Empirical Framework for Situation Awareness Measurement Techniques in Network Defense

Professor Christopher Johnson
PhD Student: Maria Evangelopoulou

Presentation Contents

- Why is there a need to concentrate on Situation Awareness in Network Defense?
- Introducing Situation Awareness.
- Endsley's three Levels.
- Situation Awareness and Decision Making Relationship.
- Most Common Situation Awareness Measurement Techniques.
- The Role of Cognitive Factors.
- Proposed Method of Measuring SA in Network Defense Part 1 & 2.
- Visualization Tools & Sample set of Questions.
- Conclusions and Future Work.

University of Glasgow

Why is there a need to concentrate on Situation Awareness in Network Defense?

- Cyber security is one of the most important subject nowadays. → accuracy and timely detection.
- Rise of Cyber-crime.
- Several studies identify poor Situation Awareness (SA) as an important factor in security performance failure.
- The role of the defenders plays a major part in the system security – complex cognitive tasks.

University of Glasgow

Introducing Situation Awareness

- The theory of Situation Awareness first emerged in aviation psychology and was introduced in Safety Critical Systems.
- Endsley created the following parts: 1) Three level Situation Awareness Representation (core situation) and 2) Recognition of affecting factors (experience – knowledge)
- The Situation Awareness is often confused with training or the process of decision making.
- Virtual version of Situation Awareness is known as CyberSA.

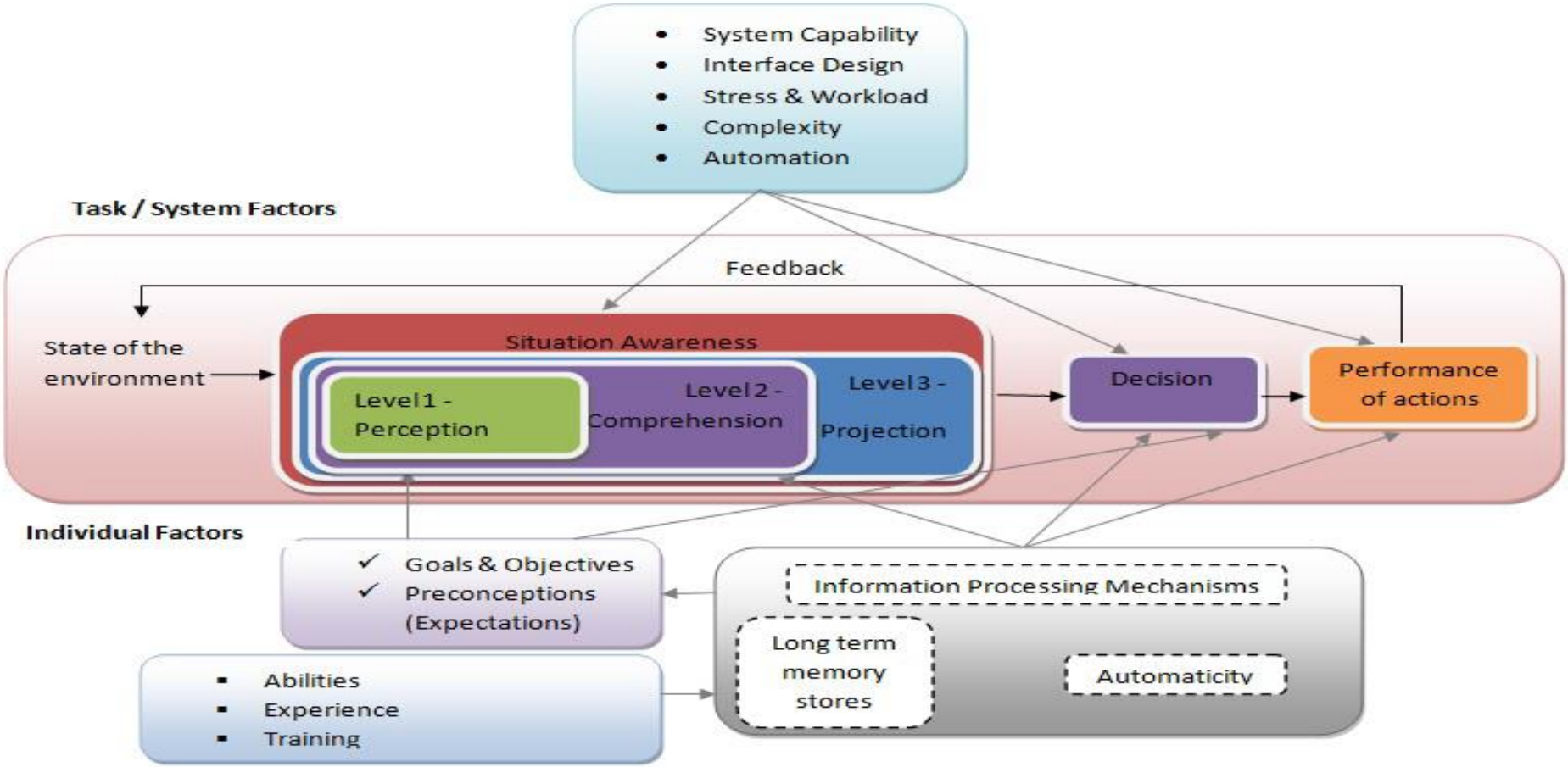
University of Glasgow

Endsley's three Levels

Levels	SA	CyberSA
Level 1	Name: Perception – identifying the given information and their relevance to a decision (identification of object, entities etc.).	Name: Event Detection– recognition of the quality of data and identifying the type/source/target of a potential attack.
Level 2	Name: Comprehension – connecting information and understanding the situation.	Name: Analysis/Situation Assessment – finding out the reason behind the behavior of the adversary and how the attack managed to occur.
Level 3	Name: Projection – predicting the near future and creating experience/knowledge for future encounters.	Name: Situation Projection – anticipating and planning effective countermeasures (response – threat assessment).

University of Glasgow

Situation Awareness and Decision Making Relationship



Most Common Situation Awareness Measurement Techniques

- SART (self rating technique): Situation Awareness Rating Scale Technique (7-point Likert questions).
- SAGAT (question database and freeze simulation): Situation Awareness Global Assessment Technique.
- SPAM (real time probe technique – verbal interaction): Situation Present Awareness Method Technique.

University of Glasgow

The Role of Cognitive Factors

- Complex cognitive tasks → cognitive factors.

- Use of a Big Five Inventory (BFI) personality test and three cognitive tasks: mental rotation (pairing with no rotation influence), syllogism (logical arguments - true or not) and comprehension span (does it make sense? / recall of the last world of every sentence in order).

University of Glasgow

Proposed Method of Measuring SA in Network Defense Part 1

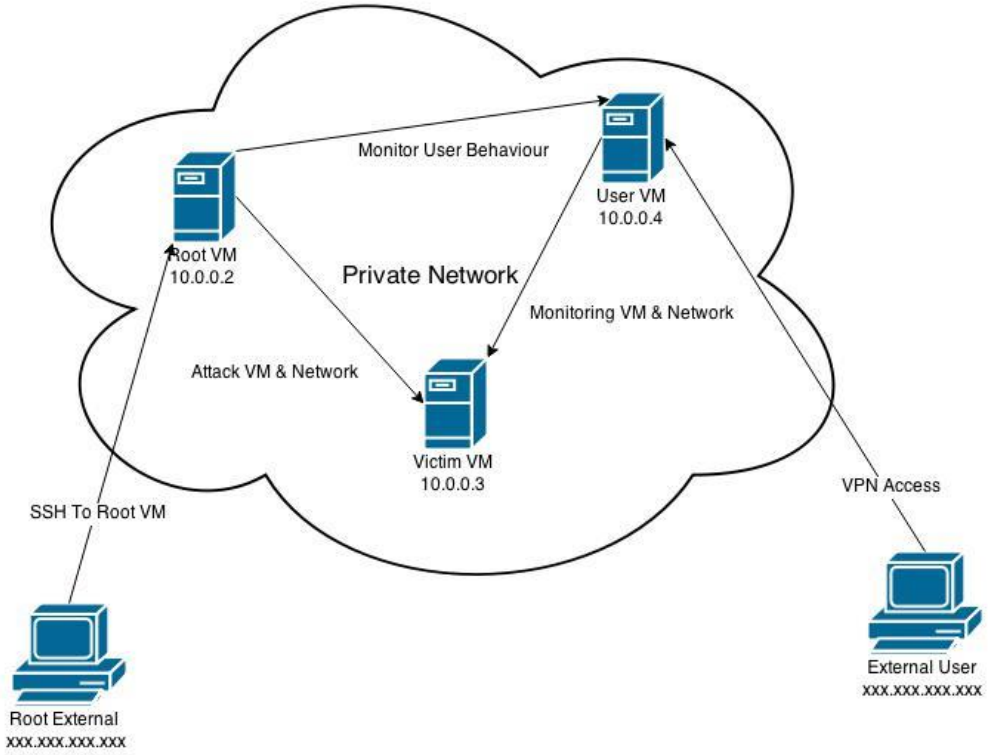
- Scope: identifying if it is reasonable to integrate the known SA Measurement techniques in the Network Defense. Investigation of how different monitoring tools and visualization techniques might affect the results.

- Part 1 - Cover of the cognitive concerns of SA and the self evaluation.
- Including: Experiment Introduction - Basic cognitive tasks – subjective data gathering through SART method.

University of Glasgow

Proposed Method of Measuring SA in Network Defense Part 2

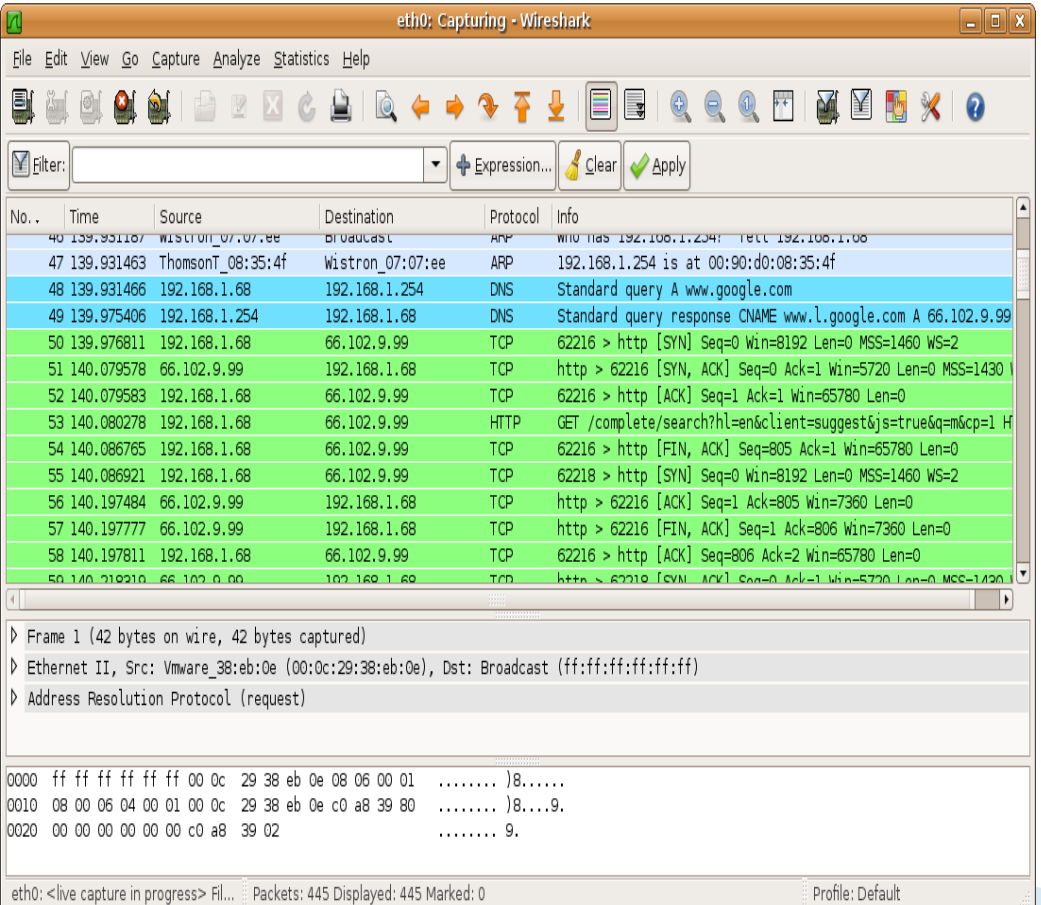
- Private Network – Recording – OS – Visualization tools:

