Supervisor's statement of a final thesis

Czech Technical University in Prague **Faculty of Information Technology**

Student:	Ing. Raúl Carmelo Benítez Netto
Supervisor:	Ing. Sebastián García, Ph.D.
Thesis title:	ManaTI: Web Assistance for the threat Analysis supported by Domain Similarity
Branch of the study:	Computer Security

Date: 5. 6. 2017

Evaluation criterion:	*The evaluation scale: 1 to 5.*
1. Difficulty and other comments on the assignment	*1 = extremely challenging assignment,* ***2 = rather difficult assignment,*** *3 = assignment of average difficulty,* *4 = easier, but still sufficient assignment,* *5 = insufficient assignment*

Criteria description:
Characterize this final thesis in detail and its relationships to previous or current projects. Comment what is difficult about this thesis (in case of a more difficult thesis, you may overlook some shortcomings that you would not in case of an easy assignment, and on the contrary, with an easy assignment those shortcomings should be evaluated more strictly.)

Comments:

The thesis assignment is rather difficult compared to the average Master Thesis because it encompass two main topics simultaneously. First, the development of a production-ready, novel and advanced web and backend software to help the company Cisco Systems in their analysis of malware traffic. Second, the development of a new algorithm of domain similarity and classification based on WHOIS information, which in itself is a good contribution to the community of researchers.

The thesis was done as part of the Manati Project, a joint project between Cisco Systems and the Department of Computer Science, FEE, CTU. Therefore, the thesis had to be valuable and usable for Cisco while at the same time develop a new algorithm using machine learning. The most difficult part of this double assignment was the verification of both parts separately. The software was evaluated by measuring several usage metrics of the webpage while experts analyze real data. The algorithm was evaluated by using real training and testing malware datasets.

Evaluation criterion:	*The evaluation scale: 1 to 4.*
2. Fulfilment of the assignment	***1 = assignment fulfilled,*** *2 = assignment fulfilled with minor objections,* *3 = assignment fulfilled with major objections,* *4 = assignment not fulfilled*

Criteria description:
Assess whether the thesis meets the assignment statement. In Comments indicate parts of the assignment that have not been fulfilled, completely or partially, or extensions of the thesis beyond the original assignment. If the assignment was not completely fulfilled, try to assess the importance, impact, and possibly also the reason of the insufficiencies.

Comments:

This thesis fulfilled the assignment statement completely. The assignment was to develop a software that can help analysts and to develop a new algorithm to classify domains. Both parts were created, evaluated and reported.
The importance of the thesis can be seen in how the final software is currently used in Cisco Systems for production and how there is a necessity to keep improving it. Thanks to this thesis the Manati Project will be extended and new features will be added.
Among the extensions beyond the original assignment was the creation of a classification algorithm besides the original idea of a distance measure between domains.

Evaluation criterion:	*The evaluation scale: 1 to 4.*
3. Size of the main written part	***1 = meets the criteria,*** *2 = meets the criteria with minor objections,* *3 = meets the criteria with major objections,* *4 = does not meet the criteria*

Criteria description:
Evaluate the adequacy of the extent of the final thesis, considering its content and the size of the written part, i.e. that all parts of the thesis are rich on information and the text does not contain unnecessary parts.

Comments:

The size of the main written part of the thesis meets the criteria of a standard thesis. With 85 pages, the thesis makes place to the most important parts, without being too extensive. If anything, the thesis could have included more details about the development part, since there is a lot of work that could not be explained easily. This is why the main code was published on the Internet, so it is possible to actually try it.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
4. Factual and logical level of the thesis	*85 (B)*

Criteria description:
Assess whether the thesis is correct as to the facts or if there are factual errors and inaccuracies. Evaluate further the logical structure of the thesis, links among the chapters, and the comprehensibility of the text for a reader.

Comments:
The thesis presents correct factual data and there are no inaccuracies that I can find. However, the comprehensibility of the thesis is not as good as it can be. In particular the English should be improved, both syntactically and semantically. In particular there are parts of the thesis that lack a coherent fluidity and it is difficult to follow. Therefore I would suggest the student to improve his written English in general and his scientific English in particular.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
5. Formal level of the thesis	*100 (A)*

Criteria description:
Assess the correctness of formalisms used in the thesis, the typographical and linguistic aspect s, see Dean's Directive No. 14/2015, Article 3.

