Visual Analytics

in Cyber Security

Karolína Burská, Tomáš Pitner, Radek Ošlejšek

MASARYKOVA UNIVERZITA

Introduction

The ability to use interactive visual interfaces and advanced analytical methods is essential to help the security experts explore causalities or suspicious behaviour, and to gain insight into the problem area. For this reason, many visualization are being developed for an environment for mitigation cyberattacks, called KYPO. 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.

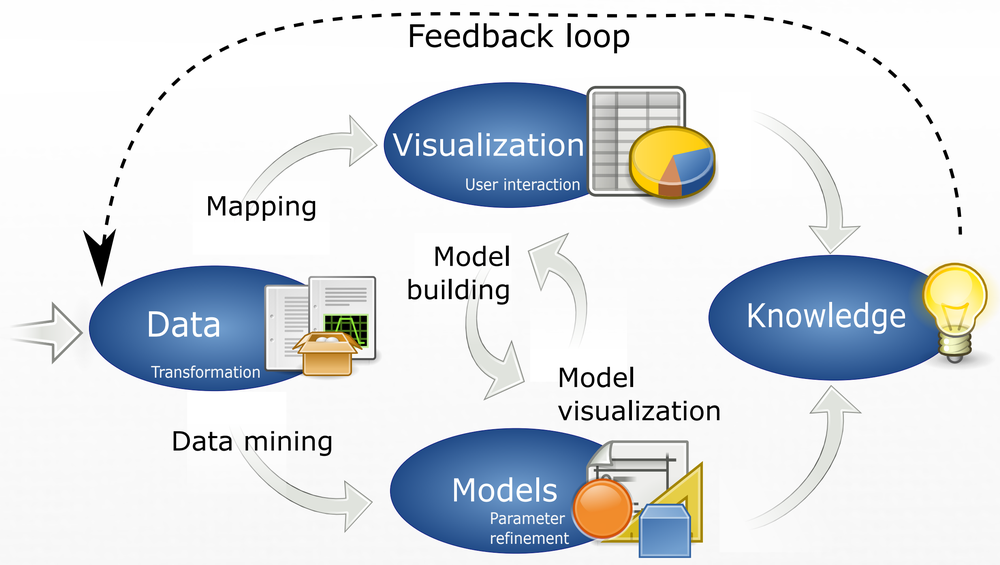

Figure 1: Knowledge generation loop by Keim et al.

The Goals

- Adjustment of some existing visualization techniques into a context of cyber security
- Design of security data (processes, attacks) taxonomies
- Creation of complex formal knowledge base in the form of ontologies
- Development of interactive tools for visual analysis

Methodology

The new visualizations will be developed through an extension of a model for knowledge generation (see Figure 1). The model will be adjusted to be applicable to the domain of cyber security and it will then help us to progressively refine the resulting visualizations.

The model will be based on a mantra per which a human should be a part of the loop for knowledge generation. To ensure the involvement of the human factor in the process we plan to use the KYPO testbed. Through the testbed we can focus on linking the knowledge with the proper visualization techniques.

References

- The kypo - cyber exercise & research platform. http://www.kypo.cz/
- D. A. Keim, J. Kohlhammer, G. Ellis, and F. Mansmann. *Mastering The Information Age - Solving Problems with Visual Analytics*. Eurographics, 2010.
- Endert, A., Hossain, M. S., Ramakrishnan, N., North, C. , Fiaux, P., Andrews, C., *The human is the loop: new directions for visual analytics*, Journal of Intelligent Information Systems (2014)

Masaryk University
Botanická 68a 602 00 Brno
Czech Republic

esf european social fund in the czech republic
EUROPEAN UNION
MINISTRY OF EDUCATION, YOUTH AND SPORTS
OP Education for Competitiveness
INVESTMENTS IN EDUCATION DEVELOPMENT

KYPO

lasaris