FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Supervisor's statement of a final thesis

Supervisor:	Ing. Tomáš Pajurek
Student:	Bc. David Mládek
Thesis title:	Security and Performance of IoT Application Protocols
Branch / specialization:	Computer Security
Created on:	January 15, 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

Thesis covers all topics required by the assignment. Although it is very brief in some places, all essential information is presented and experiments are performed and evaluated.

Implementation of experiments was very challenging and required knowledge in many areas from flashing programs to ESP32 board, through writing programs in Rust, Go and C and working with associated build tool chains, up to configuring several message brokers, reasoning about application protocols and network traffic monitoring.

2. Main written part 72/100 (C)

Main written part is very brief, with an extent that is near the lower limit for a master thesis. However, all necessary parts with sufficient information depth are present.

Overall, the thesis is well organized into chapters and sections. Author clearly defines the intended scope and provides references for additional details where appropriate. However, individual sections could be organized in more friendly manner for the reader. There are long sections of text that lack structure. The readability of the thesis would greatly benefit from logically separating these sections by additional headers and emphasizing new and important terms.

The thesis is written in very good English. Citations are used correctly. There are only a few typos. Facts are property-cited and are clearly distinguished from the author's hypothesis and findings. Used sources are of high-quality, mainly RFCs and OASIS specifications which are expected for this kind of work. Formally, the thesis is all right.

Experiment design is sufficient but it could be improved and better organized. Information that could be surely provided to the reader in a concise manner at one place is scattered across many places. Reader must deduce that sending of messages during the experiments was done in parallel if possible and sequentially otherwise (due to platform/implementation limitations). On one side, it is very interesting to see the behavior of protocols with parallelism involved but on the other side, comparison of the protocols loses some of its value given that the messages were sent in parallel for some protocols and sequentially for the others.

During the implementation, there were some issues that prevented execution of all intended experiments. Although all these issues are described and valid, the reader might wonder why some of them were not resolved (e.g. inconsistencies in CoAP token size in various libraries could be resolved by configuring the libraries differently). The author should also take better care of making the impact of these issues explicit in the presented results (e.g. missing results for protocols with TLS for ESP32).

Some of the less important information is also missing from the experiment design, such as description of used HTTP server or size of keys used for TLS handshakes. Reader must find this information in the attached source code.

Results are presented properly in table format. Author includes all necessary information such as exact meaning of the presented numbers, number of measurements and standard deviations. However, the results could be also presented visually to improve readability.

3. Non-written part, attachments 79/100 (C)

Non-written part contains source codes for all the experiments, experiment results as well as TEX sources of the written part. However, there are a few missing parts. For example, run scripts/configuration of MQTT/AMQP brokers is missing. Also, the folder `src/code/rpi/http` is empty.

Overall, the non-written part contains only the essentials and does not allow for easy reproduction of experiments.

4. Evaluation of results, publication outputs and awards 80/100 (B)

Author did a lot of work preparing and running the experiments. Putting AMQP into work on ESP32 proved to be very challenging and although ultimately unsuccessful, the author proved strong dedication to solving the problem and ruled out many not viable options for the benefit of others.

In the course of writing the thesis, the author contributed to several open source projects by submitting issues as well as a pull request (https://github.com/quartiq/minimq/pull/68).

The thesis can surely be used as a source of unique information on the topic by experienced readers but it is not suitable as a primer for the topic. The results of performed experiments surely bring interesting insights into the behavior of the protocols. Unfortunately due to some problems with the experiment design and implementation issues, results must be interpreted very carefully by the reader and as the author himself correctly concludes, selection of proper protocol must be based on the intended use case in the first place.

5. Activity of the student

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

Activity was not great. Student had a lot of time for writing the thesis but the time was not utilized well.

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

Student was completely self-reliant. Student found and used proper references immediately. When dealing with implementation issues, no help was needed from the supervisor and student proved great orientation in the world of many independent open source technologies.

The overall evaluation 79 /100 (C)

Student did tremendous amount work studying the protocols, analyzing them and running them on various platforms. There were many implementation issues caused by immaturity of used technologies. Student overcame most of the issues which required diving into many technological topics (such as multiple programing languages, message brokers and messaging libraries), many of them new for the student.

Unfortunately, presentation of this work in the form of written thesis has several problems, mainly with experiment design and providing all necessary information to the reader in suitable manner.

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.