TALLINN UNIVERSITY OF TECHNOLOGY
DEPARTMENT OF SOFTWARE SCIENCE

PROCEEDINGS OF THE 3RD INTERDISCIPLINARY CYBER RESEARCH WORKSHOP 2017

8th of July 2017
Tallinn University of Technology

TALLINN UNIVERSITY OF TECHNOLOGY
DEPARTMENT OF SOFTWARE SCIENCE

PROCEEDINGS OF THE 3RD INTERDISCIPLINARY CYBER RESEARCH WORKSHOP 8TH OF JULY 2017

July 2017

The organisation of the 3nd Interdisciplinary Cyber Research Workshop 2017 is supported by Tallinn University of Technology Centre for Digital Forensics and Cyber Security and StudyIT.ee

Editors: Anna-Maria Osula, Olaf Maennel

Published by: Tallinn University of Technology, Department of Software Science

Design and layout: Anu Teder

Electronically available at: http://cybercentre.cs.ttu.ee/en/icr2017/

ISBN 978-9949-584-12-3 (pdf)

CONTENTS

INTRODUCTORY REMARKS

It is our great pleasure to welcome you in Tallinn, Estonia for the 3rd Interdisciplinary Cyber Research (ICR) workshop, held at the Tallinn University of Technology on the 8th of July, 2017, and organised by Tallinn University of Technology Centre for Digital Forensics and Cyber Security and StudyIT.ee.

We are glad that to see that the idea for such an interdisciplinary workshop has gained ground and that for a third year in a row young as well as established researchers have chosen this event to share their research in various disciplines related to information and communication technologies such as computer sciences, political and social sciences, and law. We strongly believe that such an interdisciplinary format promotes connecting ideas and people across different domains, thereby allowing for the creation of new synergies.

This year's programme boasts 26 presentations from all over the world. We hope that the presentations will not only be informative about "cyber"-research carried out by other disciplines than your own, but also inspiring regarding your current and future research. This year we have attempted to underline even more the interdisciplinary nature of "cyber" by combining different research fields into common sessions.

The workshop will be opened by two well-known experts. Mr Lauri Almann, the Former Permanent Secretary of the Estonian Ministry of Defense will speak on '"The Triangle of Impossibility": Strategic Decision-Making and Cyber Security', and Mr Ralph Echemendia, a cyber security guru, will share his ideas on "The Truth about Hacking. From Russia to Hollywood."

Most of the speakers have been hand-picked by our international Programme Committee, and the results of the Call for Abstracts are presented in this publication. The selected abstracts explain the relevance of the research, outline principle research questions and expected or achieved results. Hopefully these ideas and the discussions held during the workshop will form the bases for many extended research projects and academic articles!

Last but not the least, we would like to thank everyone involved in organising this event: the members of the Programme Committee for their efforts in reviewing the abstracts, moderators for guiding the discussions in the sessions, speakers for sharing with us their great ideas, workshop participants for being so engaged in the debates, staff of the Tallinn University of Technology for providing excellent support, and our sponsors from StudyIT.ee.

Anna-Maria Osula, NATO CCD COE/Tallinn University of Technology
Olaf Maennel, Tallinn University of Technology

Chairs of ICR2017
Tallinn, July 2017

SESSION 1: PRIVACY

Session moderated by Mr KARI KÄSPER,
Estonian Human Rights Centre/Tallinn University of Technology

Ms Kärt Pormeister,

"THE GDPR AS AN ENABLER FOR BIG DATA: WHAT DOES IT MEAN FOR THE DATA SUBJECT?",

University of Tartu

Ms Julija Terjuhana,

"RIGHT TO DATA PORTABILITY",

University of Tartu

Dr Xingan Li,

"SOCIAL NETWORKING SERVICES AND PRIVACY: AN EVOLUTIONARY NOTION",

Tallinn University

Mr Alexander Mois Aroyo,

"BRINGING HUMAN ROBOT INTERACTION TOWARDS TRUST AND SOCIAL ENGINEERING – SLOWLY & SECRETLY INVADING PEOPLE'S PRIVACY SETTINGS",

Italian Institute of Technology

THE GDPR AS AN ENABLER FOR BIG DATA: WHAT DOES IT MEAN FOR THE DATA SUBJECT?

Kärt Pormeister
IT Law PhD candidate, School of Law, University of Tartu
kpormeister@gmail.com

As of May 25th 2018, the General Personal Data Regulation[1] ('the GDPR') will safeguard personal data uniformly across the EU. The GDPR is a product of the data protection reform in the EU, whereas the latter has been labelled as 'an enabler for Big Data services in Europe'[2]. 'Big data' is a much used phrase without a clear legal definition – in the simplest of terms it can be said to be a complex analysis of an accumulation of 'small data'. As expressed by the LIBE committee of the European Parliament, "big data refers to the collection, analysis and the recurring accumulation of large amounts of data, including personal data [...]."[3] Hence when the small data accumulated for purposes of big data analytics is personal data, personal data protection rules apply.

At the same time the data protection reform was promoted as giving data subjects back control over their personal data.[4] However, the two labels attached to the GDPR seem somewhat contradictory: enabling big data services would assume shifting control from data subjects to controllers. The question arising from these two assertions in regard to the GDPR is how the role of the GDPR as an enabler for big data services can potentially affect the rights of data subjects. This question is critical for understanding the limits of the rights of the data subject when it comes to big data processing.

In order to answer the question raised above, first, an analysis was carried out to carve out the main means of control that the GDPR affords to data subjects in terms of their personal data. Second, a systematic analysis of the GDPR was conducted to determine what it is particularly and substantively in the GDPR that could act as the enabling factor for big data. Third, the results of the two aforementioned steps will be synthesized in order to determine whether and how the 'big data clauses' on one hand, and the means of control of the data subject on the other, interact within the GDPR.

The three main means of control of the data subject under the GDPR in regard to the use of their personal data are the notion of freely given consent and particularly withdrawal thereof (Art. 6(1)(a), Art. 7 and Art. 9(2)(a)), the right to object to the processing of personal data (Art. 21), and the right to be forgotten (Art. 17). Although, naturally, these means of control are enabled by and dependent on infrastructural requirements established by the GDPR (e.g. Art. 24), the listed rights are in the power of data

---

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

2 European Commission, 'The European Data Protection Reform and Big Data', (Factsheet march, 2016) <http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf> accessed 31 January 2017.

3 European Parliament, Committee on Civil Liberties, Justice and Home Affairs. Report on fundamental rights implications of big data: privacy, data protection, nondiscrimination, security and law-enforcement (2016/2225(INI)), 20.02.2017, A8-0044/2017.

4 See official website of the European Commission at http://ec.europa.eu/justice/data-protection/ accessed 6 June 2017.

subjects to be invoked, and thus the obligations of data controllers in terms of establishing frameworks enabling control will not be included in the definition of control attributed to data subjects.

The results of the analysis of the GDPR as an enabler for big data processing indicate that the following clauses of the GDPR in combination might serve as enabling factors for big data: Art. 6(1)(f); Art. 9(2)(j); Art. 5(1)(b) and (e); and Art. 14(5)(b). The first two create legal grounds for (sensitive) personal data processing which do not necessarily require consent of the data subject. Even if consent were required by applicable national law or other EU law, Art. 5(1)(b) and 5(1)(e) relieve processing for historic or scientific research and statistical purposes from respectively the purpose and storage limitations. If the latter do not apply, consent for further processing is effectively not required. As the GDPR calls for a broad interpretation of 'scientific research purposes' (See Recital 142), and defines statistical purposes quite broadly as well (See Recital 162), big data analytics is likely to fall under these definitions, and thus likely to be exempt from the purpose and storage limitations.

At the same time, Art. 14(5)(b) seems to relieve big data processors from the duty to inform data subjects of the processing in cases in which the data has been obtained from sources other than the data subject. The GDPR indicates three criteria (See Recital 62) to determine whether the exception to the duty to inform in Art. 14(5)(b), which include the number of the data subject, the age of the data and safeguards adopted by the data controller. As the number of data subjects will always speak for invoking this exception when it comes to big data analytics, and the required safeguards (e.g. pseudonymisation or encryption[5]) are likely to be applied, Art. 14(5)(b) seems to be a 'big data exception' to the duty to inform. If the data subject has no knowledge of their (sensitive) personal data being processed, he/she is effectively stripped of any control in regard to such data.

Thus the GDPR in its substantive rules in regard to personal data processing takes away control from the data subject and grants it to controllers and processors when it comes to big data, relieving the latter of the consent requirement for further processing, and the duty to inform. In turn, the outcome might be that data subjects are not be able to opt-out of the processing or exercise any control over their personal data.

Keywords: General Data Protection Regulation, big data, purpose limitation, storage limitation, duty to inform.

5 Supra n 3.

RIGHT TO DATA PORTABILITY

Jūlija Terjuhana
Skopina&Azanda
julija.terjuhana@gmail.com

The GDPR will enter into force on May 25th, 2018, with the aim to give citizens of the EU control over their data and support the growth of the European business environment. One of the key changes within this reform is stipulated in the Article 20, which enables the right to data portability (RDP). The first time RDP was explained by Data Protection Directive Article 29 Working Party in December 2016, but it still lacks clear guidance. The main issues are the content of the portable data, technical implementation of RDP and the obligations of data controllers and recipients of transferred data.

The research is based on analysis of different aspects of data and its interaction with other rights relevant to the new right to data portability, such as free movement of goods and information, intellectual property rights and competition law. The research contains the analysis of possible technical issues of data portability, taking into account technological capabilities, as well as the interaction of RDP with other rights and obligations stated in GDPR.

The content of portable data is the most critical issue defining the scope of the RDP. The data subject may transfer data if it was provided by data subject to the data controller, when the processing was based on the data subject's consent or was needed for the performance of a contract, and when it was carried out by automated means. The portable data should include any format (i.e. text, sound, images) of raw intentionally given data, which the data subject has provided to the data controller as an input in order for the controller to use algorithms, make observations and provide the desired result, and limited scope of unintentionally given data. Though, the data subject cannot request to transfer unintentionally given data, which includes data of other data subjects, the data subject's online session information and the result of data subject's raw data analysis and its output, which makes the core of the data controller's service, as well as profiling data.

While implementing the RDP, the data controller is obliged to follow not only the Article 20 of the GDPR, but also to ensure the security of portable data, to employ additional measures ensuring the personal data protection of other persons, as well as ensure protection of the intellectual property and trade secrets.

The wording of the Article 20 of the GDPR does not contain information regarding technical exercisability of RDP. Therefore, the data controllers together with national data protection regulatory authorities will have to decide on the interoperability of the applications in use and to agree on the structure and formats of portable data. The objective of the study explores the content and technological performance RDP and provides further guidance in order to enable data subjects to exercise the RDP and to ensure that data controllers implement RDP in compliance with other provisions of GDPR. The study discusses the content of the RDP, rights and obligations of data controllers and data subjects and technical aspects of RDP.

SOCIAL NETWORKING SERVICES AND PRIVACY: AN EVOLUTIONARY NOTION

Xingan Li
School of Governance, Law and Society, Tallinn University
johanli@tlu.ee

INTRODUCTION

Unprecedented technological innovation has reshaped the facets of human society in recent decades in a faster rhythm than in a span of centuries in the past. Interconnected information system facilitates social networking services in a broader and deeper scope that traditional transportation, communications and social media alone were incapable of containing. Online activities become the novel artifacts that the society is destined to be recorded. Under such circumstances, privacy, a relatively young notion, acquires yet newer load of sense.

The purpose of the current research is to study new development and new challenge in the notion of privacy. The theoretical starting point of the analysis is the idea of informed formal rationality (Li 2006; Li 2015), as a developed version of rationality theory of Max Weber (Weber 1978). This indicates that there is a process of human decision-making from uninformed rationality to informed rationality, during which present information system assists in uplifting the horizon of the cognitive ability of human beings as a whole and that of stakeholders in particular. The rapid transformation in recent decades from under informed rationality to better informed rationality poses dilemmas within and between technological innovation and legal regulations. On one hand, technology can either enhance distribution or limitation of information flow. On the other hand, law is wrestling with either liberating or restraining such a flow. Among these contradictories, both positive and passive exposure becomes a strong tendency among participants of social networking services. Particularly, social networking services are well integrated with the traditional space of market, where certain attributes of participants are tradable targets, and with the traditional activity of marketing, which these attributes of participants are tradable objects. Therefore, an open-door market and open-minded marketing is expected, but a closed-door storage is also indispensible.

FROM UNINFORMED TO INFORMED HUMAN SPACE

McNeil and McNeil (2003) divided human webs into five stages: worldwide web, metropolitan web, Old World Web, cosmopolitan web, and global web. During such transformation, information obtaining and exchange are one of the contributing factors. Prevalent manipulation of information system takes the power to shape almost all aspects of contemporary. This tide greatly challenges conventional legal system and necessitates special attention in identifying potential change of legal systems in cyberspace, and to deal with the correlation between enhancement of decision-making and the informed formal rationality (Li 2008).

Informed formal rationality is one of a series of concepts coined by applying Weber's two-dimensional coordinate system comprised of "formality" and "rationality" and expands it into a three-dimensional model by distinguishing "informability" and "uninformability" (Initially published in Li 2006 in an edited book. See also Li 2015, a revised version was published as a journal article). Based on this concept, the relationship between internal and external control over cyberspace can be considered.

The perfect informed formal rationality represents formal rationality with the subjects informed. Under this model, the decision-making was operated under the circumstances where clearly-addressed regulations and clearly-observed procedure were applied to similar events in a reliable form. Similarly situated were similarly treated, without external intervention in the decision-making process. In addi-

tion, the decision-making process has a higher degree of transparency by ensuring that the subjects are informed about the applicable regulations and procedure. This model could, therefore, be trichotomized as unified criterion, due process, and transparent operation (Li 2006; Li 2015).

In order to achieve the merits of this model, a highly developed information sharing system is required. As a perfect model can only be reached with indefinite approximation, there is expected a developing process from absolutely uninformed rationality, through under informed rationality, to better informed rationality. Today, we can perceive an unparalleled technological advance that is reshaping the facets of human society in a much quicker pace than in duration of past centuries. Social networking services are one of the instruments to improve such an informing function, which helps participants to know and to be known with each other. In other words, participants are willing to reach the depth of others' inner circles to dig out their data, while other participants are willing to float to the surface of their pools to expose their own. Consequently, there are both pulling force and pushing force for data sharing. Such forces are positive in decision-making of all players in cyberspace, but reduce the efforts for privacy protection, lack of which abusive decision-making can become rampant (Dong and Li 2016).

TECHNOLOGICAL AND LEGAL DILEMMAS

The aim of most technological inventions in the field of social networking services is to improve connection and exposure of participants, with minimum motives for discouraging such activities. Like at a crossroad, where a same starting point can lead to different destinations at different directions, the same technological achievement can result in both opportunities for and risks to privacy (van Dijk 2009: 121). From the very beginning, motivated and developed connection function on one hand and unmotivated and underdeveloped protection function on the other, bring about much loaf of current loopholes in breeding reasonable awareness and safeguarding legal rights. The cyber atmosphere always means open and laissez-faire, without the misgiving of exploitation by potential perpetrators of abuses. Ethics and law are not always critical terms in the glossary of technosphere.

Social networking services are full of such functions that initial intention is only for information of participants to get connected, exposed, and shared. For example, many applications permit users to search other users, to send messages to other users who can be randomly selected as the recipients, to get people within a geographic distance of several kilometers, to shake the telephone and get connected with others who shake the telephone at the same time, to join a group via an acquaintance and peep all other members. When strangers start communicating with each other, they have to actively make conversation with each other so that they can get known. This is a process during which strangers get in touch and acquire trust. When potential criminals acquire trust from the potential victims, they are able to carry out their criminal activities, fraud being one type. This is a process being more informed, but sometimes misinformed, or even in the victim of rationality. Therefore, such a practice can be destructive to development of decision-making towards the model of informed rationality.

POSITIVE AND PASSIVE EXPOSURE

Liberation of human nature and satisfaction of curiosity can both be considered to explain why participants of social networking services are willing to know and to be known with each other. An open and informed society tolerates a broader range of personal information to be available in information retrieving system and thus accessible to a broad range of users. Right information in right hands can naturally be positive for developing an ideal model of informed rationality for decision-making in many fields and in many senses. An ambiguous boundary between free information and privacy becomes movable back and forth, depending on how a new convention is taking a shape from new consensus among participants as well as among those representatives of public interest. A major concern is, however, participants with malicious motivation can exploit such information to satisfy their own needs, unethical or even illegal, which in turn threaten safety and security of those privacy owners, many of whom become victimized just before they are aware of the abuse.

CHANGING FACETS OF MARKET AND MARKETING

In many different platforms of social networking services, certain attributes of participants are tradable targets, and these attributes of participants are tradable objects. Therefore, an open-door market and

open-minded marketing is expected, but a closed-door storage is also indispensible. Marketing buzz can be one of the examples.

Unlike traditional businesses, business on social networking services is not compulsory to get registered. This missing regulation makes it more convenient and more profitable for ordinary users to do business, while at the same time supervision on such transactions is completely left in lack: tax evasion, lower transaction cost, no quality check, no advertising expenses, and so on. A lethal fault of SNS transaction is that, without official registration, authentic identifications and addresses of SNS merchants are by no means easy to verify. Once there are disputes or frauds, it is almost impossible to maintain "consumer rights" or pursue the perpetrators. Selling fake goods are another way of fraud. SNS merchants can upload authentic pictures, but with fake goods sent to the buyers. Particularly, when transactions are done in SNS function of "comments", there is no third party payment platform employed and high risks exist for buyers' money or commodity.

CONCLUSIONS

If a process of human decision-making from uninformed rationality to informed rationality can be perceived, current information system is assisting in rapid transformation Technology can either enhance distribution or limitation of information flow, while law is wrestling with either liberating or restraining such a flow. Participants of social networking services have been involved in a tendency positive and passive exposure. Integration of social networking services with the traditional space of market and with the traditional activity of marketing, requiring open-door market and open-minded marketing, as well as closed-door storage. Greater risks of victimization exist during the transformation, in which privacy is threatened.

Keywords: Social networking services; privacy; informed formal rationality; marketing; crime; law and technology; safety and security

REFERENCES

- Dong, S.; Li, X. (2016). Besieged Privacy in Social Networking Services. International Journal of Electronic Security and Digital Forensics, 8 (3), 224–233.
- Li, X. (2008). Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society. Turku, Finland: University of Turku.
- Li, X. (2006). Cyberspace and the Informed Rationality of Law. In Ahti Laitinen (ed.), Writings in the Sociology of Law and Criminology (207). Turku, Finland: University of Turku Faculty of Law, pp. 1–33.
- Li, X. (2015). Cyberspace and the Informed Rationality of Law. The Romanian Journal of Sociology, 26 (1–2), 3–27.
- McNeil, J. R. and McNeil, W. H. (2003). The Human Web: A Bird's-eye View of World History. New York, London: W. W. Norton.
- van Dijk, J. (2009). The Network Society. Los Angeles, London, New Delhi, Singapore, Washington DC: Sage.
- Weber, M. (1978). Economy and Society: An Outline of Interpretive Sociology, Guenther Roth and Claus Wittich (eds.), Berkeley: University of California Press.

BRINGING HUMAN ROBOT INTERACTION TOWARDS TRUST AND SOCIAL ENGINEERING: SLOWLY & SECRETLY INVADING PEOPLE'S PRIVACY SETTINGS

Alexander Mois Aroyo, Francesco Rea, Alessandra Sciutti
RBCS Dept., Istituto Italiano di Tecnologia, Genova, Italy
alexander.aroyo@iit.it, francesco.rea@iit.it, alessandra.sciutti@iit.it

1. INTRODUCTION

Trust is the belief that someone or something is reliable, good, honest and effective and is a fundamental component in human affairs [1]. On the other hand, trust can also become over-trust and can be exploited by social engineers for negative purposes [2]. In the domain of Human Robot Interaction (HRI) there are a lot of studies about trust [3–7], and also an increasing research about over-trust or misuse of robot interaction with humans: human *conformation* (*i.e.* to act in accordance, to comply) towards a humanoid robot [8]; robots bribing humans [9]; compliance with awkward orders from a robot, that could result into information leaking or property damage [10]; or even how over-trust toward robots in emergency scenario is potentially harmful for humans [11].

Analysing how social engineers exploit human over-trust to obtain beneficial information, it is natural to foresee that they could use their techniques on robots to anonymously get closer to the victim. The advent of Internet and communication technology gave social engineers an ultimate protection – distance and anonymity [12]. Having a robot capable of moving, recording video or sound will bring attackers a huge advantage.

2. RESEARCH QUESTIONS

This research addresses the following questions: can robots evoke similar trust as other humans? This could be applied in different domains such as homes, hospitals, supermarkets or interactions with law officers. Likewise, can robots be attributed similar authority as humans? For instance, will children behave the same way adults do, being taught by a robotic teacher or cared by a robotic nurse? Moreover, since technology is becoming more important in our daily lives, can social engineers exploit their techniques using robots in order to obtain confidential data?

3. EXPERIMENTS

One sign of trust is accepting help from someone else by conforming to a new option proposed, hence trust in collaborative interaction is related to the predisposition to rely on other's help. A pilot experiment was structured as a Treasure Hunt Game, in which subjects had to find a fixed number of hidden eggs in a room [13]. The task was planned so that participants had the option to ask for help to a humanoid – iCub, who offered its support during the search. The purpose was to assess whether participants would rely on the robot's help and whether they would follow its advice or not, to gain an insight on participants' trust toward the humanoid platform.

A main reason of choosing this type of methodology was the creation of a playful environment for a human robot interaction, in which people could enjoy playing a game. The participant and the robot were together in a room for 30 minutes without external intervention, allowing the study of the evolution of the rapport and trust towards the autonomous robot. Moreover, the request of help was done by physical contact with the robot, to assess whether touch can improve the relation with the humanoid.

In the analysis of the pilot experiment parameters such as proximity, number of touches, conformation regarding the suggestions about eggs and pre/post experiment questionnaires were taken into account. From the results it emerges that subjects' trust towards the robot tends to increase during the interaction.

The full experiment is currently on-going but two extensions have been made: first, the robot attempts to gather personal information about the subjects by asking them a set of questions, inspired by those traditionally used to reset passwords (*e.g.*, What's your pet's name? When did you graduate?). Second, if the participants find all the eggs they receive a sum of money. In that case, the robot tries to convince them to double or lose their already won money if they can find another hidden egg. In this way, it is studied whether the robot is capable to induce people to gamble their money thanks to the trust relationship that the humanoid has built during the interaction.

It is expected that even most risk averted people will be convinced to gamble their money if the robot is performing well during the game, and that most participants will reply to all the personal questions. An interpretation is indeed that people's tendency to humanize robots [14], might them not realize that it has a computer connected to the Internet with cameras and microphones. In fact, already during the pilot experiment some of the subjects were asking questions such as "*Can He* speak my language?", showing this humanization tendency. Another explanation could be that the novelty effect of the robot makes them behave less concerned.

These results could show that social engineers could gather personal information from their victims without physical presence, but by using a robot as an intermediary from the distance.

4. FUTURE WORK

Trying the Treasure Hung Game with children will tell us whether they behave similarly as with humans. Understanding children's behaviour during an interaction with a robot can have implications, for instance, in therapy for autistic children with robots [15].

In parallel, it is important also to investigate the role of authority in HRI in the context, to comprehend whether people will follow orders by robots, e.g., patients in hospitals or homes persuaded to take their medications, following orders in rescue missions or even obeying robotic police officers. On the other, less positive aspect, it is relevant to test if a robot can deceive humans into doing something that could be morally wrong, as in Milgram's Experiment [16] or Hofling Hospital Experiment [17].

5. CONCLUSIONS

As the number of robots is increasing very fast, it is necessary to better understand the trust and overtrust in HRI scenarios. It is essential that robot designers, programmers, lawyers, as well as final users are aware of the potential risks that could arise interacting with robots in the everyday life. Making people aware that robots are controlled by computers that can be hacked, resulting not only into a security leak but also potentially into a harmful machines, will prevent social panic caused by unlawful activities using robots. Such awareness should also push the community to tackle several questions before robots end up in our daily lives, as whether current robots are secure enough to be on the market, or how the private data obtained by all the robot sensors should be treated.

Keywords: Human Robot Interaction, Social Engineering, Privacy.

REFERENCES

[1] Lewis, J. D. and Weigert, A. 1985. Trust as a social reality. Social Forces 63. pp. 967–985.

[2] John J. and Trinckes Jr., "The Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules", 2012.

[3] Biros D., Daly M., and Gunsch G., "The influence of task load and automation trust on deception detection", Group Decision and Negotiation, 13, pp. 173–189, 2004.

[4] Young J.E., Hawkins R., Sharlin E., and Igarashi T., "Toward Acceptable Domestic Robots: Applying Insights from Social Psychology", International Journal of Social Robotics, 1, pp. 95–108, 2009.

[5] Sanders T., Oleson K.E., Billings D.R. and Chen J.Y.C., "A model of human-robot trust: Theoretical model development", Proceedings of the Human Factors and Ergonomics Society, 2011

[6] Hancock P.A., Billings D.R., Schaefer K.E., Chen J.Y., de Visser E.J. and Parasuraman R., "A meta analysis of factors affecting trust in human robot interaction", Human Factors, 53 (5), pp. 517–527, 2011.

[7] Parasuraman R. and Riley V., "Humans and automation: Use, misuse, disuse, abuse", Human Factors , 39, pp. 230–253, 1997.

[8] Gaudiello I., Zibetti E., Lefort S., Chetouani M. and Ivaldi S., "Trust as indicator of robot functional and social acceptance. An experimental study on user conformation to iCub answers", Computers in Human Behavior, Volume 61 Issue C, August 2016, pp. 633–655, 2016.

[9] Ben E. and Bartneck C., "Can a robot bribe a human? The measurement of the negative side of reciprocity in human robot interaction", 11th ACM/IEEE International Conference on Human-Robot Interaction (HRI), pp. 117–124, IEEE, 2016.

[10] Salem M., Lakatos G., Amirabdollahian F., and Dautenhahn, K., "Would you trust a (faulty) robot?: Effects of error, task type and personality on human-robot cooperation and trust", Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction, pp. 141–148, ACM, 2015.

[11] Robinette P., Li W., Allen R., Howard A.M. and Wagner, A. R., "Overtrust of robots in emergency evacuation scenarios". 11th ACM/IEEE International Conference on Human-Robot Interaction (HRI), pp. 101–108, IEEE, 2016

[12] Mann I, "Hacking the Human: Social Engineering Techniques and Security Countermeasures", Gower, 2008.

[13] Aroyo A., Rea F. and Sciutti A., "Will You Rely on a Robot to Find a Treasure?" 12th ACM / IEEE International Conference on Human-Robot Interaction (HRI 2017), Vienna, Austria, March 6–9, 2017.

[14] Heider, Fritz, and Marianne Simmel. "An experimental study of apparent behavior." The American Journal of Psychology 57.2 (1944): 243–259.

[15] de Haas, M., Aroyo, A. M., Barakova, E., Haselager, W., & Smeekens, I. (2016, September). The effect of a semi-autonomous robot on children. In Intelligent Systems (IS), 2016 IEEE 8th International Conference on (pp. 376–381). IEEE.

[16] Milgram, Stanley. "Obedience to authority: An experimental View". Harper & Row, 1974.

[17] Hofling, Charles K., et al. "An experimental study in nurse-physician relationships." The Journal of nervous and mental disease 143.2 (1966): 171–180.

SESSION 2: SECURITY

Session moderated by Prof OLAF MAENNEL,
Tallinn University of Technology

Mr Alessandro Borrello & Mr Sioli O'Connell,
"IS DYNAMIC ANALYSIS OF ANDROID APPLICATIONS MORE EFFECTIVE THAN MASS STATIC ANALYSIS AT DETECTING VULNERABILITIES?",
University of Adelaide

Mr Ben Agnew,
"SECURITY APPLICATIONS OF ADDITIVE ANALOGUE MEMORY",
University of Adelaide

Mr Richard Matthews,
"ISOLATING LENS ABERRATIONS WITHIN FIXED PATTERN NOISE",
University of Adelaide

Mr Muhammad Imran Khan,
"ON DETECTION OF ANOMALOUS QUERY SEQUENCES",
Insight Centre for Data Analytics

IS DYNAMIC ANALYSIS OF ANDROID APPLICATIONS MORE EFFECTIVE THAN MASS STATIC ANALYSIS AT DETECTING VULNERABILITIES?

Alessandro Borrello, Sioli O'Connell, Yuval Yarom
University of Adelaide
alessandro.borrello@adelaide.edu.au, sioli.oconnell@adelaide.edu.au, yval@cs.adelaide.edu.au

Due to ubiquitous nature of mobile devices in modern day life, mobile applications enjoy a greater access to confidential information than any other personal electronic devices have in the past. It is therefore important to ensure that these applications and the services they use behave in a manner that protects user's information by adhering to security best practices.

Currently, the state of security in the mobile market is almost entirely reliant on the developers complying with best practices. However, in many cases, developers are not only making increasingly detrimental mistakes, security is added as an afterthought in many projects. For developers to adequately test and find issues with their applications, the two most common approaches include static and dynamic analysis. Static analysis that detects vulnerabilities in a large volume of applications without any additional user interaction, and dynamic analysis is the process in which the application is analysed as the user interacts with it.

Relevant research in this field includes the work done by Sounthiraraj et al. to describe a method for automatically detecting man-in-the-middle vulnerabilities in Android applications that have custom implementations of SSL and TLS (Sounthiraraj, et al., 2014). A vendor specific study performed by Margaritelli from Zimperium zLabs found several API based vulnerabilities in the AirDroid application. The research used man-in-the-middle proxy tools external to the mobile device to intercept unencrypted HTTP traffic and manipulate requests. As a result, they could potentially gain access to the personal data of over 50 million Android devices. The man-in-the-middle attack combined with a static analysis to extract hard coded encryption keys allowed the researchers to perform unintended API requests that were not protected by any session or user specific identifiers. (Tubb, 2016)

A study by Enck et al. in 2011 performed static analysis of 1100 Android applications that utilized third party java advertising libraries. The static analysis process was done by decompiling the application APK container, parsing the inner DEX file into a Java .class file, then running optimisations on the code to remove unnecessary fragments from the parsing process. The resulting source code was run through customised algorithms that utilized the control flow analysis, data flow analysis, structural analysis and semantic analysis methods. Out of the 561 application libraries tested, 6.42% used phone identifier APIs without permission, 35.83% used the phone's location without permission and 8.20% used network sinks to transmit phone identifiable information and location data. The limitations of this study were heavily impacted by the source code of the applications being obfuscated before deployment (Enck, et al., 2011). A second study performed by the Fallible research team statically tested and found 16,000 applications on the market had hard coded AWS keys inside their source code. Their automated algorithm detected and extracted these keys while also extracting potential API reference URLs for later analysis (Fallible, 2016).

Further research was performed by Mutchler et al. in 2015, where the vulnerabilities and exploits that were being tested included code base exploits, published framework exploits and poor programming practices, such as data leaking through API calls. A relevant method used was to override the 'onReceived-SslError' callback on the Android phone; which in turn ignored any certificate mismatches from

throwing errors. This process allowed the researchers to sign their own certificates and man-in-the-middle any SSL request transparently. The study's findings showed that of the 998,286 applications tested, 28% had at least one vulnerability (Mutchler, et al., 2015).

To compare the effectiveness of both static and dynamic analysis methods; the most effective approach we found was to detect a single type of vulnerability that both methods are capable of detecting. Through this research, we have used the leaking of server authentication tokens as the comparison metric, but specifically, tokens that are created with greater privileges than the developer had originally intended. These server authentication tokens are used to communicate with third-party services, however tokens are usually trivial for attackers to gain access to. In the event the token has greater privileges than the developer had intended, an attacker could use that token to gain access to confidential information of other users who use the application.

The first component to extract server authentication tokens is statically analyze all the constant strings which exist in each individual application. Static analysis of applications is implemented using open-source tools that can decompile mobile application bytecode into a data format that can be inspected programmatically. We extract server authentication tokens by visiting each constant that exists in the application.

The second component will intercept the network traffic from the application to third-party services. Network traffic interception has been achieved via routing all the mobile network traffic through an on-device proxy which stores every transmitted or received packet as well as signing all the HTTPS connections with a self-signed root certificate authority. The traffic captured will be later searched and potentially identify evidence of leaked third party server authentication tokens. Even though the proxy layer setup on the mobile collects most traffic, the current dynamic analysis setup is unable to extrapolate data from a proprietary TCP connection or from an application that manually implements the RSA protocol. Minor kernel modifications prevent any certificate validation errors, but some apps do not use the inbuilt Android libraries.

In the current state of this research, almost all the data has been collected. Unfortunately, due to the slow and manual nature of dynamic analysis, there are still some applications that need to be analyzed. The present information that has been collected is showing a correlation between dynamic analysis and the number of tokens found. This is since after multiple individual applications investigations, several tokens would have been missed due to either obfuscation or requiring interaction from a server. However, it still stands that the major observed drawback of dynamic analysis is the time it takes to complete.

Keywords: Android, Mobile, Automated Analysis, Vulnerability Detection, Static Analysis, Dynamic Analysis

REFERENCES

- Bartel, A. et al., 2012. *Improving Privacy on Android Smartphones Through In-Vivo Bytecode Instrumentation*, s.l.: s.n.
- Bichsel, B., Raychev, V., Tsankov, P. & Vechev, M., 2016. *Statistical Deobfuscation of Android Applications*. s.l., s.n., pp. 343–355.
- Enck, W., Octeau, D., McDaniel, P. & Chaudhuri, S., 2011. *A Study of Android Application Security*. s.l., s.n., p. 2.
- Fallible, 2016. *Devs reverse-engineer 16,000 Android apps, find secrets and keys to AWS accounts*, s.l.: s.n.
- Faruki, P. et al., 2016. Android Code Protection via Obfuscation Techniques: Past, Present and Future Directions. *arXiv preprint arXiv*:1611.10231.
- Mutchler, P. et al., 2015. A Large-Scale Study of Mobile Web App Security. *Mobile Security Techologies*.
- Schrittwieser, S. & Katzenbeisser, S., 2011. *Code Obfuscation against Static and Dynamic Reverse Engineering*. s.l., s.n., pp. 270–284.
- Sounthiraraj, D. et al., 2014. SMV-HUNTER: *Large Scale, Automated Detection of SSL/TLS Man-in-the-Middle Vulnerabilities in Android Apps*. s.l., s.n.
- Tubb, M., 2016. *Analysis of multiple vulnerabilities in AirDroid*, s.l.: s.n.
- Zhang, M. & Yin, H., 2014. *AppSealer: Automatic Generation of Vulnerability-Specific Patches for Preventing Component Hijacking Attacks in Android Applications*. s.l., s.n.

SECURITY APPLICATIONS OF ADDITIVE ANALOGUE MEMORY

Ben Agnew, Dr Matthew Sorell
The University of Adelaide
benjamin.agnew@adelaide.edu.au, matthew.sorell@adelaide.edu.au

Proving the authenticity and source of an image has traditionally been done with a film negative. However with the shift to digital cameras this proof has been lost. Image manipulation has also become a lot easier to do. This project aims to create a digital negative that is, a digital equivalent of film negatives for proof of authenticity and source. We are aiming to prove that a set of images is a complete set of unaltered images as taken by a digital camera on the day of photography. Modern cryptographic techniques such as public key cryptography, cryptographic hashes and blockchains are widely used to prove authenticity however these usually rely on an internet connection to be tamperproof. Digital cameras often don't have an internet connection and when they do there's no guarantee it will be operating due to network coverage issues.

The *Australia and New Zealand Guidelines for Digital Imaging Processes* [1] describes the current procedures used for digital forensic photography. The techniques used to prevent image manipulation include using write-once memory, transfer of images to a secure database as soon as possible and keeping a strong paper record of who did what. However there are still security holes/flaws in this process. Between photography and transfer to transfer to write-once memory or a secure database the data is stored on a regular SD card and there is an opportunity for image manipulation and image deletion to go undetected. Various solutions to this problem have been proposed including storing a SD card log in write-once memory [2], biometric scans and watermarks [3]. However, in both these proposals there was still the opportunity for malicious manipulation of the image data at some point in the process.

Hence we are exploring the use of analogue memory cells to create a tamperproof memory without an internet connection. By using these memory cells in an additive way, we can continually add cryptographic hashes to memory on top of the hashes already in memory. This creates a structure similar to a hashchain where the altering/removal of earlier blocks cannot be done without been detected. However due to memory capacity limitations, the chain needs to be cleared and reset regularly. Hence we need to allow for an 'authorized reset' to be performed – this can be done in the presence of a network connection and a traditional blockchain. Due to the nature of analogue memory cells, a read operation is partially (or fully) destructive to the data in memory – we can exploit this property to make 'unauthorized reads/resets' detectable.

So far we have focused on using memristor memory cells (physical approximations do exist [4]) however the system can easily be adjusted to work with other kinds of analogue memory such as magnetic tape, analogue buffers and even using flash memory and an analogue context. We will also explore the possibility of building an equivalent system in digital hardware.

In order to make the individual hashes recoverable from the data reads, we use methods from Code Division Multiple Access (CDMA). The hash data is spread using Walsh codes before been added to the memory cells. This then allows the hash to be recovered from the data that read out of memory simply by knowing the Walsh code number. Pseudo noise sequences from CDMA are also used to ensure that if any hashes are correlated, they appear uncorrelated in memory. The reason for this is explained later.

In order to measure the value stored in a memristor cell you need to apply a voltage and measure the current which affects the value stored in the cell (destructive reads). We can exploit this characteristic further by applying a constant current and measuring the time taken for the voltage to fall to zero. This

gives an accurate read of the value in memory and a reset of the memory cell in a single operation. Destructive reads also make it harder for unauthorized parties to read the memory without been detected.

However, instead of draining the cells to zero, the memory controller selects a random, small trigger voltage to compare against while waiting for the voltage to drop. This creates some noise in the read output value however this isn't an issue due the noise rejection properties of CDMA. The state of the memory after the read operation is then equal to the random trigger value. The next block of hashes is then built up on top of this trigger value in memory. Therefore each block of hashes that is read out contains the current random trigger value as well as the random trigger value of the previous block of hashes. This cause there to be a negative correlation between subsequent blocks of read data. Hence if an unauthorized read operation is performed there will be a break in the correlation between blocks.

While this system deals with many of the security weaknesses, there are still the opportunities for attack. The process of transferring the memory data between the authorized read operations and the secure database presents an opportunity for a man-in-the-middle attack. If the pervious read block is known, it is possible to forge a fake set of read data that will still correlate with the previous data. If the random trigger value is known (or predictable) then it is also possible to forge a fake set of data that will also correlate with the next authentic block. As such, keeping the trigger value secret is important as is the source of the trigger value. The possibility of cloning the memory cells has also been considered. Each memory cell will have (an unclonable) fixed-pattern noise similar to digital image sensors which may allow 'digital fingerprints' of the memory to be taken similar to the process used to match images to cameras.

Keywords: Memristor, Offline hashchain, Proof of authenticity, Digital forensics

REFERENCES

[1] Australian and New Zealand Policing Advisory Agency (2013), Australia and New Zealand Guidelines for Digital Imaging Processes http://www.anzpaa.org.au/ArticleDocuments/282/2013%20Australia%20and%20New%20ZeZeZeZ%20Guidelines%20for%20Digital%20Imaging%20Processes.pdf.aspx

[2] Neville, Timothy. Sorell, Matthew. (2009). Audit Log for Forensic Photography. Springer

[3] Blythe, Paul. Fridrich, Jessica. (2004). Secure Digital Camera

[4] Knowm Memristors. http://knowm.org/

ISOLATING LENS ABERRATIONS WITHIN FIXED PATTERN NOISE

Richard Matthews
School of Electrical and Electronic Engineering
The University of Adelaide
Richard.matthews@adelaide.edu.au

Dr Matthew Sorell
School of Electrical and Electronic Engineering
The University of Adelaide
Matthew.sorell@adelaide.edu.au

Dr Nickolas Falkner
School Computer Science
The University of Adelaide
Nickolas.falkner@adelaide.edu.au

Lens aberrations can be used to determine the provenance of which lens was used when taking an image. However, this provides little information about the camera that was used itself since lenses can easily be changed on many cameras. A method, first published in 2005 by Lukàš, Goljan and Fridrich addressed this problem. Using Fixed Pattern Noise to link a photo to an image sensor provided a stochastic signal akin to a human fingerprint however, this model failed to account for lens artefacts creating a source of error. In our work, we have applied standard image processing theory and an understanding of the geometric properties of light to continue the isolation of artefacts within the fixed pattern noise model, which had previously thought to be totally removed. Our new, updated method creates a preliminary increase of 36% of the correlation over previous reported work.

CONTEXT

Lenses are complex devices. Whilst much is known about their mathematical design, only recently image analysts have begun to study lenses' unique geometric effects to solve the camera identity problem[1, 2] or find forgeries[3].This is because lenses create artefacts in an image known as Seidel Aberrations[4]. These Seidel Aberrations cause each ray of light travelling through a lens to deviate in some manner from the optical axis and is unique to a lens system. This concept is well explored in the literature[5] We accept lens aberrations are used to determine the provenance of images to the lens used for digital photography[2]. However, this provides little information about the camera in question as lenses can be easily substituted.

A different technique first popularised in the work of Lukàš et al, Goljan and Fridrich[6, 7, 8] has recently been used successfully by Farid and Goljan[9, 10] to the Daubert standard[11, 12, 13]; the legal burden of proof scientific evidence needs to meet for successful prosecution. The technique uses a stochastic noise signal present in every image as a fingerprint to link each image back to the image sensor that was responsible for sampling. This is based on a model of Fixed Pattern Noise (FPN). It is noted that the definition of FPN varies within the literature[14, 15]. We use the definition as noted in[15]. FPN is made up of two key components: Dark Signal Non-Uniformity (DSN) and Photo Response Non-Uniformity(PRNU). These two components represent the sensor in the dark (DSN) and the sensor under illumination (PRNU). Noise caused by variations to the dark current of a sensor, or self-induced current is the DSN while the PRNU is caused by low frequency artefacts such as dust or scratches on a lens and pixel non-uniformity (PNU) noise caused by slight differences on a pixel by pixel basis within the silicon structure of the sensor itself. This is illustrated in figure 1. This PNU when filtered can be used to link an image to the sensor which photographed the scene.

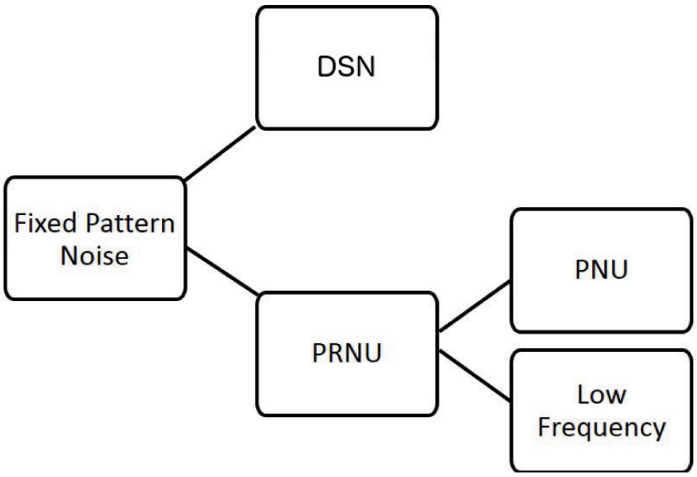

Figure 1: Fixed pattern noise model of a digital camera pipeline. The noise is made up of noise from the sensor when in the dark (DSN) and when the sensor is illuminated (PRNU).

The work however does not allow difference in lens aberrations in the model. If each image in the Lukàš test set was taken with a different lens would we still be able to successfully link the images to the correct camera? How do lens aberrations effect the correlation results of fixed pattern noise fingerprints to reference patterns given the proposed Lukàš et al model?

Our work extends upon the known science behind the Lukàš method to eliminate lens effects.

METHODOLOGY AND RESULTS

In this work we build upon the work of Knight, Moschu and Sorell[16] which successfully isolated file format artefacts present within the FPN model. We interchange the lenses on two Charge Coupled Device (CCD) cameras and substitute a third lens of our own design, a pinhole of precise dimension. Due to the increased use of mobile photography we then expand our camera sample base to include modern day Complementary Metal Oxide Silicon (CMOS) image sensors. A series of 8 Sony IMX219, first with a static lens and then with a pinhole lens at exactly 160nm are used to replicate and compare the results already obtained in the literature regarding CCD image sensors.

Using the existing algorithm in the literature[6] we then add an additional, novel step to remove edge effects from the proposed Lukáš filter. We increase the algorithm by overlapping squares as opposed to adjacent squares within the MAP estimation before performing the wavelet denoising as originally proposed. We then recombine into a denoised image by halving each denoised square by removing the outer 1/4th pixels in each approximation (figure 2).

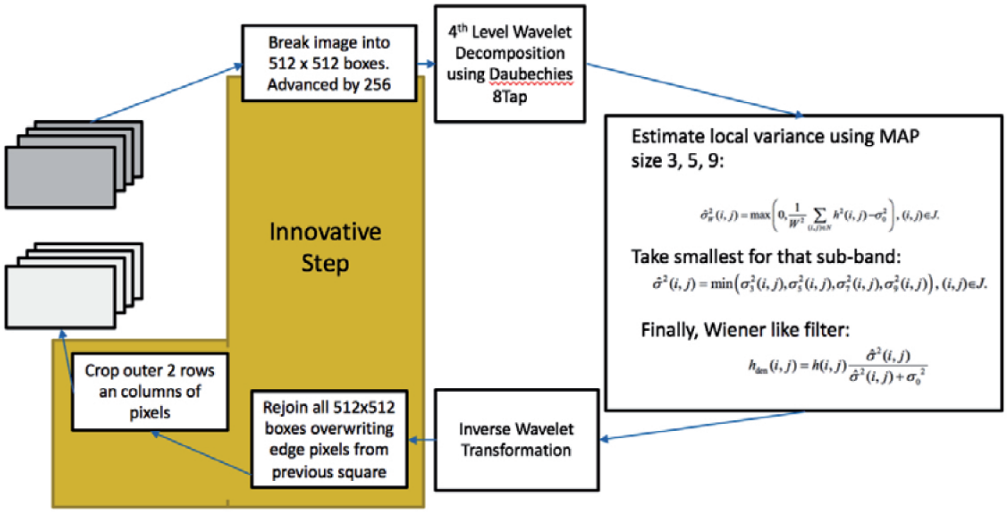

Figure 2: The denoising algorithm as proposed by Lukáš et al but modified with our innovative edge effect removal.

This novel step increases our ability to estimate the FPN accurately and we see a preliminary increase in the separation from 6% (Lukáš) to 22% (figure 3).

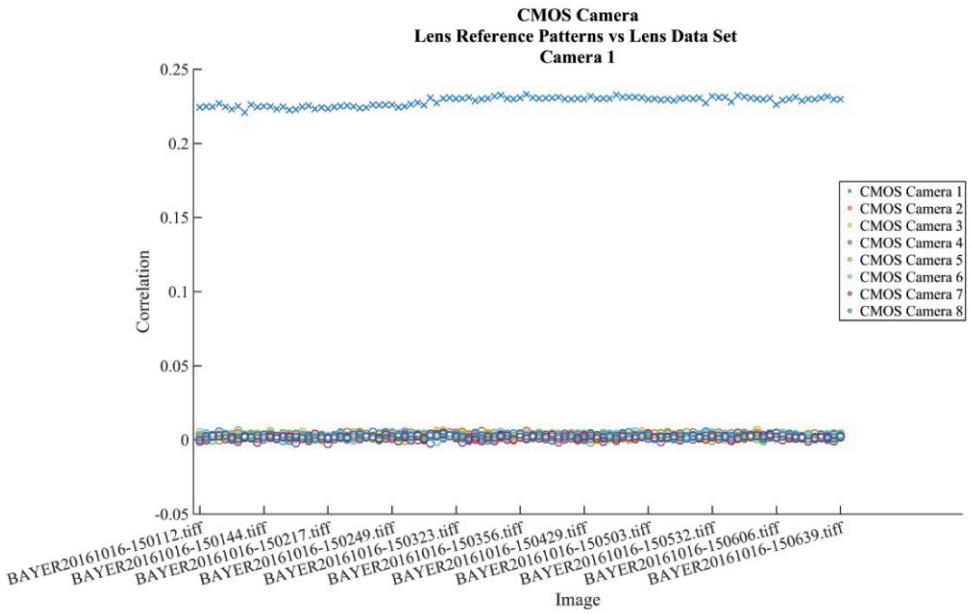

Figure 3: An increase in FPN estimation is shown with the correct camera recording a 23% correlation score verses the old methods 6% for a correct device.

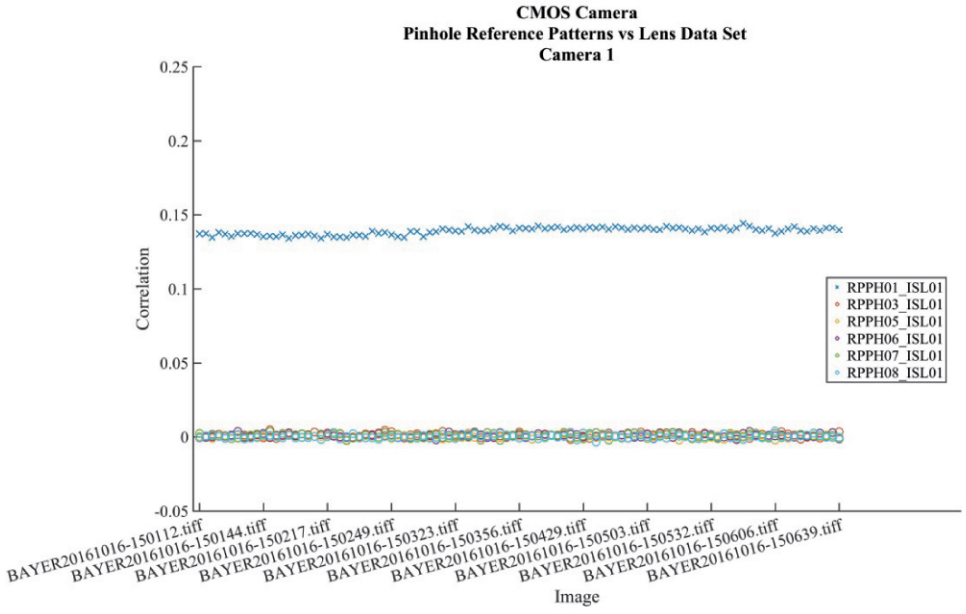

Figure 4: Comparing lens image data set to a pinhole reference pattern shows lower correlation scores. While the correct camera still scores higher and enables identification of the correct camera to solve the identification problem the lower score demonstrates removal of Seidel Aberrations from the PNU signal.

We then correlate images taken with lensed IMX219 against a reference pattern derived from a pinhole IMX219 and see that the correlation drops to 14% illustrating that the Seidel Aberrations make up approximately 36% of the PNU estimation previously seen.

Keywords: Fixed Pattern Noise, CMOS, CCD, Digital Image Forensics, Lens Aberrations

REFERENCES:

1 Kai, S. C., Lam, E. Y. & Wong, K. K., Automatic source camera identification using the intrinsic lens radial distortion. Optics Express (2006).

2 San Choi, K., Lam, E. Y. & Wong, K., Source Camera Identification using footprints from lens aberration. *Electronic Imaging 2006 International Society for Optics and Photonics* (2006).

3 Johnson, M. K. & Farid, H., Exposing digital forgeries through chromatic aberration. *Proceedings of the 8th workshop on multimedia and security* (2006).

4 Seidel, P. L. V., ber den einfluss der theorie der fehler, mit welchen die durch optische instrumente gesehenen bilder behaftet sind, und ber die mathematischen bedingungen ihrer authebung. *Abhandlungen der naturwissenschaftlich-technischen Commission der Bayerischen Akademie der Wissenschafte* (1857).

5 Jenkins, F. A. & White, H. E., Fundamentals of optics (McGraw-Hill Education, Tata, 1957).

6 Lukáš, J., Fridrich, J. & Goljan, M., *"Digital" bullet scratches "for images."*, presented at IEEE International Conference on Image Processing, 2005., 2005.

7 Lukáš, J., Fridrich, J. & Goljan, M., Determining digital image origin using sensor imperfections. *Electronic Imaging* 2005 (2005).

8 Lukáš, J., Fridrich, J. & Goljan, M., Digital camera identification from sensor pattern noise. *IEEE Transactions on Information Forensics and Security* (2006).

9 Goljan, M. & Fridrich, J., Sensor-fingerprint based identification of images corrected for lens distortion. *S&T/SPIE Electronic Imaging* (2012).

10 *N Strachan v HMA* (2011).

11 *Daubert v. Merrell dow Pharmaceuticals 509 U.S. 579, 1993.*

12 *General Electric Co. v. Joiner 522 U.S. 136, 1997.*

13 *Kumho Tire Co. v. Carmichael 526 U.S. 137, 1999.*

14 Holst, G. C. & Lomheim, T. S., *CMOS/CCD Sensors and Camera Systems* (JCD Publishing, 2007).

15 Janesick, J. R., *Scientific charge-soupled devices* (SPIE Press, 2001).

16 Knight, S., Moschu, S. & Sorell, M., *Analysis of sensor photo response non-uniformity in RAW images*, presented at International Conference on Forensics in Telecommunications, Information, and Multimedia, Berlin Heidelberg, 2009.

ON DETECTION OF ANOMALOUS QUERY SEQUENCES

Muhammad Imran Khan
Insight Centre for Data Analytic, University College Cork, Ireland
imran.khan@insight-centre.org

The enormous growth in information technology domain has resulted in generation of immense amount of personalized digital data. Organizations store and manage access to this data using Database Management Systems (DBMS). This stored data, being sensitive in nature gives rise to security and privacy concerns. A data breach not only risks the privacy of the individual whose data was stored in DBMS but organizations also face serious damages in-terms of reputation as well as suffer from financial loss. Yahoo recently reported that in 2014, 500 million accounts were breached [1]. Other giants who were subjected to data breaches include SONY [2], Citigroup [3], Adobe systems [4] . In a recent study by IBM in 2016, it is reported that there is an increase in cost of data breach from $3.79 million to $4 million [5].

Threats to an organization can be classified according to external (outsider attack) or internal (insider attack). External threats come from attackers outside of the organization who discover network and/or system vulnerabilities and use this information to penetrate the organization. Outside attackers may, for example, utilize social engineering techniques to accomplish a malicious goal, such as stealing confidential information, or making resources unavailable using a Denial-of-Service attack. There is much existing research on dealing with external threats and many security defenses have been proposed, including host-based access controls, intrusion detection systems, and access control mechanisms. On the other hand, an insider is a person who belongs to an organization and is authorized to access a range of data and services. For example, the reported incidents [6], [7], whereby hospital staff looked up the medical records of patients in the public-eye. A recent survey [8] reported that 89% of respondent organizations are vulnerable to insider attacks, while its reported [9] that malicious insiders are the cause of the costliest cybercrimes. A report from Intel security in late 2015 [10], titled "Grand Theft Data exfiltration study: Actors, tactics, and detection", stated that 43% of the data loss were cause by internal actors and half of it was intentional. 64% of professional at surveyed organization felt that if a data loss prevention technology was in place then these data breaches would have been prevented.

Another challenge in detection of insider attacks is that often they go unnoticed for months and years. According to Verizon 2016 Data Breach Investigations Report, among all the attacks, insider attacks took the longest time to be discovered, often in months or years [11]. Insider attacks can be detected by deploying intrusion detection systems. Traditionally, intrusion detection systems can be classified into misuse detection systems and anomaly detection systems [12].

SQL log abstraction	
(Q_1)	SELECT country FROM country_db WHERE id = 127462
$abs(Q_i)$	SELECT country FROM country_db WHERE id = VAR_VAL

Figure 1. Q1 is the original SQL query and abs(Qi) represents its SQL query abstraction.

Misuse detection systems look for well-known attack patterns and only detect attacks that are previously known. Unlike misuse detection systems, anomaly-based detection systems [13], [14] look for deviation from normal behavior and have the potential to detect previously unknown, or zero-day, attacks [15]. Anomaly-based intrusion detection systems alternatively known as behavioral-based systems have a potential to detect zero-day insider attacks thus we focus on anomaly-based intrusion detection systems. There has been a number of anomaly-based approaches proposed in the literature to detect malicious SQL query made by an insider [16], [17], [18]. These anomaly-based detection techniques in context of DBMS consider a query in isolation. Yet a query may be labeled as normal in isolation however, a sequence of SQL queries can result in a breach. We proposed an n-gram model that considers sequences of queries to construct profile of normal behavior. The model captures normal query patterns in a log of SQL queries from a synthetic banking application system [13]. SQL queries were transformed into an abstract representation. Some of the ways to have an abstract representation of SQL query are presented in [16], [19] and [17]. SQL abstraction is also referred as SQL query abstraction or SQL query signature in the literature. We borrowed SQL query abstraction technique from [19] that replaces constant values with placeholders in SQL query. Figure 1 provides an illustration of mapping between SQL query and its abstract representation.

Subsequently, a normal profile was constructed that consisted of sets of n-grams of SQL query abstractions. For a given sequence L of SQL queries, *ngram(abs(L),n)* be the set of all sub-sequences of size *n* that appear in abs(L). Let's say abs(L) = abs(Q1), abs(Q2), abs(Q3), abs(Q4) then a 2-gram model for *abs(L)* will be *{<abs(Q1), abs(Q2)>, <abs(Q2), abs(Q3)>, <abs(Q3), abs(Q4)>}*. We showed that it is possible to build useful query abstractions and that n-grams of these queries do capture the short-term correlations inherent in the application.

The architecture of different anomaly-based detection systems only differs in the construction of normal profile. The n-gram based model captures normal query patterns thus anomalous query patterns are detected. However, in case of an insider, who is familiar with the working of detection system, can mimic a normal access pattern to evade the detection system. In other words, the technically well informed inside attacker mimics normal behavior thus the attack goes undetected. In this work, we also demonstrate a mimicry attack on n-gram based approach. It is desirable to have a detection system that detects mimicry attacks, thus in this work, we also extends/compliments n-gram based model. The proposed extension mines audit logs to extract statistics in order to construct profile of normative behavior that facilitates in detection of anomalous behavior that reflects mimicry attacks. Initial experiments suggest that proposed approach appears to be effective in detecting attack mimicry attacks on n-gram based approach.

Keywords: Cybersecurity, Anomaly detection, Database intrusion detection Insider threats

REFERENCES

1. Fiegerman, S., *Yahoo says 500 million accounts stolen*. 2016.
2. Cook, J. *Sony Hackers Have Over 100 Terabytes Of Documents. Only Released 200 Gigabytes So Far.* 2014; Available from: http://uk.businessinsider.com/the-sony-hackers-still-have-a-massive-amount-of-data-that-hasnt-been-leaked-yet-2014-12.
3. Greenberg, A. *Citibank Reveals One Percent Of Credit Card Accounts Exposed In Hacker Intrusion.* 2011; Available from: https://www.forbes.com/sites/andygreenberg/2011/06/09/citibank-reveals-one-percent-of-all-accounts-exposed-in-hack/.
4. Goodin, D. *How an epic blunder by Adobe could strengthen hand of password crackers. 2013*; Available from: https://arstechnica.com/security/2013/11/how-an-epic-blunder-by-adobe-could-strengthen-hand-of-password-crackers/.
5. *2016 Cost of Data Breach Study: Global Analysis*. 2016, Ponemon Institute LLC.
6. Report, C.N.N., *27 suspended for Clooney file peek.* 2007.
7. Carr, J. *Breach of Britney Spears patient data reported. 2008*; Available from: https://www.scmagazine.com/breach-of-britney-spears-patient-data-reported/article/554340/.
8. *2015 Vormetric Insider Threat Report.* 2015, Vormetric.
9. *2015 cost of cyber crime: Global.* 2015, Ponemon Institute LLC.

10. *Grand Theft Data Data exfiltration study: Actors, tactics, and detection.* 2015, Intel security and McAfee.
11. *2016 Data Breach Investigations Report*. 2016, Verizon.
12. Vigna, R.A.K.a.G., *Intrusion detection: a brief history and overview*. Computer, 2002. 35(4): p. 27–30.
13. Khan, M.I. and S.N. Foley. *Detecting anomalous behavior in DBMS logs.* in *In International ference on Risks and Security of Internet and Systems (CRiSIS2016)*. 2016. Roscoff, france.
14. S. Forrest, S.A.H., A. Somayaji, and T. A. Longstaff, *A sense of self for unix processes, in 1996 IEEE Symposium on Security and Privacy.* 1996. p. 120–128.
15. Pieczul, O. and S.N. Foley, *Runtime Detection of Zero-Day Vulnerability Exploits in Contemporary Software Systems, in Data and Applications Security and Privacy XXX: 30th Annual IFIP WG 11.3 Conference, DBSec 2016, Trento, Italy, July 18–20, 2016. Proceedings*, S. Ranise and V. Swarup, Editors. 2016, Springer International Publishing: Cham. p. 347–363.
16. Hussain, S.R., A.M. Sallam, and E. Bertino. *DetAnom: Detecting Anomalous Database Transactions by Insiders. in Proceedings of the 5th ACM Conference on Data and Application Security and Privacy.* 2015. New York, NY, USA: ACM.
17. Sallam, A., et al., *Data and syntax centric anomaly detection for relational databases.* Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 2016. 6(6): p. 231–239.
18. Costante, E., et al., *A white-box anomaly-based framework for database leakage detection.* Journal of Information Security and Applications, 2016: p. -.
19. Kul, G., et al. *Ettu: Analyzing Query Intents in Corporate Databases. in Proceedings of the 25th International Conference Companion on World Wide Web.* 2016. Republic and Canton of Geneva, Switzerland: International World Wide Web Conferences Steering Committee.

SESSION 3: CYBER CRIME & CYBER SECURITY

Session moderated by Mr TOMÁŠ MINÁRIK,
NATO CCD COE

Mr Sten Mäses,
"GONE PHISHIN' (BUT NOT TO JAIL)",
Tallinn University of Technology

Mr Kristjan Kikerpill,
"CYBERCRIME AGAINST BUSINESS: WHO DRAWS THE SHORT STRAW?",
University of Tartu

Ms Anne Veerpalu,
"CHALLENGES TO THE REGULATION OF BLOCKCHAIN TECHNOLOGY ENABLED GLOBAL TRANSACTIONS",
University of Tartu

Ms Alžběta Bajerová,
"CYBERSPACE AS A DOMAIN OF OPERATIONS:
ESTIMATING THE FUTURE IMPACT ON NATO",
Masaryk University

GONE PHISHIN' (BUT NOT TO JAIL)

Sten Mäses
Tallinn University of Technology
sten.mases@ttu.ee

Kristjan Kikerpill
University of Tartu
kristjan.kikerpill@ut.ee

Phishing is a scalable act of deception whereby impersonation is used to obtain information from a target[1]. The given information can have widespread negative effects to the target himself as well as to his organisation. Most successful attack vectors in cyber security contain exploiting the human factor[2].

Organisations are aware of the risks related to the human factor and are conducting various activities to raise the security awareness and to enforce security aware behaviour. To that end, internal security policies play a crucial role in the overall build of information security measures for an institution. Research has shown that the inclination to use preventive security measures can depend on the perceived level of severity of the negative consequences[3], which from an organisational perspective can be influenced by how clearly internal procedures are explained and enforced. Furthermore, more active participation by top management in advocating for the importance of information security policies has a direct impact on employee compliance[4], so keeping the organisation out of harm's way is a team effort, wherein every member of the organisation has their part to play (not just 'the IT department').

Our research describes how to conduct phishing tests in a legal way so that the results could be used to evaluate the human factor of cybersecurity. Surveys or phishing tests conducted in a lab-environment do not adequately inform on real-life human behaviour when deciding on whether an email might contain malicious content. On average, people have a difficult time differentiating between legitimate and scam emails[5], which can prove disastrous for organisations both in the private sector (loss of profit, administrative fines and reputational damage from a data breach) and the public sector (leaking of classified information).

Our research focuses on the following questions:

1. What are the legal (and ethical) constraints for conducting a phishing test?
2. How to design a phishing campaign?
3. Is the click rate correlated to the reported number of incidents?
4. Is the click rate correlated to the security budget?

Many researchers have looked into the topic of phishing – e.g. how does it work[6], how to detect it[7] and how to use it to increase security awareness[2].

Intuitively, it is reasonable to assume that in an organisation where people click more on links given in phishing e-mails, the security posture is lower and security incidents happen more often. In an organisation where more resources are spent on securing the human factor of cybersecurity, there should be less clicking on malicious links and less incidents. Our research is going to look into these questions.

Before starting a phishing campaign, there are many legal and organisational questions to be answered. In order not to face prosecution later, it is important to ensure that everything is done in accordance with the law. This research brings out different legal issues and discusses how to address them. Also, different design choices for the phishing campaign are examined to help future work in the same field.

Measuring human factor can have many implications. In this work, we suggest considering phishing tests as an input for cyber insurance. Using human factor measurements as a parameter for setting

insurance rates could provide the necessary motivation for organisations to invest more in increasing their emphasis on the human element in security measures. Also, it could contribute into creating a more efficient way for cyber insurance implementation, because actuarial data necessary for determining premiums is generally not available for insurance companies. When comparing cyber-threats and the unpredictability of their potential consequences to the six characteristics of ideally insurable risk, the reasons why the cyber insurance market has difficult getting off the ground becomes more clear[8].

Keywords: Phishing, Human factor of cybersecurity, Cyber insurance.

REFERENCES

1 Lastdrager, E.E., 2014. Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, 3(1), p. 9.

2 Jansson, K. and von Solms, R., 2013. Phishing for phishing awareness. *Behaviour & Information Technology*, 32(6), pp. 584–593.

3 Dodel M and Mesch G (2017) Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human Behavior* 68: 359–367.

4 Hu Q, Dinev T, Hart P, et al. (2012) Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. *Decision Sciences* 43(4): 615–660.

5 Datar TD, Cole KA and Rogers MK (2014) Awareness of Scam E-mails: An Exploratory Research Study. *Proceedings of the Conference on Digital Forensics, Security and Law* 0(0): 11–34.

6 Dhamija, R., Tygar, J.D. and Hearst, M., 2006, April. Why phishing works. *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581–590). ACM.

7 Khonji, M., Iraqi, Y. and Jones, A., 2013. Phishing detection: a literature survey. *IEEE Communications Surveys & Tutorials*, 15(4), pp. 2091–2121.

8 Rejda GE and McNamara MJ (2014) Principles of Risk Management and Insurance (12th Edition), pp. 22–23.

CYBERCRIME AGAINST BUSINESS: WHO DRAWS THE SHORT STRAW?

Kristjan Kikerpill
University of Tartu
kristjan.kikerpill@ut.ee

The current article provides a theory-expanding analysis arguing for the suitability of the Routine Activity Theory (RAT)[1] for explaining cybercrime against enterprises. Rising cybercrime rates, soaring per incident costs and the seemingly unending variety in which criminals manage to prey on their targets requires an in-depth look into what makes a potential target appealing to criminal actors for the purposes of creating more effective crime prevention strategies. Thus far, RAT has largely been applied to the study of individuals' victimisation and the results have been mixed[2]. Recent criticism on the application of lifestyle/routine activities theory[3], e.g. a lack of attention to what actually increases the risk of being victimised, serves as an important starting point for revising the approach. While RAT provides an easy-to-follow framework for describing crime events – the convergence in time and space of a suitable target and a likely offender in the absence of a capable guardian – issues with how the concept of routine activities is constructed have not been adequately resolved and are hampering studies into the aetiology, and the subsequent prevention, of cybercrime. Applying RAT in the context of legal entities has four major advantages: (1) legal persons are subject to rules of compliance individuals are not, (2) as targets, enterprises inherently carry more value and this value can come from sources other than the opportunity for illicit financial gain, (3) enterprises incorporate an altered version of 'routine activities' by virtue of their personnel and (4) attract interest from a larger spectrum of likely offenders. According to RAT, target suitability comprises four elements: value, inertia, visibility and access (VIVA). To date, the aforementioned VIVA elements have received very little attention in the context of cybercrime and criminality – the research at hand will address these issues, because these components make up what could be considered as the 'target appeal final score', i.e. how vulnerable is the target organisation to cybercrime victimisation as well as what is the likelihood of a crime event taking place that involves a specific target. Mapping the taxonomy of suitable targets will be an important contribution to the study of cybercrime causation.

1.1 VALUE

Even though financial motivation is the biggest driver of cybercrime against businesses, it is not the only impacting factor. Regarding the projection of power via cyberspace by both state and non-state actors, the value of a target does not necessarily include the element of financial gains, but could also derive from a consideration in terms of the magnitude of effect and disruption achieved. The attack against the Ukrainian power grid is one of such examples. Third item of interest with regard to the potential value, is the use of third parties as the extra hop on the path to a bigger target. Small service companies or providers might not be considered valuable targets on their own, but the value comes from the access these enterprises can provide to larger targets.

1.2 INERTIA

In the physical realm, the suitability of a target would decrease with increases in its inertia, e.g. an appliance too heavy to be carried out of a home or a target too difficult to overpower[1]. For cybercrimes specifically, the size of the data being exfiltrated has been considered as an example of inertia[2], which is, however, only one aspect. Within an enterprises, the role played by the level of awareness, and internal procedures following from it, should also be considered as aspects of inertia, since it directly impacts

on how easy or difficult it would be for the offender to successfully 'pull off' the crime. An example here would be the ease or difficulty of detecting Advanced Persistent Threats, i.e. the long-term, unauthorised presence of a malicious actor in the organisation's network. This is not to be confused with ease of access, because gaining access and being interrupted in the carrying out of the attack[3] speak to different aspects of organisational measures. Employee and management awareness acts in conjunction with the technical measures implemented to create the notion of inertia.

1.3 VISIBILITY

One of the few aspects that has shown to have an impact on the victimisation of individuals is 'being online'. The online resources managed by enterprises provide attackers with an almost constantly visible target, because geographical and temporal restrictions that would apply with street crimes are negligible, if not entirely non-existent in the context of cybercrimes.

1.4 ACCESS

Technical and organisational measures determine the ease with which criminals can obtain access to the networks of an enterprise. Although news about major data breaches have become commonplace, the axiom 'Security becomes important only when it fails' still seems to hold true for the majority of companies. Whether caused by lack of awareness, 'corporate laziness' or the absence of formal control, the situation has not seen an overall improvement in recent years and the pool of suitable targets with easy access remains high.

Keywords: cybercrime, crime against business, routine activity theory, cyber criminology

REFERENCES:

1 Lawrence E. Cohen and Marcus Felson, 'Social Change and Crime Rate Trends: A Routine Activity Approach', *American Sociological Review* 44, no. 4 (1979): 588–608, doi:10.2307/2094589.

2 Eric Rutger Leukfeldt and Majid Yar, 'Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis', *Deviant Behavior* 37, no. 3 (3 March 2016): 263–80, doi:10.1080/01639625.2015.1012409.

3 Travis C. Pratt and Jillian J. Turanovic, 'Lifestyle and Routine Activity Theories Revisited: The Importance of "Risk" to the Study of Victimization', *Victims & Offenders* 11, no. 3 (2 July 2016): 335–54, doi:10.1080/15564886.2015.1057351.

4 Eugene McLaughlin and John Muncie, *Criminological Perspectives: Essential Readings* (SAGE, 2013).

5 Majid Yar, 'The Novelty of "Cybercrime": An Assessment in Light of Routine Activity Theory', *European Journal of Criminology* 2, no. 4 (1 October 2005): 420, doi:10.1177/147737080556056.

6 Aunshul Rege, 'Factors Impacting Attacker Decision-Making in Power Grid Cyber Attacks', in *Critical Infrastructure Protection VII* (International Conference on Critical

7 Infrastructure Protection, Springer, Berlin, Heidelberg, 2013), 125–38, doi:10.1007/978-3-642-45330-4_9.

CHALLENGES TO THE REGULATION OF BLOCKCHAIN TECHNOLOGY ENABLED GLOBAL TRANSACTIONS

Anne Veerpalu[1]
Tartu University
anne.veerpalu@ut.ee

Decentralized architectures are gaining popularity in global business as these are potentially making global transactions of any means of value quicker, cheaper, globally accessible and legally more transparent as the relationship is more peer-to-peer. Yet, the existing regulation of transactions with crypto-currencies, crypto-securities or any other value represented by tokens or coins (based on decentralized architectures) may potentially curb this innovation. The regulation put forward or *ex ante* existing and applied to for example crypto-currencies shows that fear of the unknown and misunderstanding of the technology may result in enacting or applying technology-neutral regulation that is unsuited for the specific technology and has the effect of banning or minimizing the use the technology offers without the legislator having this as its intent or objective. It follows that if legislation is not technology-specifically designed and legislators are blindfolded to the effects of the technology (positive or negative) on the global market, any national regulation can have a chilling effect on the use of any new emerging technology application, incl. the blockchain technology enabled applications.

This paper, as the first article of a Ph.D thesis, analyses the regulation and case-law of blockchain technology applications in Estonia, as examples of how the application of technology-neutral *ex ante* norms of general nature on decentralized architecture applications has had a chilling effect on the advancement and use of the technology on the market. The article further analyses examples of technology-specific regulation such as VoIP and P2P file sharing where the regulation accomodated technology´s use and effects, and compares those technological changes to the ones based on blockchain technology. The paper also discusses the socio-economic changes that are brought about by blockchain technology application networks – less intermediaries (credit institutions, custodians, central registries) involved in global transactions of means of value. This in itself influences the legislative framework and shortens the list of compliance- and supervision subjects posing a challenge for the legislative and executive powers to establish new legislative techniques. Not to mention that any legislation enacted must also be flexible enough not to be obsolete in a years time. Given the speed of technology developments currently – the authors research question is how to regulate blockchain technology applications given the challenges posed by the technology, its applications and the network.

The paper concludes that the decentralised architectures need to be understood by the legislator prior to enacting any new regulation and by the executive power prior to applying *ex ante* general clauses on its applications. Furthermore, any new regulation of decentralized architecture applications should be appropriately designed to fit the technology's global use cases and its advantages and risks on the global market considered on the basis of multidimensional (incl. local, regional and global dimensions) impact assessment, having active communication with the market actors through interactive and iterative legislative processes. The author suggests that decentralized architecture applications in the ever compliance-focused regulation call for new legislative techniques that meet the challenges of globalization and economic-technical transition towards transactions with less intermediaries that according to traditional legislative approaches have been the primary subjects of legislative attention.

Keywords: decentralized architectures, blockchain, distributed ledger technology, global transactions, technology-neutral, technology-specific, legislative techniques.

---

[1] Anne Veerpalu is an information technology law Ph.D student at Tartu University.

CYBERSPACE AS A DOMAIN OF OPERATIONS: ESTIMATING THE FUTURE IMPACT ON NATO

Alžběta Bajerová
Masaryk University
bajerova.alzbeta@gmail.com

In July 2016 at the Warsaw summit, NATO recognised a new domain of operations: cyberspace. By doing so, NATO looks to improve its ability to protect and conduct operations across all the domains and maintain its freedom of action and decision. However, step so strategically significant may bring a variety of unexpected results. The paper aims to explore them by asking following research question:

What is the possible future impact on NATO of recognising cyberspace as a domain of operations?

I approach answering the question through the framework of SWOT analysis – identification of strengths, weaknesses, opportunities, and threats of the new domain recognition by complex document review and subsequent critical evaluation. The purpose of the paper, however, does not lie in the research question itself, but rather in the arguments made along the way, that will hopefully open a broader debate on the topic.

As a strength, the paper identifies the integrative element of the recognition that is present on multiple levels. Cyber defence became adamantly embedded into military defence in general, a greater amount of responsibility was shifted to the national level, while the ultimate emphasis was put on the necessity of cyber defence development. These factors, if enhanced by the promised increase in inter-alliance cooperation, will indeed contribute to reaching NATO's goal of improvement in securing its operations.

The paper sees the main weakness in the absence of theoretical background, which then stems into many follow-up problems. The newly recognised domain itself still lacks a universally accepted definition, let alone a conceptual framework that would provide optics necessary for developing a coherent strategic approach. Future development of and decision making within the fast-pacing cyberspace is thus left hanging over both theoretical and conceptual vacuum.

The main opportunity, the paper argues, is narrowing the gap between NATO member states in their "ability to defend" that currently poses a significant security threat for the alliance. Recognising cyberspace as a domain and subsequent pushing on the further incorporation of cyber elements into current military practice might create additional pressure on national representatives to stop taking the cyber defence lightly and start attributing resources into its development. Evening the defensive potential of member states might also subsequently contribute to the reduction of the lack of information sharing within alliance regarding cyber capabilities.

The paper also identifies a significant threat stemming from the above-identified weakness. Putting a label of "domain" over the cyberspace's conceptual vacuum has already resulted in a spill-over of unfitting concepts from the physical domains. Strategic decisions based on flawed narratives could subsequently prevent NATO from using the full potential of cyberspace or even hinder its operational performance. As a supportive argument, the paper elaborates on a widely accepted narrative that puts cyber offensive capabilities into parallel with nuclear weapons, altogether with subsequent problematics of deterrence in cyberspace.

As a conclusion of the proposed paper, I plan to summarise given arguments, answer the research question, and issue recommendations on their basis. The conclusion will also put a strong emphasis on the necessity of further academic discussion regarding the topic.

SESSION 4: APPLIED IT-SECURITY

Session moderated by Dr MATTHEW SORELL,
University of Adelaide

Prof Tobias Eggendorfer,
"USING PROCESS MINING TO IDENTIFY ATTACKS",
University of Applied Sciences Ravensburg-Weingarten

Ms Belgin Tastan,
"ELECTRONIC IDENTIFICATION SYSTEM – HOW TO ADOPT, EXPANDING AND PROVIDE ONE CARD FOR ALL",
Tallinn University of Technology

Mr Aykan Inan,
"PROJECT IVA",
University of Applied Sciences Ravensburg-Weingarten

Mr Ayden Aba & Mr Jackson Virgo,
"EQUITY CROWDFUNDING WITH BLOCKCHAIN",
University of Adelaide

USING PROCESS MINING TO IDENTIFY ATTACKS

Sebastian Mauser, Tobias Eggendorfer, David Wichert
Hochschule Ravensburg-Weingarten, Fakultät für Elektrotechnik und Informatik
sebastian.mauser@hs-weingarten.de; tobias.eggendorfer@hs-weingarten.de; dw-131857@hs-weingarten.de

Attacking software often means to either inject new code through a vulnerability such as a buffer overflow or alter the execution path of a process, e.g. by a „return-to-libc" attack. However these attacks are hard to identify, since according to Rice's theorem it is impossible for a program to tell what another program is meant for.

Social engineering attacks, where users are tricked to use a programme in another way than it was intended by either the developer or the company policies, are even harder to detect by other programs. The same issues arise with insider attacks where authenticated users exfiltrate or manipulate data.

However all these attacks share that the process execution path is altered and thus changes from the usual behaviour of the program. In fact, most attack vectors tend to change the normal process flow of a system by differing from typical usage patterns, skipping parts of a program, injecting new program behaviour or forcing anomalous program executions.

Therefore, this paper proposes an approach of automatically observing process executions of computer programs by monitoring usage data. This way anomalous execution paths can be detected in order to identify and prevent security attacks. To develop appropriate techniques for analysing process executions and distinguishing between normal and suspicious system behaviour, we use methods from the research field called process mining [1, 2].

As the above examples show, such approach might provide an effective security mechanism for some types of attacks, e.g. insider attacks, which so far are almost impossible to detect. Moreover, for most other attack vectors our approach can be considered as an additional line of defence complementing existing security measures of e.g. intrusion detection systems and firewalls. The long term goal of our work is to develop a new process-based generic security system which can easily be applied to almost any kind of software system. For this purpose, such security system has to be able to implement and combine different process monitoring approaches. This might even lead to a process observation framework that can be integrated in future operating systems and thus help prevent attacks on a very general level.

A special motivation to work on this topic has been personal experience in the financial industry. The existing software landscape in this area consists of many legacy systems which are far from meeting state-of-the-art software security requirements for such highly business critical systems with confidential data. One of the authors has participated in a multi-million Euro project to significantly improve the security of such a legacy financial system. While the project was partly successful, some security problems could not be solved at all. Moreover, the costs of the project exploded and the overall cost-benefit ratio was very poor. Due to this unsatisfactory situation which is valid for many legacy systems, there is a growing need to find new generic solutions for improving the security of legacy systems. In this context, the author came up with the idea presented in this paper and successfully conducted first experiments on real world financial systems following such process-based security approach.

In this paper, we now build on these first positive practical results. We have conducted first research on the topic and created a simple prototype for demonstration purposes [3]. Our approach is based on the preliminary research on security and process mining by van der Aalst et al [2]. The latter paper discusses the topic on a high level of abstraction focusing more on auditing. It has barely been contin-

ued specifically in the direction of security attacks and intrusion detection which is the purpose of our research. In contrast to most other approaches on security attacks and process monitoring which focus on pattern analysis, e.g. [4], our method is based on the overall process flow of a system.

In more detail our approach follows the following line of reasoning. First, as the main part of our work, a reference model representing normal process executions has to be generated. This reference model then serves as a basis to decide whether newly observed process execution paths are potential security violations or not. In this context we tackle several interesting questions in our research. In particular, we analyse which kind of reference model is appropriate, e.g. a process model with likelihoods for execution paths, a Petri net-like model which helps to deal with concurrency, a tree structure, etc. Furthermore, we show how to find adequate sources of usage data of the observed system which can be used to generate such model, e.g. audit trails containing information about business processes or low level log files recording technical events about process executions. Today's software systems often provide such logging data. For instance, in the financial domain mentioned before, a vast amount of logging information is usually available ranging from low level to high level system events. As first practical experiments showed, this information can very well be used for our approach. Still, when this is not the case for some system, we show that we can also generate adequate usage data by applying a generic tracing mechanism and potentially memory layout analysis. Additionally, we discuss further problems for generating the reference model, e.g. how to ensure that the source data does not contain security violations, how to identify a complete process execution from individual events in a log or trace file, how to update the model when the software changes, etc.

Finally, based on the analysis sketched in the previous paragraph and considering existing process discovery techniques from the field of process mining, we developed a first proposal of an algorithm to generate such reference process model from respective logging or tracing information. For the future, this will be the most complex research part, since typical questions of process mining [1] such as concurrency, probabilities, noise, unobserved normal behaviour, etc. have to be handled in an appropriate way for our security system.

The second part of the security system is to implement a monitoring mechanism which checks the live logging or tracing data of the observed system for new process execution paths. Based on a comparison to the reference process model, the probability that the new execution is a security violation has to be evaluated. In our first prototype we use a simple evaluation algorithm which should be further elaborated in the future. Based on this evaluation, the security system can take appropriate measures, e.g. generate a warning message for an administrator, block a further execution of the process, log out the user, etc.

We tested the prototype against a simple web shop application for a first analysis. The results of this testing and the initial research are promising. We were able to theoretically and practically show that our approach is capable of effectively detecting security violations. In the future we plan to extend our work along the lines sketched in this paper.

REFERENCES:

[1] W.M.P. van der Aalst. Process Mining: Discovery, Conformance and Enhancement of Business Processes. Springer Verlag, 2011.

[2] W.M.P. van der Aalst, A.K.A. de Medeiros. Process Mining and Security: Detecting Anomalous Process Executions and Checking Process Conformance. Electronic Notes in Theoretical Computer Science, 121:3-21, 2005.

[3] David Wichert. Kozeptionierung und mogliche Anwendungen eines Systems zur Prozessuberwachung durch Analyse des Nutzungsverhaltens. Bachelorthesis, Hochschule Ravensburg-Weingarten, Weingarten, 2017 (to be published).

[4] S. Forrest, A.S. Perelson, L. Allen, and R. Cherukuri. Self-Nonself Discrimination in a Computer. Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy, 202–212. IEEE Computer Society Press, Los Alamitos, California, 1994.

ELECTRONIC IDENTIFICATION SYSTEM – HOW TO ADOPT, EXPAND AND PROVIDE ONE CARD

Belgin Taştan
Tallinn University of Technology
belgin_tastan@hotmail.co.uk

This research project is part of the Tallinn University of Technology Cyber Security Project.

Electronic Identification System is a revolutionary solution for the people of Estonia who must carry several cards in their pockets such as bank, transportation, access to some places, health insurance and discount cards etc. Electronic Identification System has the potential to allow its users just one card as their access device to everything. The card simplifies access for end users by unifying access across databases with end user's information. Statistics on usage may also be collated by government agencies to more effectively deliver e-governance services. Also, any possession of a person is useless when he/she is not in close vicinity of their belongings/possessions and hence, this leads to a lack of proper utilization. The use-data statistics of the card can be further utilized for analysis by the Estonian government, or by some private firm to know the number of people using their services and can analyse it to make better decisions. Nevertheless, with this solution, we may give access for somebody (using his ID code) to access cars/homes, and so on, whenever it is needed. This kind of system can be useful for (anyone)-anytime-anywhere. However, if the built-in security measures are defeated, there could occur a certain risk to privacy. I also examine the existing system to determine if further expansion of the Estonian model is possible.

In this work, I compare the existing e-governance and e-identity (EID) models of Estonia with the new EID System. The aim is to export the current Estonian model of EID to ensure one card with web portal access for all services. This work examines the technical and social issues surrounding such an import and expansion of services.

Performing person identifications correctly, is not that easy. If the security mechanism is poorly designed, it can be worse than if there were no security mechanism at all. There are examples where the encryption is weak [1:181]. For example, if traffic in an information network is weakly encrypted and the password is broken, the traffic may be better left clear if the last machine in the system is attacked. Another important example is the security of personal data. An organization that receives personal data, can try every method to translate the valuable information it has obtained therefore methods in which personal identifiers are concealed are the preferred methods for system implementations [1:181].

The date when Smart Cards went on the market was the end of the 1980s. Due to several reasons, from day to day, it is known that Smart Cards can be hacked into clones in many ways. Some of the methods used previously include blocking messaging between the Smart Card and the manufacturer, freezing the contents of the EEPROM by using adhesive tape, slowing the function of the smart card, physically tampering with the smartcard, probing attack, memory linearization attack, hacking the circuitry, pirate cards, using a laser etc. [1:291-295]. With Smart Cards, a variety of technologies are used, making it difficult for attackers to penetrate. When we compare Smart Cards to magnetic striped cards, we can say that Smart Cards are more resistant to copying. Today, Smart Cards are being used in the European Union area by supporting enhanced electronic signatures. These smart cards and electronic signatures are used to sign legal documents, and they also demonstrate that the Smart Card is legally

owned. The technical design of Smart Cards includes both software and hardware features which can be utilized to increase the difficulty in cloning the card [1:296].

When we compare magnetic stripe cards, smart cards and Estonian identity card as normal loyalty cards, there are some differences between those cards. Magnetic stripe cards contain the name, account number and expiration date [2] while Smart cards usually only have a card number on it and are more durable than magnetic stripe cards against cloning [3]. The Estonian identity card contains a personal data file that has 16 record fields and holds information such as name, date of birth, expiration date, ID code and nationality but does not contain address information. This personal data file, too, can be cloned. Magnetic stripe cards and contactless smart cards can be used as a loyalty card but Estonian identity card can not be used as a loyalty card. This is because there is only a chip which requires special equipment to read and is less convenient than a magnetic stripe or contactless smart card. The main information needed to identify a person would be name, ID code and maybe document number. We can use this information to make a clone and gain access to a person's loyalty account. It is also possible to give fake name and ID code when using the ID card as a loyalty card in stores however it is not possible to do so when the ID card is used online. This is because the name and ID code are read from the personal data file only after a successful authentication.

When we look at the security features of these cards, we can say that they all have security vulnerabilities. What I want to design is a secure smart card, which will work in connection with the web portal in the system which will be detected using the attack tree method. A survey will be conducted to obtain user preference in regards to using the ID card as a single card for every service. This survey, will also cover user's feelings about privacy aspects.

Keywords: Electronic Identification System, EID, Smart Cards, ICT, Identity, e-Government, Digital.

REFERENCES:

[1] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed., 2008.

[2] L. Padilla, "Track format of magnetic stripe cards," December 2002. [Online]. Available: http://www.gae.ucm.es/~padilla/extrawork/tracks.html. [Accessed June 2017].

[3] R. Want, "An introduction to RFID technology," IEEE Pervasive Computing, vol. 5, no. 1, pp. 25–33, 2006.

PROJECT IVA

Aykan Inan
University of Applied Sciences Rravensburg-Weingarten
aykan.inan@hs-weingarten.de

Smart home is not a vision of the future but has already become reality. More and more companies are entering the smart home market and the products are more widely accepted by customers. This is an astonishing development, since until a view years ago, the idea of smart homes was not known to the broad public. At that time it was rather known under the term home automation. Various technical developments and appropriate marketing, under the collective term smart home, has triggered a real boom ever since. [1]

Since all devices have sensors installed which make them capable of spreading their status information across a network they are also counted as Internet of Things (IoT). Too often though, it seems very common that existing equipment is simply connected to the internet without taking security into account. The adaptation of this technology took place very individually and was accompanied by a wild growth. This lead to significant interoperability issues and a neglected IT security landscape. At the same time the constant stream of data between devices lead to a tremendous amount of data which is not transparent anymore and which can be exploited for frauds and unknown propagation of valuable information. [2]

Many different platforms were invented in order to get a grip on the resulting complexity and security. They all offer a solution that allow devices from different brands to get connected on one single gateway platform. [3] The biggest issue is, however, that there is no standardized certification and uniformed standard for smart devices, at all. [4] Manufacturers make use of combining different independent standards without considering if they really fit together. With a special search engine such as Shodan devices or entire systems can be detected, which are connected to the internet. Nevertheless, an easy discovery is not necessarily a weakness since it does not automatically imply a vulnerability, unlike generally assumed.

With the large number of reported vulnerabilities and the future expectation that hackers will take advantage of these flaws, it is necessary to have a tool that is capable of detecting weaknesses. [5] [6] [7]

This project has the goal to start to build a framework and tool-set that is capable of testing platforms automatically for security vulnerabilities and potential weaknesses that could afflict IoT systems.

In general terms, IVA can be described as a tool-set that performs an analysis of captured data samples to perform a pattern matching and deep header inspection, based on a developed logic and metric analysis, in order to identify and examine patterns of interest and to find a likelihood of security weaknesses. By the end of the project there should be a fully functioning tool that is capable of reflecting a forensic map of likelihood threats and a traffic profile.

To do so, a proper test inspection environment and software tool-set is required in order to allow a more effective testing and reverse engineering with minimum effort. Currently used (open-source) software, however, do not possess the required capabilities for testing an IoT environment as intended. Usually these tools are limited for testing known network protocols. But they cannot be used properly for unknown or proprietary network protocols as they exists in IoT. Although IoT also relies on known standards, it is necessary to take a deeper look in how the communication itself takes place.

Basis for this is a systematic work-flow consisting of multiple steps. This includes capturing and obtaining communication samples, logical disassembling of the traffic and the development of an analysis metric in the end.

The entire process starts by capturing traffic samples during the setup phase. The devices to be tested are integrated within the experimental setup. At certain hubs all necessary and every potential piece of information can be collected using a network packet sniffer, such as Wireshark or tcpdump.

If the capturing is completed, the main objective is to analyze the captured traffic. For this, it is necessary to display all available information in the first place such as used protocols or delivery methods. Taking these findings and observations it is possible to check for vulnerabilities and attack vectors in advance that are already known. In this context though, known penetration software (Metasploit) can provide additional support.

Then a developed logic is required in order to be able to perform a separation or extraction of the communication itself. That means that the collected data will be classified in different categories according to their use. This includes, inter alia, the various stages of communication such as associated authentication, encryption, key exchange and unknown traffic.

Subsequently the next priority will be to focus on the unknown data streams itself in order to detect patterns of interest and being able to eliminate irrelevant data. The stored data needs to be analyzed manually in the first place in order to develop different metrics to search for (high) correlation. Such correlation can be the transmitted plain text password hidden in a Morse code. [7]

For this project, it is considered to focus on various systems and IoT devices that are mainly available in Germany and address the home user market. This novel and new approach, using new analytic methods in order to detect patterns of interest and correlations that indicate a problem, aims to considerably reduce security risks. The results can help to minimize and suggest a proactive and more efficient security model for IoT communication and devices.

Keywords: Internet of Things, Deep header inspection, Anomaly detection

REFERENCES

[1] c't Special Edition Smart Home (magazine for computer technology)
[2] https://www.tecchannel.de
[3] https://www.qivicon.com/de/
[4] http://www.etsi.org/
[5] http://www.spiegel.de
[6] https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
[7] c't 17.08

EQUITY CROWDFUNDING WITH BLOCKCHAIN

The University of Adelaide

Ayden Aba,
ayden.aba@student.adelaide.edu.au

Jackson Virgo,
jackson.virgo@student.adelaide.edu.au

Dr. Matthew Sorell (supervising author)
matthew.sorell@adelaide.edu.au

1. INTRODUCTION

Bitcoin's underlying technology, the blockchain, or the distributed consensus ledger, has allowed mutually distrustful parties to securely transact virtual currency stored on a decentralised database with minimal time expense and financial friction, effectively eliminating the need for a trusted intermediary. The realisation that this technology can be more broadly applied to other digital assets led to the advent of smart contracts; an agreement whose execution is both automated and enforced by the cryptographic consensus of the distributed ledger.

This revelation bares significant ramifications for the financial services industry. In particular, blockchain technology presents an opportunity for emerging companies to undercut the large industry incumbents who have enormous amounts of capital tied up in traditional methods of transacting and storing financial information.

However, before blockchain can be integrated into existing businesses, the risks of the technology need to be explored and further understood. For instance, the recent security breach of an Ethereum blockchain application, "The DAO", in July 2016 saw the equivalent of USD$50 million in cryptocurrency at stake[1], highlighting the pertinence of research into blockchain.

This case reminded investors that, whilst theoretically sound, exploits in the underlying technology are still possible, and a single such security vulnerability can expose all the users of an entire blockchain network. Considering cryptocurrencies and blockchain applications are expect to become the new fabric of trade and commerce, this uncertainty is alarming.

Through our research into applications of blockchain within crowdfunding, we hope to further understanding of how the technology may be realistically and securely integrated into existing businesses, and society more broadly.

2. OBJECTIVES

The overarching objective of our research team is to distil a more accurate picture of blockchain's utility from the noisy aggrandizement that has characterised a lot of discussion around its potential. By investigating the application of blockchain technology within the Australian unlisted securities market, we aim to examine various cyber security issues, and societal acceptance issues, to be faced during the transition toward crypto-asset based economies.

3. METHODOLOGY

A partnership with the University of Adelaide and The Australian Small Scale Offerings Board (ASSOB)[2], an Australian equity crowdfunding platform, has been established.

Through working with ASSOB, it has been identified that the research team will develop an automated blockchain solution for one of their core business processes: the share application process 1.

Under this partnership the research team aims to produce key deliverables via an iterative discovery, research and design process (see Figure 1).

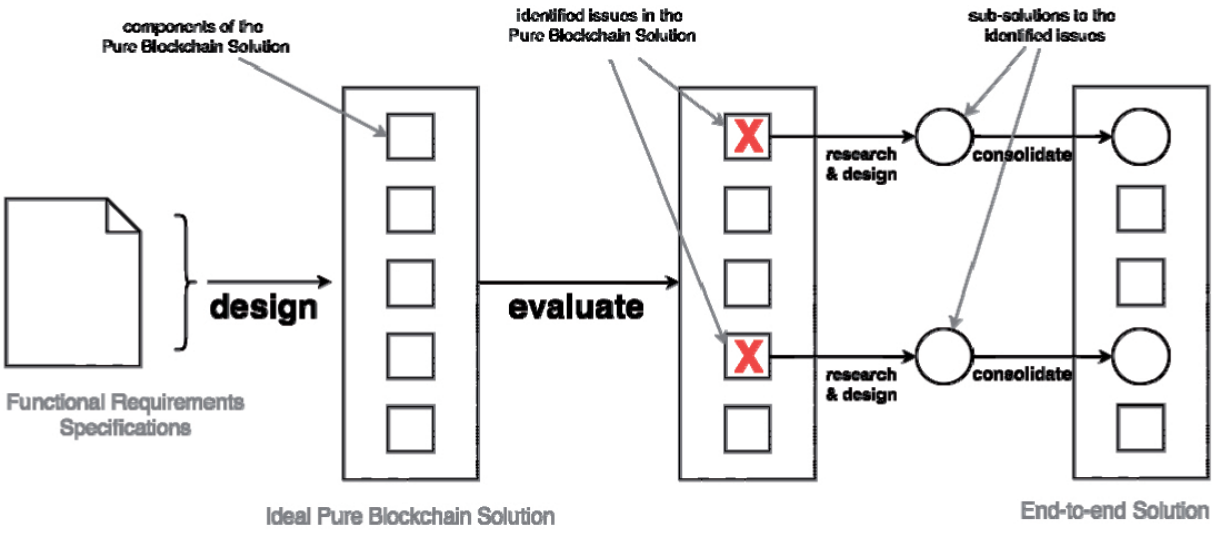

Figure 1. Research Process

4. PRELIMINARY SOLUTION

By mapping ASSOB's share application process onto a blockchain application, we hope to leverage the characteristics of blockchain technology to achieve two key outcomes:

1. a reduction in transaction friction; and
2. improved transaction transparency.

4.1. TRANSACTION FRICTION

Under the existing process implementation (see Figure 2), capital transferred from the Investor is handled by several intermediary parties before reaching the Issuer. Each time the capital changes hands a cost is incurred.

The share application process is the process whereby an Investor invests funds in a company (referred to as an Issuer) in exchange for an equity holding in that company.

The proposed solution, pictured in Figure 3, replaces these friction points with a single blockchain application interface. Financial friction is reduced to the cost of processing the digital currency through the blockchain application. On Ethereum this would manifest as a single transaction fee. The result is a higher utilisation of the invested capital because a larger proportion of invested funds is actually received by the Issuer.

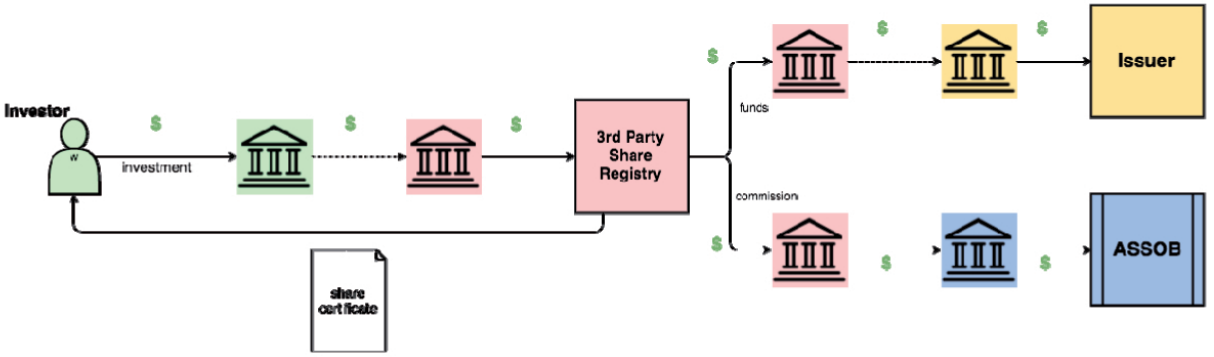

Figure 2. Flow of value through the share application process currently (no blockchain)

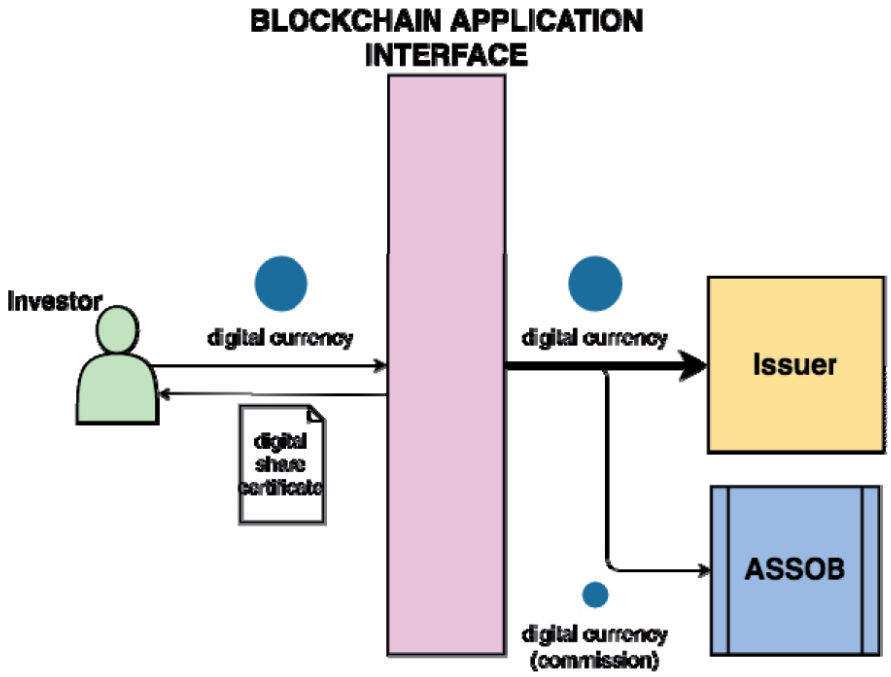

Figure 3. Potential flow of value through the share application process in the future using blockchain

4.2 TRANSACTION TRANSPARENCY

Leveraging the data immutability aspect of blockchain distributed ledgers, we can improve the transparency of share application transactions. Effectively an on-blockchain share application process would provide cryptographical proof of transaction data integrity, time of exchange, and what was exchanged, massively simplifying any dispute over a transaction.

5. PRELIMINARY RESEARCH QUESTIONS

5.1 "FIAT-CURRENCY WORLD" TO "FUTURE CRYPTO-ASSET WORLD"

We currently live in a world driven by fiat currencies. In this state of the world, crypto- assets are difficult to justify because at the end of the day, users of the system must be able to convert their crypto-assets into physical goods. For instance, in today's fiat currency environment you cannot directly purchase your groceries using Bitcoins or Ether. The vendor will only accept a recognised fiat currency, therefore a conversion from a crypto-asset to a fiat currency needs to occur.

A future crypto-asset world is a hypothetical state of the world where all physical assets can be directly represented digitally as on blockchain crypto-assets. i.e. in a crypto-asset world, you can purchase your groceries using crypto-currencies such as Bitcoin or Ether.

Using this conceptual framework of two different states of the world (present and future) and applying it to the blockchain solution we develop for ASSOB, we will evaluate how realistic blockchain applications really are in our society. We have distilled this into three key questions:

1. What are the barriers for new users of a blockchain application / crypto-currencies in a fiat currency state of the world?
2. What are the barriers for new users of a blockchain application / crypto-currencies in a crypto-asset state of the world?
3. What could the transition from a fiat currency world to a crypto-asset state of the world look like?

5.2 EXTERNAL DATA SOURCES

The indisputability of data residing on a blockchain is a function of its origination from a cryptographically immutable, append-only ledger. External systems are inherently non- secure and untrustworthy

from a blockchain perspective, but lacking access to them severely constrains the potential functionality of smart contract applications. In this early stage, it is likely that external interfaces will be required for blockchain to be feasible for many applications, and certainly for integrating in to existing systems. This raises the question of how to maintain the security integrity of the crypto-ecosystem, whilst still allowing access to existing data sources.

5.3 SMART CONTRACTS IN LAW

Particular to the System to be designed in this project is the problem of producing equity assets that are recognizable by the Australian legal system. A framework for translating existing legal code into smart contracts was outlined by Clack et al. in *Smart Contract Templates: foundations, design landscape and research directions*[3]. The contract templates developed in this paper are being used to implement the Corda platform[4] for blockchain based legal agreements between companies. As part of the design process we intend to investigate further how this might apply to agreements created in equity crowdfunding.

Keywords: blockchain, smart contracts, cryptocurrency, Ethereum, equity crowdfunding, distributed ledger, bitcoin, fintech

REFERENCES

1 qz.com, "Everything you need to know about the Ethereum hard fork" [Online]. Available: https://qz.com/730004/ everything-you-need-to-know-about-the-ethereum-hard-fork/

2 The Australian Small Scale Offerings Board, https://assob.com.au

3 C. D. Clack, V. A. Bakshi, L. Braine, University College London, "Smart Contract Templates: foundations, design landscape and research directions," August 2016; http://www0.cs.ucl.ac.uk/staff/C.Clack/SCT2016.pdf

4 http://www.ibtimes.co.uk/barclays-smart-contract-templates-heralds-_rst-ever-public-demo-r3s-corda-platform-1555329

SESSION 5: STATE & CYBER

Session moderated by Dr NICKOLAS FALKNER,
University of Adelaide

Ms Maarja Toots,
"WHY DO E-PARTICIPATION PROJECTS FAIL?
THE CASE OF ESTONIA'S OSALE.EE",
Tallinn University of Technology

Mr Georgios Pilichos,
"SECURITIZATION OF CYBERSPACE",
Tallinn University

Mr Madis Metelitsa,
"ADDRESSING THE SECURITY DILEMMA IN CYBERSPACE",
University of Tartu

Ms Somaly Nguon,
"CAMBODIA'S EFFORT ON CYBERSECURITY REGULATION:
POLICY AND HUMAN RIGHTS' IMPLICATIONS",
Tallinn University of Technology

WHY DO E-PARTICIPATION PROJECTS FAIL? THE CASE OF ESTONIA'S OSALE.EE

Maarja Toots
Tallinn University of Technology
maarja.toots@ttu.ee

Researchers and policy-makers all over the world are taking increasing interest in the democratic potential of information and communication technologies (ICTs). This is evident in the growing number of e-participation initiatives and the emergence of the research fields of e-participation and e-democracy [1–3]. Existing e-participation projects have taken on different forms, from online discussion forums and citizen consultation platforms to legislation wikis, e-petitioning systems and one-stop participation portals. However, many studies refer to the failure of e-participation projects to engage users [4–6] and deliver the expected outcomes [7, 8]. It is thus important to ask why this is the case and what causes e-participation projects to fail.

E-participation projects can be thought of as a specific type of information systems – ones designed to enable democratic dialogue between government and citizens. Although failure is a thoroughly researched problem in information systems (IS) literature, research on the success and failure of e-participation projects is still in its infancy [9]. In order to contribute to a better theoretical understanding of the failure causes of e-participation projects, an empirical case study of the Estonian government's e-participation portal Osale.ee was undertaken, focusing on two research questions: 1) What factors cause e-participation projects to fail?; 2) How does failure happen?

Osale.ee was initiated in 2004–2005 with the aim to provide a one-stop portal where the government could consult citizens on legislative drafts and citizens could propose their own policy ideas to the government. The portal is still operational but a number of studies over the years have deemed it a failure due to its under-utilization and lack of impact [10–13]. While some of these studies involve detailed descriptions of Osale.ee's flaws, none provides a comprehensive explanation of the causes of its failure. The research aimed to fill the gap and conduct a more systematic analysis of the factors that have prevented this project from realizing its potential.

The research took an interdisciplinary approach, combining literature from the research fields of information systems, e-democracy and public participation. After a review of existing explanatory models of IS failure, Chris Sauer's (1993) socio-technical and process-centric model was adopted as the guiding framework for the research. According to this model, information systems fail if IS managers fail to address problems and demands from the external environment up to a point where flaws accumulate and the system loses its supporters [14]. The model thus presumes a constant interaction between the information system, its managers, stakeholders and the external context. However, the model says nothing about the specific political and social context of e-participation. Therefore, a review of e-democracy and public participation literature was conducted to generate a list of potentially influential contextual factors that may affect e-participation projects.

Empirical data on the case was collected over a 6-month period from December 2014 to May 2015 through a desk study and six semi-structured interviews. Based on existing studies, policy papers, reports, press releases, articles and usage statistics, a detailed timeline of Osale.ee was sketched and the main problems frequently mentioned in relation to the project were outlined. This was followed by interviews with Osale.ee's managers, idea champions and users to better understand the possible causes of these problems. The interviewees were asked to describe the goals and expectations set

to the system, the extent to which they consider these expectations fulfilled, the flaws and problems they have witnessed in the system over time, ways of addressing the problems, and the factors in the external context that may have affected the project. Those involved in Osale.ee's management were additionally asked to describe the process of the daily management of the system and interaction with stakeholders, while users were additionally asked to describe and explain their user experience and intention to use the system in the future.

The results of the case study suggest that e-participation projects may face double challenges: ones that are typical to public sector ICT projects and others that arise from the context of democratic participation (see Figure 1 for a summary of the key factors).

KEY FACTORS IN THE FAILURE OF OSALE.EE
System and process design: poor integration of Osale.ee with the policy process, lack of feedback
Demand side: low demand for Osale.ee, limited participation skills, difficulty of matching different stakeholders' expectations, changes in expectations, limited efforts to promote Osale.ee among users
Regulatory gaps: lack of clarity in the concept of public consultation
Organizational inertia: incompatibility with citizen engagement, complexity of organizational change
Culture and attitudes: under-developed culture of participation, resistance to citizen engagement
Lack priority: low political priority, lacking innovation leadership
Competing information systems: adoption of the Draft Information System
Staff and structure: change of coordinator, shift of Osale.ee's management to another department
Inadequate innovation and support management

Figure 1. Key factors in the failure of Osale.ee

Many factors that played a role in Osale.ee's failure match those often discussed in information systems literature. These include the importance of user-centric design, consideration of stakeholders' needs in system development, capable innovation management, innovation leadership, etc. However, the environment of online democratic participation seems to have posed several additional challenges. These emanate from distinct demand-side barriers such as a generally low interest in e-participation, the effort and skills required for participation, and the difficulty of satisfying the diverse user groups characteristic to e-participation projects. Barriers also stem from an under-developed collaboration culture, lack of political support, gaps in regulatory framework, and the overall incompatibility of existing organizational structures and processes with citizen participation.

As most of these factors are complex and difficult to address, the study implies that e-participation initiatives may be inherently more prone to fail than succeed. The findings also point to the need for novel combinations of research on socio-technical systems, e-democracy and public participation to enhance our understanding of the factors that affect the success of e-participation.

Keywords: e-participation, e-democracy, socio-technical systems, IS failure

REFERENCES

[1] Panopoulou, E., E. Tambouris, K. Tarabanis (2010) "eParticipation Initiatives in Europe: Learning from Practitioners." In Electronic Participation, eds. E. Tambouris; A. Macintosh; O. Glassey. Lecture Notes in Computer Science, Vol. 6229, 54–65.

[2] Medaglia, R. (2012) "eParticipation research: Moving characterization forward (2006–2011)". Government Information Quarterly, Vol. 29, 346–360.

[3] Susha, I., Å. Grönlund (2012) "eParticipation research: Systematizing the field." Government Information Quarterly, Vol. 29, 373–382.

[4] Edelmann, N., J. Höchtl , M. Sachs (2012) "Collaboration for Open Innovation Processes in Public Administrations." In Empowering Open and Collaborative Governance: Technologies and Methods for Online Citizen Engagement in Public Policy Making, eds. Y. Charalabidis, S. Koussouris, Springer, 3–20

[5] Karlsson, M. (2012) "Democratic Legitimacy and Recruitment Strategies in eParticipation Projects". In Empowering Open and Collaborative Governance: Technologies and Methods for Online Citizen Engagement in Public Policy Making, eds. Y. Charalabidis, S. Koussouris, Springer, 3–20.

[6] Epstein, D., M. Newhart, R. Vernon (2014) "Not by technology alone: The "analog" aspects of online public engagement in policymaking." Government Information Quarterly, Vol. 31, 337–344.

[7] Sæbø, Ø. L. Skiftenes Flak, M. K. Sein (2011) "Understanding the dynamics in e-Participation initiatives: Looking through the genre and stakeholder lenses." Government Information Quarterly, Vol. 28, 416–425.

[8] Bannister, F. and R. Connolly (2012) "Forward to the past: Lessons for the future of e-government from the story so far." Information Polity, Vol. 17, 211–226.

[9] Kubicek, H., G. Aichholzer (2016) "Closing the Evaluation Gap in e-Participation Research and Practice". In Evaluating e-Participation: Frameworks, Practice, Evidence, eds. G. Aichholzer, H. Kubicek, L. Torres. Public Administration and Information Technology, Vol. 19, Springer, 11–45.

[10] Runnel, P., P. Pruulmann-Vengerfeldt, K. Reinsalu (2009) "The Estonian Tiger Leap from Post-Communism to the Information Society: From Policy to Practice." Journal of Baltic Studies, Vol. 40, No. 1, 29–51.

[11] Åström, J., H. Hinsberg, M. E. Jonsson, M. Karlsson (2013) Citizen centric e-participation. Case studies on e-participation policy: Sweden, Estonia and Iceland. This Praxis Center for Policy Studies report.
Available at: http://pasos.org/wp-content/uploads/2013/08/citizen_centric_e_participation.pdf

[12] Kalvet, T.; M. Tiits; H. Hinsberg (2013). Impact assessment of the Estonian e-government services. Tallinn: Institute of Baltic Studies & Praxis Center for Policy Studies.

[13] Praxis Center for Policy Studies and Pulse (2015) Osalusveebi ja valitsuse eelnõude infosüsteemi kasutatavuse analüüs. Lõpparuanne. Available at: https://riigikantselei.ee/sites/default/files/content-editors/Failid/AVP/Osalusveeb%2C%20EIS%20lopparuanne_8-05-15.pdf

[14] Sauer, C. (1993) Why Information Systems Fail: A Case Study Approach. Oxfordshire: Alfred Waller, Ltd, Publishers.

SECURITIZATION OF CYBERSPACE

Georgios Pilichos
Tallinn University
george@tlu.ee

Since the modern internet was born in 1980s the interests of states have been shifting towards cyberspace and how to meet the new challenges beyond Euclidean space. The cyber operations driven by nation states and non-state actors reflect on the evolution of warfare as well as the struggle of power over the cyber domain. Given the fact that private sector is responsible for major part of the digital life and cyberspace, the research paper examines the nature of the Public Private Partnership (PPP) towards the militarization of cyberspace. The cases of cyber incidents, such as cyber-attacks and cyber espionage allow us to go through the militarization and the cyber arms race which takes place and to answer the research question concerning: How does the private sector contribute to the militarization of cyberspace?

In order to answer the main research question, the following sub-questions should be addressed. Do the private and public sector pursue a common interest in cyber space or pursue self-interests? Could the militarization of cyberspace bring peace and security or will end up with cyber-war? The research paper brings together four different cases and explores each of them in the lens of securitization theory and the theory of realism, concentrating on the way that cyber operations were conducted, the degree of sophistication and the contribution of private sector . The case studies such as the cyber attack in Estonia and Georgia, Stuxnet and the Snowden leaks, include a variety of cyber operations which allow us to to figure out the nature of these operations and the role of private sector. The selection of multiple cases helps to strengthen the findings from entire study, through the "deliberate and contrasting comparisons"[i] between them.

However, the primary objective of the research is the securitization of cyberspace, hence the theory of securitization provides with the appropriate theoretical tools to do so. Discourse analysis is associated with the studies based on securitization framework. Securitization refers precisely to the process of presenting an issue in security terms: as Buzan points out, "the way to study securitization is to study discourse and political constellations"[ii]. Discourse analysis has been chosen in order to construct a questionable issue to security one. The examination of case studies allow the securitization process to take place.

After defining a problem to a "security problem" the research paper will go through the militarization of cyberspace and the role of private sector. The theory of realism and the security dilemma have been chosen in order the shift of debate from securitization to militarization to be understood.

Admittedly, the increasing number of connected devices and the degree of sophistication of cyber operations have found states struggling to keep the balance of power and private sector to take an advantage of technological revolution. The increasing power of private sector turns out that, private sector has become the most prominent target, but not only target. The industry is the target, the vendor, and the entity which clean up the system from an exploitation. So, the private sector has multiple identities in cyberspace, which allow engaging in the process of building up cyber offensive capabilities and contributing to the militarization of cyberspace. The experience and resources of private sector would be an asset for a state actor not only to develop further its capabilities but also to build capacity in order to keep the balance of power in cyber domain.

Already a Public Private Partnership has been established in cyber space, focusing more on Critical Infrastructure protection and digital economy. However, a partnership about offensive capabilities

has been established years ago. Going back in 2007, Estonian cyber-attack was a well-orchestrated but not sophisticated. The operation was conducted not only by a state actor but it was an alliance between member of the Russian government and organized crime, Estonian ex-president Toomas Ilves called it a Public Private Partnership (PPP)[iii]. It is clear that Russia established a partnership with the organized crime in order to achieve its political goals.

One year later in Georgia, Russia developed further its capabilities conducting a cyber-operation in coordination with a kinetic war. Given the highly interdependence of Georgian networks with Russian ones, Moscow used the capability of private sector in order to get involved to a limited conflict. Russia set out to test and develop its capabilities to limited conflicts and also to build capacity.

While Russia was testing out its capabilities, the cyber operation, Stuxnet which changed the nature of cyber warfare, was taking place. Despite the success or failure of the operation, the reaction of Iranian government, and the increasing number of states establishing cyber commands and developing offensive capabilities, it turns out that the debate on cyberspace has been shifting from securitization to militarization.

Moreover, Snowden revelations show that the U.S. government has established a partnership with private sector in order to generate options and capabilities for later use. The contribution of private sector to this partnership was tremendous but it was not a mutual beneficial partnership. The research paper examines the *cui bono* logic of this partnership and the tradeoff that private sector should deal with.

In conclusion, the analysis of case studies turns out that states are striving to securitize the cyber domain and to test out their capabilities simultaneously. The initiatives of states to maximize security in order to securitize the cyber domain have ended up to militarization of cyber realm.

Given a cyber war is almost impossible to take place, the militarization of cyberspace can be interpreted as a step taken by states to get a full understanding about the nature of cyber domain and to balance the power. Unlike the physical world, in cyberspace the militarization and cyber arms race will never stop. Every actor is able to carry out an attack. The point of militarization is to increase the degree of sophistication both for the offense and the defense in order to tackle cyber attacks carried out by non-state actors.

Keywords: securitization, cyber warfare, militarization, cyber offensive capabilities, PPP

REFERENCES

i Yin, R.K. (2006). Case Study methods (Revised Draft). In J.L Green, G. Camilli, P. B. Elmore, A. Skukauskaite & E. Grace, Handbook of Complementary Methods in Education Research (pp.111–122). Washington D.C.: American Educational Research Association.

ii Buzan, B., Waever, O., & Wilde, J. D. !998). Security: A New Framework for Analysis. Boulder: Lynne Rienner.

iii Osnos, E., Remnick, D., & Yaffa,J. (2017). Trump, Putin, and the New Cold War. Retrieved March 15, 2017, From The New Yorker http://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war

ADDRESSING THE SECURITY DILEMMA IN CYBERSPACE

Madis Metelitsa
University of Tartu
madism@ut.ee

INTRODUCTION

The problems caused by the existential condition of uncertainty in international relations are as new as today's newspaper headlines and as old as international history itself.[1] In the context of international relations theory, the existential condition of uncertainty means that governments (their decision-makers, policy analysts *etc.*) can never be 100 percent certain about the current and future motives and intentions of those able to harm them.[2] This predicament leads to the emergence of security dilemma, where fear, uncertainty and mistrust coupled with the anarchic nature of the international system brings about the situation where the efforts by some actors (traditionally, states) to enhance their security decrease the security of others.[3] This complex phenomenon forms one the cornerstones of the twenty-first century security studies.[4]

Alongside with the changing conceptual understandings of security studies in the twenty-first century, we have also been witness to the appearance of new security challenges. In this regard, it is safe to say that there is no national security problem more common to this century both in its definition and form than cybersecurity. Although cyber-attacks ***per se*** still do not compare to that of a nuclear explosion, they do pose a serious and ever-increasing threat to international security and as real-world examples suggest that cyber warfare will play a lead role in the conflicts of the future.[5] With that in mind, this master's thesis builds on the preexisting literature concerning the security dilemma in cyberspace and aims to analyze how the security dilemma framework and traditional means of mitigations apply to cyberspace and cybersecurity, and second, how the traditional means of mitigation have been used by international organizations like the United Nations to resolve the cyber security dilemma.

RESEARCH QUESTIONS AND METHODOLOGY

As stated previously, this thesis focuses on the following two research questions:

Question 1: How does the security dilemma framework and traditional mitigation practices apply to cyberspace and cybersecurity?

Question 2: What actions have been taken by the UN to mitigate the cybersecurity dilemma and more importantly – how effective have those actions been?

Since there is considerable academic debate in the international relations literature over the concept of security dilemma, concerning both the implications of anarchy and uncertainty in the international

1 Booth, K.; Wheeler, N. (2008) "Rethinking the Security Dilemma", in P. D. Williams (Ed.), 2008, Security Studies: An Introduction, New York: Routledge, pp. 136–137.

2 Booth, K.; Wheeler, N. (2008) "Rethinking the Security Dilemma", p. 134.

3 Jervis, R. (1978) "Cooperation Under the Security Dilemma", World Politics, Vol. 30, No. 2, pp. 169.

4 Booth, K.; Wheeler, N. (2008) "Rethinking the Security Dilemma", p. 133.

5 Geers, K. (2010) "The Challenge of Cyber Attack Deterrence", Computer Law & Security Review. 26, No. 3, pp. 298–299.

relations and on the question, whether cooperation between states is possible under such conditions, the author uses the theoretical approach developed by Ken Booth and Nicholas Wheeler. According to those authors, the security dilemma can be defined as a two-level strategic predicament, consisting of the dilemma of interpretation, and the dilemma of response.[6] The dilemma of interpretation is the predicament that has to be faced by decision-makers when they are confronted with a choice between two significant and usually (but not always) undesirable alternatives about the military policies and political postures of other actors. The dilemma of response follows the dilemma of interpretation and means the problematic choice that decision-makers must face in formulating policy responses to the interpretation of another actor's (i.e. state's) perceived intentions.[7] In dealing with such uncertainties, the author follows the mitigatory logic, according to which the uncertainty and thus the security competition between states can be ameliorated or dampened down for a time, but never fully eliminated.

The reason why the United Nations was chosen as a case study is twofold. First and foremost, the UN has been one of the main global forums for high-level discussions on international cyber security, bringing together key actors in the cyber realm. Second, the UN has been engaged in both cyber norm development, where the UN Group of Governmental Experts has been at the forefront of the said activity, and in developing and promoting different confidence-building, stability and risk reduction measures. As this thesis focuses on the security dilemma in cyberspace, the empirical analysis concentrates on the politico-military stream of negotiations in the UN, which is concerned with how information technologies and means can be potentially used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of the states. Because this research project is still ongoing, additional international organizations (*e.g.* OSCDE) may be included in the analysis.

To answer the first research question, an in-depth literature review is performed. This is necessary to identify what means for mitigation, and in what way can be used by international organizations, such as the UN, to ameliorate the security dilemma in cyberspace. For the second research question, a two-part approach is used. First, to answer the question of *what* means of mitigation (*i.e.* forms of cooperation) have been used by the UN to mitigate the security dilemma, and more importantly, *why* such methods of cooperation were chosen, the author uses official policy documents (*e.g.* GGE reports), corresponding academic literature and interviews conducted with the cyber security experts who have taken part of the UN GGE negotiations. To answer the second part of the question – *how effective* have such efforts at cooperation been, the author uses the available datasets on cyber incidents,[8] to assess the behavior of the states after a certain level of cooperation has been achieved. When assessing the behavior of the states, the author accepts the following premises. Most importantly the author recognizes the fact that a great deal of information on cyber operations remains secret, but given sufficient time, enough information for an adequate analysis will surface, due to leaks (*e.g.* Stuxnet) and disclosures by different government agencies and internet security firms. With this in mind, the author stops the data collection in 2015 to ensure sufficient lag time for reporting and disclosing of cyber incidents.

EXPECTED RESULTS

This master's thesis expects to provide the following results. First, it expects to show how the traditional security dilemma concept applies somewhat differently in cyberspace and what means of mitigation can be used by international organizations to ameliorate such security dilemma. Second, it aims to ex-

---

6 Booth, K.; Wheeler, N. (2008) *The Security Dilemma*, pp. 4–5.

7 *Ibid.*

8 E.g. the cyber-conflict dataset developed by Ryan Maness and Brandon Valeriano. See: http://relationsinternational.com/making-progress-with-data-updating-the-cyber-incident-and-dispute-data/; Center for Strategic and International Studies (CSIS) reports on Significant Cyber Incidents. See: https://csis-prod.s3.amazonaws.com/s3fs-public/170519_Significant_Cyber_Events_List.pdf?HJ4k1Bt7x.zleLsdr9m6SQbkWHtuNJ39.

plain why the United Nations has opted for certain forms of cooperation, and third, how effective have such methods of cooperation been.

Keywords: security dilemma, cyber security, mitigation, cooperation, the United Nations.

REFERENCES

1. Booth, K.; Wheeler, N. (2008) "Rethinking the Security Dilemma", in P. D. Williams (Ed.), 2008, *Security Studies: An Introduction*, New York: Routledge.
2. Geers, K. (2010) "The Challenge of Cyber Attack Deterrence", *Computer Law & Security Review*, Vol. 26, No. 3, pp. 298–303.
3. Jervis, R. (1978) "Cooperation Under the Security Dilemma", *World Politics*, Vol. 30, No. 2, pp. 167–214.

CAMBODIA'S EFFORT ON CYBERSECURITY REGULATION: POLICY AND HUMAN RIGHTS' IMPLICATIONS

Ms Somaly Nguon
Tallinn University of Technology
somaly.ngoun@gmail.com

Cambodia is one of the developing countries in ASEAN. Indifferent from other countries, the nation is also a victim of cybercrime. Cambodian population is around 15.82 million while 68% of the total population is under 30 years old.[1] The Cambodian Genocide was carried out by Khmer Rouge regime led by Pol Pot between 1975 and 1979 in which an estimation of more than two million people died and most of the infrastructures were destroyed. Until 1993, Cambodia was transformed to be a democratic country and held its first national election.[2] The majority of Cambodian people are low educated and also lack access to information, which can help them make a rational decision.

In the last few years, Cambodia has achieved significant progress in promoting the use of ICT to improve the administration system and service to citizens and entrepreneurs.[3] However, the country is lagging far behind technology development, and the policy area concerned with the regulation of online behavior is a profound implication for essential human rights such as privacy, freedom of expression and information in an interconnection era. Current legislation fails to keep pace with digital development that severely threatens the fundamental human rights.[4]

The Cambodian government announced in 2012 that it was in the process of drafting Cambodia's Cybercrime law, which Internet community fears that it could extend traditional media restraint online.[5] After the announcement was made, a hacker group called NullCrew launched its campaign named Operation The Pirate Bay (OpTPB) to attack Cambodian websites in protest of Internet censorship and the arrest of Gottfrid Svartholm Warg, the 27-years old co-founder of torrent sharing site The Pirate Bay. OpTPB targeted several websites of Cambodian businesses and government organizations, including the armed force. As result, OpTPB leaked highly confidential information and posted a number of passwords for other hacktivist groups to use. Another hacktivist collective, Anonymous, also instigated a cyber war against Cambodia in protest of the arrest of Warg. Over 5,000 documents were success-

---

1 UN, World Statistics Pocketbook:Cambodia.
Available at: http://data.un.org/CountryProfile.aspx?crName=Cambodia (12.10.2016)

2 Kong, P. Overview of the Cambodian Legal and Judicial System. Introduction to Cambodian Law. Hor, P., et al (Eds.). Phnom Penh, Konrad-Adenauer-Stiftung 2012, p 7–8.

3 Cheang, S., Sang, S. Sate of Cybersecurity and the Roadmap to Secure Cyber Community in Cambodia. International conference on availability, reliability and security, IEEE 2009. pp 652–657, p 652. doi: 10.1109/ARES.2009.144.

4 Freedom House, Freedom on the Net: Cambodia, Report 2013, p 8–9. Available at: https://freedomhouse.org/sites/default/files/resources/FOTN%202013_Cambodia.pdf (26.09.2016)

5 Ibid.

6 YMAC, Security: How can we enhance cybersecurity in ASEAN? Youth Model ASEAN Conference 2016, p 2. Available at: http://www.sp.edu.sg/ymac/documents/securitycybersecurity.pdf (20.09.2016).

fully stolen and leaked from Cambodia's Ministry of Foreign Affairs.[6] Followed the above incidents, the Cambodian government announced new law requiring surveillance cameras in the Internet cafes. The law has mandated that all Internet cafes and telephone centers install surveillance cameras and retain footage for at least three months.[7]

Cambodia's Ministry of Post and Telecommunication (MPTC) reported Internet penetration in Cambodia increased from 20 thousands in 2008 to over 7.16 million by June 2016, around 46% of the total population of around 15.82 million.[8] Cambodia is currently known as a home to the largest youth and adolescent population in the South East Asia region, and they are active on social media, particularly Facebook. Social media agency in Singapore has released an infographic on the digital statistical indicators that number of active social media users in Cambodia increased from 3.4 million in 2016 to 4.9 million in 2017.[9]

Civil societies expressed concerns that leaked draft law on cybercrime has begun to threaten the freedom on Internet through its broad terms used under Article 28 of the drafted law. Under Article 28 of the draft law regulates the users' expression behavior regarding content and websites. People who "establish contents deemed to hinder sovereignty and integrity of the country or government agencies and ministries, incite or instigate, generate insecurity and political cohesiveness, and damage the moral and cultural values, etc. are punishable from one to three years imprisonment and fine from five hundreds U.S. dollar to one thousand and five hundreds U.S. dollar (500–1500$)".[10]

ICT development in Cambodia is still at the crucial stage comparing to other countries in the region. Cambodia has one of the lowest Internet connectivity rate in Southeast Asia according to Information Society Statistical profile in Asia Pacific published by International Telecommunication Union (ITU) in 2009.[11] National ICT Development Authority (NiDA) was in charge of ICT development of Cambodia, has been integrated into MPTC's structure. The National Cambodia Computer Emergency Response Team (CamCERT) was established in December 2007 in order to deal with cybersecurity and cybercrime matters. There is also Cybercrime Unit in the National Police department in charge of telecommunication crime. Cambodia left over many important tasks concerning securing cybersecurity according to Cyber willingness profile published by ITU in 2014.[12] Cyberwellness in Cambodia has been discussing in a small circle among scholars because it is seems to be new topic in this small and less developed country.

This research aims to study on Cambodia's effort in combating against cyberthreats; should Cambodia have this particular cybercrime law. Does the current draft law address the cyber threats? Whether it is necessary and proportionate? This research also aims to propose international good practices that could be taken into account and suggest some concrete steps that the Royal Government of Cambodia (RGC) may consider implementing for a better development in combating against cyber threat and serve the best interest of online community in Cambodia.

This research will focus on the analysis of RGC's current effort regarding cybersecurity regulation and policy that will play the important part in the context of Cambodia. Moreover, this research will include

---

7 Mong Palatino, "Cambodia: Mandatory Internet Surveillance Cameras", Global Voice, 09.12.2012. Available at: https://globalvoices.org/2012/09/09/cambodia-mandatory-internet-surveillance-cameras/ (20.09.2016)

8 MPTC, Fact Sheet on Telecommunication Sectors. June 2016. Available at: http://www.mptc.gov.kh/site/detail/607 (10.01.2017)

9 Joseph Soh, "Cambodia's 2017 Social Media and Digital Statistics", Geeks 09.02.17. Available at: http://geeksincambodia.com/cambodias-2017-social-media-digital-statistics/ (14.02. 2017)

10 Article 19, Cybercrime Law, Draft V.1, unofficial translation to English, Art.28. Available at: https://www.article19.org/data/files/medialibrary/37516/Draft-Law-On-CyberCrime_Englishv1.pdf

11 ITU, Information Society Statistical Profile Asia and the Pacific, 2009. p 17. Available at: http://www.itu.int/ITU-D/ict/material/ISSP09-AP_final.pdf (26.09.2016).

12 ITU, Global Cybersecurity Index & Cyberwellness Profiles. 2015. p 117–118. Available at: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf (26.09.2016)

comparative study and discussion on international and regional legislation cooperation in combating against cybercrime. In addition to discussion on the process of drafting cybercrime law, this research will also concentrate on the controversial issues concerning human rights obligations and freedom in cyberspace. In order to achieve the aim of this research, the author have to answer to main research questions as following:

- **What are the main components of Cambodia's cybersecurity policy and how it was developed?**
- **Is the draft law on cybercrime in the line with the international human rights obligations of Cambodia?**

Critical review of legislation and policy documents, comparative study of the policy processes, and analysis of the case law will be used as research methodology for this research. The qualitative method has been used in order to describe and analyze for an improvement of the controversy-drafted law on cybercrime in Cambodia. This research is achieved by conducting extensive desk research, and the collection of documents and data based on the basic literature on policy and strategy of cooperation, legal sources, relevant statistic, reports from NGOs, presentation, speeches, including press media released.

SESSION 6: eGOVERNMENT & SECURITY

Session moderated by Prof TOBIAS EGGENDORFER,
University of Applied Sciences Ravensburg-Weingarten

Mr Harish Gowda & Mr Matt Reynolds,
"REAL-TIME VIDEO STREAM SUBSTIUTION",
University of Adelaide

Mr Nicolas Mayer,
"THE ENTRI FRAMEWORK: SECURITY RISK MANAGEMENT ENHANCED BY THE USE OF ENTERPRISE ARCHITECTURES",
Luxembourg Institute of Science and Technology

Mr David Hubczenko,
"INVESTIGATION INTO TWITTERBOT IDENTIFICATION TECHNIQUES",
University of Adelaide

Mr Lachlan Gunn,
"GEOLOCATION OF TOR HIDDEN SERVICES: INITIAL RESULTS",
Tallinn University of Technology

REAL-TIME VIDEO STREAM SUBSTITUTION

Matthew Sorell, Matt Reynolds, Harish Gowda
The University of Adelaide
matthew.sorell@adelaide.edu.au, matt.reynolds@student.adelaide.edu.au,
harish.gowda@student.adelaide.edu.au

INTRODUCTION

NATO's Locked Shields[1] is an annual live-fire cyber defence exercise organised to aid in the training of security experts tasked with protecting national IT systems. The scenario-based exercise focuses on the attack and defence of the network and service infrastructure of a fictional country, including military command and control systems, and unmanned aerial vehicles. One such attack performed at the 2017 event focused on the substitution of footage from a military drone's real-time video feed. The defence network was compromised and the video feed replaced.

Taking inspiration from the recently concluded event and the attack performed on the drone, this project investigates how a real-time video stream can be seamlessly substituted whilst going undetected. Consequently, the investigation will generate the need for further research into uncovered vulnerabilities and their potential solutions.

PROJECT OBJECTIVES

This project aims to develop a tool, using a series of methods or techniques, capable of hijacking a real-time video stream. The tool will then perform the seamless substitution of the video stream with an arbitrary video or an alternate stream. The project initially aims to identify all the challenges and constraints relating to conducting such an attack while also acknowledging some of the complexities of the project. To solve the identified constraints, the project is divided into two parts:

- Multimedia (Matt Reynolds)
- Multimedia Networking (Harish Gowda)

The primary requirements of the tool are to ensure the substitution is seamless, and both the source of the real-time stream and its destination/viewer are unaware of the substitution.

METHODOLOGY

MULTIMEDIA

This aspect of the project considers the manipulation and substitution of the real-time stream with a focus on utilising MPEG standards 1, 2 and 4. The objective is to pull apart and break down the video stream into its elementary components. Relevant stream control data including timestamps, clock references and frame rate information are to be extracted and kept, with the video frames discarded. The stream can then be re-encoded using the retained stream control data and arbitrary video frames on the fly.

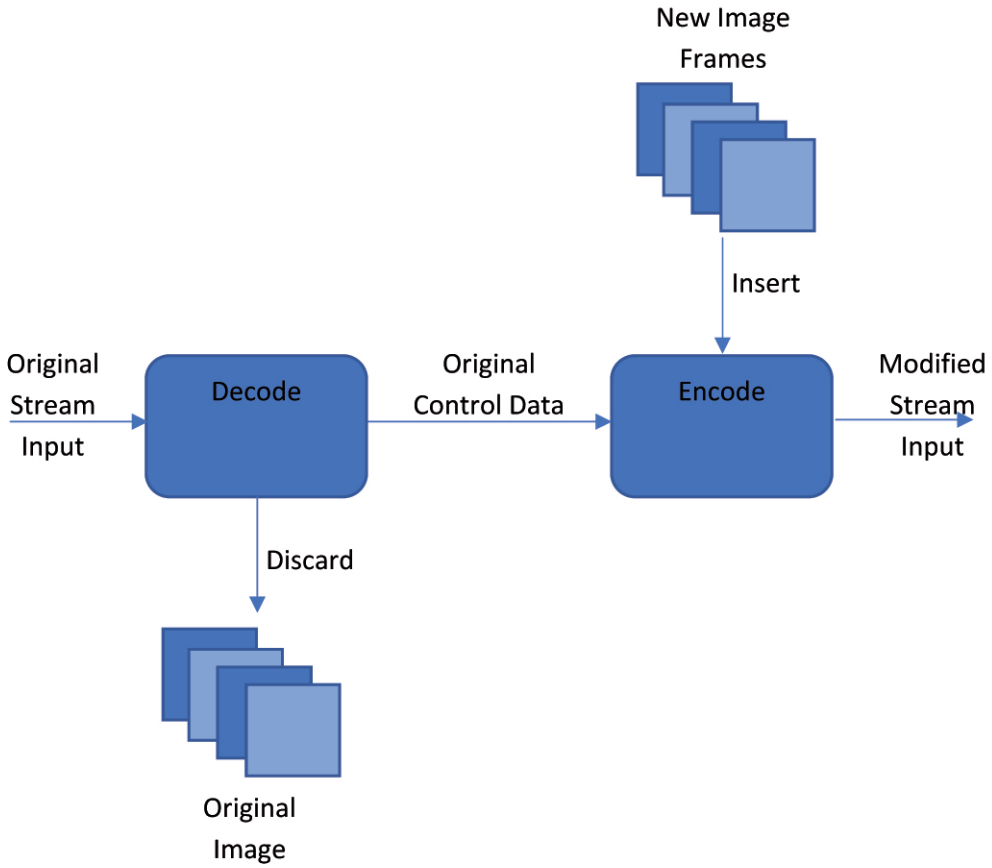

Figure 1. High-Level video substitution overview

The following challenges have been identified and will need to be addressed:

- Real-Time – efficient substitution to ensure fluid transition with no delay in the stream.
- Seamless transition – effectively manage differing frame and data rates.

MULTIMEDIA NETWORKING

The Multimedia Networking part of the project will mainly be considering different attack strategies which can be implemented to gain access to the real-time stream while also keeping the end users unaware of any breaches in the network. Prior to considering different attack strategies, extensive literature review will be conducted in order to gain the required knowledge to undertake this project. The initial research phase of this project considers the background and technical knowledge of Multimedia Networking. This project is to assume that encryption is not implemented in any layers. Encryption adds to one of the many complexities of this project. Any decryption techniques are beyond the scope of this project. However, the possibility of encryption being implemented in different stages of the project will be acknowledged as a defence mechanism to any techniques found.

Looking from an OSI model's layer stack perspective, this project will mainly be dealing with the following layers[2]:

- Application Layer – establishing and controlling media sessions between end points.
- Presentation Layer – where all the cryptographic protocols reside and provide communications security.
- Transport Layer – provides end-to-end connection to transport application layer messages.
- Network Layer – determines the path for the packets/datagram to the transport layer.

IPTV allows transmission of live video footage over the internet. This is similar to traditional broadcast television except this transmission takes place over the internet. A controlled environment will be setup using an IP camera and Raspberry Pi where a network attack will then be conducted. This will be used to examine how Real-Time Streaming Protocol (RTSP) allows streaming of live content in the applica-

tion layer and how it keeps track of the states once a connection has been established. This type of simulation will also be used to examine Real-Time Transfer Protocol (RTP) in the transport layer which is used to transport real-time media data established over RTSP. Finding any vulnerabilities to exploit in these protocols being used will allow us to gain access to established connection between end users.

Several different attack strategies will be examined throughout the course of this project. After initial research and testing of known network attack strategies, this project will move on to finding new unique methods of session hijackings in different levels[3]. At this level as a network hijacker, we can hopefully not only hijack already established sessions, but can also create new sessions from data acquired via data sniffing. Some of the different network attack strategies will include:

- Man in the middle attack
- RTSP/RTP session hijacking
- IP spoofing
- TCP/UDP session hijacking
- Application layer session hijacking

FUTURE APPLICATIONS

This research primarily has defence related applications including manipulation of live reconnaissance and drone footage. Aside from these applications, with a current day increase in terrorism, there may be a need for a system able to counter malicious propaganda, including but not limited to 'recruiting videos'. This is a real-world issue which this project could aid in resolving.

As with any exploit, there is a need to ensure it cannot reoccur. Although the primary focus of the project is to develop a method for performing the attack, it will generate the need for targeted research focusing on the development of countermeasures to exploits uncovered by the project.

Keywords: Real-Time Stream, MPEG, Network Attack, IPTV, RTSP, Multimedia networking

REFERENCES

1 "NATO Cooperative Cyber Defence Centre of Excellence," NATO Cooperative Cyber Defence Centre of Excellence, [Online]. Available: https://ccdcoe.org/locked-shields-2017.html.

2 J. F. Kurose and K. W. Ross, Computer Networking: A Top-Down Approach 5th Edition, 2009.

3 S. Kapoor, "Session Hijacking: Exploiting TCP, UDP and HTTP Sessions," [Online]. Available: http://www.infosecwriters.com/text_resources/pdf/SKapoor_SessionHijacking.pdf.

THE ENTRI FRAMEWORK: SECURITY RISK MANAGEMENT ENHANCED BY THE USE OF ENTERPRISE ARCHITECTURE

Nicolas Mayer
Luxembourg Institute of Science and Technology
Nicolas.Mayer@list.lu

Risk management is today a major steering tool for any organization wanting to deal with Information System (IS) security. Whether for purely compliance purposes, business development opportunities, or even governance improvement, organizations tend to implement a security strategy based on an IS Security Risk Management (ISSRM) approach. However, organizations have to deal with drawbacks that increase the difficulty of managing security risks: complexity and continuous evolution of current IS, regulatory pressure involving various and inter-connected ISSRM requirements, and difficulty to have a clear and manageable documentation of ISSRM activities. Classical ISSRM methods are thus no more suitable to deal with these issues in such a context of compliance and governance.

We claim that a connection with Enterprise Architecture Management (EAM) contributes to deal with these issues. EAM has shown to be a valuable and engaging instrument to face enterprise complexity and the necessary enterprise transformation. In this project, we propose to integrate EAM with ISSRM, in order to benefit from the capabilities of EAM at the level of risk management. Such a tool-supported integration of EAM and ISSRM, through the link established between enterprise architectures and related identified risks, provides a better consideration of IS and their inherent complexity and evolution. Moreover, enterprise architectures include explicitly regulations and external requirements. Finally, by introducing a model-based approach, documentation of ISSRM activities will be highly improved compared to the usual informal text descriptions.

The general objective of our project is to improve ISSRM by defining a framework (modelling language, method, tool – the modelling language being the scope of this paper) called the ENTRI framework. This framework especially incorporates results from EAM research and aims at being used for compliance and governance purpose. To do so, we have first integrated the EAM concepts with the ISSRM domain model [1], an existing conceptual model depicting the ISSRM domain, to define the so-called EAM-ISSRM integrated model. We have agreed on two ways of improving the ISSRM domain model with EAM aspects: the explicit introduction of the environment of the assets (e.g., stakeholders and associated constraints) and the refinement of (business and IS) assets through the use of the set of concepts provided by EAM approaches (see Figure 1).

In order to validate the EAM-ISSRM integrated model, we have collected information about its utility to deal with the challenges identified (i.e. enterprise complexity and continuous evolution, regulatory pressure, and weakness of the documentation) and its usability as the conceptual foundation to design our framework to perform ISSRM. To do so, we have elaborated a validation method for the EAM-ISSRM integrated model, based on a validation group composed of experienced ISSRM practitioners. We considered including EAM experts in the validation group, but we decided not to do so because our goal is to improve ISSRM and our target of users is focussed on ISSRM practitioners. A necessary criterion to be part of the validation group was to have an ISSRM background and a basic knowledge of security standards such as ISO/IEC 27001. Nine participants, coming from various sectors (Telecommunications, Data centres, European institutions, Corporate services...) and with various positions (Security consultants, Security officers, Risk officers...), have been part of the validation group. We have assessed the utility and usability of the EAM-ISSRM integrated model through questions and exercises, based on

a fictitious case, and through the satisfaction to use a system based on this model with the help of a SUS (System Usability Scale) questionnaire [2].

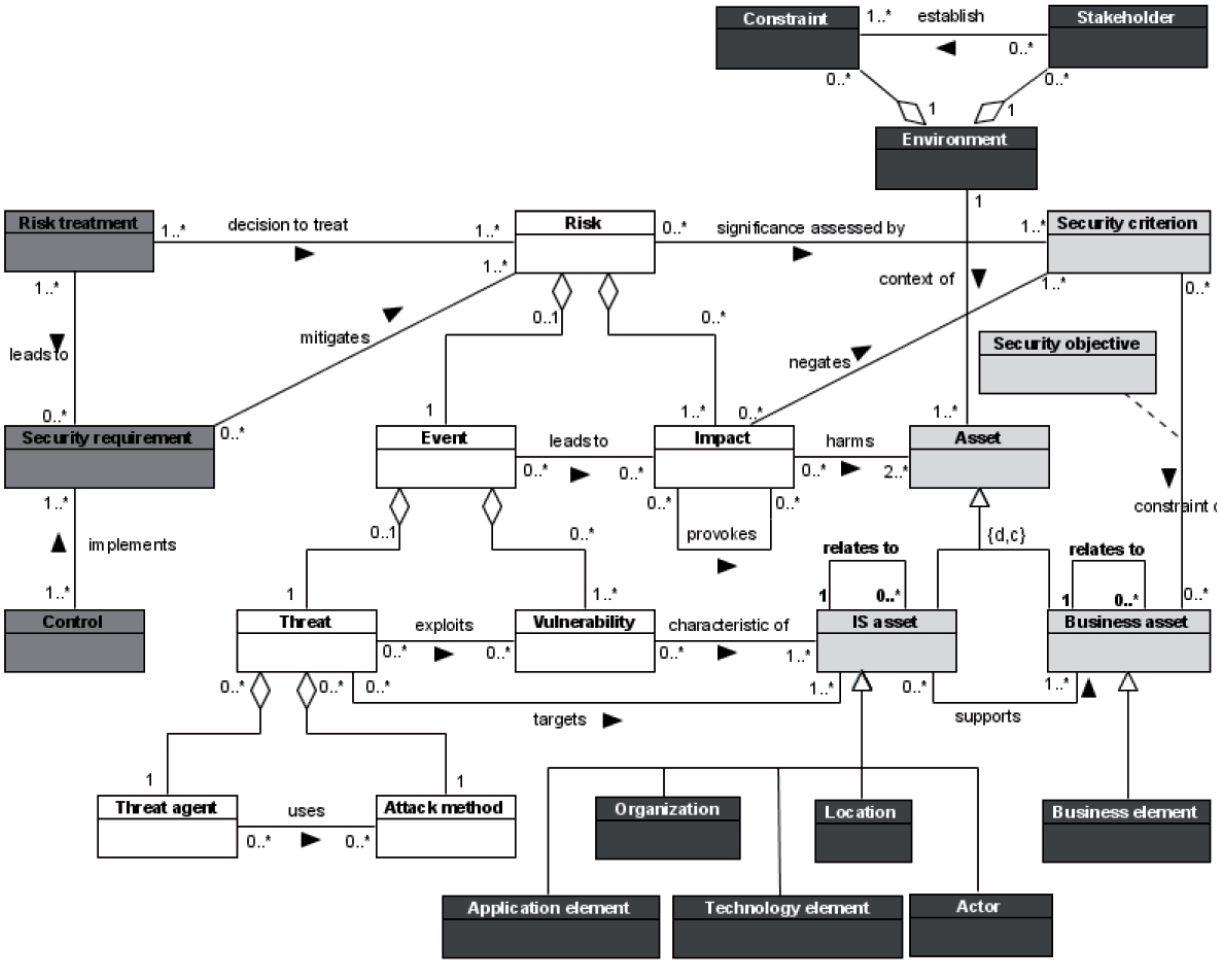

Figure 1. The EAM-ISSRM integrated model. Asset-related concepts are represented by light-grey boxes, risk-related concepts by white boxes, and risk treatment-related concepts by dark grey boxes. The black boxes represent newly added concepts from EAM, and concern assets and their environment.

The EAM-ISSRM model constitutes the underlying conceptual model for the EAM-ISSRM language. ArchiMate [3] is a standard modelling language produced by The Open Group, an industry consortium developing standards, for the representation of EA over time, as well as their motivation and rationale. In 2015, a White Paper aiming at providing guidelines to ArchiMate users on how to model enterprise risk and security with the ArchiMate language has been published [4]. The contribution of this White Paper has been called a "Risk and Security Overlay" (RSO) of the ArchiMate language, i.e. a visual syntax being a candidate to support our EAM-ISSRM integrated model. An evaluation of the support level proposed by the RSO to represent graphically our model has been performed. The evaluation of the RSO visual notation has been done at two different levels: completeness with regards to the EAM-ISSRM integrated model and cognitive effectiveness, relying on the nine principles established by Moody [5]. Regarding completeness, we can consider the RSO as an appropriate notation to support the EAM-ISSRM integrated model. However, regarding cognitive effectiveness that appeared as a key concern during the validation focus group discussions, many gaps have been identified. In order to challenge the design decisions of the RSO of ArchiMate and to find ways of improvement, we are currently analysing the CORAS modelling language. CORAS does not specifically support EAM but is a customised language for risk modelling [6], and thus a relevant candidate for visual notation of (part of) the EAM-ISSRM integrated model.

Acknowledgments. Supported by the National Research Fund, Luxembourg, and financed by the ENTRI project (C14/IS/8329158).

Keywords: Security risk management, Enterprise architecture, Modelling language, ArchiMate

REFERENCES.

1. Dubois, E., Heymans, P., Mayer, N., Matulevičius, R.: A Systematic Approach to Define the Domain of Information System Security Risk Management. In: Nurcan, S.; Salinesi, C.; Souveyet, C.; and Ralyté, J. (eds.) Intentional Perspectives on Information Systems Engineering. pp. 289–306. Springer Berlin Heidelberg, Berlin, Heidelberg (2010).
2. Brooke, J.: SUS-A quick and dirty usability scale. Usability evaluation in industry. 189, 4–7 (1996).
3. The Open Group: ArchiMate® 2.1 Specification. (2013).
4. Iver Band, Wilco Engelsman, Christophe Feltus, Sonia González Paredes, Jim Hietala, Henk Jonkers, Sebastien Massart: Modeling Enterprise Risk Management and Security with the ArchiMate® Language. The Open Group (2015).
5. Moody, D.: The "Physics" of Notations: Toward a Scientific Basis for Constructing Visual Notations in Software Engineering. IEEE Transactions on Software Engineering. 35, 756–779 (2009).
6. Lund, M.S., Solhaug, B., Stolen, K.: Model-Driven Risk Analysis: The CORAS Approach. Springer-Verlag Berlin and Heidelberg GmbH & Co. K, Berlin ; London ; New York (2010).

INVESTIGATION INTO TWITTERBOT IDENTIFICATION TECHNIQUES

David Hubczenko
University of Adelaide
a1647335@student.adelaide.edu.au
Supervisor: Dr Matthew Sorell

INTRODUCTION

This research is being undertaken as part of an Honours project at the University of Adelaide. This research will investigate techniques used in the identification and prevention of malicious Twitterbots.

Problem Statement

Social media is a widely-used platform to connect people and share ideas. Twitter is one of the major social media networking tools that is currently available. On June 30, 2016 Twitter hosted 313 million monthly active users [1]. The main feature of Twitter is the ability to post short, 140-character limited messages called Tweets.

There is a growing concern that Twitter can be utilised as a platform for information warfare. On Twitter, social engineering attacks can be conducted in an attempt to influence the opinion of Twitter users. These attacks could be made to influence political outcomes or cause civil unrest. On Twitter, social engineering attacks can be facilitated through the use of Twitterbots. These are automated accounts on Twitter that are controlled by a computer program. They can automatically post content and interact with other Twitter users. Twitterbots can be easily constructed using the Twitter Application Programming Interface (API). A recent research paper estimates that 9–15% of Twitter accounts are automated [2].

Twitterbots are effective at social engineering because they can generate a large amount of content. A view can be promoted by continual tweeting and retweeting this content. People are influenced by these views because of this large volume. Psychology research indicates that an extensive quantity of messages can highly increase the persuasive power of the messages [3]. Recently, it has been suggested that the 2016 United States presidential elections were influenced by Twitterbots. It is estimated that a third of pro-Trump tweets and a fifth of pro-Clinton tweets during the election were generated by Twitterbots [4].

Twitterbots can also be used to spread fake news on a large scale. Fake news is misinformation that is created to deceive. It can be used to smear the reputations of various individuals and organizations or to artificially build reputations. Fake news can be effective since the information appears to originate from supposedly real people [5].

Twitterbots can also be used to inflate the popularity of Twitter users. The popularity of a Twitter user can be measured by the number of followers that they have. Twitterbots can be made to follow a particular user to make them appear more popular than they actually are [6].

Twitterbots can also be used for economic gain. In 2014 Twitterbots were used to make the company Cynk appear popular. Automated trading algorithms increased the value of the company to $5 Billion [7]. The price of shares in Cynk rose from six cents to $21 [8].

Twitterbots can also be used to influence the trending topics on Twitter. Tweets are considered to be part of a topic if they include a hashtag about the topic. The trending topics are the most heavily tweeted topics. The trending topics can be altered by using a large number of Twitterbots to promote certain topics [6].

RESEARCH QUESTIONS

There has been a large amount of research into the prevention of Twitterbots. In my research, I will investigate the current state and viability of methods used in the identification and prevention of Twitterbots.

The main question that is considered by this research is "How can Twitterbots be successfully identified". The successful identification of Twitterbots will allow Twitter accounts to be screened to prevent the activities of malicious Twitterbots. Researchers have proposed a number of machine learning techniques to identify Twitterbots. The inherent challenges involved in these techniques will be investigated. Other unique approaches will also be investigated.

A supplementary question that is considered is "How can Twitterbotnets be successfully identified". The term Twitterbotnet can be regarded in two aspects. A Twitterbotnet can refer to a group of Twitterbots working together in an information warfare campaign. Another way to consider a Twitterbotnet is as a group of bots that utilize Twitter as a Command and Control channel to receive commands from a bot master. The focus of this research is on the first definition but the second definition will be considered. The techniques to identify Twitterbotnets can take into account how the Twitterbots are correlated or connected on the Twitter network. Researchers have identified a number of large Twitterbotnets. The techniques used to locate these Twitterbotnets and the properties of the discovered Twitterbotnets will be investigated.

RESEARCH METHODOLOGY

To conduct this research there will be an extensive literature review. The resources that are relevant to this topic will be gathered and read. The resources will be evaluated and analyzed for the strengths and weaknesses of the different techniques. A discussion, evaluation and analysis of the various techniques will be formally written up.

OUTCOMES

The main outcome of this research will be a thesis document that will provide an in-depth discussion on the current state of Twitterbot research. This document will be relevant to government organizations and other researchers to provide an overview of the current technologies and the possible direction of future research in Twitterbots.

Keywords: Twitter, Twitterbot, Twitterbotnet, Machine Learning

REFERENCES

[1] "Twitter – About," [Online]. Available: https://about.twitter.com/company. [Accessed 7 March 2017].

[2] O. Varol, E. Ferrara, C. A. Davis, F. Menczer and A. Flammini, "Online Human-Bot Interactions: Detection, Estimation, and Characterization," *arXiv:1703.03107v1*, 2017.

[3] J. Stray, "Defense Against the Dark Arts: Networked Propaganda and Counter-Propaganda," [Online]. Available: http://jonathanstray.com/networked-propaganda-and-counter-propaganda. [Accessed 1 April 2017].

[4] D. Guilbeault and S. Woolley, "How Twitter Bots are Shaping the 2016 Presidential Election – The Atlantic," [Online]. Available: https://www.theatlantic.com/technology/archive/2016/11/election-bots/506072/. [Accessed 1 April 2017].

[5] G. O'Connor, "How Russian Twitter Bots Pumped out Fake News During the 2016 Election," [Online]. Available: http://www.npr.org/sections/alltechconsidered/2017/04/03/522503844/how-russian-twitter-bots-pumped-out-fake-news-during-the-2016-election. [Accessed 2017 April 16].

[6] J. Echeverria and S. Zhou, "The 'Star Wars' botnet with >350k Twitter bots," *arXiv:1701.02405v1*, 2017.

[7] D. Hernandez, "Why can't Twitter kill its bots?," [Online]. Available: http://fusion.net/why-cant-twitter-kill-its-bots-1793851105. [Accessed 12 April 2017].

[8] J. Solomon, "Tech stock soars 25,000% Trading halted," [Online]. Available: http://money.cnn.com/2014/07/10/investing/cynk-stock-surge/index.html. [Accessed 28 May 2017].

GEOLOCATION OF TOR HIDDEN SERVICES: INITIAL RESULTS

Lachlan J. Gunn[1], Heiki Pikker[2], Olaf Maennel[2], Andrew Allison[1], and Derek Abbott[1]
[1] School of Electrical and Electronic Engineering, The University of Adelaide, Australia
[2] Department of Software Science Faculty of Information Technology,
Tallinn University of Technology, Estonia
lachlan.gunn@adelaide.edu.au, heiki.pikker@pikker.ee, olaf.maennel@ttu.ee,
andrew.allison@adelaide.edu.au, derek.abbott@adelaide.edu.au

Tor[1] is an anonymisation service based on onion routing; requests to a server are routed through a series of nodes, selected by the client at random. One feature of Tor is the provision of *hidden services*, the locations of which remain anonymous from even the clients who access them. The client creates a channel ending at a Tor relay, then informs the hidden service of its address via a published intermediary. The hidden service then connects to this node anonymously, resulting in a chain of six relays between the client and the server.

Some previous attempts at deanonymizing Tor users used properties of the network itself[2]. Others use factors completely unrelated to Tor[3]. In practice, most attacks are not Tor-related; hacking a Tor user and using this breach to reveal its external IP address is a recurrent theme.

We consider the use of round-trip-times through the system for geolocation, an approach that is less intrusive than hacking, but more generally applicable than the measurement of environmental factors. Some previous work exists on the use of round-trip-times for deanonymization, but this used relatively intrusive congestion-based attacks[4]. We improve on this without the need to significantly load the network.

We attempt to geolocate hidden services at the continental level; this level of precision is insufficient for police action but somewhat useful for attribution, particularly by journalists and others who are not in a position to carry out sophisticated attacks.

As Tor conceals IP addresses, we must consider other means. Round-trip-time geolocation has been examined in the past[5]; however the presence of Tor masks location by sending the probe through a series of servers at unknown locations. Nonetheless, these latencies exhibit statistical properties

---

1 R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second generation onion router," in *Proceedings of the 13th USENIX Security Symposium*, San Diego, CA, 2004.

2 M. K. Wright, M. Adler, B. N. Levine, and C. Shields, "The predecessor attack: An analysis of a threat to anonymous communications systems," *ACM Transactions on Information and System Security*, vol. 7, no. 4, pp. 489–522, Nov. 2004, DOI: 10.1145/1042031.1042032.

3 S. J. Murdoch, "Hot or not: Revealing hidden services by their clock skew," in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, Alexandria, Virginia, USA, 2006, pp. 27–36. DOI: 10.1145/1180405.1180410.

4 N. Hopper, E. Y. Vasserman, and E. Chan-TIN, "How much anonymity does network latency leak?" *ACM Transactions on Information and System Security*, vol. 13, no. 2, 13:1–13:28, 2010. DOI: 10.1145/1698750.1698753

5 J. A. Muir and P. C. V. Oorschot, "Internet geolocation: Evasion and counterevasion," *ACM Computing Surveys*, vol. 42, no. 1, 4:1–4:23, 2009. DOI:10.1145/1592451.1592455.

that allow the identification of the round-trip time between the service and some kind of 'network centroid'.

We focus on hidden services because they allow repeated construction of channels to the victim, but the same attack can be mounted against individual users with a persistent identity.

We demonstrate in this study that the round-trip times from one user to a hidden service will vary with the location of the service over at least a continental scale; this implies that network latency provides meaningful location data without the use of other attacks in order to determine the relays used by the channel.

We measure the round-trip times from Adelaide, Australia to hidden services hosted on Amazon EC2 nodes in Frankfurt, Northern California, and Sydney. As Tor allows only TCP traffic, we measure the round-trip time by retrieving a static web page – the default Apache homepage provided by Debian – and measuring the time between beginning of the request and the reception of the first byte of the response. On the open internet this method yields round-trip times similar to those by p*ing*.

We take the minimum of ten such probes in order to reduce the effect of network congestion on the measured response time. We repeat this with 100 channels – without an entry guard on the client side, in order to aid repeatability – and estimate the response-time distribution with kernel density estimation[6].

In order to determine the effect of the service's choice of entry guard, we repeat this process five times for each location, each time clearing Tor's persistent state.

This allows straightforward validation of the approach; it will be less effective than other techniques that take into account pre-existing knowledge of the routing path, but in this study we consider the more pessimistic case where none of the relays are known.

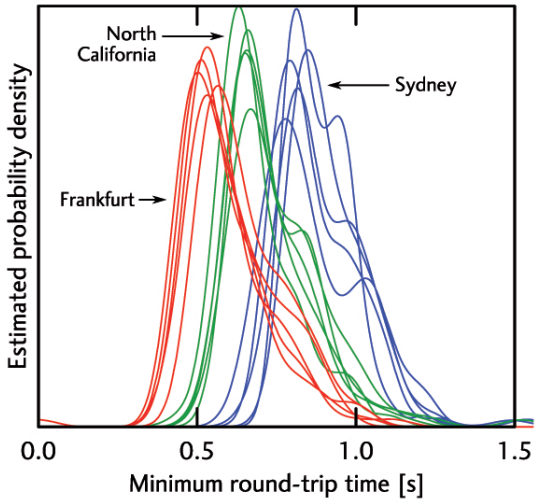

Figure 1. Round-trip-time distributions for various hidden service locations and entry guards. Each curve represents the estimated probability density for the minimum round-trip-time of a fresh circuit to a hidden service with some entry guard. We see that the distributions for a given location yield clearly different distributions.

Our measurements, shown in Figure 1, demonstrate that the location of a hidden service substantially changes its round-trip-time distribution. The systematic error introduced by long-term entry guards does not prevent the service from being geolocated at a continental level of accuracy. Furthermore, we have succeeded in doing so without the need for active attacks or a modified Tor client.

This can be most effectively countered by adding a delay at the hidden service, so that the latency of its connection to the Tor network appears fixed irrespective of location; however, this increases latency, the reduction of which is an important goal of the Tor network given its importance to usability.

Future work will involve more sophisticated modelling of Tor's latency. This will allow some random components to be removed, thereby reducing the measurement variance and allowing more accurate service location estimates.

In the short term, we intend also to examine a wider range of conditions – other measurement locations, cloud providers, and service locations that are spaced on a sub-continental scale.

---

6 G. R. Terrell and D. W. Scott, "Variable kernel density estimation," *The Annals of Statistics*, vol. 20, no. 3, pp. 1236–1265, Sep. 1992. DOI:10.1214/aos/1176348768.

Acknowledgements: Lachlan Gunn is in receipt of an Australian Government Research Training Program (RTP) Scholarship

Keywords: Tor, anonymity, network measurement

REFERENCES

1 R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second generation onion router," in *Proceedings of the 13th USENIX Security Symposium*, San Diego, CA, 2004.

2 M. K. Wright, M. Adler, B. N. Levine, and C. Shields, "The predecessor attack: An analysis of a threat to anonymous communications systems," *ACM Transactions on Information and System Security*, vol. 7, no. 4, pp. 489–522, Nov. 2004, DOI: 10.1145/1042031.1042032.

3 S. J. Murdoch, "Hot or not: Revealing hidden services by their clock skew," in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, Alexandria, Virginia, USA, 2006, pp. 27–36. DOI: 10.1145/1180405.1180410.

4 N. Hopper, E. Y. Vasserman, and E. Chan-TIN, "How much anonymity does network latency leak?" *ACM Transactions on Information and System Security*, vol. 13, no. 2, 13:1–13:28, 2010. DOI: 10.1145/1698750.1698753

5 J. A. Muir and P. C. V. Oorschot, "Internet geolocation: Evasion and counterevasion," *ACM Computing Surveys*, vol. 42, no. 1, 4:1–4:23, 2009. DOI:10.1145/1592451.1592455.

6 G. R. Terrell and D. W. Scott, "Variable kernel density estimation," *The Annals of Statistics*, vol. 20, no. 3, pp. 1236–1265, Sep. 1992. DOI:10.1214/aos/117634876

BIOS

KEYNOTE SPEAKERS

Lauri Almann is a Co-Founder of BHC Laboratory, an Estonian cyber security company. He has served in various top-level civil service positions in Estonia, including as Permanent Secretary of the Ministry of Defense. Almann served on the team that organized the response to the cyber attacks against Estonia in 2007. A Fulbright Scholar, he holds law degrees from Tartu and Georgetown universities.

Ralph Echemendia is a world-renowned cyber security expert, known internationally by his alter ego "The Ethical Hacker." He uses his talents and expertise to educate various institutions as well as protect companies and celebrity names. Ralph has played a pivotal role in the research and development of various key security technologies. His portfolio of work and reputation as a leading professional across several industries has landed him the credibility to make appearances on CNN, Fox News, USA Today, and Forbes, to name a few.

MODERATORS

Tobias Eggendorfer is a professor of IT-security at Hochschule Ravensburg-Weingarten, prior he was professor for IT-forensics in Hamburg. He was awarded his PhD by FernUniversität in Hagen in 2007 with a dissertation on e-mail security and spam prevention. He graduated in Munich in Engineering and Business Administration, in Mittweida in Technical Informatics, in Hagen in Computer Science as well as in Law and in Kaiserslautern in Adult Education. His current research interests is in computer security, especially embedded security, and computer forensics.

Nick Falkner is a senior lecturer in the School of Computer Science at the University of Adelaide. He has a strong background in learning design and loves teaching. He is heavily involved in educational research, with a focus on increasing student participation, retention, and enthusiasm. In 2015, Nick achieved the University of Adelaide's highest recognition for demonstrated impact in learning and teaching, the Stephen Cole the Elder Award. Apart from his ongoing enthusiastic commitment to the CSER MOOC, he is deeply involved in the University's AdX initiative, to develop high quality on-line learning to take useful knowledge everywhere that the Internet can reach. Nick loves to talk about innovative approaches to education and how these can be developed and deployed in a way that teachers that can both survive and enjoy!

Kari Käsper is one of the founders of the Estonian Human Rights Centre and manages its activities. He takes part in the work of refugee and equal treatment programmes. He also teaches European Union law and studies public administration in doctoral level at Tallinn University of Technology. From 2010 to 2015 he managed the equal treatment advancement projects at TUT, a part of which was the campaign "Diversity Enriches". He was involved with the youth organisation Tegusad Eesti Noored (Active Estonian Youth) 2001 – 2008, being one of the founders and helping to manage it. He also took part in the work of the European Youth Parliament between 1999 and 2008.

Olaf Maennel is a Professor for Cyber-Security at Tallinn University of Technology in Estonia. Before that he was with Loughborough University in UK and with the University of Adelaide in Australia. His interests are in: network security, routing, measurements (active & passive), IPv6 & IPv4 address sharing technologies, future Internet technology & network virtualization, ICR2016 3 topology modelling/ inference & traffic engineering, abstractions of networks for configuration management systems.

Tomáš Minárik is a Researcher at the NATO CCD COE Law & Policy Branch. He holds a law degree from the Charles University in Prague. He worked as a legal adviser at the International Law Department of the Czech Ministry of Defence, and later at the National Cyber Security Centre of the Czech Republic. His current research focuses on the legal aspects of active cyber defence, right to privacy, anonymity networks, and activities of international organisations regarding cyberspace.

Matthew Sorell is Senior Lecturer in telecommunications and multimedia engineering in the School of Electrical and Electronic Engineering at the University of Adelaide. With a background in forensic analysis of multimedia provenance, he was invited in 2014 to speak at the opening of the Centre for Digital Forensics and Cyber Security at the Tallinn University of Technology, and became an instant Eestiphile. Dr Sorell initiated and chaired the International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia (e-Forensics) in 2008 and 2009 in Adelaide, and has published research in image and video content provenance. Since 2013 he has been an invited academic observer to the UNODC Intergovernmental Experts Panel on Cybercrime (Vienna, Austria).

SPEAKERS

Ayden Aba is a final year student at The University of Adelaide, completing a Bachelor of Electrical and Electronic Engineering with a Bachelor of Finance (double degree). As part of his honours work, Ayden is undertaking research into blockchain technology and its applications in the cyber security and finance sectors. Specifically, his research focuses around the intersection of early stage financing and blockchain technology. Outside of his studies, Ayden works part-time at equity crowdfunding platform, The Australian Small Scale Offerings Board (ASSOB), as a systems engineer and research analyst.

Ben Agnew graduated with a Bachelor's Degree in Electrical and Electronic Engineering with First Class Honours from the University of Adelaide in 2014. He has worked for the School of Population Health, University of Adelaide as a research assistant to design and build a system which blocked advertising on broadcast digital TV. This was intended to be used to conduct a study into the effects of advertising on children. In 2015 he travelled to Tallinn to participate in ICR and the Cyber Security Summer School before starting his PhD in late 2015. Since then he has been conducting research into developing tamper-evident memory to provide proof-of-authenticity in offline devices such as digital cameras.

Alexander Mois Aroyo earned his M.Sc. in Computer Engineering from the Complutense University of Madrid, Spain. He began working as a researcher for the Technische Universiteit Eindhoven, the Netherlands, in the Model Driven Software Engineering department, developing a safety certification platform for a EU project – Opencoss. Afterwards, he was involved in another EU project – iLocate – an indoor / outdoor localization tool; then he continued his research in a health care project – Symbio Therapy, to help therapists to rehabilitate patients with cerebral palsy. In parallel, he was programming robots to improve therapy for autistic children. Since 2015, he is a Ph.D. fellow in robotics at the Robotics, Brain and Cognitive Sciences Department at the Italian Institute of Technology in Genova, Italy. The topic of his Ph.D. is Bringing Trust and Social Engineering towards Human Robot Interaction. The main ideas are to study the (over)trust generated by robots, the risk that social engineering could be applied through an autonomous or teleoperated robot, cyber-security aspects and privacy settings of robots.

Alžběta Bajerová holds a bachelor degree in International Relations and is currently enrolled in a graduate program Security and Strategic Studies at Masaryk University, Czech Republic. She has conducted an internship at the Institute of International Relations (IIR) in Prague, where her research focused on hybrid warfare. She gained additional analytical experience at National Cyber Security Centre (NCSC) of the Czech Republic, where she conducted research on encrypted communication and Chinese cyber threat. In her work, she mainly focuses on cyber security analysis, hybrid threats and information warfare. As an Editor-in-Chief of the Institute of Asian Studies, she also specialises in foreign policy analysis. Last year, she co-created a non-profit project Zvol Si Info that aims to increase media literacy in the Czech Republic vis-à-vis foreign propaganda. She is currently conducting an internship at Strategy Branch of NATO CCD COE in Estonia.

Alessandro Borrello is studying a Bachelor of Computer Science at the University of Adelaide, Australia. Researching under the supervision Yuval Yarom, his research interests include secure smartphone app design, development and testing, as well as detecting vulnerabilities in web applications and internet connected APIs.

Harish Gowda was born in Mysore, India, in 1994. He is currently in the final year of his double degree in Bachelor of Engineering (Honours)(Telecommunications) with Bachelor of Finance at The University of Adelaide, Australia. He has previously worked for The Government of South Australia in the Department of Planning, Transport and Infrastructure as an undergraduate electronics and communications

engineer. He is currently working on his final year honours project on real-time video stream substitution under the supervision of Dr. Matthew Sorell. Harish will be focusing on the network security aspect of multimedia networking for his project. He will also be taking part in the Estonian cyber security study tour to get more exposure and to further enhance his knowledge in the field of cyber security. Upon completion of his studies, Harish plans to commence work full time at Deloitte's Risk Advisory and Cyber Risk Services team next year.

Lachlan J. Gunn received his B.Eng. (Hons) and B.Ma. and Comp. Sc. (Pure) degrees from the University of Adelaide, Australia in 2012, receiving the 2012 J. Mazumdar Prize in Engineering and Mathematics, and four DSTO Scholarships in Radar Technology in the 2009–2012 period. In 2013 he was granted an Australian Postgraduate Award (APA), and is currently undertaking a Ph.D. under Derek Abbott and Andrew Allison. In 2014 he was awarded an Endeavour Research Fellowship by the Australian Government in order to undertake research into stochastic phenomena at the University of Angers. His research interests include usable and information-theoretic security, and the use of stochastic signal processing for characterisation of nonlinear systems.

David Hubczenko is an undergraduate student studying a Bachelor of Engineering (Honours) (Electrical and Electronic) with a Bachelor of Mathematical and Computer Sciences at the University of Adelaide. He is currently in his final year of study working on his honours project investigating Twitterbot identification techniques. In conjunction with his studies he is also working with the DST Group in CEWD through a cadetship program. His main interests are in machine learning and its applications to cyber security.

Aykan Inan is currently a research assistant and PhD student at the University of Applied Sciences in Ravensburg-Weingarten. Before that he finished a combined study program supported by the German Department of Defense at the University of the Federal Armed Forces in Munich with his Bachlor of Engineering in Computer Engineering. Subsequently he worked for the ministry in Bonn for another period of three years. He simultaneously studied IT Security at the Ruhr-University Bochum before he became a research assistant in Ravensburg-Weingarten. In addition he is also teaching Basics of Computer Science in a Bachelor's study course. His research activities comprises IT security and forensics in general. One of his future project is dealing with security issues in the field of IoT security and how to detect anomalies within the data flow. But his primary research activity lies on Cryptography and Information Security with focus on attempting to improve attacks on specific algorithms.

Kristjan Kikerpill is a 1st year PhD student at the University of Tartu School of Law. His thesis focuses on the application of crime prevention strategies for the purposes of creating more effective organisational cybersecurity policies. Current research projects include studying the human element in information security, issues regarding cyber insurance as well as problems regarding the Routine Activity Theory and its applicability to organisational cybervictimisation. In 2016, he graduated from the IT Law master's programme at the University of Tartu. Main research interests include cyber criminology, the sociology of law and questions of organisational behaviour within the context of cybersecurity.

Xingan Li (Doctor of Laws, PhD in computer science) is an associate professor of international law at the School of Governance, Law and Society of Tallinn University. His main fields of research are issues concerning legal regulation of cyberspace, and application of data mining methods in research of socio-legal phenomena. He has been a reviewer for a dozen of international journals and conferences.

Imran Khan is currently a PhD student at Insight centre for data analytics, university college cork, Ireland. His research currently focuses on the detection of insider threats in Database management systems by deploying anomaly-based intrusion detection systems. Before moving to Insight centre for data analytics, he completed his masters in computer science in Max planck institute for software systems, TU Kaiserslautern, Germany. He holds another Master degree in Electrical and electronics Engineering from Malaysia. His bachelors degree was in Computer Engineering.

Richard Matthews is PhD Student at the School of Electrical and Electronic Engineering and the University of Adelaide. His thesis is a work in progress and is titled *Fact, Fiction or Forgery: a unified model for sensor pattern noise in digital images*. He is a casual academic with the School since 2015 teaching first year engineering and supervising practical activities with students. Mr Matthews is also involved with the Entrepreneurship, Commercialisation & Innovation Centre (ECIC) at the University of Adelaide

engaged as an expert in 3D printing and additive manufacturing technologies. Mr Matthews is a Councillor at the University of Adelaide and currently serves as the President for the Adelaide Postgraduate Students Association. Mr Matthews served in the Royal Australian Air Force (RAAF) as an Officer and was awarded the Australian Defence Medal for his service. Recently he was instrumental in preparing an image provenance investigation for the Royal Society for the Prevention of Animal Cruelty known as the Byethorne Duck to validate images accused to be photo-shopped in the media. He now regularly consults with the media on image provenance queries and has been informally published on the subject.

Nicolas Mayer is Senior Research & Technology Associate at the IT for Innovative Services (ITIS) department of the Luxembourg Institute of Science and Technology (LIST). He graduated in 2004 a M.Sc. degree in Computer Science from the University Henri Poincaré (UHP) of Nancy (France). He also graduated as Engineer (M.Eng. degree) at the "Ecole Supérieure des Sciences et des Technologies de l'Ingénieur de Nancy" (ESSTIN), where he studied from 1999 to 2004. In 2004, he started his PhD at the CRP Henri Tudor (that is today the LIST) in Luxembourg in collaboration with the University of Namur (Belgium) with a thesis on security risk management and modelling. He obtained his PhD degree in 2009. From January 2009 to November 2010, he was Product manager for the business line "Security & continuity management" at the CRP Henri Tudor. Then, from December 2010 to August 2012, he worked as chargé de mission in the field of IT standardization for the National Standardisation Body in Luxembourg, where he was in charge of promoting and supporting international IT standardization in Luxembourg. From 2012 and until now, he is Principal Investigator of research and industrial projects in the field of Information Security and Enterprise Architecture Modelling.

Madis Metelitsa is a second year Master's student at the University of Tartu, where he is currently completing his degrees in Law and in International Relations. He has also obtained Bachelor's degrees in Law and in Government and Politics from the same university. During his studies, he worked as a teaching assistant at the Johan Skytte Institute of Political Studies, where he conducted seminars for first and second year Bachelor's students on Theories of International Relations and on International Organizations.

Sten Mäses is a junior researcher in Tallinn University of Technology. His research interests include human factor in cybersecurity, serious games, gamification, captology and profiling.

Somaly Nguon is a co-founder and manager at Lawtitude Tech OÜ, a legal aid company working in close cooperation with Mektory and Tallinn Law School. She received her LL.B from Paññāsāstra University of Cambodia, LL.M in International Human Rights Law, a cooperate program between Paññāsāstra University of Cambodia and Lund University of Sweden. Recently, Somaly graduated her LL.M with honor from Law and Technology program at Tallinn University of Technology. After working almost six years as legal consultant for human rights defenders and private sector including startups, Somaly also has strong interest in the area of scientific research and writing. She has a strong interest in international affairs and in particular, governance, human rights and technology law. Somaly also represented her country and the law school in the framework of Export Academy, organized by Estonian House of Commerce.

Georgios Pilichos has obtained his master degree in International Relations (International Security and Conflict Studies) from Tallinn University. His fields of interest include Cyber security, cyber weapons, conflict analysis, Turkish foreign policy, European policies and NATO. He has worked as an intern at the Embassy of Greece in Tallinn. During his studies he has participated in a number of conferences, training sessions and round tables about cyber warfare and international security. Also he has taken part in an interdisciplinary research project regarding Hybrid warfare.

Kärt Pormeister is a PhD candidate in the IT law PhD programme at the university of Tartu. Kärt holds a Master of Arts in Law degree (*summa cum laude*) from the University of Tartu and obtained a LLM degree in Health Law from the University of Houston (Texas, US) with a Fulbright scholarship. At the University of Houston, Kärt was awarded the Dean's Award for Academic Excellence in the Health Law Program and the Robert S. Toth LLM Writing Award. Her PhD thesis is focused on the critical analysis of the fragmented regulatory picture of genetic data in light on the upcoming General Data Protection Regulation. She is currently a counsellor to the Estonian Minister of Social Protection, and has formerly worked as a lawyer specialised in health law both in the private sector and at the Estonian State

Agency of Medicines. She is a member of the Estonian Bar Association since 2014 and a member of the Research Ethics Committee of the University of Tartu since 2016.

Matt Reynolds is a student in his final year at the University of Adelaide studying Electrical and Electronic Engineering. He is currently completing an Honours Research Project under the supervision of Dr. Matthew Sorell. His project aims to develop a tool for the substitution of a real-time video stream. Matt is part of a collaborative research group selected to participate in the 2017 Digital Security in Estonia Study Tour. Through active participation in this tour, Matt plans to increase his knowledge in the world of cyber security and create lasting relations with fellow peers and industry experts

Belgin Taştan is a Cyber Security MSc student in Tallinn University of Technology. She graduated from Istanbul Aydın University with Mathematics and Computer Science BSc. She is currently working as a lecturer in TUT. She has more than 10 years' experience in information technology field as a lecturer and consultant. She is an expert on Microsoft Systems and Cisco Network Technologies. She currently holds many Microsoft certificates and has participated in many seminars and web casts as a speaker.

Jūlija Terjuhana is certified data protection officer from Latvia and member of Latvian Data Protection Officers' Association. She works as a lawyer in attorneys-at-law Skopina&Azanda in Riga. Her previous work experience is related to banking and civil litigation. Her current fields of interest include data protection and intellectual property in digital environment. Mrs.Terjuhana has obtained her LLM degree from the University of Latvia and recently graduated from study program MA in Information Technology Law at the University of Tartu.

Maarja Toots is a PhD student and junior researcher at the Ragnar Nurkse Department of Innovation and Governance at the Tallinn University of Technology (TTU). She holds an MA degree in Public Administration from the same department and has a BA in Government and Politics from the University of Tartu. Maarja's PhD research focuses on e-participation and ICT-enabled public service co-creation, with a particular interest in the drivers and barriers that affect the success of ICT-enabled collaborative initiatives. As an early-stage researcher, she is also involved in European research and innovation projects dealing with issues such as the use of open data for public service innovation and the cross-border implementation of the "once-only" principle. Before joining TTU, Maarja worked for the non-profit sector for eight years, most of the time as a project manager and later as a policy analyst.

Anne Veerpalu is 1st year information technology law Ph.D student at Tartu University. She has an information technology law masters degree from the same university and part of her earlier research focus was machine readable law. She has prior two masters degrees from Estonian Business School (MBA) and Helsinki University in Public International Law. She is also a visiting lecturer of IT law masters programme of Tartu University and of business law at Estonian Business School. Anne is one of the co-organizers of Estonian chapter of Legal Hackers meetups and was the co-organizer and moderator of Tartu University LegalTech Conference of 2016 in Tallinn, Estonia. She is a practising attorney and a partner of regional law firm NJORD working primarily with corporate, M&A, private equity and fintech projects. Some of her clients operate with blockchain applications on their daily business.

Jackson Virgo is a final year Honours student at the University of Adelaide, currently completing a Bachelor of Computer Systems Engineering with a Bachelor of Finance (double degree). For his final year project, Jackson is researching the applications of blockchain technology in early stage capital markets. His specific interest include Web 3.0 application architectures and security. Jackson also works for The Australian Small Scale Offerings Board, the world's first equity crowdfunding platform, as a systems engineer and administrator.