I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

I have followed a research plan that, along with the suggestions of my scientific coordinator, would fit to the research programme prepared since the beginning of this fellowship.

I started with the literature review in the field of Behavioral Economics of Information Security, in order to elaborate the need for further research on this field. I conducted this review mainly in the first months of this fellowship, but I have been continuously reading further in the remaining period as well.

Then, I started to create the conceptual framework and build the first tentative artefact. It was back then when I first started to work on the simulation tool, which was chosen as the right approach to fulfill the objectives of this research.

The artifact has been redesigned, improved and tested with different groups of users, and is still a work in progress. The ongoing work around the tool has been successful enough to help me and my colleagues here publish several papers, 4 of them already accepted in international scientific events, with more papers pending review in the following months.

II – PUBLICATION(S) DURING YOUR FELLOWSHIP

Accepted papers

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.


Abstract.
We hardly pass any day without hearing of a new cyber-attack. The recent ever-increasing occurrence of such attacks has given to researchers, practitioners and others an opportunity to raise awareness and train staff from the public and private institutions, as well as other people within the society, about the evolving nature of cyberspace threats. As a first step in this process, we aim to present main findings from a pilot study conducted with a target group of Master students with diverse backgrounds and knowledge about cyber security practices.

The study was done using an agent-based simulation tool, CyberAIMs as the core component of the experiment. Students were involved in a pre-test/post-test study in order to assess the probable change in their thinking process after using CyberAIMs. A scenario created from a real cyber case was additionally used to get the participants accustomed to the tool. The experiment is still in progress, while preliminary data indicate that there is a shift in students' perspective on the most relevant attributes affecting defense agents' performance, results that could be related to both adversarial and systems thinking processes.


Abstract.
CyberAIMs stands for Cyber Agents’ Interactive Modeling and Simulation. We designed this tool in order to use it as an educational tool to teach Master students in a Cyber security course. This paper aims to describe the model and explain the design choices behind CyberAIMs in terms of associating them with the emerging concepts within cyber security curriculum, namely adversarial and systems thinking. The preliminary results indicate that the current distribution of values and entities allows most of the defense agents to avoid losing all their resources to their attack counterparts. We intend to use this tool as part of a lab with students in Information Security and further extend our target users, by including others who need training in adversarial and systems thinking. We conclude by providing rough results from running simulations with the tool and giving further directions of our future research, in order to improve the usability and level of detail for this tool.

Selected references


Selected references
Pending papers

III – ATTENDED SEMINARS, WORKHOPS, CONFERENCES

Conferences
1. EU – Health in Horizon 2020 conference, 16 January 2018, Oslo, Norway
2. 30th International Conference on Advanced Information Systems Engineering, CAISE'2018, 11-15 June 2018, Tallinn, Estonia

Workshops
1. ICR2018: 4th Interdisciplinary Cyber Research workshop, 9th of June, 2018, Tallinn, Estonia
2. 14th International Workshop on Enterprise & Organizational Modeling and Simulation, June 11th-12th, 2018, Tallinn, Estonia
3. 4th International Workshop on Socio-Technical Perspective in IS development, June 11-12th, 2018, Tallinn, Estonia
4. The 8th International Defence and Homeland Security Simulation Workshop, September 17 – 19, 2018, Budapest, Hungary

Seminars
1. NISseminar on CyberAIMs, September 14, 2018, Gjøvik, Norway

Symposiums
1. CCIS/Simula Cyber Symposium 2018, May 29, 2018, Oslo, Norway
2. The 30th European Modeling & Simulation Symposium, September 17-19, 2018, Budapest, Hungary

Other events
1. Cyber Academy, ISA CSP 2018, July 12-14, 2018, Tirana, Albania
2. Opening Ceremony of the Norwegian Cyber Range, September 4th, 2018, Gjøvik, Norway
3. Open Research Day, September 27th, 2018, Gjøvik, Norway

IV – RESEARCH EXCHANGE PROGRAMME (REP)

REP Institution: Security Lab, RISE SICS, Stockholm, Sweden
Scientific Coordinator: Shahid Raza, PhD, Director of Security Lab
Dates: September 6-12, 2018

I have had a very good experience while visiting the Security Lab in Stockholm as an ERCIM Fellow. The local coordinator and the staff were very welcoming and I was able to make several good contacts with common research interests.