FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Supervisor's statement of a final thesis

Supervisor:	Ing. Karel Hynek
Student:	Richard Plný
Thesis title:	Crypto-currency miner detection from extended IP flow data
Branch / specialization:	Computer Security and Information technology
Created on:	26 May 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

The assignment was fulfilled. The student described network monitoring approaches and mapped the cryptocurrency environment. On top of the assignment, the student has surveyed related research works about crypto miners detection. This knowledge was then used to design a cryptocurrency miner detector based on extended flow data. The student has decided to use the concept of heterogeneous classifiers, which increases the robustness and accuracy of detection; however, this decision also caused a significant increase in the required work.

2. Main written part

100 / 100 (A)

The thesis is written in English, and it is logically structured. During my reading, I have not found any language or typographical errors. The text perfectly describes the student's thinking and provides full reasoning of his decisions during the design of the classifier.

3. Non-written part, attachments

100 / 100 (A)

The thesis attachment consists of created datasets and python source codes, used for their analysis and classifier design. Additionally, it also contains the source code of the NEMEA module for miner detection, which is already deployed at the CESNET monitoring infrastructure. Even the attachments of the thesis are excellent, and I could not find any mistakes. The source codes are easily understandable and commented. Moreover, the datasets can be used for other network analysis tasks since it contains valuable real-world traffic.

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

I found the design of the classifier unique. The heterogeneous principle of its operation increases its robustness and precision, which outperforms current state-of-the-art detectors deployable on large infrastructure. Thus, we plan to publish the results at an academic conference. Apart from the research outputs, the implemented classifier is already deployed on the CESNET2 network and it is already protecting its users. Moreover, since CESNET2 is the internet service provider for the national computational grid Metacentrum, the implemented detector protects against the abuse of its massive computational resources.

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 was very active and always came to scheduled consultation meetings on time.

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 student was always prepared for scheduled consultation meetings and brought new ideas.

The overall evaluation 100/100 (A)

Overall, the student created an excellent thesis, which is according to my opinion without any flaws. The thesis presents an innovative crypto miner detector design based on a thorough data analysis of created datasets, which capture multiple months of real-user traffic. Whole detection architecture consists of three different classifiers, which are then combined together using a mathematical model called Dumpster-Shaffer Theory. The whole detector was then thoroughly tested and achieved outstanding accuracy. Due to the quality of the text, and the innovative design of the detector, I consider the thesis excellent. Therefore I would kindly suggest nominating the thesis for the Dean's Award.

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.