V

Visual Security Analytics

Fabian Böhm
Chair of Information Systems, University of Regensburg, Regensburg, Germany

Synonyms

Security visualization

Definition

Despite the application of increasingly advanced methods and technologies to automate tasks within cyber security, human domain knowledge remains indispensable. Especially monitoring a system's security posture as well as detecting and analyzing cyber threats requires involvement of security experts. However, the large amount of data relevant for these tasks poses a major impediment for any kind of manual analyses. It is therefore necessary, to enable security experts to efficiently deal with large amounts of data. Visual Security Analytics (VSA) aims to achieve this through generating interactive visual representations of log data or any other data relevant for monitoring, ensuring, and preserving cyber security and covering different ways of analyzing security data using visual approaches (Marty 2009). It is a combination of automated and visual analysis aiming for a "best-of-both" worlds approach. Thus, VSA is a highly interdisciplinary field covering information security, security analytics, information visualization, and human-computer interaction among several others.

Background

Combating the wide variety of threats within cybersecurity involves the necessity to deal with large amounts of data from heterogenous sources. Modern developments such as the IoT and the resulting interconnectedness of contemporary company's architectures additionally increase their attack surface. This leads to a skyrocketing amount of relevant data as well as a high complexity of the task to secure them. Specially to deal with the data, it is inevitable that the application of algorithmic methods and technologies is necessary. Many of these automated approaches have matured throughout the last two decades and are a huge relief to manual analysis approaches (Marty 2009). Although they are very effective and efficient in combating familiar threats or at least attacks that follow previously known schemes, they fall short in detecting targeted and tailored threats. These often comprise of several benign activities that only add up to a malicious incident when analyzed together. Especially for these types of threats, it is highly relevant to enable human domain experts to identify and analyze them. Their domain knowledge about the company, its

S. Jajodia et al. (eds.), *Encyclopedia of Cryptography, Security and Privacy*,
https://doi.org/10.1007/978-3-642-27739-9_1674-1

architecture, and other particularities is crucial and cannot be automated. However, the amount of data relevant for analyses is too much for humans to handle (Goodall 2008).

Since more than 15 years, the field of Visual Analytics (VA) offers a pathway for a solution to this and similar mismatches (Thomas and Cook 2005). It aims at a "best-of-both-worlds" approach with automated data processing and analysis combined with visual representations of the data to enable manual analyses as well. The application of VA approaches in the context of security (i.e., VSA) combines human pattern recognition abilities as well as domain knowledge with the data-processing powers of computers. VSA has been playing a major role within VA since its early days (Keim et al. 2010). It enables security experts but also experts from other domains (e.g., IoT) to analyze security data using visual approaches. Visual representations of data allow domain experts to discover preemptive and actionable security measures to combat threats and increase information security (Jacobs and Rudis 2014). A crucial part of VA and therefore also VSA is a feedback loop which enables experts to adapt and adjust any automated analysis (and its parameters) or any step that is part of the process (Keim et al. 2010).

Theory and Applications

Theory of VSA is mostly based on the theoretic research in the fields of information visualization, visual analytics, as well as human-computer interaction. The application of this theoretical research to the context of information and cyber security is the core of visual security analytics. Thus, the relevant background is naturally highly interdisciplinary. It first covers understanding the pattern seeking and visual capabilities of the human brain (Ware 2012), the involvement of users in the design process of VSA solutions (Meyer et al. 2015), and a clear understanding of the users' tasks and activities (Kirk 2019). All of these aspects are crucial to develop an appropriate visual representation for the intended users. Additionally, literature examines a plethora of ways to efficiently map multidimensional security information into interactive, visual representations (Hall et al. 2015). This, application-driven research is the core of VSA. However, there are several smaller streams of research within respective literature such as the development of knowledge-generation models (describing how users derive knowledge from visual representations (Sacha et al. 2014)) or the design of knowledge-assisted visualizations which focus mainly on the exchange of knowledge between humans and machines (Federico et al. 2017).

Open Problems and Future Directions

Current widely discussed open problems and emerging future directions within security visualization are mainly the following:

1. The most pressing problem is a so-called dichotomy in the development of VSA solutions (Marty 2009). They are either designed by security experts without the necessary visualization or by visualization experts without the proper security domain knowledge. It is necessary to bring both security and visualization experts together to build effective VSA solutions.
2. Identification of user tasks: There are several taxonomies identifying and defining the tasks and activities of domain experts (Brehmer and Munzner 2013). Understanding these is crucial for the design of appropriate VA solutions supporting security experts in the best possible way. Existing taxonomies are mostly too high-level or too general to be completely applicable in the context of information security.
3. The appropriate evaluation of interactive visual representations has been an issue within information visualization ever since.
4. A raising topic within VA and VSA is the one of Explainable AI (XAI). Visual approaches can be used to enable domain experts to understand and reproduce the decision made by machine learning and artificial intelligence solutions. This effort aims to open black boxes of ML and AI allowing humans to debug,

adjust, and fine-tune the underlying models resulting in possibly better and more accurate analysis results. As ML and AI are also highly relevant in the context of information security, this poses an interesting future direction for VSA.

References

Brehmer M, Munzner T (2013) A multi-level typology of abstract visualization tasks. IEEE Trans Vis Comput Graph 19(12):2376–2385

Federico P, Wagner M, Rind A, Amor-Amorós A, Miksch S, Aigner W (2017) The role of explicit knowledge: a conceptual model of knowledge-assisted visual analytics. In: Proceedings of the IEEE conference on visual analytics science and technology (VAST), Phoenix, pp 92–103

Goodall JR (2008) Introduction to visualization for computer security. In: VizSEC 2007, Mathematics and visualization, Springer, Berlin, Heidelberg, pp 1–17

Hall P, Heath C, Coles-Kemp L (2015) Critical visualization: a case for rethinking how we visualize risk and security. J Cyber Secur 1(1):93–108

Jacobs J, Rudis B (2014) Data-driven security analysis, visualization, and dashboards. John Wiley & Sons, Hoboken, New Jersey

Keim D, Kohlhammer J, Ellis G, Mansmann F (2010) Mastering the information age – solving problems with visual analytics. Eurographics, Geneve

Kirk A (2019) Data visualisation. A handbook for data driven design, 2nd edn. Sage, London

Marty R (2009) Applied security visualization. Addison Wesley, Boston, Massachusetts

Meyer M, Sedlmair M, Quinan P, Munzner T (2015) The nested blocks and guidelines model. Inf Vis 14(3): 234–249

Sacha D, Stoffel A, Stoffel F, Kwon B, Ellis G, Keim D (2014) Knowledge generation model for visual analytics. IEEE Trans Vis Comput Graph 20(12):1604–1613

Thomas J, Cook K (2005) Illuminating the path. The research and development agenda for visual analytics. IEEE Computer Society Press, Los Alamitos, California

Ware C (2012) Information visualization, 3rd edn. Morgan Kaufmann, Waltham, Massachusetts