 2.2 should be explored in more detail. In section 2.2.1, it's not obvious whether the limitations described are universal or specific to Yubikeys. Section 2.2.3 should explain the issues inherent in the proposed approach straight away, not leave them until the Implementation chapter. Section 2.2.4 should explore the actual meaning of the claim 1 at the end of page 25: as far as I can tell, it does NOT guarantee that the metadata is actually encrypted, only that it's not returned to the caller without proper user verification; that may mean the database's master key (a highly sensitive piece of information!) is stored in plaintext on the device and may be accessible through hardware manipulation. The user should be made aware of that! And the whole of section 2.2 should make it clear that this use of the FIDO2 device pretty much defeats the basic idea of tokens in general - that it should not be possible to access the protected data without having an access to the device.

The student used English for his thesis and used it well. My chief complaint is that the usage of commas tends to be directed by Czech custom rather than the English one. Still, the text is clear and easy enough to understand. It seems rather sparse, though - despite being 38 pages long (minus some empty pages), it feels much shorter and could use additional detail.

The text refers to Github for the plugin's source codes (e.g. on page vi), but the repository is not available at the time of writing this evaluation.

Evaluation criterion: *The evaluation scale: 0 to 100 points (grade A to F).*

3. Non-written part, attachments

85 (B)

Criteria description:
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.

Comments:

The implemented plugin solves the stated goals. In doing so, the student had to overcome several setbacks, e.g. the need to use a high-privileged component for the actual plugin-to-device communication. That was done according to the recommended practices, for the most part. A few security issues remain, though:

1) DeviceCommunicator violates the least-privilege principle by requiring PROCESS_ALL_ACCESS access to the process token. A much more limited token would be sufficient.
2) The student tried but failed to securely delete all sensitive data. In data[], a copy of the PIN remains, in icon[], a copy of the master key remains. Not even pin[] is guaranteed to be destroyed after use, the student should have used SecureZeroMemory instead of memset.
3) There are no checks whatsoever on the size and structure of the transferred memory block. As a result, the application is dependent on the goodwill of all involved to never modify the structure in any way. I would recommend that a structure version field and/or structure size field be included to facilitate future growth and to reduce dangers caused by mismatched versions of DeviceCommunicator and KeePassFIDO2.

Note that even though KeePass itself and libfido2 are compatible with multiple platforms, the choice of the communication channel pretty much enforces the use of Windows.

Evaluation criterion: *The evaluation scale: 0 to 100 points (grade A to F).*

4. Evaluation of results, publication outputs and awards

88 (B)

Criteria description:
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.

Comments:

The student managed to implement the FIDO2 support in the context of protecting the KeePass database, which is certainly a worthwhile thing. I am particularly glad the plugin is implemented in such a way that FIDO2 is an *alternative* to using the regular password rather than the *second factor* (which is the standard approach of KeePass) as it allows for easy backups. However, the code is not quite production-quality and it is unclear whether it can ever be - the issues listed in section #3 of this evaluation can be fixed, but the overall unsuitability of FIDO2 for the purpose intended by the plugin may well be impossible to overcome. The application is certainly usable even in its current form, but the user should be well aware of the outstanding issues. And the plugin should definitely be modified to allow one authenticator to be used with more than one database, this limitation is a serious detriment to the practical use of the plugin.

Evaluation criterion: *No evaluation scale.*

5. Questions for the defence

Criteria description:
Formulate questions that the student should answer during the Presentation and defence of the FT in front of the SFE Committee (use a bullet list).

Questions:

1) What needs to be done to allow one authenticator to decrypt multiple KeePass databases?
2) Which *minimal* privileges are *actually* necessary for the plugin to work? Do we really need the Administrator?
3) When it became apparent that FIDO2 is not a very suitable standard for this purpose, did you explore any alternatives? Which would be your preferred one?

Evaluation criterion: *The evaluation scale: 0 to 100 points (grade A to F).*

6. The overall evaluation

88 (B)

Criteria description:
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.

Comments:

In spite of my complaints in the previous sections, I actually quite like this thesis. No part of it is a clear A-grade material, but overall it is very well done. The student approached an interesting and important subject and manged to resolve the unforeseen complications more successfully than I would have expected. The plugin he created does work and provides a valuable alternative to the traditional password-based protection mechanism of the KeePass database. I recommend the thesis for the defense and grade it B-very good.

Signature of the reviewer: