THESIS SUPERVISOR'S REPORT

I. IDENTIFICATION DATA

Thesis title:	**Identifying Groups of Attackers Using Minimal Honeypots**
Author's name:	**Miroslav Hanák**
Type of thesis :	master
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	Department of Measurement – K13138
Thesis reviewer:	Ing. Pavel Píša, Ph.D.
Reviewer's department:	Department of Control Engineering - K13135

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment — challenging

How demanding was the assigned project?

The main implementation goal was to replace previous Turris honeypot design (telnet only) by a new one with support for HTTP, FTP, and SMTP protocols in addition. Support for new protocols data collection and logging was integrated into CZ.nic Sentinel system and used to collect actual attacker attempts. There has been demanding to cooperate with a larger team working on other components of the system. The durability of the design is critical because a potential flaw can endanger thousand of Turris router users after large scale deployment. The last goal was focused on the research of behavioral and distribution patterns of attackers and botnets and requires integrate theory proven algorithm novel way into attack prevention fields of study.

Fulfilment of assignment — fulfilled

How well does the thesis fulfil the assigned task? Have the primary goals been achieved? Which assigned tasks have been incompletely covered, and which parts of the thesis are overextended? Justify your answer.

The student fulfilled completely goal 1 to get familiar with the required phases of HTTP, FTP, and SMTP protocols and collected important information and references in the thesis text, which is useful even for followup work and developers. Goal 2 to reimplement and extend honeypot has been fully fulfilled. Goal 3, the data collection and analysis tools have been designed and integrated into the Sentinel system and have been deployed on the first 48 devices. The deployment has been delayed due to testing and review needed for confidence in the design security from other team members the confidence in design security. That is why analyzed data has been acquired in a short period only (9 days). The preparation of multiple cluster analysis algorithms has been done in parallel and tested with the obtained dataset. Initial results are presented, and discussion of future work is attached, goal 4.

Activity and independence when creating final thesis — A - excellent.

Assess whether the student had a positive approach, whether the time limits were met, whether the conception was regularly consulted and whether the student was well prepared for the consultations. Assess the student's ability to work independently.

The student started to work on the project immediately after the assignment (more than one year before submission). He became a member of the Sentinel team and started coding even before official work assignemnt. He has delivered honeypot implementation in the planned time even that he has been hit by objective obstacles, an internship in quarantine time preventing him from returning to the Czech Republic for months. However, due to these events, he has started late on the actual theses text preparation, which negatively impacts its quality. There have been delays in the cooperation on system deployment and data collections due to the global situation, as well.

Technical level — A - excellent.

Is the thesis technically sound? How well did the student employ expertise in his/her field of study? Does the student explain clearly what he/she has done?

The technical level of the implementation work has been evaluated mainly by project leader at the CZ.nic, Ing. Karel Kočí

with expression of significant respect for the work. I evaluate the actual implementation and code versioning as fulfilling a high standards level. However, I, personally, miss structured comments and documentation generated from the sources.

Formal level and language level, scope of thesis C - good.

Are formalisms and notations used properly? Is the thesis organized in a logical way? Is the thesis sufficiently extensive? Is the thesis well-presented? Is the language clear and understandable? Is the English satisfactory?

The text of the work reflects the fact that it has been written under tight time constraints, and there are many places where language can be improved if more time and review cycles fit. I miss better documentation of some decisions made during honeypot architecture design and highlighting and connection of the used principles to actual core function and data structures in the code.

Selection of sources, citation correctness A - excellent.

Does the thesis make adequate reference to earlier work on the topic? Was the selection of sources adequate? Is the student's original work clearly distinguished from earlier work in the field? Do the bibliographic citations meet the standards?

The number of references and sources is high and valuable for project extensions, maintenance, and followup developers.

Additional commentary and evaluation (optional)

Comment on the overall quality of the thesis, its novelty and its impact on the field, its strengths and weaknesses, the utility of the solution that is presented, the theoretical/formal level, the student's skillfulness, etc.

III. OVERALL EVALUATION, QUESTIONS FOR THE PRESENTATION AND DEFENSE OF THE THESIS, SUGGESTED GRADE.

The thesis work results are valuable for the whole Turris, and CZ.nic attacks prevention project. The project is connected to national wide (NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost) activities. There are more developers and many users interested, working and cooperating in the project, and the respectable organization, CZ.nic, initiated and backs it. There is high confidence in its continuation and widespread use. Designed systems and tools provide valuable data for state of the art and beyond going research of attackers behaviors and ways to prevent it.

The grade that I award for the thesis is A - excellent.

Date: **26.8.2020** Signature: