Internal examiner report – PhD thesis proposal

Title: **Flow-based Intrusion Detection in Large and High-Speed Networks**

Proposer: **Jan Vykopal**

Examiner: **Václav Matyáš, KPSK, FI MU**

Proposer's PhD thesis deals with selected issues of flow-based intrusion detection that are relevant to network behaviour analysis of high-speed networks, namely with respect to online dictionary attacks on systems with password-based authentication. The stated goals of future research are quite clear and should lead to both promising results and also to an interesting PhD thesis. The plans are both challenging and realistic, with only one considerable drawback – unclear methodology (or even path to its achievement) with respect to the method(s) evaluation.

The text starts with an introduction, and then Chapter 2 provides an overview of relevant issues in network behaviour analysis and dictionary attack detection. Chapter 3 describes the author's plan for future research. This chapter succeeds to properly outline the (proposed) steps and goals of proposer's research – only the issue of unclear approach to the evaluation(s) of both the detection method aimed at dictionary attacks against web services and application, and also of other extension to this basic detection method.

There are some minor issues in the proposal, like some statements not supported sufficiently with convincing arguments (e.g., end of p. 3 or p. 4) or too general to be true (e.g., end of p. 11), the definition of flow on p. 6 is somewhat unclear (e.g., are the flows that are not exported not really flows, are any common properties enough to call a sequence of packets a flow). However, these problems do not have a serious impact on my overall positive view of the proposal. Language of this proposal is acceptable, while not anywhere near perfect.

Proposal: Approve the proposal as suggested, with a minor warning that the issue of evaluation must be thoroughly considered, and also award the RNDr. degree.

Recommendation to the author: Make sure that when you speak of evaluation of a new method/system/approach that it is very clear how the evaluation will be undertaken, what the evaluation criteria will be (or how will you obtain them) and that the progress of your proposed effort can be objectively monitored and measured/evaluated.

Bílovice nad Svitavou, April 28, 2010

Václav Matyáš