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

Margaret Varga[1,2], Carsten Winkelholz[3] and Susan Träber-Burdin[3]

[1]Seetru Ltd., [2]University of Oxford and [3]Fraunhofer, FKIE

ABSTRACT

This paper reports a study, conducted by the North Atlantic Treaty Organization (NATO) Research Task Group on Exploratory Visual Analytics, exploring user centered interface design and system based design approaches to cyber situation awareness. The former provides detailed information on the performance of network components while the latter provides information of the operational aspects of the network performance, i.e. the big picture. The paper shows that the two approaches complement each other in providing the necessary awareness of different aspects of the network situation.

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 ever more dependent upon the perpetually expanding Internet with its growing complexities and inter-dependencies. Although we benefit from it, we are vulnerable to cyber-attack. The goal for an interface design is to enhance the cyber analysts' situation awareness to provide vital support for informed decision making to safeguard our networks [1, 2 and 3].

This paper reports a study developing, exploring and comparing different human machine interface design approaches applicable to addressing the analysis and presentation of information for cyber situation awareness.

2 HUMAN MACHINE INTERFACE DESIGN APPROACHES

Different approaches to human machine interface design can be developed and applied to address different operational and users' needs, for example:

- user centered design (UCD) approaches on one hand, and
- system based approaches, such as the Ecological Interface Design (EID), on the other hand.

These two approaches are fundamentally different in their manner of providing situation awareness. The UCD approach focusses on the users' and the tasks' needs, the users' skills, and limitations, as well as their mental models [4]. Whereas, an EID focuses on the system [8 and 10]: the objective being to show the complex relationships in the system to the user in a readily accessible and informative manner.

3 DATA

A common dataset is required in order to explore and compare the two different approaches. The simulated VAST 2013 Mini Challenge 3 (MC3) data was used in this study [6]. It is concerned with the fictitious Big Marketing Corporation which has three different branches, each with approximately 400 employees and each branch having its own web servers. The scenario was that the Big Marketing Corporation was targeted by external attackers.

• Margaret Varga is with Seetru Ltd. and Oxford University, Email: margaret.varga@zoo.ox.ac.uk

• Carsten Winkelholz and Susan Träber-Burdin are with FKIE, Franhoufer, Email: carsten.winkelholz@fkie.fraunhofer.de and susan.traeber-burdin@fkie.fraunhofer.de

4 USER CENTERED DESIGN (UCD) APPROACH

Visual Analytics exploits interactive visualization and human cognitive abilities [7 and 9]. It offers a powerful data driven methodology when applied in a user centered manner (user centered visual analytics). The UCD approach is structured directly according to the perceived users' needs, the task(s) in hand, the users' skills and their mental models; it can operate at a speed that is resonant with the speed of human thought [4 and 5].

Figure 1 shows a user centered dashboard, developed as part of this study, in which the sub-displays are all synchronised and integrated together. The Sankey diagram shows ten external hosts launched a DDoS attack at the WEB03.BIGMKT.COM (172.30.0.4) on 2nd April. The destination port 80 was the targeted port. The time and time span of the event can be seen; in addition, details of the log information (bottom right) can be accessed and examined to conduct further analysis of the attack. The bi-directional temporal colour-coded column chart shows the inbound and outbound traffic, the time and duration of each occurrence. The donut rings show the inbound and outbound traffic together and separately, and their associated ports. This user centered dashboard shows the network situation and provides awareness of the threats being faced, such as a DDoS attack. The analysts comprehend the situation through their perception of the display thus decide their cause of action.

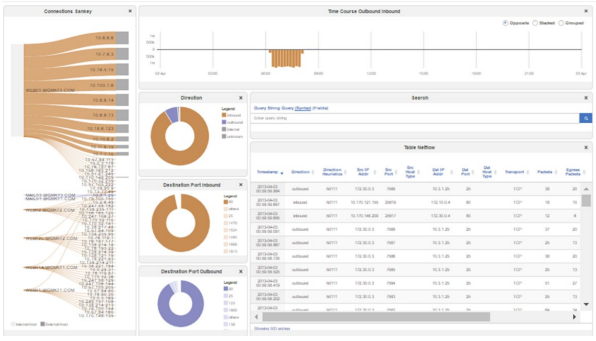

Figure 1: DDoS attack

Although effective and informative about the network situation and events in detail, this approach does not naturally provide awareness of the performance of the network as a whole, i.e. the big picture: the EID approach, explored below, provides this.

5 ECOLOGICAL INTERFACE DESIGN (EID) APPROACH

In contrast to the UCD approach, the EID approach focuses

on the structure and operation of the system [10]. It is based on the idea that, by understanding how a system works and is operating, users can manage and diagnose problems in a system 'more' effectively and efficiently. EID enables the user to navigate through the system and solve problems in familiar or similar situations, as well as in unexpected situations.

There are two types of network topology, namely, physical and logical, that together make up the system and the way it operates. Physical topology refers to the physical layout / structure of devices in a network, while the logical topology refers to the manner that the data moves around the network. The objective of the network EID here is to create a multi-layer display of the system and its operation. Figure 2 shows the ecological representation, developed during this study, for the VAST 2013 MC3; it combines both the physical and logical topologies. There are three regions: the main region in the center is the logical network visualization / representation; the left hand region represents the network physical attributes such as memory utilization, CPU etc.; the right hand region can be used for physical links. In the central region, the topmost region or layer represents the outward facing internet of the three branches of the Big Marketing Cooperation. The internet is separated from the intranet by a firewall. The three columns represent the Big Marketing Corporation's three branches. The third layer is the router. The fourth, fifth and the sixth layers represent the three branches' internal servers, such as mail, domain controller etc. respectively. The seventh layer links the Administrator with the service applications of the three branches. The last layer represents the work stations of the three branches and the administrator. The display shows the logical network relationships between the administrators, all the servers and work stations and their inter-dependencies. Figure 2 shows that Web03 is in critical condition, colour coded in red. The reason for the condition, e.g. system overload, can be localised in the physical region on the left (highlighted); however, the cause of this critical situation is not represented. It is necessary to use a UCD type analysis, such as that in Figure 1, to establish the 'why' or the cause of the situation, i.e. a DDoS attack in this instance.

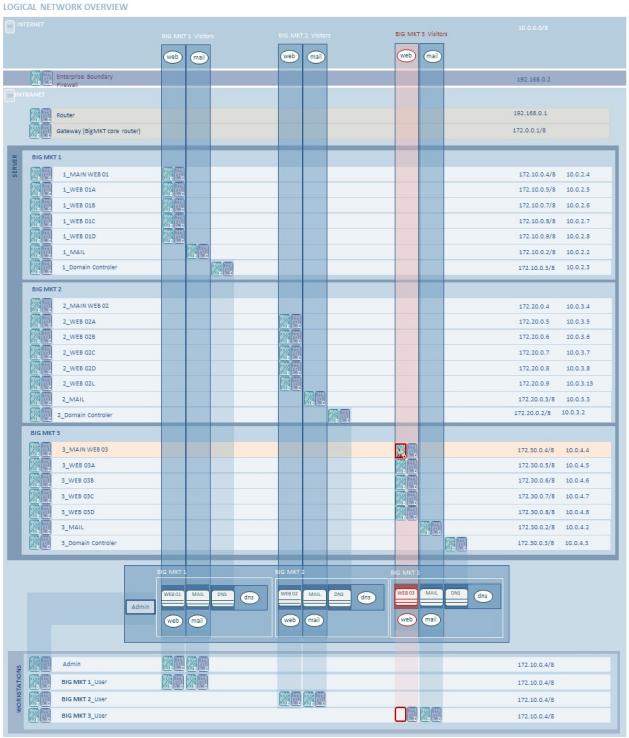

Figure 2: 2nd April WEB 03 at critical situation

It can thus be seen that the EID design approach provides salient information about the network situation, its logical network relationships and inter-dependencies across the network as well as between the three different branches, i.e. the big picture, but not the cause of the situation.

6 Conclusions

Initial evaluation by Analysts was carried out of the UCD and the EID approaches developed in this study.

The UCD was found to provide an effective means of analysing, detecting, discovering and identifying patterns, anomalies, violations and threats; as well as correlating events. The approach is based on the understanding and exploitation of the captured needs of the users, their tasks and their limitations. The resulting intuitive visualizations are suitable for the provision of detailed information on the situation and performance of network components, such as IPs, ports, protocol, packages, CPU load, disk and memory usages, etc.

The EID developed in this study includes depiction of the logical network topology as well as the functionalities of the network, showing the relationships and dependencies between servers, firewalls etc. It provides a visualisation that guides the users in their understanding of how the network functions and is functioning. The patterns of the 'normal situation' can easily be familiarised, and thus any changes from the normal patterns can be detected readily. Thus, in the EID concept, the Analysts easily see the operational aspects of the network, i.e. the big picture.

To conclude, the two approaches complement each other in providing awareness and information of different aspects of the network situation. The UCD approach provides the root cause of the network situation, while the EID approach provides information about the impact of problems on the network.

References

[1] Cyber Defense and Situational Awareness, Edited by A. Kott, C., Wang, C. and R. F. Erbacher. Springer, January 2015.

[2] A. D'Amico and K. Whitley. The real work of computer network defense analysts: the analysis roles and processes that transform network data into security situation awareness in *Proceedings of the workshop on visualization for computer security (VizSec 2007)*, Springer, Berlin, pp.19–37, 2008.

[3] A. D'Amico and M. Kocka. Information assurance visualizations for specific stages of situational awareness and intended uses: lessons learned, IEEE Workshop on Visualization for Computer Security, 2005.

[4] M. R. Endsley and D. G. Jones. Designing for Situation Awareness: An Approach to User-Centered Design, Second Edition, CRC Press, 2004, ISBN 9781420063554.

[5] J. Heer and B. Shneiderman. Interactive Dynamics for Visual Analysis', ACM Queue 10(2), pp 1 -30, February 2012.

[6] http://www.vacommunity.org/vastchallenge2013

[7] Mastering the Information Age Solving Problems with Visual Analytics, Edited by D. Keim J. Kohlhammer, G. Ellis, and F. Mansmann. 2010, ISBN 978-3-905673-77-7, http://diglib.eg.org

[8] J. Rasmussen. Mental models and the control of action in complex environments. Mental Models and Human-Computer Interaction 1 (pp. 41-46). D. Ackermann, D. & M.J. Tauber (Eds.). North-Holland: Elsevier Science Publishers. ISBN 0-444-88453-X, 1990.

[9] 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.

[10] K. Vicente and J. Rasmussen. Ecological Interface Design: Theoretical foundations, IEEE Transactions on Systems, Man and Cybernetics 22, PP 1 – 18, 1992.