Internal examiner report – PhD thesis proposal

Title: **Behavioral Distributed Dictionary Attack Detection**

Proposer: **Martin Drašar**

Examiner: **Vashek Matyáš**

Proposer's PhD thesis proposal deals with issues of anomaly-based attack detection, and in particular the network-level detection based on analyses of network flows. The stated goals of future research include a preliminary implementation of aspect-based detection mechanism; definitions of dictionary attack sets; and then suddenly a production deployment of the dictionary attack detection in the university network.

The text starts with an introduction, followed by Chapter 2 with a state-of-the-art overview. Both these chapters are reasonably well written in all but the closing part of Chapter 2. The closing summary (part 2.4) of the second chapter provides only negative observations without any clear statement why the author decided for this approach. Moreover, the criticism is not clearly related to particular methods (phrases like "most of these methods" and "many methods" appear a way too often). Since it is clear (from these phrases) that the individual points of the criticism do not apply to all methods, the author failed to provide a solid conclusion what advantages and disadvantages are to be found in the alternative approaches considered. I am afraid that the author is too dismissive of other approaches without any solid arguments. A minor observation is that the problem of "a high positive rate" is not clear – does this imply a high level of false positives or something else? Chapter 3 describes the proposed research and its scheduled steps.

Language of this proposal is very good, there only very minor issues (commas, some mistakes like "methods that crafts", etc.) that I found. References to literature should be separated by spaces and also multiple references done properly.

While I have to admit that I have certain reservations about this thesis proposal, my view is that the goals and overall focus of the proposed work are (with some added information and interpretation) of a sufficient merit for a PhD dissertation.

Unclear issues and questions:

1. How is the level of stealthiness measured or judged, i.e., how will it be decided whether one attack is "stealthier" than others or how will an increase in stealthiness be judged?

2. The *WitchdOCtoR* tool is not properly referenced and namely it is not clear why only this tool is to be used to simulate attacks for further work. It should be made clear what other approaches were considered and why those are not as useful as the WitchdOCtoR based generation.

3. It is not clear from the proposal what approach/method will be taken to make the step from a (simulated) attack description to the proposal of detection. Is the description of anomalies actually so trivially derived from simulated attacks? If so, why only one tool

for the attack simulation is to be considered? If not, what approach(es) will you consider to derive the anomaly descriptors from the attack descriptors, and how will you derive the attack descriptors from the simulated attacks?

4. In the third step of the proposed schedule, an "evaluation of capabilities of other detection methods" is planned. What methods will these be?

5. Last but not least, the most serious issue I see in the proposed schedule concerns that fact that a heavy focus is aimed at "crafting" sets of attacks and refining their specification, but the author pays very little attention to the actual attack detection.

Proposal: Approve further work on the topic and goals suggested, with a strong warning that a substantial part of research work still has to be undertaken (see points above and recommendations below). With respect to the award of the RNDr. degree, I am unable to decide for or against since it is not clear from the documentation provided:

- what is the author's contribution to the two documents attached,
- why are these two documents not referenced in the PhD thesis proposal, and
- whether these two documents contain original results that are integral to the actual research proposal.

Recommendations to the author: Firstly, extend your evaluation of other approaches to attack detection and properly consider their pros and cons. Secondly, consider more than one approach to attack simulation and generation – and make sure you have representative attack sets. Thirdly, be very careful when you consider what approaches you take to advance from a (simulated/generated) attack description to the proposal of detection approach(es) that is/are the ultimate core aim of your research. Be considerate and keep your eyes open when investigating and considering different approaches, do not make (too) early conclusions based on immature results – consider alternatives and examine them in more breadth and depth.

Bílovice nad Svitavou, March 5, 2011

Vashek Matyáš