ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

REVIEWER'S OPINION OF FINAL THESIS

I. IDENTIFICATION DATA

Thesis name:	**The Attacker IP Prioritizer: An IoT Optimized Blacklisting Algortihm**
Author's name:	**Tomas O'Hara**
Type of thesis :	bachelor
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	Computer Science Department.
Thesis reviewer:	Carlos A. Catania (phD)
Reviewer's department:	Computer Science Department. National University of Cuyo, Mendoza, Argentina

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment — challenging

Evaluation of thesis difficulty of assignment.

The thesis involves the development of several strategies for building blacklists focused on the current hardware limitation of IoT devices. Despite the simplicity of the solutions, the elements required for the evaluation of blacklists strategies (including the generation of a labeled dataset) implies a significant amount of time and work.

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 work in the thesis has clearly met the assignment. The student has developed the central aspects of a strategy for generating blacklists capable to deal with IoT devices resource limitation. According the results shown in the thesis, the three approaches applied to blacklist generation were competitive compared with well-known blacklists. One major contribution of the thesis is the methodology for evaluating different blacklists approaches. I personally was surprised about the poor performance of very well-known blacklist. Clearly, as stated by the student in the conclusions, blacklist approaches should put more efforts in estimating their blocking performance.
A major shortcoming of the proposed evaluation methodology is not including information about the specificity and recall of the blacklists generated. The current evaluation methodology seems to be only focused in measuring the impact on malicious traffic and not considered background and normal traffic.

Method of conception — correct

Assess that student has chosen correct approach or solution methods.

Despite the lack of a significant amount of research in the field of blacklists generation, the student has followed a coherent methodology for developing and evaluating a novel approach for blacklist construction from network data. The methodology includes a carefully designed dataset and a set of metrics for consistently comparing the performance against well-known blacklist approaches.

Technical level — B - 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 student has proven himself capable of dealing with a new problem and provided a valid solution using a different set of tools. He has showed expertise in several areas such as basic

statistics, machine learning and network security.

Formal and language level, scope of thesis B - very good.

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

In general, the document is well written. The student expressed in a simple but clear language the different aspects involved in the process of building blacklist generation algorithms using formal notation when required.

Selection of sources, citation correctness A - 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.

The student has always made reference to third party articles and software applications used for meeting the thesis assignment. All references used in the work followed the proper quality standards.

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.

Please insert your commentary (voluntary evaluation).

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.

In this thesis, the student has presented a new methodology for generating blacklists according to the hardware limitations observed in IoT devices. The students has proposed three novel strategies for black list creation together with a complete new framework for evaluating their performance. In addition, the student has provided to the community a carefully curated dataset for further comparison of blacklist approaches.

APT questions:

1) What are the reason behind the election of Random Forest for classification? Have you considered the use of other tree-based algorithms (i.e. Xgboost, catboost)

2) Why have you not considered the use of resampling techniques during for Random Forest algorithm?

3) Why have you only considered malicious traffic for the evaluation framework. Shouldn't be normal traffic also included in your metrics? According the your state of the art review, this seems to be a common approach.

REVIEWER'S OPINION OF FINAL THESIS

4) How difficult could be for someone else to replicate your results using his own generated datasets? Are the tools you used during your work freely available?

5) In the introduction the student mentioned that the blacklists were freely available. However, I could not find any other mention to the feed in the rest of the document. What are the URLs of the blacklist feeds?

I evaluate handed thesis with classification grade A - excellent.

Date: 06/09/2021 Signature:

Carlos A. Catania (PhD)