Effective Visual Analysis on Information Security

Baijian Yang
Department of Computer & Information Technology
College of Technology,
Purdue University
byang@purdue.edu

Yingjie Chen
Department of Computer Graphics Technology
College of Technology,
Purdue University
victorchen@purdue.edu

Keywords
Visual Analytics, Information Security, Cyber Security Visualization.

1. INTRODUCTION

Many works have been done applying visual analytics in the field of information security. Since the first visualization workshop for the cyber security [1], researchers have explored many possible visualization methods [2]. However, to the best of authors' knowledge, no mature visual analytic tools have been deployed by the IT industry for security protection. Questions remain to be answered by the researchers are, while apply visual analytics (VA) to solve issues in information security, 1) what are the strengths of VA; 2) what are the limitations of VA; 3) what are the challenges of this strategy; 4) and most importantly how do we effectively applying VA methods in information security. Gates and Engle, along with many other researchers, tried to answer similar questions from different perspectives [3].

So what are the strengths of applying VA in information security? To answer this question we need to examine what visual analytics can offer yet existing security techniques are much harder to achieve. In an enterprise environment, network is typically secured by implementing firewall, IDS, or IPS at the perimeter. Servers and workstations are managed through security policies and antivirus software. Security logs are generated from firewalls, servers, and client computers, to help professionals figure out what had happened. Security alerts can also be configured when the status of the system is significantly different than the baseline behaviors. All existing techniques assume security attacks can be described or identified by certain signatures or patterns, and systems can be guarded by implementing a set of well-defined rules. This is certainly not true because attack patterns can be dynamically changing and attacks have also become more and more complicated. Without any additional techniques, current information security practice works well enough on known threats and attacks but often not so effectively on detecting new or complicated threats. Therefore, the core benefit of applying VA in information security is to help security professionals to discover possible new threats or attacks by creatively presenting the system information through figures and user interactions. This is particularly helpful when the data in question is huge and data mining techniques might be resource intensive and time consuming. Additionally, VA may also help security professionals to quickly figure out who started attacks, how the attacks evolve, and etc.

The limitations of VA are also straightforward. First of all, the audiences of VA are human beings. In information security, it meant to help security professionals understand the system better and quicker by reading the graphs. As such, you cannot automate the process: it always requires the involvement of human beings. Secondly, to use VA effectively, there is hardly one size fits all: so the graphs need to be designed case by case to fulfill the business needs. Last but not least, unlike techniques such as IDS or IPS where countermeasures can be defined to protect the system, VA can only help you discover the problems. Further analyses and additional actions may be needed to actually solve the problems.

There are several additional challenges in information security. The biggest challenge is data. Security related data may be stored through many different devices, using different formats, and with different time stamps. When multiple security logs present, which one should you use? How do you correlate data to tell the whole story? And how do you normalize data such that users' privacy can be protected? And more interestingly, what if some of the security log is not available? Another challenge is the design of overview. In VA, the very first step is usually providing an overview of the system. In the age of cloud computing, a small percent of security related incidents are buried in the huge amount of normal traffic. Therefore, providing a meaningful summary of the system such that potential unknown attacks can be revealed in the overview remains very challenging. As cyber-attacks getting more and more complicated, it also demands researchers to have in-depth knowledge of security and be able to adopt appropriate visualization techniques to interpret complex events.

2. OUR APPROACH

It is our beliefs that the following principles should be followed to effectively promote VA in information security.

2.1 Understand the targeted system.

In each project, researchers and professionals need to first conduct threat and risk analyses. The core assets of information can be identified and data protection plan can be prioritized. Then best data sources can be determined. This is very different from many current researches where researchers try to figure out how to visualize a given set of data without a deep understanding of the system.

2.2 Build your team.

Securing information in an enterprise system can be fairly complex. It requires researchers and practitioners with various skills to collaborate. A perfect team needs to have experts from information security, data mining, and VA. Security professionals can identify the best data sources; provide insights into different data; and be able to relate security incidents to security logs. Data

VizSec 2013, Oct.14, 2013, Atlanta, GA, USA

mining experts will be able to help determine what is normal and what is abnormal. VA experts will gather information from the security experts and data mining professionals to design a graphic user interface to best capture possible incidents. It worth pointing out that it might be difficulty to visualize complex attacks if we solely rely on the raw data. Instead, processed data might be a better source to present the system status much more effectively.

2.3 Know your audience.

Since the end product is meant to be designed for the security professionals. Researchers need to communicate with the users in the VA design and UI design. Ideally, what we would like to provide to the security professionals is not just some optimized graphic interfaces that tied to a fixed set of data; but also a framework that enable the security professionals to select different data combinations and different ways of visual presentations.

2.4 Know the operations/processes.

It is also critical to understand what the data operations and the processes are. A baseline needs to be established and re-evaluated periodically to understand what is 'normal' and what is abnormal. Also realize that from the viewpoint of information security, the entire subnets might be questionable if when one host is victimized. And even worse, when the firewall or the routers at the security boundary is attacked, then the entire system is in jeopardy.

2.5 Get in the healthy cycle.

Like the life cycle of software engineering, VA tools for information security need to be revisited and revised on a regular base to better characterize the system visually. Furthermore, threats and risks should be regularly revaluated, data sources and data mining techniques need to be re-examined; better visualization techniques and UI needs to be amplified or enhanced.

3. CONCLUSION

Here we present our thoughts of how to improve the application of visualization and VA on information security. In recent years (including this year 2013), the VAST challenges [4][5] have provided benchmark datasets to stimulate researchers to create new ideas and evaluate their VA systems. From those awarded entries like [3] and [6], we can see that a successful system has to integrate multiple visualizations together to let the user see the data from different perspectives. Also, with the help of network security experts, the visualization could be much simpler and yet more effective [7]. Building a VA system for cyber security is really a comprehensive project that demands a team of professionals from different areas and requires lifecycle management for a healthy development.

4. ACKNOWLEDGMENTS

Our sincere thanks to the Research Hub of the College of Technology at Purdue University.

5. REFERENCES

[1] VizSec, "Visualization for cyber security (VizSec)." [Online]. Available: http://www.vizsec.org/. [Accessed: 08-Jul-2013].

[2] H. Shiravi, A. Shiravi, and A. A. Ghorbani, "A survey of visualization systems for network security," *Vis. Comput. Graph. Ieee Trans.*, vol. 18, no. 8, pp. 1313–1329, 2012.

[3] C. Gates and S. Engle, "Reflecting on Visualization for Cyber Security," in *Evaluating Security Visualizations in Supporting Analytical Reasoning & Decision Making in Cybersecurity*, Seattle, WA, 2013.

[4] G. Grinstein, K. A. Cook, P. Havig, K. Liggett, B. Nebesh, M. Whiting, K. Whitley, and S. Konecni, "VAST 2011 Challenge: Cyber Security and Epidemic," presented at the IEEE Symposium on Visual Analytics Science and Technology, Providence, RI, 2011, pp. 299–301.

[5] K. A. Cook, G. Grinstein, M. Whiting, M. Cooper, M. Havig, K. Liggett, B. Nebesh, and C. L. Paul, "VAST Challenge 2012: Visual Analytics for Big Data," in *IEEE Conference on Visual Analytics Science and Technology*, Seattle, WA, 2012, pp. 151–155.

[6] V. Y. Chen, A. M. Razip, S. Ko, Z. C. Qian, and D. S. Ebert, "Multi-aspect Visual Analytics on Large-scale High-dimensional Cyber Security Data," *Inf. Vis.*, no. Special Issue on VAST challenges, 2013.

[7] Choudury, S., Kodagoda, N., Nguyen, P., Rooney, C., Attfield, S., Xu, K., Zheng, Y., Wong, B.L.W., Chen, R., Mapp, G., Slabbert, L., Aiash, M., and Lasebae, A., "M-Sieve: A Visualisation Tool for Supporting Network Security Analysts. Vast 2012 MC1 Award: 'Subject Matter Expert's Award'," presented at the IEEE Conference on Visual Analytics Science and Technology, Seattle, WA, 2012, pp. 165–166.