FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Review report of a final thesis

Student:	Bc. Jan Michal
Reviewer:	Ing. Josef Kokeš
Thesis title:	Analýza bezpečnosti elektronických jednotek vozu Tesla Model 3
Branch of the study:	Computer Security

Date: 18. 1. 2021

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:

As I understand the assignment, the student completed approximately the first half of it - he performed a research into the security of the modern cars, described some theory behind penetration testing and created a threat model for connected vehicles. The actual security analysis was performed in an extremely rudimentary way, though, by running a small set of common penetration testing tools and partially interpreting their output. No analysis of the autopilot or the media unit was performed and no advanced approaches (such as using reverse engineering for anything else than a brief look at the filesystem) were taken.

It should be noted that the thesis is written in English, even though the assignment requests Czech to be used.

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

2. Main written part

50 (E)

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:

While the written part formally satisfies the requirements for length, it feels rather empty. Many of the necessary areas are actually covered, but generally not in sufficient detail and/or not in the proper place. For example, I feel that chapters 3.1 and 3.2 should actually be a part of chapter 2 and chapters 2.3 and 2.4 should either be greatly expanded or put into chapter 6 - or perhaps both. The research of the known cyber-attacks on vehicles is OK, if a bit shallow, but doesn't seem to affect the rest of the thesis at all. Threat modelling seems to be at the same time rather wide (briefly covering a number of methodologies, even those not actually used) and quite limited, which may have been a caused by a lack of clear focus of the work; I feel that both the assets and the threat agents could be greatly expanded and they should definitely be used in the execution of the vulnerability analysis - currently they are listed and then not used. The vulnerability analysis is the weakest part of the work - as far as I can tell, it consists of running several simple third-party pentesting tools and then partially interpreting their output; the tools often disclosed potential attack surfaces (such as an open SSH port) which were subsequently not explored at all. Reverse engineering, required by the assignment and supposedly used as per chapter 2.4, was not performed, except that the student did unpack the root filesystem of the upgrade package and gave it a cursory inspection. Some network traffic was captured and then discarded with a statement of "I did not find anything important so I moved to the next step", which seems rather premature given that the traffic seems to be unencrypted; why wasn't ARP poisoning tried to verify whether the car can detect e.g. packet replacement?

The thesis is written in English, but the language level is not very high. It suffers greatly from incorrectly structured sentences which follow the Czech composition rules rather than the English ones. I also encountered a number of problems with verb tenses and other grammatical errors. Despite that, the work's content was mostly clear to me, except in a few places where it was impossible to decide whether the missing verb was meant to be positive or negative. Also, a thesis should not tell the reader what to do or not do.

The technical aspects of the work are generally OK, except for the structuring of chapters - see e.g. chapter 5 which has four levels of subchapters, often without any connecting text between two levels; this is frequently repeated elsewhere in the work, too.

Overall, I think the written part barely meets the criteria for passing, and then only thanks to the threat modelling part. The actual security analysis is insufficient and its outputs, if at all present, unreliable.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
3. Non-written part, attachments	*10 (F)*

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:

There is hardly any non-written part to speak of, and none of it the student's own work. There are a few captured network packets without any interpretation and without even explaining what they show, a report from nmap, a report from Nikto and a report from OWAST ZAP. There is a severely limited discussion of these in chapter 5, but not enough to even repeat the measurements, not to mention verify them. No files related to reverse analysis were provided at all.

I find it very sad because the chapter 3.3 gave me the impression that the student was able to get at some of the internals of the car, which is something quite rare on FIT, and I expected he would make use of that opportunity. Unfortunately, that did not happen.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
4. Evaluation of results, publication outputs and awards	*25 (F)*

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 only usable output that I can see is the threat model of the car, and that with the caveat that it would need to be more focused and subjected to a more in-depth study to be really useful for some future work. I can't imagine what other possible use could the thesis in its current state have.

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:

No questions.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
6. The overall evaluation	*30 (F)*

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:
I am afraid that the thesis cannot be defended in its current form. Several major parts of the assignment, such as the analysis of the autopilot and of the media center, were completely skipped. What analysis was performed, was performed in an extremely basic way and with minimal input from the student. The results of the analysis are at best unreliable because there is no data to verify them and it is quite apparent that many aspects were not explored at all. It is true that the work requested by the assignment was very difficult - completing the assignment to the letter and in high quality would, in my opinion, be significantly beyond the scope of a master's thesis, but unfortunately the submitted work does not meet even the minimal criteria for passing. I would recommend that the assignment was modified to give the student a clear focus on some narrow security aspect of the car - if the car is still available for testing, that is, because the measurements and tests need to be performed again and in much more detail. Sadly, I cannot recommend this thesis for the defense and must grade it F-failed.

Signature of the reviewer: