SUPERVISOR'S OPINION OF FINAL THESIS

I. IDENTIFICATION DATA

Thesis name:	Anomaly detection of host roles in computer networks
Author's name:	**Click here to enter text.**
Type of thesis :	Bc. Yury Kasimov
Faculty/Institute:	Faculty of Electrical Engineering
Department:	Department of Computer Science
Thesis supervisor:	Sebastian Garcia
Supervisor's department:	Department of Computer Science

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment **Extraordinarily challenging**

Evaluation of thesis difficulty of assignment.

The topic of Anomaly Detection (AD) in security is in general a very difficult and hard problem. The difficult is not only in applying the algorithms correctly, but in the scarce amount of real labeled datasets, the difficulty of the verifications and the high cost of errors. Working with AD requires a lot of work and understanding, but also clear methodologies and careful experiments.

Satisfaction of assignment **fulfilled**

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.

The thesis fulfils the assignment. Considering that the topic of AD in security is vast and complicated, the thesis manages to study, research and finish a good work. The shortcomings of the thesis are: (1) the need for a better dataset that includes a large variety of situations in the normal users, (2) an more extensive analysis of the errors to better understand why the method failed, (3) a more complex voting mechanism to get together the output of each AD on each feature. However these shortcoming

Activity and independence when creating final thesis **Very good**

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

The student had a very positive approach to get into a difficult topic, dealing with new ideas, problems, algorithms and times. The time limits were perfectly meet. Yury consulted regularly and on every occasion he was perfectly prepared to discuss the topics and talk about his work. Yury is perfectly capable for working independently. At the contrary, he may do well in exercising working with peers.

Technical level **Very good**

Assess level of thesis specialty, use of knowledge gained by study and by expert literature, use of sources and data gained by experience.

The thesis has a very unique and different approach. Common research in Anomaly Detection methods focus on creating new algorithms. However, Yury proposed to see the problem from the point of view of understanding the security issues around using AD for network malware detection. This means that he did a large analysis of the data structures which better represent the behavioral characteristics to the malware studied. This required from Yury a deep commitment to understand the deepest levels of security attacks. He studied the literature and created his own datasets alone.

Formal and language level, scope of thesis **Very good**

Assess correctness of usage of formal notation. Assess typographical and language arrangement of thesis.

The use of formal notation was correct and precise. The language used in the thesis is English, which is not the native language of Yury. To be able to write a Master thesis with this level of English, shows that Yury is capable of expressing himself without problems.

Selection of sources, citation correctness **Excellent**

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.

Yury did a very good and extensive use of sources, citations and background work. The sources were paramount in the understanding of the topic and they are the state of the art in this area. All the citations are correct.

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.

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

SUPERVISOR'S OPINION OF FINAL THESIS

The thesis presented a new method to detect the behavior of malware in the network by using anomaly detection methods. The primary results were achieved by applying the algorithms in a novel way that required the understanding the the malware actions. The primary goals of the thesis, then, were met. More importantly, Yury finished and published his code in order to be usable and extendable.
My main concern is that his work has to be continued and improved, because a good AD algorithm takes time to evaluate and reach the production level.

III. OVERALL EVALUATION, QUESTIONS FOR DEFENSE, CLASSIFICATION SUGGESTION

This thesis presents a system to detect the behaviour of real malware in the network based on anomaly detection methods. The system is based on real malware that was executed by the student in a unique and novel way. The datasets are the first ones of their kind to be published. The method used by the student was novel and showed to be enough to detect anomalies with a 0 False Positive Rate. Which is a very good result. Its true that more variability is needed in order to better estimate the performance of the algorithm and that a more suitable methodology would be needed to balance the detections of each algorithm.

I evaluate handed thesis with classification grade **: B**

Date: **2018/06/04** Signature: