Using a socio-technical systems approach to design and support systems thinking in cyber security education

Erjon Zoto, Stewart Kowalski, Edgar A. Lopez-Rojas, Mazaher Kianpour

Norwegian University for Science and Technology, NTNU Gjøvik, Norway

{erjon.zoto; stewart.kowalski; edgar.lopez}@ntnu.no;
m.kianpour2011@gmail.com

Abstract. Information security (IS) has been categorized as protecting the confidentiality, integrity, availability, authentication and accountability of information. There is a gap between what companies and institutions plan to do while developing their internal IS-related policies and what it should be done according to a system perspective in this area. Our task as researchers is to bridge this gap by offering potential solutions. The aim of our work is to promote the usage of a socio-technical systems (STS) approach to support the emerging role of systems thinking in cyber security education using simulation as a supporting tool for the learning. Meanwhile, new trends in cyber security curricula suggest an important shift towards new thinking approaches to be used, such as systems thinking.

Keywords. Socio-technical systems, information security, cyber security, systems thinking, simulation, modeling, education

1 Introduction

We hardly pass any day without hearing of new cyber security incidents. With all these vulnerable systems and threat actors out there, organizations today are in a constant race to defend adequately against potential cyber-attackers through technical or social means. A properly educated and aware staff has been identified as one of the most cost-effective means to keep your organization ahead in the race, as in [1].

In order to improve the cyber security education of the Information Technology (IT) staff, the Joint Task Force on Cyber security Education (JTF), a worldwide research group, was established to develop comprehensive curricular guidance in cyber security education. The JTF has produced just recently a new curricular volume that focused on the new thinking processes, namely adversarial and systems thinking [2].

The aim of this poster paper is to present our ongoing work using a STS approach to model and build a simulation-based teaching tool in “Adversarial and Systems Thinking” to raise the awareness towards cyber security of students participating in a Master Program in Information Security.

The ongoing modeling work is based on a combination of theoretical models [3] and data from real-world reported cases about cyber-attacks news[1]. In the simulation case, we present a scenario where attackers with diversity in skills and motivations try to break into different objectives from states to corporations, while defenders use their skills and resources to stop and deter the attacks. The learning objective of the simulator is to indicate students the relevance between different conditions that make a cyber-attack and a cyber-defense effective.

2 Background

A socio-technical system can be seen as being composed from two components: the social and the technical [4].

.

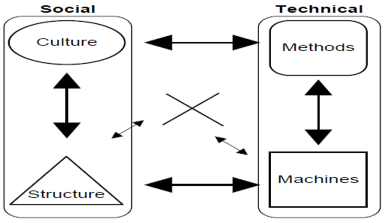


Figure 1. The typical socio-technical system

As Figure 1 shows, each of the components can be broken down in two subcomponents. The social component has its cultural and structural subcomponents, while the technical side has its own machines and methods as subcomponents. We have used the same approach when designing a simulator dealing with cyber security issues.

Pastor et al. [5] have done an extensive research work on the available state-of-the art simulation tools that can be used on the purpose of teaching and training. They suggest that such simulation tools should be designed to have a user-friendly interface and, at the same time, allow the user to obtain a deep understanding of the concepts.

We believe that modeling and simulation create a good and efficient way to produce data that can be mapped to real cases of cyber events. The modeling phase purpose is to create a normalized view of the cyber security situation, while the simulation phase allows the imitation of typical attack activities against a specific infrastructure, with specific security controls in place, grouped in sets of possible scenarios.

We built the tool in Netlogo [6], inspired from a relevant work in the same area from Ben-Asher and Gonzalez [7] and a study prepared from Ponemon Institute [8], while developing their works further by introducing the STS approach within our tool.

Ben Asher and Gonzalez came up with a simple cyberwar game that takes place in a network of *n* players. Each player has two main attributes, *Power* and *Assets*. *Power* represents the player's cyber security infrastructure, seen also as the investment in cyber security, while *Assets* entail the confidential information available for use.

[1] https://thehackernews.com/2017/09/apt33-iranian-hackers.html

The Ponemon Report showed the relationships between the time spent and compensation of today's cyber attackers and the way that organizations can thwart attacks. Some relevant findings were the average cost of $1,367 on a yearly basis for the tools that an attacker needs to execute his attacks and the average time spent against different target security infrastructures, ranging from 70 up to 209 hours on average.

