THESIS SUPERVISOR'S REPORT

I. IDENTIFICATION DATA

Thesis title:	**Machine learning privacy: analysis and implementation of model extraction attacks**
Author's name:	**Vít Karafiát**
Type of thesis :	Master
Faculty/Institute:	Faculty of Electrical Engineering
Department:	Department of Computer Science
Thesis reviewer:	Maria Rigaki
Reviewer's department:	Department of Computer Science

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment **A - excellent.**

How demanding was the assigned project?

The project was demanding because it required a significant amount of both research and software development. In addition, the research part was on privacy attacks in machine learning which was not part of the student's study area .

Fulfillment of assignment **B - very good.**

How well does the thesis fulfill 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 thesis fulfilled the majority of the goals successfully. The developed tool covered all the requirements and with a good design and software quality. The student also proposed and implemented improvements in various attacks, however there was not enough time to fulfill some of his ideas or perform even more extensive experiments.

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.

Communication was very good and frequent during the thesis development. The student was able to work independently and to propose solutions and improvements during the project. Although the topic was out of the student's main area of study he managed to read, understand, and implement attacks based on research papers that sometimes did not provide software implementations.

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 software part of the thesis was of high quality. The implementation of the attacks were tested for correctness and the different experiments were explained clearly.

Formal level 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 structure is well defined and it is easy to follow. The document is quite extensive and covers all necessary aspects of a diploma thesis. The language is quite clear but the English could be a little better. The discussion of the experimental results could have been more extensive so that the reader would get some clear outcomes and takeaways from the experiments.

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?

All necessary prior work was cited and referenced properly. The student covered a number of model extraction attacks which were also explained clearly in the related work chapter. Other prior work including tools was also referenced and compared.

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.

The quality of the overall work is quite high. Privacy attacks are a developing area of research and having a tool to test different model extraction attacks and compare them under different conditions is very useful. The thesis can be a stepping stone for further research as it already showed some interesting initial results in the experimental evaluation. The thesis' software can also be used by people that want to test their own models and verify them against these attacks.

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.

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

The thesis goals were quite demanding, however the student managed to fulfill them. During the year the student worked hard and showed critical thinking and ability to perform research, even though parts of the topic such as machine learning, were not in his main area of study. The final outcome was of high quality, both in terms of software and also in terms of experimental results.

Date: **11.6.2021** Signature: