Exploring the role of experts' knowledge in visualizations for cyber security

Fabian Böhm* University of Regensburg
Noëlle Rakotondravony† University of Passau
Günther Pernul‡ University of Regensburg
Hans P. Reiser§ University of Passau

1 Introduction

Knowledge-assisted visualization is a concept in information visualization that incorporates the knowledge conversion processes into the design, implementation and the utilization of visualization tools. Four different knowledge conversion processes describe the exchange of knowledge between humans and machines [4, 8]:
Internalization encompasses the transformation of *explicit knowledge* (machine-readable and persisted in database [2]) into *tacit knowledge* (human knowledge, specific to each individual [2]) using a visual representation of the first one and making it accessible and understandable to the user. This process is implemented into any visual representation of data or information.
Externalization is the transfer of knowledge following the opposite direction of internalization. Common implementations let users access a pattern database or ontology used by automated analysis methods. By using the visual interface to formulate new patterns, users transfer their tacit knowledge to the machine, making it machine-readable and therefore, translating it into explicit knowledge.
Collaboration describes the process of combining the tacit knowledge of two or more humans. We extend the description and interpret collaboration as a process of combining the tacit knowledge using visual interfaces. Although collaboration can be done without visual interfaces by direct communication between humans, tools should provide functional support for this process.
Combination is very similar to collaboration as it describes the exchange of explicit knowledge between computers by including new explicit knowledge into an existing knowledge base. This process can work completely without visual interfaces.
We present a work in progress in which we study the implementation of the knowledge conversion processes in visualizations for cyber security. By doing so, we are able to explore the current role of experts' knowledge in the VizSec community. Drawing from our preliminary results, we identify shortcomings in the support of two knowledge conversion processes within current literature.

1.1 Motivation and objectives

In the domain of cyber security, the expert knowledge is very crucial and needed to interpret and make sense of automatically generated analysis results like machine learning models or anomaly alerts. Automated analysis methods often do not have the needed insight for those contextual decisions and therefore, security experts must be included in the decision process [5]. However, automated analysis methods are crucial to cope with the vast amount of raw data at hand. They express their insights using visual representations. However, those visualizations for cyber security also offer an appropriate solution to externalize the domain knowledge of security experts making it accessible for automated data analyses and other experts [8].

*e-mail: fabian.boehm@ur.de
†e-mail: nr@sec.uni-passau.de
‡e-mail: guenther.pernul@ur.de
§e-mail: hr@sec.uni-passau.de

Overall, our goal is to identify and understand the current state of knowledge-assisted visualization in the perspective of cyber security visualizations, through the analysis of ten years of VizSec literature. This analysis serves as a starting point for identifying design implications that allow to tightly integrate security experts' knowledge into visualization for cyber security.

1.2 Relevance to the community

In the information visualization area, Best et al. [1] and Federico et al. [4], among others, identified the benefits of considering knowledge management and conversion in the development of effective visualization systems.
VizSec is a field at the intersection of several related or parent fields such as information visualization, human-computer interaction, cyber security. Researchers in VizSec employ visualization and human-computer interaction to better address security challenges [7].
The necessity to incorporate results and ideas from related research areas in cyber security visualization comes from the diversity of the field but also from the communities identifying such need. To the best of our knowledge, no work has been done yet to specifically analyze the role of expert knowledge in terms of support of knowledge conversion processes in for visualizations for cyber security.

2 Analysis methodology

Since combination in general is done more efficiently without visual interfaces, and as any visual representation of data or information can be seen to be an internalization of explicit knowledge, we focus our work on the analysis of externalization and collaboration concepts.
To explore the role of experts' knowledge, we need a methodology for identifying the relevant knowledge conversion processes in the academic papers proposing new visualization tools. As only very little work is available on this topic, we define our own analysis methodology. Our approach is separated into two main steps.

2.1 Paper selection

The literature from VizSec includes papers introducing new tools, systems, or techniques but also other papers that describe design methodologies as well as surveys and position papers.
We select only papers that are proposing new visualization tools. Afterwards, we narrow our focus on interactive systems because from our point of view interaction is the only possible channel through which the two relevant knowledge conversions (externalization and collaboration) can happen.

2.2 Paper analysis

The *paper analysis* is intended to find the knowledge conversion processes within the selected papers. We identify the externalization processes by checking whether the visualization tools includes an underlying automated analysis according to the definition in [4] and allows direct or indirect interaction with it.
Direct interactions, in which the user interacts with an appropriate interface and explicitly externalize her tacit knowledge (e.g. using sliders to manipulate the parameters of a machine learning algorithm), allow to identify an *explicit externalization* [4]. Indirect interactions, in which the user's interactions with the visual metaphors (e.g. dragging nodes to a different location) are used to

