

Exploration of User Centered and System Based Approaches to Cyber Situation Awareness

Margaret Varga^{*†} Carsten Winkelholz[‡] and Susan Traeber-Burdin[‡]

^{*}Seetru Ltd.,
[†]University of Oxford

[‡]Fraunhofer, FKIE

[‡]Fraunhofer, FKIE

ABSTRACT

The North Atlantic Treaty Organization (NATO) Research Task Group on exploratory visual analytics works to promote the research and deployment of visual analytics and visualization techniques among NATO member and partner nations. This poster reports a study conducted by the group in exploring User Centered and System Based approaches to cyber situation awareness.

Keywords: Visual analytics, visualization, cyber security, situation awareness, user centered design, ecological interface design

Index Terms: H.2.8.h Interactive data exploration and discovery, I.6.9.a Applications, I.6.9.c Information visualization

1 INTRODUCTION

We are increasingly dependent on the ever expanding Internet with its increasing complexities and interdependencies. While on the one hand its immensely powerful infrastructure underpins society, on the other hand its vulnerabilities to cyber-attack pose immense risks. Cyber situation awareness is vital in support of making informed decisions for maintaining a safe and secure environment [1, 2].

2 SITUATION AWARENESS

Endsley's work on situation awareness (SA) provides an established definition of SA, in particular for dynamic environments:

"Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future." [3].

Endsley considered that there are three stages of situation awareness, namely: (1) perception, (2) comprehension and (3) projection [3]. This links cognitive psychology with human factors in the explanation of making sense in complex situations, such as the cyber domain.

3 HUMAN INTERFACE DESIGN APPROACHES

Different approaches to human machine interface design can be developed and applied to the different operational and users' needs. This poster reports a study in exploring the User Centered and System Based approaches to cyber situation awareness.

4 DATA

The VAST 2013 Mini Challenge 3 (MC3) data was used for this study [4]. It is concerned with the Big Marketing Corporation that was targeted by external attackers over a two week period. The

Corp. has three different branches with one administrator, each branch has about 400 employees and its own servers. There are three data sets: Netflow, Big Brother's Health & Status data, and the Intrusion Prevention System (IPS) logs (second week only).

5 USER CENTERED APPROACH

Visual Analytics offers a powerful data driven methodology, when applied in a user centered manner (user centered visual analytics) it focuses on the users' and tasks' needs, the users' skills and their mental models, and it can operate at a rate that is resonant with the speed of human thought [5, 7].

Fig. 1 shows an integrated interactive user centered dashboard for the netflow data, developed in this study. The core element is the Sankey on the left, which is used to show the inbound (brown) and outbound (blue) traffic where internal hosts (light grey) are on the left and external hosts (dark grey) are on the right: width represents the volume of the traffic. Using spatial coding of the internal and external attributes of the endpoints of connections instead of source and destination makes it easier for the user to interpret the patterns emerging in the Sankey. This figure shows scanning activities from two external hosts and the DDoS attack from eight infected Corporation own hosts, onto an external server (10.1.0.100). The column chart shows the temporal outbound and inbound traffic in the opposite directions. The donut rings show the inbound and outbound traffic together and separately and their associated ports. This user centered dashboard shows clearly the temporal network situation and awareness of the threats being faced. The users can interactively explore the data easily to gain awareness of the situation.

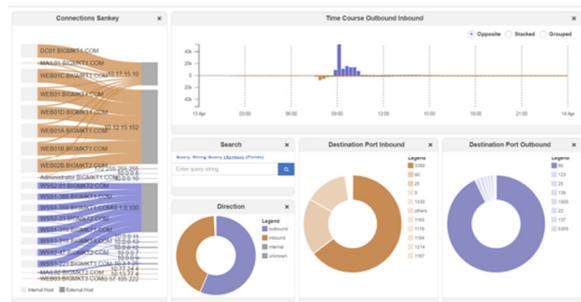


Figure 1: User Centered Netflow Analysis

Fig. 2 shows a large volume of data was exfiltrated from the Administrator to the IP address 10.7.5.5. This can be easily seen by displaying the maximum number of bytes per flow (top right column chart). The peak at 12:30 is very salient, and Sankey shows that this transfer originates from the workstation of the compromised administrator and the destination port is 20 (FTP).

Fig. 1 and Fig. 2 illustrate the effectiveness of the user-centric approach that has been developed for detecting and discovering threats. The numerous threat events in the challenge were detected by the users using the dashboard. The resulting visualizations provide detailed information on the network

[†] margaret.varga@oncology.ox.ac.uk

[‡] [carsten.winkelholz, susan.traeber-burdin@fkie.fraunhofer.de](mailto:carsten.winkelholz,susan.traeber-burdin@fkie.fraunhofer.de)

components, such as IPs, ports, protocol, timestamps etc., and performance of particular aspects of interest. However, it does not provide information on the operational status of the network, i.e. the Big Picture.

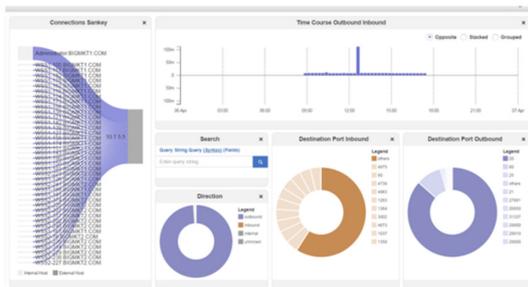


Figure 2: Exfiltration of large files

6 ECOLOGICAL INTERFACE DESIGN (EID)

An EID is a system based interface design approach which aims to make complex relationships in the system intuitively clear to the user. It is based on the idea that by understanding how a system works, users can manage and diagnose problems in a system more effectively and efficiently. EID is composed of two concepts, namely the Abstraction Hierarchy (AH) and the Skills, Rules, Knowledge (SRK) framework [6, 8].

7 NETWORK TOPOLOGICAL INFORMATION

There are two types of network topology namely physical and logical. Physical topology refers to the physical layout of network devices while the logical topology refers to the manner that the data moves around the network.

Fig. 3 shows the logical network topology EID developed in this study based on the very basic MC3 architectural information. It shows the servers and their relationships to the workstations: each workstation icon in the display represents ten workstations, their associated IP addresses are also shown, traffic lights are used to represent the status, i.e. green for good, yellow for warning and red for problem – based on the Health & Safety and IPS data. Schematics such as this showing dynamic operational information could be used to identify vulnerabilities. It shows that the administrator is in a critical condition, which will propagate through the network. However, information on the reason / cause of the situation is not available, i.e. exfiltration of data, see Fig. 2. Fig. 4 shows that eight workstations are “infected” in the 3 different branches. The cause of this critical situation is not, known, though it is shown clearly in the user centered representation in Fig. 1. It can thus be seen that the EID approach provides salient information about the network situation, i.e. the Big Picture, but not the detailed information of the cause (why) of the situation, c.f. the user centered display.

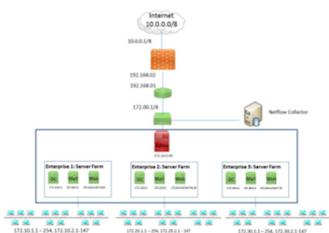


Figure 3: Administrator in critical situation

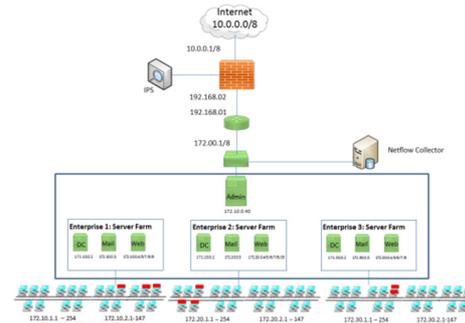


Figure 4: Infected workstations

8 CONCLUSIONS

Informal evaluation was carried out of the user-centric and the EID approaches with four users. It was found that the user-centric approach provides an effective means of analysing, detecting, discovering and identifying MC3 events in the challenge. The resulting visualizations provide detailed information on the network components and performance of particular aspects of interest, c.f. the network Big Picture. The ecological representation of the logical network topology, on the other hand, shows the status, relationships and dependencies between servers, firewalls, workstations, etc. It provides a visualization that guides the users in their understanding of how the network functions and its operational status. The patterns of the ‘normal situation’ can easily be familiarized, and thus any changes from the normal patterns can be detected readily. In the EID concept, the Analysts see the operational aspects of the network, i.e. the Big Picture, but not the reasons for malfunctions, e.g. DDoS, exfiltration, etc.

The user centered approach provides threat information which manifests into the operational status of the whole network, i.e. the Big Picture. Equally, the EID provides the Big Picture which leads to the investigation of the cause of threats/malfunctions, i.e. information from the user centered display. The two approaches complement each other in providing situation awareness of the network in different aspects and against different operational needs. Preliminary evaluation of the two approaches with security personnel was positive and further exploration is underway such as the switching between the two displays.

REFERENCES

- [1] Cyber Defense and Situational Awareness, Edited by Kott, A., Wang, C. And Erbacher, R. F., Springer, January 2015.
- [2] A. D’Amico, Visual Analytics for Cyber Defense Decision-Making, Washington, USA., VAC 2011.
- [3] M. R. Endsley, Toward a theory of situation awareness in dynamic systems. Human Factors, 37(1) : 32-64, March, 1995.
- [4] <http://www.vacommunity.org/vastchallenge2013>
- [5] Mastering the Information Age Solving Problems with Visual Analytics, Edited by Keim, D., Kohlhammer, Ellis, G., and Mansmann, F. 2010, ISBN 978-3-905673-77-7, <http://diglib.eg.org>
- [6] J. Rasmussen, Skills, rules, knowledge; signals, signs, and symbols, and other distinctions in human performance models. IEEE Transactions on Systems, Man and Cybernetics, 13, 257-266, 1983.
- [7] J. J. Thomas, and K. A. Cook, (Eds.), Illuminating the Path: The Research and Development Agenda for Visual Analytics, National Visualization and Analytics Center, 2005.
- [8] K. Vicente and J. Rasmussen, Ecological Interface Design: Theoretical foundations, IEEE Transactions on Systems, Man and Cybernetics 22, PP 1 – 18, 1992.