ERCIM "ALAIN BENSOUSSAN"
FELLOWSHIP PROGRAMME

ERCIM
European Research Consortium
for Informatics and Mathematics

Scientific Report

First name / Family name	Erjon Zoto
Nationality	Albanian
Name of the *Host Organisation*	NTNU Gjovik
First Name / family name of the *Scientific Coordinator*	Stewart James Kowalski
Period of the fellowship	01/10/2017 to 30/09/2018

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

1. Zoto, Erjon, Kowalski, Stewart J., Lopez-Rojas, Edgar A. and Kianpour, Mazaher, (2018), Using a socio-technical systems approach to design and support systems thinking in cyber security education, Proceedings of the 4th International Workshop on Socio-Technical Perspective in IS development, STPIS'18, June 2018 online proceedings at link: http://ceur-ws.org/Vol-2107/Paper11.pdf)

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.

2. Zoto, Erjon, Kowalski, Stewart J., Frantz, Christopher, Lopez-Rojas, Edgar A. and Katt, Basel, (2018), A Pilot Study in Cyber Security Education using CyberAIMs: A Simulation-Based Experiment, Proceedings of the 11th IFIP WG 11.8 World Conference on Information Security Education, WISE 11, Poznan, Poland

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.

3. Zoto, Erjon, Kowalski, Stewart J., Katt, Basel, Frantz, Christopher, and Lopez-Rojas, Edgar A.,(2018), CyberAIMs: A tool for teaching adversarial and systems thinking, Proceedings of the International Defence and Homeland Security Simulation Workshop 2018, ISBN 978-88-85741-12-6; Bruzzone and Sottilare Eds., Budapest, Hungary

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

1. Lillian Ablon, Martin C Libicki, and Andrea A Golay. Markets for cybercrime tools and stolen data: Hackers' bazaar. Rand Corporation, 2014.
2. E Anne Bardoel and Tim Haslett. Success to the successful: The use of systems thinking tools in teaching ob. Organization Management Journal, 1(2):112–124, 2004.
3. Noam Ben-Asher and Cleotilde Gonzalez. Cyberwar game: A paradigm for understanding new challenges of cyber war. In Cyber Warfare, pages 207–220. Springer, 2015.
4. J Bologna. Momm's (motivations, opportunities, methods, means)-a taxonomy for computer related employee theft. Assets Protection, 6(3):33–36, 1981.
5. S Brahima. Global cybersecurity index 2017. International Telecommunication Union (ITU), pages 1–77, 2017.

6. Barbara Filkins and GM Hardy. It security spending trends. A SANS Survey. SANS Institute, 2016.
7. Seth T Hamman, Kenneth M Hopkinson, Ruth L Markham, Andrew M Chaplik, and Gabrielle E Metzler. Teaching game theory to improve adversarial thinking in cybersecurity students. IEEE Transactions on Education, 60(3):205–211, 2017.
8. Joint Task Force on Cybersecurity Education. Cybersecurity curricula 2017 – curriculum guidelines for post-secondary degree programs in cybersecurity - csec2017 v. 0.95 draft. Technical report, November 2017.
9. Vicente Pastor, Gabriel Díaz, and Manuel Castro. State-of-the-art simulation systems for information security education, training and awareness. In Education Engineering (EDUCON), 2010 IEEE, pages 1907–1916. IEEE, 2010.
10. Ponemon Institute. Flipping the economics of attacks. Technical report, January 2016.
11. Marc Rogers. A new hacker taxonomy. University of Manitoba, 2000.
12. Ronald W Rogers. A protection motivation theory of fear appeals and attitude change1. The journal of psychology, 91(1):93–114, 1975.
13. Fred B Schneider. Cybersecurity education in universities. IEEE Security & Privacy, 11(4):3–4, 2013.
14. Vijay Vaishnavi and William Kuechler. Design research in information systems. 2004.
15. Uri Wilensky. Netlogo. evanston, il: Center for connected learning and computer-based modeling, northwestern university, 1999.

4. Lopez-Rojas, Edgar A., Gultemen, Dincer, Zoto, Erjon, (2018), On the GDPR introduction in EU and its impact on Financial Fraud Research, Proceedings of the European Modeling and Simulation Symposium, 2018, ISBN 978-88-85741-03-4; Affenzeller, Bruzzone, Jiménez, Longo, Merkuryev and Piera Eds., Budapest, Hungary

Selected references

1. Claudio Reginaldo Alexandre and João Balsa. A multiagent based approach to money laundering detection and prevention. In International Conference on Agents and Artificial Intelligence, number April 2016, pages 230–235, 2015. doi: 10.13140/2. 1.2227.2327.
2. The Norwegian Data Protection Authority Datatilsynet. Artificial intelligence and privacy. Technical report, Datatilsynet, The Norwegian Data Protection Authority, 01 2018.
3. Chrystel Gaber, Baptiste Hemery, Mohammed Achemlal, Marc Pasquet, and Pascal Urien. Synthetic logs generator for fraud detection in mobile transfer services. In 2013 International Conference on Collaboration Technologies and Systems (CTS), pages 174–179. IEEE, may 2013. ISBN 978-1-4673-6404-1. doi: 10.1109/CTS.2013.6567225.
4. Dan Gorton. IncidentResponseSim: An agent-based simulation tool for risk management of online Fraud. In Sonja Buchegger and Mads Dam, editors, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), volume 9417 of Lecture Notes in Computer Science, pages 172–187, Cham, 2015. Springer International Publishing. ISBN 978-3-319-26501-8. doi: 10.1007/978-3-319-26502-5.
5. Dave Lewis, Joss Moorkens, and Kaniz Fatema. Integrating the management of personal data protection and open science with research ethics. In Proceedings of the First ACL Workshop on Ethics in Natural Language Processing, pages 60–65, 2017.
6. Edgar Lopez-Rojas and Stefan Axelsson. Multi agent based simulation (mabs) of financial transactions for anti money laundering (aml). In Audun Josang and Bengt Carlsson, editors, Nordic Conference on Secure IT Systems, pages 25–32, Karlskrona, 2012a.
7. Edgar Lopez-Rojas, Dan Gorton, and Stefan Axelsson. Using the RetSim simulator for fraud detection research. International Journal of Simulation and Process Modelling, 10(2):144, 2015.
8. Edgar Alonso Lopez-Rojas and Stefan Axelsson. Money Laundering Detection using Synthetic Data. In Julien Karlsson, Lars ; Bidot, editor, The 27th workshop of (SAIS), pages 33–40, Örebro, 2012b. Linköping University Electronic Press.
9. Edgar Alonso Lopez-Rojas and Stefan Axelsson. Social Simulation of Commercial and Financial Behaviour for Fraud Detection Research. In Advances in Computational Social Science and Social Simulation, Barcelona, 2014. ISBN 9789172952782.
10. Edgar Alonso Lopez-Rojas and Stefan Axelsson. Using the RetSim Fraud Simulation Tool to set Thresholds for Triage of Retail Fraud. In 20th Nordic Conference on Secure IT Systems, NordSec 2015, pages 156–171, Stockholm, 2015. Springer.

Pending papers

1. Lopez-Rojas, Edgar A., Zoto, Erjon, (2018), Triple Helix approach for Anti-Money Laundering (AML) Research using Synthetic Data Generation Methods
2. Zoto, Erjon, Kowalski, Stewart J., Katt, Basel and Frantz, Christopher, (2018), A Simulation Model for Teaching Adversarial and Systems Thinking

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
3. The 15th International Multidisciplinary Modeling & Simulation Multiconference, I3M 2018, 17-19 September 2018, Budapest, Hungary

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.