In the next section we will explain how we used the STS approach for the tool.

3 Designing the simulator with a STS approach

We started designing the simulator by thinking that Defense or Attack actors in a potential cyberwar can be represented by their own socio-technical systems. Actors will have their own *culture* - defined by certain values, traditions and laws, along with a certain *structure* - the actor's position in an organization or the whole society. They also have a certain level of access to the infrastructure already built (*machines*) and, depending on the former abilities and their will or cultural background, they can use some or other available tools (*methods)* compared to their colleagues or potential opponents. Moreover, the type of infrastructure and tools in use should depend on the attitude of the actors or the structures above them regarding the amount of investments made while being part of the cyberwar.

Following the reasoning above, we defined three attributes that could explain the behavior and performance of the actors in the agent-based simulation tool. The attributes were *Resources* - the budget related to cyber activities, *Skills* - level of training, literacy and awareness on cyber events, and *Motivation* - the level of self-motivation and incentives in a certain time.

We used various sources of data for *Resources*, including [8], while we used the GCI Index, [9], for the *Skills* units. We did not make use of any relevant literature on *Motivation*, but we are willing to conduct it in the future stages.

Resources are most important when dealing with the technical component, spread equally between machines and methods for both attack and defense, and somewhat relevant when dealing with the structural subcomponent, in the process of allocating funds to different strategies applied.

Skills are mostly related to the social component, almost equally spread between the cultural and structural subcomponents, and somewhat relevant to the methods used. Motivation is generally related to the cultural background, but it can also be affected from the structural subcomponent, depending on the direct link within the different levels of management. Motivation, depending on the provided incentives, can lead to the intentional or accidental misuse of machines. Both Skills and Motivation are slightly biased towards culture in the social component. Figure 2 depicts this type of relationship between each attribute and the STS subcomponents, where attributes are located and weighed according to the reasoning above.

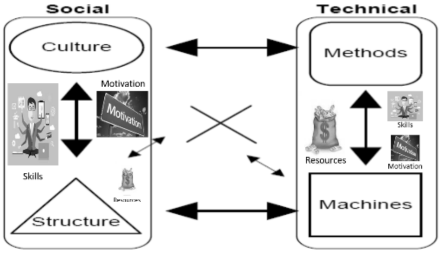
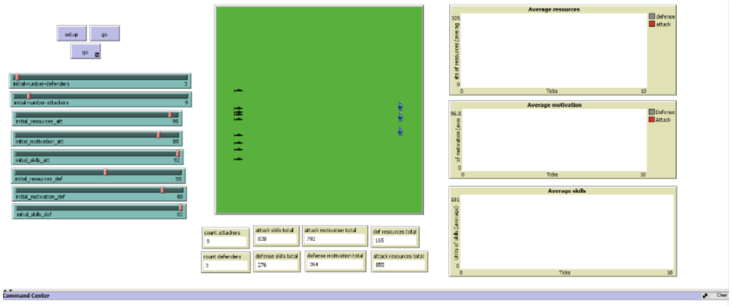


Figure 2. Attributes "produced" by the STS approach

The current version of the simulator allows the user to define initial number of agents in each side of the battlefield and also the initial value for each of the attributes for all agents on each side. The user can choose in a range of [1, 100] for the number of agents on each side, along with initial units of Resources and Motivation, and [1, 93] for the Skills attribute. Figure 3 shows a screenshot of the current version of the simulator's interface.



initial-number-defenders 3
initial-number-attackers 9
initial_resources_att 95
initial_motivation_att 88
initial_skills_att 92
initial_resources_def 55
initial_motivation_def 88
initial_skills_def 92

count attackers 9
attack skills total 828
attack motivation total 792
def resources total 165
count defenders 3
defense skills total 276
defense motivation total 264
attack resources total 855

Figure 3. The simulator's interface, in Netlogo

The simulator performs each run in a period of max 120 ticks. Each tick represents a fixed period of time of 3 days, mapping the minimum time required for an attacker to perform a successful attack [8], thus making it able to predict the behavior of agents on both sides within a year. The current version allows a random attack agent to attack one or more random defense agents in each tick, only if the former combined product of attributes' units is at least a third of the combined product of attributes' units of the latter. That means that an attack agent should finish the attack in 3 ticks or less, otherwise it will quit the attack and target another opponent.

If the attack is performed, the defense agent loses some *Resources* units, based on the relative power that they have compared to the attacker, taking in consideration the total amount of combined products between them. The successful attack agent gains the *Resources* units lost from the defense agent, while *Skills* units are also updated by increasing values in both sides, with the defense agent having a larger increase in terms of learning experience. *Motivation* is also updated on the attack agent's side, increasing the units by the value of the relative power.

If the attack is avoided, only the *Motivation* units are updated on the defense agent side, by the same value of the relative power.

Continuous successful attacks can actually decrease one defense agent's *Resources* units towards reaching zero. When this happens, the defense agent goes "offline", meaning he does not interact anymore with the other agents.

According to the assumptions above, the current simulator runs typically end in not more than 10-12 ticks out of a total of 120 ticks, depending also on the initial values. Thus, in the current version the attack agents mostly outscore the defense ones.

4 Preliminary Result

The simulator was used for the first time this spring in a course entitled Socio-Technical Enabled Crime. This course is an elective course in a 2 years Master Program in Information Security. Eight students responded surveys and used the simulator in order to provide their overall appreciation as related to learning adversarial and systems thinking.

Surveys results indicate that most of the respondents expected the simulator could help them develop their understanding of adversarial and systems thinking. The most important finding is related to the question on the most relevant attributes that would affect the chances of defense agents to avoid attacks until the end of the run. In the pre-simulation survey, the respondents expected that the most relevant parameter would be the defense *Resources*, followed by defense *Skills* and then *Motivation*. However, after trying the simulator, the respondents answered that defense *Motivation* was the most relevant parameter, followed by defense *Skills* and then attack *Motivation* parameter. This shift from defense *Resources* to defense, and especially attack, *Motivation*, shows that, at least from the preliminary results, the simulator was able to change the respondents' way of thinking.

5 Conclusions and Future work

In our poster, we presented how a STS approach can be used to design and support an agent-based simulation tool, in order to introduce the emerging role of systems thinking in cyber security education. We defined three main attributes, namely *Resources*, *Skills* and *Motivation*, affecting the behavior and performance of each actor within the simulation.

In the future stages, based on the STS approach, we intend to go deeper into the *Motivation* attribute, by conducting a more detailed literature review on the theories explaining attack actors' motivation, such as the ones related to the MOMM's taxonomy [10], and other theories explaining defense actors' motivation, such as the protection motivation theory [11].

We will use the same approach to analyze and interpret findings from current and future versions of the designed tool to argue about the benefits of using STS in this area.

References

1. Khan, Bilal, et al. "Effectiveness of information security awareness methods based on psychological theories." African Journal of Business Management 5.26 (2011): 10862.
2. Cyber security Curricula 2017 - Curriculum Guidelines for Post-Secondary Degree Programs in Cyber security - CSEC2017 v. 0.95 draft, p. 21, Joint Task Force on Cyber security Education, November 2017
3. Kshetri, Nir. "Simple economics of cybercrime and the vicious circle." The global cybercrime industry. Springer, Berlin, Heidelberg, 2010. 35-55.
4. Rogers, M, A new hacker Taxonomy, Department of Psychology University of Manitoba, Winnipeg RSA Security Conference, 2001
5. Pastor V., Diaz G., Castro M., State-of-the-art simulation systems for information security education, training and awareness. IEEE EDUCON Education Engineering 2010 – The Future of Global Learning Engineering Education, April 2010, Madrid, Spain
6. Wilensky, U. (1999). NetLogo. http://ccl.northwestern.edu/netlogo/
7. N. Ben-Asher and C. Gonzalez (2015), CyberWar Game: A Paradigm for Understanding New Challenges of CyberWar. Chapter in: Cyber Warfare - Building the Scientific Foundation, Advances in Information Security, Vol. 56, Springer
8. Flipping the Economics of Attacks (2016), Ponemon Institute© Research Report
9. Global Cyber security Index 2017, ITU 2017
10. Bologna, J., MOMM's (Motivations, Opportunities, Methods, Means) - A Taxonomy for Computer Related Employee Theft, Journal of Assets Protection 6 (3): 33-36), May/June 1981
11. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. Journal of Psychology. 91: 93–114