Empirical Framework for Situation Awareness Measurement Techniques in Network Defense

Maria Evangelopoulou
University of Glasgow
17 Lilybank Gardens
Glasgow, United Kingdom
m.evangelopoulou.1@research.gla.ac.uk

Prof. Christopher W. Johnson
University of Glasgow
17 Lilybank Gardens
Glasgow, United Kingdom
Christopher.johnson@glasgow.ac.uk

***Abstract*—This paper presents an empirical framework for implementing Situation Awareness Measurement Techniques in a Network Defense environment. Bearing in mind the rise of Cyber-crime and the importance of Cyber security, the role of the security analyst (or as this paper will refer to them, defenders) is critical. In this paper the role of Situation Awareness Measurement Techniques will be presented and explained briefly. Input from previous studies will be given and an empirical framework of how to measure Situation Awareness in a computing network environment will be offered in two main parts. The first one will include the networking infrastructure of the system. The second part will be focused on specifying which Situation Awareness Techniques are going to be used and which Situation Awareness critical questions need to be asked to improve future decision making in cyber-security. Finally, a discussion will take place concerning the proposed approach, the chosen methodology and further validation.**

Keywords: Situation Awareness, Situation Awareness Measurement Techniques, CyberSA, Network Defense, Cyber Security, Intrusion Detection, Decision Making.

I. INTRODUCTION

In 2011 Barack Obama declared that the "cyber threat is one of the most serious economic and national security challenges we face as nation". After this statement he proposed a strategy for reducing cyber threats and improving the resilience to cyber-attacks. A key factor is the accurate and timely detection of attacks [18]. The role of the defenders consists of complex cognitive tasks. Several studies identify poor Situation Awareness (SA) as an important factor in security performance failure [3].

Situation Awareness theory first emerged from aviation psychology and was introduced in Safety Critical Systems (Air Traffic control, Train control etc.), but in the last few years there have been attempts to transfer this theory to Network Defense (known in this case as CyberSA) [3,12]. Focusing mostly on improving data and attack visualization by using different technologies and interfaces, so the defenders can easily process network data [14,16,17]. This paper focuses on experiments with different SA Measurement techniques in the networking environment [1,2,4,13].

Situation Awareness is sometimes confused with decision making or training, because of the close relationships between these subjects. Situation Awareness is the process that leads to a decision and training is a tool for improving the level of Situation Awareness. Moreover, the result of measuring Situation Awareness can give valuable inputs to decision making and training processes.

Following Endsley's model of Situation Awareness; three levels have been identified. However, in CyberSA these levels have been converted so they can refer to a Network Defense environment (see Figure 1):

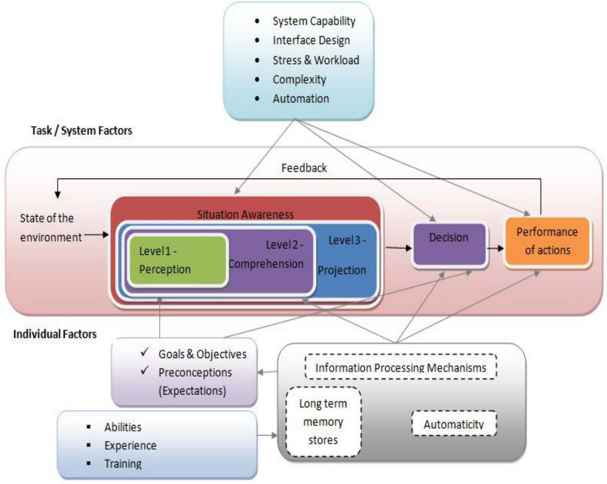

Figure 1: The three levels of Situation Awareness and their Relationship with other attributes in the Decision Making process [8, 11].

- Level 1 – Perception: In the perceptual level the user must be able to identify the information given and their relevance to a decision (identification of object, entities etc.). But in CyberSA Level 1 is concentrated on situation recognition and identification. In this context, the defender must be able to recognize the quality of the data and identify the type/source/target of a potential attack (event detection) [2,9].
- Level 2 – Comprehension: The user must be able to connect information and understand the situation. In CyberSA, this level is concentrated on finding out the

reason behind the behavior of the adversary and how the attack managed to occur (analysis – situation assessment) [2,9].

- Level 3 – Projection: Projection is about predicting the near future and creating experience/knowledge for future encounters. Situation Projection (CyberSA), concentrates on the future too, by anticipating and planning effective countermeasures (response – threat assessment) [2,9].

Considering the differences on the Levels of SA and CyberSA, differences in the SA Measurement Techniques will also exist. In any case the system health must be maintained and the attacks must be identified and dealt with. For this reason the rest of the paper is organized as follows: section 2 presents an overview and background of the Situation Awareness Measurement Techniques that exist; section 3 explains the methodology followed; and section 4 provides a summary, conclusions and areas for further work.

