**FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE**

Supervisor's statement of a final thesis

Student:	Jan Fajfer
Supervisor:	Ing. Josef Kokeš
Thesis title:	Correlation Attacks on TOR
Branch of the study:	Computer Security and Information technology

Date: 17. 5. 2018

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 work studies an attack on TOR user's anonymity using correlations between data streams. While the attack involves both networks and statistics, it is not overly complicated.

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:
The assignment was fulfilled.

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 length of the finished text meets the requirements for a bachelor's thesis.

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 factual level of the work is very good, as is,for the most part, its logical structure. Some concepts would benefit from being described in more detail, though, particularly the separation of the observed traffic into individual streams. A comparison with previous results would be nice, too.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
5. Formal level of the thesis	*90 (A)*

Criteria description:
Assess the correctness of formalisms used in the thesis, the typographical and linguistic aspect s, see Dean's Directive No. 26/2017, Article 3.

Comments:

The formal level of the thesis meets the expectations we have of such works. The language used is easy to understand and only contains very few errors; the notable exception is section 4.3, which needs a more detailed spellcheck. Typographically, I have just a few minor complaints, mostly limited to section 4.3. I don't understand the frequent separation of paragraphs with empty lines.

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

6. Bibliography *90 (A)*

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 work references 40 sources. The website torproject.org appears 15 times in the list, which is a lot, but the reason for that was to provide more accurate references rather than pointing just to the homepage and I have no complaints with that. The remaining works are relevant and are cited properly. More effort could have been put to dating the references, though.

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

7. Evaluation of results, publication outputs and awards *85 (B)*

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 results convincingly show that correlation attacks represent a viable strategy for adversaries attempting to break the anonymity purportedly provided by the TOR network, and that users should be wary of that fact. The student also proposes several possible counterstrategies and verifies their effectiveness. I consider that a nice contribution.

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:

While the theoretical aspects of this thesis aren't new, the practical results should force the TOR users to sit up and reconsider whether their setup is as secure as they might have believed. Apparently, to maintain anonymity, more effort than just installing and using TOR Browser might be needed. That awareness is definitely a worthwhile result.

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 worked mostly on his own, perhaps too much so. I would have appreciated a more frequent meeting frequency. However, it seems that it wasn't necessary.

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

10. The overall evaluation *90 (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:

The thesis focuses on an important topic of maintaining user's anonymity on the internet. It demonstrates an attack that can violate that anonymity even though TOR network is being used to protect it, and it suggests - and measures - several strategies for reclaiming the anonymity. While there are a few issues with the work, none of them are significant enough to prevent me from recommending a grade A - excellent.

Signature of the supervisor: