Review on the habilitation thesis "CYBER SITUATIONAL AWARENESS IN THE NETWORK SECURITY" by Dr. Pavol Sokol

Main results of the thesis

The main results of the thesis are devoted to various topics on all levels of cyber situational awareness. The author propose new methods and comparative analysis in the following recent topics: perception and comprehension levels CSA, and predictive analytics. According to this topics, the results are divided into two main parts.

The first chapter is devoted to the basic notions and approaches related to cyber situational awareness in general as well as on a special part of network security. The whole taxonomy including the levels are introduced and the subtopics related to the author's contributions are identified and detailed.

The second chapter is devoted to the perception and comprehension levels in three topics, namely deception systems, threat agent profiling and multi-stage attack detection. Firstly, the author examine security, privacy and legal aspects of honeypots, as a special example of deception systems. The legal issues of the collected data, especially related to the GDPR are discussed. The results are summarized in the paper [P1]. Honeypots and additional deception systems are also analyzed in several conference papers as well (see [29-35]) Secondly, the author focuses on threat agent profiling as part of the results on the comprehension level. The author uses the security alerts attributes, proposes new attributes, approaches and combine various methods to threat profiling agents. Examples for new methods and approaches are various clustering methodolgies and one or two-stage profiling analysis. The results are summarized in articles [P2], [P3] and also in conference papers [34], [45]. Finally, the author examines detection methods of multi-stage attacks, focusing on similarity-based approach. The author proposes the usage of aggregated version of the security alerts and a novel correlation algorithm based on that meta-alerts. The analysis of meta-alerts or hyper-alerts is also useful for analysis of the skill level of threat agents. The results are summarized in journal papers [P4], [P5].

In the third chapter, the author summarizes his results on projection level of situational awareness and predictive analysis methods. The comparative analysis of all predictive methods, namely attack projection, attack prediction and network security situation forecasting is the first main contribution of this part, see journal paper [P6]. Second, the author introduces and discusses a hybrid model for early-stage detection of cyber-attacks using Bayesian networks. The results are summarized in journal paper [P7] and conference paper [69]. Second, the author examines forecast of network security situation based on statistical and neural network methods. The author suggests to categorize the individual time series into three groups including preprocessing, methodology and analysis. Additionally, the analysis of the impact of loss function in neural networks is presented together with the comparison of neural networks and the statistical methods in NSSA forecasting. Several loss functions, neural networks and statistical methods are compared and analyzed. The results are summarized in journal papers [P8], [P9] and in conference papers [61], [81].

Evaluation

The dissertation is well written and contains several interesting new results. The quantity and the quality of the related publications is very impressive. The proposed methods contain new ideas and novel improvements of previous results as well. The proposed methods and ideas are presented clearly, the analysis of the novel models is correct. Most of the results was presented on prestigious international conferences and appeared in leading journals. The number of citations is high, suggesting that the papers contain significant contributions of the topics.

Summarizing the above, I recommend giving the docent title for the candidate.

August 2022

Péter Ligeti
Eötvös Loránd University
Faculty of Informatics
Budapest