II. Situation Awareness Measurement Techniques

A. *Assessment Approaches of Situation Awareness*

There have been several proposed classifications of SA measurements. In this paper, three approaches will be considered [3]: subjective measures, query methods and implicit performance measures.

The most widely known subjective technique in Situation Awareness is the SA Rating Technique (SART) [3]. The SART technique consists of a set of 7-point Likert questions investigating the understanding of the situation, the available information etc. [3,15].

There are many concerns; on one hand if the defender thinks the level of SA is relatively low and it is not, mistrust and concerns are possible when a situation takes place and the defender's performance might be affected. Overconfidence at the defender's SA can also lead to a potential problem in SART [3]. This problem was identified in a previous mini study [7], were defenders were asked to rate their expertise and fail to match it with the results. Specifically, by rating their expertise in network monitoring the participants were separated in groups (experts – medium experienced – inexperienced). After completing a questionnaire and matching videos and images representations with attacks, it was noticed that the experts made more mistakes than the medium experienced and the inexperienced participants.

Moving on to the query methods, the most popular are the SA Global Assessment Technique (SAGAT) and the Situation Present Assessment Technique (SPAM). The SAGAT method has accuracy as dependent variable. After the creation of a question database, which contains questions covering the three SA levels content, a simulation is being created. While the defender is inside the simulation, randomly it freezes and a set of selected queries is revealed for the defender to answer. However, the use of this freeze-probe technique raises many concerns; interfering with normal processing and heavy dependability on memory [3,10,15].

The SPAM approach has the same structure as SAGAT with two exceptions. First the beginning is signaled with the word "Ready" and the defender must press the spacebar. Secondly, by presenting different scenarios and questions, the defender needs to respond verbally [9,15].

The implicit performance measures have been proven and used in many previous studies. This technique is mostly used for measuring performance and factors like time, accuracy etc. The discovery of information revealing changes in a natural way in a simulation would indicate a good SA level. Generally, it is based on the idea that someone with a good level of Situation Awareness will perform better in contrast with someone with a poor level of Situation Awareness [3].

B. *Cognitive Factors in Measuring Situation Awareness*

As previously mentioned, Situation Awareness involves a serious of complex cognitive tasks and it is important to include cognitive factors as a measure, when constructing Situation Awareness Measurement Techniques for Network Defense.

A previous study [13], suggested investigating cognitive aptitudes associated with the decision making process and adaptive thinking. For this purpose a personality assessment containing a Big Five Inventory (BFI) personality test and three cognitive tasks: mental rotation, syllogism and comprehension span were analyzed.

Mental orientation tasks paired same figures, without the rotation affecting the result (measuring visual-spatial ability and mental flexibility). The syllogism consisted of logical arguments with a set of premises and the operators were asked to say if it can be true or not (measuring reasoning). The comprehension span included a series of questions and the operator was asked to say if each sentence made sense and recall the last world of every sentence in order [13].

III. Proposed Method of Measuring Situation Awareness in Network Defense

This section is divided in two main parts. The first is concentrating on a mini study covering the cognitive concerns of SA and the self-evaluation (SART method). The second part is focusing on simulation and proposed techniques for measuring the Situation Awareness level. It is important to mention that this experimental approach must be completed by network experts/security analysts.

The scope of this framework is to identify if it is reasonable to integrate the known SA Measurement techniques in the Network Defense. Also, an initial investigation of how different monitoring tools and visualization techniques might affect the results, will take place. The personality and cognitive tasks were chosen only for making sure that the participant is able to handle complex cognitive tasks. The reason for having different operating systems is for giving the opportunity to participants to feel comfortable in the simulation environment.

A. *First Mini Study*

In this first mini study, the participants were requested to complete some basic cognitive tasks, covering any concerns that may arise and affect the study's results. After this part was completed, they were given an introduction about what this experiment is about and the SART technique was used, in order to compare their personal opinion with their results later. This is a small session covering main areas and answering any questions that might occur.

The results of the mini study, will inform about the experience and training level of the participants. Also, by using the SART method subjective results were obtained and can be compared with the simulation results in the end.

B. *Main Simulation Experimental Approach*

A private cloud-based network was created, so it can be accessed remotely. In this network, there are three types of users: root, normal user and the victim. The participants had to connect via VPN as normal users (see Figure 2 below). When someone logs in an automatic record will start. Their actions will be recorded and saved for further analysis. In order to make it as user-friendly as possible, three options of normal users were given from the beginning with different operating systems (Windows, Linux and MacOS). Three different tools were available for network monitoring: 1) log analyzer; Log files are records containing vital information for monitoring the system (information such as: password attempts, remote login, connected users on the system, etc.), 2) Wireshark (commonly used monitoring tool); Wireshark is a network protocol analyzer, which reveals information by inspecting the traffic of the network. (Webpage requests, decryption data etc.) and 3) Logstalgia (Google visualization tool); replays or streams web-server access logs as a ping pong game. In this case the server is represented by a paddle, which is trying to respond to all the requests (small balls) by hitting them [6].

The method that was used in the simulation is neither SAGAT nor SPAM. If SAGAT was chosen the freeze probe technique could alert participants that an attack was happening. The SPAM choice was not considered because we are not interest in human-computer voice interaction. In conclusion, a real-live environment is going to be used, but there is total isolation (private network) in order to avoid any accidents.

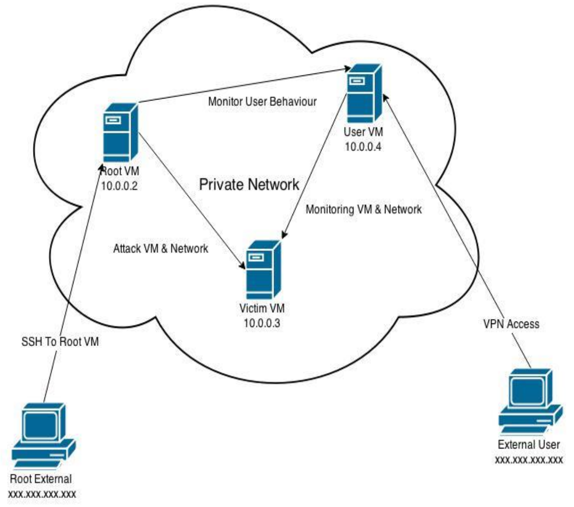

Figure 2: Proposed Network Architecture Representation.

When the experiment began, the participants were able to watch what is happening to the network. It must be noted that most of them according to previous studies [7], are used to using automated intrusion detection systems. But automation can lead to a decrement of the operator's Situation Awareness. It was noticed that even though the Situation Awareness level was decreasing by increasing the automation level, the confidence of the operator was increasing [3,5]. For this reason, no automation was included for this experiment. The participants then had a series of questions to answer while doing live monitoring. This series of questions will be explained prior, reducing any misunderstandings and delays.

The first set of questions covers the event detection. Sample questions: 1) what systems are up or down on my network? 2) Is my network status normal? 3) Is something happening to my network right now? 4) Is there more or less traffic than normal? Then the second set of questions is relevant to the event orientation: a) what does the attack looks like? b) Who is attacking the network? c) What is the purpose of this attack? d) How serious is the attack? e) How successful is the attack? These two set of questions cover Level 1 and Level 2 Situation Awareness [2]. For Level 3, threat assessment: i) how can I stop the attack? ii) What is the priority level of this attack? iii) Should I report this attack? iv) Is it likely to happen again?

A set of programming scripts was used to create real attacks in the network. There were different groups of scripts with different normal operation time frames and different kind of attacks, happening at different times. The initial study will include three attacks (Distributed Denial of Service, Man in the Middle, Brute Force).

After doing live monitoring and the relevant questions, participants had to check a previous log file and try to answer the set of questions again. After finishing that, a discussion took place clarifying some choices and dealing with any concerns.

C. *Explanation of Proposed Method*

This approach is better from SAGAT and SPAM. All of them are simulations, but by using this method the interactions while live monitoring will not exist. SAGAT by using the freeze-probe technique is interrupting the cogitation of participants and the voice interaction technique (SPAM) is not appropriate for the purpose of this study.

The simulation data will help in realizing where the current Situation Awareness level varies over time both before and during an attack in different monitoring context and there will be a comparison between the postgraduate networking students and the network experts/security analysts.

Taking all the psychological aspects and limit their affect on the experiment, by doing some personality/ability tests would be sufficient. In further analysis, the correlation between them with the Situation Awareness level can be investigated.

By reviewing the answers given by each participant for the experimental study and indicating the correctness and the response time for each one, the SA level can be decided as high, medium and low. In the end the comparison with data obtained from a previous log file can give more understanding for any stress related issue that might arouse from the live monitoring. The experimental approach data with the SART mini study data will be able to give a more insight for each participant's perspective. Also, the SART method with the experimental approach used correlation will be investigated.

IV. Conclusion

This paper illustrated the most common SA Measurement Techniques and a thorough examination of how they can be implemented in CyberSA took place. However, because our study is based on how to measure effectively CyberSA, it was preferred to propose a new approach.

