Implementation of *Safety Techniques* in a Cyber Domain

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

Due to the rise of Cyber crime it is important to explore the Cyber security area. The threats are real and can cause severe damage to both the system and its clients. Many examples can be given; one of them is BitBucket which encountered a denial of service attack (based on Amazon Cloud infrastructure) and led to 19 hours outage [6]. Bearing in mind the importance of the Cyber security and the factors that play a major role, the human factor was recognized as one of the most important.

For this reason, this paper focuses on the application of safety techniques to the Cyber domain. More specifically it investigates the possibility of a successful implementation of the *Situation Awareness* theory into a Networking Environment. By concentrating on the Network Intrusion Detection Systems and the human factor involved (Network Administrators / IT specialists), it is attempted to propose a procedure that can identify the influence level of the human factor's awareness in the case of an attack to the system.

In order to explain this approach the theory of *Situation Awareness* and its characteristics will be introduced. Moreover the most known *Situation Awareness Measurement Techniques* will be presented and their adoption to the Cyber domain will be discussed. There is a lack of research in the *Situation Awareness Measurement Techniques* for a network system which leads to the need for further exploration.

General Terms

Situation Awareness, Situation Awareness Measurement Techniques

Keywords

Situation Awareness,Intrusion Detection, Cyber Security, Cyber Warfare

SIN '14 Sep 09 - 11 2014, Glasgow, Scotland UK
Copyright 2014 ACM 978-1-4503-3033-6/14/09 ...$15.00.
http://dx.doi.org/10.1145/2659651.2659740.

1. INTRODUCTION

Situation Awareness theory is mainly being used in the safety sector and not in the security (train safety, plane safety etc.). It is generally used to explain human behaviour and the decision making process in complex Safety Critical Systems. Although *Situation Awareness* is the basis of the decision process, there is a disconnection between them. In order for a good decision to be made, proper inputs from the administrator's *Situation Awareness* are necessary. However the result is not guaranteed because of the variety of the different factors that can affect the decision process [3].

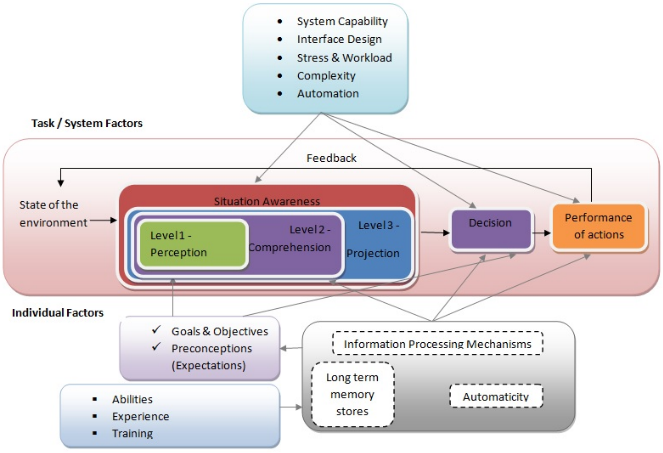

Figure 1: The role of *Situation Awareness* in the Decision Making Process [3].

As it is obvious in Figure 1 (based on Endsley's model), *Situation Awareness* plays a major role in the decision making process. However, as previously mentioned, there are other factors that can affect a decision, such as training, past experience and gained abilities. By looking at this schema it is also clear that factors like the complexity of the system, the stress levels, the automation can directly affect the *Situation Awareness* level and any decision to be made.

More analytically, as Endsley stated *Situation Awareness* is separated in two main portions: a three level *Situation Awareness* representation and a recognition of affecting factors.

The first one is also referred to as the core situation which is the mental representation of the situation someone is dealing with. This portion has been divided into three levels: Level 1 - Perception: is the main foundation of the whole process. It is the step which includes all the important information and by having a wrong perception of this information, creating an incorrect picture is something highly possible. Essentially it presents information for all the elements of the environment and the identification of aspects such as the status, attributes and dynamics are critical. (What are the current facts?) - Level 2 - Comprehension: gives the person a more organised picture of what is happening by combining existing knowledge and new information. The importance of identifying and perceiving things is not covering this step but the combination of all the information and the selection of what is significantly relevant completes the comprehension process. (What is actually going on?) - Level 3 - Projection: is the last step and it includes the ability to make predictions based on all the knowledge acquired.(What is most likely to happen if?) [2, 3].

The second portion of this model is the identification and exploration of factors that can affect *Situation Awareness*. Experience and knowledge can be considered as factors that can affect the *Situation Awareness* process. If someone does not know something, he / she can learn it or even discover it. A major area of knowledge discovery is Data mining (extraction of potentially useful information). There are two ways of gaining this knowledge: First one is by recognizing patterns of activity by gathering information of past events and outcomes and the second through pattern learning: identifying patterns on event associations. The pattern of the learning process can be also transformed in an Anomaly Detection process. Data is the key of this process and many mistakes can be made either by missing data, corrupted data or by processing faults [5].

After this explanation of the decision process model, it will be useful to present the most common measurement techniques and discuss their potential use in the Cyber domain.

2. THE MOST COMMON *SITUATION AWARENESS MEASUREMENT TECHNIQUES*

Situation Awareness can be measured by taking into account different approaches: performance based, subjective techniques and questionnaires / queries. In order for the measurement to be successful the use of understandable Measures of Performance and Measures of Effectiveness is essential. Moreover, the measures must have both quantitative and qualitative characteristics and be directly tied to the target of the environment in question. Pierce et al [8], investigated and compared three *Situation Awareness* techniques, which are most common, however concentrating on complex Safety Critical systems [5]. It was emphasized that all *Situation Awareness* methods have limitations which cause the prevention of accurate predictions. The relationships between all the entities in an environment can be extremely complicated, causing the *Situation Awareness* theory to be difficult to understand. Efficiency, safety and security are primary goals causing the need of valid *Situation Awareness* measurements essential. The three techniques which were mentioned above are: Situation Awareness Global Assessment Technique (SAGAT); Use of a simulation which is being paused in order questions to be asked to the participants(freeze probe technique). Situation Awareness Rating Technique (SART); Use of rating scale questions (1-7) concerning the demand and supply of resources and understanding of the situation (self rating). Situation Present Awareness Method (SPAM); Voice and keyboard interactive questionnaire (real-time probe technique)[3, 8].

These three techniques can give very different outputs and must be used with extra care. For example, the Situation Awareness Rating Technique is based on the participant's understanding and may be the opposite of the reality. For that reason the decision of what to use as an approach is extremely important and sometimes a combination of different methods, may result to be more effective.

2.1 Examples of use of *Situation Awareness Measurement Techniques*

From previous research in Safety Critical Systems and more specifically in the aviation area; Pilots were asked to do a one week training, then do a self rating process (SART method) and enter a flight simulator in order to be evaluated (SAGAT method). Also, sometimes the completion of tasks through human machine interaction was used (SPAM method - questions and verbal answers). Specifically, the purpose of the flight simulator was to measure the pilot's knowledge of the system, his / hers perception of the information that could be extracted, their ability of combining the information and finally the possible outcome of the situation (three *Situation Awareness* levels). All these experiments, helped in the evaluation process and also in the improvement of the system [8].

A research for adoption of the *Situation Awareness* theory in the healthcare system has also taken place. The discussion of the use of patient simulators for training and evaluation of medical practitioners and medical equipment was presented but the lack of measuring methods was the problem [7].

In both cases, the *Situation Awareness Measurement Techniques* have a double role. The obvious one is to help evaluate the participant's *Situation Awareness* level and increase the quality of the service. However, the *Situation Awareness Measurement Techniques* can be transformed to training tools that both the participants and the system can benefit from.

2.2 *Situation Awareness* in a Networking Environment

Situation Awareness theory can be implemented in Intrusion Detection Systems. A key word is CyberSA which represents the virtual version of *Situation Awareness*. As seen in real life examples of Cyber attacks, the impact can be vast and the importance of the administrator of the system (defender) and the scale of its security is high. As in every system, the human factor is critical [10].

So, Endsley's model is used in CyberSA by adjusting the three levels in a Network Environment. More specifically: Perception; Situation recognition (awareness of the situation: source of attack / type). Comprehension; Why and how was caused, what is the impact. Projection; Situation projection - Tracking of the Situation, Reports etc [9].

As it is expected, there is a technology that can help improve the *Situation Awareness* by detecting threats called Intrusion Detection Systems. It is important for the defender to be able to develop a timely and accurate threat perception, leading to a successful attack detection. At least 3 factors can influence the defender's CyberSA: 1) stored experiences gathered from non threat and threat events, 2) level of tolerance the defender has with the Cyber attacks and 3) the strategy of the attacker which can influence the whole process [10].

One of the ways of measuring the CyberSA that can be adopted is by using the Receiver Operating Characteristic analysis or ROC analysis (usually used in Machine Learning and Artificial Intelligence)[1] and is based on four basic criteria:

- Recognition of a successful attack [4].
- Faulty recognition of an attack [4].
- Faulty perception of an attack taking place [4].
- Faulty perception of no attack is taking place [4].

2.3 Proposed approach of *Situation Awareness* adoption in a Networking Environment

As it was presented in the previous examples, *Situation Awareness* theory can be adopted in different kind of areas (like the healthcare system). The purpose of this paper is to introduce the idea of creating a formal procedure of measuring the CyberSA. By exploring the different *Situation Awareness Measurement Techniques* and creating simulations and experiments concentrated on the Network Environment, it would be beneficial for both parties (Safety and Security research area). With the success completion of this proposal, the increase of Intrusion Detection incidents and the response / reaction procedure can be significantly improved.

3. CONCLUSIONS

This proposal paper underlines the importance of the human factor in the Cyber domain and tries to explain the need of adopting safety techniques in a security environment. It is clear that *Situation Awareness* is the basis of the decision making process and the need of testing Measurement Techniques in a Networking Environment is high.

References

[1] A. P. Bradley. The use of the area under the roc curve in the evaluation of machine learning algorithms. *Pattern Recognition*, 30(7):1145–1159, July 1997.

[2] M. R. Endsley. Situation awareness global assessment technique (sagat). In *Aerospace and Electronics Conference, 1988. NAECON 1988. Proceedings of the IEEE 1988 National*, pages 789–795. IEEE, May 1988.

[3] M. R. Endsley. Measurement of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 37(1):65–84, March 1995.

[4] T. S. Guzella and W. M. Gaminhas. A review of machine learning approaches to spam filltering. *Expert Systems with Applications*, 36(7):10206–10222, December 2009.

[5] M. Hinman J. Salerno and D. Boulware. Building a framework for situation awareness. Technical report, DTIC Document, June - July 2004.

[6] W. A. Jansen. Cloud hooks: Security and privacy issues in cloud computing. In *System Sciences (HICSS), 2011 44th Hawaii International Conference*, pages 1–10. IEEE, January 2011.

[7] J. Taekman M. Wright and M.Endsley. Objective measures of situation awareness in a simulated medical environment. *Quality and Safety in Health Care*, 13(suppl 1):65–71, October 2004.

[8] 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), Anchorage, ASl*, pages 3525–3532. ICAS, September 2008.

[9] G. P. Tadda and J. S. Salerno. Overview of cyber situation awareness. In *Cyber Situational Awareness*, pages 15–35. SPRINGER, 2010.

[10] Y. S. Ahn V. Dutt and C. Gonzalez. Cyber situation awareness modeling detection of cyber attacks with instance-based learning theory. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 55(3):605–618, October 2013.