

I. IDENTIFICATION DATA

Thesis name:	Trust Model for Global Peer-To-Peer Intrusion Prevention System
Author's name:	Lukáš Forst
Type of thesis :	master
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	Department of Computer Science
Thesis reviewer:	Ing. Dita Hollmannová
Reviewer's department:	

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment	extraordinarily challenging
<i>Evaluation of thesis difficulty of assignment.</i>	
The thesis aims to propose a solution to a problem that was not yet fully solved. Trust models for other use cases are known, but applying them to the field of IPSs is mostly not possible. Furthermore, in an IPS, a trust model is part of a critical security system, and must be resilient. This makes the assignment very challenging.	

Satisfaction of assignment	fulfilled
<i>Assess that handed thesis meets assignment. Present points of assignment that fell short or were extended. Try to assess importance, impact or cause of each shortcoming.</i>	
The thesis proposes a trust model, discusses its properties and analyses its behavior in experiments. The trust model is also implemented as a module to an IPS.	

Method of conception	outstanding
<i>Assess that student has chosen correct approach or solution methods.</i>	
The student researched existing trust models, their advantages and weak points. The model proposed in the thesis builds on an older trust model from a different field, modifying and extending it to be able to work with threat intelligence data. Several functions needed for inner workings of the model were designed, each with a justification of the thought process. The experiments were designed to rate the performance of those functions, and the thesis proposes a well-performing configuration.	

Technical level	A - excellent.
<i>Assess level of thesis specialty, use of knowledge gained by study and by expert literature, use of sources and data gained by experience.</i>	
The thesis contains thorough research, the model is well constructed and extensible and the source codes are documented and easily readable.	

Formal and language level, scope of thesis	B - very good.
<i>Assess correctness of usage of formal notation. Assess typographical and language arrangement of thesis.</i>	
The thesis is well structured, with all the topics properly introduced. The document appears to be based on the professional-looking LaTeX template provided by the school. High-level technical English is used, but there are a few small typographical or grammar errors.	

Selection of sources, citation correctness	A - excellent.
<i>Present your opinion to student's activity when obtaining and using study materials for thesis creation. Characterize selection of sources. Assess that student used all relevant sources. Verify that all used elements are correctly distinguished from own results and thoughts. Assess that citation ethics has not been breached and that all bibliographic citations are complete and in accordance with citation convention and standards.</i>	
The thesis is based on research of trust models, and multiple citations on the subject are included. No violation of citation policy was encountered.	

Additional commentary and evaluation

Present your opinion to achieved primary goals of thesis, e.g. level of theoretical results, level and functionality of technical or software conception, publication performance, experimental dexterity etc.

The student fulfilled the assignment, designing and implementing a trust model for an IPS. The thesis describes the model, justifies design choices and discusses model performance in different environments. The provided source codes are structured and follow a code style. In future work, several promising improvements are suggested. Overall, the student researched a difficult topic, proposed and implemented a solution that can be deployed in the real-world, and described the process in a comprehensive way.

III. OVERALL EVALUATION, QUESTIONS FOR DEFENSE, CLASSIFICATION SUGGESTION

Summarize thesis aspects that swayed your final evaluation. Please present apt questions which student should answer during defense.

Question 1: What is the behavioral pattern of pre-trusted peers in the experiments? How does the model behave if some of the pre-trusted peers are uncertain?

Question 2: The model assigns a weight to each interaction. According to the thesis, the weight of an interaction is higher when a remote peer shares Threat Intelligence, as opposed to when a remote peer requests it. Why was this decision made?

I evaluate handed thesis with classification grade **A - excellent**.

Date: **8.6.2022**

Signature: