Review of Ph.D. Thesis

Ph.D. candidate: Ing. Ivan Homoliak
Title: Intrusion Detection in Network Traffic

Reviewer: doc. Ing. Pavel Čeleda, Ph.D.
Department: Institute of Computer Science
Masaryk University
Botanická 68a
602 00 Brno

The submitted Ph.D. thesis "Intrusion Detection in Network Traffic" investigates selected topics in the network intrusion detection using supervised machine learning. The research questions addressed in the Ph.D. thesis are a state of the art problem in the network security and provide research challenges required for Ph.D. level work.

The presented work has several original contributions in the network security field i) network traffic features definition and extraction, ii) supervised machine learning classifiers, and iii) network layer based obfuscation techniques. The key contribution is in the network based buffer overflow detection. Evaluation of detection capabilities of these attacks and introducing obfuscation techniques to evade the detection. The thesis is reasonable organized and written. I would prefer more authors comments going beyond pure survey style of background and state of the art knowledge in Chapters 2 through 4.

The results of Ph.D. thesis were published (or are accepted for publication) on several conferences and in some journals. Ph.D. candidate significantly contributed to all papers. The Ph.D. candidate should focus more on selection of the venues (select conferences based on their ranking) and strong impact factor of the journals. This is currently weakest point of presented work and Ph.D. candidate should improve it in future.

Ph.D. candidate is an expert in intrusion detection. He was involved in research project AIPS (Automated Intrusion Prevention System) where he worked on some parts of his thesis. He further proved team work and leadership of students working on joint research topics and publishing results on conferences.

I have two defense questions.

1) In your research effort you have performed a lot of experiments and created datasets with buffer overflow attacks to evaluate detection classifiers. What about your plans to make it available to other researchers to be able to verify your work and achieved results?
2) You are mentioning in the thesis "the surprising imbalance between the extensive amount of research on machine learning-based anomaly detection pursued in the academic intrusion detection community, versus the lack of operational deployments of such systems." What about your

contribution to this issue? Will your work go beyond lab experiments and any chance on operational deployment?

I have an overall positive view on presented work and the Ph.D. candidate. My review is based on the submitted Ph.D. thesis, personal meeting with Ph.D. candidate and several questions I raised during reviewing Ph.D. thesis. I am able to state that Ph.D. candidate was able to work independently and creatively in the field of computer science. The Ph.D. thesis meets the standard requirements for the Ph.D. degree and I would like to recommend them for acceptance. I support the award of Ph.D. degree to Ivan Homoliak.

Brno, August 12, 2016 doc. Ing. Pavel Čeleda, Ph.D.