TALLINN UNIVERSITY OF TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE

PROCEEDINGS OF THE 1ST INTERDISCIPLINARY CYBER RESEARCH WORKSHOP 2015

18th of July 2015
Tallinn University of Technology

TALLINN UNIVERSITY OF TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE

PROCEEDINGS OF THE 1ST INTERDISCIPLINARY CYBER RESEARCH WORKSHOP 2015

July 2015

The organisation of the 1st Interdisciplinary Cyber Research Workshop 2015 is supported by Tallinn University of Technology Centre for Digital Forensics and Cyber Security, IT Academy and the IT Law Programme at the University of Tartu

Editors: Anna-Maria Osula, Olaf Maennel

Published by: Tallinn University of Technology, Faculty of Information Technology, Department of Computer Science

Disain and layout: Anu Teder

Electronically available at: http://cybercentre.cs.ttu.ee/en/icr2015/

ISBN 978-9949-430-89-5 (pdf)

CONTENTS

INTRODUCTORY REMARKS

It is our great pleasure to welcome you in Tallinn, Estonia for the 1st Interdisciplinary Cyber Research (ICR) workshop, held at the Tallinn University of Technology on the 18th of July, 2015, and organised by Tallinn University of Technology Centre for Digital Forensics and Cyber Security, IT Academy and the IT Law Programme at the University of Tartu.

The idea to organise this workshop was born out of a practical need to have a platform for young as well as established scholars undertaking 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 sharing and discussing novel research across different domains, thereby allowing for the creation of new synergies.

Our programme consists of 25 presentations delivered by great minds 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. The workshop will be opened by two well-known researchers from Great Britain. **Prof Christopher Millard** from Queen Mary University of London will speak on "*Data Sovereignty, Data Flow, and International Jurisdiction in Cloud Computing*", and **Prof Jon Crowcroft** from the Computer Laboratory of the University of Cambridge will present on "*Gnawing away at Internet of Things Silos*".

Most of the speakers have been hand-picked by our international Programme Committee, and the results of the Call for Paper 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 (especially Ms Anu Teder for helping with the layout and design of this publication), and our partners from the IT Academy and the IT Law Programme at the University of Tartu.

Anna-Maria Osula, Tartu University, NATO CCD COE
Olaf Maennel, Tallinn University of Technology
Organisers of ICR2015
Tallinn, July 2015

SESSION 1: STATE AND CYBER

Session moderated by Dr RAIN OTTIS,
Tallinn University of Technology

GOVERNANCE OF CYBER-SECURITY IN ELECTIONS

Robert Krimmer, Angelica Rincon Mendez, Morten Meyerhoff Nielsen

E-ESTONIA UNDER AN ACTOR NETWORK THEORY PERSPECTIVE

Carlos Ivan Vargas Alvarez del Castillo

CHINA AND CYBER: ATTITUDE, STRATEGIES, AND ORGANISATION

Mikk Raud

DESIGNING NEW SECURITY MODELS: THE EFFECT OF AN INCREASED PROTECTION OF IDENTITY ON THE STATE

Lea Hricikova

GOVERNANCE OF CYBER-SECURITY IN INTERNET-BASED ELECTIONS

Robert Krimmer[1,2], Angelica Rincon Mendez[1], Morten Meyerhoff Nielsen[1]
Tallinn University of Technology, Ragnar Nurkse School of Innovation and Governance
[robert.krimmer | angelica.rincon | morten.nielsen]@ttu.ee

1. INTRODUCTION

In May 2007, the denial of service attacks against Estonian government information systems (see amongst others Landler & Markoff, 2007; Lesk, 2007) started an international debate about how states could defend against attacks on the national Internet infrastructure. This debate usually also highlighted the fact that only two months before the first national election had taken place that offered the possibility to vote via the Internet (OSCE/ODIHR, 2007).

In the last couple of years there have been election-related attacks on IT systems as well as incidents endangering the database security in several countries. Some of these events caused serious interruptions to the electoral process or raised suspicion that more serious problems were concerned. In a recent survey amongst election management bodies (EMB) incidents have been reported in Algeria, Bolivia, Burma, Canada, Columbia, Ecuador, Estonia, France, Honduras, Hong Kong, India, Malaysia, Mozambique, Pakistan, Russian Federation, South Africa, South Korea, Turkey, Ukraine, United States and Zimbabwe (A-WEB, 2015), and this shows that elections have become a target for attacks for a number of motives, including political reasons.

While all of these reports would warrant a closer analysis, but due to a lack of available ressources, the authors decided to focus on past experience with Internet voting in elections in Norway, Estonia, France and Switzerland where independent election observation reports by OSCE/ODIHR (2011a, 2011b, 2012a, 2012b, 2013) are publicly available.

We analyze the procedures by mainly looking at how EMB prepare against these threats. For this we look at reports available in four countries, Estonia, France, Norway and Switzerland. While we mainly rely on election observation reports, we complement this with other publicly available sources.

2. CYBER-SECURITY AND INTERNET VOTING

Internet voting is one form of electronic voting, which can be defined as using remote electronic means (ICT) in at least the casting of the vote as defined by the Council of Europe in the only available international legal document Rec (2004) 11 (Council of Europe, 2004).

Possible attacks include amongst others (Ehringfeld et al., 2010):

- Secure platform problem (Trojan horses intercepting the communication);
- Malicious code inserted on the Internet voting or result presentation servers;
- Orchestrated Distributed Denial of Service attacks on the networks;
- Man-in-the-middle attacks;

[1] Research for this article was supported in part supported by TUT basis financing project B42.

[2] Research for this article was supported in part by Estonian Research Council's institutional grant IUT19-13.

- Website spoofing;
- Identity theft;
- Socially engineered attacks on voters;
- Demonstrations of vulnerabilities without actually executing them.

3. BACKGROUND

For this analysis we have selected four very different countries in Europe that all have conducted Internet voting in the recent years (for an overview see also Krimmer, 2015).

- Switzerland has been pioneering Internet voting for the past 15 years. It follows a very conscious step-by-step approach with the aim to introduce electronic elections to the electoral process within 30 years time.
- Estonia, in contrast, has decided shortly after Switzerland to go forward with Internet voting, and selected the big-bang approach and deployed Internet voting for all elections from 2005 on.
- France has put an emphasis on including citizens living abroad in their elections from 2002. After several test elections, it held for the first time a legally binding election via the Internet for six seats in the Senate in 2012.
- Norway started its efforts last of the four, with a feasibility report published in 2006, and two test runs in 10 respectively 12 municipalities in elections in 2011 and 2013. The generally successful project failed to convince parliament politicians who decided in 2014 to discontinue the project.

Of the four countries, Switzerland committed the largest financial resources on the long term, Norway on the short term. Estonia stands out as it managed the project with the smallest budget but the strongest political and social commitment. France convinced with a dedicated project that succeeded in involving the target group.

4. OBSERVATION

The four countries followed very different approaches in protecting their elections from cyber-attacks:

- Switzerland is following not only a step-by-step approach but also a decentralized one. Here, the regional level implements Internet voting, the cantons with the federal chancellery having a coordination role. The protection of the actual servers and internet voting software is done by the cantons themselves, coordination overall internet monitoring as well as risk communication is done by the Federal chancellery. As one of the few, Switzerland has actually a plan B, in case of emergencies, with clear chains of commands and action scenarios.
- In Norway, Internet voting was set up as a project within the ministry of local government and regional affairs, which is home to Norway's EMB. The ministry financed and managed the project and also took care of the IT security as well. For various reasons, cooperation with large Internet providers in the country was limited. For the 2013 elections, the ministry decided to route Internet voting traffic via one dedicated provider in Denmark. This provider offered services against dDoS attacks and close monitoring of the traffic.
- In France, the cooperation to protect the election from any attacks was formalized in the form of the Electronic Vote Board (EVB) that was in charge of the election process. Members included representatives from the Ministry of the Interior and Foreign Affairs, the Association of the French Abroad, as well as representatives from the French Network and Information Security Agency, who was also in charge to analyse the source code of the software.
- In Estonia, partly due to the size of the country, different measures to protect the Internet voting were taken. While the country's number of Internet connections to abroad is small (at the time only four sea-cables to Sweden and Finland were used) and with it the number of IT administrators, personal relations between the responsible persons for Internet voting and Internet connectivity were fostered by organizing asocial event in Tallinn right before the actual Internet-based advance voting was started. In addition, close contacts to the network established by the Cyber-Defense League also helped in making sure that reacting in short time was actually possible.

These short descriptions already show that cooperation is generally key for keeping Internet voting secure. While Switzerland relied on decentralized control and formalized communication channels, France relied on institutional cooperation, Norway limited the amount of interference by outsourcing the control to a private company, and Estonia managed the personal connections in order to ensure the security of the Internet election.

5. CONCLUSION

Cyber-security in Internet voting it is nowadays considered as a security challenge. There is not enough research available nor there is a large amount of practice. The cases presented herein already give an idea of the different approaches to defend against cyber-attacks in elections, however more (systematic) and thorough evaluations need to be done. For this a clear evaluation framework needs to be developed that will help assess the efforts by EMB and other involved actors. This in turn will also benefit election observation efforts such as those by the OSCE/ODIHR and other organizations.

REFERENCES

- A-WEB. (2015). Survey on Cyberattacks on Elections, (forthcoming).
- Council of Europe. (2004). Legal, operational and technical standards for e-voting. Recommundation Rec (2004)11 and explanatory memorandum. Strassbourg: Council of Europe.
- Ehringfeld, A., Naber, L., Grechenig, T., Krimmer, R., Traxl, M., & Fischer, G. (2010). Analysis of Recommendation Rec (2004)11 Based on the Experiences of Specific Attacks Against the First Legally Binding Implementation of E-Voting in Austria.
- Krimmer, R. (2015). The 2015 World Map of Electronic Voting. Retrieved 2015-06-11 from http://www.e-voting.cc/en/it-elections/world-map/.
- Landler, M., & Markoff, J. (2007). Digital fears emerge after data siege in Estonia. New York Times.
- Lesk, M. (2007). The new front line: Estonia under Cyberassault. Security & Privacy, IEEE, 5(4), 76–79.
- OSCE/ODIHR. (2007). Election Assessment Mission Report on the 4 March 2007 Parliamentary Elections in Estonia. Retrieved 2015-04-23, from http://www.osce.org/odihr/elections/estonia/25925.
- OSCE/ODIHR. (2011a). Election Assessment Mission Report on the 6 March 2011 Parliamentary Elections in Estonia. Retrieved 2015-04-01, from http://www.osce.org/odihr/77557.
- OSCE/ODIHR. (2011b). Election Assessment Mission Report on the 23 October 2011 Elections in Switzerland. Retrieved 2012-04-01, from http://www.osce.org/odihr/87417.
- OSCE/ODIHR. (2012a). Election Expert Team Report on the 12 September 2011 Local Government Elections in Norway. Retrieved 2015-04-01, from http://www.osce.org/odihr/88577.
- OSCE/ODIHR. (2012b). Election Assessment Mission Final Report on the 10 September 2012 Parliamentary Elections 10 and 17 June 2012. Retrieved 2015-04-01, from http://www.osce.org/odihr/elections/93621.
- OSCE/ODIHR. (2013). Election Assessment Mission Final Report on the 9 September 2013 Parliamentary Elections in Norway. Retrieved 2015-04-01, from http://www.osce.org/odihr/elections/109517.

Keywords: Internet-based voting, Elections, Governance, Cyber-Security, Election Observation

E-ESTONIA FROM AN ACTOR-NETWORK THEORY PERSPECTIVE

Carlos Ivan Vargas Alvarez del Castillo
RaulWalter LLC/ Tallinn University
carlos.vargas@raulwalter.com

The following abstract is part of a PhD research that is intended to provide an academic resource in the field of e-governance from the point of view of political science. The theoretical approach that is used in e-governance belongs to a non-mainstream Social Theory called Actor-Network Theory (ANT). In terms of practical use, I chose E-Estonia (E-Estonia consider as the whole running e-project of the country. The concept of E-Estonia is integrated by all users of the existent infrastructure. From a single citizen to a large business, the concept is related to E-Estonia as a "Black Box") as an example of how to apply this theory to an existing case with the purpose to shed light on the importance of ANT usage. Nowadays, e-governance represents a challenge for scholars and new questions and challenges arise if it should be studied by political science and how to approach the topic. The proposal of this paper is to give one of many solutions to these questions. The main concern of the research is to uncover the influences of power in an e-Government which enables practitioners identify the value of actors in the network.

The Actor-Network Theory and methodology provide a good way to analyze E-Estonia as its ontological approach (flat ontology)[1] considers not only human actors as part of the social world but also technology as power recipients. The concept of power with ANT has a small foucauldian influence (extended to non-living actors) of micro-politics and micro-power as local groups that diffuse and decenter forms of power spreading throughout society and, thanks to its plurality, its turn into political struggle.[2] Therefore it can be suitable for Estonia because the technology is developed to such a point that makes it essential for the correct functionality of the government.

In order to stay close to the methodology[3] proposed by the creators of ANT, the article will follow a "history" of E-Estonia. It is necessary to build a case study to understand and have a broad view of the ''actants'' (ANT concept for actors; understanding actors as human and non-human) involved in the creation of E-Estonia. Then I will exemplify the adaptation for moments of "translation" and finalize with the "obligatory passage points" and conclusions.

The use of ANT as the theoretical option over other possibilities in social-sciences is well supported by its technological approach and the fact that it offers the opportunity to analyze the government. Another point which is important to explain is the understanding of power in the theory, as power is essential for political science research. The concept of power that will be used relies on the ability to enroll from one to others based on strategies, regarding the actor-networks from the beginning as heterogeneous, all at the same epistemological level.

First of all it is highly important to clarify the distinction between e-governance and e-government as it might confuse the reader. The concepts are vast as both terms are relatively new and every researcher in the topic has a way to understand it. E-government in broad terms it is referred to the "discipline dealing with the development of online services to the citizen, more the "e-" on any particular government service – such as e-tax, e-transportation or e-health"[4], E-governance on the other hand is:

"A broader topic that deals with the whole spectrum of the relationship and networks within government regarding the usage and application of ICTs. It is a wider concept that defines and assesses the impacts technologies are having on the practice and administration of governments and the relationships between public servants and the wider society, such as dealings with the elected bodies or outside groups such as not

for profits organizations, NGO's or private sector corporate entities. E-Governance encompasses a series of necessary steps for government agencies to develop and administer to ensure successful implementation of e-government services to the public at large." [5]

Therefore, the approach of the research takes E-Estonia as a concrete example to analyze a case of "e-governance", as it is trying to yield up power relations and networks in it. It will not be a matter of the research to focus in specific topics that concern to "e-government" yet it is necessary to take in consideration some aspects of it to fulfil the methodological steps that "ANT" requires.

It's noteworthy that ANT is easy to critique, even by its own creators. It falls in the tendency of over-emphasizing the local processes and completely ignores social structures. The existence of other possible theories[6] like: Critical Theory, Attribution Theory, Theory of Reasoned Action/, Planned Behavior, Stakeholder Theory, Social Exchange Theory, Social Capital Theory or Contingency Theory might offer solutions to the same problem. The reality is that within the academic field of e-governance and e-government there is a vast space of action, giving the possibility for researchers to experiment with possible solutions. At this point new ideas expand and increase knowledge on the topic.

The expected outcomes of the research are to reveal a possible way to analyze power relationships and networks in e-governance using a specific case study, also to identify "actors" and their importance in the process of an e-governance implementation. After completing these goals the research could expand in the direction of analyzing the importance of local and global actors in the development of e-governance.

Keywords: Actor-Network Theory, E-Governance, Networks, Power

REFERENCES

1 Manuel De Landa, Intensive Science and Virtual Philosophy, Transversals (London; New York: Continuum, 2002).

2 Steven Best and Douglas Kellner, Postmodern Theory: Critical Interrogations, Critical Perspectives (New York: Guilford Press, 1991).

3 Darryl Cressman, "A Brief Overview of Actor-Network Theory: Punctualization, Heterogeneous Engineering & Translation," 2009, http://summit.sfu.ca/item/13593;
Ritske Dankert, "Using Actor-Network Theory (ANT) Doing Research," 2011, http://ritskedankert.nl/publicaties/2010/item/using-actor-network-theory-ant-doing-research;
Bruno Latour, Reassembling the Social an Introduction to Actor-Network-Theory (Oxford; New York: Oxford University Press, 2005), http://site.ebrary.com/id/10233636;
Richie Nimmo, "Actor-Network Theory and Methodology: Social Research in a More-than-Human World," Methodological Innovations Online 6, no. 3 (2011): 108–19.

4 W. Sheridan and T.B. Riley, "Comparing E-Government vs. E-Governance," 2006, http://www.theinformationdaily.com/2006/07/03/comparing-e-government-vs-e-governance.

5 Ibid.

6 Gregory Peggy, "Introduction to Social Theories Used in IS Research." (UCLAN, n.d.).

CHINA AND CYBER: ATTITUDE, STRATEGIES AND ORGANIZATION

Mikk Raud
University of Hong Kong, in cooperation with NATO Cooperative Cyber Defence Centre of Excellence
raudmikk@gmail.com

Today's China has become a key actor in world politics, deterring any other state from overlooking its opinion or intentions on whichever terrain concerned. With its immensely growing influence to the whole mankind, cyberspace is no exception. Hosting almost 700 million internet users, China is the largest online community on the globe. Aware of the challenges and vulnerabilities that dependence on the internet creates, the Chinese authorities have paid increasingly more attention to establishing protective cyber security measures, as well as taking advantage of the opportunities cyberspace provides in the international power strife.

Understanding China's cyber policies and organization is not an easy task. Unlike with various other countries, one cannot refer to a general cyber strategy document, as such exhaustive approach has been simply absent. This has created uncertainty in both China's domestic environment and understandably outside, as the complex hierarchies, command structures and various policy papers are strongly confusing, leaving it unclear whether the Chinese even want to establish a unified approach or prefer to remain rather covert. One may ask why bother to examine those questions at all – are there not enough issues within our own cyber borders? There are indeed, but the challenges that China is posing are likewise affecting our domestic concerns.

First, how the biggest internet community is governed expectedly influences the overall development of global internet. The Chinese government can either grant netizens the opportunity to become a part of the online world free from physical constraints, or further restrict their access to information and use the internet as a tool against dissidents. Having so far stuck to the second option, China's participation in the global online community has been strongly hindered and is thus preventing the countless cooperation opportunities. Instead, leading to the second point, there is sufficient evidence proving that the Chinese government, military and unaffiliated hacktivists have been conducting daily institutionalized cyber attacks around the world. Relying on various reports by cyber security firms such as Mandiant and CrowdStrike, it is fair to say that the illegally exhausted data from governments, industries or academia amounts to an unimaginable number.[1] As Richard Clarke, the former cyber security advisor to President George W. Bush has described, China has accessed everything from pharmaceutical formulas to bioengineering designs, nanotechnology, weapons systems or everyday industrial products.[2] The underlying motivation behind such activities is to gain advantage in economic, political and military affairs, and to reduce the technological development gap so sensitive to China's leaders. While the West has not remained silent on counter-moves, some suggest a strong underestimation of China's actual threat, even saying that the American counter-operations have been so far "outmanned and outclassed".[3] Whereas this statement does not convey the situation comprehensively, it does reflect the general anxiety that goes together with any developments in China's cyberspace.

To diminish the uncertainty and intimidation, it is important to establish an extensive understanding of China's position in the cyber environment. Bearing in mind the information above, the author seeks to remove the question marks about China's strengths and weaknesses and aims to provide a detailed overview of China's attitude to cyberspace, its strategies, and organization of cyber command.

The first chapter introduces China's position in cyber field and seeks to analyze the major challenges that must be taken into account when observing the area. The research concludes that different cyber

definitions, mismatching understandings of sovereignty and applicability of international law to cyberspace prevent sophisticated cyber cooperation between China and the West. Furthermore, the underlying perception of free information as a threat to state stability allows assuming that such stance will not see a significant change anytime soon.

The second chapter examines China's official cyber policies and their main goals. Due to the absence of one comprehensive cyber strategy document, the author asks what exactly China's cyber policies are based upon. It appears that analyzing several key documents such as the Fifteen-Year Strategy for National Medium and Long Term Science and Technology Development from 2006, or the State Council's New Policy Opinion from 2012 allows drawing a distinctive picture of the country's general cyber goals and ambitions. The author concludes that China's persisting concerns are to improve the security of the domestic internet infrastructure, to reinforce the move towards indigenous innovation, and most importantly, to become a leader on the global stage through promoting new, rather anti-Western attitude to internet governance. Creating the Central Internet Security and Information Leading Group in February 2014, for which President Xi Jinping has taken personal responsibility for, only reinforces China's commitment to fulfilling these goals.

The third chapter inspects how the command structure of Chinese cyber security is organized and who executes different cyber operations. While the institutional fragmentation and overlapping duties created by a mixture of government institutions and military departments has previously impeded well-coordinated development, the research suggests that recent reforms in both civilian and military sectors have paved the way toward a more streamlined approach, led by the newly established Cyberspace Administration of China. Perhaps most intriguingly, the chapter also observes the PLA's General Staff Department's 3rd and 4th Departments, which bear the main responsibility for cyber espionage and electronic warfare against other countries. Finally, the paper draws attention to the patriotic hacktivist group phenomenon, and argues that despite being useful to the authorities, these units may seriously hamper China's general cyberspace development.

Overall, the paper acts as a clarifying document to understand the reasons, methods and actors behind China's cyber conducts. Even though the author has mostly relied on publicly available academic articles, no existing works have analyzed the interrelated aspects together in such a comprehensive package. Taken the sensitivity of the topic, ensuring the validity of each used source is a challenge of its own, but having carefully picked works from recognized experts and organizations, the author believes this paper to be an objective study. Touching upon contemporary issues, the research also offers opportunities for further investigations, suitable for a larger team of experts capable of overcoming both linguistic and cultural issues common in studying this intriguing field.

Keywords: China's attitude to cyberspace, China's cyber policies, China's cyber command and cyber espionage

REFERENCES

1 APT1: Exposing One of China's Cyber Espionage Units. Mandiant Intelligence Center, Feb. 2013. Web; Global Threat Intel Report. CrowdStrike, Feb. 2015. Web.

2 Clarke, Richard, and Robert Knake. Cyber War: The next Threat to National Security and What to Do about It. New York: Ecco, 2010.

3 Hannas, William, James Mulvenon, and Anna Buglisi. Chinese Industrial Espionage: Technology Acquisition and Military Modernisation. Routledge, 2013. Asian Security Studies.

DESIGNING NEW SECURITY MODELS: THE EFFECT OF AN INCREASED PROTECTION OF IDENTITY ON THE STATE

Lea Hricikova
Junior Consultant, Civitta, lea.hricik@gmail.com

The weekly feed of "hacks and vulnerabilities" that is now available in almost all security journals is a good reminder of the fact that the cybersecurity industry never sleeps.[1] When a security giant's signing certificate is seized and used for signing malware, or when password management software is compromised, improvements to restore the trust in the industry take priority.[2] Yet, the interesting part of the security industry's advance lays not in its abilities to recover from security breaches, but its capacity to grasp the wider spectrum of challenges. As the United Nations call attention to stronger encryption, condemn backdoors and advocate for word-wide anonymity, can the security industry prevent breaches and deal with emerging challenges, e.g. recognition technology in the commercial context that brings anonymity in public spaces to be "a thing of the past"?[3]

The answer to this question unfolds a series of implications for the states, which are the main focus of this research paper. These will be mapped with the help of the key concept of the research: the security models. The models currently known demonstrate that security and privacy principles and properties aimed at delivering assurance or preventive measures are complementary, and indeed applicable in a situation like the one outlined above. However, their distinctive features need to be further inspected, together with the effects of such models on the industry, on the services that the industry provides, and on the state as the regulator of the industry.

The arguments proposed in this paper stem from the current and future security, privacy and interoperability requirements set in the perceived environment as described herein. Improvement in digital processes and technology facilitated the emergence of a far more interactive environment for users

---

1 For the purpose of this paper, the term "security industry" represents the efforts of vested professional to advance the technical means for coping with past, current and future security concerns.

2 Kaspersky Labs' Global Research & Analysis Team (June 10, 2015). The Mystery of Duqu 2.0: a sophisticated cyberespionage actor returns. New zero-day used for effective kernel memory injection and stealth. From https://securelist.com/blog/research/70504/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/ [accessed on 24/06/2015]; see also Zetter, Kim (June 10, 2015). Kaspersky Finds New Nation-State Attack – In Its Own Network. *The Wired*. From: http://www.wired.com/2015/06/kaspersky-finds-new-nation-state-attack-network/ [accessed on 24/06/2015]; and Grauer, Yael (June 20, 2015). Security News This Week: Your Phone Ain't As Safe As You Think. The Wired. From: http://www.wired.com/2015/06/security-news-week-phone-aint-safe-think/ [accessed on 24/06/2015];

3 Kaye, David (May 22, 2015). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. United Nations, Office of the High Commissioner for Human Rights, Geneva. From: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx [accessed on 24/06/2015]; Sobel, Ben (June 11, 2015). Facial recognition technology is everywhere. It may not be legal. The Washington Post. From http://www.washingtonpost.com/blogs/the-switch/wp/2015/06/11/facial-recognition-technology-is-everywhere-it-may-not-be-legal/ [accessed on 24/06/2015];

and providers of digital services (typically, the private sector or public authorities). The extensive digitalisation encourages the users to interact, share, engage and participate more, through uploading and downloading more contents. As the increased interactions gain more value, the industry explores new and more cost-effective ways for the adequate management of the data produced. The drop in prices of hardware that further opens the door to the digital processes completes the picture of an increasingly interactive environment.[4]

The cost of keeping the security solutions up to date with the digital services increases in this interactive environment. So does the impact of data exposure to the privacy of users. It is fair to say that privacy and security are an add-on to business solutions for current and future needs, yet never deserving the same attention as more flexible processes (e.g. possibility of moving data to the cloud or to virtualise spaces and entities). Unlike security components, these save costs when it comes to upgrades. Thus, basic security requirements mandated by legal rules are growingly complied with on a best-effort basis. However, the legal rules are formulated prior to innovation, without taking the particular circumstances of it into account. As a result, preventative action lags behind.

The perceived environment as described above permits more interaction to leave more sensitive data with a badly-adaptable security solution in place. Subsequently, a sum of internal and external assurances instead of preventive measures is applied to secure transactions and to protect sensitive data. This is called "the re-active security model". Instead, a pro-active model with a strong privacy solution and flexible security processes implemented in the system in the very beginning (as opposed to being added at the end) seems more desirable. The different security models aim at satisfying the security requirements of innovative technology, the user's needs, and the operational needs of business processes, IT systems and infrastructure.[5] Comparing the different models will allow to indicate what model design accommodates the security industry challenges introduced in the first paragraph: strong privacy as well as flexible processes.[6]

Overall, this paper aims to convey an alternative perception of security by analysing, altering or combining the principles in the security models described here. The key problem is whether an alternative perception of security can capture the attention of state decision-makers. The research gathers information on the potential impact of newly introduced principles on the protection of users' identity, the computer-security industry and ultimately on the states, as all three interact by using or providing services. The first part of the paper will focus (beyond outlining the differences) on what the differences between the models mean for security and privacy. The second part of the paper will draw on the available literature and case studies and go into what effects have had e.g. the implementation of *attribute-based credentials or systems replacing identification with validation* on the security industry and service providers in a selected country[7]. The third and final part will assess how (if at all) that has influenced the legislation-makers in a particular context of the countries implementing the alternative models (e.g. voicing Denmark's experience within the EU).

A side note: this paper spares the reader from the technical details of the security models for the sake of familiarising the topic to the decision-makers and non-technical audience.

Keywords: privacy, security model, validation, security by design, privacy by design.

---

4 Metz, Cade (March 31, 2015). Google Unveils a Stick That Turns Any Display into a PC. The Wired. From: http://www.wired.com/2015/03/google-unveils-chrome-stick-turns-display-pc/ [accessed on 24/06/2015];

5 e.g. via end-to-end security, verifiable encryption, anonymity and selective disclosure, or transaction-isolation

6 The National IT and Telecom Agency, Denmark (August, 2011). New Digital Security Models. Discussion Paper. Ministry of Science Technology and Innovation. ISBN (internet): 978-87-92572-46-2 (see p. 5, 7, 12 and 15);

7 Ibid, p. 17

SESSION 2: EDUCATION AND DIGITAL SAFETY

Session moderated by Dr ANDREAS VENTSEL,
University of Tartu

EDUCATIONAL COMPUTER GAME FOR CYBER SECURITY: GAME CONCEPT

Tiia Sõmer

ADELAIDE TO TALLINN: A COLLABORATIVE RESEARCH EFFORT IN PURSUIT OF KNOWLEDGE, EXPERIENCES AND SUSTAINABLE EDUCATIONAL PARTNERSHIPS

Benjamin Cosh, Carmela Panuccio, Matthew Sclauzero, Pellegrino Coscia and Dr Matthew Sorell

DIGITAL SAFETY CONTEXTUAL MODEL FOR SCHOOLS

Birgy Lorenz

REPRESENTATION OF SNOWDEN'S CASE IN ESTONIAN MEDIA: SEMIOTIC LOGIC OF FEAR

Mari-Liis Madisson

EDUCATIONAL COMPUTER GAME FOR CYBER SECURITY: GAME CONCEPT

Tiia Sõmer
Tallinn University of Technology
tiia.somer@ttu.ee

1. INTRODUCTION

Cyber security training and education can benefit from innovative teaching methods, and the gamification approach has the potential to provoke interest in everyone. Game-based cyber security awareness training can be more effective and less expensive than traditional lecture- and laboratory-based teaching[1]. This thesis has analyzed gamification and serious games, the current situation and current practices of cyber security teaching in Estonian schools, and proposed an addition – educational computer game.

2. PROBLEM

Education is a key element in combating cyber threats and in increasing awareness, and well thought-through security awareness training is important. Games have become increasingly accepted as having enormous potential as teaching tools, they can provide an engaging environment that may result in an "instructional revolution"[2]. The focus of the current thesis was on teaching cyber security topics within the national defense elective in Estonia. The thesis proposed that cyber security education should start in schools, and use of serious games could contribute to raising cyber security awareness.

3. RESEARCH QUESTIONS

To understand the issue thoroughly, the thesis looked at theories of gamification and serious games. This was accomplished through literature review, where well-known experts on gamification suggest definitions for the terms and give theoretical background to the issue.

In the current work, a definition by Kapp was used: gamification means adding game elements, game thinking and game mechanics to learning content. Goal of gamification is to take content that is usually presented as a lecture or an e-learning course, add game-based elements and create a gamified learning opportunity[3].

The thesis then studied use of serious games in education in Estonia. This was accompliched through interviews with educators who are using serious games in their teaching, mostly for teaching economy subjects[4].

In order to understand how cyber security is taught in Estonian schools, a survey was conducted among teachers, followed by semi-structured interviews with teachers and other educators. National school curricula and other documents regulating the area were also analyzed.

Finally, the thesis suggested what should be included in a game concept and proposed a concept for educational computer game on cyber security.

4. METHODOLOGY

To gain understanding on "gamification", "serious games" and "educational games", literature review of well-respected academic literature on the subject was undertaken. According to sources, gamification means using game-based thinking and mechanics to deliver content other than pure entertainment;

and creation of serious game falls under the process of gamification and serious games are a form of gamification. The idea of using games in education, health, and other sectors have already yielded positive results and research is advancing in modeling and simulation that could be applicable to cyber security and defense gaming[5].

In order to understand teaching of cyber security in Estonian schools, survey among teachers was conducted in 2014 focussing on the current state of teaching cyber security. The survey was followed by more in-depth interviews with some teachers. The combination of survey and interviews provided thorough data and interesting nuances, since teachers have a unique view on real skills, requirements, wishes and worries of students.

Additionally, the national school programs for all levels of school in Estonia were also analysed. The national curriculum states the main competencies students should be able to possess upon finishing school[6]. The curricula do not mention cyber security as such, there is no standardised national cyber security teaching program, but elements are included in other subjects.

5. RESULTS

A serious game can be any game, from which one can learn something, in which the activities of players can be measured, and where the player can be awarded[7]. There are a number of cyber security games available and used around the world, and some of these were analysed in this thesis. There are games focused more on the technical side of cyber security, and there are those focused more on the human aspects.

This thesis focused on developing a game concept for an educational computer game, which can be used in cyber security teaching under the auspices of national defense elective in Estonia. Based on results, a computer game for cyber security is being worked on and the first functional prototype is available.

The empirical study showed that cyber security topics are mostly taught in Informatics / Computer Science and National Defense classes, and the focus is to a big extent on basic cyber hygiene. The teachers noted that security awareness of students is quite low and this has to be improved.

Having studied the theory of gamification and serious games, and the current situation in Estonia, the thesis continued with provision of proposal for game concept. The game concept developed is usable for cyber security teaching within national defense elective. The game concept provided objectives for game, scenarios and general game mechanics. Target audience for the game is upper secondary school, age group 15–19. The game is intended to be teaching aid, used in parallel with other means of teaching. The game will provide a virtual world, combining human and technical factors, allowing students to learn about cyber security. Main aim of the game is to introduce cyber security topics in a way that students get personal experimenting environment, where they can make security choices and see results of these choices. The game will be a web-based computer game that can be played on any modern PC with an internet connection.

6. FUTURE WORK

The current functional prototype bases game resource calculations on expert assessments alone, and next step in developing the game will be development of a theory and model, explaining how game resources are calculated. For future work it is recommended to develop a user-friendly scenario development mechanism that would enable to define additional scenarios as required. It is important that the game could be configured and managed in real time.

In later stages of development, it is suggested to study the potential of using multi-player and cooperative versions of the game, as well as conduct research for that purpose.

Keywords: cyber security, gamification, education, serious game, computer game, educational game, instruction, national defense

REFERENCES

1 E. Adams. Fundamentals of Game Design, 2nd edition, Berkeley 2010

2 C. Mead. War Play, Boston, New York, 2013

[3] K. M. Kapp. The Gamification of learning and instruction, San Francisco 2012

[4] M. Sillaots. interview 2014

[5] A. Nagarajan, T.L.Janssen. Exploring Game Design for Cybersecurity Training. In Proceedings of the 2012 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, 27–31 May 2012, Thailand

[6] Riigi Teataja 2011. Põhikooli Riiklik õppekava. https://www.riigiteataja.ee/akt/13273133?leiaKehtiv [WWW] may 2014; Riigi Teataja 2011. Gümnaasiumi Riiklik õppekava. https://www.riigiteataja.ee/akt/13272925?leiaKehtiv [WWW] may 2014

[7] K. M. Kapp. The Gamification of learning and instruction, San Francisco 2012

ADELAIDE TO TALLINN: A COLLABORATIVE RESEARCH EFFORT IN PURSUIT OF KNOWLEDGE, EXPERIENCES AND SUSTAINABLE EDUCATIONAL PARTNERSHIPS

Benjamin Cosh, Carmela Panuccio, Matthew Sclauzero, Pellegrino Coscia and Dr Matthew Sorell
University of Adelaide
matthew.sorell@adelaide.edu.au

INTRODUCTION

The University of Adelaide's "Cyber-Security Study Tour in Estonia" is a pilot Honours level research project at the University of Adelaide (UoA). The three-week study tour introduces students to a broad range of Estonian experiences – culture, government, defence, commerce and government. Moreover, there is a deep focus on cyber-security through a year-long Honours project, "Analysis and visualisation of packet data for cyber security purposes", supervised in collaboration with the Tallinn University of Technology (TUT), and participation in TUT's Cyber Security Summer School.

The pilot program explores how to collaborate across extreme international distances – Australia to Estonia, using modern communication tools such as Skype.

The inspiration comes from taking some of Estonia's vision back to Australia. Estonia, the "Silicon Valley" of Europe, is a country internationally regarded for its heavy investment in technological advancement and support of an entrepreneurial environment. Participants will be exposed to Estonia's 'e-society' infrastructure and its subsequent economic and social benefits.

The tour encompasses UoA's Global Learning initiatives set out in the University's "Beacon of Enlightenment"[1] strategic plan creating sustainable research partnerships and providing insightful international experiences. The opportunities provided will further enrich those offered by university studies alone, bridging the link between academic teaching and the unfamiliar social context that is Estonia.

PROJECT OBJECTIVES AND FACILITATION

The tour is the focal point of a year-long research project, which is a requirement of completing a four-year Bachelors degree in Engineering with Honours at UoA. Conducted concurrently with final year studies, the Honours project immerses students in contemporary engineering research, with either an academic or applied focus. There is an added emphasis on developing design and research skills for future transition into industry or postgraduate study[2].

The formulation of a specific research question developed over a four-month period, where students conducted literature reviews across a broad scope and progressively narrowed focus. With direction from the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) and discussion with TTÜ contributors, a specific research question was developed.

In this work we explore the possibility of forming IPv4 and IPv6 hybrid sessions, where data is sent using both protocols, as a method of detection avoidance (obfuscation). The foundation idea is that this technique prevents the reconstruction of higher-level protocol sessions using existing network analysis tools. The research objectives address the following areas:

- Defining the attack space: What is the context of this attack? What are the assumptions and constraints placed on the attack pattern?

- Theorise the attack: What does this attack achieve? How will it achieve its objectives? How is it implemented? What are the variables that define the attack?
- Simulation: Is the attack possible? Can it be prototyped in an isolated environment? What are the appropriate tools for testing? Is the simulation scalable?
- Analysis and Classification: What are the appropriate analysis tools? Does the attack pattern prevent the current models of session reconstruction? Is the attack pattern classified by specific anomalies?
- Detection avoidance/mechanisms: Are the objectives of the attack achieved? Can this attack pattern be used to avoid detection by available mechanisms? What mechanisms are required for the detection of malicious use of hybrid sessions?

Although this specific focus is an innovative direction, the project's value is not exclusively the research contribution. The true educational benefit lies in the facilitation of a collaborative project across geographical and time zone barriers. Cyber security is presently a domain that requires constant cooperation and facilitation across various nations and organisations. Thus, the project creates a simplified replica of this scenario, allowing students to develop the necessary social and business skills to work in this environment.

It also provides the opportunity to work with TUT's leading academics in this space. Students facilitate communication links via video conferencing and adjust working hours accordingly. Limited face-to-face communication time encourages students to prioritise all areas of project management and work towards weekly self-set deadlines to ensure available progress updates. Students, thus far, have demonstrated that not only is the collaboration possible but the pilot model has had early success in achieving its objectives.

TOUR OBJECTIVES AND DESIRED EDUCATIONAL OUTCOMES

While the research aspect provides the depth of the project, the impact is achieved through the intensive Estonian study tour. The objective is to expose students to the inner workings of a technologically progressive 'e-Society' and the subsequent environment it fosters. Organised visits to areas of innovation, industry and government will aid in demonstrating the motivation behind Estonia's direction. The pilot program itinerary includes the following visits:

- **MEKTORY (Modern Estonian Knowledge Transfer Organisation for You)**: TUT's innovation hub to give insight into Estonian's entrepreneurial mindset and start-up investment focus[3].
- Successful Estonian technology companies such as **Skype**, **Cybernetica** and **Guardtime**, each with a significantly different history and model for international engagement.
- **The e-Estonia Showroom**: This visit coupled with meetings with government official will demonstrate the reasoning behind policy decisions and the positive impact on Estonian society[4].
- **NATO Cooperative Cyber Defence Centre of Excellence**

During the tour, students will attend the annual Cyber-Security Summer School[5] to network with academics and researchers in the field. The desired outcome is that participants will actively engage in all these organised activities and reflect upon their relevance to the current landscape in Australia.

The time in Estonia will also provide opportunities for students to explore Tallinn and immerse themselves in the rich history and culture of the city. It is envisioned that students will reflect upon their experiences and appreciate the value of e-Society in an industrial, social and historical context.

THE FUTURE

The pilot tour has demonstrated the value of an international program with both depth, through a year-long research project, and breadth, through experience on the ground in Estonia.

Plans are now being made to expand the program for Australian students from 2016, from a broader range of disciplines including informatics and possibly law and commerce, and for a reciprocal program for Estonian students.

Keywords: cyber security, hybrid sessions, University of Adelaide, Tallinn University of Technology, global learning, e-Society

REFERENCES

1 University of Adelaide. (2012, December). Beacon of Enlightenment. Retrieved July 2015 from University of Adelaide: https://www.adelaide.edu.au/VCO/beacon/beacon-of-enlightenment.pdf

2 University of Adelaide. (2015, February). University Course Planner. Retrieved July 2015 from https://cp.adelaide.edu.au/courses/details.asp?year=2015&course=107829+1+3510+FY1

3 Tallinn University of Technology. (2015, July). MEKTORY. Retrieved July 2015 from http://www.ttu.ee/projects/mektory-eng/

4 e-Estonia. (2015, July). e-Estonia Showroom. Retrieved July 2015 from https://e-estonia.com/e-estonia-showroom/

5 Study IT in .ee. (n.d.). Cyber Security Summer School 2015. Retrieved July 2015 from http://studyitin.ee/c3s

DIGITAL SAFETY CONTEXTUAL MODEL FOR SCHOOLS

Birgy Lorenz
Tallinn University, Informatics Institute
birgy.lorenz@tlu.ee

In cyber security of a modern information society, digital safety is becoming more and more important regarding governance, schools as well as well-being of common people, especially children. There are models to evaluate cyber-attacks and technical risks in institutions and ICT services, but there are no good model yet to help understanding the concerns and issues of laypeople everyday e-life and students – especially the ones that can be encountered at schools (from primary to upper secondary). The aim of this paper is to propose a model that helps to build up supporting internet security trainings and other actions that will improve children's e-safety skills, resistance to security threats. A big problem is that all internet safety issues seem to be of equal importance to the overworked school administration or are missed completely as considered to be a "parental challenge" not an educational one. The biggest security risk in the future is predicted to be "located between the keyboard and the chair", the defense always lagging behind the attackers and challenges. Training security mindset is not only a workplace and adults challenge, it should be dealt already in a basic school level, where school can give students the right digital citizen's skills and security understanding that can help them throughout their lives. This model, for the educational sector, helps to unfold the digital competences models digital safety and literacy part, hopefully makes changes in national curricula subjects and themes and will be baseline for projects such as Safer Internet Centre in Estonia SIC EE III. We (Digital Safety Lab in Tallinn University) have studied the guidelines from EU and Estonian policies, development plans and strategies (EU Cyber Security Strategy[2]; Cyber Security Strategy 2014–2017[1]; Information Society Development Plan 2020[5]; Life Long Learning Strategy 2020[8] and other), visions and standards (example ICT Education Road Map[4]; DIGICOMP: A Framework for Developing and Understanding Digital Competence in Europe[3]; ISTE standards[7]); prior research that concerns education field in that matter and conducted our own. We have chosen education field to be the main focus as in education one school can represent a small society and how it is lead. We have analyzed the curricula's from preschool to university to understand what kind of risks are dealt with and how (awareness or consequences). Qualitative and quantitative analysis methods was used through keywords and later on through Coding Analysis Toolkit (CAT). The digital safety contextual model was used to propose methods and strategies in school curricula's. Final report in Estonian language DigiTurvis is accessible here: http://1drv.ms/1N7KmtZ Throughout a number of my articles we have been studying the challenges and concerns that are faced by youngsters and adults alike in school environment: spam, overuse of technology, viruses, fraud, easy passwords, identity theft, hacking, bullying, harassment, slandering, privacy issues, pornography, sexual abuse, data protection and direct financial losses[10]. We also attempt to understand the rules and regulations[9] and school culture impact on it[11] to build the model. My contextual model of digital safety is based on school as a smaller-scale image of society (with institutional and personal levels) that is dealing with digital world risks. The model is divided into zones, types, challenges as well as levels and solutions. The first is **Zones** ("people are concerned or not or how much") that are divided into two: public and private; the second is **Types** – cyber security and internet digital safety cases can be divided into two areas regarding with their nature: a. technical concerns, where the solution lays in technical approach (example technical restrictions or monitoring) and b. behavioral concerns, that solutions usually are related to company internal procedures, habits, guidelines or other. The third is **Challenges** or concerns of digital safety and security can be divided into 5 categories (reputation, data, fraud, health, and free will) that in turn will be divided into 9 areas of challenges, 7 layers in each. This is the basic conceptual model or taxonomy we are proposing; the Layers are the 7-step program schools to tackle with the issues from „not caring" to

„burning case" and „not knowing" to „developing protection plans"; And the Solution part is using simplified Bowtie model[6] where in the middle is risk/case/concern and in the right side there are options to deal with the issue through awareness and on the left through consequences. All together it can be explained as „Full model to evaluate digital safety concerns of student and its environment". Combining the model and report of Digiturvis we can imply that today the education sector practices more in prevention area: flexibility in digital competences, critical thinking, safe identity usage online, understanding of some legal issues (software), ethics, safe banking; than consequences area where there are some mentioning about using secure software that helps also to prevent cybercrime, using better passwords, safer behavior, understanding data protection and authentication policies after something have already happened. In the end the suggestion is to implement digital safety/security topics to the national curricula is a must; measure student's digital skills rather now that later; there is a need for an environment where students can practice and do self-testing if there are no other trainings available; for schools to use the model to evaluate current situation, gather and analyze evidences and make changes in trainings or other measures.

Keywords: digital safety contextual model, internet safety, schools security risks, security curricula

Acknowledgements. This research was supported by the Tiger University Program of the Information Technology Foundation for Education.

REFERENCES

1 Cyber security strategy 2014–2017 in Estonia (Küberjulgeoleku strateegia 2014–2017, Majandus- ja Kommunikatsiooniministeerium, 2014) https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf

2 EU Cyber security strategy (JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, European Comission, 2013) http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

3 DIGICOMP: A Framework for Developing and Understanding Digital Competence in Europe (Ferrari, A. JRC Scientific and Policy Reports, 2013) DIGCOMP: Kuidas arendada ja mõista digipädevust Euroopas? https://www.hm.ee/sites/default/files/digipadevuse_enesehindamise_raamistik_0.pdf

4 ICT Education Road Map (IT hariduse teekaart (EST_IT@2018 raport infotehnoloogia kasutamisest hariduses, Arengufond) http://www.arengufond.ee/upload/Editor/Publikatsioonid/IT+Haridus_teekaart_est.pdf

5 Information Society Development plan 2020 in Estonia (Infoühiskonna arengukava 2020, Majandus- ja Kommunikatsiooniministeerium) http://www.riso.ee/sites/default/files/elfinder/article_files/infoyhiskonna_arengukava_2020_f.pdf

6 Introduction to Bowtie model, Civil Aviation Authority, http://www.caa.co.uk/default.aspx?catid=2786&pagetype=90

7 ISTE standards – International Society for Technology in Education (ISTE standardid, Hariduse Infotehnoloogia Sihtasutus, 2012) http://www.innovatsioonikeskus.ee/sites/default/files/ISTE/ISTE_NETS_S%20%28Estonian%29.pdf

8 Life Long Learning Strategy 2020 in Estonia (Eesti Elukestva õppe strateegia 2020, Haridus- ja Teadusministeerium, 2014) https://hm.ee/sites/default/files/strateegia2020.pdf

9 Lorenz, Birgy; Kikkas, Kaido; Laanpere, Mart (2011). Bottom-Up Development of E-Safety Policy for Estonian Schools. 5th International Conference on Theory and Practice of Electronic Governance (ICEGOV2011), 26.–28.September 2011, Tallinn, Estonia. (Toim.) Estevez, E., Janssen, M.. ICEGOV '11, September 26–28 2011, Tallinn, Estonia: ACM, (ACM International Conference Proceedings Series), 309–312.

10 Lorenz, Birgy; Kikkas, Kaido; Laanpere, Mart (2012). Comparing Children's E safety Strategies with Guidelines Offered by Adults. The Electronic Journal of e-Learning, 10(3), 326–338.

11 Lorenz, Birgy; Kikkas, Kaido; Laanpere, Mart (2013). Exploring the Impact of School Culture on School's Internet Safety Policy Development. In: HCI International 2013 – Posters' Extended Abstracts: International Conference, HCI International 2013 Las Vegas, NV, USA, July 21–26, 2013. (Toim.) Constantine Stephanidis. Springer, (Communications in Computer and Information Science, 374), 57–60.

REPRESENTATION OF SNOWDEN'S CASE IN ESTONIAN MEDIA: SEMIOTIC LOGIC OF FEAR

Mari-Liis Madisson
Tartu University, Department of Semiotics, PhD student
ml.madisson@gmail.com

The aim of this paper is to explicate how the leakages concerning details of top-secret United States government mass surveillance program PRISM were contextualized in Estonian public informational space. The Snowden affair found a strong public feedback because this topic addressed even people who had normally been distant from politics. It touched the cornerstone of contemporary identities: the right for free internet. Internet is frequently associated with anonymity (in the context of: race, confession, class, location), interactivity and decentralized organization – and those characteristics are often interpreted as signs of the democratic nature of the medium. This study tries to explain how that kind of positive connotations start to resonate with cultural fears of unregulated surveillance and un-transparent control.

For explaining why PRISM received so vast public feedback in Estonia, I have to place Snowden's scandal in a wider context. Commonsense understanding seems to assume that innovations of ICT are performing a progressive social revolution and new kind of politics. Albrecht Hofheinz has conceptualized that kind of continuous searching for political utopia through the next generation of technology as a NEXTOPIA. Our interpretational horizon gets limited by a preoccupation with the new, and we tend to hail progressive nature ICT without placing it into the context of historical and social context[1]. In case of Estonia that kind of NEXTOPIA is spreading via marketing discourse and schools; it is also enthusiastically expressed by state institutions. Estonian example offers a rich and concentrated material for analyzing how cultural fears resonate with techno-utopian visions because E-discourse has a focal role in future-oriented Estonian identity.

This work relies methodologically mainly on cultural semiotics which defines culture as the sphere of organization of (information) in human society which is opposed to disorganization (entropy) (Theses 1.1.1.). The object of cultural semiotics is the functional correlation of different sign systems (Theses 1.0.0.); and the goal of its studies is to explain how different sign-systems are modeling reality and how they co-function[2]. My study applies the frameworks of cultural semiotics in order to map how different explanations of Snowden's scandal were constructed in Estonian media. I explain what kind of key-signifiers, including and excluding processes of meaning-making and strategies of association were relied on in case of interpreting the socio-cultural impacts of PRISM. It is important to note that cultural semiotics is not interested in reality in its entire diversity but rather in its sign-based models; and in most cases those models tend to be simplifying[3]. Therefore, my study is concentrating on PRISM's representations in Estonian online-media but not on specific aspects concerning the mass surveillance program itself. Despite that analyzed representations were usually addressed to so-called ordinary readers who don't have special knowledge about ICT (and actually the vast majority of the authors also don't have that kind of expertise), and their content is rather simplistic, stereotypic and unverifiable; it is relevant to study this material. Namely, the sphere of meanings which was constructed around Snowden's leakages allows exploring the understandings and values that are connected with contemporary ICTs and which have a significant impact on our attitudes towards particular technologies and platforms.

For elaborating the methodology for analyzing representations of PRISM I followed the abductive logic: the specifics of observed material directed me to framing the categories of analysis; and also to synthesizing different conceptual approaches (semiotics of fear, media sociology, virtual ethnography) for explaining the results of analysis. I developed 4 major categories of analysis: 1) the leading topic of the

representation, 2) the attribution of agency, 3) the focal signifiers of prevailing discourse; 4) the usage of tropes (metaphors, metonyms).

For grasping representations from professional and amateur media, I analyzed opinion-articles of the main newspapers and popular blog-postings as well the comments which followed both. I studied 35 opinion articles and 140 comments that were explicitly discussing leakages of Edward Snowden, mass electronic surveillance data mining program PRISM or NSA. From mainstream media I analyzed articles and comments from Postimees (as Estonian biggest daily newspaper) and Eesti Ekspress (as Estonian biggest weekly newspaper) and Delfi (as Estonian biggest internet-based news portal which has the most popular forum for reader comments). Analyzed sources were published in summer 2013, few months after Snowden's leakages were released, the earliest source was published on 7th June 2013 and the latest on 15th August. I also analyzed postings of two blogs Memokraat and a Persona in fieri as representative examples of alternative media. I decided to analyze those particular blogs because they concentrated on the topic of PRISM most explicitly and also because they are popular among the readers who are interested in contemporary politics.

To put it very brief, my analysis showed that a common feature which characterizes PRISM reception of (in newspapers but also in amateur media) was a strong conviction that surveillance program has a vast social impact. The other important center of reception of PRISM is was the idea that contemporary surveillance programs were unregulated but also unpredictable and uncontrollable. Almost all representations understood PRISM and its social influences alarming or at least potentially dangerous. Different authors articulated various fears that were connected with mass surveillance technologies, my analysis indicated 3 major types of those fears: 1) The fear of fear (socio-cultural phobophobia); 2) The fear that surveillance technology may directly harm a) independent countries and/or b) citizens; 3) The fear that PRISM is a part of NWO conspiracy.

In the viewpoint of cultural semiotics the collective fear activates a specific logic of generating associations; and it significantly transforms previously existing structures of meaning. Visions that articulate future scenarios which are caused by technological revolutions, are often built on binary modelling. Social developments are contextualized by relying on two oppositional variants: utopia or dystopia. That kind of dualistic understanding has much in common with mythological consciousness which creates strong associations between seemingly incompatible values and phenomena.

Keywords: PRISM, Semiotics of fear, Identification processes, NEXTOPIA, Technological determinism, E-democracy

REFERENCES

1 Hofheinz, Albrecht 2011. Nextopia? Beyond Revolution 2.0. International Journal of Communication 5, 1417–1434, p. 1423.

2 Theses on the semiotic study of culture 1998 [1973]. Tartu Semiotics Library 1. Tartu: Tartu Ülikooli Kirjastus.

3 Lotman, Mihhail 2001. Paradoksaalne semiosfäär. – Kultuur ja plahvatus. (ed.) Pruul, Kajar. Tallinn: Varrak, 215–226, p. 216–217.

SESSION 3: PRIVACY

Session moderated by Prof CHRISTOPHER MILLARD,
Queen Mary University of London

A STUDY OF SOCIETY'S PERCEPTION OF ONLINE PRIVACY

Meredydd Williams
University of Oxford
Meredydd.Williams@cs.ox.ac.uk

Online privacy is a matter of great importance as we increasingly live our lives on the Internet. The growth of social networking sites, ubiquitous wireless connections and Internet of Things devices has led to a significant amount of our data being stored online. Advances in machine learning and big data analytical techniques have also allowed both researchers and marketers to extract information from previously-opaque data. People frequently give their support for privacy, listing it as a fundamental human right, whilst millions of individuals continue to make use of convenient online services that collect their personal data. Do those who truly care about their privacy understand enough to protect it? And do those which extol the virtues of privacy actually practice what they preach?

To explore this, we propose a paper-based survey of the adult general public across several cities in the UK. These sites were selected based on their differing population sizes: Oxford (154,000[1]), Cardiff (350,000[2]), Birmingham (1,000,000[3]) and London (8,300,000[4]). Participants will be asked questions relating to how they value privacy, how privacy-conscious they believe themselves to be, and what measures they take to protect themselves online. A risk exists that respondents might claim to value privacy, and then alter their replies to match that claim, hoping to cast themselves in a more favourable light. Therefore, several novel approaches have been implemented to gain a deeper insight into participant's responses. Firstly, in addition to mandatory demographic questions for data analysis, numerous optional questions are also included. If an individual claims to be highly privacy-conscious and yet needlessly reveals personal information, then perhaps they do not practice what they preach. Secondly, repeated but rephrased questions will be included to test a respondent's comprehension: if they answer positively and negatively to the same enquiry then they might possess gaps in understanding. Thirdly, questions regarding fake applications will be used to judge whether a participant is changing their answers to match their initial claims. Finally, surveys which are returned hurriedly are at an increased risk of being completed without serious thought. In these cases, a mark will be applied to the reverse of the sheet, so this can be taken into account during data analysis.

Online privacy has become increasingly relevant over the past years, especially in light of the Snowden revelations. Intelligence agencies in both the US and UK have found themselves under pressure regarding data collection, reminding us all of our growing digital footprints. Whilst the publication of sensitive material garnered press coverage, it is unclear whether the average citizen values their online privacy. Studies have shown that 30% of US adults aware of the surveillance programs have taken steps to shield their personal information[5], but this figure also presents the apathy of the 70% which know of the risks but have not altered their online habits. Alternatively, it can be said that since 87% of those questioned had heard of the surveillance programs[6], this still amounts to tens of millions of US citizens making changes. Our research looks to directly interact with the UK public to understand whether they actually care about privacy and, if so, whether they can effectively protect themselves. In light of the media attention that GCHQ have faced, it will be interesting to see the public reaction. Also presenting the relevance of online privacy research, a lack of confidence in online transactions can be economically-damaging to a modern state. Governments and private entities alike are rushing to transfer their services online, reducing operating costs and granting easy access to millions of citizens. Online retail alone is estimated to contribute £52.25bn to the UK economy this year[7], money that could be jeopardised if the masses lose confidence in the Internet. For this reason, studies of privacy are important to

gauge public sentiment, as well as furthering research into how to best prepare individuals to protect themselves online. Both YouGov and TRUSTe have undertaken recent UK research, finding respectively that 72%[8] and 88%[9] of those surveyed are concerned about their privacy. However our methodology differs in that our surveys are in person and answers are analysed alongside optional responses.

Our principle research questions aim to study how the general public regard online privacy, rather than the captive university students who are often targeted for research. Firstly, do those who claim to care about online privacy act privately with their optional demographic data? Secondly, do those who state they care about their privacy actually understand how to protect it? Finally, as we are often told, are today's youth careless with their privacy? Or do they actually have better knowledge of privacy-enhancing technologies? Through analysing our respondent's demographics, it will be possible to compare the views of different age groups.

Whilst it is impossible to truly predict the survey results, we can give some expected findings. Firstly, we would expect those who claim to be private online would also act more privately in person, and therefore refrain from completing optional demographic questions. Whilst the effect of participating in a survey might cause some respondents to answer for completeness, over dozens of participants there should be a noticeable difference. Secondly, we would expect that even if participants state that they care about privacy, that they do not adequately protect their data online. Research has previously shown the complexity of privacy-protecting tools[10] and how the general public are often ill-equipped to defend their data[11]. Thirdly, we would expect the digitally-native young to have a better knowledge of cybersecurity practices and therefore defend themselves better. Whereas today's youth share more data online, we would imagine they are more likely to understand technological safeguards, as compared to their parents and grandparents.

This proposed online privacy survey has passed University of Oxford ethical approval and is planned to be undertaken later this summer. The across-UK approach directly targeting the general public will help us assess how citizens view privacy, with novel approaches implemented to judge whether respondents practice what they preach.

Keywords: privacy, society, awareness

REFERENCES

1 Oxford City Council. Population Statistics. Available at: http://bit.ly/1MrFRJw. 5th December 2014.

2 World Population Review. Cardiff Population. Available at: http://bit.ly/1Ks1Jpx. 19th October 2014.

3 Birmingham City Council. Population in Birmingham. Available at: http://bit.ly/IIApXI. 6th January 2014.

4 BBC News. London's population hits 8.6m record high. Available at: http://bbc.in/1CRi8zU. 2nd February 2015.

5 L. Rainie and M. Madden. Americans' Privacy Strategies Post-Snowden. Pew Research Center. Available at: http://pewrsr.ch/1O0OT2P. 16th March 2015.

6 Ibid.

7 D. Moth. UK online retail sales to reach £52.25bn in 2015: report. Econsultancy. Available at: http://bit.ly/1zo779R. 26th January 2015.

8 S. Gibbs. Data protection concerns 72% of Britons in post-Snowden world, research shows. The Guardian. Available at: http://bit.ly/1H78wn7. 9th April 2015.

9 TRUSTe. TRUSTe Privacy Index: 2015 Consumer Confidence Edition. Available at: http://bit.ly/1e51fJX. 2015.

10 A. Whitten and J. D. Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. Usenix Security. 1999.

11 M. Bishop. Education in information security. IEEE Concurrency vol. 8 no. 4 pp. 4–8. October 2000.

SOCIAL NETWORKING SITE PRIVACY: AN EMPIRICAL EXPLORATION OF THE RELATIONSHIP BETWEEN RISK TOLERANCE AND USER BEHAVIOUR ON PATIENTSLIKEME

Francisco J. Grajales III, BHK (Hons.), MS, PhD (c), CSEP-CEP
University of British Columbia
cisco@franciscograjales.com

Background: Today's interconnected society has adopted social networking sites faster than policy can adapt to meet the privacy needs of its citizens. In healthcare, patients are sharing and managing their personal information, such as the medications they use and their respective side effects, on sites similar to Facebook but centred around disease (e.g., PatientsLikeMe, PLM). Unfortunately, however, the data that are being shared on these sites are not protected by privacy statutes in the traditional sense, as users must accept User Agreements to use these websites, which may publicly or pseudo-anonymously show these patients full medical history. Also, these legal contracts, waive user's data ownership rights and/or allow third parties to use patient's data for commercial or ethically-questionable purposes. Taken to an extreme, it could be argued that patients, in dealing with the isolation and fear of their disease, are socially coerced into giving their data away as a means to improve their quality of life. At stake is not whether the data shared should be used for commercial purposes; rather, it is about how the laws of, for, and by society can delicately balance the needs of capitalism (the sale of goods and services) whilst protecting its ideals; that is, maintaining citizen rights, freedoms and ensuring that discrimination does not occur. My research builds a foundation for policymakers to harmonize these tensions from different perspectives – the patient, the law, and the corporation.

Objective: My dissertation explores the relationship between privacy, user behaviour on social networking sites, and the perceived retribution that could be enacted by third parties. More specifically, it is an evaluation of: 1) users' habits and incentives for sharing data on health-related social networking sites; 2) the relationship between data sharing practices, anonymity, and the perceived risk of future retribution by future employers, insurance companies and government entities; and 3) how policy and data protection legislation may balance the universal human-right to privacy with institutions that operate in a for-profit market.

Methods: A partnership has been established between the University of British Columbia's Industry Liaison Office and PLM Inc. in Cambridge, MA. Under this partnership, PLM has shared the results of a survey on Privacy measures that were conducted on behalf of the US National Academies of Sciences. Under this agreement, PLM has also shared anonymized user profile data. I am currently using these data to answer the questions outlined above. Data analyses, including descriptive statistics and regression modelling are being conducted using the XLStat software. Results have been ethically validated and will be reported in congruence with the Checklist for Reporting Results of Internet E-Surveys.

Preliminary Results: 2,725 (73.5%) respondents completed the survey. 1,636 (77%) of them were female and 1,417 (52%) had shared their profile with at least one person outside the site (e.g., spouse, friend, clinician, or other). Overall, 1,036 (38%) and 954 (35%) believed that their data from Personal Health Records would be used to deny them healthcare benefits or would limit job opportunities in the future, respectively. In contrast, 1,553 (57%) of respondents believed that their data was currently being used to improve the care of future patients who might have the same or similar condition. Generally,

non-American patients shared 30% more data than their American counterparts, regardless of perceived risk of future discrimination by third parties.

Conclusions: Our preliminary results strongly suggest that American users share significantly less data than their international counterparts. The potential reason for this is the fear of future retribution and discrimination by third parties, such as health insurance companies or (future) employers. Despite this however, more than two third of patients, regardless of nationality, want their data used anonymously to improve the care of other patients. Furthermore, there is a gap between the reality and perception of how the data that are being shared on these sites are and may be used. Further research will be required to explore whether these attitudes are a direct result of universal healthcare coverage and/or sociological factors across different geographical contexts.

Keywords: Social Networking Sites, Privacy, Risk Tolerance, User Behaviour, Public Policy

IF ONLY IT WASN'T HER TENTH SELFIE TODAY: YOUNG PEOPLE SETTING THE RULES FOR PHYSICAL PRIVACY ONLINE

Ilze Borodkina
University of Tartu, Institute of Social studies
i.borodkina@gmail.com

Privacy is very often defined as one's basic right to determine and control, what kind of one's personal information is accessible to others, to whom it is accessible and what are the further uses of the information after it is accessed.

However, this represents just one of four dimensions assigned to privacy by Judee Burgoon already in 1982. Along with psychological, social and informational dimensions, she describes also physical, defining it as freedom from "unwanted intrusions upon one's space by the physical presence"[1]. Although it has received less attention than other dimensions, one's physical accessibility to others is sometimes described as "precondition for privacy"[2] in general.

With digital communication space becoming a full part of individual's everyday environment, the physical or spatial perspective of privacy gains new aspects. In addition to dealing with this space being cognitively constructed rather than physically experienced, an individual has to deal also with the fact that the perceived personal space in digital context itself has significantly changed. From clearly limited environments like e-mails or Web 1.0 versions of personal websites it has turned into social networking, where the only boundaries exist where the individual perceives them to be.

Within this networked privacy[3], third persons are continuously involved not only in constructing one's identity by their content publishing and sharing practices, but also take part in deciding what information will actually constitute individual's experience of his/her perceived personal space online. Especially for young people, who are labelled as tech-savvy digital generation, but also as having traits of consumerist and narcissist generation, this means that in a territory they perceive as their own, they have to spend their time on something they have not chosen and might not even like. But in the age, when the information flow is constantly accelerating and one has to create strategies of keeping up[4], time has become even more valued resource than before.

In the case of online content, especially in social networking sites like Facebook, site mechanics work in a way that often places consumption before the choice of content. Thus degree to which individual's actual personal information space reflects one's imagined or ideal personal information space, and thus also degree to which actual allocation of time to content coincides with ideal one, depends very much on how much other people comply to what the individual sees as communication behaviour fit for his/her personal information space.

This rises question, what are the rules and norms young people would like others to observe when creating content within the perceived boundaries of their personal information space and what rules and norms would these young people observe themselves when publishing or sharing content online.

In order to explore this issue, one hundred students were asked to write observation journals for a week, evaluating online content that they encountered within their normal digital communication practices and that caught their attention for any reason. By answering guideline questions about each such content unit, they reflected both, on their personal and perceived public standards of what the proper content of digital communication space should be.

The results of analysis show that the norms and rules young people tend to define when evaluating a content produced by others, not always are applied to themselves. In fact, it is possible to say that two sets of rules exist, in several cases even for the same person, that are used depending on whether the individual is producer or consumer of the information. The same type of content condemned as "useless" or "irrelevant" when one has to consume it as part of one's own personal information space, may reach at least neutral evaluation when the individual is the person publishing or sharing it. In addition, the data suggests that having control over the content allows for more positive attitude towards it and demands less specific rules.

In general, categorization of a content-creation activity as suggested or condemned is subjective and depends on individual's personal perceptions and experiences. However, the data still show certain trends. For example, there is connection between acceptability of the content and time and effort needed to consume it, as well as with possible immediate gain from consuming it. In terms of time-consumption, even as seemingly minor thing as imperfect grammar can cause negative reaction, if the imperfections lead to having to put more effort to understand the content. On contrary, if consumption of the content provides a sense of satisfaction or gain, even if this gain is only potential, as it is in different versions of raffles.

Eventually, when evaluating the online content published by others, along with time-consumption related issues, audience attention appears to be an important resource. In several cases participants state explicitly that wrongdoings of other people within their publishing/sharing activities cause great risk to exhaust the audience, thus solely usurping the rights to use a very specific shared resource.

Keywords: physical privacy, personal space, young people, online communication norms

REFERENCES

1 Burgoon, J.K., Parrot, R., Le Poire, B.A., Kelley, D.L., Walther, J.B., Perry, D. (1989). Maintaining and Restoring Privacy through Communication in Different Types of Relationships. Journal of Social and Personal Relationships, 6, p132.

2 Leino-Kilpi, H. et al. (2001). Privacy: a review of the literature. International Journal of Nursing Studies, 38, p663.

3 Boyd, d. (2012). Networked Privacy. Surveillance & Society, 10(3/4), 348–350

4 Turkle, S. (2011). Alone Together. Why We Expect More from Technology and Less from Each Other. New York: Basic Books

FOSTERING INFORMATION WITH DATA PROTECTION LAW

Ignacio N. Cofone
Rotterdam Institute of Law and Economics, Erasmus University
cofone@law.eur.nl

In writings about privacy legislation and data protection law, there is often an implicit idea that there is a tradeoff between data protection and the amount of information available to reach other social goals, such as research that will in turn lead to innovation (Etzioni 2008; World Economic Forum 2011). This idea is sometimes depicted as a tradeoff between rights and efficiency, prioritizing one or the other depending on the normative views one could have, and it is sometimes left unstated, proposing a balance between the right to privacy and the right to freedom of expression or to the access of information. This idea determines the extent to which the normative arguments that have it embedded recommend protecting privacy.

Contrasting with this idea, there is an argument to be made for a certain level of data protection leading to more production of information, and hence to more information flow, which would in turn increase the scope of the same rights to which privacy is sometimes balanced against. To illustrate this point, one must evaluate the ex-ante incentives generated by the creation of entitlements either to protect or to abstain from protecting personal information.

The way in which we deal with our personal information and the limits of our privacy mutate with new technologies. The internet, the biggest agent in this change, has turned into a zero marginal cost distribution channel, both for voluntary and for involuntary exchanges; the transaction costs of distributing information in cyberspace are much lower than in physical spaces (Hardy 1996; Ku 2002).

Informational privacy, and in particular data protection, concerns the ability to exclude others from our personal information. Exclusion, in turn, takes us to the realm of entitlements. In a low transaction-cost scenario such as the one described, it is irrelevant from an economic perspective to whom an entitlement is given, since in any case it will be allocated ex-post to its highest valuer after a negotiation process (Coase 1960). However, there is a caveat to this principle for goods that do not exist yet in the market (Hart and Moore 1990; Merrill and Smith 2001; Merrill and Smith 2011). Given that a requirement for labeling something as a good is that it is available in order to be able to readily satisfy the needs of others (Milgate 2008), personal data is included in the caveat since it does not fulfill all characteristics of a good until it is disclosed. In those cases, to whom the entitlement will be given is relevant to determine levels of investment, and hence the amount of the good that will be available in the future.

This argument is strengthened further when paired with the public good characteristics of information, which provide an additional reason for the relevance of these levels of investment. The internet has turned from a system of information storage by some and information retrieval by others to a system for connecting people, where everyone creates and retrieves content – also called peer-to-peer, or Web 2.0 (Lessig 2006). This change leads to personal information behaving as a good that, while still costly to produce, can be given to others at zero marginal costs (Stigler 1980; Schwartz 2004). This implies the existence of positive spillovers that potentially lead to a production-deficit problem: if the benefits of generating information are not fully internalized, the level of generation of information will be lower than what is socially desirable.

These two characteristics alter the incentive structure of the generation and the sharing of information. Consequently, they lead one to revisit the interdependence between privacy and access to information

in the context of new technologies. From this point of view, inasmuch as data protection introduces entitlements that allocate an exclusion power, there is some degree of data protection that increases the amount of personal information available for exchanges from a dynamic perspective. No data protection would lead to the persistence of the production-deficit problem and hence to a level of information production that is lower than what is socially desirable. Data protection and information, for this reason, are often not at a tradeoff.

Some level of data protection (this is, some level of entitlement-created exclusion levels) creates incentives to generate information, reducing the aforementioned production-deficit problem. The question is then not so much whether to grant data protection at all in order to allow for freedom of speech and access to information to take place, but how much of it to grant.

By focusing on data protection law as a mechanism to promote the generation of information, two gaps so far present in the literature regarding proposals to protect privacy are closed. First, the question of why the allocation of the entitlement is relevant in a scenario of low transaction costs (Posner 1978; Posner 1981) is answered by seeing that distributional effects matter to incentivize production. Second, the question regarding how entitlements over intangible goods can be justified in the face of a mismatch between the reasons to protect personal information and the reasons to protect intellectual property (Samuelson 1999) is addressed by noting that both branches of law foster the generation of information.

These considerations lead to consider that privacy and access to information are not countervailing rights; the social costs of lacking an adequate data protection are not only those corresponding to chilling effects, but also to underproduction of information. In such way, one can explain data protection law from an economic perspective and, in doing so, have a simplified framework for the evaluation of data protection measures.

Keywords: economics of privacy, data protection, privacy law, online privacy, access to information, freedom of expression, law and economics

REFERENCES

- Coase, Ronald H. 1960. "The Problem of Social Cost." Journal of Law and Economics 3 (1): 1.
- Etzioni, Amitai. 2008. The Limits of Privacy. Basic Books.
- Hardy, Trotter. 1996. "Property (and Copyright) in Cyberspace." University of Chicago Legal Forum 1: 217.
- Hart, Oliver, and John Moore. 1990. "Property Rights and the Nature of the Firm" 98 (6): 1119.
- Ku, Raymond. 2002. "The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology." University of Chicago Law Review 69 (1): 263.
- Lessig, Lawrence. 2006. Code 2.0. Basic Books.
- Merrill, Thomas, and Henry Smith. 2001. "What Happened to Property in Law and Economics." Yale Law Journal 111 (2): 357.
- ———. 2011. "Making Coasean Property More Coasean." Journal of Law and Economics 54 (4): 77.
- Milgate, Murray. 2008. "Goods and Commodities." In The New Palgrave Dictionary of Economics, edited by Lawrence Blume and Steven Durlauf. Macmillan.
- Posner, Richard A. 1978. "The Right of Privacy." Georgia Law Review 12 (3): 393.
- ———. 1981. "The Economics of Privacy." The American Economic Review 71 (2): 405.
- Samuelson, Pamela. 1999. "Privacy as Intellectual Property?" Stanford Law Review 52: 1125.
- Schwartz, Paul. 2004. "Property, Privacy, and Personal Data." Harvard Law Review 117 (7): 2056.
- Stigler, George J. 1980. "An Introduction to Privacy in Economics and Politics." Journal of Legal Studies 9: 623.
- World Economic Forum. 2011. Personal Data: The Emergence of a New Asset.

SESSION 4: TECH I

Session moderated by Prof JON CROWCROFT,
University of Cambridge

CAN WE ACHIEVE BOTH PRIVACY PROTECTION AND EFFICIENT MALWARE DETECTION ON SMARTPHONES?

Jelena Milosevic, Alberto Ferrante, Miroslaw Malek

INFORMATION SECURITY PARADIGM SHIFTING IN BLOCKCHAIN-BASED FINANCIAL INFRASTRUCTURE

Yevheniia Broshevan, Pavel Kravchenko

A DATASET ANONYMIZATION FRAMEWORK FOR PUBLIC TRANSPORT OPERATORS

Andrea Melis, Franco Callegati, Marco Prandini

CAN WE ACHIEVE BOTH PRIVACY PROTECTION AND EFFICIENT MALWARE DETECTION ON SMARTPHONES?

Jelena Milosevic, Alberto Ferrante, Miroslaw Malek
Advanced Learning and Research Institute (ALaRI), Faculty of Informatics,
University of Lugano, Lugano, Switzerland
Email: name.surname@usi.ch

We are witnesses to the ubiquitous usage of smartphones. We use them to communicate, do business and even to perform financial transactions. However, the widespread usage of mobile devices attracted also the attention of malicious software writers. Malicious software, or malware, has the goal of stealing sensitive information from users, taking control over the operating system, and damaging or even completely disabling the device.

In order to limit the effectiveness of malware, a malware detection system has to be incorporated in the phone and on the cloud. The proposed approach goes in this direction. Namely, we propose a malware detection system that consists of a two-steps detection algorithm: the first step is running detection on the phone and the second one on the cloud. A less complex detection algorithm, suitable for the limited resources of mobile environments, is running on the phone. The goal of this algorithm is to collect data related to the phones state, detect potentially malicious activities and, upon their detection, to send data to network to be analyzed. Upon receiving this data, the detection mechanism on the cloud processes information and classifies the application as malware or benign. In case of malware being detected, the decision is communicated to the user. By sending data into the network for further analysis only upon detection of potential threats, the best possible trade-off between privacy protection and effective malware detection is achieved. In order to establish such a system, we expect to go beyond the state of the art. In the initial phase of the investigation, we will start with the evaluation of existing algorithms. For on-phone malware detection, we will start the analysis with Naïve Bayes, Support Vector Machines, and logistic regression, due to their simplicity and variety of successful application areas. Exploration of the most suitable algorithm to be run on the cloud will start with Neural Networks and Hidden Markov Models, due to their ability to perform deep learning and more complex detection. While more detailed description of the complete methodology can be found in[1], the focus of this abstract is to foster the discussion on the tradeoff between privacy-preserving malware detection on the one side and efficient and precise detection on the other.

The proposed research is relevant due to the increased importance of protection from malware. According to McAfee Labs[2] the collection of mobile malware continued its steady climb as it broke 6 million samples in the fourth quarter of 2014, up 14% over the third quarter of the same year. It is clear that more efficient methods to protect from malware are needed, and we believe that our approach is one of them, enabling users to detect early suspicious activity and keeping the resource consumption low. The further advantage of the approach lies in its privacy preserving capability. Namely, as previously mentioned, data is not constantly being sent into network but only if a potential threat is observed. In our opinion, this is very important having in mind the sensitivity of the information stored in the phone and its variety: ranging from photos from previous parties, friends contact list and their numbers, up to confidential business data and stored passwords.

The authors propose the approach that advances existing state-of-the-art mobile malware detection methodologies. To the best of our knowledge, current detection algorithms are based either on the phone or on the cloud detection, but not on both. ParanoidAndroid detects malware on the synchro-

nized copy of the phone state that runs on a server[3]. However, a disadvantage of such approach is that private user data is constantly being sent into a network, thus risking to be abused for malicious purpose. In order to avoid information leakage, running simplified detection algorithm on the phone itself is proposed in[4]. This approach avoids revealing user data to the other side and saves bandwidth. Nevertheless, the accuracy of such algorithm is limited due to the lack of general knowledge about the network conditions. An accurate approach to malware detection is proposed in [5] where good detection accuracy is achieved by using static features (i.e., features that can be collected without execution of malware, such as manifest file or information from disassembled code). The main disadvantage of such approach, as it is based on static analysis, is lack of dynamic inspection and, therefore, its inability to detect malware at runtime. Our approach overcomes this problem by observing dynamic features (i.e., features that are collected during execution of malware such as memory and CPU usage related information, so as network behavior and battery consumption).

To summarize, the main research goals of the proposed approach are following:

1. Develop an efficient and low-complexity set of algorithms to be run on the mobile device, and a set of more powerful algorithms to be executed on the cloud to detect malware with higher confidence. The algorithms running on the device will trigger the execution of the ones on the cloud only when necessary (i.e., a potential malware is discovered); for this reason, the algorithm running on the phone will be designed to have high sensitivity, so that the number of suspicious activities that are missed is as low as possible, and the one running on the cloud has high accuracy, so that identification of malware is done as precisely as possible.
2. Optimize the distribution of battery, power, and communication overhead among a cloud service and a mobile device by taking into account the limited computation possibilities of mobile devices on one side and the importance of privacy on the other.

Keywords: mobile malware, privacy protection, dynamic malware detection

REFERENCES

1 Milosevic, J., Dittrich, A., Ferrante A. and Malek, M. "A Resource-optimized Approach to Efficient Early Detection of Mobile Malware." 3rd International Workshop on Security of Mobile Applications (IWSMA). 2014.

2 M. Labs, "Threats report," McAfee Labs, Tech. Rep. 2015.

3 Portokalidis, G., Homburg, P., Anagnostakis, K. and Bos, H. "Paranoid Android: versatile protection for smartphones." Pages 347–356 of: 26th Annual Computer Security Applications Conference (ACSAC). 2010.

4 Kou, X. and Wen, Q. "Intrusion detection model based on Android." Pages 624–628 of: Broadband Network and Multimedia Technology (IC-BNMT), 2011 4th IEEE International Conference on. 2011

5 Arp, D., Spreitzenbarth, M., Hubner, M., Gascon, H. and Rieck, K. "Drebin: Effective and explainable detection of android malware in your pocket." Proceedings of the Annual Symposium on Network and Distributed System Security (NDSS). 2014.

INFORMATION SECURITY PARADIGM SHIFTING IN BLOCKCHAIN-BASED FINANCIAL INFRASTRUCTURE

Yevheniia Broshevan[1], Pavel Kravchenko[2]
[1]National Aerospace University n. a. N. E. Zhukovsky "KhAI"
evgeniya.broshevan@live.ru
[2]Tembusu Systems
kravchenkopo@gmail.com

The financial crisis has driven the impetuous growth of alternative financial services models, including cryptocurrencies. These technologies have a great potential to reshape and replace existing mechanisms for storing and exchanging of values.

The goal of the paper is to research the area of blockchain-based financial technologies, to define the main security problems in this sphere and suggest appropriate solutions. The result of the work is the model for financial infrastructure based on cryptocurrency principles for mass adoption.

The most interesting principle, which was suggested by innovations, is the ability to connect multiple entities to a single digital record shared by all and available in real time. For example, it's implemented in one of the most popular cryptocurrencies, Bitcoin and it is called blockchain. It is a public distributed ledger, which stores all transactions. This makes financial history unalterable, and makes it difficult for attackers to change it. Strong cryptographic mechanisms are used to ensure integrity of the blockchain and protect transactions in the public network. As a result, any document can be digitized, codified and inserted into the blockchain and it becomes a record that cannot be tampered with. The advantages of this model include higher speed, efficiency, and the elimination of single failure points in the system.

During last 5 years the idea of decentralized applications based on blockchain technology for financial industry was properly designed and released. These applications can be divided into following groups: wallets, payment processors, exchanges, remittance services, P2P lending services, micropayments, smart contracts and different alternatives of usage like voting, property title, notary services, etc. Unfortunately, there are different security issues, which cause enormous financial loss. For instance, Slovenian exchange Bitstamp has revealed the loss of roughly 19000 BTC as a result of a platform security breach. Or one of the last examples: Chinese Bitcoin exchange Bter hacked, $1.75 million worth of cryptocurrency stolen. In this paper the most significant cryptocurrency exchanges hacking and its reasons are reviewed.

Bitcoin's main principle is decentralization, which influences its security. Traditional centralized model, like in bank or payment network, depends on access control for preventing malicious actor intrusion1. But in bitcoin the responsibility rests with the users. The network security is based on proof of work (the requirement for a service user to prove that they have performed a costly action in order to deter network attacks, and in bitcoin application it is used hashcash), that is why the network is open and no traffic encryption is required.

For example, in the banks, payments are open-ended, because they contain private information. In this way, the payment network has to be end-to-end encrypted and prevent man-in-the-middle attacks. However, bitcoin transactions are protected by hashes (SHA-256) and digital signatures (ECDSA), hence bitcoin payment network doesn't need traffic encryption. Therefore information security paradigm was shifted from communication lines protection to protection of transmitted data.

With all its benefits, the main problem is to maintain the secrecy of keys. Bitcoin relies on public key cryptography. That is why there are different ways to store keys: in local storages, in password-protected (encrypted) wallets, in offline key storages, in hosted wallets or in air-gapped key storages2. But they still have weak places.

The basic idea of the paper is to define main problems for cryptocurrency large-scale implementation and to suggest the "ideal" model for the future adoption.

Considering the aforesaid, the following problems are highlighted and appropriate solutions are suggested.

One of the main issues is key management[3], which includes lost key protection, virus protection, trustless key storage and key exchanging. For preventing losing or attacking by viruses multisignature can be used. There are different hardware tokens for key storing: BitLox, Trezor, Ledger Wallet and of course our Ukrainian developments ("Institute of Information Technologies" in Kharkiv is produced special crypto tokens). + signature process. Also KeyChain technology can be used as key management system for Android or iOS, for example.

Nowadays Internet security systems (SSL/TLS, HTTPS, and Certificate Authorities) don't provide the security that they claim to provide. Today's surveillance is made possible because most protocols that facilitate online communication do not provide all of the following properties: 1. End-to-end encryption. 2. Secure authentication. 3. Perfect Forward Secrecy (PFS). 4. Plausible deniability (sometimes). But for solving these problems DNSChain can be used. It does this first by combining DNS with Namecoin (NMC)[4], and then by encouraging a "trust only those you know" policy. Namecoin is an open source decentralized key/value registration and transfer system based on Bitcoin technology. Namecoin "squares Zooko's Triangle", meaning, it makes it possible to have domain names that are: authenticated, decentralized, human-readable. The existing solution to provide secure communications is okTurtles + DNSChain[5]. okTurtles takes the authentication provided by DNSChain, and uses it to provide secure communication through virtually any website.

Transaction database security is provided by the main principles: decentralization and verifiable consensus. But there are several issues with consensus in existing protocols. Consensus mechanisms don't take the past into account – in Bitcoin past is not relevant and can be always overwritten by longest chain rule. Since validators in Ripple are trusted they have to be responsible for all actions they have done. It can be strengthened via security deposit. It doesn't have clear mechanisms how to find a malicious node and mechanisms that track "unusual" situations in the consensus, etc. Solution principles are overviewed in the work.

The last, but not least problem is how to identify every user legally. The proposed solutions are physical identification, authentication of user's device using, identification of transaction initiators and proof-of-identity.

In the paper, the main issues in current system are reviewed and ways how to fix it are proposed. The model is at the design stage now. The future work is about the elaboration of integration ways to above mentioned technologies in universal crypto financial model. This model will be taking into account technology interaction features and possible security problems.

Keywords: security issue, blockchain, cryptocurrency, key management, Bitcoin, Ripple, Namecoin

REFERENCES

1 Andreas M. Antonopoulos, Mastering Bitcoin

2 S. Eskandari, D. Barrera, E. Stobert, J. Clark, A First Look at the Usability of Bitcoin Key Management, http://www.internetsociety.org/sites/default/files/05_3_3.pdf

3 J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, E. W. Felten, SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, http://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf

4 "Namecoin", Namecoin, http://namecoin.info/

5 G. Slepak, "OKTurtles + DNSChain", https://okturtles.com/other/dnschain_okturtles_overview.pdf

A DATASET ANONYMIZATION FRAMEWORK FOR PUBLIC TRANSPORT OPERATORS

Andrea Melis, Franco Callegati*, Marco Prandini§*
**DEI – Department of Electrical, Electronic and Information Engineering*
§ DISI – Department of Computer Science and Engineering Università di Bologna
{andrea.melis6,franco.callegati,marco.prandini}@unibo.it

Increasingly, public administrations offer services to citizens by means of the coordination of different private companies. These companies usually have to collect data about the users' services, and very likely will have to share them to enable the coordinated provisioning of the service.

A representative scenario is the public transport of a whole Region, where the Regional administration wants to offer citizen a unified view of the service, built as a composition of private transport operators. This scenario introduces the need to guarantee a strong respect of passengers' privacy, while the transport operators should still be able to properly share revenues and costs. Consequently, a set of anonymization techniques should be implemented, striving to achieve contrasting goals: minimizing possible privacy breaches, and preserving essential information to compute economic compensations.

In the literature, there are a few reference anonymization techniques[1, 2, 3] that are effective against identification of individuals, but also many examples of how to circumvent them. Attacks like composition of auxiliary information[4] or Data Mining[5] show the weakness of techniques like k-anonymity or l-diversity. Even worse, a more general approach[6] shows how techniques as t-closeness or differential privacy cannot reach a satisfactory trade-off between effectiveness against de-anonymization and utility for legitimate purposes, according to various metrics. For these reasons, researchers developed many domain-specific projects, aimed at overcoming the limits of the general techniques by building algorithms strictly related to a particular context. Research attack this limits introducing an evaluation metric about the presence of an individual in a data set called δ-presence; and subsequently present algorithms for effectively anonymizing to meet δ-presence. Other kind of work[7] operate by complementing existing techniques with PRAM (Post Randomization Methods)

Our work has a twofold goal: solving the specific issue of protecting passengers against possible tracking of their travels in public transport systems, and generalizing the result enough to be applied to similar contexts. These objectives cannot be reached by applying existing techniques. We start from a real-case scenario, in order to build a general anonymization framework that could work in the context of different public transport operators that share private data.

The studied scenario stems from the project of the Regional Government of Emilia-Romagna (Italy) to unify all the different transport operators under a single centralized system. The final goal is to enable the issuing of an inter-operable ticket, that can be sold by any operator and used in every part of the Region. The necessary component of this system is a clearing system, to redistribute the profits among the transport operators according to the tickets sold and validated. To this end, the clearing system needs to correlate data describing all individual trips; it introduces two possible kinds of privacy breaches:

- Identification attacks to correlate user identities with travel titles identifies
- Pattern discovery to steal competitive advantages from "fellow" operators

Despite this scenario may seem quite common, the above requirements make it structurally different from other known systems such as that in force in London with Oyster card or in Netherlands that also implements anonymization techniques that unfortunately we cannot reuse. This problem has led us to try to, starting from our context, generalize the problem, and therefore, the solution.

To address these issues in a way that can be generalized, we started by classifying the structure of any plausible data-set of public transport operator, identifying and grouping attributes in three categories: Sensitive values (SV), Quasi-identifiers (QI), and not sensitive.

On the reference data-set we implemented a composition of anonymization techniques that provides strong anonymization of the users, and masking of the data to prevent effective evaluations over the operative parameters of competing operators. This was done in a way that preserved the utility of data. A critical constraint is that the specific scenario requires keeping track of tickets serial numbers to be able to correlate different segments of the same travel; in particular any transfer from one medium to another must be reconstructed from the series of validations.

Techniques as k-anon and l-div are not suited for our purposes; for example, applying k-anon to the "validation date" attribute and pooling the entries according to whole hours, destroys the link between legs of the same trip (in Fig. 1), and at the same time it is not sufficiently strong against data-mining attacks with Bayesian classifiers.

The heart of the first stage of the project will be the testing phase of this framework over a significant quantity of real-world data, that we are starting to collect. The testing methodology will make use of metrics already described in the literature like[8] which take into account the need for a trade-off between privacy and utility. We will also perform pattern discovery tests/attacks, using Data Mining algorithms tailored for this context and also other kind of classifiers such as those described in[9].

The main expected result is that our framework could show a significantly greater strength against attacks and privacy breaches; at the same time we expect that the anonymized data will preserve quantitative properties that allow the precise computation of useful clearing functions.

We strive to define an approach which is general enough to be directly comparable to the most widely accepted algorithms, so that we can measure the improvement level using established metrics. Starting from real-world scenario, this work wants to fill a gap in the literature, creating a new framework to anonymize a data-set while preserving a measurably good utility, in a context of public transport operators that share private data.

At this stage, we are not able to predict whether the results will be robust enough to apply them also to high-sensitivity scenarios, like (as a useful review pointed out) the case of Tallinn where e-ID cards are used to directly tie travel cards to the traveller identity.