The mini study plays a major role in grouping participants and can give valuable inputs after doing a correlation analysis. The simulation part provides information by examining the three levels of CyberSA and the participant's behavior. By adding different monitoring and visualization techniques, the information can be processed by using a different angle. This approach will be examined thoroughly in another study.

The results of this study will be presented in a companion paper.

For future work the issue of cost metrics and scalability is worth covering. The cost metrics were not investigated for this proposal. However, it can be mentioned that this proposed approach does not encompasses high demands. The mini study can be conducted with no material costs and the simulation part needs only resources depending on the magnitude of the experiment. Moreover, this study was designed for a medium sized experiment and a future work for adaptation on a bigger and more complex organisation like Amazon services etc. might be useful.

References

[1] A. Kaur, V. Dutt, and C. Gonzalez, “Modelling the security analyst’s role: effects of similarity and past experience on cyber attack detection,” in Data and Applications Security and Privacy XXV, 2011, [Springer, pp.280-292].

[2] C.L. Paul, and K. Whitley, “A taxonomy of cyber awareness questions for the user-centered design of cyber situational awareness,” in Human Aspects of Information Security, Privacy and Trust, 2013, [Springer, pp.145-154].

[3] F. T. Durso, and S. D. Gronlund, “Situation awareness,” Handbook of Applied Cognition, 1999, [pp.283-314] .

[4] G. Fink, D. Best, D. Manz, V. Popovsky, and B. Endicott-Popovsky, “Gamification for measuring cyber security situational awareness,” in Foundations of Augmented Cognition, 2013, [Springer, pp.656-665].

[5] L. Bainbridge, "Ironies of automation," in Automatica, 1983, [19(6), pp.775-779].

[6] Logstalgia. "Website access log visualisation," in Google Project Hosting, [20/02/1015, https://code.google.com/p/logstalgia].

[7] M. Evangelopoulou, and C.W. Johnson, “Attack visualization for cyber-security situation awareness,” 2014, awaits publication information.

[8] M. Evangelopoulou, and C.W. Johnson, “Implementation of safety techniques in a cyber domain,” in Proceedings of the 7th International Conference on Security of Information and Networks, September 2014, [ACM, p.261].

[9] M. R. Endsley, “Measurement of situation awareness in dynamic systems,” in Human Factors: The Journal of Human Factors and Ergonomics Society, 1995 [37(1), pp. 65-84].

[10] M. R. Endsley, “Situation awareness global assessment technique (sagat),” in Aerospace and Electronics Conference, NAECON 1988, May 1988 [Proceedings of the IEEE 1988 National, pp. 789-795].

[11] M. R. Endsley, “The role of situation awareness in naturalistic decision making,” in Naturalistic Decision Making: Experise: Research and Applications, 1997, [pp. 269-283].

[12] M. R. Endsley, “Toward a theory of situation awareness in dynamic systems,” in Human Factors: The Journal of Human Factors and Ergonomics Society, 1995 [37(1), pp. 32-64].

[13] S. Stevens-Adams, A. Carbajal, A. Silva, K. Nauer, B. Anderson, T. Reed, and C. Forsythe, “Enhanced training for cyber situational awareness,” in Foundations of Augmented Cognition, 2013 [Springer, pp.90-99].

[14] S. Wood, J. Mathewson, J. Joy, M.O. Stehr, M. Kim, A. Gehani, M. Gerla, H. Sadjadpour, and J. Garcia-Luna-Aceves, “ICEMAN: a practical architecture for situational awareness at the network edge,” 2013.

[15] T. Z. Strybel, R. S. Pierce, and K. P. L. Vu, "Comparing situation awareness measurement techniques in a low fidelity air traffic control simulation”, in Proceedings of the 26th International Congress of the Aeronautical Sciences (ICAS), September 2008, [pp. 3525-3532].

[16] V. Dutt, Y.S. Ahn, and C. Gonzalez, “Cyber situational awareness: modeling detection of cyber attacks with instance-based learning theory,” in Human Factors, 2013, [The Journal of the Human Factors and Ergonomics Society, 55(3), pp. 605-618].

[17] W. Yu, S. Wei, D.Shen, M. Blowers, E. P. Blash, K. D. Pham, G. Chen, H. Zhang, and C. Lu, “On detection and visualization techniques for cyber security situation awareness,” in SPIE Defense, Security and Sensing, May 2013 [International Society for Optics and Photonics, pp.87390R-87390R].

[18] Whitehouse, Office of the Press Secretary, 2011, "Remarks by the President on securing our nation's cyber infrastructure," [http://www.whitehouse.gov/the_press_office/Remarks-by-the-president-on-Securing-Our-Nations-Cyber-Inrastructure/] .