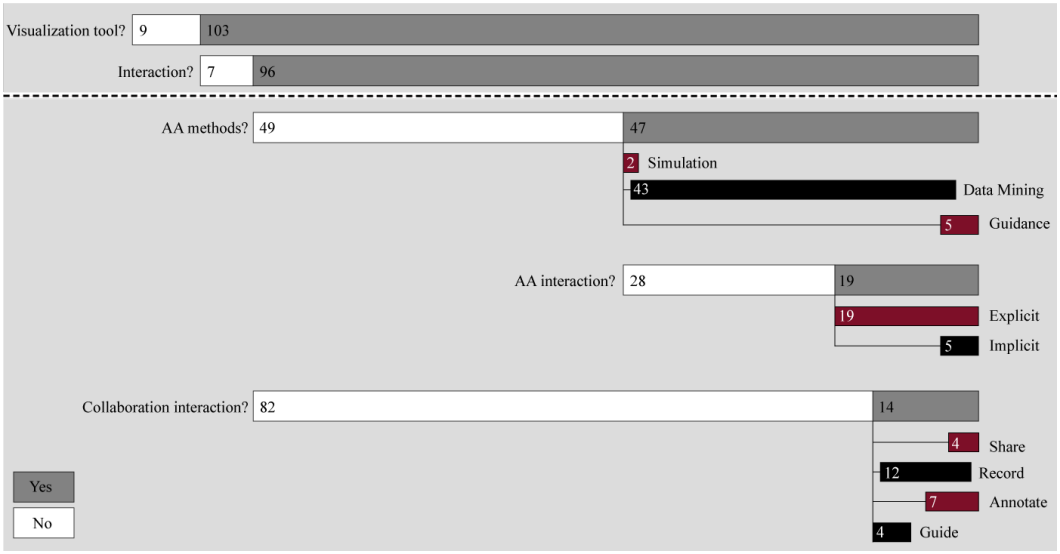

Figure 1: Statistical overview of the analysis results

automatically infer the tacit knowledge from the users sense-making process, allow to identify *implicit externalization* [3].
To identify the collaboration processes, we verify whether a tool supports one or more of the Heer and Shneiderman's *Process & Provenance*-interactions [6]. Any interaction falling into this category of their taxonomy allows to communicate a user's domain knowledge and sense-making process through the system to another user which is an indicator for functional support of collaboration.

3 Current Status

The detailed results of our analysis are publicly available at `http://bit.ly/2LgrG3p`.

3.1 Analysis results

Figure 1 shows the statistical overview of our analysis results with the number of publications introducing new tools (103 out of a total of 112), interactive tools (96 out of 103), tools that allow for externalization (19 out of the 47 with automated analysis), and interactive tools with functional support for collaboration (14 out of 96).
The results indicate that explicit externalization is more practiced than implicit externalization. We can see two main reasons for this. First of all, explicit externalization is more straightforward to implement. Additionally, implicit externalization requires an additional layer in the tool to analyze the semantics of the interactions.
Furthermore, also very few tools (14) provide support for the collaboration between domain experts using one or more of the collaboration forms: record, annotate, share, and guide.

3.2 Future work

We now have an overview and a clear understanding of the current role of experts' knowledge in the VizSec community. Our future research path consists of employing the current analysis results for defining design guidelines that leverage the concepts of knowledge-assisted visualization in order to improve the integration of human and machines in cyber security visualizations.
Additionally, it is necessary to further analyze the benefits of involving functional support for collaborative features in existing visualization tools for cyber security.

4 Conclusion

Our analysis has shown that only few tools allow users to interact with the underlying automated analysis. Most of them follow the process for explicit externalization which makes users to leave the visual metaphor. We also identified a surprising gap for the functional support of collaboration in cyber security visualization tools. The integration of domain experts and automated analyses is a major future challenge for cyber security visualization. For advancing our study towards establishing design guidelines for including knowledge-assisted visualization concepts, the feedback of and discussion with experts in the field would be highly beneficial.

Acknowledgments

This research was supported by the Federal Ministry of Education and Research, Germany, as part of the BMBF DINGfest project (https://dingfest.ur.de), and by the Deutsche Forschungsgemeinschaft, as part of the ARADIA project.

References

[1] D. M. Best, A. Endert, and D. Kidwell. 7 key challenges for visualization in cyber network defense. In *Proceedings of the Eleventh Workshop on Visualization for Cyber Security*, VizSec '14, pp. 33–40. ACM, New York, NY, USA, 2014.
[2] C. Chen. Top 10 unsolved information visualization problems. *IEEE Computer Graphics And Applications*, 25(4), 2005.
[3] A. Endert, P. Fiaux, and C. North. Semantic interaction for visual text analytics. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 473–482. ACM, 2012.
[4] P. Federico, M. Wagner, A. Rind, A. Amor-Amoròs, S. Miksch, and W. Aigner. The role of explicit knowledge: A conceptual model of knowledge-assisted visual analytics. In *Proc. 2017 IEEE Conference on Visual Analytics Science and Technology (VAST)*. IEEE, 2017.
[5] C. Gates and S. Engle. Reflecting on visualization for cyber security. In *IEEE International Conference on Intelligence and Security Informatics (ISI), 2013*, pp. 275–277. IEEE, Piscataway, NJ, 2013.
[6] J. Heer and B. Shneiderman. Interactive dynamics for visual analysis. *Queue*, 10(2):30, 2012.
[7] P. Ren. Ensuring the continuing success of vizsec. In *Proceedings of the 3rd International Workshop on Visualization for computer security*. ACM, New York, NY, 2006.
[8] X. Wang, D. H. Jeong, W. Dou, S.-W. Lee, W. Ribarsky, and R. Chang. Defining and applying knowledge conversion processes to a visual analytics system. *Computers & Graphics*, 33(5), 2009.