THESIS REVIEWER'S REPORT

I. IDENTIFICATION DATA

Thesis title:	**Global P2P Network for Confidential Sharing of Threat Intelligence and Collaborative Defense**
Author's name:	**Bc. Martin Řepa**
Type of thesis :	master
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	Artificial Intelligence Center
Thesis reviewer:	Ing. Karel Hynek
Reviewer's department:	Department of Digital Design, Faculty of Information Technology

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment **challenging**

How demanding was the assigned project?

The student needed to study the design principles of P2P networks, its abuse possibilities, and apply this knowledge to create a novel P2P security intelligence sharing platform. Therefore, I consider the assignment challenging.

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.

All points from the assignment have been fulfilled. The designed system is built on top of the libp2p project, minimizes the risk of information abuse by threat actors and each design step is thoroughly analyzed from a security point of view.

Methodology **correct**

Comment on the correctness of the approach and/or the solution methods.

I do not have any objections against the approach and design solutions presented in the thesis. The student spent time in the validation of design solutions against known security attacks on P2P networks and performed an extensive evaluation of information spreading to avoid network overload. The whole system was implemented in the GO language and integrated with SLIPS IPS. However, I miss a description of the implementation testing and verification methods.

Technical level **A - excellent.**

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

The technical level of the thesis is excellent. The student correctly applied his knowledge about P2P networks and designed a novel one. All design choices are clearly described in text parts, even though it would sometimes be better to add an explanatory figure.

Formal and language level, scope of thesis **B - very 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 thesis is logically structured and covers all required topics from the assignment. However, I noticed the usage of terms (such as bootstrapping attack) before their explanation in the thesis. Moreover, I found some typographical errors and text inconsistencies. However, overall, I found the thesis understandable with clear and satisfactory English.

Selection of sources, citation correctness **C - good.**

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 citations and references are, unfortunately, the weakest part of the thesis. Collaborative Intrusion detection systems and alert sharing is a well-established area; however, the student describes and reference only a handful of approaches.

Moreover, some paragraphs in Chapter 2 would benefit from additional references that would support the statements (e.g., in Section 2.4.2, 2.4.3). I have also found mistakes in bibliography records.

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.

I really enjoyed the thesis, which tackles the problems rising from decentralized P2P networks. Moreover, the proposed design principle of trusted organizations is very good and could work in a real deployment.

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

Summarize your opinion on the thesis and explain your final grading. Pose questions that should be answered during the presentation and defense of the student's work.

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

Bc. Martin Řepa designed a P2P communication extension of SLIPS to allow decentralized and collaborative intrusion detection. The proposed design considers security aspects and possible abuse of P2P principles, moreover it also deals with users' trust by so-called trusted organizations.

The thesis provides necessary background knowledge about P2P network principles and analyzes them from a security point of view. Possible attacks on P2P networks are thoroughly discussed. This information is then used during the description of the system design.

I found the P2P system design very good. It successfully solves the requirements from the assignment. Moreover, the student also perfectly dealt with the integration of the black box trust model. Since a low-latency response is crucial for a successful defense, the student also comprehensively evaluated the propagation delay of information across the P2P network. The thesis also discusses potential room for improvement in future work.

Questions:

Can you describe the methods used for verification of the implemented extension of SLIPS?

The designed network opinion protocol uses Time To Live (TTL) for network overload prevention. What if a malicious peer fills TTL with an enormous number and continuously asks?

Even though the thesis has some weak spots in references and typography, I found them marginal and consider the thesis in the overall evaluation excellent — grade A.

Date: **7.6.2022**

Signature: