Visual Analytics for Network Security and Critical Infrastructures

Karolína Burská, Radek Ošlejšek

Visual Analytics for Network Security and Critical Infrastructures

Karolína Burská and Radek Ošlejšek

Faculty of Informatics, Masaryk University, Brno, Czech Republic
burska@mail.muni.cz,oslejsek@fi.muni.cz

Abstract. A comprehensive analysis of cyber attacks is important for better understanding of their nature and their origin. Providing a sufficient insight into such a vast amount of diverse (and sometimes seemingly unrelated) data is a task that is suitable neither for humans nor for fully automated algorithms alone. Not only a combination of the two approaches but also a continuous reasoning process that is capable of generating a sufficient knowledge base is indispensable for a better understanding of the events. Our research is focused on designing new exploratory methods and interactive visualizations in the context of network security. The knowledge generation loop is important for its ability to help analysts to refine the nature of the processes that continuously occur and to offer them a better insight into the network security related events. In this paper, we formulate the research questions that relate to the proposed solution.

Keywords: Visual Analytics, Network security, Knowledge generation

1 Introduction

Although network security is strongly connected with technology (e.g., network infrastructure, cloud computing), the context is usually much broader and must be mediated by human interaction. While some of the known attack methods may be detectable rather easily, many attacks can be identified only with the participation of a human, by analysis. The analysts' goals are to identify, track, and understand these attacks. One of the viable approaches is to combine the human flexibility, creativity, and background knowledge with the enormous storage and processing capacities of todays computers to gain insight into complex problems and to understand causality. Especially, when involving large and complex data sets that require a high degree of interaction, the support of knowledge generation techniques is likely to prove as very beneficial.

In what follows, we formulate research questions that are related to the loop of exploratory visual analysis in the context of cyber security. Each question aims to describe a broader motivation and current state and then formulates approaches enabling us to tackle the goals in proposed PhD thesis.

2 Research Questions and Proposed Approaches

How to model cyber-security data and its semantics? Cyber security data has a strong heterogeneous nature. Data sets can be temporal, geospatial, multivariable, or graph-based, for instance. And also mixed together. Although there exist some formalizations that describe how various data types can be mapped to visual properties [8] in general, a clear taxonomy of data types used in cyber security domain is missing. However, a formal classification scheme is necessary if we want to build an adaptive data gathering and construct a knowledge base – two mandatory parts of any visual analysis loop.

In our research, we initially focus on the design of taxonomies for cyber security data and corresponding analytical processes. We plan to utilize formal OWL ontologies to provide semantically correct vocabulary enabling as to (semi)automatically construct adaptable data sets and derived knowledge models. Using existing taxonomies and approaches, e.g. those described in [6, 1, 13], we aim to unite the different perspectives and apply them in the visual analysis loop in the cyber security domain.

How to provide insight into cyber security processes via exploratory visualizations? Many works confirm that the involvement of the human factor in the process of data analysis may contribute to revealing new information in a significant way [5, 12]. One of the basic principles used in this field is the *visual analytics process* by Keim et al. [7], which is described as an approach that combines data analysis, visualization, and human factor, as well as the areas of cognition and perception. This approach follows the Shneiderman's visual information-seeking mantra: "Overview first, zoom and filter, then details-on-demand" [11]. By applying this mantra in the visual analysis domain, Sacha et al. [10] proposed an approach enabling the visual analytic theories to go beyond the inclusion of the human factor in the process, to the theory where human is a part of the loop [3].

Our approach to the cyber security knowledge management and its visual analysis would combine the Keim's and Sacha's approaches. Their models have to be significantly adapted since the cyber security domain requires a wide range of network-related manipulation techniques. Our model would consist of two parts. The first part would deal with the automated processes connected to data monitoring and knowledge management, while the second part would involve human interactions by means of exploratory visualizations. Unfortunately, there is no clear separation between the two parts since the whole model for exploratory visual analysis attempts to connect the benefits of both – humans are creative and able to find subtle connections between two seemingly unrelated events, but they miss the ability to deal with large data sets. On the contrary, computers offer large storage spaces and fast data processing, but they lack the human reasoning and the background knowledge of the problem domain. Therefore, finding a balanced solution based on the feasible technical background makes this goal challenging.

How to utilize exploratory visualizations for efficient protection of critical information infrastructures? Protection of critical information infrastructures is ensured by security experts. Their skills and the ability to react to incidents quickly and correctly are affected by two factors: a training and an online situation awareness. In general, decision making is viewed as consisting of an analyst's state of knowledge in a dynamically changing environment [4].

To facilitate a cyber protection training and to evaluate benefits of visualization techniques for situation awareness, we attempt to use KYPO Cyber Range [9], where various attacks and threats can be easily simulated. KYPO enables us to focus on linking the knowledge base with suitable visualizations and to evaluate their benefits. New approaches can be tested and evaluated by means of cyber defense exercises focused on improving skills of participants [2].

3 Conslusion

Acknowledgements. This research was supported by the Security Research Programme of the Czech Republic 2015-2020 (BV III/1 VS) granted by the Ministry of the Interior of the Czech Republic under No. VI20162019014 Simulation, detection, and mitigation of cyber threats endangering critical infrastructure.

References

1. Chi, E. H., A taxonomy of visualization techniques using the data state reference model, In: IEEE Symposium on Information Visualization 2000. (2000)
2. Čeleda, P., Čegan, J., Vykopal, J., Tovarňák, D., KYPO - a platform for cyber defence exercises. In: M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence. NATO Science and Technology Organization (2015)
3. Endert, A., et al., The human is the loop: new directions for visual analytics, Journal of Intelligent Information Systems **43** (3) (2014)
4. Endsley, M. R., Toward a theory of situation awareness in dynamic systems, Human Factors: The Journal of the Human Factors and Ergonomics Society **37** (1) (1995)
5. Fischer, F., Visual analytics for situational awareness in cyber security (2016)
6. Gao, J., et al., Ontology-based model of network and computer attacks for security assessment, Journal of Shanghai Jiaotong University (Science) **18** (5) (2013)
7. Keim, D.A., Mansmann, F., Stoffel, A., Ziegler, H., Visual analytics, Springer, (2009)
8. Kott, A., Wang, C., Erbacher, R.F., Cyber Defense and Situational Awareness. Springer, New York (2014)
9. Kouřil, D., et al., Cloud-based testbed for simulation of cyber attacks. In: IEEE Network Operations and Management Symposium (NOMS), pp. 16, May 2014
10. Sacha, D., et al., Knowledge Generation Model for Visual Analytics, IEEE Trans. on Visualization and Computer Graphics (Proceedings Visual Analytics Science and Technology) **20** (12) (2014)
11. Shneiderman, B., The eyes have it: a task by data type taxonomy for information visualizations In: Proceedings 1996 IEEE Symposium on Visual Languages (1996)
12. Sun, Wu, G., Y. et al., A survey of visual analytics techniques and applications: State-of-the-art research and future challenges, J. Comp. Sci. Tech. **28** (5) (2013)
13. Zareen S. et al., UCO: A Unified Cybersecurity Ontology, In: Proc. of the AAAI Workshop on Artificial Intelligence for Cyber Security (2016)