Keywords: privacy, anonymity, Public Transport

Serial	Ty.	Time V.
002679	4	1420260949
004844	4	1420257349
077364	3	1420268149
017942	3	1420325749
044337	5	1420296949

Serial	Ty.	Time V.
002679	4	4 AM
004844	4	3 AM
077364	3	6 AM
017942	3	10 PM
044337	5	2 PM

Serial	Ty.	Time V.
002679	4	Morning
004844	4	Morning
077364	3	Morning
017942	3	Afternoon
044337	5	Evening

Figure 1. Example on how it's possible to use k-Anonymization to the data validation.

REFERENCES

1 Personal Privacy vs Population Privacy: Learning to Attack Anonymization. Graham Cormode

2 UMicS: From Anonymized Data to Usable MicroData. Graham Cormode, Enotng Shen, Xi Gong, Ting YU,Cecilia M. Procopiuc, Divesh Srivastava

3 The cost of Privacy: Destruction of Data-Mining Utility in Anonymized Data Publishing Justin

4 Privacy for Public Transportation Thomas S. Heydt-Benjamin, Hee-Jin Chae, Benessa Defend, and Kevin Fu

[5] Empirical privacy and empirical utility of anonymized data. Graham Cormode, Cecilia M. Procopiuc, Divesh Srivastava Entong Shen, Ting Yu

[6] Simple and Effective Privacy Preservation X. Xiao and Y. Tao

[7] Toward inference attacks for k-anonymity Yan Sun, Lihua Yin, Licai Liu, Shuang Xin

[8] Hiding the Presence of Individuals from Shared Databases M. Ercan Nergiz, Maurizio Atzori, Christopher W. Clifton

[9] Data Fusion: Resolving Conflicts from Multiple Sources. Xin Luna Dong, Laure Berti-Equille and Divesh Srivastava

SESSION 5: LAW

Session moderated by ANNA-MARIA OSULA,
University of Tartu,
NATO CCD COE

DIRECT PARTICIPATION IN CYBER HOSTILITIES

Allyson Hauptman

DIGITAL EVIDENCE COLLECTION AND FUNDAMENTAL RIGHTS: CHALLENGES IN FINDING A RIGHT BALANCE

Eneli Laurits

NEW REALM OF GATEKEEPERS IN EUROPE

Karmen Turk

DIRECT PARTICIPATION IN CYBER HOSTILITIES

2LT Allyson Hauptman
United States Army
allybook@verizon.net

In contrast to the kinetic domains of warfare, cyberspace is uniquely civilian in character. Because the internet was developed primarily as a tool of business and academia, its most proficient talent exists in those worlds, as opposed to the military world. The fast-paced development of technology, as modelled by Moore's Law,[1] requires computer experts to continuously study. This constraint is feeding the need for governments to employ civilians alongside their armed forces in the pursuit of military cyber capabilities. In the past, this civilian employee would have primarily been responsible for intelligence collection activities, but in the modern age government cyberspace operations include a variety of hostile acts, some of which the civilian workforce is currently tasked to perform. Under the Laws of Armed Conflict, these civilians could lose their civilian protections as de facto[2] – but not legal – combatants. The proliferation of de facto combatants undermines the very notion of discrimination on the battlefield, and this should be a major concern for governments who wish to protect their civilian employees.

The concept of Direct Participation in Hostilities refers to the loss of a person's non-combatant privileges (mainly targetability) for such a time he is engaging in hostile acts against an enemy. If this person is consistently engaging in the acts, he may be considered to have a continuous combat function. While a civilian who accompanies the armed forces or performs a non-combat function retains his civilian protection, if his job meets the criteria for a continuous combat function described above, he becomes a de facto combatant.[3] De facto combatants, because they are not distinguished as legal combatants, are not entitled to the traditional combatant privileges, such as Prisoner of War status. The primary question this research sought to answer is what State cyber activities constitute a Direct Participation in Hostilities and, thus, should only be performed by uniformed, military personnel.

The analysis primarily used the three criteria developed by the International Committee of the Red Cross for evaluating whether an act constitutes a Direct Participation in Hostilities. The first criteria is threshold of harm, that the act will likely cause an adverse effect to the military operations or military capacity of one of the conflict's parties and/or cause death, destruction, or injury to a protected person or object.[4] The second ICRC requirement is that there must be a direct causation between the act committed and the effects incurred. This means that there must be a direct causal link between the act and the effects that are likely to result from the act.[5] The final criteria of the test for whether an act constitutes a direct participation in hostilities is if there exists a belligerent nexus. This asks if the act was designed to cause the harm either in support or to the detriment of a party to the conflict.[6] It should be noted that the analysis of whether an act meets these criteria is based upon United States definitions and policy documents, such as how to define an "offensive" verses "defensive" cyber operation.

For the analysis, the research used an effects-based approach, drawing parallels between activities conducted in the kinetic and cyber domains. It considered six different types of State cyber activities: routine operations, passive defensive cyber operations, defensive cyber response actions, cyber intelligence collection, cyber preparation of the environment, and cyber attacks. A feasible scenario was developed for each category and the scenario's hypothetical actor's activities considered under the ICRC's criteria for direct participation. The research concludes that there are three main types of cyber activities that should not be performed by non-uniformed State personnel: defensive cyber response actions, cyber preparation of the environment, and cyber attacks.

Keywords: military, government, cyber operations, IHL, international law, warfare, combatant

REFERENCES

1 Moore's Law Inspires Intel Innovation, (Intel: January 14, 2014), available at http://www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html. Moore's law states that the number of transistors on a chip will double every year. Since its formulation it has come to symbolize the concept of quick innovation in computing technology. It has adapted to include equations for the size and speed of a multitude of hardware and software capabilities.

2 By "de facto combatants" this paper refers to individuals who can be considered combatants by the actions they perform but are not labeled as combatants by their sponsor/host state.

3 Jody Prescott, Direct Participation in Cyber Hostilities: Terms of Reference for Like Minded States?, INTERNATIONAL CONFERENCE ON CYBER CONFLICT (NATO CCCOE: 2012), at 39. Domestic provisions may consider these people to be contractors or not members of the armed forces and thus entitled to civilian protections, but if their jobs require them to essentially do what the armed forces do, then under international law they are combatants. When authorized by the state to perform these activities, weight is lent to the concept of them having a continuous combat function, which is not subjected to the temporal limitation of direct participation in hostilities.

4 Id, at 47. The word likelihood is key in this definition, because it is not necessary for the effect to materialize. As long as it is reasonably likely that the act would have this result, the threshold of harm has been reached. This means that a person would be targetable even if the enemy is able to block the effects of the attack or the attack fails to materialize in the foreseen way.

5 NILS MELZER, INT'L COMM. OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 46 (2009), at 51. Direct causation is defined by those effects that are reasonably likely to result from the commission of a specific act. That is, given the knowledge the perpetrator had and given the effects a reasonable person would have foreseen, there can be either a direct or indirect causal link. An indirect link, one resulting from a chain of events unforeseen or an effect the perpetrator could not have foreseen, would not cause a civilian to lose his protections.

6 Id, at 58. This is the most subjective part of the analysis. Not only must the act be reasonably likely to result in harm that's meets the specified threshold and be directly linked to that harm, but the actor must also intend for the event to occur to the benefit or detriment of a party to the conflict.

DIGITAL EVIDENCE COLLECTION AND FUNDAMENTAL RIGHTS: CHALLENGES IN FINDING A RIGHT BALANCE

Eneli Laurits
Tartu University
eneli.laurits@just.ee

The need to alter national laws and international norms in the context of digital evidence has been intensively discussed among researchers and practitioners throughout the last decade. Consideration has been given to the fact that digital evidence is so specific in its nature that it requires a separate regulation.

Already in 2005, Orin S. Kerr stressed the need for special regulation over the collection of digital evidence: „Digital evidence is collected in different ways than eyewitness testimony or physical evidence. The new ways of collecting evidence are so different than the rules developed for the old investigations often no longer make sense for the new."[1] Moreover, continuously many authors have stressed the need for „new regulations".

It is easy to make fatal errors when collecting digital evidence. Digital evidence is latent, like fingerprints or DNA evidence; crosses jurisdictional borders quickly and easily; is easily altered, damaged, or destroyed and can be time sensitive. Decision-makers should be able to rely on the standard to determine the credibility of digital evidence. However, legislations in Europe mostly do not stipulate in their legal codes a specific definition of what electronic evidence is: electronic evidence is equivalent to traditional evidence.

The present paper analyses the need for a special regulation over digital evidence by the example of the Estonian Code of Criminal Procedure. The biggest distinction in collection of evidence in the Estonian Code of Criminal Procedure is made for the collection of children testimony, since it is a particularly delicate personal evidence. So, is it possible to take the example from this regulation and apply it to digital evidence? There are some obvious similarities between these two kinds of evidence: both of them are easily altered, damaged, or may even be destroyed.

Also, years ago, the DNA was as unknown as digital evidence is now, that it too evoked strong opposition among participants in proceedings; and a certain veil of secrecy surrounded it. Now, there is the same situation with digital evidence. The same problems needed to be overcome: is it possible to change this kind of information and if so, how easily; how can we be sure that the information presented to us is indeed the whole truth?

In case of digital evidence, the problem perhaps is not so much in formalizing and collecting the evidence, since these acts probably do not differ very much from formalizing and collecting other, so-called physical evidence. The core difficulty about digital evidence is abundance of information – evidence must somehow be searched and selected out of the huge amount of data. Defenders fear that in course of such an intensive search, some fundamental rights of individuals might be infringed and that collection of evidence might not conform to the principle of proportionality. If in the physical world the search of evidence, such as on-premise search, is limited by the physical world itself, then the search of computer data has no limits. Often, it is so in the literal meaning of the word: the searches may last for an indefinite period of time, they might be conducted several times, and it is not unusual for them to pass the state borders.

Estonian Code of Criminal Procedure does not have any specific rules for pre-trial procedure and for the conduct of proceedings, stipulated in the Convention on Cybercrime; instead, when dealing with cyber-

crimes, general provisions that regulate investigative activities are applied. When in the absence of specific provisions, general provisions are applied, arises the problem of protection of fundamental rights. An entry into a room and an entry into a computer cannot be directly compared from the infringement of fundamental rights point of view, while the Estonian Code of Criminal Procedure does not make any distinction between the two[2]. Thus, adoption and incorporation of the principles of procedural law that arise from the Convention on Cybercrime into Estonian law is deemed deficient[3].

The Supreme Court of Estonia has found that when searching and seizing computer data, one must take into account the principle of proportionality. Therefore, is there a need for supplementing the Estonian Code of Criminal Procedure with specific cases of search regulation, such as seizure of encrypted or password-protected data, introduction of a ban on deliberate destruction of data? Should the differences between conducting the search via computer network and via computer systems without any physical connections (including the ones with "cloud" solutions) be stipulated as well?

What are these specific provisions, which the Estonian Code of Criminal Procedure lack, and are they still needed? How to prevent possible over-regulation, which often haunts cognitively alien to each other and rapidly developing areas. Where does the borderline fall between the possibility of criminal proceedings and the protection of fundamental rights? The problems connected to digital evidence regulation and the balance with protection of fundamental rights are the subject of this article.

Keywords: digital evidence, digital evidence regulation, fundamental rights, principle of proportionality

REFERENCES

[1] Orin S. Kerr „Digital evidence and the new criminal procedure". Columbia Law Review 279 (2005)

[2, 3] E. Kergandberg. Eesti kriminaalmenetlus: mõned rindeteated. – Juridica IV/2013

NEW REALM OF GATEKEEPERS IN EUROPE

Karmen Turk
University of Tartu, PhD Candidate
Karmen.turk@triniti.ee

European Court of Human Rights (ECHR) delivered a Grand Chamber judgement on 16th June 2015 in the matter of Delfi versus Estonia.[1] The case concerns Delfi AS, the news portal, that was found liable by the Estonian courts for its failure to prevent unlawful comments from being published in its comments section, despite having taken down the offensive comments as soon as it had been notified about them. This was the first case in which the ECHR has been called upon to examine a legal questions regarding user generated content on the Internet.

The facts of the case were simple: Estonian biggest Internet newsportal published an article on shipping company wrecking an iceroad between the mainland and the island. The newsportal business model allowed for users anonymously to comment it's articles. That particular article attracted 185 comments. Six weeks after the publication, the owner of the shipping company sent a notice to Delfi AS requesting takedown of 20 comments. Delfi AS complied the same day and deleted the comments.

Regarding the commenting platform, there was a set of safeguards in place:

1. rules of the platform prohibiting insulting comments;
2. automatic filtering system for vulgar words;
3. notice-and-take-down button next to each comment;
4. contacting Delfi AS and
5. in case of articles on controversial topics, the editors were moderating the comments' platform.

The Court essentially regarded the article itself as a neutral and balanced one and took note of the safeguards in place. However, it concluded that that imposing liability on Internet news portals would not contravene the tight to impart users' comments, if the platform operator fails to take measures to remove clearly unlawful comments without delay, even without notice from the alleged victim or from third parties.

The question is, whether there is a legal contradiction. Namely, the judgement relates to the legal environment comprising of two relevant acts in Europe – the Council of Europe standard on freedom of communication on the Internet as well as the European Union law.

In a widely cited 2003 Declaration, the Committee of Ministers of the Council of Europe urged member states to adopt the following policy: "*In cases where ... service providers ... store content emanating from other parties, member states may hold them co-responsible if they do not act expeditiously to remove or disable access to information or services as soon as they become aware ... of their illegal nature. When defining under national law the obligations of service providers as set out in the previous paragraph, due care must be taken to respect the freedom of expression of those who made the information available in the first place, as well as the corresponding right of users to the information.*"[2]

The same position was essentially adopted by the European Union through the Electronic Commerce Directive of 2000.[3] Under the Directive, member states cannot impose on intermediaries a general duty to monitor the legality of third-party communications; they can only be held liable if they fail to act "expeditiously" upon obtaining "knowledge" of any illegality.

This approach is considered a crucial guarantee for freedom of expression since it tends to promote self-regulation, minimizes the need for private censorship, and prevents overbroad monitoring and filtering of user content that tends to have a chilling effect on online public debate.

The European Union Court of Justice has dealt with the issue of intermediary liability in numerous cases. In one of the widely cited judgements of SABAM, The court ruled that the implementation of general filtering systems collides with the prohibition contained in the E-Commerce Directive to Member States to impose a general obligation to monitor on service providers conducting activities of mere conduit,

caching and hosting. The Court acknowledges that such a system would put at risk the freedom to receive or impart information, as the system might not have been always able to distinguish between unlawful content and lawful content, eventually blocking lawful communications.[4]

In abstracting the judgement of *Delfi versus Estonia*, the *judges Sajó and Tsotoria* in their joint dissenting opinion concluded: "*The duty to remove offensive comments without actual knowledge of their existence and immediately after they are published means that the active intermediary has to provide supervision 24/7. For all practical purposes, this is absolute and strict liability, which is in no sense different from blanket prior restraint. […]For the sake of preventing defamation of all kinds, and perhaps all "illegal" activities, all comments will have to be monitored from the moment they are posted. As a consequence, active intermediaries and blog operators will have considerable incentives to discontinue offering a comments feature, and the fear of liability may lead to additional self-censorship by operators. This is an invitation to self-censorship at its worst.*"

Thus, considering the somewhat different approaches of two courts in Europe, it might be now a time to redefine the liability standards of intermediary – the recent ECHR judgement does not fit well with the letter and spirit of relevant legal acts or the jurisprudence of the European Union courts. However – a state being a member of the European Union would also be a contracting party to the European Convention on Human Rights. Consequently, 28 member states of EU are today in a legal "limbo" regarding the regulation of intermediary liability.

Keywords: intermediary liability, freedom of expression, host, news portal

REFERENCES

1 Case no.64569/09.

2 Declaration on freedom of communication on the Internet, 28 May 2003, adopted at the 840th meeting of the Ministers' Deputies.

3 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16.

4 European Court of Justice, 16.02.2012, case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) versus Netlog NV.

SESSION 6: TECH II

Session moderated by Prof OLAF MAENNEL,
Tallinn University of Technology

EVENT MANAGEMENT AND INCIDENT RESPONSE FRAMEWORK FOR SMALL COMPANIES

Markus Kont

QUALITATIVE AND QUANTITATIVE ANALYSIS OF SOFTWARE DEFINED NETWORKING CONTROLLERS FROM THE POINT OF VIEW OF SECURITY

Sara I. González, Javier Alonso, Isaías García

ADVANCED SECURITY ASSURANCE CASE BASED ON ISO/IEC 15408

Oleg Illiashenko, Oleksandr Potii

EVENT MANAGEMENT AND INCIDENT RESPONSE FRAMEWORK FOR SMALL COMPANIES

Markus Kont
Spin TEK AS, CCD COE, Tallinn University of Technology
markuskont@gmail.com

Over the last decades, the world has become increasingly dependant on various online services, such as e-mail, e-commerce applications and information exchange pathways. While the tendency from end-user perspective is to demand seamless integration and continuous availability, the technical complexity of such solutions creates significant overhead for professionals, who are tasked with maintaining the supporting infrastructure. This is especially true within the context of small business web hosting and content providers, where the Network Operations Center (NOC) is usually comprised of no more than three to five persons. Sometimes less.

The nature of such services requires constant availability over public networks, making them also subject for constant malicious probing. While it is mostly conducted by automated botnet nodes, any targeted attack can severely cripple or compromise confidential data. To make matters worse, vulnerable web services, which may not be owned by the hosting provider, can be hijacked and used as an attack platform. Constant monitoring of events and immediate incident response must be conducted, but are usually done manually and after the damage has already been inflicted.

Commercial security solutions are not affordable for small companies in terms of licensing fees, hardware requirements and technical integration issues that have to be overcome by the same NOC personnel, who already spend their time on multiple projects. Several open-source monitoring solutions have emerged over the past years, but usually focus on passive alert generation, network capture, data visualization and log collection. Small companies lack the technical means to store network packet captures for a meaningful time period, while the high false positive rate of Intrusion Detection (IDS) and Intrusion Prevention Systems (IPS) can prove problematic. The risks associated with IPS solutions in particular are usually considered too high within modern heterogenous networks, as detection rules are written quite specifically for certain types of packet streams. Valid traffic can be flagged as malicious, which would result in negative business impact.

Forensic evidence for attacks, which is commonly distributed across multiple systems, can be found within operating system and application log files, but require human interpretation and correlation of data. System administrators already have the experience to identify malicious activity. Verbosity of logs and data fragmentation make such analysis difficult to conduct, therefore the event data must be gathered for processing. Administrators also have a simple rule – if any action is to be conducted on continuous basis, then it should be automated. Open-source syslog daemons and event correlation tools, such as Simple Event Correlator (SEC), provide the toolset for achieving that.

Rapid development rate and lack of proper implementation methodologies, especially in scientific publications, were the main motivating factors for writing this thesis, which focuses on building an event monitoring and active response framework for a small company for security incident handling automation. One of the main contributions of this thesis is an analytical and performance comparison of existing log collection and event correlation tools. Analysis of log collection tools includes three syslog message collection solutions – Rsyslog, Syslog-ng and NXLog. A number of tests were conducted by the author, in order to evaluate the performance of these solutions for different event collection scenarios.

Apart from the tests, the thesis also provides a detailed assessment of event correlation capabilities of SEC and NXLog.

An overview of syslog daemon functionality and configuration syntax can be found within the official software documentation, but system administrators often prefer to utilize older stable versions of software. Therefore the author conducted the analysis across multiple stable software builds that are packaged for popular Debian and Ubuntu Server LTS operating systems. Different server configurations and use-case scenarios were tested within specifically build environment to provide the best overview of performance constraints.

Another contribution of this thesis is the description of event monitoring and incident response framework for a small company environment. Based on conducted experiments and comparisons, Syslog-ng and SEC were selected for building the framework. The proof-of-concept of the proposed framework has been implemented in Spin TEK AS by the author. Apart from describing the architecture of the implementation, the thesis also provides a publicly available repository of SEC rules, infrastructure configuration guidelines and control scripts. The content of the repository is maintained by the author, and helps the reader to set up a similar system for real-time event monitoring and incident response.

The author devised a hierarchical event correlation ruleset, which comprises of three principal tiers. Firstly, events are aggregated to provide common canonical meaning with relevant information attached as synthetic event prefix or suffix. Secondly, a relatively small amount of correlation rules monitors the pattern in which they occur. Finally, if an attack has been correlated, then the attacker source IP address is extracted from synthetic event and forwarded to control script. The latter maintains firewall rules, which drop all traffic from malicious host for a predefined time period. Additional notification is sent to administrator if that host has been detected for ten times, which results in five to thirty notifications per day within production environment of Spin TEK AS.

After a period of one year, the project has been considered a success. The author is currently in the process of integrating network analysis software and visualization tools into the framework. Additionally, NATO CCD COE technology branch has recognized the project.

Keywords: event correlation, syslog daemon, open-source, event message, cpu core, log collection, log message, monitoring system, performance benchmarking, SEC, syslog server, configuration syntax, comparison, implementation, rsyslog, syslog-ng, nxlog

REFERENCES

1 Kont, M. “SagittariuSEC”, 2014, [https://github.com/markuskont/SagittariuSEC]

2 Adiscon, “Rsyslog v5-stable documentation”, Web. May 2014, [http://www.rsyslog.com/doc/v5-stable/]

3 Adiscon, “Rsyslog v7-stable documentation”, Web. May 2014, [http://www.rsyslog.com/doc/v7-stable/]

4 BalaBit, “The Syslog-ng Open-Source Edition 3.3 Administrator Guide”, Web. May 2014, [http://www.balabit.com/sites/default/files/documents/syslog-ng-ose-3.3-guides/en/syslog-ng-ose-v3.3-guide-admin-en/html-single/index.html]

5 BalaBit, “The Syslog-ng Open-Source Edition 3.5 Administrator Guide”, Web. May 2014, [https://www.balabit.com/sites/default/files/documents/syslog-ng-ose-3.5-guides/en/syslog-ng-ose-v3.5-guide-admin/html-single/index.html]

6 [Botyabzky, B. “NXLOG Community Edition Reference Manual for v2.7.1189”, Web. May 2014, [http://nxlog.org/nxlog-docs/en/nxlog-reference-manual.html]

7 Vaarandi, R. “sec manual page”, Web 2014, [http://simple-evcorr.sourceforge.net/man.html]

QUALITATIVE AND QUANTITATIVE ANALYSIS OF SOFTWARE DEFINED NETWORKING CONTROLLERS FROM THE POINT OF VIEW OF SECURITY

Sara I. González, Javier Alonso, Isaías García
University of León, Spain
[sara.gonzalez, javier.alonso, isaias.garcia] @unileon.es

The emergence of Software Defined Networking (SDN) paradigm shifts from traditional completely distributed network management to a (logically) centralize management. SDN represents the answer to address the increasing network management complexity.

The modern data center with increasing demands as well as the need to accelerate innovation in networking has led to conduct research of new networking solutions in order to cope with all these needs[1]. Traditional networks are complex and hard to manage and there has been a growing need for simplification in the management of these technologies. Some of the reasons of this complexity are the difficulty to define a correct procedure for configuring the network or the heterogeneity of the network devices, each of different vendors and configuration options, which must be setting up individually. In order to get this simplification and reduce the cost of traditional technologies, it has been proposed to move the control software off the device.

Software Defined Networking (SDN) represents a paradigm shift to try to cope with these problems by centralizing network management in a logically centralized controller[2]. Besides SDN provides a network-wide view, including topology and traffic, and direct control of the data plane through the controller, which avoids having to configure each network device separately.

As a new network architecture, a fundamental characteristic of SDN is the separation of the control plane and the data plane in order to get networks more programmable, automatable and flexible.

The last defining feature provided by the SDN approach is the automation and virtualization of the network. Abstractions help against the actual complex problem of network control faced by networks today, by providing a global network view as well as its current state in order to better configure and install specific flow rules based on the reality and the desired goal of the overall network, which also helps solving network-wide problems.

SDN architecture[3] is composed of three main layers, each of them has its own specific functions: the application layer, the control layer and the infrastructure layer. Controllers, located in the control layer, are a crucial part of a SDN network since they are the brain of the network and, through the definition of network policies, they communicate with the switches whenever is necessary and provides primitive instructions in order to allow them to make fast decisions about how to deal with incoming packets. This communication is made through the standardized OpenFlow protocol[4]. The controller has the view of the entire network and provides a northbound API in order to be able to communicate with applications, which belong to the application layer. A controller is a software program that often comes with its own set of common application modules that, although they are SDN applications, are often bundled with the controller.

There are very diverse sets of implementations of SDN controllers available today, including open source and proprietary SDN controllers, with different design and architectural choices. Therefore, they can be categorized based on different aspects. One of the objectives in this master thesis is to analyze

qualitatively all the current controllers up to now regarding to these aspects and identify some others to extend the analysis.

Another objective is the realization of a quantitative analysis of some open source controllers through some experimental practices. For these experiments, Mininet[5] will be used as a SDN emulation tool because it offers the possibility to easily experiment with and test new ideas, what should greatly accelerate innovation in SDN.

Finally, although SDN can offer a lot of advantages in controlling and configuring the network and could even help improve its security through the development of applications for the controller, which can manage and monitor the whole network, the SDN framework has introduced new vulnerabilities too[6]. Due to the new network design proposed by SDN, specific attacks on the control plane communication and logically-centralized controllers appeared. Also the way that an attack affects the network is different. So traditional security policy approaches may not address the needs of SDN and thus it is required to look for new solutions. Nevertheless, most threat vectors are independent of the technology or the protocol, because they represent threats on conceptual and architectural layers of SDN itself. Therefore, SDN, as a layered architecture, requires each layer have its own security, where its elements must provide secure boundaries around services and access. Therefore, the final aim of this master thesis will be to study and compare SDN controllers from security principle perspectives.

In summary, this master thesis has three-fold goals:

1. Qualitatively analysis of SDN controllers respect to the different capabilities offered,
2. Quantitative analysis of a pre-selected open source SDN controllers from performance metrics, and
3. Qualitative analysis of security by design analysis of the current SDN controllers under consideration.

Keywords: Software Defined Networking, SDN Controllers, Security

REFERENCES

1 Feamster, N., Rexford, J., & Zegura, E. (2013). The road to SDN. Queue, 11(12), 20.

2 Fundation, O. N. (2012). Software-defined networking: The new norm for networks. ONF White Paper.

3 Fundation, O. N. (2014). SDN architecture. https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf, 2015.

4 McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., ... & Turner, J. (2008). OpenFlow: enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review, 38(2), 69–74.

5 Lantz, B., Heller, B., & McKeown, N. (2010, October). A network in a laptop: rapid prototyping for software-defined networks. In Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks (p. 19). ACM.

6 Kreutz, D., Ramos, F., & Verissimo, P. (2013, August). Towards secure and dependable software-defined networks. In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking (pp. 55–60). ACM.

ADVANCED SECURITY ASSURANCE CASE BASED ON ISO/IEC 15408

Oleg Illiashenko
National Aerospace University "KhAI" / Assistant lecturer
o.illiashenko@csn.khai.edu

Oleksandr Potii
National Aerospace University "KhAI" / Professor
potav@ua.fm

In attempt to define and regulate IT-products evaluation the Common Criteria for information technology security evaluation (abbreviated as CC) as an International standard ISO/IEC 15408[1,2] has been developed. Requirements of objectivity, repeatability, reproducibility, impartiality and comparability are put forward for the evaluation results. They can be met in case of supporting scope, depth and rigor of evaluation process only. Another international standard ISO/IEC 18045[3] contains description of the methodology of security evaluation, but it doesn't contain any formal technique for evaluation, what makes performing of evaluation process complicated and one-sided[4]. In a broader sense assurance reduces the uncertainty associated with vulnerabilities of the IT-product, and thus the potential vulnerability is reduced leading to a reduction in the overall risk.

About to 74% of organizations base their compliance mechanism mostly on manual methods (e.g. text editors, spreadsheets, etc.), indicating lack of existence of satisfactory solutions in 37% of cases[5]. As a starting point the statements described in[6] are used.

Todays the case as a concept is limited as a means of a tool for formalization of requirements, but it should be enhanced by decision making procedure of conformity with requirements that will tend to reducing of uncertainty and increasing of objectivity, repeatability, reproducibility, impartiality and comparability of assessment in order to satisfy needs of all groups of CC in evaluation of the security properties of targets of evaluation: consumers, developers, evaluators, others.

It's needed to have a unify methodology for both parties. This methodology should be based on international standards[1-3,7] and contain the requirements how to prove that the decision of conformity is solely correct. Such kind of methodology is building of cases for justification of correctness and implemented requirements. A significant reliance on people during security assurance activities and further application of assurance procedure (by the target audience of CC) is a danger that particular "experts" become a bottleneck on any solution. The loss of knowledge, lack of traceability, consistency, proficiency, maturity, inappropriate use of artefacts can lead to problems in maintaining the case[8]. There is a great need for providing clear and comprehensible argumentation process of demonstrating and justifying how evidence fulfils the safety requirements[5,6].

Most of known cases contain claim- and evidence-based justification that a system under assessment meet or should meet the specified objectives (e.g. safety, security, dependability etc.) in a particular field. Among them are: safety case, assurance case, trust case, security-informed safety case, etc. No one type of known cases does not contain a technique for justification that decision of an expert is solely correct and couldn't be treated in another way by any other person. Uncertainty of such kind could lead to loss of money and time. The evidence of conformity should correspond to the constructed claim in order to link the solution with the judgment. In modern cases construction of evidence for claims mostly relies upon an experience of a particular person, but the logic of this construction is absent. This fact significantly increases influence of a case from the person, who is involved in process of evaluation. The decision, which is based on empirical experience of evaluator or expert, potentially increases

an uncertainty (characteristics, history, observations, measurements, evaluative results, analyses, inferences) of evaluation process and the final result (which could be potentially inadequate), that may lead to hazardous consequences in the end of the day.

We enhance the concept of assurance case, proposed in[6] with the fifth element, a decision-making technique, which allows decreasing uncertainty of assessment (table 1).

Argument Element	Description
Clains	Statements that something has a particular property
Evidnce	Empirical data on which a judgment can be based
Reasoning	Statements which tie evidence together to establish claim
Assumption Zone	Limit of an argument where claims are accepted without evidence
Decision making technique	**The basis for decision of conformity**

Table 1. Assurance case components with added decision-making technique

We propose to name this type of assurance case – Advanced Security Assurance Case (ASAC). Figure 1 depicts four main stages of ASAC building.

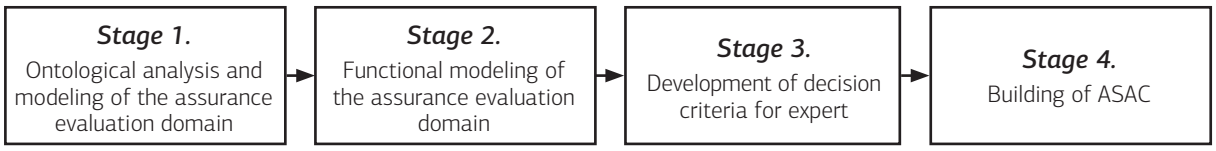

Figure 1. Stages of Advanced Security Assurance Case building

For ASAC's representation the DRAKON language is used. It contains requirements for assessment algorithm of their validation and result of assurance assessment. The advances of DRAKON are clarity and simplicity of algorithms representation and fully formal representation of visual rules of structured programming. DRAKON is an algorithmic visual programming language developed within the Buran space project[9,10]. ASAC greatly reduces the workload of the expert, allowing him to start work immediately, without firstly developing a methodology for assessment, what is time consuming in practice. An example of ASAC for evaluation of vulnerabilities AVA_VAN.1 "Vulnerability survey" from assurance class "AVA: Vulnerability assessment"[1] with corresponding actions of expert is provided (figure 2)[11].

The main peculiarities of ASAC are:

- Analysis of verbal requirements in CC written in natural language (NL) form;
- Identification of properties that the object should possess. Verbal NL requirements should be decomposed to the level of elementary properties which forms a tree of properties;
- Linking of properties with corresponding evidences (both quantitative and qualitative) from the set of evidences (in other types of case-based techniques there is no such technique);
- After the linking of properties with evidences the corresponding actions for the proof of evidences are defined;
- If the particular evidence is satisfied, the tree is aggregated and it is concluded that the corresponding property is satisfied;
- To prove that evidences of related properties correspond to particular requirement the actions are defined. It means that there is an algorithm of conformity decision making, and so the new concept of case is proposed – an algorithmic concept, which is the core idea of ASAC.

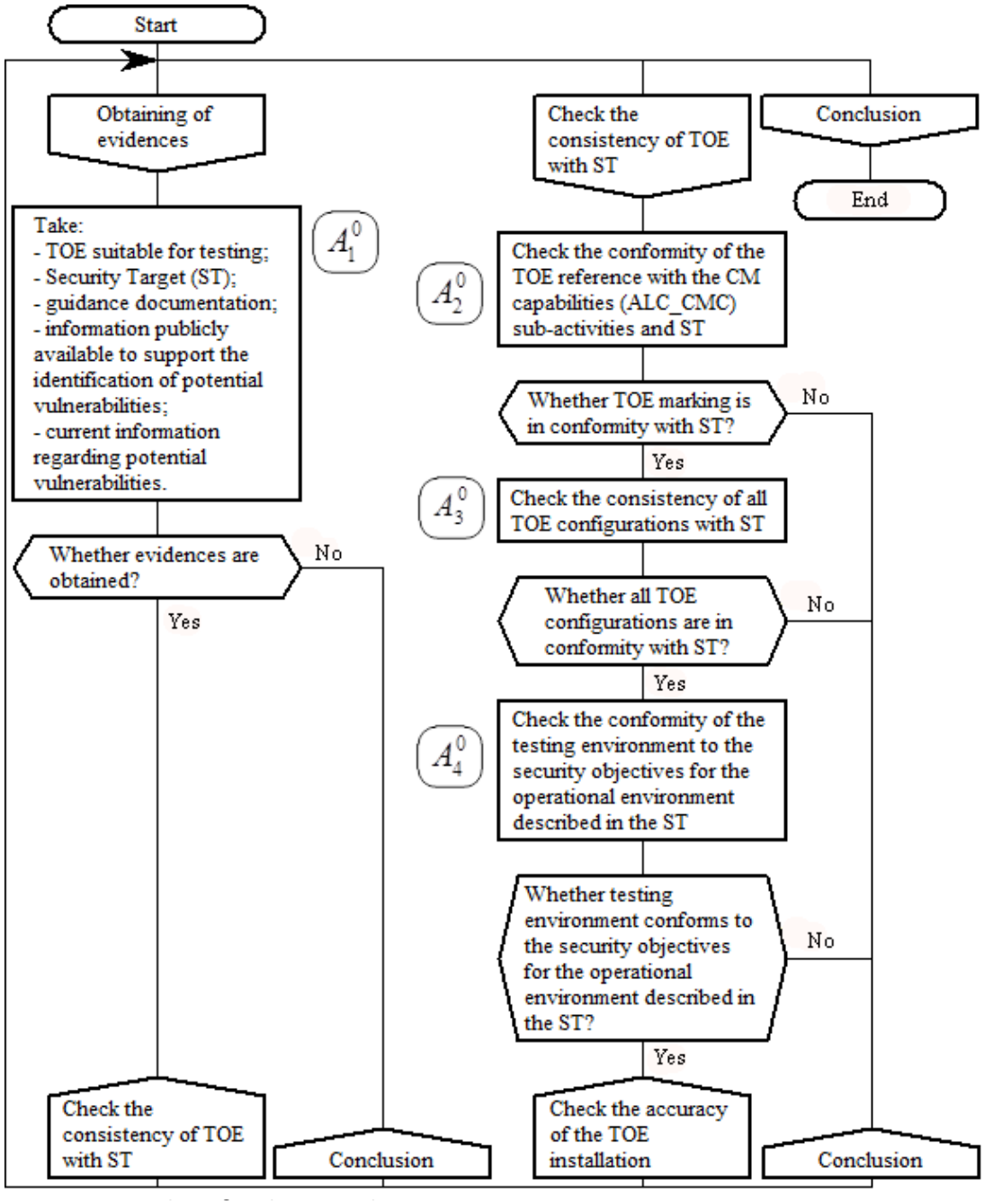

Figure 2. An example of Advanced security assurance case ASAC in DRAKON notation

Figure 3 shows the new concept of assurance as a notion. An assurance argument starts with claims about risks and then gathers all the evidence and supporting arguments into a logical hierarchical structure. The goal is that these arguments are capable of reuse in a wide variety of applications, easing the burden of security evaluations.

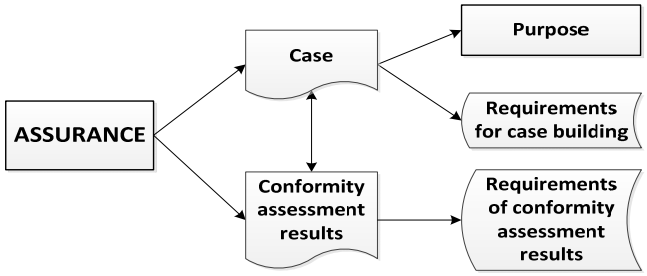

Figure 3. Refinement of assurance definition concept

The future work is concerned to improve of proposed security assurance case formalization technique ASAC. We also plan to develop tool support for described methodology. In particular, we wish to explore how: to build ASACs more effectively and provide rigorous decision-making procedure for building ASACs using subjective logic. We have starting developing of ASACs in DRAKON language for each class of CC to obtain full coverage and reduce time and cost of expertise.

Keywords: information security assurance, cyber security, advance security assurance case, ASAC, DRAKON

REFERENCES

1 ISO/IEC 15408-1:2009, Informational technology – Security techniques – Evaluation criteria for IT security, Part 1: Introduction and general model (2009)

2 ISO/IEC 15408-3:2008, Informational technology – Security techniques – Evaluation criteria for IT security, Part 3: Security assurance requirement (2008)

3 ISO/IEC 18045:2008, Informational technology – Security techniques – Methodology for IT security evaluation (2008)

4 Potii, O., Komin, D., Rebriy, I.: Method of Assurance Requirements Evaluation. In: Kharchenko, V., Tagarev, T. (eds.) Kharkiv, National Aerospace University n. a. N. E. Zhukovsky "KhAI", vol.1, pp. 123–132 (2011)

5 Cyra, L., Gorski, J.: SCF – A Framework Supporting Achieving and Assessing Conformity with Standards. Special Issue: Secure Semantic Web. 33(1), 80-95 (2011)

6 Williams, J. R., George F. J.: A Framework for Reasoning about Assurance, Document Number ATR 97043. Arca Systems, Inc. 23 April 1998

7 ISO/IEC TR 15443-1:2012, Information technology – Security techniques – Security assurance framework – Part 1: Introduction and concepts (2012)

8 Kelly, T. McDermid, T.: Safety Case Construction and Reuse Using Patterns. In: Daniel, T. (Ed.) Proceedings of the 16th International Conference on Computer Safety, Reliability and Security (SAFECOMP'97), pp. 55–69. Springer-Verlag, London, (1997)

9 Parondzhanov, V.: How to improve the work of your mind. Algorithms without programmers – it's very simple! Delo. Moscow (2001)

10 DRAKON official web-site, http://drakon-editor.sourceforge.net/ (access date: June 2015)

11 Potii O., Illiashenko, O., Komin D.: Advanced Security Assurance Case Based on ISO/IEC 15408. In: Theory and Engineering of Complex Systems and Dependability. Proceedings of the Tenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX, Brunów, Poland, pp 391–401 (2015)

SPEAKER BIOS

Allyson Hauptman was born in Pennsylvania, USA and attended the United States Military Academy for her undergraduate, where she double majored in International Law and Information Technology Systems. In May 2014 she graduated and commissioned as an Air Defense Artillery Officer. She is currently a master's student at Tallinn University of Technology, specializing in Digital Forensics. Her work experience includes positions at US Cyber Command, LTS Research Labs, and the NATO Cooperative Cyber Defense Centre of Excellence, where she has interned in both the Law & Policy and Education & Exercise branches. Her work on autonomous weapons under international law has been published in Military Law Review and presented at the 2014 Autonomous Weapon Conference in France. Her main research interests include military cyber operations, distinction in cyberspace, and cyberspace attribution techniques. She is married to a fellow Army officer, 2LT Mark Mihalik, who is stationed in Belgium. In her spare time she enjoys craft beer, playing guitar, and wandering Old Town with her dog, Tansy.

Andrea Melis is a research fellow at the University of Bologna. He got my Master at University of Bologna with a thesis about possibles privacy exploitation attacks on a public transport system; in 2013 he also obtained another Master at Polytech of Sophia-Antipolis with an Internship about data sanitization techniques in public transport operators dataset scenario. Andrea's job focuses on the security and privacy aspects of the Emilia-Romagna Regional Government project called "Mi Muovo" (I move). The goal of his work is to analyse the structure of the system architecture, with different kind of tests, try to discover security vulnerabilities and possible privacy violations; and propose and implement a solution for that issues. He likes every topic related to the security exploitation; penetration testing, vulnerability discovering and privacy risk assessment.

Benjamin Cosh is a fourth year honours student at the University of Adelaide studying Electrical and Electronic Engineering with a network security focus. He is currently engaged in a project with three others looking into the potential cyber security issues regarding IPv4/IPv6 hybrid sessions.

Birgy Lorenz is a PhD student from Tallinn University, Estonia (syllabus Information Society Technologies) and Digital Safety Lab. She is also eSafety trainer in Estonia in a program Safer Internet in Estonia EE SIC. Her activities include being part of developing National Curricula ICT syllabus, writing articles about e-safety, project management in TurvaLan project what has been awarded by: Microsoft (2009): Innovative Teacher Award and European Schoolnet (2010): 1st eLearning Award, in 'Internet Safety' category. Teacher of the year in Estonia (2011). Her current research is titled "Safety Strategies of the Teenager Internet User" so her interest is student-teacher online relationship, schools' policy on e-safety and students' online behaviour. She am also active in the Estonian InSafe project "Smart on the Net" developing materials and lecturing teacher's students about the topic. As she am a teacher and ICT development manager in Pelgulinna Gymnasium she is also interested in e-learning, mobile learning, innovation in leadership at schools and educational technology.

Carlos Ivan Vargas Alvarez del Castillo is a PhD student at Tallinn University in Estonia since 2014 and E-Government Specialist at RaulWalter LLC since beginnings of 2015. As PhD student he is focused in analyzing E-governance through a political science perspective under the University program "Government and Politics". In his professional life he works in a company specialized in digital identity and security solutions. Carlos is in charge of analyzing possible applications to developing countries. He has a multinational background in his academic life as he previously got a Master Degree in "Political Science" at Warsaw University, Poland on 2014. Before that he finished his Bachelor's studies in "Political Science and Public Administration" at the National Autonomous Mexican University on 2012. While studying his bachelor's degree he volunteer for several NGO's across Europe, from Italy to Poland mostly in social or political related activities. He worked and proposed an e-solution for kids' education

in the Ministry of Culture in Mexico. More recently he published two opinion articles one for "Migration-tothecentre" in Poland and the second one in the Estonian newspaper "Postimees".

Eneli Laurits is working as a counselor in the criminal policy department of the Ministry of Justice in Estonia. She is currently the leader of an IT project for developing an infosystem for prosecutors. Before this project, since 2006 until the beginning of the year 2015 she worked as a prosecutor in the Northern District of Prosecutor's Office. As a prosecutor she directed pre-trial criminal procedure and represented public prosecution in court in the crimes committed against children in internet (child pornogarphy and online grooming) and in all other crimes committed in internet (cybercrime). She enjoys giving lectures on cybercrime and digital evidence. She is giving lectures on the subject of criminal proceedings and digital evidence in Tartu University and in Estonian Academy of Security Sciences. She has held many in-service trainings for prosecutors and police officers on the subject of digital evidence and digital evidence collection in criminal proceedings. She is also studying in Tartu University in the department of Law to obtain a PhD with a field of interest is digital evidence. She has graduated from Estonian Information Technology College (2001).

Francisco Grajales's (Cisco's) passion lies in the implementation of disruptive technologies that drive meaningful and measurable change to organizations' vertical and horizontal stakeholders. As a Sauder S3i Fellow, Cisco's doctoral research evaluates the relationship between user behaviour, privacy, and the risk factors associated with the information that is shared on the PatientsLikeMe Social Networking Site and Patient-Powered Research Network. Cisco also collaborates and co-directs a number of ongoing international research projects. Cisco is trilingual and has served for over twelve years as a reserve medic with the Canadian Armed Forces Health Services. He has also worked for the REshape Centre at RadboudUMC, the World Bank, the World Health Organization, and Scotiabank. Cisco has also completed an interdisciplinary MS in Knowledge Management, a Bachelor's in Exercise Physiology with a specialization in Information Systems (risk assessment and algorithm scoring performance) and the Google Singularity University's Executive Program. After work Cisco can be found tinkering with new technologies, climbing the Niagara Escarpment or scuba diving in places where the sun negates the need for a wet suit.

Ignacio Cofone is a PhD student at Erasmus University Rotterdam in the framework of the European Doctorate in Law & Economics. Previously, he studied law at Austral University (2010), pursued the European Master in Law and Economics at the Universities of Bologna/ Hamburg/Aix-Marseille (2012), and worked as a legal advisor for the Government of the City of Buenos Aires and as an assistant professor at the University of Buenos Aires. His research focuses on the law & economics of privacy in Information Technology.

Ilze Borodkina is a PhD student at University of Tartu, Institute of Social studies. Her thesis is concerned with the privacy and private space in adolescents' online communication, focusing on content/ audience management as a dimension of identity construction process among the digital generation.

Jelena Milosevic is a PhD student at the Advanced Learning and Research Institute (ALaRI), Faculty of Informatics, Università della Svizzera italiana, Lugano, Switzerland. Jelena works on a design of a methodology for early detection of malware in mobile phones. She is especially interested in the application of the methodology on mobile devices running Android operation system. She obtained her Master and Bachelor degree in Electrical and Computer Engineering from University of Novi Sad, Serbia in 2011. Prior PhD studies, Jelena has worked as a DSP Audio embedded software engineer.

Karmen Turk works as an attorney-at-law at TRINITI Tallinn. She is also a lecturer of 'Intellectual Property in Informational Society' at University of Tartu, and has been lecturing on 'Human Rights and Technology' at the Tallinn University of Technology. Additionally, Karmen serves as an expert of the committee on Cross-border flow of Internet traffic and Internet Freedoms (MSI-INT committee) attached to the Council of Europe and as a coordinator of UN IGF Coalition on Freedom of Expression of media on the Internet. She was admitted to the Estonian Bar Association in 2009.

Lea Hricikova has finished her LLM studies on Law and Politics of International Security from the Vrije Universiteit in Amsterdam in 2013. Since then, Lea conducted research with focus on cybersecurity for different organisations: the Ministry of Defence in Bratislava, ECIPS in London and NATO CCD COE in Tallinn. In 2014, Lea has joined the European Agency for the operational management of large-scale IT

systems in the area of freedom security and justice (eu-LISA) as an intern and she settled in Tallinn as a consultant for Civitta on IT security policy. Her research is focused on comparing international cybersecurity cooperation regimes and on IT industry for intelligence and surveillance solutions. Lea underwent a professional course on security sector reform in 2014 by the European Security and Defence College and focuses further on adding the impact of IT security sector to the concept of security sector reform.

Mari-Liis Madisson is a PhD student in the Department of Semiotics, in Tartu University. Her main research fields include cultural semiotics, sociosemiotics and (hyper)media studies. Her main research interests are: identification-processes in online communities, political extremism, semiotic construction of conspiracy theories, participatory culture, everyday culture and cultural memory. She has published articles in various interdisciplinary journals including: *Semiotica: Journal of the International Association for Semiotic Studies, National Identities and Lexia.*

Markus Kont is a server administrator with 4 years of experience with managing production systems. While currently living in Tallinn, he is originally from a small town of Kose-Uuemõisa, where he grew up near to his grandparents farm. After getting the first computer at age 11, he familiarized himself with its components within a year, after which followed a youth of constant tinkering. Therefore, it was an easy choice to enter Estonian IT College after graduating from secondary school. There he was learning system administration and, after taking a year off due to mandatory military service, eventually got an internship in Spin TEK AS. There he took an interest in infrastructure architecture, replacing the backup solution (though he is still not happy with it), and wrote a thesis on the implementation. While numerous other systems have been built or replaced, he has been especially interested in monitoring solutions. Particularly log management. Being directly responsible for the well-being of systems, he immediately applied to Cyber Security master program, which he graduated in 2014 just 0.01 points short of cum laude. He now spends 50 percent of his working time in NATO CCD COE as a technology branch researcher.

Meredydd Williams is a PhD student in the Cyber Security Centre at the University of Oxford. He holds previous degrees from Aberystwyth and the University of Cambridge, specialising in Computer Science on both occasions. Currently Meredydd conducts research through an EPSRC scholarship in the intersection between cybersecurity and society. In particular, he is studying the public perception of security, the transformational effect of social media, and how groups interact and mobilise within the online world.

Mikk Raud, a native Estonian, is a final year student at the University of Hong Kong, where he is obtaining a Bachelor's degree in Government & Laws. Mr Raud has spent the last six months in Beijing, China, where prior to starting an exchange semester in Tsinghua University, he completed an internship at the Estonian Embassy, observing China's political developments with the focus on cyberspace. Mr Raud's interest toward cyber affairs was sparked when participating in the International Conference on Cyber Conflict (CyCon) in Tallinn last year and realizing how much intriguing unanswered questions this field poses. The paper Mr Raud will be presenting at the Interdisciplinary Cyber Research workshop was initiated in cooperation with the NATO Cooperative Cyber Defence Centre of Excellence. His previous experience further includes internships in the Ministry of Foreign Affairs of Estonia and in the Atlantic Treaty Association headquarters in Brussels. Mr Raud is a reserve officer candidate in the Antiaircraft Battalion of the Estonian Defence Forces. After finishing his Bachelor's degree in summer 2016, Mr Raud hopes to gain professional experience in international security affairs before starting graduate studies.

Oleg Illiashenko was born in Ukraine, 1989. Oleg obtained BSc degree in Computer Engineering (2010) and MSc degree in Computer Engineering (2012) in National Aerospace University "KhAI" and also Sp.Ed. in Information Security (2013) in Kharkiv National University of Radioelectronics "KNURE". Since 2011 Oleg holds a position of Assistant lecturer of computer systems and networks department at National Aerospace University "KhAI", teaching hardware-oriented courses for English-speaking students. Oleg is an author and co-author of more than 20 scientific works (including papers, 2 joint monographs) that are devoted to reliability, safety and security assessment and assurance of complex systems of critical applications. Currently he is doing PhD thesis on the topic «Methods of evaluation and choice of protection means for information security in PLC-based computer systems». In National Aerospace University Oleg manage TEMPUS-financed projects: GREENCO, SEREIN, CABRIOLET. Oleg is information administrator of International conference DESSERT. Research interests: safety and se-

curity assessment and assurance of critical FPGA – based embedded systems, regulatory aspects of critical I&C systems, techniques and tools for safety and security assessment, FPGA safety and security. My mission statement is to influence the world in sense of its harmony and binding together both empirical and spiritual ways of discovering the Universe.

Robert Krimmer was in 2014 elected as Full Professor of e-Governance within Ragnar Nurkse School of Innovation and Governance at the Faculty of Social Science, in Tallinn University of Technology, Estonia. He is focusing on electronic democracy, the transformation of the public sector, and all issues further developing a digital society. Associate Editor of the international scientific journal Government Information Quarterly (GIQ). Teaching on e-Governance, Open Data and Government, e-Democracy, e-Voting as well as End-User Management Information Systems at Tallinn University of Technology, University of Applied Sciences Hagenberg, Danube University Krems, and WU Vienna University of Economics and Business. Mentor of more than twenty graduation theses. Author and/or editor of ten books/special issues of scientific journals. Author of some 80 international scientific articles. He has been cited some 600 times with an Hirsch index of 12 according to Google Scholar. Prior to returning to academia, he served as Senior Adviser on New Voting Technologies in the Election Department of the Organization for Security and Co-operation in Europe's Office for Democratic Institutions and Human Rights (OSCE/ODIHR) in Warsaw. His role was to coordinate and support election-related activities, where new technologies were used in elections, and contribute to developing the methodology in this respect. He edited the 2013 OSCE/ODIHR Handbook on Methodology for Observation of Electronic Voting.

Sara Isabel González Álvarez received her B.S. degree and holds a Professional Master in Security Technologies from the University of León. She is currently studying for a Master Degree in Cybernetics Research at the same university and simultaneously works for the Research Institute of Applied Sciences in Cybersecurity of the University of León, where she is focused on the topic of security issues of Software-Defined Networking.

Tiia Sõmer is an early stage researcher at Tallinn University of Technology. Her research focuses on cyber crime and cyber forensics, leading TUT work on the EU E-CRIME project. E-CRIME is a three-year European Union project, researching the economic aspects of cyber crime. In addition to research, she has undertaken teaching in preparation of students for cyber-defence international policy-level competitions. Before starting academic career, she has worked for more than twenty years in the Estonian defence forces, filling various positions at different levels. This work included teaching at staff college level as well as working in diplomatic positions at national, NATO and EU levels. Her Master thesis concentrated on using gamification and serious games in teaching cyber security in high schools in Estonia. The thesis was entitled "Educational Computer Game for Cyber Security: a Game Concept".

Yevheniia Broshevan was born in Izmail, Ukraine, 1995. She is bachelor student of Information and Communication Systems Security department and head of Security Team in Student Laboratory of Mobile and Wireless Technologies at National Aerospace University "KhAI". Together with other lab members, Yevheniia Broshevan took part in "IT-Eureka Ukraine" (innovative projects contest which is searching for new ideas and solutions) with project "Smart University", where she was a business adviser and cyber security analyst. She is developing cybersecurity courses for MSc students, project TEMPUS SEREIN. She organizes different security meetings to encourage fellow students to participate in different activities. She is also leading the group of foreign students helping them to improve their cyber knowledge and skills. Also she participated at the International school-seminar with the support of TEMPUS-CABRIOLET (Chernivtsi city, July, 2014). She always interested in new technologies and future progress. Research interests: IT Security Management, e-government, cryptocurrency, blockchain-based apps. She is also cryptocurrency researcher at Distributed Lab and Hacker High School interpreter and event manager at HackUp. The recent achievement is organizing of international FinTech conference BIP001.


LOADING 100%
WORLD
-EUROPE
-AMERICA
-ASIA
-AFRICA
BUSINESS