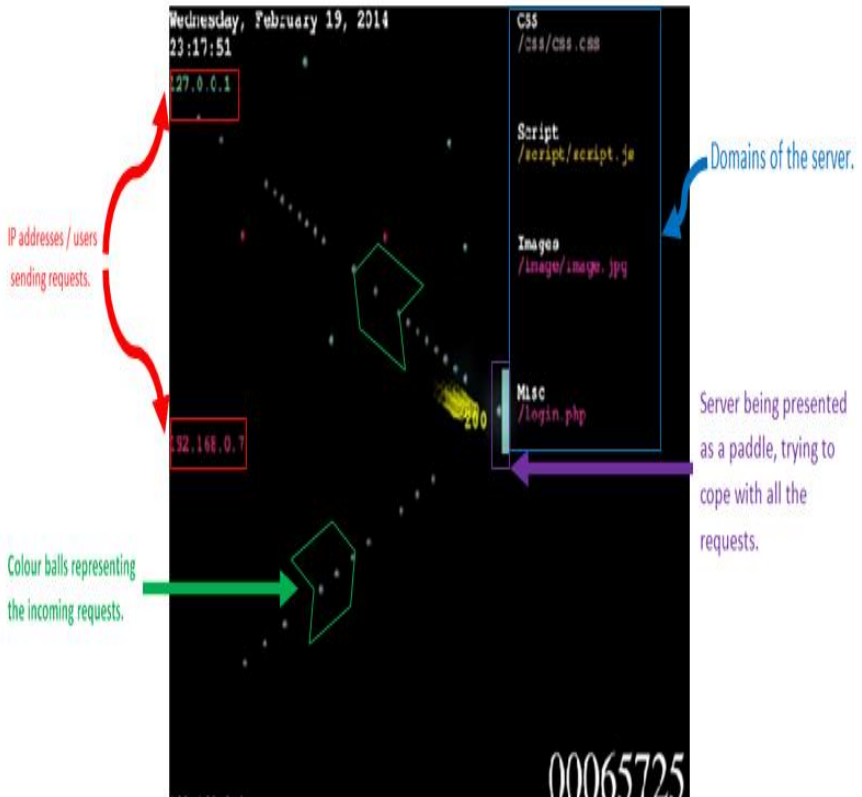


University of Glasgow

Visualization Tools

- Automation? decrement of the operator's SA, but increment of confidence.
- Wireshark (wiki photo) - Logstalgia





Sample Set of Questions

- Sample questions: 1) what systems are up or down on my network? 2) Is my network status normal? 3) what does the attack looks like? 4) Who is attacking the network? 5) How successful is the attack? 6) What is the priority level of this attack?

- Initial Attacks → Brute Force, Distributed Denial of Service and Man in The Middle.

- Examination of previous log files.

Conclusions & Future Work

- Many more attacks can be added and the simulation can be enriched.
- By grouping the participants and adding different monitoring and visualization techniques, the information can be processed by using a different angle.
- Issue of cost metrics and scalability: the mini study can be conducted with no material costs and the simulation part needs only resources depending on the magnitude of the experiment.
- This study was designed for a medium sized experiment and a future work for adaptation on a bigger and more complex organisation might be useful.

University of Glasgow

The End…

Any Ouestions?

University of Glasgow