Comments:
The formal level of the thesis is correct. It includes all the requirements in the Article 3 of Dean's Directive, including the typographical and linguistics aspects.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
6. Bibliography	*70 (C)*

Criteria description:
Evaluate the student's activity in acquisition and use of studying materials in his thesis. Characterize the choice of the sources. Discuss whether the student used all relevant sources, or whether he tried to solve problems that were already solved. Verify that all elements taken from other sources are properly differentiated from his own results and contributions. Comment if there was a possible violation of the citation ethics and if the bibliographical references are complete and in compliance with citation standards.

Comments:
The bibliography of the thesis is one of its weakest points. Although the student covered the main topics regarding the previous work, there is a general lack of deepness in the works covered. The fact that there are two main topics in this thesis made this more difficult, but anyway the coverage of other works should have been more extensive.
The student reported enough previous works to make it clear that the problem is not solved and that there is a large opportunity for more research. However, due to the large amount of topics covered by the thesis, there are several works left aside. This issue did not diminish the value of the thesis, but it made it appear less precise.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
7. Evaluation of results, publication outputs and awards	*95 (A)*

Criteria description:
Comment on the achieved level of major results of the thesis and indicate whether the main results of the thesis extend published state-of-the-art results and/or bring completely new findings. Assess the quality and functionality of hardware or software solutions. Alternatively, evaluate whether the software or source code that was not created by the student himself was used in accordance with the license terms and copyright. Comment on possible publication output or awards related to the thesis.

Comments:
The evaluation of the results has been well accomplished since the thesis was evaluated in two different manners. First there was an evaluation of the software from the point of view of how it really helped the analysts. This was an important evaluation since the goal of the software was to improve the evaluation of data. The evaluation using real experts took into consideration how much their analysis improved in time because of the tool.
The second evaluation was of the machine learning algorithm to classify similar domains. This was done by using a real malware and normal dataset created (and more importantly labeled) by the student.

Regarding the results obtained in the evaluation of the software, an improvement of 4.3 times in the time spend by the analysts working on the data is a very good start. This means that the same work can be done now in less than a quarter of the original time.
In contrast, the results obtained for the machine learning algorithm can be possible improved in the future. This may not seem as a clear option since the results reported had a FPR or 0%, but our suspicion is that given more data, the errors will be larger. As with any machine learning algorithm, testing in other real environments may help to find its true generalisation power.
The work done in the thesis is completely fit for publication in an academic conference, both from the perspective of the software and the algorithm.
However the most important reward was the approval from Cisco Systems to continue this research.

Evaluation criterion:	*No evaluation scale.*
8. Applicability of the results	

Criteria description:
Indicate the potential of using the results of the thesis in practice.

Comments:
The results are 100% applicable. Moreover, the results are right now 100% being applied.
Since this thesis was done inside a project with Cisco Systems, the thesis was used and evaluated during the whole time the student was doing it. This guaranteed that the company was satisfied with the final product.
Also, this thesis has the potential to be a product that other companies may find suitable. Therefore, this line of work will be evaluated in the future.

Evaluation criterion:	*The evaluation scale: 1 to 5.*

9. Activity and self-reliance of the student	*9a:* *1 = excellent activity,* ***2 = very good activity,*** *3 = average activity,* *4 = weaker, but still sufficient activity,* *5 = insufficient activity* *9b:* *1 = excellent self-reliance,* ***2 = very good self-reliance,*** *3 = average self-reliance,* *4 = weaker, but still sufficient self-reliance,* *5 = insufficient self-reliance.*

Criteria description:
Review student's activity while working on this final thesis, student's punctuality when meeting the deadlines and consulting continuously and also, student's preparedness for these consultations. Furthermore, review student's independency.

Comments:

The student had a good activity during his thesis. In particular he was excellent for the development of the software. However, his research skills need to be improved and honed. He was puntual to all the meetings and he took care of half the meetings with Cisco Systems.

Regarding his independency, I very much appreciated his proactiveness and ideas, specially for new features and improvements in the software.

However, as a Master, he still needs to learn to be more independent and focus more on his research. There is place for growing.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
10. The overall evaluation	*95 (A)*

Criteria description:
Summarize the parts of the thesis that had major impact on your evaluation. The overall evaluation **does not** have to be the arithmetic mean or any other formula with the values from the previous evaluation criteria 1 to 9.

Comments:

Overall the thesis is a good work with a lot of effort and dedication. If something the thesis document fails to reflect all the work done, which somehow diminish its importance. The student successfully solved the double assignment and worked particularly well on the software development to help a production security company and the WHOIS classification algorithm.

In the WHOIS algorithm, the larger impact was attributed to the selection of features and the evaluation in real data.

In the software, the larger impact was its real use in production environments (which means high stability), its improvement of the analysis tasks and the extensibility with modules.

Signature of the supervisor: