ÓBUDA UNIVERSITY BUDAPEST

DONÁT BÁNKI FACULTY OF MECHANICAL AND SAFETY ENGINEERING

and

UNIVERSITY OF ECONOMICS IN BRATISLAVA

FACULTY OF ECONOMIC INFORMATICS

Department of Applied Informatics

REVIEWED PROCEEDINGS

Eighth International Scientific Web-conference of Scientists and PhD. students or candidates

„Trends and Innovations in E-business, Education and Security "

April 28, 2020

Óbuda University Budapest

TIEES 2020

Trends and Innovations in E-business, Education and Security

Eighth International Scientific Web-conference of Scientists and PhD. students or candidates

Editors: Rajnai Zoltán – Schmidt Peter - Jurík Pavol

Publisher : Óbuda University, Budapest, Hungary

Donát Bánki Faculty of Mechanical and Safety Engineering

ISBN: **978-963-449-206-1**

Date: April 28, 2020

REVIEWED PROCEEDINGS

Eighth International Scientific Webconference of Scientists and PhD. students or candidates

„Trends and Innovations in E- business, Education and security "

Held under patronage

of dean of Donát Bánki Faculty of Mechanical and Safety Engineering

prof. Dr. Zoltán Rajnai,

and of dean of Faculty of Economics Informatics

prof. Ing. Ivan Brezina, CSc.

INTERNATIONAL SCIENTIFIC COMMITTEE

REVIEWERS

Erzsébet Ancza

Igor Bandurič

Petr Doucek

Vladimir Galyaev

Veronika Horniaková

Pavol Jurík

Silvia Komara

Tibor Kovács

Jaroslav Kultan

Martin Mišút

Nurasil Kerimbaev

Anna Ondrejková

Jan Pittner

Peter Procházka

Eva Rakovská

Meruert Serik

Peter Schmidt

Jozef Stašák

Lajos Szabó

Endre Szűcs

Vladimír Zuev

ORGANIZING COMMITTEE

Peter Schmidt

Tibor Kovács

Jaroslav Kultan

Endre Szűcs

Pavol Jurík

EDITORS

Zoltán Rajnai

Peter Schmidt

Pavol Jurík

Table of Contents

FOREWORD 8

THE OBSTACLES OF AUTONOMOUS CARS BEFORE TAKING THE WHEEL IN THE FUTURE 9

Huu Phuoc Dai Nguyen, Zoltán Rajnai

ANALYSIS OF THE PROBLEM OF CONFORMITY OF THE PLANNED SPECIALTY AND SATISFACTION OF THE ACQUIRED PROFESSION 17

Andrey Rybalchenko, Gulmira Abildinova

METHODICAL PRINCIPLES AND STRUCTURE OF FORMATION OF LABORATORY ROCK SAMPLES DATA BASE 24

Svetlana Stroganova, Natalia Teodorovich

THE OPTIMAL CAPITAL STRUCTURE FOR BIOTECHNOLOGY STARTUPS 32

Mária Szivósová

IMPROVING THE QUALITY OF EDUCATION OF COMPUTER SCIENCE TEACHERS THROUGH THE KAIZEN PHILOSOPHY 42

Riza Akhitova, Aitugan Alzhanov, Igor Vostroknutov

SUBJECT-LANGUAGE INTEGRATED LEARNING AS THE BASIS FOR PREPARING FUTURE COMPUTER SCIENCE TEACHERS 50

Saniya Nariman, Aitugan Alzhanov, Igor Vostroknutov

INDIVIDUAL OR GROUP PROJECT ASSIGNMENT IN BUSINESS PROCESS MODELLING AND SOFTWARE ENGINEERING COURSES? 56

Martin Misut, Maria Misutova

ANALYSIS OF STATIC AND DYNAMIC PARAMETERS OF PLAYERS IN CYBERSPACE 65

Zsolt Bederna, Zoltan Rajnai

COMPOSITION DIAGRAM OF A COMPLEX PROCESS: A CONTRIBUTION TO BUSINESS PROCESS MODELLING 81

Pavol Jurík, Peter Schmidt

THE IMPACT OF DIGITAL TECHNOLOGY ON THE ECONOMICS OF CONSTRUCTION 93

Svetlana Kolobova , Anastasiya Magina

FINDING A MODULAR STRUCTURE OF THE KUKA INDUSTRIAL WELDING ROBOT MAIN CONTROL PROGRAM NEEDED FOR ITS EFFECTIVE TESTING 101

Igor Košťál

MODERN APPROACHES OF CLIENT-SERVER APPLICATIONS DEVELOPMENT 109

Meiramgul Mukhambetova

BIOMETRIC SYSTEMS AND UNCERTAINTY: A GENERAL APPROACH 115

Lourdes Ruiz S.

ANALYSIS OF ATTEMPTS TO PENETRATE INFORMATION SYSTEMS OVER THE INTERNET 122

Pavol Sojka

CYBER STRATEGY AND FRAMEWORK OF INTERNATIONAL ORGANIZATIONS 134

Eva Beke, Zoltan Rajnai

DESIGN A PROTECTED ROOM FROM INFORMATION SECURITY ASPECT, A PERSONAL APPROACH 145

Gábor Bréda

ASSESSING RISKS IN MOBILE DEVICES BY USING FMEA 153

Esmeralda Kadena

PASSWORD SELECTING HABITS 164

Esmeralda Kadena

VULNERABILITIES, IDENTIFICATION AND DETECTION OF UNMANNED AERIAL VEHICLES 177

Attila Máté Kovács, Zoltán Rajnai

WHICH ONE OF US IS THE ‘PHISHERMAN’ AND WHICH ONE IS THE TROUT? 184

Tamás Kun

LINKS AND VULNERABILITIES OF CYBER-PHYSICAL SYSTEMS - TWO APPROACHES' CONTEXT AND RELEVANCE: SPAEVI AND SCYPH 193

Zoltán Rajnai, Attila Máté Kovács

A SENSE OF SECURITY AND SECURITY AWARENESS 199

Lajos Szabó

OVERVIEW OF THE INTERNET OF THINGS SECURITY RELATED THREATS AND POSSIBLE MITIGATIONS 209

Gellért Miklós

THE USAGE OF THE OPEN-SOURCE PLATFORM ARDUINO TO TEACH IOT 218

Peter Procházka

Foreword

You are currently reading the reviewed proceedings of the Eighth International Scientific Web Conference of Scientists and PhDs. students or candidates entitled Trends and Innovations in E-Business, Education and Security. The conference is organized alternately by the Donát Bánki Faculty of Mechanical and Safety Engineering, Óbuda University, Budapest and the Faculty of Economic Informatics of the University of Economics in Bratislava. This conference has become an important point for the exchange of research results between researchers and doctoral students.

At the eighth year of the web conference, a total of 24 articles from 32 authors from 4 countries were presented. The articles were from 5 thematic areas: applied informatics in business, applied informatics education, information science and technology, security and data protection and intelligent technologies and IoT.

The eighth webconference in a row is a major achievement in recent developments in the field of webconferencing. The coronavirus pandemic confirmed the legitimacy of web conferencing. The web conference is therefore an interesting opportunity to attend an international meeting at reduced cost, and especially for young researchers to improve their skills in presenting research papers in many of them in a foreign language.

The conference is over, but we have just begun to think about the next and how to improve the recognized weaknesses and maintain the strengths of future participants.

In conclusion, we would like to thank the participants for their interesting contributions and wish you a pleasant reading. We hope you find inspiration here for further research and participation in the next video conference here.

On behalf of the scientific and organizational committees

prof. Dr. Zoltán Rajnai

dean of

Donát Bánki Faculty of Mechanical
and Safety Engineering

THE OBSTACLES OF AUTONOMOUS CARS BEFORE TAKING THE WHEEL IN THE FUTURE

Huu Phuoc Dai Nguyen[1], Zoltán Rajnai[2]

Abstract

Like a vision in the future of transportation, autonomous vehicles (AVs) are becoming a familiar aspect to debate from different perspectives which consist of design, social issues, security and safety, and so on. Besides, autonomous vehicles 'evolution creates a new era in replacing the human being behind the steering wheel by sensors, artificial intelligence, and auto robotics. Moreover, it is also a novel technology which can reduce fatal vehicle accidents and deaths. However, it also brings several drawbacks for customers. In this article, the authors described the general view of autonomous challenges before it can apply in public transportation. Furthermore, it enhances the awareness of the manufacturers to focus on figuring out solutions to guarantee the safety and security for AVs.

Keywords

autonomous car, challenges, future, safety, security, V2V.

1 Introduction

A road traffic crash is one of the reasons which leads to human being's life shorter. Regarding the report of WHO in 2018, there were nearly 1.35 million deaths because of traffic accidents every year (W.H.O., 2018). In addition, there were more than 90% of traffic participant 's deaths happened in low and developing nations due to lower backgrounds or perception. Hence, AVs' evolution is the main purpose to enhance road safety and reduce the social burden or family sorrows from car crashes. Furthermore, with autonomous vehicle's generation, several researchers thought that AVs will bring the independent ability for drivers; diminish the stress and boring of driving; reduce traffic congestion, accident and the like (Johnson & Walker, 2016),(Keeney, 2017),(Arbib & Seba, 2017). However, this new technology also has several challenges for users such as security problems, reality issues, human factors, etc. In this paper, the authors showed a general overview of the autonomous vehicles' obstacles before they can operate in order to find the solutions for them in the near future.

2 Theoretical background

2.1 Autonomous vehicle

Autonomous vehicles, autonomous cars, or driverless cars refer to cars or vehicles which are possible to drive automatically without driver's support. In another way, autonomous cars also called self-driving vehicles based on artificial intelligence and robotics technology (Litman, 2014). Moreover, regarding National Highway Traffic Safety Administration (NHTSA) and Dr. Chandrika Nath - Parliamentary Office of Science and Technology, they divided autonomous cars into five major kinds of automation (Anderson et al., 2016),(Gillian, 2014), (Diels & Bos,

[1] Doctoral School on Safety and Security Science, Budapest, Hungary, phuoc.daitt@bgk.uni-obuda.hu,
[2] Doctoral School on Safety and Security Science, Budapest, Hungary, rajnai.zoltan@bgk.uni-obuda.hu

2016); for example, driver only, driver assistance, partial autonomy, high autonomy, and full autonomy.

a. *Driver only*: the driver has full controls of a vehicle but there are some automated systems e.g. Cruise control, electronic stability control, anti-lock brakes
b. *Driver assistance:* a human being can control some functions such as adaptive cruise control and parking assistant but the steering or/and acceleration automatically operates.
c. *Partial autonomy:* the driver doesn't need to control the vehicle, but in some cases, it requires to take back the control (adaptive cruise control with lane-keeping, traffic jam assistance)
d. High autonomy: this type of vehicle can operate itself for a whole trip and driver can be able to get back control in some emergency cases with warning signals.
e. *Full autonomy:* the vehicle can be self-driving without any assistant from a human being for the entire journey even potentially without a driver inside the car.

2.2 Vehicle to vehicle communication (V2V communication)

Vehicular ad hoc networks (VANETs) is related to mobile ad hoc network (MANETs) communication for sharing data among the vehicles. In another hand, VANETs is also the main factor of the Intelligent Transportation System (ITS) which refers to a network between vehicle to vehicle (V2V) and vehicle to roadside units (RSU). VANET has two categories: V2V communication and Vehicle to Infrastructure (V2I) communication (Kim & Lee, 2014). Vehicle to Vehicle (V2V) communication is a network for vehicles connect each other. This technology was first appeared in 2005 by General Motors (Shah & Parentela, 2015). Moreover, regarding sharing information between one vehicle and the others, V2V is also a collision avoidance method in order to warn the drivers about the dangerous cases (NHTSA, 2016). For example, vehicles with the support of an automated emergency braking function inside, it can calculate the safe zone between two cars to prevent potential accidents and activate the brake system automatically. Indeed, Huang and Lin (Huang & Lin, 2011) proposed an early collision warning algorithm (ECWA) and Global Positioning System (GPS) to alert the drivers before an accident. V2V communication uses several technologies to communicate between the vehicles together and RSU such as: Dedicated Short-Range Communication Standard (DSRC) protocol (Iyer et al., 2008) (Watson & Maple, 2017), broadcasting messages (Iyer et al., 2008), Bluetooth, ZigBee, Radio, Cellular, GPS, Wi-Fi and Ultra-Wide Band (Khairnar et al., 2014) to exchange the information (location, speed, and acceleration with neighbor vehicle). Furthermore, V2V communication technology-supported several wireless-based features in the cars which could improve the safety for traffic, roadway efficiency and driver convenience (Jurgen, 2012). Due to the benefits of this technology, it can reduce vehicle accidents, the number of injuries and make a better life.

3 Security issues

AVs operate based on sensors and network; therefore, there are not only several security issues related to the network system, physical electrical parts of vehicle such as controller area network (CAN), electronic control unit (ECUs) and the like (Nguyen & Rajnai, 2018) but also several security problems with camera and LiDAR.

3.1 Camera attack

A camera is an indispensable device to capture the world for autonomous vehicles (Petit et al., 2015). This device uses several techniques such as lane detection (Bai & Wang, 2010), horizon/vanishing point (Kong et al., 2013), object detection and tracking (vehicles and

pedestrians) (Keller et al., 2011), headlight detection (Zhang et al., 2012), and so on in order to help driverless cars to identify the objects on the street. However, the hackers can exploit the camera to blind the camera incompletely or completely to emit light into the camera for hiding the objects in front of the vehicles (Petit et al., 2015). This can cause car crashes and lead to big injuries for passengers, drivers or even deaths. This is one of the serious problems towards AVs.

3.2 LiDAR attack

In order to let AVs work effectively, there are many fundamental components like camera, sensors, Radio Detection and Ranging (Radar), radiofrequency, ultrasound, etc. In addition, there is an essential sensor in AV's observation – called Light Imaging Detection and Ranging (LiDAR) by using light reflected from the surface of the road. This sensor emits the light vibration and measures its time reflection to detect the objects in any weather condition. Nonetheless, there are many types of attacks like an attack- replay, jamming, and spoofing attacks by the hackers to make noise, fake echoes, or fake objects; as a consequence, it can make confusion for this sensor and problem for collision avoidance system.

3.3 DoS and DDoS Attack

AV's operation mainly based on VANET network via wireless communication. In addition, AVs not only communicate with other vehicles but also connect with the infrastructure (V2I); therefore, the hackers can use many methods to attack this network such as jamming the channel or denying the services in the network between V2V itself and V2V to V2I communication. For example, (Hasbullah et al., 2010), (Raghuwanshi & Jain, 2015), they showed that there are three main categories of DoS and DDoS attacks in VANET system; for example, the communication channel jamming, network overloading, and packets dropping (Blum & Eskandarian, 2004), (Nguyen & Rajnai, 2018). These attacks can cause a huge damage not only for drivers but also passengers and pedestrians on the road when the attackers hit the target.

4 Reality challenges

The obstacles of AVs not only come from the direct attacks but also originate from indirect ways such as weather, road condition, and map. These factors may influence on decision making of AVs to choose the best option on the road and ensure the safety of passengers or even pedestrians and vehicles.

4.1 Weather conditions

Mother Nature plays an essential role in transportation, especially not only conventional cars but also autonomous vehicles. Traditional vehicles with the control of drivers also have problems with the weather conditions such as heavy rain, storm, snow, fog, and sleet because they reduce driver's vision before vehicle crashes. While driverless cars rely on GPS, sensors, cameras, lasers, LiDAR, and Radar technology; they can have big challenges to operate under bad weather conditions. For example, cameras can't detect the objects or pedestrians in fog and heavy snow. Moreover, LiDAR lasers may careen during raindrops and snowflakes (Stock, 2018). In addition, GPS connections may be slow or disconnected; therefore, it can lead to AVs can't find the best way to get destination or can cause several hazardous cases for pedestrians and passengers.

4.2 Road conditions

Road conditions are also a factor which may directly influence to autonomous vehicles due to its unpredictable and various surfaces from one place to another place (Gupta, 2017). In several cases, the roads are smooth and full marked broad highways but in other cases, they have lots of potholes and obstacles where the marks or signals for direction are not clear enough. On the other hand, in the developing countries, road conditions are not good enough such as undefined lanes, many means of vehicles in the same lanes (motorbikes, cars, and trucks), lack of marked or signals on the road, road work and so on. These influence directly to AVs' decision making and their responses before the crash. Hence, road conditions are the big challenges for driverless vehicles to ensure the safety of passengers and pedestrians on the road.

4.3 Maps creating and maintaining's difficulty

AVs require the map as a reference before it uses their sensors to observe the obstacles on the road, other vehicles, pedestrians, and the like to identify the journey; however, in some cases, there are new objects, unexpected marks or construction which aren't on the map (Dass, 2018). Moreover, creating or maintaining detailed maps and updating process for all over the world frequently are difficult missions and take long time process; therefore, navigation on AVs can't get up to date the information for the map; hence, this leads AVs to get difficult to operate on the road.

5 Human factors

In parallel with security issues and reality challenges, the human being's problems are the main challenges towards AVs such as human perception, responsibility of accidents, law, and trust. These obstacles may lead the users take them into account before operating AVs on the road in a common way.

5.1 Human perception

The main problem origins from two things such as the security for a human being, the social and ethical problems. For more than one century, people have been familiar to the conventional cars; therefore, it is quite difficult to adapt the different from other new things while autonomous cars or self-driving cars can cause the injury of passengers or even death. Besides, it also depends on the driver's habit or interests in taking the steering wheel; as a result, it is quite difficult to alter people's perception to begin a journey with autonomous cars.

5.2 Responsibility of accidents

The most essential thing for autonomous vehicles is the responsibility of accidents. When an accident occurred and it caused by an autonomous vehicle, the most difficult question for the participants on the road is that whose responsibility for that is? In the conventional vehicles, the human being behind the steering wheel may be liable for the accidents; however, autonomous vehicles are operated by software which will drive the car and give all the important decisions during the journey.

5.3 Law

Autonomous vehicles currently face the big problem is legal law for implementing them in social human being's life. There are four major problems in law, as follow (Zhao et al., 2018), [Table 1]:

Tab. 1: Law problems for applying autonomous vehicles.

Types	Definition
License problem	No country establishes rules for driverless cars, only California or some American States gives a test permit
Driving regulations	It is defined based on human requirements
Responsibility	It is hard to define the responsibility belong to whom?
Information security	Mapping information related to security in a country or region.

Many countries in over the world are running on a race to design, produce, or test the safety of AVs; however, until now there is no country established rules for them. This leads people hesitate to use them as the conventional cars. In addition, this problem requires researchers, governments, companies, even citizens need to work on that more time to find the solutions for it.

5.4 Trust

Currently, there are some issues related to human being‘s trust in autonomous cars such as during the production process (trust requires for both hardware and software components when vehicles assembled), the operation process (self-driving car based on data sources e.g. GPS, map data, external devices, and other vehicles to decide how to get the destination) but how people believe on these data sources (Holstein et al., 2018)? Furthermore, hardware, software components, sensors, and cameras belong to different factories; as a result, trustworthy is the most important question when the autonomous vehicles operate.

6 Conclusion

Autonomous cars have been known as a means of transportation in the near future. Moreover, self-driving cars offer more benefits for the users than they expected; however, it is the right time to explore the security problems and challenge’s factors which impact directly to the operation of autonomous vehicles before they run on the road. This article emphasized several security issues which could affect to the effectiveness of autonomous cars on the street; for example, some attacks from hardware on autonomous cars (camera attack, LiDAR attack, DoS and DDoS attack). Besides, the author showed that several reality challenges and human factors are also important factors before the autonomous vehicles are applied in over the world. Regarding the security issues, reality and human challenges, the authors believe that figuring out the solutions for them is an urgent mission for the following research in order to minimize the risks for autonomous cars before they operate.

Resources

Anderson, J., Kalra, N., Stanley, K., Sorensen, P., Samaras, C., & Oluwatola, O. (2016). *Self-Driving Vehicles Offer Potential Benefits, Policy Challenges for Lawmakers.* Retrieved April 05, 2020, from https://doi.org/10.7249/ RR443-2

Arbib, J., & Seba, T. (2017). *Rethinking Transportation 2020-2030*. RethinkX . Retrieved March 12, 2020. from ttps://static1.squarespace.com/static/585c3439be65942f022bbf9b/t /591a2e4be6f2e1c13df930c5/ 1494888038959/RethinkX+Report_051517.pdf

Bai, L., & Wang, Y. (2010). A sensor fusion framework using multiple particle filters for video-based navigation. *IEEE Transactions on Intelligent Transportation Systems*, *11*(2), 348–358. https://doi.org/10.1109/TITS.2010.2043431

Blum, J., & Eskandarian, A. (2004). The Threat of Intelligent Collisions. *IT Professional*, *6*(1), 24–29. https://doi.org/10.1109/MITP.2004.1265539

Dass, R. (2018, September 14). 5 Key Challenges faced by Self-driving cars. Retrieved March 05, 2020, from https://medium.com/@ritidass29/5-key-challenges-faced-by-self-driving-cars-ed04e969301e

Diels, C., & Bos, J. E. (2016). Self-driving carsickness. *Applied Ergonomics, 53*, 374-382. doi:10.1016/j.apergo.2015.09.009

Gillian, Y. (2014). Autonomous vehicles - Handing over control: Opportunities and risks for insurance. Retrieved June/July, 2020, from https://www.lloyds.com/~/media/lloyds/reports/-emerging-risk-reports/autonomous-vehicles-final.pdf

Gupta, A. (2017). *Five challenges in designing a fully autonomous system for driverless cars*. https://iiot-world.com/artificial-intelligence/five-challenges-in-designing-a-fully-autonomous-system-for-driverless-cars/

Hasbullah, H., Soomro, I. A., & Manan, J. A. (2010). Denial of Service (DOS) Attack and Its Possible Solution in VANET. Retrieved July 7, 2020, from https://pdfs.semanticscholar.org/4787/b92f4489496b539c7ffb4d9dcc9a92877b7e.pdf

Holstein, T., Dodig-Crnkovic, G., & Pelliccione, P. (2018). *Ethical and Social Aspects of Self-Driving Cars*. http://arxiv.org/abs/1802.04103

Huang, C., & Lin, S. (2011). An early collision warning algorithm for vehicles based on V2V communication. *International Journal of Communication Systems, 25*(6), 779-795. doi:10.1002/dac.1259

Iyer, A., Kherani, A., Rao, A., & Karnik, A. (2008). Secure V2V communications: Performance impact of computational overheads. *Proceedings - IEEE INFOCOM*, *May 2008*. https://doi.org/10.1109/INFOCOM.2008.4544660

Johnson, C., & Walker, J. (2016). Peak car ownership report. *Rocky Mountain Institute*. https://www.rmi.org/insights/reports/peak-car-ownership-report/

Keeney, T. (2017). *Mobility-As-a-Service : Why Self-Driving Cars*. http://research.ark-invest.com/hubfs/1_Download_Files_ARK-Invest/White_Papers/Self-Driving-Cars_ARK-Invest-WP.pdf

Keller, C. G., Enzweiler, M., Rohrbach, M., Llorca, D. F., Schnörr, C., & Gavrila, D. M. (2011). The benefits of dense stereo for pedestrian detection. *IEEE Transactions on Intelligent Transportation Systems*, *12*(4), 1096–1106.

Khairnar, M., Vaishali, D., & Pradhan, D. (2014). V2V communication survey wireless

technology. *ArXiv Preprint ArXiv:1403.3993*, *3*(1), 370–373. http://arxiv.org/abs/1403.3993.

Kim, S., & Lee, I. (2014). A Secure and Efficient Vehicle-to-Vehicle Communication Scheme using Bloom Filter in VANETs. *International Journal of Security and Its Applications, 8*(2), 9-24. doi:10.14257/ijsia.2014.8.2.02

Kong, H., Akakin, H. C., & Sarma, S. E. (2013). A generalized laplacian of gaussian filter for blob detection and its applications. *IEEE Transactions on Cybernetics*, *43*(6), 1719–1733. https://doi.org/10.1109/TSMCB.2012.2228639.

Litman, T. (2014). Autonomous Vehicle Implementation Predictions: Implications for Transport Planning. *Transportation Research Board Annual Meeting*, *2014*, 36–42. https://doi.org/10.1613/jair.301.

Nguyen, H. P. D., & Rajnai, Z. (2018). The Current Security Challenges of Vehicle Communication in the Future Transportation System. *SISY 2018 - IEEE 16th International Symposium on Intelligent Systems and Informatics, Proceedings*, 161–165. https://doi.org/10.1109/SISY.2018.8524773.

Petit, J., Stottelaar, B., Feiri, M., & Kargl, F. (2015). Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR. *Blackhat.Com*, 1–13. https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp1.pdf

Raghuwanshi, V., & Jain, S. (2015). Denial of Service Attack in VANET: A Survey. *International Journal of Engineering Trends and Technology*, *28*(1), 15–20. http://www.ijettjournal.org

Jurgen, R. K. (2012). *V2V/V2I communications for improved road safety and efficiency*. Warrendale: SAE International. doi:doi.org/10.4271/PT-154

Shah, K., & Parentela, E. M. (2015). A Case Study on Potential Benefits of V2V Communication Technology on Freeway Safety. Retrieved July/August, 2020, from https://www.westernite.org/annualmeetings/15_Las_Vegas/Papers/7C-Shah.pdf.

Stock, K. (2018). *Self-Driving Cars Can Handle Neither Rain nor Sleet nor Snow*. https://www.bloomberg.com/news/articles/2018-09-17/self-driving-cars-still-can-t-handle-bad-weather.

U.S. Department Of Transportation, NHTSA. (2016). *FMVSS No. 150 Vehicle-To-Vehicle Communication Technology For Light Vehicles.* Office of Regulatory Analysis and Evaluation National Center for Statistics and Analysis. Retrieved April 02, 2020, from https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/ v2v_pria_12-12-16_clean.pdf.

Watson, T., & Maple, C. (2017). *Cyber Security Standards and Issues in V2X Communications 1 Ivan Ivanov, 2 Sang-Woo*. *9*, 2–7. http://www.worldresearchlibrary.org/up_proc/pdf/722-14918904992-7.pdf

W.H.O. (2018). Road traffic injuries. Retrieved June/July, 2020, from https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries

Zhang, W., Wu, Q. M. J., Wang, G., & You, X. (2012). Tracking and pairing vehicle headlight in night scenes. *IEEE Transactions on Intelligent Transportation Systems*, *13*(1), 140–153. https://doi.org/10.1109/TITS.2011.2165338

Zhao, J., Liang, B., & Chen, Q. (2018). The key technology toward the self-driving car. *International Journal of Intelligent Unmanned Systems*, *6*(1), 2–20. https://doi.org/10.1108/IJIUS-08-2017-0008

ANALYSIS OF THE PROBLEM OF CONFORMITY OF THE PLANNED SPECIALTY AND SATISFACTION OF THE ACQUIRED PROFESSION

Andrey Rybalchenko[3], Gulmira Abildinova [4]

Abstract
Expectations of future employment is a source of considerable stress for students and active professionals alike. We have conducted a survey of five hundred professionals employed in the field of innovative technologies. It demonstrates that there are statistically significant differences between planned and current specialties. Furthermore, the poll suggests that the problem can be solved by providing the students with the means to monitor their progress towards desired goals. We present such a framework - "Students' progress monitor" - a dedicated software designed to collect and analyse students' academic performance.

Keywords
Education, profession, innovative technologies, choice of specialty.

1 Introduction

According to the results of 2019, the Republic of Kazakhstan ranked 35th in the world in terms of education index and was one of the twenty countries that effectively solve the problems of employment. In the youth progress index, we rank 63rd out of 102 countries, and in the globa-l youth development index 61st out of 180 countries. However, the problem of choosing a future profession in our country is still significant, given that about 60% of graduates do not work in their respective study fields (Kazakhstan Today, 2018).

Many internal and external factors can influence the specialty choice (Kovalenko A.A., 2013):

- the level of knowledge in fields of STEM(science technology engineering and mathematics) (Du Preez , 2019);
- the theory of fitting a person to work postulates a personality trait, which is one of the most important factors that determine how a person will adapt to a particular work (Van Der Aar et al, 2019);
- the current state of affairs in the country (for example, popularity for IT), the wishes of parents, the influence of friends;
- the chosen higher education institution, the obtained scientific degree, whether education was obtained remotely or not (Tomsik, 2019).

All factors above can influence the decision to receive a specialty / profession at the end of school or higher education. The consequences of making the wrong choice can only be revealed years after getting a job (Kampkötter, 2018).

The change of profession is quite a laborious process, as it takes time to accumulate experience (Lem, 1964), acquire professional skills, and complete additional education. Thus, becoming a professional in any activity is a long process (Hannaway, 2019). According to a study conducted by Sberbank people that continually invest in their further education, earn 2.5 times more (Shafranov-Kutsev & Efimova, 2019). Various theories can help to understand the relationship between performance evaluations and job satisfaction, which in turn affects productivity (Gladwell, 2008).

[3] L.N. Gumilyov Eurasian National University, Faculty of Information Technology, Department of Informatics, Kazakhstan, Nur-Sultan, rybalchenkoas@gmail.com
[4] L.N. Gumilyov Eurasian National University, Faculty of Information Technology, Department of Informatics, Kazakhstan, Nur-Sultan, gulmira_2181@mail.ru

Our government research goal is to arrange and organize vocational guidance of schoolchildren, to adjust the vector of vocational guidance to towards the market needs. For this purpose, vocational guidance rooms are opened in secondary schools; forums and seminars are held jointly with the regional education department; a database is compiled about enterprises in the city and the region, about specialties in the labour market that are in high demand; systematic excursions for schoolchildren to enterprises; and a cycle of classroom hours and career counselling consultations are developed . The Ward's Human Capital Development Department developed a training manual "To Help a Graduate of the School" , which outlines an algorithm of actions for determining a future profession, and, together with Nazarbayev Intellectual School (NIS), prepared a collection of methodological resources on career guidance in the school "Successful Choice of a Profession" (NCE of the RK «Atameken», 2016).

There are also various other tests to determine the future profession (Jovaysha test, EA Klimov's method, career counselling J. Holland), which school students can use independently (Ravhuhali et al, 2019).

The problem remains in the incorrect definition of the future profession. Today, when choosing a profession, young people are not interested in what areas of the economy will develop in the future, and whether there will be a need for personnel. This led to an imbalance in the specialties, that is, many choose specialties that are not in demand in the economy.

As you can see, a fairly wide range of tools can help with the choice. Support is provided by the state and entrepreneurs are interested in the selection of qualified personnel. But, unfortunately, most graduates are not serious about choosing their profession (Potvin & Hasni, 2017).

Thus, the aim of our study is to demonstrate the necessity of applying student performance analysis.

The subject of our research is the analysis of the dependence of the planned specialty on the acquired profession and its' satisfaction.

2 Research and analysis

Our analysis is based on the results of a survey among employed people aged 24 to 38 years with higher education, employed in various positions in the IT field: programmers, IT analysts, database administrators, teachers, project managers.

The questionnaire included the following questions:

- Performance in school (in the context of subjects and types of tasks);
- The specialization of the school (exact sciences, humanities, art, etc.);
- Hobbies;
- Personal qualities;
- Special achievements in school years;
- knowledge of languages;
- Plans for higher education;
- Higher education (country, specialty, etc.);
- The average GPA at the university;
- Satisfaction with the choice of university;
- The presence of work experience while studying at the university;
- Further plans for labor activity;
- Current profession;
- Satisfaction with the current profession;
- Further plans for professional activities.

Some questions allowed participants us to give an open answer, we used this for a broader analysis and collection of various characteristics. As a result, before proceeding to the analysis,

it was required to unify the obtained information. The data was entered into the dedicated program - "Monitoring the educational achievements of schoolchildren", that we have developed. Using the program, we have constructed the initial tables for further calculations using the Pirsen chi-square test method:

Tab.1: Dependence of the main direction in the school on satisfaction with current work in the field of IT (source:author)

Selected direction at school	The number of participants satisfied with the current job	Neutral attitude to work	The number of participants dissatisfied with the current work	Total
Exact sciences	21	4	4	29
Humanitarian sciences	7	5	1	13
Natural Sciences	5	2	0	7
Other	3	1	0	4
Total	36	12	4	53

Tab.2: Dependence of the chosen specialty upon graduation from satisfaction with current work in the IT field (source:author)

Selected specialty at school	The number of satisfied with the current job	Neutral attitude to work	The number of dissatisfied with the current work	Total
Programmer	9	2	2	13
Engineer	8	2	2	12
Medicine	1	1	1	3
Humanities	8	3	0	11
Arts	2	0	0	2
Other	8	4	0	12
Total	36	12	4	53

Tab.3: Dependence of plans after graduation with satisfaction with current work in the field of IT (source:author)

Plans after graduation	The number of participants satisfied with the current job	Neutral attitude to work	The number of participants dissatisfied with the current work	Total
IT sphere	10	2	1	13
Engineer	1	0	0	1
Any work	8	1	0	9
Education	1	0	0	1

Interpreter	0	1	0	1
No plans	10	6	0	16
Own business	3	1	1	5
Continuing education	3	2	1	6
Scientific activity	0	0	1	1
Total	36	13	4	53

We modified Tables 1 and 2 without loss of data to calculate the exact Fisher criterion.

Tab.4: Dependence of the main direction in the school on satisfaction with current work in the field of IT (according to the Fisher criterion) The indicators were reduced to Exact sciences and Other. (source:author)

Selected specialty at school	The number of satisfied with the current job	The number of dissatisfied with the current work	Total
Exact sciences	21	4	25
Other	15	1	16
Total	36	5	41

Tab.5: Dependence of plans after graduation with satisfaction with current work in the field of IT (according to the Fisher criterion). The "Programmer" is combined with the "Engineer" in the Technical Field, all the rest are added to the "Other"(source:author)

Plans after graduation	The number of satisfied with the current job	The number of dissatisfied with the current work	Total
Technical direction	17	4	21
Other	19	1	20
Total	36	5	41

Table 1 - The number of degrees of freedom is 6.

The value of the criterion $\chi 2$ is 4.730. The critical value of $\chi 2$ at a significance level $p < 0.05$ is 12.592. The relationship between factor and resultant traits is not statistically significant, the significance level is $p > 0.05$

Table 2 - The number of degrees of freedom is 10.

The value of the $\chi 2$ criterion is 8.012. The critical value of $\chi 2$ at a significance level $p < 0.05$ is 18.307. The relationship between factor and effective traits is not statistically significant, the significance level is $p > 0.05$

Table 3 - The number of degrees of freedom is 16

The value of the $\chi 2$ criterion is 22.560 The critical value of $\chi 2$ at a significance level $p < 0.05$ is 26.296 The relationship between factor and resultant traits is not statistically significant, the significance level is $p > 0.05$

Table 4 - Fisher's exact test is 0.6317, p > 0.05
Criterion φ - 0 .145
Table 5 - Fisher's exact test is 0.34334, p > 0.05
Criterion φ - 0 .2 15

Tables No. 1, No. 2, No. 3 show three stages of training: the direction of school education, plans for graduation, plans after graduation and with each stage, fewer people planned to be IT specialists, but more than 90% of them satisfied that they have become them. Tables No. 4 and No. 5 reinforce our assumptions, showing that only 60% of the interviewed IT specialists studied exact sciences, and 50% planned to go into the technical field.

Based on these tables, we can conclude that the mismatch of plans at any stage of education (general, special or professional) with the current professional sphere does not affect the satisfaction with the profession.

Below is a summary table that shows how many people of those we interviewed who adhered to their plans from school to university, and how many of them are satisfied with their current work.

Tab.6: Dependence of people's satisfaction with their current work on their plans (source:author)

Planned profession at the time of graduation	Satisfied with current job	Difficult to answer	Dissatisfied with current job	Grand total
Doctor	1	1	0	2
Plans have changed	1	1	0	2
Humanities	8	3	0	11
Find a job by profession	1	0	0	1
Plans have changed	5	2	0	7
Continue education	2	1	0	3
Engineer	8	2	2	12
Find a job by profession	1	0	0	1
Plans have changed	7	2	2	11
Programmer	9	2	2	13
Find a job by profession	7	0	1	8
Plans have changed	1	2	0	3

Continue education	1	0	1	2
Other	8	4	0	12
Find a job by profession	1	1	0	2
Plans have changed	7	2	0	9
Continue education	0	1	0	1
Arts	2	0	0	2
Plans have changed	2	0	0	2
Grand total	36	12	4	52

About 15% of people adhered to their plans. About 70% are satisfied with the current result.

It turns out that 55% of people lost a part of their time when learning unnecessary skills and abilities to gain unnecessary knowledge. Our research demonstrates the need for student performance analysis, which in the future can be used to build individual learning models and predictive analysis.

3 Conclusions

Our research shows that the relation between the chosen specialty and satisfaction with the current profession in IT is insignificant. In other words, the specialists in the field of innovative technologies, regardless of their education and plans for the future profession, and satisfied with the current work in most cases

However, at the moment, education does not use an effective tool to help assess the performance and abilities of each student, which leads to many problems of a personal nature (dissatisfaction, depression) and general problems (low-quality specialists, low labor productivity).

Resources

Du Preez, M. (2018). The factors influencing Mathematics students to choose teaching as a career. *South African Journal of Education, 38*(2). doi:10.15700/saje.v38n2a1465

Gladwell, M. (2013). *Outliers: The story of success*. New York: Back Bay Books, Little, Brown and Company.

Hannaway, D. (2019). Mind the gaps: Professional perspectives of technology-based teaching and learning in the Foundation Phase. *South African Journal of Childhood Education, 9*(1). doi:10.4102/sajce.v9i1.674

Kampkötter, P. (2016). Performance appraisals and job satisfaction. *The International Journal of Human Resource Management, 28*(5), 750-774. doi:10.1080/09585192.2015.1109538

Kaukenova, S. (2013). Pri vybore professii molodezh ne interesuetsya perspektivnymi sferami ehkonomiki. Retrieved July 21, 2020, from https://www.zakon.kz/4560761-pri-vybore-professii-molodezh-ne.html

Kazakhstan Today, (2018, October 19). Kazakhstan nakhoditsya na 35m meste v mire po indeksu obrazovaniya. Retrieved July 21, 2020, from https://www.kt.kz/rus/education/kazahstan_nahoditsja_na_35m_meste_v_mire_po_indeksu_obrazovanija_1153664298.html

Kovalenko, A. (2013). Analiz faktorov, vliyayushchikh na vybor professii molodezhi: mezhdunarodnyi aspekt. Nauka i Sovremennost*, 26(1)*., 119-123.

Lem, S. (1964). *Summa technologiae*. Krakow: Wydawnictwo Literackie.

NCE of the Republic of Kazakhstan "ATAMEKEN", (2016, November 14). V pomoshch pravilnomu, osoznannomu vyboru budushchei professii. Retrieved July 21, 2020, from https://atameken.kz/ru/news/24694-v-pomosh-pravil-nomu-osoznannomu-vyboru-budushej-professii

Potvin, P., & Hasni, A. (2017). Encouraging Students with Different Profiles of Perceptions to Pursue Science by Choosing Appropriate Teaching Methods for Each Age Group. *Research in Science Education, 48*(6), 1339-1357. doi:10.1007/s11165-016-9605-z

Ravhuhali, F., Macdonald, Z., Mashau, T., Lavhelani, P., & Mutshaeni, H. (2019). Being first year B.Ed. Foundation phase student teachers at a university: Wrestling apprehension in and through a chosen career. *South African Journal of Higher Education, 33*(3). doi:10.20853/33-3-3005

Shafranov-Kutsev, G. F., & Efimova, G. Z. (2019). The Place Of Professional Education System In Formation Of Graduates' Competitiveness. *The Education and Science Journal, 21*(4), 139-161. doi:10.17853/1994-5639-2019-4-139-161

Tomšik, R. (2019). Choosing Teaching As A Profession: Validation Of An Smvup-4-S Assessment Tool. *Problems of Education in the 21st Century, 77*(4), 545-559. doi:10.33225/pec/19.77.545

Van Der Aar, L.P.E., Crone, E. A., & Peters, S. (2019). What Characterizes Adolescents Struggling With Educational Decision-Making? *Mind, Brain, and Education*. doi:10.1111/mbe.12209

METHODICAL PRINCIPLES AND STRUCTURE OF FORMATION OF LABORATORY ROCK SAMPLES DATA BASE

Svetlana Stroganova[5], Natalia Teodorovich [6]

Abstract
The developed structure and functions of laboratory and analytical databases of laboratory experiments on loading rock samples provide a unification of a set of relevant information about acoustic events and loading process parameters, structured storage and data management, and an intuitive user interface. Databases are implemented in the MS ACCESS DBMS, combining ease of use, reliability and wide distribution. The program provides the conclusion and display, input and storage of identification, chronological, parametric and reference information about the tests, as well as information about the results of the tests, including graphic data. It can be used to organize and systematize the results of experiments on the mechanical loading of rock samples in a testing laboratory for scientific research.

Key words
Database, acoustic emission, laboratory rock samples, MS ACCESS, seismic modeling

1 Introduction

In the experiments on rock loading test large number of rock samples, there is a problems of organizing a structured database of heterogeneous data on these samples (Smirnov, et al., 2001). Data can be identity data, weight and size, petrophysical data, test results. The database structure should include the different data level and the relationships between them. Principles of construction of such base are considered. It allows to uniquely identify the sample between irreversible impacts (test/experiment) and track the impact history. It can be used to organize and systematize the results of experiments on the mechanical loading of rock samples in a testing laboratory for scientific research. (Kaznacheev, et al., 2019; Ponomarev, et al., 2010).

Databases are intended for the collection and storage of primary data of laboratory experiments, the preparation and generation on their basis of data for subject analysis. The specificity of the database of laboratory experiments lies in the fact that they must be coupled with the data generated by the hardware-software complex (AIC) directly during the experiment. Ensuring the performance requirements of the AIC and the specificity of its software modules requires recording information during the experiment in the internal binary files of the AIC. After the end of the experiment, this information is subjected to primary processing, after which it is loaded into the laboratory database, which is the main repository of laboratory experiment data. To prepare for the subject analysis, the data from the laboratory database are transformed and loaded into the analytical database. The need to maintain two databases - laboratory and

[5] State Educational Institution of Higher Education Moscow Region «University of Technology» / Institute for engineering and digital technology, Faculty for Infocommunication Systems and Technologies (IT areas), Department of Information Technology and Control Systems, Russia, 141070 Moscow Region, city of Korolev, Gagarin St., 42, e-mail: stroganova.sm@ut-mo.ru

[6] State Educational Institution of Higher Education Moscow Region «University of Technology» / Institute for engineering and digital technology, Faculty for Infocommunication Systems and Technologies (IT areas), Department of Information Technology and Control Systems, Russia, 141070 Moscow Region, city of Korolev, Gagarin St., 42, e-mail: teodorovich.nn@ut-mo.ru

analytical - is due to the following factors: different purpose of the database; location of physical database carriers in various settlements (laboratory database - in the village of Borok, Yaroslavl region, analytical database - in Moscow); inexpediency at this stage of the implementation of a distributed database with network access due to the low bandwidth of the channel allocated for the laboratory at the Borok Geophysical Observatory. (Patonin, et al., 2012; 2014; 2019)

2 Laboratory DB

Laboratory database is a repository of data (the database storage tables) generated by the agro-industrial complex during laboratory experiments. Primary data is generated directly during the experiment in the form of a set of specialized binary files by four workstations and an agricultural press control system.

The press control system generates data once per second. This data consists of the readings of the sensors of the axial load of the press, axial deformation, the level of the master oscillator of the position of the piston, the number of acoustic events and their energy in the second interval.

A strain gauge station generates data once per second. They include readings of two sensors for radial deformation of the sample, two additional sensors for axial load, a comprehensive pressure sensor, and a pore pressure sensor. Additional axial load sensors are located directly in the high-pressure chamber in the lower punch of the mandrel for installing the sample and duplicate the readings of the main axial load sensor of the press.

An ultrasonic station for recording the propagation velocities of elastic waves records the waveforms of ultrasonic sounding signals along predetermined paths and at predetermined time intervals. The number of sensing paths is determined by the number of receiving and emitting sensors and their configuration. The maximum number of sensing paths is 16. The maximum sampling frequency is 40 MHz.

The station for recording waveforms of acoustic emission signals records the waveforms of these acoustic emission signals for all receiving sensors participating in the recording. The maximum number of receiving sensors is 16, and the maximum sampling frequency for 16 receiving sensors is 2.5 MHz. The maximum speed of writing waveforms to the hard disk is limited by the operating system and amounts to 100 events per second.

The station for synchronization and continuous recording of the acoustic emission stream generates the data of the acoustic emission sensor readings with a time resolution of 25.6 μs. At the same time, time stamps of synchronization signals of all workstations and the press control system are formed.

A system for recording external influences on a sample generates data once a second. Data includes comprehensive pore pressure and fluid spill readings. The start and end times of external exposure are recorded.

After the experiment, the information of the internal binary files of the agro-industrial complex is transformed and placed in the laboratory laboratory database.

The database of a laboratory experiment is a database storage tables obtained as a result of one experiment.

For each type of measurement and press control, separate tables with data are generated. For slowly changing processes, data is generated at intervals of 1 second. These data include axial and radial deformations, axial pressure, steps of the generator that sets the position of the press piston, and the intensity of the acoustic emission flow. In the tables of data on the propagation velocities of elastic waves, the time of each sounding session is indicated. The structure of the catalog of events of acoustic emission is similar to the structure of the catalog of earthquakes. Here, there is the time of each event, its coordinates, amplitudes and signs of

entry to each of the receiving sensors. As additional information, the catalog includes data on the acoustic noise preceding the event, the duration of the signal itself for each of the sensors. A bulletin of all identified events is included in the data tables of continuous recording of the flow of acoustic energy. For each identified event, its time, maximum signal amplitude and its energy are recorded.

2.1 The logical structure of the information base

The database includes a schema or metadata that describes the logical structure of the database in a formal form.

The information base includes database storage tables. The database storage is a set of tables for storing data from laboratory experiments. These data include: specimen loading parameters, stress-strain characteristics of the specimen obtained during loading, ultrasonic wave propagation velocity, catalogs of acoustic events, extended bulletins of acoustic events, parameters of external influence on the sample.

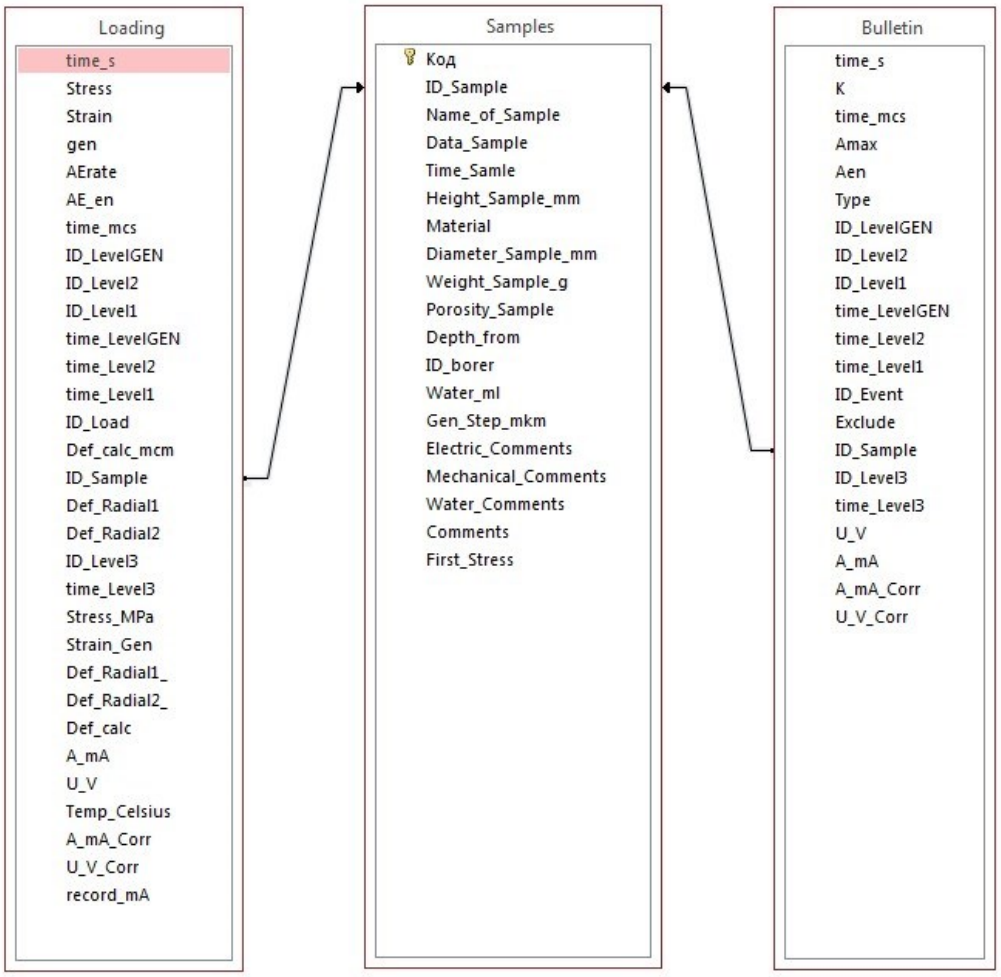
The database storage tables are united by a common time, to which all data of the current experiment are tied.

The database provides the following tables for storing data:

- Table "Press control station data";
- Table "Strain measurement";
- Table "Velocity of propagation of elastic waves";
- Table: "Energy of the first half-period of the probe wave";
- Table: "The total energy of the probe signal in each of the directions"
- Table: "Amplitudes of sounding signals"
- Table "Catalog of acoustic events";
- Table "Zoning of the catalog of acoustic events";
- Table "Bulletin of acoustic events";
- Table "Sample Identification";
- Table "External exposure data";

A record in each table is a minimal set of data for an informative unit. The database data model is relational, the relationship of the database tables is supported by an external key and relationships based on primary keys. Figure 1 shows a diagram of the logical connections between the above arrays of information in the form of a diagram in accordance with the requirements of the DBMS.

Fig. 1: Logical connections between arrays of information in the form of a diagram in accordance with the requirements of the DBMS: Loading, Samples and Bulletin of Catalog (source:author)



2.2 Organization of maintaining the information base

Information Base Creation Procedure.

The database layout is stored as a binary file of the MS ACCESS DBMS with a fully formed information base structure. This does not require any special steps to create the database, just copy the layout file to a separate directory and rename it accordingly.

Laboratory DB Filling Procedure.

Before importing into the database, the primary data is pre-processed by external utilities, managed according to a script implemented by a set of scripts. Pre-processing includes: converting all data to a single high-precision time scale, the basis of this scale is the time of the station for continuous recording of acoustic emission flux; processing waveforms of ultrasonic sounding signals and obtaining data on the propagation velocities of elastic waves along selected paths; processing waveforms of acoustic emission signals and obtaining the coordinates of signal sources, entry signs and signal energy, compiling a catalog of acoustic events; processing a continuous flow of acoustic energy, highlighting individual events, determining their characteristics, compiling a bulletin of acoustic events.

Data import from generated ASCII files is carried out by the operator by importing local text files in ASCII format.

Procedure for changing the infobase.

Replenishment of the generated database is not required, since the primary data of the records of the workstations and the press control system are unique for each experiment and are not subject to change.

Information Base Maintenance Procedure.

No actions specific to this database that go beyond the standard operations for working with the DBMS as a whole are not required when servicing the database. Maintenance of the database can be carried out by the built-in DBMS MS ACCESS, ensuring the following operations: creation and delimitation of the rights of the database system roles (if necessary); incremental backup; full backup. It is recommended that you configure periodic database backups.

3 Analytical DB Catalog

The analytical database is designed to store acoustic catalogs, prepare and generate their data for subject analysis.

3.1 The logical structure of the information base

The database includes a schema or metadata that describes the logical structure of the database in a formal form. An analytical database consists of a kernel of identical structure and functions to the database of seismic catalogs. The information base includes tables, interconnected queries, and macros. The tables are designed to store data on the parameters of the stress-strain state of the sample created by the press. A system of interconnected queries and macros implements the basic functionality of the database.

The database provides the following tables for storing data:

- Table "History of loading";
- Table "Characteristics of the sample";
- Table "Bulletin of acoustic events";

A record in each table is a minimal set of data for an informative unit. The database data model is relational, the relationship of the database tables is supported by foreign keys and relationships based on primary keys.

3.2 The Procedure for creating and organizing the maintenance of the information base

The database layout is stored as a binary file of the MS ACCESS DBMS with a fully formed information base structure. This does not require any special steps to create the database, just copy the layout file to a separate directory and rename it accordingly.

The database is filled by the operator by importing data from the ASCII file of the Laboratory database. After importing the data, the following queries should be executed: "Bulletin_Fill_Bull" and "Loading_Fill_Loading". After that, the database is ready to work.

Procedure for changing the infobase

Replenishment of the database is not provided. In case of recalculation of the primary data of a previously conducted laboratory experiment, the database must be re-formed.

Information Base Maintenance Procedure

No actions specific to this database that go beyond the standard operations for working with the DBMS as a whole are not required when servicing the database. Maintenance of the database can be carried out by the built-in DBMS MS ACCESS, ensuring the following operations: creation and delimitation of the rights of the database system roles (if necessary); incremental backup; full backup. It is recommended that you configure periodic database backups.

3.3 Analytical DB Catalog

The analytical database DB is intended for storing acoustic catalogs, data from an ultrasonic sensing station, recording waveforms of AE signals, and allows preparing and generating data for subject analysis.

3.4 Logical structure of the information base

The database includes a schema or metadata that describes the logical structure of the database in a formal form.

An analytical database consists of a kernel of identical structure and functions to the database of seismic catalogs.

The database implements the following functions: storage and provision of information about the acoustic catalog and the parameters of ultrasonic sounding of the sample along given paths.

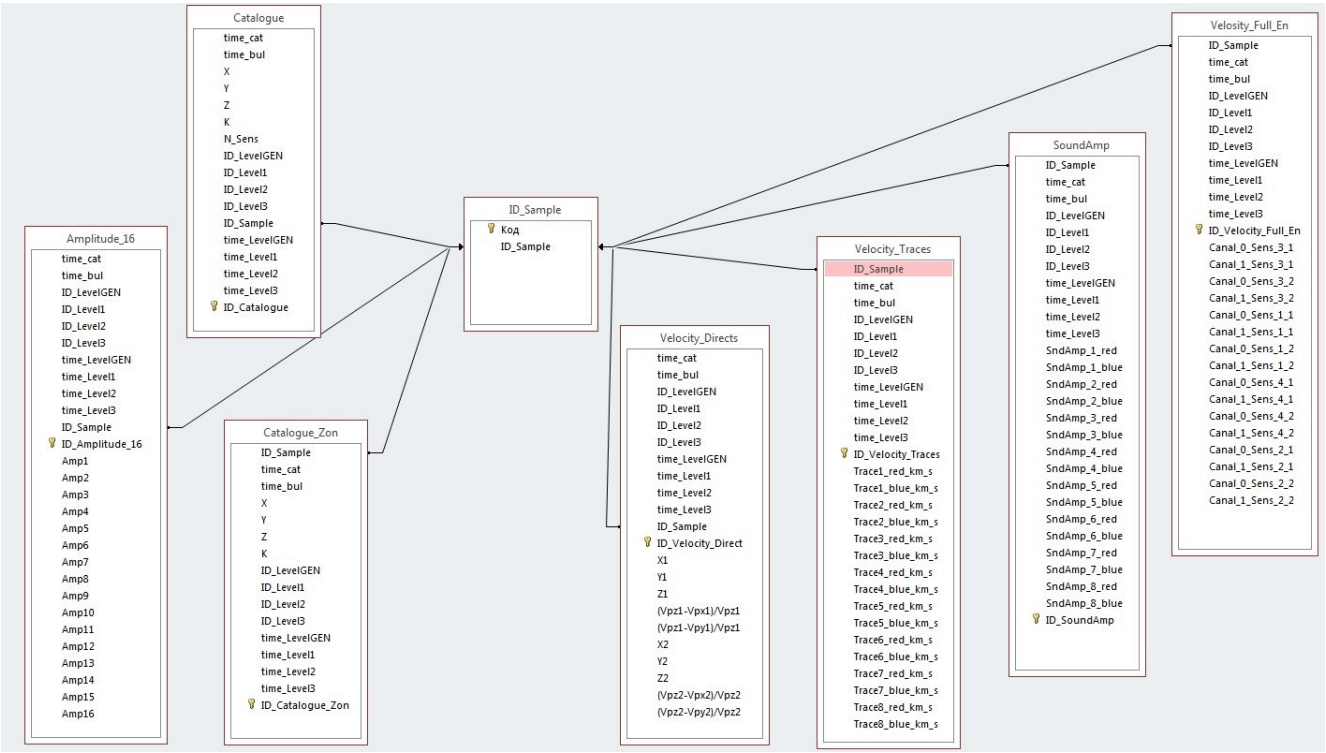
The information base includes tables, interconnected queries, and macros. The tables are designed to store data on the speed of propagation of elastic waves in the directions of sounding, the energy of the first half-period of the sounding wave, the total and maximum energy of the sounding signal in each direction, data from the catalog of acoustic events. The system of interconnected queries and macros implements the basic functional capabilities of the database.

The database provides the following tables for storing data:

- Table "Velocity of propagation of elastic waves";
- Table: "Energy of the first half-period of the probe wave";
- Table: "The total energy of the probe signal in each of the directions"
- Table: "Amplitudes of sounding signals"
- Table "Catalog of acoustic events";
- Table "Zoning of the catalog of acoustic events";
- Table "Sample ID";

A record in each table is a minimal set of data for an informative unit. The database data model is relational, the relationship of the database tables is supported by foreign keys and relationships based on primary keys. Figure 2 gives a demonstration of the diagram of the logical connections between arrays of information in the form of a diagram in accordance with the requirements of the DBMS. The diagram includes tables of analytical part of DB Catalog.

Fig. 2: Logical connections between arrays of information in the form of a diagram in accordance with the requirements of the DBMS: Analytical part of DB Catalog. (source:author)



3.5 The procedure for creating and organizing the maintenance of the information base

The database layout is stored as a binary file of the MS ACCESS DBMS with a fully formed information base structure. This does not require any special steps to create the database, just copy the layout file to a separate directory and rename it accordingly.

The database is filled by the operator by importing data from the ASCII file of the Laboratory database. After importing the data, you should run the macros: "_Clean_All" and "_Fill_All". After that, the database is ready to work.

Procedure for changing the infobase

Replenishment of the database is not provided. In case of recalculation of the primary data of a previously conducted laboratory experiment, the database must be re-formed.

Information Base Maintenance Procedure

No actions specific to this database that go beyond the standard operations for working with the DBMS as a whole are not required when servicing the database. Maintenance of the database can be carried out by the built-in DBMS MS ACCESS, providing the following operations: creation and delimitation of the rights of the database system roles (if necessary); incremental backup; full backup. It is recommended that you configure periodic database backups.

4 Conclusion

The developed structure and functions of laboratory and analytical databases of laboratory experiments provide for the unification of a set of relevant information about acoustic events and loading process parameters, structured data storage and management, and an intuitive user

interface. Databases are implemented in the MS ACCESS DBMS, combining ease of use, reliability and wide distribution. Laboratory and analytical databases provide the ability to import data from internal databases of the hardware-software laboratory complex; bringing technical indicators of the loading process to SI units; selection by given parameters, including aftershock sequences and data export to ASCII format.

Resources

Kaznacheev, P.A., Stroganova, S.M., Ponomarev, A.V., Majbuk, Z. Ju. Ja., Smirnov, V.B., Krasnova, M.A., & Patonin, A.V. (2019). Methodical principles of formation of laboratory rock samples data base. *Physical-chemical and petrophysical studies in Earth sciences. Proceedings of the conference.* (pp.137-140). IGEM. http://www.igem.ru/petromeeting_XX/tbgdocs/sbornik_2019.pdf

Patonin, A.V. (2012). *Hardware and software laboratory complex for solving problems of rock destruction physics*. [PhD thesis, The Schmidt Institute of Physics of the Earth of the Russian Academy of Sciences (IPE RAS)]. https://www.dissercat.com/content/apparatno-programmnyi-laboratornyi-kompleks-dlya-resheniya-zadach-fiziki-razrusheniya-gornyk

Patonin, A. V., Ponomarev, A. V., & Smirnov, V. B. (2014). A laboratory instrumental complex for studying the physics of the destruction of rocks. *Seismic Instruments, 50*(1), 9-19. doi:10.3103/s0747923914010046

Patonin, A. V., Shikhova, N. M., Ponomarev, A. V., & Smirnov, V. B. (2019). A Modular System for Continuous Recording of Acoustic Emission for Laboratory Studies of Rock Destruction Processes. *Seismic Instruments, 55*(3), 313-326. doi:10.3103/s0747923919030101

Ponomarev, A., Lockner, D., Stroganova, S., Stanchits, S., & Smirnov, V. (2010). Oscillating Load-Induced Acoustic Emission in Laboratory Experiment. *Synchronization and Triggering: From Fracture to Earthquake Processes Geoplanet: Earth and Planetary Sciences,* 165-177. doi:10.1007/978-3-642-12300-9_9

Smirnov, V. B., Sergeeva, S. M., & Ponomarev, A. V. (2001). On the similarity and feedback in experiments on rock fracture. *Izvestiya - Physics of the Solid Earth, 37*(1), 82-88. doi:10.1134/11486.1555-6506

THE OPTIMAL CAPITAL STRUCTURE FOR BIOTECHNOLOGY STARTUPS

Mária Szivósová[7]

Abstract
Biotechnology firms and startups are atypical in terms of their capital needs. The life-cycle capital structure theory suggests that startups are generally financed through internal sources, but research has shown that R&D in the biotechnology sector is capital intensive and biotechnology startups are mostly financed by venture capitalists. This article clarifies what is the theory of optimal capital structure for biotechnology startups and what are the causes of differences and deviations in decision-making on the capital structures of biotechnology startups.

Key words
Biotechnology, Capital structure, Financing, Research and Development

1 Introduction

The problem with most capital structure theories is that they are based on assumptions which are not applicable to young firms and startups. The life cycle theory by (Berger & Udell, 1998) is the most relevant and appropriate theory for the study of startups, because it is based on the supposition that firms have particular sources for financing within each firm stage. In spite of this, the life cycle theory is presumed to be true for a typical, average firm and may be incorrect for firms that are in specific industries.

The motivation behind this study is to understand the capital structure trends and decisions of biotechnology firms and startups, because the biotech industry is atypical in terms of financing. In particular, biotech firms have different financing and capital needs, due to the extremely large costs of research and development of biotechnology products and technologies (Jayasundara, 2019). Hence, biotechnology startups are generally unable to finance through internal financing, like it is suggested by the life cycle theory.

2 Modern Capital Structure Theories

Biotechnology is a fascinating science that has no defined limits in terms of its application. Biotechnology can be differentiated into three major subsections consisting of: green biotech - focusing on application in plants, animal feed and the environment, red biotech - associated with human health, and industrial biotech - looking at ways to improve industrial processes in order to increase desired products or reduce waste and emissions. The US and Europe based publicly traded companies in the biotech sector, have employed more than 200,000 people and reached record-high revenues of $139.4 billion in 2016 (EY, 2017).

Furthermore, the number of early stage deals in biotech startup sector has grown over 57.2% from 2012 to 2017 and biotech startups account for 1.8% of all global startups that were established from 2017 to 2018 (Startup Genome, 2018). Biotech startups in Europe and the US have raised more than $250 billion in 2016, $1.1 trillion was spent by biotech firms into

[7] University of Economics in Bratislava, Faculty of Economic Informatics, Department of Applied Informatics, Dolnozemská cesta 1, 852 35 Bratisava, E-mail: maria.szivosova@euba.sk

biopharmaceutical research and there are currently over 600 clinical trials that are currently conducted by VC-backed startups (EY, 2017; Startup Genome, 2018).

The biotech sector as a whole is growing at unprecedented levels and is expected to continue growing in the future. It is projected that major investors such as China, will increase its spending into the biotech sector by 9-10% through 2020 (Startup Genome, 2018). The largest firms within the US biotechnology sector consist of Amigen (revenue $23 billion), Biogen ($11.4 billion) and Celgene ($11.2 billion); meanwhile, Europe is dominated by British Shire ($11.4 billion), Swiss Actelion ($2.5 billion) and Irish Horizon Pharma ($1 billion) (EY, 2017).

3 Capital Structure for Typical Startups

The most accessible and straightforward financing for startups is to use founders capital, where it can come from from multiple founders or a single founder and can be both equity or debt. Current research on startups has shown that in many cases founders capital is the biggest source of financing for young firms and startups. Roughly 50% of the capital used by U.S. based startups came from the preeminent founder and 80% of innovation based startups in Belgium have used founder capital for financing (Berger & Udell, 1998; Bozkaya & Van Pottelsberghe De La Potterie, 2008). In startups, the most common form of founder equity comes in the form of personal savings, however founder debt on personal credit is used as well to a lesser degree (Robb & Robinson, 2010).

Bygrave & Hunt (2008, p.2) describe financing from friends and family as ‘‘the lifeblood of entrepreneurial ventures’’ making it pivotal for young firms. Financing from friends and family can be based on equity or debt and it is a considerably important form of financing in the U.S., where research has shown it to be the third or even second most used type of financing (Bates & Robb, 2013; Campbell & De Nardi, 2009). Research on European firms have shown more varied results in comparison to the U.S. because startups in the UK have demonstrated similar results to the U.S. (Ullah et al., 2010). On the other hand, the innovative startups in Belgium portrayed restricted use of family and friend capital for financing (Bozkaya & Van Pottelsberghe De La Potterie, 2008).

Winborg & Landström (2001, p.235) define financial bootstrapping as ‘‘the use of methods for meeting the need for resources without relying on long-term external finance from debt holders and/or new owners.’’ It is possible to split strategies in bootstrapping into two distinctive groups, with the first category focusing on alternative investment sources, while the second category intends to minimize the necessity of economic capital.

Startups in **the biotechnology sector** have specific requirements in terms of financing when compared to a more average and regular startup, as they require higher amount of capital for initial research and testing (Jayasundara et al., 2019). It can take multiple years for a biotech product or service to reach the market as there strict regulations for monitoring and testing placed by the government. Consequently, biotech startups can operate for a multitude of years without generating any revenue. Hence, biotechnology startups are expected to not adhere to the life cycle capital structure theory, as they are extremely capital intensive, forcing them to rely on external financing.

4 Venture Capital

Venture capital (or VC in short) is a form of financial investment focusing on private firms with high growth potential that are presently in their early firm stages. Given the emphasis of financing startups or young firms with high growth potential, VCs provide capital and financing in sectors where innovation and different advancements are being created. Or in other words, VCs focus on industries that are based on knowledge and have an outstanding business prospective.

Accordingly, VCs gravitate towards young firms in the biotechnology sector or startups in the internet associated services, telecommunications and information technology industry (Fraser- Sampson, 2007; Gompers & Lerner, 2001). A VC will generally look for minority ownership in the investee company, allowing the firm management to maintain majority ownership. Howbeit, a VC will have decisive impact on strategically significant choices of the startup through extensive contractual limitations, despite minority ownership and therefore will retain close control over their investee companies (Cumming, 2008; Kaplan & Stromberg, 2003).

There are different kinds of VCs, where most standard companies use close-end funds to invest their assets and capital. Usually this kind of funds are organized in a way where the investors are limited partners and the VC function as the general partner. The limited partners supply the majority of the capital used for investment and consist primarily of wealthy people and institutional investors. In addition to this, VCs can be autonomous and self-reliant, where they invest their own capital and are controlled by the management. There is yet another kind of VC firms, which specialize in investment of their capital into firms that are publicly listed and are traded on the stock exchange. VCs can likewise be captive or corporate VCs, where they function as a subsidiary or a affiliate of an insurance/industrial firm or a bank. The last kind of

VC firms are made up of government-partnered investment programs, which support young firms through regional or state financing and operate as government-financed VC enterprises.

Research into financing has highlighted two noteworthy benefits of equity which can be either from a VC or a business angel. To start with, business angels and also VCs are regarded to as investors that possess ‘value added’ in comparison to other forms of financing. Both type of investors can provide sector-specific expertise and new connections through their networks. Furthermore, the likelihood that the firm fails because of problems with fulfillment of covenants or payment of amortization and interest is decreased through equity financing (Carpenter & Peterson, 2002).

However, the procedure of raising capital through equity will be in general more expensive for unknown and new startups, because equity financing will require entrepreneurs to provide larger share of control and ownership of their firm. Just a couple of startups have the qualities and potential that is required to appeal to VC investors, making VC financing relatively uncommon for an average startup. This claim is further confirmed in many studies, where Robb & Robinson (2010) have indicated that VCs only finance 4% of US based startups. However, biotechnology startups differ from an average startup by having an much higher ceiling for financial gain, which is dependent on the success of research and development of the biotech startup.

5 Grants

To promote, aid and facilitate funding of startup firms, governments mediate in the market in different approaches. Asymmetries of information and spillover effects of information are two types of market failures that require intervention and correction from the government. Stiglit & Weiss (1981) suggest that the first type of market failure happens because potential investors have less information about the capability and potential of a project from a innovating firm, and hence the potential investors can not fully comprehend the project and the risks or quality associated. The second type of market failure points out the situations where competitors can copy the knowledge of a firm, thus making it harder for firms to completely capture benefits from the investments they make (Nelson, 1959).

It can be said that the two types of market failures lead to innovative projects of firms being undercapitalized. To make up for this underinvestment, governments are spending substantial amounts of funding and efforts on activities and programs aimed at promoting

innovation. Nonetheless, a balancing act must be undertaken by governments when they try to correct these kinds of market failures because governmental financing shouldn't interpolate inefficiencies in the financing market or function as a replacement for financing that would have occurred in any case (Georghiou, 2002).

Grants are a form of direct financial assistance from the government that is provided to firms. Salamon & Elliott (2002, p.341) define grants as ''a gift that has the aim of either 'stimulating' or 'supporting' some sort of service or activity by the recipient''. Governments aren't the only providers of grants as a minority of them are provided by corporations and foundations.

6 Debt

Commercial banks and other financial institutions are an essential source of finance which offers short-dated and long-term loans to firms. Collateral is of the most imperative determinants that affects the access a firm has to debt capital when borrowing from a commercial source and it is the total amount of assets that a firm can vow as loan guarantee.

Berger & Udell (1998) argue that restrictive covenants are generally added to debt contracts in order to lessen moral hazard problems and also disadvantageous selection. From an entrepreneur's viewpoint, it can be appealing to finance through bank debt because it can be relatively cheap and in contrast to equity, bank debt has no effect on control or the ownership of the firm. However, banks likewise to entrepreneurs are also increasingly interested to work with startups and this is due to a multitude of factors.

To start with, it is very common practice for banks to require personal assets, from at least one owner to act as insurance and collateral when lending to a young firm or a startup (Berger & Udell, 1998). Therefore, even the bank loans given to startups are guaranteed, not necessarily by the firm, but the owners assets. Secondly, lending is currently just one part of the multiple services that are offered by most banks. Financial institutions have multiple financial services that are available to startups which are non-lending fee-based products (de la Torre, Martínez Pería & Schmukler, 2010). Per se, the bank's income streams coming from doing business with startups can be maximized through cross-selling.

Thirdly, Huyghebaert & Van de Gucht (2007) with Hellmann, Lindsey & Puri (2007) argue that financial institutions are probable to be interested in developing long-term partnerships that might pay off later on. For instance, as a startup expands, a bank might strive to become the firm's main provider for financial services. In relation to decreasing exposure through firm owners' guarantees, banks utilize other ways to reduce risk. For example, instead of right away denying high risk applications for loans, banks will select to shorten the period of loan or will only provide financing for a lower financial sum than originally requested (Huyghebaert & Van de Gucht, 2007). As such, banks can reduce their exposure to risk and at the same time build future longterm partnerships. Moreover, Korosteleva & Mickiewicz (2011) have demonstrated that startups have easier access to financing through debt because of developments in innovation that have been able to lower the transaction expenses of banks when dealing with startups, along with higher global competition between banks.

7 Accelerator

Accelerators in general support startups in constructing their first products and services, successfully determining their clients or customers and also seizing the necessary assets for operation, which can include labor or capital. In particular, accelerator programs will last for approximately three months and they assist novel firms with setting up. Normally accelerator programs supply startups with some work space along with little seed capital. Furthermore, these

programs provide numerous possibilities for networking, learning and mentoring. This can be through a multitude of people that can include other peer firms in the accelerator program, firm managers, VCs or angel investors. It is common for accelerator programs to finish with a 'demo day', which is a big event where startups have the opportunity to pitch and present their firms to accomplished investors (Cohen, 2013).

Certain parallels between accelerators, business angels and incubators as all target to assist startups during the early firm phases. Hence, it can assumed that all three provide relatively similar assistance. But in several aspects accelerators can vary from the other two, with the most essential distinction being the restricted duration of an accelerator program. Business angels and incubators in many cases do not have a specified time period within which they provide assistance to startups.

There can me major differences between various accelerators because there can be differences in the support and assistance they provide. For example, the period for mentoring, training and education can differ and certain accelerator programs can be non-profit, while others are looking for profit. Furthermore, accelerator programs can be associated with numerous organizations including NGOs, VCs, universities, business angels or the government. The set duration, intensity and competitiveness in admission is what differentiates accelerator programs from other comparable options like incubators.

Several studies portray the part played by accelerators in the communication among young firms and investors. For instance, a study that was based on multi-case research has indicated that accelerator programs which are mentorship driven, link up participating firms with potential investors (Radojevich-Kelley & Hoffman, 2012). However, an important point to consider is that accelerators can be shareholders in the startups that they certify, which can encourage them to retain adverse information about startups within the programme (Kim & Wagman, 2014).

8 Merger and Acquisition

Mergers and acquisitions (M&A) can be tremendously valuable and strategically beneficial for both parties involved. Acquirers can achieve instant ownership of patents and technologies, access to specific products or services and even advantageous market positions. On the other hand, firms that are acquired can gain capital, expertise, machinery, new services, economies of scale and other business elements that are extremely difficult to obtain as a smaller and younger firm. Trautwein (1990) has suggested that managerial motivations for M&A could include diversification or firm expansion to a new country. In addition, the driving force for a M&A can be to gain precious assets such as technology, skills or know-how (Ahuja & Katila, 2001).

Walter and Barney (1990) have described in their research the different objectives that managers may have during a M&A. For example, a firm may use M&A as a way to maximally utilize the financial capability of the firm or to reduce the interdependency on different firms. Furthermore, Patzelt, Schweizer & Aufsesse (2007) looked at what are the main motives and benefits of M&A in the German biotechnology industry. They have suggested that key motives were related to improving firm technology or expansion to the U.S. through increased presence and improved access to networks. The main benefits consisted of higher visibility for investors (including VCs and potential investors at IPO) and quicker product development.

9 Business angels

Business angels play a significant role in the funding of firms in their early stages of growth. Mason & Harrison (2008, p.309) define business angels as 'A high net worth individual, acting alone or in a formal or informal syndicate, who invests his or her own money directly in

an unquoted business in which there is no family connection and who, after making the investment, generally takes an active involvement in the business, for example, as an advisor or member of the board of directors.'

Differently said, business angels use their own capital to directly invest into few firms while assuming an active position within them. Dissimilar to VCs which have fiduciary liability towards separate stakeholders, business angels in general utilize different economic tools which extend from sheer equity to sheer debt (Shane, 2012). It is more common for business angels to operate alone and a large number of them are former or active executives or entrepreneurs. However, occasionally business angels collaborate together in investment organizations, e.g. angel networks.

Geographical proximity has an effect on the firms that business angels generally invest into as they frequently invest into firms that are in one region or country. Business angels will in general invest into startups that VCs would find unappealing, because of the elevated degree of uncertainty that they tend to have. This may be because casual investors are investing a lower part of their assets in unquoted businesses. Research into business angels from the UK has shown they on average invest 5-10% of their capital into startups and young private companies (Mason & Harrison, 2008). In comparison to VCs, it has been proposed that business angels and private investors have reduced transaction costs, which allows them to invest in the more risky and early stages of a firm (Adveitchikova, 2008).

Profit is normally the main motivation for business angels to provide finances for an unquoted firm, and therefore, similar to VCs, business angels will attempt to exit their investment by selling their stocks to an another party (Riding, 2008). But, business angels are not compelled to exit inside a specific time period, in comparison to VCs, where the investment period is generally more critical as they operate funds with defined lifespans. Likewise, business angels are more prepared, rather than continually pursue full exists, to receive a range of dividends from a firm which has discovered a profitable niche. In addition, it is recurrently argued in literature that business angels can have certain non-financial reasons to invest, for example, investments that are socially beneficial or 'moral'.

Howbeit, changes in the angel community have occurred as the financing market introduced a novel type of business angel, the super angel. The super angel has not been thoroughly investigated yet by researches, although has been the focal point in talks among professionals and the business media (Spencer, 2009). Super angel alludes to serial investors and entrepreneurs, who are considered to be experienced, qualified, have a good network and who can, directly or through funds, invest substantial money in young firms and startups. Moreover, super angels are known to widen their investments in terms of geographic in comparison to more traditional business angels.

10 Research Outline

The literature review has shown that there has been a multitude of capital structure theories developed by different researchers and academics over time. However, theories such as the M&M capital structure theory are outdated, while others like the market timing theory and the free cash flow theory are more applicable to firms which are more mature and are in their later stages. Hence, the life cycle theory is the most applicable to biotechnology startups because certain financing options are available during specific life stages of a firm. Furthermore, the capital structure of startups in the biotechnology sector is expected to be different in comparison to a more typical and average startup. Research in biotechnology is lengthy and capital intensive as all products and treatments related to human health and agriculture require thorough testing that occurs through clinical trials or lab testing (Jayasundara et al., 2019; Moore, Zhang, Anderson & Alexander, 2018).

Therefore, this study is examining what is the optimal capital structure for a startup in the biotechnology sector. This sector has distinctive financial requirements, meaning biotechnology startups will follow a unique a life cycle for financing in comparison to a typical startup. For this study, optimal capital structure in this research is defined as the most common used method of financing

11 Summary of Capital Structures used by biotechnology startups

Due to the exploratory nature of the study, qualitative research methods were used by using secondary data sources. Qualitative research allows for more comprehensive evaluation of data and industry specific insights, like in the case of the biotechnology sector. This study has used online financial databases to obtain secondary data on capital structure of biotechnology startups.

This allows for analysis of capital structures in terms of which financing options are available to startups and which options do biotechnology firms choose, within their various stages of growth and maturation. 27 firms were present on the Pitchbook database.

Tab.1 : Summary of Capital Structures of the Pitchbook Sample, Based on Financial Round

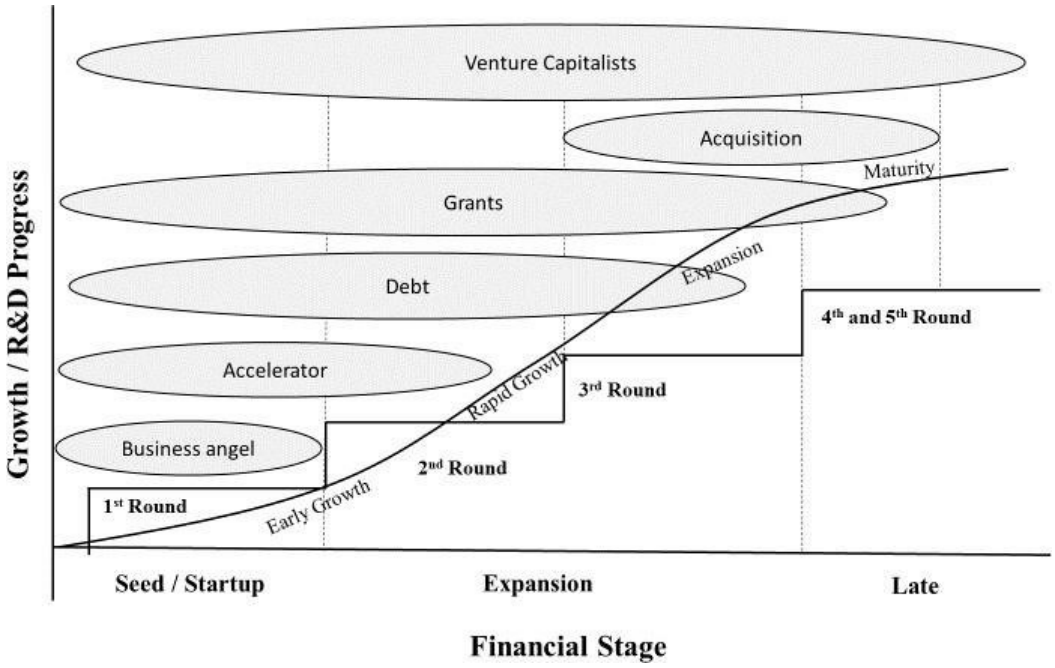
Number of Biotechnology Firms Using Particular Source of Financing						
Financial Round	**Accelerator**	**Acquisition**	**Business Angel**	**Debt**	**Grant**	**Venture Capital (VC)**
1st	**2**		**1**	**1**	**2**	**21**
2nd	**3**			**4**	**3**	**9**
3rd		**2**		**2**	**3**	**4**
4th		**1**			**2**	**2**
5th						**1**
Weighted Average	**1.6**	**3.3**	**1**	**2.1**	**2.5**	**1.7**

Source: author

12 Biotechnology Firm Specific Life-Cycle Diagram

The contribution from this exploratory study can be summarized and presented through the development of a new life-cycle theory diagram that is specific for financing of firms in the biotechnology industry.

Fig. 1 : Life-Cycle Diagram Specific for Biotechnology Firms



Source: author

13 Conclusion

This exploratory study has aimed to identify what is the optimal capital structure for biotechnology startups. It can be concluded that financing through VCs is the optimal capital structure for most biotechnology startups and this information can be presented, through the development of a novel life cycle diagram for biotechnology firms. Research and development in the biotechnology is capital intensive; (Jayasundara et al. 2019) have shown that the average clinical costs for research of one product are equal to € 37.5 million. Thus, certain types of financing, are more common and advantageous for biotech firms.

While the life cycle diagram may be true for most biotech firms, but this is not true for all biotech firms. For example, service providers in the biotech industry do not require large initial investment, because they are not developing a new biotech product and therefore, will use other types of financing in comparison to a typical biotech firm. While the sample size limits the generalizability of the results, it can be used as basis for additional research on the capital structure of biotechnology firms.

Resources

Ahuja, G., & Katila, R. (2001). Technological acquisitions and the innovation performance of acquiring firms: A longitudinal study. *Strategic Management Journal, 22*(3), 197-220. doi:10.1002/smj.157

Berger, A., & Udell, G. (1998). The economics of small business finance: The roles of private equity and debt markets in the financial growth cycle. *Journal Of Banking & Finance*, 22(6-8), 613-673. doi: 10.1016/s0378-4266(98)00038-7

Bozkaya, A., & B. Van Pottelsberghe De La Potterie. (2008). Who Funds Technology-Based Small Firms? Evidence From Belgium. *Economics of Innovation and New Technology, 17*(1-2), 97-122. doi:10.1080/10438590701279466

Bygrave, W., & Hunt, S. (2008, October 31). For Love or Money? A Study of Financial Returns on Informal Investments in Businesses Owned by Relatives, Friends, and Strangers. Retrieved March 9, 2020, from https://ssrn.com/abstract=1269442

Carpenter, R. E., & Petersen, B. C. (2002). Is the Growth of Small Firms Constrained by Internal Finance? *Review of Economics and Statistics, 84*(2), 298-309. doi:10.1162/003465302317411541

Cohen, S. (2013). What Do Accelerators Do? Insights from Incubators and Angels. *Innovations: Technology, Governance, Globalization*, 8(3-4), 19-25. doi: 10.1162/inov_a_00184

Cumming, D. (2008). Contracts and Exits in Venture Capital Finance. *Review Of Financial Studies*, 21(5), 1947-1982. doi: 10.1093/rfs/hhn072

EY Follow. (2017, August 09). EY Biotechnology Report 2017: Beyond borders - Staying the course. Retrieved March 3, 2020, from https://www.slideshare.net/ernstandyoung/ey-biotechnology-report-2017-beyond-borders-staying-the-course

Gompers, P., & Lerner, J. (2001). The Venture Capital Revolution. *Journal Of Economic Perspectives*, 15(2), 145-168. doi: 10.1257/jep.15.2.145

Jayasundara, K., Hollis, A., Krahn, M., Mamdani, M., Hoch, J. S., & Grootendorst, P. (2019). Estimating the clinical cost of drug development for orphan versus non-orphan drugs. *Orphanet Journal of Rare Diseases, 14*(1). doi:10.1186/s13023-018-0990-4

Kim, J., & Wagman, L. (2012, September 06). Portfolio Size and Information Disclosure: An Analysis of Startup Accelerators. Retrieved March 3, 2020, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2142262

Mason, C. M., & Harrison, R. T. (2008). Measuring business angel investment activity in the United Kingdom: A review of potential data sources. *Venture Capital, 10*(4), 309-330. doi:10.1080/13691060802380098

Nelson, R. R. (1959). The Simple Economics of Basic Scientific Research. *Journal of Political Economy, 67*(3), 297-306. doi:10.1086/258177

Radojevich-Kelley, N., & Hoffman, D. (2012). Analysis of Accelerator Companies: An Exploratory Case Study of Their Programs, Processes, and Early Results. Retrieved March 19, 2020, from https://www.sbij.org/index.php/SBIJ/article/view/136/93

Robb, A., & Robinson, D. (2010, August 24). The Capital Structure Decisions of New Firms. Retrieved March 19, 2020, from https://ssrn.com/abstract=1662266

Shane, S. (2012). The Importance of Angel Investing in Financing the Growth of Entrepreneurial Ventures. *Quarterly Journal of Finance, 02*(02), 1250009. doi:10.1142/s2010139212500097

Ullah, F., Abbas, Q., & Akbar, S. (2009). The relevance of pecking order hypothesis for the financing of computer software and biotechnology small firms: Some UK evidence. *International Entrepreneurship and Management Journal, 6*(3), 301-315. doi:10.1007/s11365-008-0105-0

Winborg, J., & Landström, H. (2001). Financial bootstrapping in small businesses. *Journal of Business Venturing, 16*(3), 235-254. doi:10.1016/s0883-9026(99)00055-5

IMPROVING THE QUALITY OF EDUCATION OF COMPUTER SCIENCE TEACHERS THROUGH THE KAIZEN PHILOSOPHY

Riza Akhitova[8], Aitugan Alzhanov[9], Igor Vostroknutov[10]

Abstract
This article explicates the application of Kaizen philosophy to improve the education of computer science teachers. The relevance of the research topic arising from the continuously existing modern trends in education, which require improving the quality of education of computer science teachers. The main idea of this research is anchored on Kaizen principles espoused by Kaizen expert Masaaki Imai. The article has recommendations adapted to the principles of continuing education in the field of teaching and learning. The role of teachers and students who work in the implementation of continuous quality improvement to achieve and maintain the effectiveness and efficiency of quality education is considered. The article also analyzes traditional and modern methods of teaching in higher education in order to assess the effectiveness of their application in the professional activities of future teachers of computer science. Clarifies the concept of "Continuous improvement of the quality of education" and "Monitoring the quality of education".

Keywords
Kaizen, Continuous quality improvement, Kaizen in teaching, monitoring the quality of education

1 Introduction

Modern trends in the development of computer science in higher education institutions globally will be attributed to the modernization of society. An important factor in this development is education, because in the 21st century, everyone should be aware of various fields of science, as well as have the skills of self-education and self-improvement. In this regard, the future society directly depends on the quality, intensity and mobility of the training system for future teachers in higher educational institutions. At present, the interest in computer science as a modern science by various specialists is steadily growing. This is due to social reasons.

Big changes in the scientific and technical development of modern society pose each person the task of continuously mastering more and more new knowledge and skills in the field of computer science as the basis for competitiveness in the labor market and improving living standards. Considering computer science as a subject, discipline and industry, it is necessary to highlight the modern trends of its development in such educational institutions.

Improving the quality of education of computer science teachers is based on the following modern educational trends:

[8] L.N. Gumilyov Eurasian National University, Faculty of Information Technology, Department of Informatics, Kazakhstan, Nur-Sultan, akhitova.riza@mail.ru

[9] L.N. Gumilyov Eurasian National University, Faculty of Information Technology, Department of Informatics, Kazakhstan, Nur-Sultan, alzhanov_ak@mail.ru

[10]Moscow City Teacher Training University, Department of Informatics and Applied Mathematics,Institute of Digital Education, Russia, Moscow, vostroknutov_i@mail.ru

• development of information culture and information competence;
• creative activity of subjects of the educational process of the university;
• criteria-based assessment of students;
• increasing the effectiveness of students independent work.

At the same time, in improving the quality of education of teachers of computer science, attention should be paid to modern areas of computer science development, such as information security, intelligent systems and technologies, distance support for training courses, distance learning modules, content of additional education in computer science, virtual reality, and so on.

With the development of information and communication technologies and the increasing role of information for the individual, the growth of the "digital generation" is associated, for which smart devices and gadgets: smartphones, iPads, tablets and laptops using "advanced" technologies have become the main elements of living space (Amhag et al., 2019). Smart-community is a new quality of society, in which the combination of the use of technical means, services and the internet by trained people leads to qualitative changes in the interaction of subjects, allowing obtaining new effects - social, economic and other benefits for a better life.

2 Continuous improvement of education quality

The changes that have occurred in recent decades in the economy and culture of the most developed countries make us take a fresh look at the quality of the educational process. Quality is becoming one of the main goals of the development of education. Any restructuring of education aims at improving the quality of education. It is one of the main issues of modern pedagogy and society as a whole. The international competitiveness of universities is a national challenge. Currently, there is a tendency to turn leading universities into platforms not only of a scientific nature, but also for dialogue between business, society, and the state on issues of scientific and technological forecasting, the exchange of advanced knowledge, and the solution of global problems.

Today, the issue of improving the quality of education of computer science teachers in universities in Kazakhstan is becoming relevant. Continuous improvement of the quality of teachers' education is a consequence of the constant development of modern trends in education. To improve the position of Kazakh universities in world university rankings, it is important to effectively monitor the quality of the educational process of the entire university as a whole. The graduates of educational institutions in which the correct monitoring of the quality of education is introduced will always be in demand, and organizations also receive the highest ratings in world university ratings. This is one of the most important factors for students when choosing a university in which he will study. For example, the Times Higher Education and QS Rankings, which are today the most reputable academic university ratings, are considered the most prestigious academic ratings in the world. Basically, the rest of the world ratings usually refer to the information of the above ratings (Aguillo et al., 2010).

Quality management in educational institutions is defined as a dynamic process, so the issues of quality improvement of organizations are always relevant. The proper functioning of the institutions services and the quality of its services depend on the rational use and management of faculty resources. Monitoring the quality of education is a systematic observation, analysis, assessment and forecasting of the educational process, conditions and results, conditions and dynamics of the implementation of the contingent of students, a network of educational institutions (Tam, 2001). Monitoring the quality of education systematizes available sources, diagnoses the educational situation, as well as targeted research and

measurements. This is based on the collection, processing, storage and dissemination of information about the activities of the education system, as well as the satisfaction of internal and external consumers of educational services. Creating an effective educational process management system requires three goals:

- formation of target indicators of the quality of the educational process;
- an objective comparison of the achieved indicators and, accordingly, an assessment of the quality of the educational process;
- development of quality control measures, achieved in order to minimize deviations.

Ensuring the quality of education is a systemic problem, in the solution of which all areas of the universitys functioning should be involved. Only an integrated approach can lead to positive results and to achieve the goal of ensuring the high quality of education provided. In modern conditions of competition in the market of educational services, the leader can only be a university that is constantly involved in planning and quality management. In accordance with the complex characteristics of the educational activities of the university, we get own of quality ensuring of education in higher education institutions, which is presented below in Figure 1:

Fig. 1: Model of quality ensuring of education in higher education institutions

Based on the study, analysis of experience and this model, the principles of educational Kaizen were determined. This philosophy was discovered in Japan by Japanese quality management researcher Masaaki Imai. In 1986, he published a book "Kaizen: The Key To Japan's Competitive Success" in England, and in 1997, he published his second book "Gemba Kaizen: The Way to Lower Costs and Improve Quality". Imai emphasized that Kaizen-one of the main concepts of Japanese management-is the key to Japans competitive victory. Undoubtedly, its success has been demonstrated in many organizations around the world. Thus,

many teachers have tried the effectiveness of teaching and learning principles in their field of study.

Over the past decade, Kaizen strategies have been tested and applied by universities in the United States, the United Kingdom and other European countries, Asian universities and others. In general, the word "Kaizen" occurs in Japanese as 改善 or Kaizen and consists of two parts: "Kai" is "change", "Zen" means "good", literally translates as "continuous improvement" or "best change". Unlike other strategies, this system is focused on the process, not the result (Sapungan & Cuarteros, 2016). Kaizen, as continuous improvement, the creation of individual educational processes with continuously changing production requirements and ending with senior management, from the leader to the trainee and his customer. Improving actions and processes, the ideal goal of the educational Kaizen philosophy is to train a motivated specialist with high creative potential, able to survive in the selection processes and intensive training under high loads and intense competition. Educational Kaizen as a set of proactive project management, processes, information, knowledge and wisdom, human capital, training and learning, teamwork, life strategy of a creative person, predictive planning. Based on the foregoing, the main tasks of educational kaizen are determined:

1. Constant small changes in all areas of the educational institution - selection, training of students, their interaction with potential employers;
2. Constant small changes in all areas of the educational institution - selection, student training, their interaction with potential employers, personal and team relationships, planning, etc.
3. The transfer of a certain amount of authority to each employee thanks to continuous training in many specialties, constant mastery of new skills;
4. Development of self-discipline as the ability to control oneself with self-esteem and respect of both other people and the organization as a whole;
5. Identification and honest recognition of problems at all levels.

Currently, the experience of applying the principles of Kaizen in education is gaining a special status, but it is already widely used in the workplace for a long time. When implementing this approach in education, we must take into account the difference between the use of this approach in production and in education. Since the peculiarity of applying Kaizen in the learning process is by transforming the University's activities based on the position of continuous and consistent improvement of the educational process, that is, it is a constant improvement in the quality of students learning through the use of innovative methods and learning tools that are implemented by teachers and supported by the University administration.

To solve the successful use of Kaizen in education we need to find answers to the following problems:

- how can we meet the standard of student learning;
- how a teacher can acquire a new Kaizen skill and use it in their teaching activities.

This approach is a theoretical and methodological basis for creating the concept of continuous training of computer science teachers to implement modern technologies of training and development of personal qualities of teachers. Improving the training of computer science teachers should be carried out in accordance with modern requirements and aimed at the formation of a self-developing personality with creative thinking and creativity. You can use innovative teaching methods, such as using an Iphone, Ipad, or smartphone, or using Internet resources to attract students attention and motivate them to learn. To prepare for homework, send them media content, electronic textbooks, and to improve the quality of the educational process, students can use the type of co-education or peer participation through social networks

that young people like. Active use of modern information and communication technologies in the educational process improves its quality. Providing a modern level of educational services is facilitated by the combined Internet resource of the educational institution, which hosts educational Internet resources used in teaching activities created by teachers.

When implementing these innovations in education, we must not forget about traditional teaching methods, as well as universal quality control, all stages must comply with the concept of "Just-in-Time". This system is the most common logistics concept in the world, the main idea of the concept is as follows: if the schedule for the process is set, it must be organized on time. In conditions of continuous improvement of the quality of education, the teacher must promptly eliminate errors and shortcomings of the educational process. Learning from this concept has a number of advantages that allow you to manage the learning process:

1. the most objective way is to set up an experiment, that is, to apply a new method of learning and analyze the results.
2. conducting an assessment based on the goals set. As with any training method, the introduction of this type of training initially has certain goals.
3. An experiment involving the comparison of data before and after implementation of training is also very useful. For example, it can be an analysis of data on semester grades.

Implementing the Kaizen approach requires creativity and perseverance on the part of the teacher. Equally important are the motivations that teachers should give to students who can also participate in the process of continuous improvement of their studies. Teachers can search for students ' needs through feedback, as well as through individual consultations and group discussion. Training with small groups allows each student to work in a team, that is, the student is forced to think not only about their own good, but also about the good of those who work next to them. Therefore, learning in collaboration creates conditions for positive interaction between students in the process of achieving a common goal.

Given the current modernization of learning, the Foundation for learning is known as continuous improvement, where the teacher and students are always looking for new ways to improve the system to increase the enjoyment of learning. As written in the book "the Learning revolution" by the authors who are Janet Vos and Gordon Dryden proved that this approach in the education system has an optimistic effect. The significant results have been evident in the Mt. Edgecumbe High School, Alaska, in Sitka, the school that pioneered Total Quality Management or TQM and Kaizen in America. Analyzing the data from these studies the following indicators were obtained:

- Students have created several pilot projects;
- Students simultaneously studied different programs for creating projects, as well as learned foreign languages, quality control, statistical analysis, marketing, business skills, and much more;
- Teachers and students are considered co-managers because they set their own goals and implement plans together;
- Joint elimination of interference and solving their problems;
- Improving student self-esteem;
- Increasing the motivation to work of all participants in the study.

The content of the continuous improvement strategy is determined by the following main components:

- focus on the constant reduction of all types of costs, which is aimed at a constant increase in the effectiveness of the university and the reduction of costs;

- rational organization of working places, allowing to achieve maximum discipline, efficiency and productivity of labor;
- stabilization and support of the results obtained in the standardization of work, improvement of disciplines and teaching process.

In general, thanks to Kaizen's strategy, the activities of future computer science teachers in the field of higher education are constantly improved and the principles of their work are effectively organized. For this future computer science teacher will share their suggestions with their colleagues and encourage them to solve problems quickly. In the opinion of the Japanese, it is not necessary to expect much from the proposals discussed at the first stages of the strategy, and even more so to add to this process the maximum number of employees. As the approach to continuous improvement becomes an integral part of the corporate culture, the number of proposals will be of high quality and will provide a long-term priority for the university (Topolsky, 2017).

Achieving excellence in learning is not easy, but using Kaizen approaches, computer science teachers will be able to achieve them. Teachers must have new equipment in order to improve the quality of the educational process. All lessons should be well organized and planned, taking into account the student's level of intelligence, learning style and interest. Since the main task of the teacher is to ensure the proper provision of the educational process, as well as conducting educational, scientific and educational work, they must be prepared for various problems in the training process. Teachers should be fully aware of the needs of students who have changed their learning preferences in this new wave of technology modernization. Everyone knows that today many students prefer to sit a large amount of time with their mobile phones, instead of listening to the instructions of the teacher. Creating innovative projects, the teacher should motivate the student to work, at the same time, he should focus not on the result, but on the preparation process. Controlling the quality of each stage will allow you to achieve the desired results.

In justifying the effectiveness of Kaizen principles in the areas of teaching and learning by confirming implementation in education by other universities, some difficulties can be identified in implementing the Kaizen approach:

- improving educational processes requires a lot of time;
- difficulty in involving employees of all levels and students;
- problems of a financial nature, such as the need to replace equipment in computer classes, the purchase of new equipment;
- prevent human factors - laziness, greed, dishonesty;
- weak motivation to work.

Based on all the data during the implementation of this approach, the main classification of the problems that arise when introducing Kaisen into education will be presented. And also recommendations will be offered to eliminate the identified problems, which will allow this institution not only to follow the principles of Kaisen, but also to build a new managerial model focused on continuous improvement of quality and development.

In order to effectively improve the quality of students' education, it is necessary to use the innovative areas of education that provide it. One of such innovative areas of education is the 5S workplace organization system. One way to optimize workplace improvement efforts is to ensure that the 5S system aims to efficiently organize the workplace by reducing and eliminating all costs. It consists of five simple time-saving and efficient principles. Translated from Japanese, Seiri (整理) means sorting, Seiton (整頓) means regulation, Seiso (清掃) means precision, Seiketu (清潔) means standardization, and Shituke (躾) means improvement. This system implements specific principles aimed at identifying and eliminating costs to improve

productivity and the quality of education. This system requires you to make changes once, and as a result get a significant improvement over a longer period of time. The 5S system is a springboard for scientific research, which suggests that the Kaizen principles can also manifest themselves in the academic environment, can be demonstrated by teachers and leaders in universities in an attempt to improve the quality of student learning. The purpose of the 5S system is to improve the quality of education and reduce the number of problems, create a comfortable psychological mood and stimulate students interest in education and work. The 5S system is based on the Kaizen philosophy, which means "continuous improvement" (Kabiesz & Bartnicka, 2019).

3 Conclusion

Today, many higher education institutions in the world use modern international systems for assessing the quality of education and modern methods of teaching in higher education, which allows you to compare the level and quality of education of students in different countries of the world, as well as to identify differences in national education systems. In order to effectively improve the assessment of the quality of students' education, innovative educational trends should be used to ensure the improvement of the quality of education. Important elements that influence quality are, in particular, teachers, methodology and the environment, which can also be interpreted as elements of the learning process. Therefore, it makes sense to take a closer look at the educational process of the lesson in computer science and evaluate them in terms of quality (Passey, 2016).

Today, the countrys society is focused on dynamic socio-economic development. An important factor in this development is education, since in the 21st century everyone should be aware of various fields of science, as well as have the skills of self-education and selfimprovement. In this regard, the future society will depend on the quality of the system of preparing future teachers for higher education, its intensity and mobility. Therefore, improving the quality of education of computer science teachers through Kaizen philosophy is relevant. In addition, the philosophy of educational Kaizen can be used for almost all areas and levels of training. We must advocate for continuous improvement of the quality of our positions, that is, as leaders of quality teaching, we must take into account the important role of organizing continuous quality improvement to achieve the effectiveness of educational services.

Resources

Aguillo, I. F., Bar-Ilan, J., Levene, M., & Ortega, J. L. (2010). Comparing university rankings. *Scientometrics, 85*(1), 243-256. doi:10.1007/s11192-010-0190-z

Amhag, L., Hellström, L., & Stigmar, M. (2019). Teacher Educators' Use of Digital Tools and Needs for Digital Competence in Higher Education. *Journal of Digital Learning in Teacher Education, 35*(4), 203-220. doi:10.1080/21532974.2019.1646169

Kabiesz, P., & Bartnicka, J. (2019). 5S system as a manner for improving working conditions and safety of work in a production company. *Multidisciplinary Aspects of Production Engineering, 2*(1), 496-507. doi:10.2478/mape-2019-0050

Passey, D. (2016). Computer science (CS) in the compulsory education curriculum: Implications for future research. *Education and Information Technologies, 22*(2), 421-443. doi:10.1007/s10639-016-9475-z

Sapungan, R. M., & Cuarteros, J. (2016). Improving Teaching and Learning through Kaizen and 7th Habit. *Journal of Advances in Social Science and Humanities, 2*(4), 1-7. doi:10.15520/jassh24

Tam, M. (2001). Measuring Quality and Performance in Higher Education. *Quality in Higher Education, 7*(1), 47-54. doi:10.1080/13538320120045076

Topolsky, L. (2017). Kaizen Means Developing Abilities. In *Kaizen Teian 2 Guiding Continuous Improvement Through Employee Suggestions* (pp. 3-12). New York: Routledge. doi:doi.org/10.1201/9780203749739

SUBJECT-LANGUAGE INTEGRATED LEARNING AS THE BASIS FOR PREPARING FUTURE COMPUTER SCIENCE TEACHERS

Saniya Nariman[11], Aitugan Alzhanov[12], Igor Vostroknutov [13]

Abstract
The key position for the successful promotion of trilingual education in the Republic of Kazakhstan is the choice of the optimal teaching method, which is the internationally recognized technology of integrated language and subject teaching, known as CLIL technology. The article discusses the Kazakhstan's model of trilingual education and the CLIL technology - as the optimal technology in promoting the ideas of trilingualism in the educational process. The methodology of subject-language integrated teaching acts as the main tool for teaching languages to future teachers of computer science. The experience of the Eurasian National University and other universities in creating CLIL courses is considered.

Key words
Trilingual education, target languages, educational process, CLIL technology, integrated approach, computer science teachers

1 Introduction

Trilingual education as a priority for the strategic development of education in the Republic of Kazakhstan is a subject of discussion not only for academia, but also for the general public. This is due to the phased implementation of trilingual education in all types of secondary educational institutions of the Republic of Kazakhstan, starting in 2015. The problems of scientific and methodological support for trilingual education in Kazakhstan are the works of such scientists as Zhetpisbayeva B.A., Aitbayeva B.M., (Aitbayeva et al, 2015, Kubeeva et al, 2017).

Many linguists and teachers believe that the basis of trilingual (multilingual) education should be a properly structured system of teaching target (three) languages, corresponding to the real situation of the development of scientific and methodological base of Kazakh, Russian and English languages (Shelestova, 2016, Mukatova et al, 2015).

As part of the updated educational content of the Republic of Kazakhstan, regardless of the language of instruction, some subjects are taught in English in the main school. In this regard, there is a need to apply new educational technologies for teaching English to future specialists. One of these technologies is the subject-language integrated learning CLIL (Content and Language Integrated Learning).

Currently, in Kazakhstani universities, in particular at the Eurasian National University, there is quite an active introduction of courses based on integrated subject-language training (hereinafter CLIL), combining the development of a foreign language with the mastery of professional competencies. However, it is too early to talk about a clearly defined practice of using CLIL technology, which allows to increase the effectiveness of the educational process.

[11] L.N. Gumilev Eurasian National University, Faculty of Information Technology, Department of Informatics, Kazakhstan, Nur-Sultan, saniya_khairova@mail.ru
[12] L.N. Gumilev Eurasian National University, Faculty of Information Technology, Department of Informatics, Kazakhstan, Nur-Sultan, alzhanov_ak@mail.ru
[13] Moscow City Teacher Training University, Department of Informatics and Applied Mathematics, Institute of Digital Education, Russia, Moscow, vostroknutov_i@mail.ru

This article discusses the experience of implementing CLIL courses in the preparation of future informatics teachers at the Eurasian National University (hereinafter referred to as ENU).

2 Trilingual education as a priority for the strategic development of education in the Republic of Kazakhstan

The methodology of trilingual education in modern conditions is determined, first of all, by historical and socio-pedagogical prerequisites. The first of them are due to the fact that:

1 the linguistic situation of Soviet Kazakhstan historically defined Russian-Kazakh (not Kazakh-Russian) bilingualism, therefore, the scientific and methodological basis for teaching Russian as a mother tongue and as non-native has a high level of sophistication;
2 before independence, the share of schools with the Russian language of instruction in which the Kazakh language was not studied significantly prevailed in Kazakhstan, such a peripheral position of the Kazakh language became a deterrent to the development of its functional activity and provoked a shortage of pedagogical experience in teaching the Kazakh language, including how non-native language;
3 the announcement of the state status of the Kazakh language and the real level of its functional use made it possible to increase the amount of study time in standard curricula, however, the lack of theoretical and applied studies of the linguodidactic aspects of the Kazakh language still does not allow to strengthen its scientific and methodological base;
4 the current linguistic situation is complicated by the fact that in the space of the Kazakh community, with the dominance of Russian speaking, English is actively entering, which requires study in the amount necessary for integration into the global economy (Zhetpisbayeva, 2014).

All the above positions became prerequisites for the realization in Kazakhstan of the idea of the trinity of languages, which is expressed by the following formula: we develop the state language, support Russian and study English (Nazarbaev, 2007).

The peak of this triangle is the Kazakh language as a leading factor in the consolidation of the people of Kazakhstan. This strategy is the basis of the Kazakh model of trilingual education, and it also determined the choice of target languages: Kazakh (I2), Russian (I2), English (I3). In the educational process, I2 is the Kazakh language in schools with a non-Kazakh language of instruction, I2 is the Russian language in schools with a non-Russian language of instruction, and I3 is English as a foreign language (I3 according to the standard curriculum).

The strategic goal of trilingual education is to create the necessary conditions for the simultaneous mastery of the three target languages by students in accordance with international standards, namely: - the Kazakh language as the state language, whose knowledge contributes to successful civic integration; - Russian language, which is used officially on a par with the Kazakh language; - English as a means of integration into the global economy.

3 CLIL technology - as an optimal tool for teaching languages to future informatics educators

As part of the updated educational content of the Republic of Kazakhstan in 2019, regardless of the language of instruction, in the main school the subjects “Kazakh language and literature” and “History of Kazakhstan” are studied in Kazakh, subjects “Russian language and literature” and “World history” - in Russian language, and in high school subjects "Natural Sciences", "Computer Science", "Physics", "Chemistry", "Biology" - in English.

In this regard, it becomes necessary to use new educational technologies for teaching foreign languages in the preparation of future teachers of certain specialties, in particular future teachers of computer science. One of these technologies is the subject-language integrated learning CLIL (Content and Language Integrated Learning).

CLIL technology acts as the optimal technology in promoting the ideas of trilingualism in the educational process and teaching languages to future informatics educators. CLIL technology is used as the main tool for teaching target languages in the training of future specialists. The use of this technology involves the development of a whole cycle of teaching aids and recommendations, special courses in the framework of educational programs of pedagogical specialties of various universities, and teacher training programs.

The entire CLIL target setting can be concluded in "4C" (content, cognition, communication, culture) (Coyle et al, 2010).

Content - implies the implementation of the content component not only through the acquisition of knowledge and skills, but also in the process of creating by students their own knowledge, understanding and development of skills (individual learning).

Cognition (cognitive abilities) - that is, the substantial component is associated with the development of a creative approach, a broader way of thinking and various ways of processing knowledge in the learning process. That is why in the classroom it is necessary to use texts for analytical and critical reading, assignments for isolating the main thing, juxtaposing, guessing, finding cause and effect relationships, etc.

Communication - a foreign language is studied through communication, rebuilding content and related cognitive processes. Therefore, the language must be clear and accessible. Moreover, interaction in an educational context is of paramount importance for learning. Communicative tasks for oral and written communication in a foreign language (interactive, group tasks, work in pairs, all kinds of creative and developmental exercises, use of the language in various activities) should prevail in the classroom.

Culture (cultural knowledge) - intercultural knowledge is the basis of CLIL, since an understanding of the characteristics, similarities and differences of individual cultures will help students more effectively socialize in a modern multicultural space, better understand their own culture and stimulate its preservation and development.

A distinctive feature of the CLIL methodology is its integrated approach to the content of the subject and language. It integrates the content and language when studying a subject through a foreign language and by virtue of learning a foreign language through the content of the subject. Using CLIL allows you to develop intercultural communication skills; to form a trainees' international worldview, which implies the equality of different nations and nationalities, advocating friendly relations between them; give the opportunity to consider the subject from different points of view; gain access to special terminology in a foreign language; to increase the competence of the language being studied; develop oral communication skills; diversify the methodology of the taught subject; increase student motivation.

CLIL technology is maximally aimed at the formation of the following language competencies:

- receptive skills (listening and reading);
- vocabulary;
- morphological knowledge (structure of linguistic units, such as morphemes);
- fluency and volume of colloquial speech. In addition, students have a large stock of scientific terminology and a wide academic vocabulary.

4 The experience of the Eurasian National University in creating CLIL courses

Currently, Kazakhstani universities are quite actively introducing courses based on integrated subject-language training (hereinafter CLIL), combining the development of a foreign language with the mastery of professional competencies. However, it is too early to talk about a clearly defined practice of using CLIL technology, which allows to increase the effectiveness of the educational process.

The specificity of CLIL courses consists in choosing the right balance between the level of difficulty of the content and the linguistic means of expressing it, that is, between professional and linguistic competencies, the increase in language complexity should be compensated by a decrease in subject complexity and vice versa. This balance is achieved by careful planning and selection of content that has linguistic potential, as well as at the same time a range of choice of language structures that are most typical for a particular subject area.

As one would expect, when implementing CLIL-training at ENU, the personnel issue turned out to be the most acute. The only criterion for the selection of teachers was the availability of a certificate in a foreign language for teachers, indicating the assignment of level B2 to them on the pan-European scale of competence in a foreign language.

Observations conducted at the ENU showed that the lack of linguistic training of the teacher (his insufficient knowledge of the specifics of technical translation, the construction of English phrases and terminology) forced him to constantly switch to his native language or the language of instruction, which, in turn, led to a distortion of the learning goal and failure (by default) students use a foreign language as a communication tool. Thus, all the mental processes of students were carried out in the language of instruction, and not in a foreign one. In addition, the language level of a foreign language was sometimes higher among students than that of a teacher. It seemed that the latter was not sure about the content of the course being taught regarding the content being mastered. For this reason, students did not understand the meaning and purpose of the lesson in a foreign language and showed weak activity.

Teachers conducting classes in a foreign language mainly explain concepts and terms, without observing the principle of normalizing language material. In other words, there is no semantic analysis of the text with the provision of language material in a functional form. This lesson is more consistent with EMI-training (English as a Medium of Instruction) and only partially - CLIL.

In our opinion, the basic principles for the successful and thorough implementation of CLIL courses are:

• A good training base: training materials should be authentic, informative, information rich. New texts and assignments should carry a certain degree of cognitive load. It is interactive authentic materials that can be used to create a language environment and tasks with a high degree of cognitive difficulty. It can be videos, flash animations, web quests, podcasts or other interactive learning resources of foreign language sites. They may contain creative tasks, materials for independent and differentiated training.

Active support and assistance of the teacher in the learning process: to successfully achieve the goals set, the teacher must provide the student with the necessary assistance, which gradually decreases as his foreign language competence develops. This will reduce the cognitive and linguistic loads when studying unfamiliar material in a foreign language. All assignments should have explanations. Much attention is paid to productive types of speech activity (speaking and writing). • Intensive and productive knowledge of a foreign language: a variety of teaching methods will contribute to active authentic communication in the framework of classes, as foreign language training is most successful in the presence of communicative goals and a significant communication situation.

Multiculturalism: the CLIL methodology makes it possible to consider the material, given the differences in the perception of many things by representatives of different cultures.

Sustainable learning: Learning should involve the long-term memory of students (Meyer, 2010).

Undoubtedly, the success of this technique directly depends on the teacher and his pedagogical and didactic approaches. So, if the teacher sees that the students are overloaded, it is difficult for them to perceive the material being studied, they must adapt the foreign language in which the material is presented, reduce the speed and intensity of the study, use visualized teaching aids, etc., since the thinking process in a foreign language takes more time.

In addition, the teacher should not forget that CLIL works on the principle of interaction in the audience, so listening and speaking should be balanced.

The teacher should avoid a negative assessment of the student's speech. It is necessary to create a comfortable environment for verbal communication of a trained audience. It should be understood that the CLIL technique is based on the use of not only printed authentic material, but also video and audio resources with the activation of a professional glossary, on the use of a variety of visual material on the specialty being studied in a foreign language, including the actual foreign language, on the use of educational technologies such as discussion, debate, various types of pair / group work, etc., on a rich test base with various types of test tasks (to choose one or more x answers, to restore consistency, to establish correspondences, to fill in gaps; crosswords), which allows both the teacher and the teacher to control their activities.

In scientific works on this technique, it is often noted that "the teacher must first of all be a specialist in this professional field, since the subject matter is the dominant principle of CLIL. And then, of course, a high level of knowledge of a foreign language is assumed (ideally, the teacher has additional linguistic qualifications), therefore, special attention should be paid to the foreign language training of not only students, but also teachers (Karipidi, 2015).

Thus, subject-language integrated learning allows realizing the main goal of studying a foreign language in higher education, namely: to develop practical skills in using a foreign language in situations of everyday academic (educational) communication, i.e. master the general linguistic, educational and professional communicative competencies. This technique provides students, undergraduates, doctoral students and teachers with the opportunity to use knowledge of a foreign language in the process of studying other university subjects, thereby increasing their confidence in knowledge of a foreign language, removes the language barrier in communication and promotes the growth of motivation in mastering foreign language competencies.

5 Conclusion

In our opinion, we can speak about the effectiveness of the Kazakhstan model of trilingual education only if all three target languages in the educational process will develop not in competition but in unity.

In this case, the main tool for teaching target languages is the integrated teaching of subject and language (CLIL technology). A properly organized educational process of teaching three languages in accordance with the principles of the Kazakh model of trilingual education is able to overcome the hidden or open opposition to multilingual education.

We can say with confidence that the CLIL technology acts as the optimal technology in promoting the ideas of trilingualism in the educational process and is used as the main tool for teaching target languages in the preparation of future informatics teachers.

The use of this technology involves the development of a whole cycle of teaching aids and recommendations, special courses in the framework of educational programs of pedagogical specialties of various universities, and teacher training programs.

Thus, at the current stage of reforming the education system of the Republic of Kazakhstan, there are all prerequisites for the effective implementation of the Kazakhstani model of trilingual education and the effective application of CLIL technology in higher education.

Resources

Aitbayeva, B., Akzhunusova, N., Gornaya, A. Kadina, Z., & Sateeva, B., (2015). Rol i mesto gosudarstvennogo iazika v poliyazichnom obrazovanii Respubliki Kazakhstan [Role and place of state language in multilingual education of Kazakhstan]. *Aktualnye problemy gumanitarnyh i estestvennyh nauk* [Actual problems of the humanitarian and natural sciences]*, Moskva, 12*(1), 121–123. ISSN: 2073-0071

Coyle, D., Hood, P., & Marsh, D. (2010). *CLIL: Content and language integrated learning*. Cambridge: Cambridge University Press.

Karipidi, A. (2015). The Principles of Content and Language Integrated Learning and Forming of Foreign Language Communicative Competence of the Students of Non-Linguistic Higher Educational Institutions. *Foreign Languages: Linguistic and Methodological Aspects, 31,* 35-39.

Kubeeva, A., Syrymbetova, L., & Zhetpisbayeva, B., (2017). K voprosu podgotovki pedagogov dlia mnogoyazychnogo obrazovania v Kazakhstane [On the issue of training teachers for multilingual education in Kazakhstan]. *Aktualnye problemy filologii i metodiki prepodavania inostrannyh iazykov* [Actual problems of philology and methods of teaching foreign languages]*, 11*, 168–172.

Meyer, O. (2010). Towards quality-CLIL: successful planning and teaching strategies. Pulse, 33, 11-29.

Mukatova, M., Syrymbetova, L., Tastanova, A. & Zhilbayev, Z., (2015). Sovremennoe pedagogicheskoe obrazovanie v Kazakhstane: vozmozhnosti dlia razvitia [Modern teacher education in Kazakhstan: opportunities for development]. *Nauchnyi almanakh* [Scientific Almanac]*, 10-2* (12), 183–191.

Nazarbaev, N. (2007). *A new Kazakhstan in a new world: Address by the President of the Republic of Kazakhstan Mr. Nursultan Nazarbayev to the people of Kazakhstan*. Astana: Publisher not identified.

Shelestova, T., & Zhetpisbayeva, B. (2016). Empiricheskie predposylki rannego obuchenia angliiskomu iazyku v shkolah Kazakhstana v ramkah sovremennoi praktiki trehiazychnogo obrazovania [The empirical prerequisites for early learning of English in schools of Kazakhstan in the framework of modern practice of trilingual education] *Aktualnye problemy filologii i metodiki prepodavania inostrannyh iazykov* [Actual problems of philology and methods of teaching foreign languages]*, 10,* 153–162.

Zhetpisbayeva, B. (2014). K voprosu o teoretiko-metodologicheskoi konceptualizacii poliyazychnogo obrazovania [To the question of theoretical and methodological conceptualization of multilingual education]. *Aktualnye problemy filologii i metodiki prepodavania inostrannyh yazykov* [Actual problems of philology and methods of teaching foreign languages]*, 8,* 127–135.

INDIVIDUAL OR GROUP PROJECT ASSIGNMENT IN BUSINESS PROCESS MODELLING AND SOFTWARE ENGINEERING COURSES?

Martin Misut[14], Maria Misutova[15]

Abstract
The paper describes the research aimed at investigating the impact of different ways of project assignment (group / individual assignment) on the success of FHI engineering students in IT courses: Software Engineering (SWE) and Business Process Modelling (MPP). The research described is part of extensive research, whose main objective was to determine the impact of the proposed teaching model, with an emphasis on the development of teamwork, autonomy, social skills and critical thinking of students, on their outcomes.

The research had two primary objectives. The first was to find out whether applying different forms of project assignment (group / individual assignment) has a statistically significant effect on the success of students in the subject. The second objective was to find out whether there is a statistically significant difference in the success rate of men and women in the studied informatics subjects also, whether the application of different forms of project assignment influences the success of men and women in solving the final test.

An educational test was used to answer the research questions. It contained 40 tasks of different types: open, multiple-choice and dichotomous. The test was created in MOODLE. Students passed the test in a computer room online under the supervision of a teacher. T-test and Multiple Linear Regression Analysis using SPSS were used for statistical verification of established hypotheses.

The results obtained indicate that applying different forms of project assignment has a statistically significant impact on the success of students in the subject. The results further confirmed that there is no statistically significant difference in the success rate of men and women in the studied IT subjects. There was no statistically significant difference between men and women in the success of working in the project. However, it was surprising that in the academic test, women achieved higher scores than men, and the difference was statistically significant.

The obtained results were analysed, and the results of the analysis will be used in the modification of the proposed model of teaching computer science subjects.

Keywords
Project assignment, group project assessment, software engineering, business process modelling, teaching model

1 Introduction

The research, described in this paper, is a part of extensive research. The main aim of that research is to design and verify a model of teaching computer science subjects with an emphasis on developing team problem-solving, collaboration, creativity, independence, social skills of students and critical thinking. Different forms and methods of teaching can be used to stimulate

[14] University of Economics in Bratislava, Faculty of Economic Informatics, Department of Applied Informatics, Bratislava, SLOVAKIA, martin.misut@euba.sk

[15] Slovak University of Technology, Faculty of Materials Science and Technology, Institute of Applied Informatics, Automation and Mathematics, Trnava, SLOVAKIA, maria.misutova@stuba.sk

students to take an active role in the learning process. Effective teaching methods contribute to strengthening the internal motivation of students to improve continually. The methods used in the model encourage students to participate actively in learning, which is also reflected in the evaluation of learning outcomes.

Project teaching has long been useful in preparing students for professional activities. (Orszaghova, Horvathova, & Greganova, 2017) Software engineering projects enable students to gain experience in project management, team management and professional communication. (Broman, Sandahl, & Abu Baker, 2012) On the other hand, project teaching is difficult, especially for assessing student performance in terms of educational outcomes. (Tothova, Semelakova, Hostovecky, & Fabus, 2017)

The practice has shown that teaching software engineering through projects is trendy and widespread. (Dietsch, Podelski, Nam, Papadopoulos, & Schäf, 2013) There are two reasons why this happens. Firstly, teaching organised in the form of group projects reminds of the real conditions of future employment of students and, at the same time, this way of teaching enables the students to develop soft skills in addition to teaching expert knowledge. Soft skills are an essential part of the knowledge and skills of a sound software engineer. Teaching organised through group project assignments thus also develops students' ability to cooperate, communication skills, management and organisational skills. The literature reports several strategies for addressing project-based learning experiences in software engineering courses, such as the development of hypothetical and real software products. (Heredia, Palacios, & de Amescua Seco, 2015)

Teaching through group projects, however, poses, in addition to indisputable positives, also one problem: how to assess the individual contribution of each student to a common outcome. Assessment is fundamental to student learning and achievement (Medland, 2016). Knowledge assessment is an immanent component of education and does not only provide the evaluation of student progress, but also it provides feedback and educational process reflection (Misut & Misutova, 2017). A potential assessment problem here is that grades are mostly based on group evaluation, i.e. there is one mark for the whole group. Strictly individual assessment and grading may, on the other hand, result in too much personal focus, thus sacrificing the common group goal of producing a high-quality product. As a consequence, proper assessment techniques must balance between individual and group assessment aspects. (Vasilevskaya, Broman, & Sandahl, 2015)

There are several suggestions on how to deal with this problem. For example, Broman (Broman et al., 2012) suggests extending the group's assessment with individual selfassessment, assuming that combining a group assessment with a personal evaluation would provide better classification and would maintain the motivation of students to work together as one group. Another option for supporting students during these learning experiences is implementing instances of peer assessment, where students anonymously evaluate the performance of their teammates and provide feedback to help their peers overcome conflicts and limitations (Marques, Ochoa, Bastarrica, & Gutierrez, 2018).

The primary purpose of evaluation activities is not only to assess student performance for their classification (summative assessment) but also formative assessment, which means that the evaluation activity should provide students with feedback to improve their learning. Both summative and formative assessments are essential but can be hard to combine. As states Vasilevskaya (Vasilevskaya et al., 2015), it is tough to find a single assessment activity that balances between individual and group assessment, involves both teachers and students, and is summative as well as formative.

That is why we have introduced several evaluation activities in both subjects (Software Engineering (SWE) and Business Process Modelling (MPP)). Proposed activities should together evaluate the student's work during the semester, but also give him feedback when

working on the project and thus shape his knowledge and skills. Both the teacher and the students are involved in the evaluation process. The main differences between the applied models of teaching both subjects are that within the software engineering subject the project is assigned to a group of students, within the MPP subject students work on the project individually. In each milestone, group projects are also defended in public defence meetings. To evaluate the applied teaching models for further improvement, we wanted to know whether the form of work on the project affects the students´ results achieved. Also, whether the impact of the way of work on the project will be the same for both genders and, if not, how it differs for the group of women and men. This paper answers these above-stated questions.

2 Problem definition and Methodology

The proposed model of education was verified in the teaching of Software Engineering (SWE1, SWE2) and Business Process Modeling (MPP) courses at FHI EU Bratislava. The teaching model 40-60 was applied in the teaching of these subjects. Thus, the overall evaluation of students consisted of their assessment during the semester (40%) and the final evaluation in the form of a test (60%). During the semester, each MPP student individually elaborated one project (individual project assignment). In the SWE subjects, students were divided into 4member working groups. Each group worked on a joint project (group project assignment). In all subjects, the score during the semester consisted of points for the project and points for the assessment of other students´ works. Each student was motivated to evaluate projects through points for assessment. In the end, the teacher corrected the students´ assessment of other students´ projects. A detailed description of the proposed teaching model can be found in (Misutova & Misut, 2020)

The research had two primary objectives. The first was to determine whether applying different forms of project assignment (group / individual assignment) has a statistically significant effect on the success of students in the subject. Moreover, whether or not, applying different forms of project assignment (group / individual assignment) has a statistically significant impact on the success rate of the male group and the female group.

We set out the following working hypotheses:

Hypothesis 1: Applying different forms of project assignment has a statistically significant impact on the successfulness of students in the subject.

Hypothesis 2a: Applying different forms of project assignment has a statistically significant effect on successfulness in the group of men in the subject.

Hypothesis 2b: Applying different forms of project assignment has a statistically significant effect on successfulness in the group of women in the subject.

The second objective was to find out whether there is a statistically significant difference in the success rate of men and women in the studied IT subjects also, whether the application of different forms of project assignment influenced the success of men and women in solving the final test.

We set out working hypotheses:

Hypothesis 3a: There is no statistically significant difference in the successfulness of men and women in the monitored IT projects.

Hypothesis 3b: There is no statistically significant difference in the successfulness of men and women in the final test.

Hypothesis 3c: There is no statistically significant difference in the successfulness of men and women in the solution of the project.

T-test using SPSS was used to verify hypotheses 3a, 3b and 3c.

To verify the first two hypotheses, i.e. to determine the effect of an independent variable - a different form of project assignment (group / individual assignment) on the dependent variable - success in SWE and MPP as expressed by the total score achieved, we used Multiple Linear Regression Analysis using SPSS. We compiled the equation of the model in which we used the independent control variables - successfulness in the final test and an independent variable - project.

$$y=\beta_1 x_1+\beta_2 x_2+\beta_3 x_3 \quad (1)$$

Where y - is a dependent variable of the continuous type = total score of the subject = number of points achieved during the semester + amount of points from the final test.

x_1 - is an independent variable of the continuous type = score of the final test; it takes values from 0 to 60. The final test contained 40 tasks. The tasks were of different types: open, multiple-choice, dichotomous. Students have passed the final examination in a computer classroom online. The allowed time of solving the test was 1 hour in the subjects SWEI and SWEII, in the subject MPP 1.5 hours.

x_2 - is an independent variable of continuous type - the number of points achieved during the semester from the project (points for project development and points for evaluation of assigned projects), it has values from 0 - 40.

x_3– is an independent nominal / dichotomous type variable; it has value one in case the project was solved individually and four if the group solved the project.

Dependent and independent variables are listed in Table 1. The source of data was the AIS academic information system.

Tab. 1: Variables of model

Variable	Code	Proxy/Measurement	Source	Expected sign
Dependent variable				
Success in the subject	Course_score	Total points (0-100)	AIS	
Independent variables				
Success in the final test	Test_score	Number of points in the final test (0-60)	AIS	+
Project success	Project_score	Number of points from the project (0-40)	AIS	+

Source: own work

The data consisted of the results of FHI EUSA students in the courses MPP, SWE I and SWE II in two consecutive academic years 2017/18 and 2018/19, of which 92 were women results and 160 were men results. The following tables (Table 2 – 3) contain descriptive data statistics.

Tab. 2: Descriptive statistics of data

Project Assignment		N	Minimum	Maximum	Mean	Std. Deviation	Variance
1	Course_Score	67	62	100	78,37	9,196	84,571
	Test_Score	67	30,8300	58,0000	43,884478	7,2346247	52,340
	Project_Score	67	21,4000	37,1100	32,365522	3,3166135	11,000
	Valid N (listwise)	67					
4	Course_Score	185	55	100	77,72	9,558	91,353
	Test_Score	185	26,3300	59,4000	43,694811	6,7821170	45,997
	Project_Score	185	6,8400	43,4800	32,708432	4,6906509	22,002
	Valid N (listwise)	185					

Source: own work

Tab. 3: Descriptive statistics of data

Sex		N	Minimum	Maximum	Mean	Std. Deviation	Variance
M	Course_ Score	160	56	100	76,39	8,744	76,454
	Test_ Score	160	26,3300	57,2700	42,707625	6,3772752	40,670
	Project_ Score	160	20,0000	43,4800	32,249250	4,1473454	17,200
	Valid N (listwise)	160					
W	Course_ Score	92	55	100	80,51	10,090	101,813
	Test_ Score	92	30,8300	59,4000	45,549783	7,3986500	54,740
	Project_ Score	92	6,8400	40,0000	33,257283	4,6715816	21,824
	Valid N (listwise)	92					

Source: own work

It is necessary to test normality when using Multiple Linear Regression Analysis. We used the Kolmogorov-Smirnov Test of Normality using SPSS. Based on the results, it can be concluded that the data are normally distributed for both forms of project assignment. Table 4 shows the values of Asymp. Sig. for all variables are higher than 0.05.

Tab. 4: Results of the Kolmogorov Smirnov Normality Test using SPSS

Project_Assignment	Course_Score	Test_Score	Project_Score
1	,600	,696	,052
4	,234	,563	,389

Source: own work

When using Multiple Linear Regression Analysis, it is also necessary to test linearity. The relationship between independent variables Course_Score and the dependent variables

Test_Score and also Project_Score is linear. The value sig. Deviation from Linearity is 0.971 and 0.068. Both values are higher than 0.05.

Multicolinearities should also be tested. The VIF value for both Test_Score and Project_Score is 1.011, so there is no multicollinearity. Finally, we did the scatterplot graphic heteroskedasticity test. There is no clear pattern and spreading dots. It can be concluded that there is no heteroscedasticity problem. Therefore, the use of Multiple Linear Regression is correct.

3 The results

Table 5 shows the Multiple Linear Regression Analysis results. Table 5 also shows the results for the control variables: success in the final test and the success of the project. Both have a statistically significant effect on successfulness in the course.

Tab. 5: Results of Multiple Linear Regression Analysis

Variables	All students	Man	Woman
Test_Score	+0.000	+0.000	+0.000
Project_Score	+0.000	+0.000	+0.000
Project_Assignment	-0.044	-0.044	

Source: own work

The outputs of Multiple Linear Regression Analysis using SPSS are briefly described below. Coefficient of determination (R square) is 0. 91 for all students, 0.906 for men and 0.907 for women. This suggests the notion that dependent variable y– course successfulness is influenced by 91% by x1 – success in the test and x2 – the success of the project and x3 – project assignment form. While other causes explain the rest (100%-91%=9%). A probability level of significance has value 0.00 which is much smaller than 0.05 It means that the multiple regression models can be used to predict the dependent variable, or in other words, x1 and x2 and x3 have a simultaneously significant effect on y. For the output coefficients of the variables x1 and x2, the significance value is 0.000, for x3 = 0.044, which is <0.05. Therefore we can conclude, that success in the test, success in the project and the form of the project have a partially significant effect on success in the subject. The same result is in the group of men. For the group of women, it was found that the project assignment form did not have a partially significant effect on the y-success rate in the subject.

Based on the above results, it can be concluded that:

Hypothesis 1, in which we assumed that applying different forms of project assignment has a statistically significant effect on the success of students in the subject, **was confirmed**. A different type of project assignment has a significant impact on the student's success in the subject, expressed in points, on the significance level of 0.05 (p = 0.044).

Hypothesis 2a, in which we assumed that applying different forms of project assignment has a statistically significant effect on success in the group of men, **was confirmed** at the significance level of 0.05 (p = 0.044).

Hypothesis 2b, in which we assumed that applying different forms of project assignment has a statistically significant effect on success in a group of women **was not confirmed** (p = 0.425).

Based on the results of the T-test using SPSS, it can be concluded that:

Hypothesis 3a, where we assumed that there was no statistically significant difference in the success of men and women in the IT courses examined, **was confirmed** (p = 0.085). Women achieved a higher overall score (80.51) than men (76.39). However, since p> 0.05, the difference

in average success rate in the subjects studied in the male and female group is not statistically significant.

Hypothesis 3b, in which we assumed that there was no statistically significant difference in the success of men and women in the final test, **was not confirmed** ($p = 0.036$). Women achieved a higher score in the test (45.55) than men (42.7). The difference in the average score of the final test between men and women was, therefore, statistically significant.

The **hypothesis 3c**, in which we assumed that there was no statistically significant difference in the success of men and women in the solution of the project, **was confirmed** ($p = 0.597$). Although women achieved a higher score (33.26) in the project solution than men (32.25), the difference in the average success rate of the project solution is not statistically significant.

4 Discussion and conclusions

The results of the research confirmed our assumption (hypothesis 1) that different forms of project assignment influence the success of students in courses. However, we did not verify our assumption that a higher success rate could be expected in the case of a group project assignment (expected sign +, obtained sign -). One possible reason may be the fact that some students relied on classmates in the group to solve the group project, and this negatively affected their success in the course, as the student received the score for the project according to their percentage on the project solution. Nevertheless, the group assignment of the project plays an essential role in teaching in terms of the student's future praxis. In practice, collaborating teams are usually involved in solving tasks together, and therefore it is necessary to lead students to team cooperation during their studies. Such a conclusion is supported by the fact that the students achieved a higher success rate in solving the project assigned in a group. The difference was statistically significant. This was confirmed by the results of the T-test ($p=0.03$).

We were surprised that although hypothesis 2a was confirmed in which we assumed that applying different forms of project assignment had a statistically significant effect on success in the male group. Hypothesis 2b was not confirmed in which we assumed that using various types of project assignment had a statistically significant impact on success in a group of women. One of the possible causes of the above results may be the fact that women approached the project in the same way for both individual and group assignments, although they prefer group project assignments. The results of previous research showed this. (Misutova & Misut, 2020) These results confirmed a statistically significant difference in the preference of group assignments by men and women, in favour of women.

On the other hand, the results in the group of men indicate that men seem to be more responsive to solving problems in an individual project than in a group project assignment. They could be less active in group project assignments than in individual projects. This negatively influenced their success in the course, given the allocation of gained points based on the percentage of their participation in the project solution. However, further research is needed to verify this presumption.

The results of the research confirmed our assumption (hypothesis 3a) that there is no statistically significant difference in the success of men and women in the IT courses studied. Also, there is no statistically significant difference in the project success by men and women. The hypothesis 3c was also confirmed, in which we assumed it. This result is consistent with the results of other research on similar issues. (Gorbacheva, Beekhuyzen, vom Brocke, & Becker, 2019; Yarger, Payton, & Neupane) However, we were surprised that hypothesis 3b was not confirmed, where we assumed that there was no statistically significant difference in the successfulness in the final test for men and women. However, the difference was statistically significant. One possible cause is the different approach to a study by men and women, which we had the opportunity to follow during the semester. Women approached the study more

responsibly, preparing more systematically during the semester compared to men. Further research would also be needed to verify this presumption.

The results of the described research will be used to modify the model of teaching IT courses with an emphasis on the development of cooperation, autonomy, creativity, social skills of students as well as critical thinking, to increase its educational efficiency.

5 Acknowledgements

This contribution was funded by the project KEGA 009STU - 4/2018 „The innovation of teaching the subject Intelligent Control Methods at MTF STU“ and partially supported by VEGA 1/0373/18 “Big data analytics as a tool for increasing the competitiveness of enterprises and supporting informed decisions“ and by VEGA 1/0232/18 “Using the methods of multiobjective optimization in a production processes control. “

Resources

Broman, D., Sandahl, K., & Baker, M. A. (2012). The Company Approach to Software Engineering Project Courses. *IEEE Transactions on Education, 55*(4), 445-452. doi:10.1109/te.2012.2187208

Dietsch, D., Podelski, A., Nam, J., Papadopoulos, P. M., & Schäf, M. (2013). Monitoring Student Activity in Collaborative Software Development. *CoRR*, *abs/1305.0787*. http://arxiv.org/abs/1305.0787

Gorbacheva, E., Beekhuyzen, J., Vom Brocke, J., & Becker, J. (2019). Directions for research on gender imbalance in the IT profession. *European Journal of Information Systems, 28(1),* 43-67. DOI:10.1080/0960085x.2018.1495893

Heredia, A., Palacios, R. C., & Amescua Seco, A. (2015). A Systematic Mapping Study on Software ... - CEUR-WS.org. Retrieved March 25, 2020, from http://ceur-ws.org/Vol-1368/paper2.pdf

Marques, M., Ochoa, S. F., Bastarrica, M. C., & Gutierrez, F. J. (2018). Enhancing the Student Learning Experience in Software Engineering Project Courses. *Ieee Transactions on Education, 61*(1), 63-73. DOI:10.1109/te.2017.2742989

Medland, E. (2016). Assessment in higher education: drivers, barriers and directions for change in the UK. *Assessment & Evaluation in Higher Education*, 41(1), 81-96. DOI:10.1080/02602938.2014.982072

Misut, M., & Misutova, M. (2017). Validity Of During-Term E- Assessment. *INTED2017 Proceedings,* 2812-2820. doi:10.21125/inted.2017.0762

Misutova, M., & Misut, M. (2020). Comparison Of Two Project Oriented Teaching Models In Computer Science Subjects As Viewed By Students. *INTED2020 Proceedings*. doi:10.21125/inted.2020.2386

Országhová, D., Horváthová, J., & Hornyák Gregáňová, R. (2017). Selected professional competences of future managers. In *MANAGERIAL TRENDS IN THE DEVELOPMENT OF ENTERPRISES IN GLOBALIZATION ERA* (pp. 408-414). Nitra, Slovakia: Slovak University of Agriculture in Nitra.

Tothova, D., Semelakova, L., Hostovecky, M., & Fabus, J. (2017). Teaching Support To The Educational Process By Learning Management System. *EDULEARN17 Proceedings*. doi:10.21125/edulearn.2017.2048

Vasilevskaya, M., Broman, D., & Sandahl, K. (2015). Assessing Large-Project Courses. *ACM Transactions on Computing Education, 15*(4), 1-30. doi:10.1145/2732156

Yarger, L., Payton, F. C., & Neupane, B. (2019). Algorithmic equity in the hiring of underrepresented IT job candidates. *Online Information Review, 44*(2), 383-395. doi:10.1108/oir-10-2018-0334

ANALYSIS OF STATIC AND DYNAMIC PARAMETERS OF PLAYERS IN CYBERSPACE

Zsolt Bederna[16], Zoltan Rajnai[17]

Abstract
With the advancement of Information and Communication Technologies, criminals have taken advantage as there was a lack of security and privacy at the beginning of the new era. In connection with the cyberspace, pure cybercrimes and cyber-related crimes can be distinguished in which criminals can apply various tools and techniques. It gives a considerable advantage to each entity to assess risks' composition and analyse their effects, probability of the relevant threats, and the time interval in that they exert. But the currently applied methodologies in cybersecurity do not connect with the discipline of criminology, and as a result, several import factors are not considered. As an axiom, most of the times, the weakest link is attacked in a cyberattack; therefore, each relevant element (or compositor) of the cybersecurity domain shall be analysed. In many times, humans pose to be the weakest link.

Humans as individuals have their mindset, but obviously, they form organizations as well as nations. In a cyberattack, each of them may be affected. Because defenders are in constant handicap, the appropriate questions are what they can do, and what limitations influence them. In this paper, I try to find the answers.

Keywords
Cybersecurity; Cyber criminology; Cybercrimes; Threat methodology; Cyber kill chain

1 Introduction

Information and Communication Technologies (ICT) have advanced rapidly through the last decades, which has enormous impacts on various levels of life. This was resulting in the creation of information society and digital economy, in which several interconnected networks had worked together. These networks are known as cyberspace. To be able to make a comprehensive discussion, at first, its definition must be specified.

As per the European Union Agency for Cybersecurity (ENISA), *"cyberspace is the time-dependent set of tangible and intangible assets, which store and/or transfer electronic information"* (ENISA, 2017, p. 7). A more comprehensive definition for cyberspace originates to Kuehl, according to him, it is *"a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies"* (Kuehl, 2009, p. 28).

Despite having regard the cyberspace as a separate world from the physical world in the past, there are complex interrelations between them. The appearance of cyberspace and even more the huge amount of available services have changed the way of work, entertainment, connections, and interactions between people, shopping habits, etc. Yet, the fact is that the cyberspace is a global, integrated domain as the definition states, in which several information systems process different data, or operate state critical information infrastructure. Processed data

[16] Doctoral School for Safety and Security Sciences, Obuda University, H-1081 Budapest, Nepszinhaz u. 8. fsz. 38, Hungary, bederna.zsolt@stud.uni-obuda.hu

[17] Obuda University, H-1081 Budapest, Nepszinhaz u. 8. fsz. 38, Hungary, rajnai.zoltan@bgk.uni-obuda.hu

means different information and therefore, different value for its stakeholders, and it means value for competitors and enemies, too.

Where people interact, or even where value stands, criminal activities may occur, which usually affect a real person or a group of persons. This is the point where security and criminology step in. Therefore, in the rest of the Paper, I shortly define the latter required terms in the field of cybersecurity and criminology, and I examine the connection points between them. Then I review the legislative framework in the field of cyberspace in the European Union with other specific parameters of cybercrimes. Then I separately examine criminals and victims. Finally, I advise a new methodology for the characterization of potential criminals, before summarization and conclusion.

2 Cybersecurity

Traditionally, the main conceptual problems in security are connected to the usage and application of terminology, because it is sometimes inaccurate, or even there can be simple misunderstandings or misconceptions (Ekelhart et al., 2006, p. 249).

Generally, information and communication infrastructure can be classified as Information Technology (IT) and Operational Technology (OT) (Ryba, 2014, p. 59). IT is widely applied where ICT supports business processes or processes data (e.g., finances, communication, emergency services). OT solutions are the basis in facilities associated with technological processes (e.g., manufacturing, processing). Independently from the type of systems, such as computer, IT, OT, network, etc., whom security shall be assured, systems process the whole or the sub-part of data assets.

As the main base of information society, possession of information is getting more and more advantageous for individuals, businesses, and states as well. Information security tends to continuously protect the confidentiality, integrity and availability of the whole set of data assets in every presence and each data status. Confidentiality is the preservation of authorized restrictions on information access and disclosure to access only those persons and systems to be entitled to, including means for protecting personal privacy and proprietary information. Integrity is the protection from improper information modification or destruction, and it includes ensuring information non-repudiation and authenticity. Availability includes all the activities to ensure timely and reliable access to and use of information.

On the other hand, IT security does not pay attention to the physical world, it deals with data processed by the IT system, and as a plus, it focuses on the protection of that system(s) and its (their) service(s) to ensure the confidentiality, integrity, and availability of processed data and used system(s). It is also continuous activities and effort.

Regarding Kuehl's cyberspace definition discussed before, it is a set of network and information systems (and other connected devices as well). In connection with cyberspace, cybersecurity is much more than IT security. As per International Telecommunication Union (ITU) definition, it is the "collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and *technologies that can be used to protect the cyber environment and organization and user's assets"* (International Telecommunication Union (ITU), 2008).

Another exciting and promising definition is the following: "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" (Craigen et al., 2014).

2.1 Components of cybersecurity

For further analysis, the information security perspective Business Model for Information Security (BMIS) model (von Roessing, 2010) will be applied, which was created by Information

Systems Audit and Control Association (ISACA) in 2010. The model has four essential (static) elements as (1) Organization, (2) People, (3) Process, (4) Technology. BMIS considers these elements as discussed below.

Each organisation is considered a network of interacting people through processes applying technologies. Primary, the model deals with employees and other permanent associates as contractors, vendors, and service providers, therefore, the People element contains the human resources in an organisation as employees in each level of hierarchy. On a broader view, it also links to external partners, third-party vendors, consultants, customers, and other stakeholders. The Process element simply deals with practices and procedures that People shall accomplish. Technology includes every technical application used in the organisation, and it covers a broader set than traditional IT poses to be.

But static elements may change in a more extended period through the dynamic relations which are: (1) Culture, (2) Governing, (3) Architecture, (4) Emergence, (5) Enabling, and Support, (6) Human Factors. These dynamic connectors make available a change in one element to have effects on other elements.

2.2 Managing risks

Operation of IT and OT that are available in cyberspace consumes resources in a huge amount. Usually, there is no possibility to prepare for every single threat and to respond to every single event in lack of time, human resource, knowledge, or financial capabilities. Therefore, contrary to the general supposition in the recent past, there is no full security, and even more, security is not constant in time, but it changes dynamically with its environment. In the creation of the optimal system and its operation according to expectations, only conduction of the proper risk management's tasks helps.

Risk management incorporates every necessary process to assess, evaluate, prepare for and response to all the threats and vulnerabilities that may prevent the entity (individual, organization, nation-state) from reaching his, her, or its aims. Through these processes, it helps to select, implement, and operate the proper and relevant controls from the set of potential security measures. It is repetitive from time to time to keep the actual risk level of risk profile below the acceptable risk level.

Risk profile is the register each identified risk with the related metadata, such as threat information, and the related feasible and chosen treatment options and their analysis are contained. The level of risks that are represented in the profile should be kept below the acceptable risk level (aka. risk tolerance), but the temperance depends on the judgement of each entity on their own. Risk appetite is the predefined level of risk that an entity is able and willing to accept to reach its objectives. Averse, minimal, cautious, open, and hungry qualitative risk appetite categories are distinguished (Joint Task Force Transformation Initiative, 2011). The level of risk appetite is ultimately below than the level of risk capacity, and it is supposedly below than the level of risk tolerance. Risk capacity is the maximum risk level that an entity can bear with, while risk tolerance is the maximum risk level that an entity is not willing to bear with.

Considering BMIS, cybersecurity-related risks can be connected to its static elements. Due to this fact, there are risks in Technology, People, and Process elements.

2.3 Framework of cybersecurity

Due to the global nature of the cyberspace, multi-level and multi-shareholder models are applied in its governance and operative management. Each entity (individual, business, organization, nation-state, federation, or union) is responsible for their part of the global space, but some entities have the ability to define a framework for others which or who are in connection. This means that organizations make their standards for their employees and third

parties, service providers create their terms and conditions for their customers, and nation-states create their legislative framework.

In the information society, cyber-related legislation contains governance and management related obligations. In the field of governance, strategy creation is mandatory in order to reach the predefined visions, while in the field of management, there are minimum viable processes and tasks (e.g., incident handling, co-operation between entities), knowledge (e.g., expected certification to fill a position), and technological capabilities are mandated.

In national level, more precisely in international level, the first strategy was accepted in the European Union (EU) in 2013 (European Union, 2013) with the name of "An Open, Safe and Secure Cyberspace". It articulated five strategic priorities: (1) achieving cyber resilience; (2) drastically reducing cybercrime; (3) developing cyber-defence policy and capabilities related to the Common Security and Defence Policy (CSDP); (4) develop the industrial and technological resources for cybersecurity; and (5) establish a coherent international cyberspace policy for the EU and promote its core values.

But the legislative process always advances slowly. For example, after a long preparation, the NIS Directive (Directive (EU) 2016/1148, 2016) was announced on 6 July 2016 and entered into force on the 20th day following that of its publication in the Official Journal of the EU with transposition obligation on 9 May 2018 for Member States. It defined the obligations for all Member States to adopt a national strategy on network and information system (NIS). It created a Cooperation Group to facilitate strategic cooperation and the exchange of information among Member States and to enhance trust amongst them, while it created CSIRTs network for effective operational cooperation. It laid down obligations for Member States to designate national competent authorities related to NIS, and finally, it defined essential services and for digital service providers, and their security and notification obligations.

3 Cyber-criminology

3.1 Criminology

One of the classic definitions of criminology originates back to Edwin Sutherland (Sutherland, 1924, p. 1): "Criminology is the body of knowledge regarding crime as a social phenomenon. It includes within its scope the processes of making laws, breaking laws and reacting towards the breaking of laws." From this definition, it is apparent that criminology is a combination of how society defines and deals with crimes within a social and legal context.

The most common explanatory classifications of criminology are based on biological, psychological, social-psychological, and social theories (Akers, 2013). Biological theories explain crimes with genetic, chemical, neurological basement. Psychological theories are based on personality, emotional, mental retardation, psychic disturbance, or psychological traits. Social psychological theories explain crimes as behaviour, self, and cognitive variables in a group context, while social theories are based on cultural, structural, and socio-demographical variables.

Criminology is a multidiscipline that depends on biology because of genetic, psychology as dealing with the thinking process of a criminal, psychiatry to examine mental stability and inclination of a criminal, philosophy, etc. It employs scientific methodology to study crime, its major forms, its reasons for existence or causation and how the criminal justice system can respond to crime. In its narrower sense, criminology looks at criminal behaviour of individuals in society and how they come to be perceived as such, i.e., their social, cultural, and economic background. In a wider sense, it deals with victims, sentences, too.

Victimology is simply the study of victimization. It deals with the psychological effects on victims, relationships between victims and offenders, the interactions between victims and the criminal justice system, and the connections between victims and other social groups and

institutions, such as the media and businesses (Karmen & Marek, 2014). Penology is a sub-component of criminology that deals with the philosophy and practice of various societies in their attempts to repress criminal activities and satisfy public opinion via an appropriate treatment regime for persons convicted of criminal offences (Sharma, 2017).

3.2 Interrelations of cybersecurity and criminology

Criminology and cybersecurity are seemingly two separate areas of disciplines. But in the cyberspace, there is a huge amount of human interactions accomplished by technical transactions. Unfortunately, human interactions are not free of crimes.

Regarding to cyberspace, generally, there are, or at least there should be norms to be followed. In a social context, these norms represent the collective acceptable behaviour of a group of individuals. Violations of norms are conducted with deviant acts or behaviour, which may be divided into two categories. Formal deviances are crimes which violate laws. Informal deviances are minor violations against unwritten rules. These rules in cyberspace defined by cybersecurity processes.

Social norms actually may differ in space and time (Griffin & Moorhead, 2009, pp. 135–144). A certain act or behaviour may be deviant within one society, while in another society, it is normal. Additionally, social norms and therefore, deviances change over time. Often, deviances have negative connotation, but violation of social norms is not always a negative action. Although a norm is violated, a behaviour can still be classified as positive or acceptable.

All these parameters are true in connection with risks in cyberspace. It deals with the risk-based preparation of defence resulting in measurements which are providing prevention, detection, reaction, and compensation controls for all components of security. The order of the controls gives the prioritization of them, as if an incident cannot be prevented, it should be at least detected, which implies some kind of reaction and compensation capabilities. It means that in case of malicious events (aka. security incidents or cybercrimes), there are one or more attackers (aka. threat agents) and one or more attacked entities as individuals, organizations, and nations states. After an attack occurs, the attacked entity turns to be a victim if he, she, or it cannot prevent the incident. Furthermore, there can be second hand, third hand, etc., victims, too. Criminology deals with criminal acts, the criminal, indirectly the victim of the crime, crime causation and theory, crime prevention and detection of potential offenders, and the efficacy of the criminal justice system.

So, cyber-criminology is mainly the study of “criminal behaviour and victimization in cyberspace from a criminological or behavioural theoretical perspective” (Ngo & Jaishankar, 2017, p. 4). The disciplinary was defined in 2007 by Jaishankar as *“the study of causation of crimes that occur in the cyberspace and its impact in the physical space”* (Jaishankar, 2007, p. 1). As the supporting disciplinary, cyber forensics *“involves applying computer investigation and analysis techniques to solve a crime and provide evidence to support a case. It is the process of identifying, preserving, analysing and presenting the digital evidence”* (Prasanthi, 2016, p. 266).

4 Cybercrimes

Cybercrimes can be defined as the "offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)" (Halder & Jaishankar, 2012). EU defines cybercrimes as “criminal acts committed using electronic communications networks and information systems or against such networks and systems” (Directive 2013/40/EU, 2013).

As definitions imply, pure cybercrimes and cyber-related crimes can be distinguished. In the case of pure cybercrimes, the target is in cyberspace which is attacked in cyberspace or physical world. It aims to decrease the level of the confidentiality, integrity, or availability of the processed data, or even it targets infrastructure to eliminate a whole or a part of the whole infrastructure. Finally, it may cause economical, psychological harm to the users, administrators of the affected data or system that can be even resulted in physical harm, too. Commonly, the first victim system is used by the attacker to commit further crimes. In the case of cyber-related crimes, cyberspace is used to facilitate committing crimes in the physical world such as selling drugs.

As per (Directive 2013/40/EU, 2013), the EU breaks down cybercrime as (1) traditional forms of criminal activity committing by the usage of the Internet (such as fraud, forgery, identity theft, or even international trading in drugs, arms and endangered species); (2) publication of illegal content (such as material inciting terrorism, violence, racism, xenophobia, or child sexual abuse); and (3) crime unique to ICT which can also threaten critical information infrastructures of the state and thus directly its citizens.

4.1 Complexity of cybercrimes

Inspecting from a security perspective the several actors operating in the cyberspace, each of them has its objective, preference, tools and tactics, and has some allies and some enemies. This space may be deemed as a game, and therefore, may be modelled by Game theory. A game is a description of interactions between opposing or co-operating interests of players, where each player has its strategy, constraints and payoff for actions to take. A player may be a person, machine, or group of persons (Chukwudi, 2017, p. 45).

Hence, cybersecurity is modelled by at least two actors interacting in an attempt to maximize their intended objectives. For defenders, different techniques available in game theory can be utilized to perform tactical analysis of the options of cyber threat produced either as a single attacker or as an organized group (Chukwudi, 2017, p.47).

The complexity of these games varies on a huge scale, as it can be very short and very simple, and in contrary, it can take a long time with high complexity. For the case of pure cybercrimes, attack's intensity, its resource requirements vary from systems to systems.

In 2011, the Cyber kill chain was introduced by Lockheed Martin (Hutchins, Cloppert, & Amin, 2011). Kill chain is a term that is originally used in the military. It defines the required steps to attack a target. In parallel with the original term, the cyber kill chain defines the necessary steps used by cyber attackers. The following intrusion steps have been identified by the authors (Hutchins, Cloppert, & Amin, 2011, pp. 4-5):

1. Reconnaissance is the research, identification, and selection of targets, including special technological, social, or any other information.
2. In the weaponization phase, specifically crafted malware is created to exploit the vulnerabilities based on the intelligence gathered in the reconnaissance phase.
3. Delivery is the transmission of the weapon to the targeted environment.
4. Exploitation triggers malicious code after the weapon is delivered to the victim host.
5. Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.
6. Command and Control (C2 or C&C) channel is established after the compromised host beaconed.
7. In the phase of the Actions on Objectives, intruder or intruders can take actions to achieve their original objectives.

The theory divides an attack to stages for defenders to better identify and stop attackers at each of the respective stages. As the more points at which defenders can intercept criminal activity, the better the chance they have to prevent, or detect and react.

4.2 Business model of committing crimes

Individuals can commit crime on their own separately or in group, or they can have resort to attacking resources. Cybercrime as a Service is a business model of criminals that covers various services, infrastructure, knowledge, etc., to be rented (Manky, 2013). There are three categories as discussed below.

In Crimeware as a Service, identified vulnerabilities and the related exploits are offered generally or for a specifically targeted scenario. Zero-day vulnerabilities, Advanced Persistent Threats (APTs), malware such as rootkits, ransomwares are included as well as droppers, keyloggers, and hiding tools like cryptors or polymorphism (Szőr, 2005).

Criminals offer infrastructural elements, specifically clients and servers, in the model of Cybercrime Infrastructure as a Service. Clients as part of a botnet are ready to process commands. On the other hand, the information about the vulnerabilities of scanned servers is put up for sale.

By the usage of Hacking as a Service, the complete process is outsourced to the "service provider" including planning and performing on-demand.

4.3 Tools

There are many free or proprietary tools available in the cyberspace that can be used for legitimate purpose as defence, research, etc., or to fulfil illegitimate activities as any kind of attacks through the previously defined cyber kill chain to "play the game".

In the phase of reconnaissance, threat intelligence tools can help threat agents to prepare for action by getting acquainted with useful information. It may also help defenders to know the enemies and even the information that is available about them. The special category of threat intelligence is the Open Source Intelligence (OSINT) which contains "techniques, methods, and tools to acquire information from publicly available online sources to support intelligence analysis" (Hassan & Hijazi, 2018). It is useful for many scenarios such as "financial, crime, and terrorism investigations as well as analysing business competitors, running background checks, and acquiring intelligence about individuals and other entities".

A huge number of exploits exists to take advantage of publicly known or unknown vulnerabilities in the phase of weaponization. Skilled attackers can create custom tools themselves. However, there are downloadable ones for anyone. These programs essentially automate the process of weaponizing files, and even they may help to implement tactics for evading security measures.

The heart of the attack is implemented by payloads to realize the aim of the attack as to take over the control of resources to commit cybercrimes utilizing the infected machine's resources, and/or to compromise confidentiality, integrity, or availability of data.

Rootkits are a collection of programmes that enable administrator-level access to a computer or computer network to gain root or privileged access to the infected machines. A trojan poses as a legitimate programme, while it may act in several malicious way such as spying, stealing data, deleting files, expanding a botnet, and performing Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack if several machines are infected. A backdoor/remote-access trojan (RAT) accesses the infected device remotely. It gives almost full control to the attacker to perform actions like monitoring actions, executing commands, sending files and documents back to the attacker, logging keystrokes, or taking screenshots. A scareware is a fake anti-virus software that pretends to scan and find malware/security threats on a user's device so that they will pay to have it removed. A spyware is installed on a computer without its owner's knowledge to monitor their activity and transmit the information to a third party. An adware displays advertising banners or pop-ups that include code to track the user's behaviour on the internet. A ransomware stops users from accessing their devices and demands that they

pay a ransom through certain online payment methods to regain access. A variant, police ransomware, uses law enforcement symbols to lend authority to the ransom message.

Disruptionware is a special category of malware that is designed to suspend operations within a victim organization. From the attackers' point of view, it is advantageous for OT environments. On the other hand, from the victims' point of view, it is devastating in the case of mission-critical systems and legacy systems that lack redundancy (Brichant & Eftekhari, 2019). Worms, file infectors, wipers, and even subcategory of ransomware belong to disruptionware. A worm replicates itself over network from device to device without guidance of its creator. A file infector infects executable files by overwriting them or inserting infected code that disables them. A wiper deletes all the data stored on the infected device.

Delivery technics of payloads can be manual, semi-automatic with the application of tools, or automatic by botnets. A botnet (short for robot network) is made up of computers communicating with each other over the internet. A C&C uses them to send spam, DDoS attacks and commit other crimes including espionage. Botnets are also applied to control affected machines onward after infection (Bederna & Szadeczky, 2019).

Until this point, only technical tools were discussed, but as the BMIS states, humans and their implemented processes pose to be a very important part of security. Social engineering techniques that exploit vulnerabilities in human nature, attitude, lack of knowledge, or errors of processes. It is "the art of tricking employees and consumers into disclosing their credentials and then using them to gain access to networks or accounts […] (by the) deception or manipulation of people's tendency to trust, be corporative, or simply follow their desire to explore and be curious" (Conteh & Schmick, 2016, p. 31). Phishing, whaling, tailgating, dumpster diving, baiting, pretexting, and any type of manipulation belong to this type of attack in various phase of the cyber kill chain model.

4.4 Legislation framework in the European Union

The kind of activities that are perceived as crimes is defined by legislation. Due to technical advancement, ICT had got to be a critical part of our life in several layers that results in conformity, faster administration, etc. It gave a new way of working, playing, and living for more and more individuals, but few of them knew how to use it safely and ethically in an immature culture and legislation environment.

The advancement of laws is generally a slow process in every aspect of life. The prompt research and development in the ICT sector multiply this fact. Another negative effect from this perspective is the acquis in the European Union due to its multilevel and multi-shareholder structure.

In a multi-stakeholder model, "any group with the relevant expertise (businesses) or the required political authority (states) may participate in the policy-shaping process" (Bendiek, 2012, p. 12). The plurality caused by the multi-level and multi-shareholder model creates an operating environment with "not only the dynamic nature of the challenge but also the lack of clearly delineated areas of responsibility and accountability among the different institutions" (Bendiek, 2012, p. 13).

In 2007, with the name of Towards a general policy on the fight against cybercrime, the Commission to the European Parliament, the Council and the Committee of the Regions were on to tackle them (European Commission, 2007). The Communication was to strengthen the fight against cybercrime at national, European, and international levels with the objective of (1) improving operational law enforcement cooperation; (2) coordinated and interlinked training programmes; (3) better political cooperation and coordination between EU Member States; (4) political and legal cooperation with several non-EU countries; (5) standardising legislation and definitions of Member States; and (8) raising awareness of the dangers and costs of cybercrime.

Later, it materialized on combating the sexual exploitation of children online and child pornography (Directive 2011/93/EU, 2011), strengthening cybersecurity, the directive on attacks against information systems (Directive 2013/40/EU, 2013), and the establishment of the European Cybercrime Centre (EC3) (Commision of the EU, 2012).

As (Directive 2013/40/EU, 2013) states, *"instigating, aiding, abetting and attempting to commit any of the above offences will also* be liable to punishment", and such offences shall "be punished by effective, proportionate and dissuasive criminal penalties". It also introduces the liability of legal persons.

EC3 was established in 2013 as part of Europol (1) to identify trends and threats, and improve intelligence; (2) to support Member States focusing on police and judiciary training; (3) for operational support in cross-border joint investigation and the exchange of operational information in ongoing investigations; and (4) as the *"collective voice of European cybercrime investigators across law enforcement and the judiciary"* (Commision of the EU, 2012).

5 Analysis of the concerned parties

It gives a huge advantage to each entity to assess risks' composition and analyse their effects, time interval, and probabilities (Freund & Jones, 2015, pp. 29-31). Methodologies (e.g., ISO/IEC 27005:2018 (International Organization for Standardization, 2018)) and ontologies (e.g., Factor Analysis of Information Risk (FAIR) (Freund & Jones, 2015)) in the field of cybersecurity mainly deal with attackers (precisely with threat agents), while they deal with attacked entities in the form of measuring the loss magnitude that they cause. Specific threat assessment methodologies, e.g., Threat Assessment and Remediation Analysis (TARA) (Wynn et al., 2011), Mission Oriented Risk and Design Analysis (MORDA) (Evans et al., 2004), and STRIDE (Shostack, 2014), help in the assessment. (STRIDE is a mnemonic of Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege.)

But other aspects of effects than discussed above remain unseen. The matter of fact, if defenders are attacked, they turn to be victims. All the methodologies in the field of cybersecurity deal only with the security of the cyberspace. They do not tackle the source nature of the attacker's motivation and even the interrelations with the physical world. Albeit, as per EC3's Internet Organised Crime Threat Assessment (IOCTA) report about the year 2018 (Europol, 2019), the convergence of the cyberspace and the physical world has been continued. Furthermore, cybersecurity does not deal with cyber-related crimes, or as the (Directive 2013/40/EU, 2013) differentiates, the traditional forms of criminal activity or publication of illegal content. Its only subject is crime unique to ICT.

These facts imply the discussions of the parameters of "players". In security games, as previously discussed in Chapter 4, each player has its strategy, constraints, and payoff for actions to take. But on both sides, there are inner and outer limitations. The inner ones are knowledge, attitude, etc., and the outer ones are environmental, fiscal, technological, etc. originated. These limitations can be categorized as static parameters (e.g., knowledge, attitude) for a longer time interval, while others give the dynamic nature of the game (e.g., behaviour of the player and the other players, psychological factors). The following subchapters describe the empirical decomposition of threat actors/criminals and defenders/victims.

5.1 Analysis of cyber-attackers

Generally, the following threat actors are distinguished in cyberspace by security industry: (1) script kiddies, (2) malicious insider, (3) cybercriminals, (4) hacktivists, (5) cyber terrorists, and (6) state-sponsored. Actors are listed in increased order according to knowledge and capability levels, but as a negative result, a huge amount of information wastes with the application of this kind of over-simplification categorization.

My advice on the parameters of threat includes the followings: (1) Motivation; (2) Capabilities; (3) Source of attack; (4) Applied business model; and (5) Cooperation willingness.

Motivation unfolds to source of motives and probable effects. Source of motives can be biological, social, and psychological as it is distinguished in criminology. Results of these motives materialize in intended effects on attacked entity regarding to BMIS categories. Furthermore, as another dimension of effects, they have physical (e.g., organized physical crimes), logical (e.g., DDoS), or even mental (e.g., misinform) aspects.

Capabilities represent the application of tools that reside in the attacker's portfolio. Social engineering, technical tools, and physical capabilities can be distinguished. Each of them has its effect and usability in the cyber kill chain model.

The next parameter is the location where the attacker resides. This attribute can take a value as inside, outside, while outside may be broken down as partner, customer, or unknown. It is unavoidable to differentiate the location of the starting point as this parameter defines the surrounding environment of threat agents and set parameters of the security game.

As there are several threat actors in the wild, who or which can be deemed as coequal entities. Therefore, the last two parameters set the co-operative nature of threat agents. These are the Applied Business model as discussed in Chapter 4.2 and the Cooperation willingness which can be set, for example, as collaborator, neutral, or hostile nature of the attacker.

5.2 Analysis of cyber-defenders

On defenders' side, a hierarchical layering approach is applied. The base of the pyramid is constituted by individuals. Each layer above individuals builds on the antecedent layers. These layers are made by the organization and then nation sate.

Based on BMIS, cybersecurity is a symbiosis of People, Technology, Processes under the umbrella of the Organization, which is an abstract entity and can be used for individuals and the nation. It sets the working framework for the other factors.

Attack may affect People, Technology, Processes, or a combination of them, resulting in a problem for the Organization itself. Each of them has vulnerability and impact parameters. Business impact analysis (BIA) is the composition of tasks to assess the effects (aka. impacts) of the threat agents' activities (International Organization for Standardization, 2018). These effects may be at least fiscal, compliance (legal, industrial), reputational, environmental, personal, or social. Furthermore, timescale is also a very important factor in the realisation of these effects. The effects can also be categorized as biological, social, and psychological.

On the other hand, the individual and the above levels have different parameters. Individuals have their extrinsic and intrinsic source of motives, knowledge, habit, and awareness level. As organizations are composed of individuals, awareness composed the cultural parameter of them. This means that individuals influence the level of culture as this happens with knowledge. While the power of the attackers in a group converges to the maximum of all of the individuals composing that group, the power of the defenders in a group converges to the minimum of the set of individuals in that group for People, Technology, or Process entities.

On the national level, the same statements are true. As a plus, there are critical infrastructure both on national and EU-level (Council of the, E. U., 2008), which have "vital societal functions, health, safety, security, economic or *social well-being of people, and the disruption or destruction of which would have a significant impact"*.

6 Analysis of opportunities and limitations of defenders

Through the cyber kill chain, security games are played in all stages. While the previously discussed decomposition resulted in the static parameters, which define the behaviour of each player through the game. In a preparing phase, players set their static parameters before

reconnaissance by, for example, system hardening in Technology, increasing knowledge level of People, or increasing maturity level of Process entities.

Through the game, attackers and defenders try to play their pure strategy to reach their optimum. For this purpose, they may co-operate other players in the cyberspace. For example, a defender may draw on services of a Computer Emergency Response Team (CERT) or a Computer Security Incident Response Team (CSIRT), as well as attacker may also co-operate with each other. On the other hand, attackers may compete. For example, one's botnet may hack others' bots. The security game can be considered as an asymmetric game since attackers and defenders have other sets of actions.

Because defenders are in constant handicap, the appropriate questions are what the individuals, organizations, and nations can do and what limitations, such as knowledge, fiscal, awareness, influence them.

6.1 Individuals

Individuals are the main factor in defending activities. Yet, players may not be able to play their pure strategy through the cyber kill chain due to their limitations. This means that not the optimal choice or action are made in many times.

Generally, players do not pay attention to probabilities under psychological pressure. Thin slicing (Ambady & Rosenthal, 1992) is the ability to find patterns and to make rapid inferences about the state, characteristics, or details of an individual or situation with minimal amounts of information. Thin slices of behaviour are diagnostic of many affective, personality, and interpersonal conditions.

It may help defenders to make decisions, but without previous knowledge, awareness, and experiences from similar events, it may result in wrong decisions. One of the most important factors of cognitive limitation is a low level of knowledge. Decisions throughout projects or in daily operation may be deferred as a result of indecisiveness. It is always easier for many people to add just one more item to the list of choices instead of choice itself. As Barry Schwartz wrote in his book in connection with Fred Hirsch's "Tyranny of small decisions", it is "a large array of options m[a]y diminish the attractiveness of what people actually choose, the reason being that thinking about attractions of some of the unchosen options detracts from the pleasure derived from the chosen one" (Schwartz, 2004, p. 20).

Individuals have cognitive limitations in searching for and processing information caused by their limited memory capacity and the intention of obtaining information which supports their own opinions. Most of the people prefer to obtain concrete information, that is based on their personal experience. Furthermore, accurately combining different sources of information is a cumbersome task. As a result, everyone tends to simplify, which may help to some extent, but it can also cause making wrong decisions (Chariri, 2017).

In decision making, the availability heuristic (Tversky & Kahneman, 1974) as a mental shortcut may bias mind when evaluating a specific topic, concept, method, or decision based on their remembrance. People tend to heavily weigh their judgments toward more recent information, making new opinions biased toward that latest news. If somebody can quickly think of multiple examples of something, he or she will believe that is quite common. This is something that may give advantages to attackers when conducting social engineering.

While there may be enough time to think about alternatives, there are none in stressful situations such as in incident handling due to the time factor. "*The more options we have, the more difficulty we have gathering the information necessary to make a good decision"* (Schwartz, 2004, p. 199).

6.2 Organizations

As an entity, an organization set its standards (aka. norms) in written and unwritten form. But it is built up from individuals hierarchically; therefore, the awareness and knowledge of individuals in management, business units, IT, etc. shape the culture, knowledge, and behaviour of the entire organization. In the beginning of the Internet, generally, it was normal to be unaware of security, but slowly, it should be deviant. To reach this status, users' security awareness shall be increased.

Lance Spitzner, the director of the SANS Security Awareness, examined this topic in the context of the cyber kill chain model (Spitzner, 2019). In the reconnaissance phase, aware individuals should know that he or she may be targeted in every time. Therefore, they limit publicly shared contents, do not share sensitive information with unauthorized people, and safely delete or dispose of sensitive documents. In the delivery phase, people can identify and stop attacks even in the lack of security controls, like in fraud or spear phishing. Furthermore, in any phases, they can ensure that the systems are updated and current, and observe and report any abnormal activities.

As a supplement to the cyber kill chain model, in the hypothetical preparing phase, the organization should develop administrative, logical, and physical security controls based on risk assessment and analysis, while security culture should be strengthened through the advancement of individuals' awareness.

As implicitly stated above, there are several potential limiting factors in an organization that are posed to be risks. The highest one is the lack of awareness in every level of the hierarchy. Even the management is able to forget the fact that they have the ultimate responsibility of risks as risk owners, which could easily lead to wrong strategic or tactical decisions. Deficiencies on lower levels may pose operational risks that can be materialized vulnerable systems, ineffective process implementation, or silo-based operation. Wrongly implemented technical measures may not be able to prevent or at least detect activities of malicious insiders.

The ultimate response shall be the development and enhancement of the security awareness, which comprises knowledge, behaviour, and attitude. Organizational behaviour, which is the study of human behaviour in organizational settings, the interface between human behaviour and the organization (Griffin & Moorhead, 2009, p. 4), tends to help in motivating people to elevate the common cyber-hygiene. Motivation is the reason for people's actions, willingness and goals through needs (or motives) that requires satisfaction. It is the management's task to find the right way to influence every employee with the right motivation based on, for example, reinforcement (negative reinforcement, positive reinforcement, punishment, and extinction).

6.3 National level

In the national and international level, the norm is set for the entire society. Its written form is the legislative framework. The problems are the same as discussed in the previous chapter, but the limitations are much more. Due to the multi-shareholder, multilayer approach, legislative development generally advances slowly, and it may contain problematic elements, for example, fuzzy technical requirements or overcomplicated texting. But it is the interest of the whole society to elevate the common level of cyber-hygiene with the appropriate education and awareness-raising for each age group from children to seniors, from technical people to digital immigrants.

7 Conclusion

With the growth in usage of ICT devices and services, people learnt the importance of security slowly, meanwhile, criminals learnt how to utilize the new medium. Therefore, after

analysing the cybersecurity's and cyber-criminology's basements and their interrelations, I analysed the legislative framework that defines the meaning of cybercrimes.

It can be said that the slow advancement of the legislation process is multiplied in the sector of ICT due to its rapid enhancements. The complexity of crimes committed in the cyberspace makes their treatment harder. As a possible answer, I discussed the game theory and the cyber kill chain model. I introduced or at least I gave examples the tools and techniques that criminals may apply in or in connection with cyberspace through the kill chain to maximize their payoff on their own or even with the usage of various services.

As it implies, it is a huge advantage to know relevant threats and their parameters, and in fact, the abilities and capabilities of the defenders on the other side. In my opinion, cybersecurity as a discipline can learn from (cyber) criminology to enhance methodology of risk assessment and analysis, as individuals could be the main power as well as the main weakness in security. They shall be prepared mentally against threats as well as to treat committed crimes accordingly regardless of the age, abilities, or capabilities of a (potential) victim.

Even so, organizations aggregate from individuals, and nations aggregate from individuals and organizations. Thus, the ultimate response shall be the development and enhancement of security awareness, which comprises knowledge, behaviour, and attitude. This shall aim each entity of the society in each level, for individuals, organizations, and nations, too.

Funding

This work was not funded by any party.

Acknowledgements

This work was created as part of my doctorate course. I would like to thank the advisements during my research from Katalin György, Prof Dr and Viktor Nagy, Dr, lecturers at the Doctoral School for Safety and Security Sciences, Obuda University in Hungary.

Resources

Akers, R. L. (2013). Criminological Theories. Routledge. https://doi.org/10.4324/9781315062723

Ambady, N., & Rosenthal, R. (1992). Thin slices of expressive behavior as predictors of interpersonal consequences: A meta-analysis. *Psychological Bulletin*, *111*, 256–274. https://doi.org/10.1037/0033-2909.111.2.256

Bederna, Z., & Szadeczky, T. (2019). Cyber espionage through Botnets. *Security Journal*. https://doi.org/10.1057/s41284-019-00194-6

Bendiek, A. (2012). *European Cyber Security Policy*. Stiftung Wissenschaft und Politik. https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2012_RP13_bdk.pdf

Brichant, R., & Eftekhari, P. (2019). *The rise of disruptionware*. *A Cyber-Physical Threat to Operational Technology Environments* [PDF]. Institute for Critical Infrastructure Technology. https://icitech.org/wp-content/uploads/2019/09/ICIT-Brief-The-Rise-of-Disruptionware.pdf

Chariri, A. (2017). Cognitive Limitations and Decision Making. *Jurnal Bisnis Strategi*, *3*(2), 21–28. https://doi.org/10.14710/jbs.3.2.21-28

Chukwudi, A. E. (2017). Game Theory Basics and Its Application in Cyber Security. *Advances in Wireless Communications and Networks, 3*(4), 45. doi:10.11648/j.awcn.20170304.13

Commision of the, E. U. (2012). Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre /* COM/2012/0140 final */Lex - 52012DC0140 - EN. Retrieved February 20, 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52012DC0140

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Adva*nced Computer Research (IJACR)*, *6*(23), 31–38. https://doi.org/10.19101/IJACR.2016.623006

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*. https://doi.org/10.22215/timreview835

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, (2016). http://data.europa.eu/eli/dir/2016/1148/oj

Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, (2011). http://data.europa.eu/eli/dir/2011/93/oj

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, (2013). http://data.europa.eu/eli/dir/2013/40/oj

Ekelhart, A., Fenz, S., Klemen, M. D., & Weippl, E. R. (2006). Security ontology: Simulating threats to corporate assets. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/11961635_17

ENISA. (2017). *ENISA overview of cybersecurity and related terminology*. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

European Commission. (2007). *Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime COM/2007/0267 final*. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52007DC0267

European Union. (2013). *An Open, Safe and Secure Cyberspace*. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52013JC0001

Europol. (2019). *Internet Organised Crime Threat Assessment (IOCTA) 2019*. IOCTA Report. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

Evans, S., Heinbuch, D., Kyle, E., Plokkowski, J., & Wallner, J. (2004). Risk-based systems security engineering: Stopping attacks with intention. In *IEEE Security and Privacy*. https://doi.org/10.1109/MSP.2004.109

Freund, J., & Jones, J. (2015). *Measuring and Managing Information Risk*. Elsevier, Butterworth-Heinemann. https://doi.org/https://doi.org/10.1016/B978-0-12-420231-3.01001-0

Griffin, R. W., & Moorhead, G. (2009). *Organizational Behavior: Managing People and Organizations* (9th ed.).

Halder, D., & Jaishankar, K. (2012). Cyber Crime and the Victimization of Women. *Advances in Digital Crime, Forensics, and Cyber Terrorism*. doi:10.4018/978-1-60960-830-9

Hassan, N. A., & Hijazi, R. (2018). The Evolution of Open Source Intelligence. *Open Source Intelligence Methods and Tools,* 1-20. doi:10.1007/978-1-4842-3213-2_1

Hutchins, E., Cloppert, M., & Amin, R. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In J. Ryan (Ed.), *Leading Issues in Information Warfare & Security Research* (pp. 80–106). Academic Conferences Limited.

International Organization for Standardization. (2018). *ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management*.

International Telecommunication Union (ITU). (2008). Overview of cybersecurity. In *Series X: Data Networks, Open System Communications and Security - Telecommunication Security*.

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, *1*(1), 1–6. https://doi.org/10.13140/RG.2.1.4039.9525

Joint Task Force Transformation Initiative. (2011). SP800-39 Managing Information Security Risk. In *Nist Special Publication*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-39

Karmen, A., & Marek, W. K. (2014). Crime victims: An introduction to victimology. In *American Journal of Forensic Psychology*. https://doi.org/10.1080/10345329.1993.12036610

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. In *Cyberpower and National Security* (pp. 24–42). Potomac Books and National Defense Univerity. https://doi.org/10.2307/j.ctt1djmhj1.7

Manky, D. (2013). Cybercrime as a service: A very modern business. *Computer Fraud and Security*. https://doi.org/10.1016/S1361-3723(13)70053-8

Ngo, F., & Jaishankar, K. (2017). Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime. *International Journal of Cyber Criminology*, *11*(1), 1–9. https://doi.org/10.5281/zenodo.495762

Prasanthi, B. V. (2016). Cyber Forensic Tools: A Review. *International Journal of Engineering Trends and Technology*, *41*(5), 266–271. https://doi.org/10.14445/22315381/ijett-v41p249

Ryba, M. (2014). The role of ICT components in the functioning of critical infrastructure. In J. Świątkowska (Ed.), *Critical Infrastructure Security - the ICT Dimension* (pp. 59–62). The Kosciuszko Institute.

Schwartz, B. (2004). *The Paradox of Choice*. HarperCollins Publishers Inc.

Sharma, R. K. (2017). *Criminology And Penology*. Atlantic Publishers & Dist.

Shostack, A. (2014). *Threat modeling: designing for security*. John Wiley and Sons.

Spitzner, L. (2019). *Applying Security Awareness to the Cyber Kill Chain | SANS Security Awareness*. SANS Institute. https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain

Sutherland, E. H. (1924). *Principles of Criminology*. University of Chicago Press.

Szőr, P. (2005). The art of computer virus research and defense. Addison-Wesley Professional.

Council of the, E. U. (2008, February 12). COUNCIL DECISION of 12 February 2008 establishing Statutes for the Euratom Supply Agency. Retrieved 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32008D0114

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*. https://doi.org/10.1126/science.185.4157.1124

von Roessing, R. (2010). The ISACA Business Model for Information Security: An Integrative and Innovative Approach. In *ISSE 2009 Securing Electronic Business Processes*. https://doi.org/10.1007/978-3-8348-9363-5_4

Wynn, J., Whitmore, J., Upton, G., Spriggs, L., McKinnon, D., McInnes, R., Graubart, R., & Clausen, L. (2011). *Threat Assessment & Remediation Analysis (TARA)*. The MITRE Corporation. https://www.mitre.org/sites/default/files/pdf/11_4982.pdf

COMPOSITION DIAGRAM OF A COMPLEX PROCESS: A CONTRIBUTION TO BUSINESS PROCESS MODELLING

Pavol Jurík[18], Peter Schmidt [19]

Abstract
In practice, we often encounter complex business processes that can be decomposed into a sequence of interrelated sub-processes. The flow of these sub-processes can be depicted using well-known diagram techniques designed to model business processes, such as: flowcharts, Business Process Model and Notation (BPMN) diagrams, activity diagrams, etc. However, with a large number of sub-processes we can lose the overview of how exactly the individual sub-processes relate to each other and what is their exact position or role in the parent process. Therefore, we have set our goal to create a new diagram technique, whose task is to provide a managerial (i.e. global) overview of the structure of a complex process at the highest level of abstraction. Such a managerial overview of a complex process is important not only for the owner of the process in managing it, but also for designers of an information system intended to support the proper running of the process and the individual sub-processes it consists of. Currently, a process thread diagram is used for this purpose, however, it has some drawbacks and it is unable to capture some of the facts that are essential in managing of a complex process. Therefore, we have developed a new diagram technique that removes these shortcomings. In doing so, we emphasized on the simplicity of the notation of this diagram technique. Because of this, the diagrams created using our diagram technique should be clear, simple, easy to understand, and the diagrams created using its rules and notation should be easy to read.

Key words
Business process modelling, process thread diagram, complex process, diagram technique

1 Introduction

A business process can be defined as "a workflow flowing from one person to another and, in the case of a large process, probably from one department to another" (Robson & Ullah, 1998). According to Davenport and Short, "a process is a series of logically linked tasks performed to deliver a defined business output" (Davenport & Short, 1990). A business process is characterized by its repeatability. It represents a steady and repeatedly performed activity taking place in a particular company, which consists of a number of steps designed to transform a certain set of inputs into a set of outputs and to achieve a predetermined objective. Not all of these steps need to be performed sequentially (i.e., one by one), but some of them can be performed in a parallel manner, depending on the character of the particular process. A business process is, therefore, a generalization of a complicated business activity and it represents a workflow. One particular execution of a process is then referred to as an instance of the process. As we mentioned earlier, every process can be executed repeatedly and there can be many instances of the same process in the state of a concurrent execution.

The historically older, functional approach to business management focused only on isolated monitoring and control of the execution of individual functions by organizational units (departments, divisions, sections, etc.) that are responsible for their execution. Thus, the functional approach ignored the interdependence among these functions and evaluated each organizational unit only by the extent to which it performed its functions. Functional approach

[18] Ing. Pavol Jurík, PhD., University of Economics in Bratislava, Faculty of Economic Informatics, Department of Applied Informatics, Dolnozemská cesta 1, 852 35 Bratislava, pavol.jurik@euba.sk.

[19] Ing. Mgr. Peter Schmidt, PhD., University of Economics in Bratislava, Faculty of Economic Informatics, Department of Applied Informatics, Dolnozemská cesta 1, 852 35 Bratislava, peter.schmidt@euba.sk.

to business management did not pay attention to what processes this or that organizational unit participates in and how effective these processes are. However, with a more modern, process-based approach to business management, the functions of the individual organizational units become parts of more complex activities - business processes. One, two, three or even more departments can participate in each business process. Processes consist of functions of the individual organizational units. A function of an organizational unit can be defined as an activity that is routinely performed by this unit. Thus, a function expresses what the department, which is associated with the execution of this function is in charge of and what is its mission. The functions can be interdependent. This means that the outputs of one function can be inputs into another. In this notion, business processes can be thought of as chains of business functions, some of which can be performed sequentially and others concurrently, depending on the needs and specificities of the particular process.

With too many functions, however, a business process becomes too complicated, and the overview of its exact course is lost. If this is the case it is advisable to try to split such a process internally into a few sub-processes (i.e. child processes), which makes this parent process more transparent and comprehensive. A sub-process is a business process that is a part of another business process, which we can refer to as its parent process. However, individual sub-processes may also be too complicated and it may be useful to split them internally into smaller sub-processes to make them more transparent. This brings us to an important term that we will use in this article and that is a complex process. **A complex process** can be defined as a process that can be hierarchically broken down to several levels of sub-processes until we gradually get to elementary steps that can not be further broken down. On the contrary, a process that consists only of elementary steps that can not be further broken down can be referred to as **an elementary process**.

Each business process has certain characteristics. Typical characteristics of business processes include (Jurík, 2018):

- **Process goal** – each process must have a clearly defined goal, which represents the purpose of carrying out the process. If we do not know the exact goal of the process, then we can not effectively manage the process. In this respect, it is very important to express the goal of each process in a deterministic way (i.e. to formulate it unambiguously and comprehensibly), preferably using quantifiable indicators. It is impossible to optimize a process whose objective is unclear.
- **Process owner** – it is a person who is responsible for achieving the goal of the process and for its long-term functioning. This person is responsible for monitoring each instance of the process and its performance, managing it, systematically improving the process and for solving any problems that may arise during the course of each instance of the process. In addition to accountability, he must also have sufficient competences to act actively.
- **Process customer** – it is a subject to whom the results of a certain process are intended. The customer of a process can be either internal (a specific department or an employee in the organizational structure of the company) or external (a customer, a bank, a state administration authority, etc.).
- **Process inputs** – a process is a deterministic way of transforming a set of inputs into a set of outputs corresponding to the goals of the process. The individual inputs can come either from the internal environment of the company (outputs of other processes fall into this category) or from its external environment (materials from suppliers or raw materials extracted directly in nature). Internal and external inputs can be further divided into physical, financial and informational ones.

- **Process outputs** – it is a set of outputs that are intended for the process customer. These outputs can also be divided into three categories: physical outputs, financial outputs and informational outputs.
- **Process efficiency** – this characteristic determines the extent to which the goals of the process have been met after running several instances of the process. Thus, it is the extent to which the actual outputs of the process instances are identical to the required ones. The greater the deviation from the desired state, the less efficient the process.
- **Management regulators** - these are mainly laws, directives, standards, decrees, orders, etc. Each process must be governed by certain rules, which can be divided into internal rules (internal directives and regulations) or external rules (national laws, decrees of ministries, regulations of municipalities, supranational directives, etc.
- **Process risk** – in each process, there may be some segments where the execution of the process may fail. It is important to identify these segments and to pay a special attention to them.
- **Resources** – resources are means that are used (i.e. consumed or depleted) in the transformation of inputs into outputs. For example, human work, technology (wear of machinery and equipment), financial resources, energy, time and information are considered as resources.

In this article, we focus on complex processes and the options of their visual representation. We have set our goal to create a new diagram technique, whose task is to provide a managerial (i.e. global) overview of the structure of a complex process at the highest level of abstraction. Such a managerial overview of a complex process is important not only for the owner of the process in managing it, but also for designers of an information system intended to support the proper running of the process and the individual sub-processes it consists of.

2 Current state of the art

Currently, process thread diagrams are used for the purpose of displaying the course of complex processes. However, this diagram technique has some drawbacks and it is unable to capture some of the facts that are essential in managing of a complex process.

To capture the hierarchical decomposition of a process into a few sub-processes, a process thread diagram can be used as it is recommended by the Select Perspective methodology (Schmidt, 2010). The process thread diagram is able to capture the input of a complex process and its output as well as the interconnectedness of the individual sub-processes it consists of and the hierarchical relationships among them. However, the process thread diagram does not take into account the fact that every instance of a complex process may not be successful and in some cases it may end prematurely. Such a premature end usually represents an unwanted end of the instance, however, in some situations it may occur. Let 's look, for example, at a customer order processing process. Let's imagine that we received an order from a customer who wants us to manufacture some products for him. This order can only be further processed if it meets all the requirements of a valid order. This means that it must contain all necessary data. If any essential requirement is missing, then we must reject this order, ask the customer to complete this request and resend the order to us. This means that the current instance of the customer order processing process ends, and if the customer sends a new order, a new instance of the same process begins. If the order we received from the customer meets all the requirements of an valid order, an assessment of its technical feasibility should follow. This means that we should assess whether we are technically able to produce the desired product. If not, we must refuse the order and explain to the customer that we are unable to produce the product. Again, this means that the current instance of the customer order processing process ends. If we are technically able to

serve the customer's request, then we accept his order and the current instance of the customer order processing process may continue.

The process thread diagram is unable to capture situations like the ones that are described above. In fact, the notation of the process thread diagram contains a symbol representing the output of a process, but does not contain a symbol for terminating the execution of the process. In our diagram technique, which we called the composition diagram of a complex process or simply the Jurík-Schmidt diagram, we have introduced symbols for the input into a process and the output from it, as well as symbols for its start and its end. This makes it possible to distinguish between situations when the complex process is to provide some output, but its execution has to continue nevertheless and situations when the output of the process is associated with the termination of its execution.

The process thread diagram does not allow to capture the fact that the execution of a sub-process is conditioned by the fulfillment or validity of a special condition. When the condition is fulfilled the associated instance of a sub-process can be started, if not there can be either no action or an instance of another sub-process can be started. Let's imagine the above-mentioned customer order processing process. This process may or may not include a purchase sub-process, depending on whether we have all the necessary material in stock or we need to purchase the material first in order to be able to manufacture the products the customer has ordered. The execution of the purchase sub-process is, therefore, conditioned by the actual amount of material in stock. The process thread diagram is not able to capture situations like this because it can only depict a direct sequence of sub-processes without any branching. Because of this, we have added a simple notation for branching into our new diagram technique.

In addition, the process thread diagram does not contain information about the owners of the individual sub-processes, nor about their expected or maximum allowable duration. This information is very important in order to provide a managerial overview of the course of a complex process to the owner of the process, but also for designers of an information system intended to support the proper running of the process and the individual sub-processes it consists of. The information system can be designed to continuously observe the abidance of the expected or maximum allowable duration of each sub-process while a current instance of a complex process is in execution and, if the execution of a sub-process goes into delay, it can automatically contact the sub-process owner who is responsible for the proper execution of this sub-process and inform him that the sub-process needs to be completed as quickly as possible. For this reason, in our new diagram technique we have introduced a notation that allows us to capture information about who is the owner of which sub-process and what is its expected or maximum allowed duration. This information is very important in order to provide a managerial (i.e. global) overview of the flow of a complex process.

Traditional flowcharts can not be used to depict the managerial overview of a complex process that we seek in this article. The most important reason is that a flowchart is used to capture a sequence of activities on the same hierarchical level that make up a single process. In a single diagram, it is not possible to capture a hierarchy that indicates that one process is internally split into sub-processes and these sub-processes are internally split into other sub-processes, etc. Of course, there can be a few interconnected diagrams, however, it is not possible to capture such a hierarchy using a single flowchart only. All the steps or activities depicted on a single flowchart are on the same hierarchical level, but we need to capture the hierarchical relationships among processes (more than one hierarchical level) on the same diagram.

Another reason why flowcharts can not be used for our purposes is that in a flowchart, all its elements must be interconnected by arrows to make their sequence clear. There can not be any isolated elements (i.e. there can not be elements that are not connected to at least one other element by an arrow). However, in our new diagram technique we take into account the possibility that, in some cases, a process may consist of a set of sub-processes that do not depend directly on each other and the exact order of their execution is irrelevant. Situations like this can

not be depicted in a flowchart, since it is intended solely to represent sequences of activities in a precisely defined order. Any isolated element in a flowchart would violate the flowchart creation rules.

Furthermore, a flowchart does not contain a notation to provide information about the owners of the sub-processes nor about their expected or maximum allowable duration. Such information can only be captured in the form of comments and too many comments would make the flowchart less comprendious.

Moreover, the flowchart notation contains various symbols, most of which are not related to the managerial (i.e. global) overview of a complex process. These symbols are explained in the book *Informačné systémy v podnikovej praxi* (Jurík, 2018). In our new diagram technique, we have created a notation that contains only symbols that are explicitly needed from the global point of view and therefore the notation in our diagram technique is specialized for this purpose.

Business Process Model and Notation (BPMN) diagrams have also their limitations. In a single diagram there can be a sequence of activities that are on the same hierarchical level only and make up a single process. Thus, a single BPMN diagram can not depict a hierarchical breakdown of a process into a few levels of sub-processes. Of course, there can be a few interconnected BPMN diagrams, but our goal was to create a diagram technique that enables to capture this hierarchy in a single diagram. Furthermore, in a BPMN diagram, as well as in a flowchart, all its elements must be interconnected (i.e. there can not be any isolated elements because, otherwise, it would be a violation of BPMN diagrams creation rules). As we said earlier, complex processes may contain sub-processes by which the exact order of their execution is irrelevant and such situations can not be captured by a BPMN diagram. It is true that a BPMN diagram is able to capture the information about owner of each sub-process because the whole process is divided into swimming lanes and each of them is assigned to one actor, which can be the owner the sub-processes in this swimming lane. However, it has no symbol or method for capturing the expected or the maximum allowable duration of the sub-processes. Moreover, the notation of BPMN diagrams is very complicated, since there are many symbols that are not related to the managerial (i.e. global) overview of a complex process. This notation is well explained by Révészová and Paľová (Révészová & Paľová, 2009). As we mentioned above already, the notation of our diagram technique contains only symbols that are explicitly needed from the global point of view and therefore it is very easy to use and specialized for this purpose. Furthermore, the notation of BPMN diagrams does not contain a symbol for the output of a process, which is needed for situations when the process is to provide an output but this output does not mean a termination of the execution of the current process instance. An example of such a situation was mentioned above already.

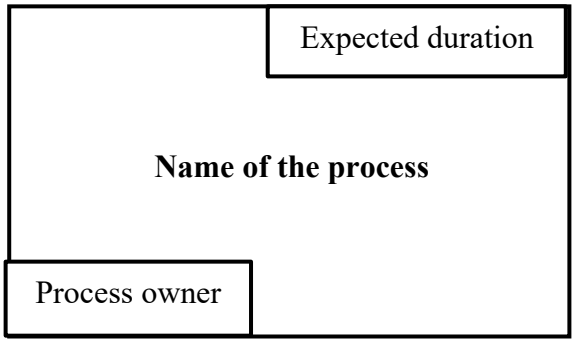
Flowcharts and BPMN diagrams are excellent techniques for displaying the course of a process consisting of a sequence of steps on the same hierarchical level. However, they are unable to provide a really useful managerial overview of a complex process consisting of a lot of sub-processes on different hierarchical levels. The process thread diagram is intended for the purpose of providing a global overview of a process indeed, however, it has some drawbacks that we have mentioned above and it is unable to capture some situations that may occur in real life. Because of this, we have created a new diagram technique that eliminates all the shortcomings of the other diagram techniques and is specially designed to provide a global overview of a complex process.

3 The new diagram technique: composition diagram of a complex process

In this chapter we will introduce a new diagram technique, which we have called the composition diagram of a complex process or simply the Jurík-Schmidt diagram. As we have explained already, this diagram technique is suitable for displaying the internal structure of complex business processes consisting of several levels of sub-processes with hierarchical

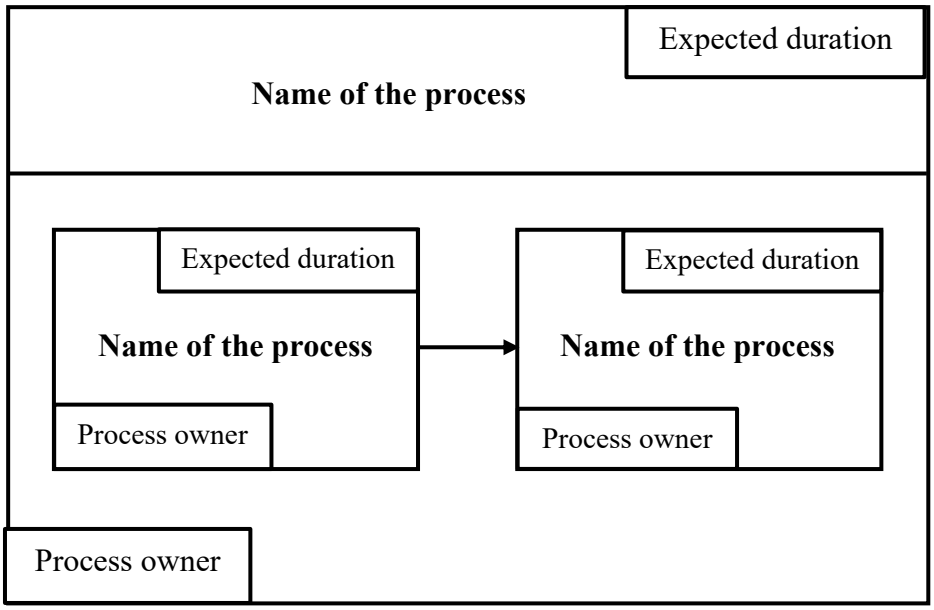
relationships among them from the global point of view. When creating this diagram technique, we emphasized the simplicity of its notation and its rules, which should be followed when creating diagrams. We kept in mind that the diagram technique should be clear, simple, easy to understand, and the diagrams created using its rules and notation should be easy to read. Every process or sub-process should be displayed using the following symbol, which is portrayed on figure 1.

Fig. 1: Symbol representing a process



The sub-processes that form a parent process together are drawn inside this parent process under the principle of a matryoshka doll as displayed on figure 2. If the execution order of the individual sub-processes matters, then we must connect them with arrows. If their execution order is not important, then we omit the arrows, thus, the sub-processes remain unconnected.

Fig. 2: A process and its sub-processes



A **trigger event** is an event that has to occur to start a new instance of a process or a sub-process and it is drawn by a symbol of an empty arrow as pictured on figure 3. In other words, a trigger event represents a signal that causes the start of a new instance of a process or sub-process, when this event occurs. If there is no trigger event in prior to a sub-process it means that there is no special signal needed to start the sub-process. It can just start when the previous activity is finished. It can be an internal or an external event. An example of an internal trigger

event is the drop in the amount of material in stock below a critical threshold value, which is a signal to trigger a new instance of a material purchasing process. An example of an external trigger event is the arrival of an order sent by a customer, which triggers a new instance of a customer order processing process. The symbol of an empty arrow may also symbolize a process input.

An **output of a process** is drawn by a symbol of a full arrow as displayed on figure 3. As we said in chapter 2, there may be situations in which the process has to provide some output (for example a document), but this output does not mean the termination of the execution of the process instance. Thus, in these situations the execution of the process instance has to continue after providing the output. Because of this we use a separate symbol for a process output, which is different from the symbol for the end of a process instance.

Fig. 3: A trigger event or a process input (on the left) and a process output (on the right)

Sometimes, it is necessary to wait for a special event to occur in order to continue with the execution of a process. Such an event can be marked as a **transition event.** For example, it is necessary to receive a special document, signal, material, or an instruction. A transition event is drawn by an oval symbol, which is portrayed on figure 4.

The **end of a process instance** execution (i.e. the place where the execution of the process instance has to be terminated) is drawn by a symbol of a circle with the letter "E" inside as pictured on figure 4. A symbol for the start of a process instance is not needed because it is represented by the symbol of the trigger event, which was introduced already. When the trigger event occurs, the execution of a new process instance starts.

Fig. 4: A transition event (on the left) and the end of a process instance (on the right)

As we said in chapter 2, there may be situations, in which the flow of the process instance is conditioned by the fulfillment or non-fulfillment of a certain condition. The branching of the process flow can be depicted by a square symbol, in which the wording of the condition is written. The condition must be formulated as a question. If the question is formulated so that it can be answered only by a "yes" or "no", then there are two branches leading from this square. A solid arrow (i.e. an arrow drawn with a solid line) represents a positive branch (the answer is "yes") and a dashed arrow represents a negative branch (the answer is "no"). The notation for this situation is depicted on figure 5.

If the question is formulated in such a way that it cannot be answered simply by a "yes" or "no", then both branches may be drawn as a solid arrow and every one of them must be marked with a specific value representing one of the possible answers to the question. There may be also situations, in which we need more than two branches. This is not a problem, since we may add as many branches as we need. The notation for this situation is depicted on figure 6.

Fig. 5: Two-way branching with a positive and a negative branch

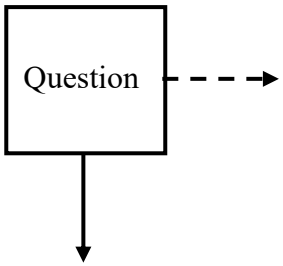
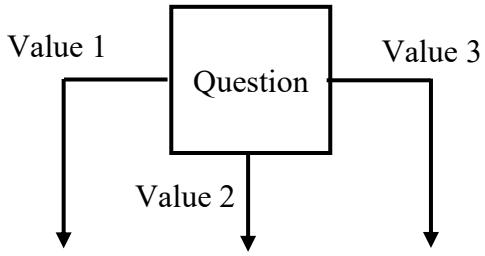
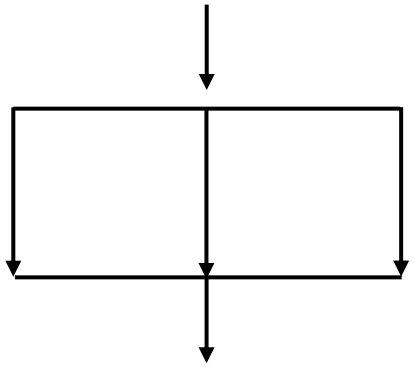


Fig. 6: Three-way branching with branches associated with a value



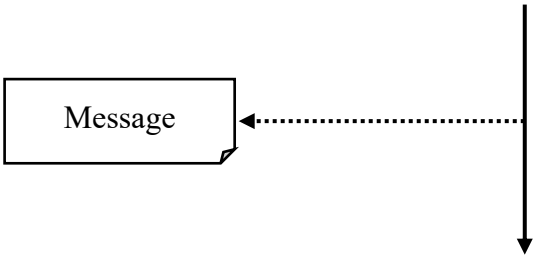
When parallel execution of the sub-processes is needed, it can be depicted using a simple fork-and-join mechanism as portrayed on figure 7.

Fig. 7: Dividing of a single branch into three parallel branches and their later joining into a single branch again



We also distinguish a specific type of parallelism, where a secondary branch is separated from a primary branch, and these two branches no longer need to be merged. The secondary branch is just a digression from the primary branch and it is usually associated with carrying out some trivial activity, which is not important for the further course of the process, such as sending a message for informative purposes only. This type of parallelism can be depicted using the notation on picture 8.

Fig. 8: Parallelism with a primary and a secondary branch representing sending of a message



A very important rule for this diagram technique is that every line between two symbols must be directed. However, in large diagrams there may be a need to move from one point to another without drawing a direct line between these two points because the line would be too long and could cross with other lines in the diagram. Crossing lines is undesirable because it makes the diagram less transparent. In such situations we can use a pair of special **redirection symbols**. This pair of symbols represents a kind of teleport, which progresses the course of the process further to a different place in the diagram. Since there may be multiple pairs of redirection symbols in a single diagram, it is necessary to distinguish these symbols by numbers so that those symbols which form a pair have the same number. Two redirection symbols forming a pair can be drawn as depicted on picture 9.

Fig. 9: Moving from one point of the diagram to another using a pair of redirection symbols

4 An example demonstrating the use of the new diagram technique

Figure 10 shows an example of an order processing process in an e-shop. The e-shop only works with payments on delivery and sending goods by a courier. Therefore, in the diagram we can see a telephone verification of the order and there is no issuing of a pro forma invoice. The whole process starts when the customer creates an order in the e-shop that appears in the system at the seller. As we mentioned already, this process is called Customer Order Processing and it is a complex process owned by vendor. As we can see the normal (i.e. expected) time from the appearance of the order to the delivery of the shipment to a courier should not exceed 70 minutes. However, this applies only in the absence of extraordinary circumstances such as lack of goods in stock.

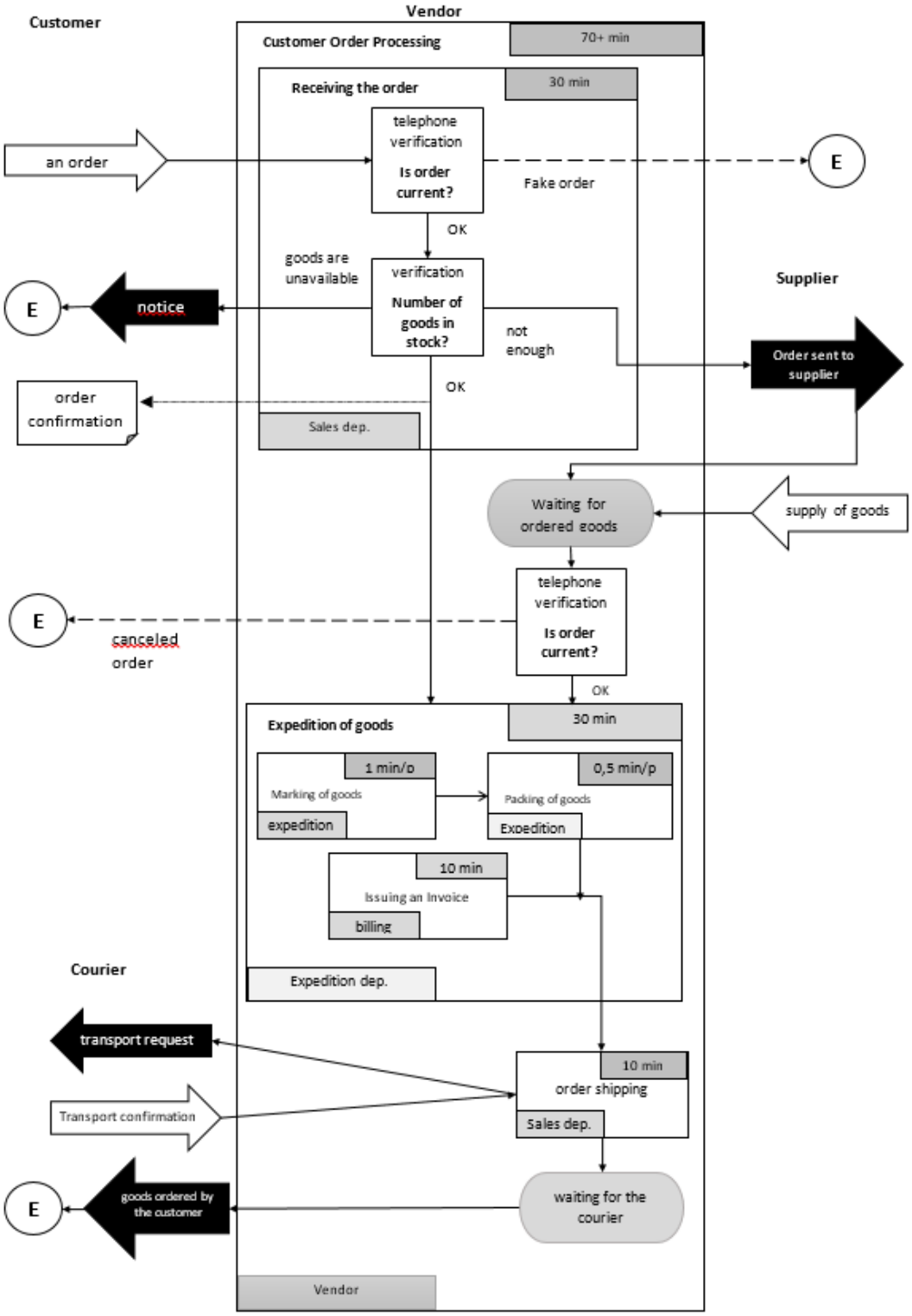
Some e-shops do not allow to order such quantities that are not in stock, but in the example mentioned the e-shop always solves any shortage of goods. This is followed by verification of the customer order by phone, as fake orders sometimes occur and if its a fake order the process instance ends. If the customer confirms the order by phone, the availability of the goods is verified. There is a decision block that has 3 possible outputs. If the product is unavailable (i.e. it is not in the vendor's warehouse and the manufacturer won't be able to produce it in the foreseeable future) then the branch associated with this situation ends with a customer

notification and the whole process instance ends. Another possibility of output of the decision block is insufficient quantity in the warehouse of the vendor while it is possible to order the product from a supplier. If this is the case, an order is sent to the supplier and i tis necessary to wait for the delivery. This is represented by a transition event called "Waiting for the ordered goods". If the shipment of goods arrives from the supplier, the transition event passes to the decision block, where the order is re-verified by telephone. The re-verification is necessary because the delivery may take several days and the vendor needs to know if the customer is still interested in buying the goods. If the customer confirms the order, then the customer order processing process continues with the sub-process "Expedition of goods", but if he is no longer interested the process instance terminates. The third branch leading from the decision block represents a situation, in which the goods are in stock in sufficient quantity. If this is the case, the vendor sents a confirmation of the order to the customer and simultaneously the sub-process "Expedition of goods“ may start. Here we can see that the Expedition department is responsible for the process "Expedition of goods" (i.e. the Expedition department owns this process) and this process internally consists of three sub-processes: "marking of goods", "packaging of goods" and "issuing an invoice". The goods packaging process is sequentially tied to the goods marking process, however, the invoice issuing process can be done in a parallel manner. When the goods are packaged and the invoice is issued, shipping is ordered from a courier service, which is a process owned by The Sales department. After the confirmation of the transport by the courier it is needed to wait for the courier, who will take over the shipment. Waiting for the courier is represented by a transition event called "Waiting for the courier".

5 Conclusion

We have developed a new diagram technique, which is specialized for providing the global overview of the internal composition of complex processes. It is intended mainly for complicated processes consisting of many hierarchical levels of sub-processes. In chapter 2, we explained that classical diagram techniques, such as process thread diagrams, flowcharts or BPMN diagrams, are not suitable for this purpose because they have their shortcomings described above. Thus, we believe that this new diagram technique is a contribution to business process modelling, since it is able to connect information in individual flowcharts or BPMN diagrams representing the flow of the individual sub-processes and provide a global overview of the whole process. This can be very useful not only for the owner of the process in managing it, but also for the designers of an information system intended to support the proper running of the process and the individual sub-processes it consists of.

Fig. 10: An example of the internal structure of a customer order processing process displayed by the composition diagram of a complex process



Resources

Davenport, T., & Short, J. (1990, January 01). The new industrial engineering : Information technology and business process redesign. Retrieved January 8, 2020, from http://dspace.mit.edu/bitstream/handle/1721.1/48613/newindustrialeng00dave.pdf.

Jurík, P. (2018). *Informačné systémy v podnikovej praxi (2nd ed.)*. Nové Zámky, Slovak Republic: Tlačiareň MERKUR, s. r. o.

Révészová, L., & Paľová, D. (2009). *Základy modelovania podnikových procesov (1st ed.).* Košice, Slovak Republic: Technical University in Košice.

Robson, M., & Ullah, P. (1998). *Praktická príručka podnikového reengineeringu (1st ed.).* Praha, Czech Republic: Management Press.

Schmidt, P. (2010). *Procesný prístup k IS organizácie* (Doctoral dissertation, University of Economics Bratislava, 2010) (pp. 89-91). Bratislava, Slovakia republika: EU Bratislava.

THE IMPACT OF DIGITAL TECHNOLOGY ON THE ECONOMICS OF CONSTRUCTION

Svetlana Kolobova[20] , Anastasiya Magina[21]

Abstract
Information and communication technologies (IKT) have a huge impact on the development of the construction industry, they have become a part of modern management systems of the construction economy. Achieving the efficiency of the digital economy is possible through the introduction of innovative technologies for processing the growing volume of data every year, which will reduce costs in the construction and provision of housing and communal services. The article discusses the impact of digitalization on the economy of the construction industry. Digital technologies, such as Bim, Big Data, 3D printing, significantly reduced the cost, simplified and accelerated the construction process. It is interesting to consider how these introductions affected the material part of the process. Whether the costs of construction enterprises have become lower at this time, or whether the cost reduction will be noticeable in the long term.

Keywords
Digitalization, construction, economics, engineering.

1 Introduction

A prerequisite for digitalizing the economy of the construction industry is to achieve a high level of informatization and automation. On this basis, in addition to programs and projects in the digital economy, there are also programs and projects in the field of developing information infrastructure and implementing automated information systems.

Today, the word digitalization means translating information into digital form. Currently, digitalization in the construction industry is developing in many business processes.

Digital transformation is not just the introduction of new digital technologies, it is an implementation that often requires a revision of the business model itself. The company not only receives a tool that allows it to work more efficiently, but also technology, which can be maximizing by changing the course of action and changing the business model. In this regard, the introduction of digital initiatives is often cross-functional projects that require significant input and open discussion from the representatives of many departments of the company.

All this pursues constant growth due to the introduction of advanced innovative technologies, the provision of improved housing and better housing and communal services, as well as the creation of an optimal development plan for the country based on the analysis of existing data using digital technologies.

For this, it is necessary to carry out such changes as increasing the use of BIM technologies in the construction of residential infrastructure, reducing the interaction of

[20] Moscow State University of Civil Engineering, Institute of Economics, management and information systems in construction, Department of social, psychological and legal communications 26 Yaroslavskoye shosse, 129337, Moscow, Russia, KolobovaSV@mgsu.ru

[21] Moscow State University of Civil Engineering, Institute of Economics, management and information systems in construction, Department of social, psychological and legal communications 26 Yaroslavskoye shosse, 129337, Moscow, Russia, MaginaAI@mgsu.ru

developers and the government, creating a better structure for the collection and disposal of construction waste, as well as ensuring un uninterrupted operation of housing and communal services.

Another element of digitalization will be the introduction of a single digital platform in the urban area, that is, a place where all participants in the construction process, including government, can interact. This platform will include information about land plots, plans for engineering communications and networks, and a personal account will be creating for each participant in urban development activities, which will contain all information on projects. The platform will present automated solutions such as registration and identification of construction sites, development of territorial planning projects using mathematical analysis and forecasting methods, and verification of the construction object for compliance with standards and requirements. Urban planning decisions will require methods of multi-factor comparative analysis of alternative scenarios of city development using digital 3D models.

This will also be an internal segment for employees of government agencies that provide services to construction companies, as well as organizations that support mechanisms for electronic approval of decisions on a construction project. Electronic coordination mechanisms should be implementing in accordance with the principles of the BPM (Business process management) concept. These activities include: the introduction of innovative Smart city technologies for the organization of a smart construction site, the creation of an integrated information system for managing all types of waste on construction sites, the use of smart contracts in construction, as well as the use of virtual and augmented reality for the construction of a smart home.

2 Literature review

Many experts, such as Gram-Hanssen, Darby, Jacobson, Boldt & Carlson agree that there is a risk that, simply by copying products, ideas and initiatives sprouted on foreign soil (in the corporate culture of the company that best meets the requirements of digital transformation), we will not be able to fully instill them in ourselves in the future and use and develop effectively (Gram-Hanssen & Darby,2018, Jacobson, Boldt, & Carlson,2016).

Without changing the corporate culture, companies automatically program themselves for a constant technological lag. Hamdy, Carluccia, Hoes & Hensen did research on the problem (Hamdy, et al, 2017). Many initiatives will be implementing with great difficulty or not implemented at all, and instead of proposing their ideas, others will be constantly copying, moreover, with a delay of several years (we begin to apply the technology at a time when the leader has already implemented it and moves to the next technological level).

Despite the fact that the term “digitalization” appeared relatively recently, the phenomenon itself for several years seems to be the subject of the careful study by the global and domestic business community. Ott & Bolliger explored the issue in his works Ott & Bolliger, 2015). This interest is primarily due to the fact that in a highly competitive environment, digitalization is perceiving not only as an opportunity for further technological development, but also as a certain threat to the existing business model of the company Currently, the construction industry is as follows: almost 95% of public services in the construction industry are carried out electronically, the environment is improved and brought into satisfactory form, in which it will be easy for the company to use information models and BIM technologies, and the Smart Standard for implementing comfortable urban environment, which contains recommendations on the use of advanced technologies, the information and technological environment of executive authorities has been formed, which, when Wang ensure efficient interaction of developers with the executive authorities, together with the unified information system set up, designed to be a common information environment for the whole sphere of urban planning, as well as in the capital, launched a new phase of the program of

renovation of the housing stock . The author, in the article «Economic efficiency of the state program of renovation in Moscow», notes that in the process of renovation, the city will receive qualitatively new areas. The design parameters that are being calculated today increase the density by about 2.5 times. The city will have modern neighborhoods, parks, squares and new social facilities» (Kolobova, 2018). The author proposes a mechanism for the relationship of entrepreneurs with each other, with residents of built-up areas and with representatives of state authorities in the framework of legal regulation (Kolobova, 2019). Russian scientists Volkov, Sedov & Chelyshkov studied the issue of building information modeling (BIM) and believe that it is a powerful technology that is used to support decision-making about construction throughout its life cycle (Volkov, Sedov & Chelyshkov, 2015).

In the future, digitalization may lead to such changes as the implementation of "green construction," that is, the energy-efficient technologies that will minimize waste both during the construction of the building and during its subsequent operation will be using in the construction procedure. Digitalization of construction processes and the introduction of BIMtechnologies will significantly reduce the time, and with them the costs of capital construction, as well as implement the procedures necessary for the construction of real estate will be possible in a shorter time. Thanks to the intelligent analysis of city data, there will be an improvement in the quality of documentation necessary for territorial planning and urban planning zoning. In their research, scientists Gustafsson, Dipasquale, Poppi, Bellini & Holmberg believe that the procedure for detecting violations will be simplifying, quality control of construction will improve, timely checks will be providing to ensure that the developer fulfills its obligations (Gustafsson ,et al, 2017).

The principle of consistent implementation and gradual scaling will be applied on the basis of pilot projects on a territorial and functional basis, including for continuous improvement of interagency cooperation, clarification of initiatives and plans, standards, regulatory, organizational, technological documents, analysis and identification of promising directions for the implementation of the city's strategy Moscow. Energy and emission analysis of scenarios for renovation of the Moscow residential area was carried out by scientists Paiho, Abdurafikov (Paiho,Abdurafikov,et al, 2014, 2015). Foreign scientists Parag, Butbul, Salvalai, Sesana, Iannaccone, Schiewecka, Uhdea, Salthammera, Lea, Morawska, Mazaheri & Kumar have also studied the economic efficiency of renovation of residential buildings in other countries (Parag & Butbul, 2018, Salvalai, Sesana & Iannaccone, 2017, Schiewecka, et al,2018).

3 Materials and methods

The introduction of information modeling technology (TIM) of capital construction projects is actively encouraged by the Russian government. By 2030, the share of design organizations using TIM in practice should be brought up to 70%. To achieve the presented goals, the following tasks will be solved. Under state and municipal contracts:

- simplification of the composition of the justification of investments when concluding a contract for the design, construction and commissioning of capital construction facilities at the same time, as well as the determination of cases in which preparation of the justification of investments is not required;
- expanding the scope of the life cycle contract for the operation phase in relation to all facilities specified in the Decree of the Government of the Russian Federation of November 28, 2013 No. 1087;

- establishing the possibility of concluding contracts for a period exceeding three years in relation to life cycle contracts and contracts for the design, construction and commissioning of capital construction facilities;
- establishing the possibility of concluding a separate contract for the development of investment justification;
- inclusion in the standard conditions of state and municipal contracts, standard contracts the possibility of establishing the obligation of the contractor to use TIM;
- approval under the standard conditions of state and municipal contracts, standard contracts, requirements for the result of information modeling, rules for maintaining an information model, requirements for submitting an information model to the state examination bodies of project documentation;
- phased introduction of the obligation to develop a justification of investments, design and construction using TIM. In the framework of the development of information modeling in construction in general:
- Creation, continuous updating and provision of free access to the classifier of construction information;
- taking into account when applying a risk-based approach in the field of control and supervisory activity of the fact of maintaining an information model and its provision to regulatory and supervisory authorities;
- the introduction of the right to submit for examination as part of project documentation an information model in a non-proprietary, standardized format with the possibility of reducing the cost and terms of examination;
- translation of the executive documentation, general and special journals into electronic form;
- the formation of a regulatory framework for a three-dimensional description of a building and structure in the unified state register of real estate and the state information system for providing urban planning activities, determining the possibility and procedure for forming a technical plan in the framework of information modeling of capital constructio4n objects;
- inclusion of information on information modeling technology in educational programs in the field of design, construction and operation of capital construction facilities;
- the creation, at the expense of the federal budget, of a special fund for supporting the development of information modeling, which will provide individuals engaged in designing with a one-time subsidy to compensate up to 50% of the cost of training personnel in information modeling technology.

Leading foreign construction companies, using artificial intelligence, perform all operations much faster, more efficiently, significantly reducing the cost of their products and increasing sales. At the same time, robots are optimally built on the basis of analysis of huge data arrays, analytical systems help control the profitability of each square meter, and predictive analytics allows optimal maintenance of equipment. Today, these and many other digital technologies are already implemented and improved further by world leaders in the construction industry, leading to increased profitability in general.

4 Results

The following tasks will be solved:

- creating a system for assigning unique numbers to each capital construction facility and introducing the obligation to use these numbers instead of describing capital construction objects (ACS) when interacting with state bodies, local authorities in the implementation

of procedures in the areas of construction, execution of state functions, as well as with organizations performing operation of engineering networks;

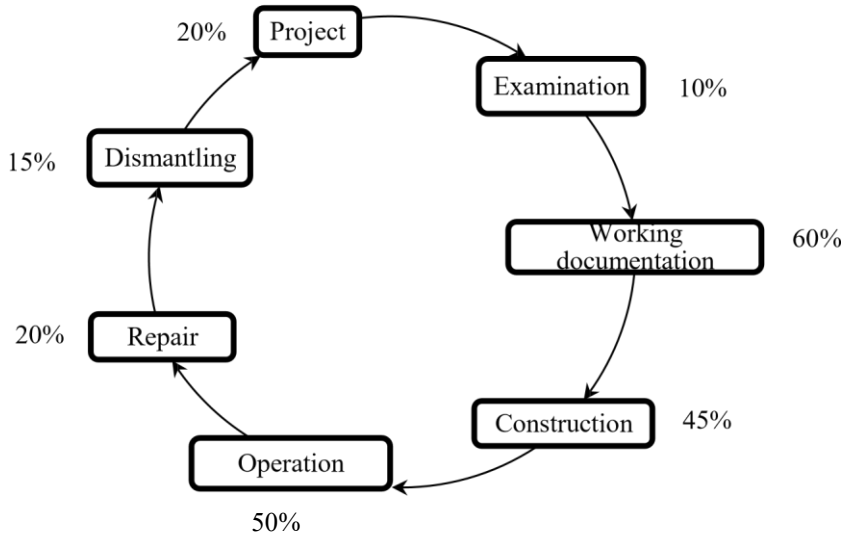
- creation of a system for assigning unique numbers to each document transferred for storage to the information system of bodies and organizations of the public sector and introducing the obligation to use these numbers instead of sending the relevant documents to state bodies, local authorities in the implementation of procedures, the performance of state functions, as well as organizations operating networks of engineering and technical support;
- Exclusion of the requirement to provide the applicant with the information available to the public authorities, local authorities and state-regulated information systems (IP);
- ensuring the legal possibility of interaction between information systems in which the developer maintains a database of ACS with information systems designed to carry out procedures in the construction industry;
- Creation of a system for storing information systems in the field of operation of buildings and structures in the IP of public sector bodies and organizations;
- inclusion in the composition of the executive and operational documentation of information about accidents and accidents during construction and operation;
- translation into machine-readable format of documents issued according to the results of urban planning procedures;
- the introduction of the principle of "one-stop shop", in which the applicant should not be obliged to support many personal accounts in various information systems for undergoing all procedures in electronic form;
- when carrying out procedures in electronic form, interdepartmental electronic interaction (including for the purpose of verifying the authenticity of a document) should be organized mainly between public authorities and IP, ensuring the storage of documents in electronic form. It is necessary to minimize the provision of information by some public authorities to other authorities;
- the general rules for storing information and documents of the city-planning sphere in electronic form and their provision will be determined by analogy with the requirements of the legislation on archiving;
- the types of generalized data were determined at all stages of the life cycle, the collection of which from IP is necessary for the implementation of state policy in the urban development sphere, as well as in the activities of participants in urban development relations.

It is planned to expand the use of BIM-technologies at all stages of construction, from planning to the conservation phase. Using the creation of digital doubles, it will be possible to monitor the state of construction projects, predict the need for ongoing and overhaul infrastructure, and digital doubles can be used by rescue services to work more efficiently. Automation of control systems will allow monitoring engineering systems and collecting information about the state of structural elements of the building. To improve the work of utilities, a city geoportal will be created, on which digital models of all the buildings under their jurisdiction will be presented, access to data will be provided according to the terms of reference.

Let us consider how the introduction of BIM technologies at each stage of the life cycle of a construction object will affect the cost. One of the most important stages of the life cycle is operation and repair; they need BIM technologies for a long time during the period of physical wear. Since the timing of these periods depends on the material of the building, the exact time of these stages cannot be said. However, with the development of the figures, the costs and labor intensity of these works will decrease. According to expert estimates of construction organizations, the implementation of BIM technologies saves at each stage of the life cycle:

project 20%, examination 10%, working documentation 60%, construction 45%, operation 50%, repair 20%, dismantling 15%. The cost reduction scheme is presented in Figure 1.

Fig. 1: Reduced labor costs at the stages of the construction project life cycle after the introduction of BIM-technologies



It is also interesting to see how the introduction of BIM technologies will affect the reduction in the construction time of a residential property. According to construction experience over the past 3 years, the average cost of building a single-section 17-story building will cost 195 million rubles (https://stroy54.ru/productlist/stroitelstvo/raschetstoimosti-stroitelstvaobektov/raschetstroitelstva-17-ti-etazhnogo-zhilogo-doma/). Thus, a residential complex of 4 two-sectional model houses will be averaged to cost 1.6 million rubles. It can be seen from the graph (Figure 2) that in the case without the use of BIM technologies, most of the investments are distributed at the end of the construction process, therefore, the time to wait for a return of money is lower than in the second case, however, the advantage of the construction option using BIM technologies is to reduce the time construction of the facility for a year. The introduction of BIM-technologies will certainly entail an increase in non-recurring costs by at least a third, however, a faster return on investment makes the second option more attractive.

Fig. 2: Decrease in the construction time of residential real estate before and after the introduction of BIM-technologies

5 Discussion and conclusions

Thus, most of the costs due to the introduction of BIM-technologies will decrease at the stages of working documentation, operation and construction up to 50%. It also revealed a decrease in labor costs at the stages of the life cycle of a construction project after the introduction of BIM technologies by about a third.

Therefore in 2021, a legislative obligation will be introduced for state bodies and state corporations to carry out the design of buildings and structures only on the basis of BIM technologies. All this will create the so-called unified digital environment.

Hence by 2030, all procedures in the construction industry will be converted to electronic form. It is forbidden to interact in paper form, except for procedures that cannot be implemented without paper media.

Resources

Gram-Hanssen, K., & Darby, S. J. (2018). "Home is where the smart is"? Evaluating smart home research and approaches against the concept of home. Energy Research & Social Science, 37, 94-101. doi: 10.1016/j.erss.2017.09.037

Gustafsson, M., Dipasquale, C., Poppi, S., Bellini, A., Fedrizzi, R., Bales, C., Ochs, F., Sié, M.. & Holmberg, S. (2017). Economic and environmental analysis of energy renovation packages for European office buildings. *Energy and Buildings, 148*, 155-165. doi:10.1016/j.enbuild.2017.04.079

Hamdy, M., Carlucci, S., Hoes, P., & Hensen, J. L. (2017). The impact of climate change on the overheating risk in dwellings—A Dutch case study. *Building and Environment, 122*, 307-323. doi:10.1016/j.buildenv.2017.06.031

Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems, 56*, 719-733. doi:10.1016/j.future.2015.09.003

Kolobova, S. (2018). Economic efficiency of the state program of renovation in Moscow. *MATEC Web of Conferences, 170*, 01082. doi:10.1051/matecconf/201817001082

Kolobova, S. (2018). Evaluation of economic efficiency of the state programme of renovation of residential buildings in Moscow. *MATEC Web of Conferences, 193*, 05023. doi:10.1051/matecconf/201819305023

Kolobova, S. V. (2019). Organizational and Economic Mechanism of Investment Management in the Renovation of Residential Buildings in Moscow. *IOP Conference Series: Earth and Environmental Science, 272*(3), 032226. doi:10.1088/1755-1315/272/3/032226

Ott, W., & Bolliger, R. (2015). Pitfalls in the Economic and Ecological Evaluation of Energy Related Building Renovation Strategies and Measures. *Energy Procedia, 78*, 2340-2345. doi:10.1016/j.egypro.2015.11.395

Paiho, S., Abdurafikov, R., Hoang, H., & Kuusisto, J. (2015). An analysis of different business models for energy efficient renovation of residential districts in Russian cold regions. *Sustainable Cities and Society, 14*, 31-42. doi:10.1016/j.scs.2014.07.008

Parag, Y., & Butbul, G. (2018). Flexiwatts and seamless technology: Public perceptions of demand flexibility through smart home technology. *Energy Research & Social Science, 39*, 177-191. doi:10.1016/j.erss.2017.10.012

Salvalai, G., Sesana, M.M., & Iannaccone, G. (2017). Deep renovation of multi-storey multi-owner existing residential buildings: A pilot case study in Italy. *Energy and Buildings, 148*, 23-36.

Schiewecka, A., Uhde, E., Salthammer, T., Salthammer, L. C., Morawska, L., Mazaheri, M., & Kumar, P. (2018). Smart homes and the control of indoor air quality. *Renewable and Sustainable Energy Reviews, 94*, 705-718. doi:10.1016/j.rser.2018.05.057

Volkov, A. A., & Batov, E. I. (2015). Dynamic Extension of Building Information Model for “Smart” Buildings. *Procedia Engineering, 111*, 849-852. doi:10.1016/j.proeng.2015.07.157

Volkov, A.A., Sedov, A.V. & Chelyshkov, P.D. (2015). The Concept of "Smart city", Monograph, Moscow state University of civil engineering, EBS ASV, Moscow, p. 7.

Wilson, C., Hargreaves, T., & Hauxwell-Baldwin, R. (2017). Benefits and risks of smart home technologies. *Energy Policy, 103*, 72-83. doi:10.1016/j.enpol.2016.12.047

FINDING A MODULAR STRUCTURE OF THE KUKA INDUSTRIAL WELDING ROBOT MAIN CONTROL PROGRAM NEEDED FOR ITS EFFECTIVE TESTING

Igor Košťál[22]

Abstract
Each KUKA industrial robot of a robotic workstation is controlled by some main control program that has some modular structure. For an effective testing of the KUKA industrial welding robot main control program the operator needs to know what a modular structure of this control program is. We have created a .NET application that connects through the Intranet to the robot control PC and searches for the directories with SRC and DAT files of all robot control programs on its hard drive. This application provides then complete modular structure of a robot main control program and further related information to the user on its output. On the basis of this found a modular structure of a robot main control program, the operator can choose an effective strategy for its testing.

Key words
robot, Tool Center Point, KRL program, modular structure of a robot main control program, testing and retesting robot

1 Introduction

Testing of particular robots of a robotic workstation is very important part of creating such workstation. For KUKA industrial welding robots, this is our case, testing the precision of the Tool Center Point (TCP) of a robot tool motion, i.e. the precision of welds positioning on a given product and with this closely related activities is very important. Whole robot activity is controlled by its control program, which mostly contains several subprograms. Therefore, if the welding robot operator wants to test the precision of the TCP of a robot tool motion, he has to know a robot main control program and its subprograms, modules, in order to know which modules he needs to test. There are many various other programs, as are testing, service and others, besides a robot main control program on the hard drive of the robot control PC. Besides that a robot can be programmed either as operating autonomously or as operating in a robotic workstation. Structures of main control programs of these two robots are different. Therefore, it need not be immediately clear to the robot operator which from programs stored on the hard drive of the robot control PC is a main control program and what is its structure. We have created a .NET application that is able to connect to the robot control PC through the Intranet, on its hard drive searches for the robot main control program and its subprograms, modules, and provides them to the user on its output.

The paper deals with ways which our .NET application uses for finding a modular structure of the KUKA welding robot main control program and its outputs, which it can provide to the robot operator during preparations of a testing procedure of particular KUKA welding robots that work either in a robotic workstation or as autonomous robots. Procedures of finding a modular structure of the KUKA industrial welding robot main control program used by our .NET application and its outputs mentioned in this paper relate to a given robot, which is the

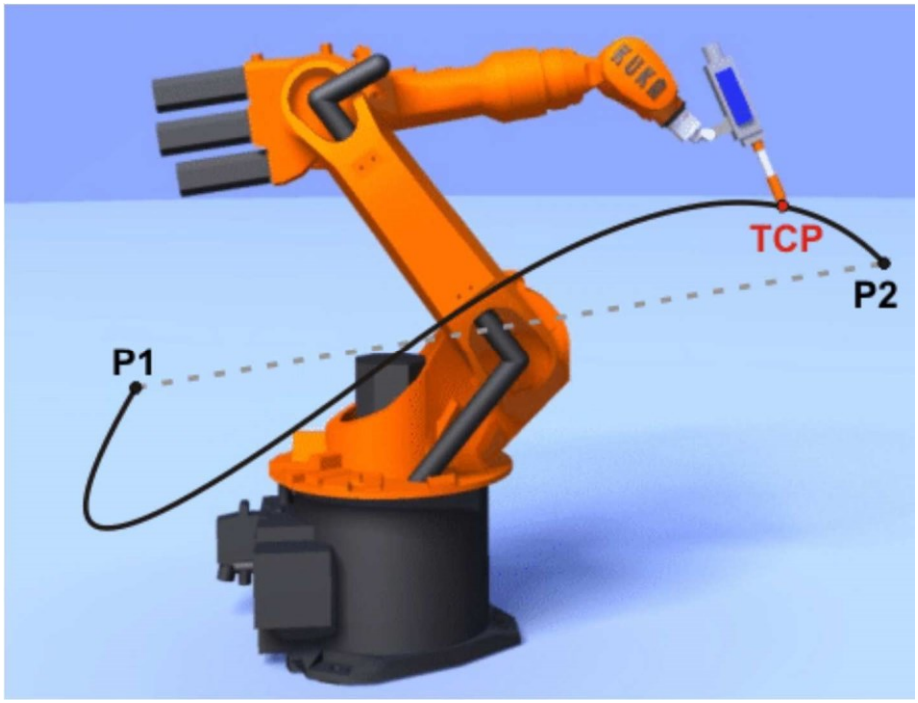
[22] University of Economics in Bratislava, Faculty of Economic Informatics, Department of Applied Informatics, Dolnozemská cesta 1, 852 35 Bratislava, Slovakia, e-mail: igor.kostal@euba.sk.

part of robotic workstation welding a cooling system radiator bracket of a passenger car. Our .NET application can be also used for finding a modular structure of another KUKA welding robots of this workstation main control programs.

2 A KUKA Welding Robot Control Program, Its Modular Structure

As we mentioned in the previous chapter, testing the precision of the TCP of a robot tool motion is very important for KUKA welding robots. By this is given the precision of welds positioning by robot tool, for example by welding pliers, on a given product. This robot tool is mounted on the mounting flange of a robot. During tool calibration, the robot operator assigns the working point to this tool. This point is called the TCP (Tool Center Point).

Fig. 1: TCP of a robot *tool*



Source: (KUKA, 2012)

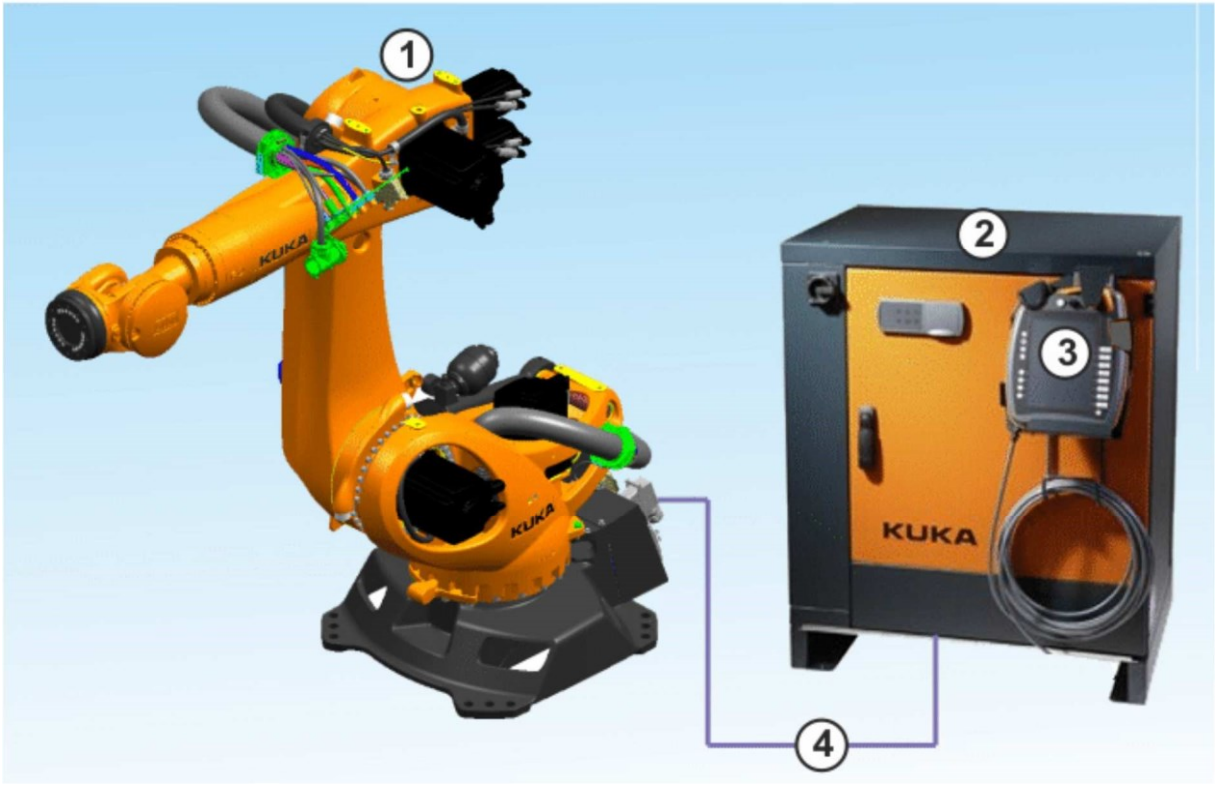
All motions of the TCP are controlled by a robot control program. This control program of the KUKA industrial welding robot, which controls the TCP of a robot tool motion, is created in the KUKA Robot Language (KRL). Its syntax allows developers motion programming, a program execution control, programming inputs/outputs, programming subprograms and functions, etc.

We can create two kinds of KRL programs:

- a motion program (KUKA, 2012)
- a SUB program, that can perform operator control or monitoring tasks, for example, monitoring of a robot safety equipment or monitoring of a robot cooling circuit. However, some KRL instructions can be used in a SUB program. These programs are always files with the extension *.SUB (KUKA, 2012).

The motion program runs in the robot interpreter and a SUB program runs in the Submit interpreter. Both interpreters run in parallel on the robot control PC. (KUKA, 2012)

Fig. 2: A KUKA industrial robot: 1 Robot, 2 Robot controller (includes a Robot control PC), 3 Teach pendant, 4 Connecting cables



Source: (KUKA, 2013)

A KRL motion program generally consists of an SRC file and a DAT file of the same name. An SRC file contains the program code and a DAT file contains permanent data and point coordinates. The DAT file is also called a data list. The SRC file and associated DAT file together are called a **module**. (KUKA, 2012)

3 Ways of Finding a Modular Structure of the KUKA Industrial Welding Robot Main Control Program Using Our .NET Application

During finding a modular structure of the KUKA welding robot main control program our .NET application searches for an important information in various configuration and program files stored on the hard drive of the robot control PC and works also with several KRL statements. We describe these statements briefly.

CWRITE statement (KUKA, 2000)

enables texts to be written to an open channel, or commands to be written to a command channel (our case in the *SPS* program).

Syntax

CWRITE (Handle, *State*, *Mode*, *Format*, Var1, ..., VarN)

Handle - The "Handle" variable of type "INT" is transferred by "COPEN" or the predefined variable "$CMD" (our case in the *SPS* program).

State - "CMD_STAT" is an enumeration type which is the first component of the *State* variable of the structure type "STATE_T".

"CMD_STAT" can have the following values which are relevant for CWRITE:

CMD_OK - Command successfully executed;

DATA_OK - The command has been successfully executed. Data are ready to be read as a reply;

CMD_ABORT - Command not successfully executed because "HANDLE" is not valid;

CMD_REJ - Only with Weltronic protocol: BCC error;

CMD_SYN - Syntax error in the command;

FMT_ERR - Incorrect format specification or non-corresponding variable.

Another component of the status variable that is important for "CWRITE": HITS - Number of correctly written formats.

Mode - Variable of type "MODUS_T" (structure type) defining how the channels are written to. It can have the following values:

SYNC - The statement is not executed until the data have been sent to the partner station; ASYNC - The statement is not executed until the channel driver has confirmed that the data have been received.

Format - The variable "Format" of type "CHAR[]" contains the format of the text that is to be generated.

Var - The variables corresponding to "Format".

The value of "Mode" is not relevant for writing to the command channel. If "Mode" is a non-initialized variable in the other cases, the statement is aborted and an error flag is set in the variable "Status".

If "Mode" has a value other than SYNC or ASYNC, data are written to the channel in the SYNC mode.

CHANNEL statement (KUKA, 2000)

is used for declaring signal names for input and output channels.

Syntax

CHANNEL :Channel_Name: *Interface_Name Structure_Variable*

Channel_Name - Any symbolic name.

Interface_Name - Predefined signal variable: SER_1 - serial interface 1; SER_2 - serial interface 2.

Structure_Variable - System-dependent structure variable specifying the protocol. Evaluation is not carried out.

The robot controller contains two classes of interface: • simple process interfaces - **signals** – and • logic interfaces - **channels**.

All of the interfaces are addressed using symbolic names. The specific interface names (symbolic names) are logically combined with the predefined signal variables for channels by means of the CHANNEL declaration.

The predefined signal variables for channels are

• **SER_1** and

• **SER_2**

for the serial interfaces, and

• **$CMD (e.g. "RUN....")** (our case in the SPS program) for the command interpreter.

The procedure for accessing channels is the same. In order to be able to access a channel, it must be declared in the "CHANNEL" declaration.

The variables are predefined in the system file `$custom.dat (directory ". . . \KRC\STEU\Mada") ":SER_1" and ":SER_2".`

The channel can then be opened with the "COPEN" statement. The "CREAD" statement can be used to read the channel, while the "CWRITE" statement is used to write to the channel. The channel is closed with the "CCLOSE" statement.

4 A Procedure of Finding a Modular Structure of the KUKA Welding Robot Main Control Program by Our .NET Application

Our .NET application uses the following procedure for finding a modular structure of the KUKA welding robot main control program:

1) First it searches for the following line in the system file *$custom.dat*

```
$PRO_I_O[]="/R1/SPS()"
```

because the program defined in this line is started in the Submit interpreter which starts automatically when the robot controller is switched on. If the *SPS* program is defined in this line (our case), then .NET application supposes that the robot main control program will be controlled centrally by the higher-level controller PLC and it searches for the *sps.sub* source file of this program on the hard drive of the robot control PC in the next step. If the *SPS* program is not defined in the mentioned line, but a different SUB program is in this line, then our .NET application supposes that the robot main control program will not be controlled centrally by the PLC. In this case, the .NET application will search for this different SUB program and try to find a modular structure of the KUKA welding robot main control program from its source file.
2) If our .NET application continues searching for the *sps.sub* source file of the *SPS* program, then it searches for the *CWRITE* statement in this source file. In the *sps.sub* file of our robot the .NET application will search it in the following *IF* statement

```
IF $MODE_OP==#EX THEN
    CWRITE($CMD,STAT,MODE,"RUN /R1/CELL()")
      ENDIF
```

This *IF* statement examines whether the robot is switched to the Automatic External mode. This is the operating mode in which our robot operates at programmed velocity in a serial production, when it is controlled together with other robots of a robotic workstation by the PLC. If this robot is switched to the Automatic External mode `($MODE_OP==#EX)`, then the statement `CWRITE($CMD,STAT,MODE,"RUN /R1/CELL()")` is executed, which, besides other, starts up the *CELL* main control program of our robot.

3) Next the .NET application searches for the *cell.src* source file of the *CELL* main control program of our robot. This source file was created by a robot programmer using the *Cell* template. A programmer only changed and added some parts of this source file. In this source file the .NET application searches for the *SWITCH* statement placed in the *LOOP* statement, from which it can find a modular structure of our robot main control program. A mentioned sequence of the source code of the *CELL* program is displayed in the following figure.

Fig. 3: The part of the cell.src source file of the CELL program

```
;FOLD AUTOEXT INI
P00 (#INIT_EXT,#PGNO_GET,DMY[],0 ) ; Initialize extern mode
;ENDFOLD (AUTOEXT INI) LOOP
     P00 (#EXT_PGNO,#PGNO_GET,DMY[],0 ) ; The robot controller calls the
program number from the PLC.
      SWITCH  PGNO ; Select with Program number
      CASE 1 ; CASE branch for program number == 1
            P00 (#EXT_PGNO,#PGNO_ACKN,DMY[],0 ) ; Receipt of program number
1 is communicated to the PLC.
            csrb325 ( ) ; The programmer-defined program csrb325 is called.
     CASE 10
            P00 (#EXT_PGNO,#PGNO_ACKN,DMY[],0 )     milling_caps ( )
     CASE 11
            P00 (#EXT_PGNO,#PGNO_ACKN,DMY[],0 )     replacement_caps ( )
     CASE 12
            P00 (#EXT_PGNO,#PGNO_ACKN,DMY[],0 )     service_position ( )
     CASE 13
            P00 (#EXT_PGNO,#PGNO_ACKN,DMY[],0 )     brake_test ( )
     CASE 14
            P00 (#EXT_PGNO,#PGNO_ACKN,DMY[],0 )     masref_main ( )
     DEFAULT ; DEFAULT = the program number is invalid.
            P00 (#EXT_PGNO,#PGNO_FAULT,DMY[],0 ) ; Error treatment in the
case of an invalid program number
     ENDSWITCH
ENDLOOP
```

Source: (author)

In this sequence of the source code our .NET application is able to identify particular subprograms of the robot main control program *csrb325*, *milling_caps*, *replacement_caps*, *service_position*, *brake_tes*t and *masref_main*, which create with their SRC and DAT files modules of the robot main control program. These modules together with the CELL main control program create the modular structure of our robot main control program. Now our .NET application found the complete modular structure of the KUKA industrial welding robot main control program. The robot operator has an exact information, which subprograms, modules, of the robot main control program will test.

5 A .NET Application Finding a Modular Structure of the KUKA Industrial Welding Robot Main Control Program

Our .NET application was developed in the C# language in the development environment Microsoft Visual Studio 2017 for the Microsoft .NET Framework version 4. Therefore this

framework must be installed in the compatible operating system, for example Microsoft Windows 8.1, 64 bit, of the computer on which our application runs. This .NET application finds a modular structure of the given KUKA industrial welding robot main control program needed for its effective testing. The control computer name of this KUKA welding robot is KUKA-NG6FHLRLN2.

Immediately after the start-up our .NET application attempts to connect through the Intranet to the robot control PC and searches for the directories with DAT and SRC files, which needs for finding a modular structure of the given KUKA industrial welding robot main control program. When the .NET application is connected to the correct directories on the robot control PC hard drive, then it will find a modular structure of this given robot main control program. This application will display the results of finding this modular structure in its text box. Besides that the .NET application also creates the disk file with the name, for example, `modular_struct_control_prog_KUKA_NG6FHLRLN2_20200220_213022.DTX` containing the date and time when the file was created (2020-02-20 21:30:22). This file will contain the same data as the .NET application displayed in its text box.

*Fig. 4: The file modular_struct_control_prog_KUKA_NG6FHLRLN2_*

20200220_213022.DTX with the results of finding a modular structure of the given robot main control program (the .NET application displays the same outputs in its text box)

```
The modular structure of the KUKA industrial welding robot main control
program with the control computer name KUKA-NG6FHLRLN2 and details this
program operation (found on 2020-02-20 21:30:22Z)


Robot processes are controlled centrally and synchronized with other processes
of a robotic workstation robots by the PLC.


The parts of modular structure of the robot main control program:
 the main control program:
CELL              (cell.src, without a DAT file) (. . .\KRC\R1)


the subprograms (modules)
(all in . . .\KRC\R1\Program\Programs):
csrb325                 (csrb325.src, csrb325.dat) milling_caps
      (milling_caps.src,          milling_caps.dat)          replacement_caps
(replacement_caps.src,         replacement_caps.dat)        service_position
      (service_position.src, service_position.dat)
brake_test   (brake_test.src, brake_test.dat) masref_main  (masref_main.src,
masref_main.dat)
```

Source: (author)

The output of our .NET application displayed in Fig. 4 provides to the robot operator useful information, that this given robot is controlled centrally and synchronized with other processes of a robotic workstation robots by the PLC, it has the ***CELL*** main control program, which has subprograms ***csrb325***, ***milling_caps***, ***replacement_caps***, ***service_position***, ***brake_test*** and ***masref_main***. These subprograms with their SRC and DAT files create modules of the robot main control program, which together with the *CELL* main control program create the **modular structure of the given robot main control program**. These are very valuable information for the robot operator in a preparatory stage of testing or retesting of this robot, because they saves his time and his effort, which he would invest to finding the modular structure of this robot main control program. He need not manually examine, in our case 49

program source files on the hard drive of the robot control PC, in order to search this robot main control program with subprograms. From the output of our .NET application the robot operator has an exact information, which subprograms, modules, of the robot main control program will test. It makes a preparatory stage of testing and retesting of this given robot more effective.

Subprograms of the robot the *CELL* main control program have exactly determined purpose. Using the *csrb325* subprogram the robot carries out welding a given part of a cooling system radiator bracket of a passenger car. The robot uses remaining subprograms to carry out service operations. For example, if the cover caps of robot welding pliers spikes are worn, the TCP of the robot moves to the specified position, where these cover caps are milled (the *milling_caps* subprogram). If these cover caps are worn more than the permissible value, they are exchanged for new ones (the *replacement_caps* subprogram) in the TCP service position (the *service_position* subprogram).

6 Conclusion

Our .NET application provides to the robot operator exact information about the modular structure of the given KUKA industrial welding robot main control program by which it is able to make a preparatory stage of testing and retesting of this robot more effective and easier for him. He need not examine a relative considerable quantity of the robot programs source files that are on the hard drive of the robot control PC and need not search for the main control program between them. By this he saved much time, especially when a robotic workstation includes several KUKA welding robots. Sequential testing of robots is then clearly determined for the operator by the number of and names of subprograms of these welding robots main control programs. Thus, our .NET application can be a very effective software support for the operator during a preparatory stage of testing and retesting of subprograms of robots main control programs.

Resources

KUKA Roboter GmbH. (2000). *SOFTWARE KR C1 / KR C2 / KR C3, Reference Guide, Release 4.1*. [PDF]. Augsburg: KUKA Roboter GmbH.

KUKA Roboter GmbH. (2012). *KUKA System Software, KUKA System Software 8.2, Operating and Programming Instructions for System Integrators*. [PDF]. Augsburg: KUKA Roboter GmbH.

KUKA Roboter GmbH. (2013). *Controller, KR C4; KR C4 CK, Specification*. [PDF]. Augsburg: KUKA Roboter GmbH.

Adkinn. (2020). Technical documentation, API, and code examples. Retrieved March 17, 2020, from https://docs.microsoft.com/en-us/

MODERN APPROACHES OF CLIENT-SERVER APPLICATIONS DEVELOPMENT

Meiramgul Mukhambetova[23]

Abstract
In this article discusses emerging approaches for client-server applications development using the ASP.NET MVC 5. The concept of MVC (model-view-controller) pattern to optimizate the process creation of modern web and mobile interfaces. Improved features of the MVC 5 pattern as Bootstrap provides the ability to create adaptive client applications that can be easily works on all levels of hardware devices.

Key words
Client-server, application, ASP.NET MVC 5, Visual Studio, Visual C#, IIS (Internet Information Services)

1 Introduction

Information is an important and valuable resource of all sectors of the socio-economic sphere, as well as private individuals. Data transmission in the context of digitalization is growing every year. Today's corporate information systems must have flexibility, scalability and high performance.

As a modern technology to solve the problem of data management in many modern organizations, the client-server functions as a set of infrastructure or conglomerate combining a computer device and software for efficient computing (Yadav & Singh, 2009). Client-server technology operates in the structure of information systems through distributed database management systems and network services. Client-server architecture is used in two, three and multi-tier (also calls N-tier) structures. During the analyse of scientific works was given priority to the organization of modern client-server systems on three-level architecture (as an independent case of multi-level architecture). This is due to the fact that the modern Internetbased web application platform is implemented using a three-tier client-server architecture.

In this article describes of approaches use the ASP.NET MVC 5 Framework for developing web applications on the base multi-tier client-server architecture. Also consider of ways to use modern approaches in the computer science specialty educational process in teaching clientserver technologies.

2 Infrastructure ASP.NET MVC Framework

By adopting and adapting the MVC template, ASP.NET MVC Framework is a strong competitor to Ruby on Rails and similar platforms, bringing the MVC model to the forefront of the development of the .NET world . The MVC Framework is built as a set of independent components that satisfy the .NET interface or are based on an abstract base class. Components that are native to the routing system, visualization engine, and controller factory can be easily replaced with other components with their own implementation.

[23] L.N.Gumilyev Eurasian National University, Kazakhstan, mukhambetovamj@gmail.com

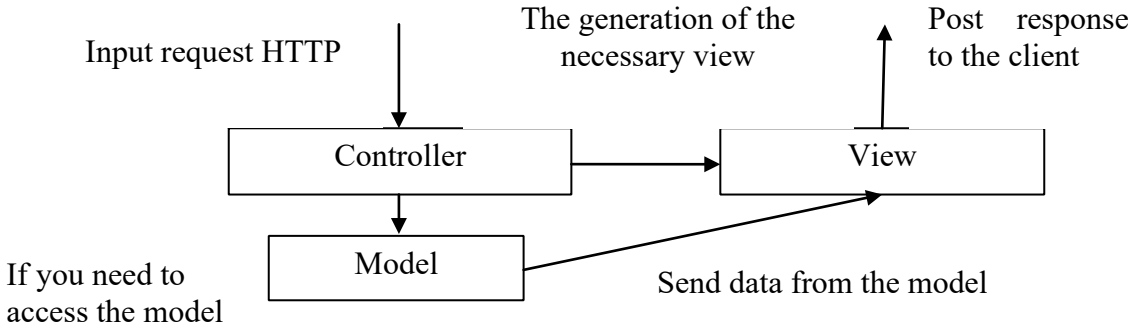
Components that are part of the routing system, visualization engine, and controller factory can be easily replaced with other components with their own implementation. In General the MVC Framework offers three features for each component:

- Using the standard component implementation as it is (this is sufficient for most applications).
- Creating a subclass from the standard implementation to correct existing behavior.
- Completely replace the component with a new implementation of the interface or abstract base class ("Advantages ASP.NET MVC", 2019).

MS SQL Server, IIS, and ASP.NET integration serves as an effective complex for building multi -level client-server applications. Since the hardware and software developer is a single company (Microsoft), matching objects and components is acceptable for programming (Grishchenko, 2013).

To connect configured servers to the web client interface ASP.NET MVC 5 Framework infrastructure implements through the Visual Studio Community 2017 environment.
The MVC structure consists of independent components, such as model-view-controller. The functions of each component are shown in the following figure 1.

Fig.1: Functions of the components in MVC structure

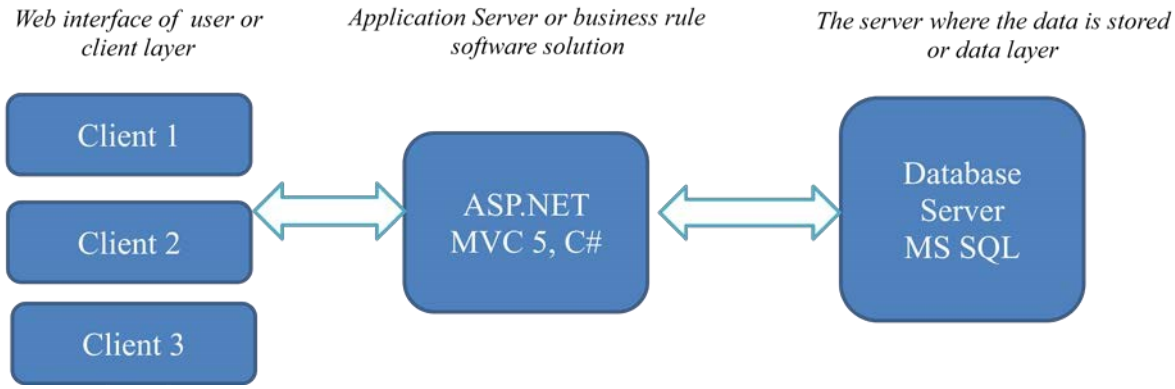


An important achievement of the latest fifth release of the MVC framework is the integration of the Bootstrap framework for creating adaptive applications. Adaptability - allows you to easily read client applications from any device. Here a web client application an automated read from to screens of different sizes. Therefore, you don't need to writing a mobile version of the apps. The results of simple and convenient innovative techniques will help to increase the speed of preparation of modern client-server applications.

3 Implementation of approaches

In our case the client-server system created was implemented on multi-tier client-server architecture. ASP.NET MVC 5 was used as business rules organizer. Visual C# was used for programming. MS SQL Server was applied as a server where data is stored (figure 2).

Fig.2: Approach of using multi-tier client server architecture



3.1 Creating a model to establish database connectivity. Data migrating

To create a model of web client apps, the following two methods were used. 1) The database was created in SQL Server Management Studio. For connect ASP.NET MVC 5 apps to the server and we used command connection string in Visual Studio Community 2017. 2) The database was implemented using the Visual C# programming language, as a class in model. If you need to make changes and additions to the database structure commands for data migration are executed. The migration mechanism in ASP.NET MVC is used for break-even database updates. To do the main steps will be performed will look like this:

- on the manager console window we activate migration mode using the enable
- migrations command;
- in folder Migration will appear file Configuration.cs;
- on the method Seed we can initialize database;
- to create the migration is run the Add-Migration “MigrateDB” command.
- in this case, Visual Studio switches to automatic generation of the migration class, and we entering our extensions into the program code; - using command Update-Database.

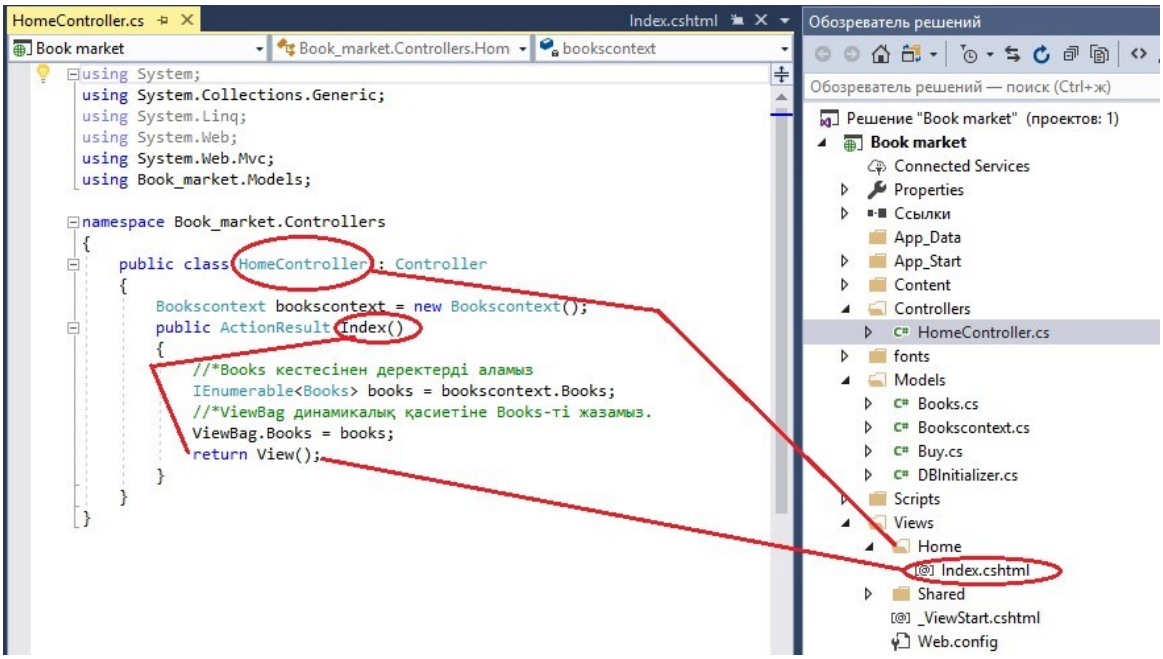
3.2 Creation of controller

To link a view to a database, we should create a controller. To work with database in the program code we add libraries System.Data.SqlClient and System.Data. Also need to consider

if we create controller will formation new file in view with similar name. The method called

on the controller body should match the name of the file being sent for execution in the view (figure 3).

Fig.3: Link of controller and view on programming level



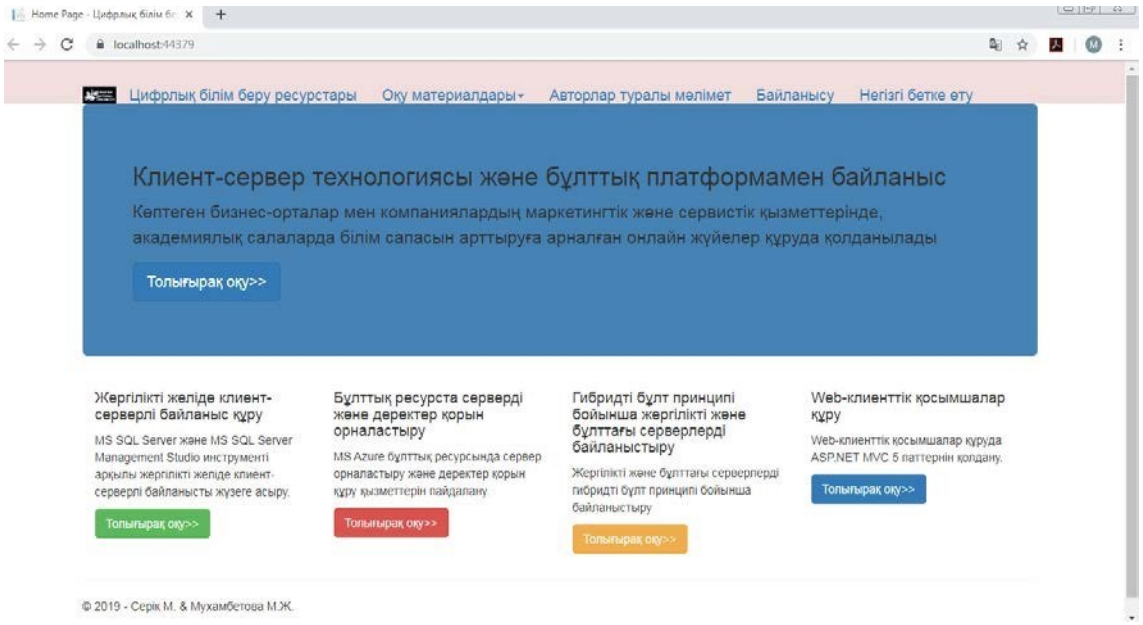
3.3 Creating a user interface or view

At this stage, when writing the visual part of the application, the interpretation of html and C # codes is performed using Razor visualization. With Razor, we can embed server code in web pages. As a result, we get dynamic content. We can use the web page wizard and the Bootstrap framework features (Moreto, 2017). To create a uniform type of web client application, a common template is created for all pages. A common interface structure is developing for all files, the view is executed using the Layout command. This method is useful when creating the header or footer information block for web client applications. When the web client application is running, the IIS server starts. IIS (Internet Information Services) is a Windows module integrated into the server. It easily installs and configures web client applications on a local network or the Internet and allows programs to work in a web browser.

4 Applying in educational process

The development of web-client applications using these methods is included in the educational programs of Kazakhstan universities in the field of information technology. Including in the specialty 5B011100-Computer Science in L.N. Gumilyov Eurasian National University and in the specialties 5B011100-Computer Science and 5B060200-Computer Science Kh.Dosmukhamedov Atyrau State University. The topics introduced into the educational process had a positive effect on the quality of education. The textbook "Clientserver technology" was developed (Serik, Mukhambetova, & Yeskermessuly, 2019), in which the chapter "Creating Web Client Applications in the Visual Studio Integrated Environment" contained additional materials necessary for students. For independent work, it was necessary to create projects in specific subject areas and students performed tasks related to future activities. In addition, digital educational resources have been prepared for teaching. The development of digital educational resources was also developed using the ASP.NET MVC 5 Framework (Serik, Mukhambetova, & Yeskermessuly, 2019).

Fig.4: Main page of a digital educational resource created using ASP.NET MVC 5



5 Conclusion

The natural separation of the various responsibilities of the application into independent parts of the software, which is supported by the MVC architecture, allows you to initially build easily maintained and tested applications. However, ASP.NET MVC designers did not stop there. For each fragment of a component-oriented infrastructure project, they provided the structure needed to meet the requirements of unit testing and simulation tools.

Using frameworks to create web-based apps simplifies the process of programming and allows you to work with a powerful environment for creating flexible and visual apps. Integrating JQuery and Bootstrap functions into ASP.NET MVC Template improves web page design. The adaptive Bootstrap feature helps you read applications from any device, like mobile phones and tablets. That is, you do not need to write a version of the client application for a mobile device.

We believe that teaching modern approaches of creating client-server applications in the educational process at the university will help students to acquire the necessary professional competencies for future activities. Research in this area will continue.

Resources

Grishenko, L. P. (2013). Practical aspects of reducing some risks of it Outsourcing. Retrieved February 5, 2020, from https://cyberleninka.ru/article/n/upravlenie-prakticheskie-aspekty-umensheniya-nekotoryh-riskov-it-autsorsinga/viewer

Moreto, S. (2016). *Bootstrap by example: Master Bootstrap 4's frontend framework and build your websites faster than ever before*. Birmingham, UK: Packt Publishing.

Professor Web. (2016). Структура проекта ASP.NET MVC 5. Retrieved January 15, 2020, from https://professorweb.ru/my/ASP_NET/mvc/level1/1_3.php

Serik, M., Mukhambetova, M., & Yeskermessuly, A. (2019). Improving the Content of a Client-Server Technology Training Course: Set up and Collaborative Implementation of Local and Cloud-Based Remote Servers. *International Journal of Emerging Technologies in Learning (iJET), 14*(21), 191. doi:10.3991/ijet.v14i21.10643

Yadav, S. C., & Singh, S. K. (2009). *An introduction to client/server computing*. New Delhi, India: New Age International.

BIOMETRIC SYSTEMS AND UNCERTAINTY: A GENERAL APPROACH

Lourdes Ruiz S.[24]

Abstract
Human recognition systems are becoming very popular nowadays for identifying individuals and granting access to physical or virtual facilities compared to traditional recognition systems such as passwords, pins, or cards. Due to the nature of the acquired biometric data, uncertainty can be present in every step of the biometric recognition system and could affect the performance and safety of the systems involved. The following study presents a detailed description of the concept and the sources of uncertainty in biometric systems. Its main goal is to serve as a guide for detecting and managing uncertainty for developing better systems, improving biometric technology procedures, and enhancing safety.

Keywords
Biometrics, Systems, Uncertainty

1 Introduction

Uncertainty can be defined as not knowing for sure or the absence of information (Hummeltenberg, 2014). On a corporate level, it represents the difference between the amount of data needed to execute a task and the amount of data an organization already has. This concept is applied at organizations in daily business activities, strategic decisions, and at a professional level by analyzing the present and future uncertainties to manage them (Galbraith, 1973).

When planning and executing engineering systems, uncertainty plays a significant role in attaining a quality design. This approach goes beyond traditional engineering practices based on meeting certain specifications or regulations and stimulates the expansion of the designing process, including external forces (Neufville et al., 2004).

Nowadays, the constant technological and scientific advancements and the generation of data require a holistic methodology that includes not only product criteria setting but new factors such as environmental, economic, and political into the development of new technologies. Uncertainty approach takes into consideration these factors and keeps the pace of this changing environment. Moreover, it aids to envisage new challenges for a successful evolution of the technology and protection of the systems.

Biometric characteristics have been used to identify individuals using unique biological identifiers such as fingerprint, vein pattern, hand geometry, palm print, voice, iris, and face recognition (Ross, 2007) (Ong et al., 2008). Biometric systems are based on pattern recognition. The system acquires the biometric data from a person, extracts the features from the received data, stores them as a template, and compares them with the template previously stored in the database (Nadort, 2007) (Watanabe, 2008).

Biometrics acquisition is an emerging technology in which uncertainty management is needed for the different processes derived from it and to protect the characteristics collected. The following work presents a comprehensive summary describing uncertainty and the sources in biometric systems. Its main objective is to serve as a general guide for biometric operators and implementers to control uncertainty, develop better processes, contribute to the success of technology and safety.

[24] Obuda University / Doctoral School on Safety and Security Sciences, Banki Donat Faculty, Budapest, Bécsi út 96b, 1034, lourdes.ruiz@bgk.uni-obuda.hu

a. Uncertainty

The main goal of uncertainty quantification is to determine the source of uncertainty in the system and assess the impact on it. Uncertainty evaluation enhances the system's safety and generates robustness in the process. Its main characteristics are:

- Multidisciplinary
- Cross-cutting
- System centric (Ayyub, 2015)
-

Uncertainty is closely related to the company's decision making. It can be divided into three components:

1. State uncertainty, the probability of an event to happen.
2. Effect uncertainty, it is the cause-effect relationship due to the lack of information regarding the outcomes of an event.
3. Response uncertainty, it is related to the absence of information regarding responses and their consequences (Milliken, 1987).
4.

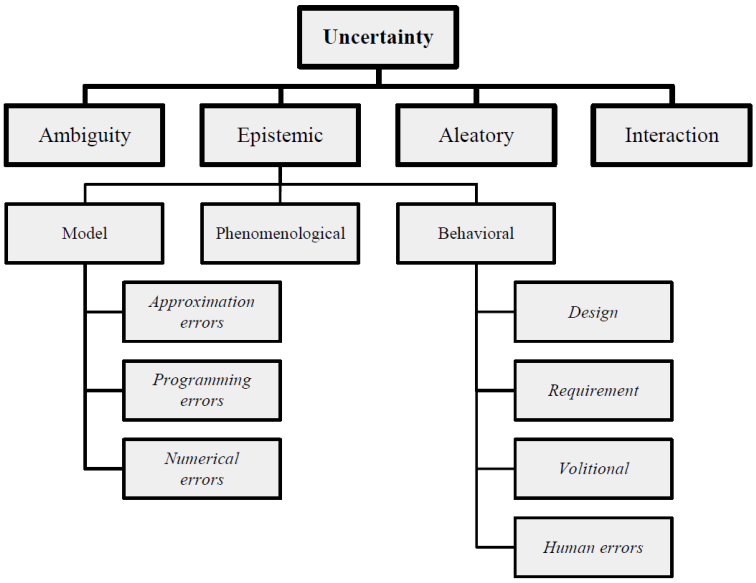
Uncertainty occurs due to the following sources: incomplete information, inadequate understanding of available information, and undifferentiated response alternatives. Moreover, it can be caused by the organization by the technology or supplies used in the processes, and it can be external due to the customers or competitors (Hummeltenberg, 2014).

Furthermore, uncertainty has been classified for the designing and development of complex systems such as biometric systems. This classification comprises of 4 sub-groups:

1. Ambiguity, defined as the imprecision of terms and expressions.
2. Epistemic is the absence of knowledge of information during any stage or step of the system modeling process. This type of uncertainty can be divided into mode, phenomenological, and behavioral.
3. Aleatory is the intrinsic variation related with the system analyzed.
4. Interaction is the uncertainty that originated from unforeseen interaction of different events, which should have been in the first place estimated (Thunnissen, 2003) (Szamosi & Pokoradi, 2016).

Figure 1 presents a detailed diagram of this classification.

Fig. 1: Classification of uncertainty for the design and development of complex systems.



Source: (Thunnissen, 2003)

a. Biometric Technology

Biometric technology is based on the concept that physical or behavioral characteristics in humans can be distinctive; for this reason, it eases the identification of a specific person. These biometric characteristics can be divided into two groups: hard biometrics, which are physical and behavioral traits such as fingerprint, face, iris, hand recognition, gait or keystroke and soft biometrics which are continuous or discrete human identifiers such as height, weight, gender, race (Drosou et al., 2012).

The biometric authentication process focuses on what an individual is, instead of on what he/she knows or has. Therefore, this technology offers high levels of security compared with traditional recognition systems such as passwords or identification cards. The recognition is closely linked to a specific person due to the usage of inherited attributes that are unique.

Biometric technology has numerous uses in different fields such as forensics, border control, terrorist or criminal identification, grant access to physical or virtual facilities, healthcare, social services and time and attendance control in the workplace (Callahan, 2010) (Jain et al., 2011).

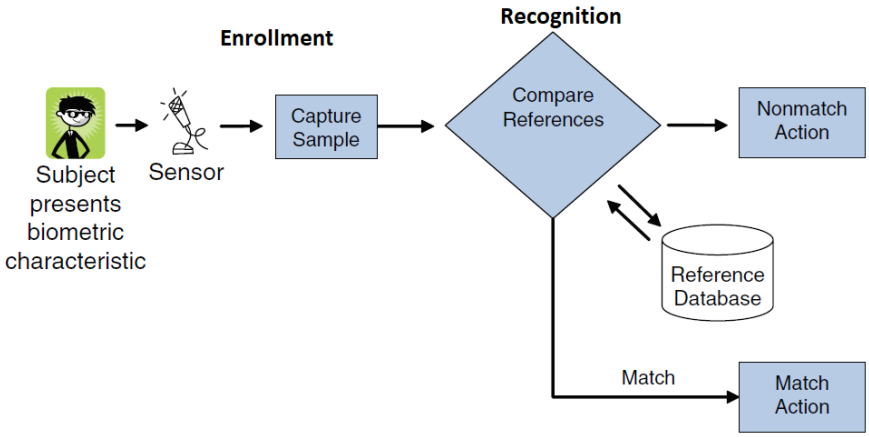
b. Biometric Systems and Uncertainty

Biometric systems use pattern recognition, which consists of two parts:

1. Enrollment: biometric traits are obtained from the person via a sensor. Only the individual's distinctive features are stored in the database.
2. Recognition: biometric data is collected from the individual and compared with the data stored at the enrollment step to recognize and authenticate the person's identity (Jain et al., 2011).

Figure 2 shows how a biometric system is functioning

Fig. 2: Biometric System Operational Process



Source: (Pato, Millett, & Committee, 2010)

Generally, these systems are associated with larger systems since they measure biological characteristics. Thus, their performance is affected by other technologies, environmental factors, security policies, political, privacy, and social issues, and uncertainty could emerge.

Uncertainty is present in biometric systems due to the complexity and the probabilistic nature of them. Some ways uncertainty is originated in these systems are because of the lack or incomplete understanding and the stability of the biometric identifiers, the probability of forging the system, and the attitude of the users towards the system (Pato et al., 2010).

Diverse sources of uncertainty are present in biometric systems; some of them are presented below:

Nature of biometric characteristics

Biometric traits acquired by the system can change due to different factors such as age, environment, illness, stress, occupational, social, or cultural issues (Theofanos et al., 2007). In a larger population, these characteristics can be challenging for authentication and authorization processes due to the following constraints:

- Noninvasive or distinctive features in scale are difficult to find since, within the population, some members lack this trait because of an accident, environment, or the attribute is abnormal and cannot be extracted by the system.
- Some biological characteristics that are not invasive in larger population samples are not sufficiently unique to correctly identify an individual.

Human interaction within the system

Uncertainty can be associated with user interaction in each of the steps of the biometric system, such as enrollment, recognition, and matching. Attempts to hinder the identification by individuals also contribute to uncertainty in the system. Furthermore, biometric identification involves decision making between the system, the implementers, and operators, which also carries a level of uncertainty.

Operational Factors

Biometric systems functioning comprise of different elements in which uncertainty can arise:

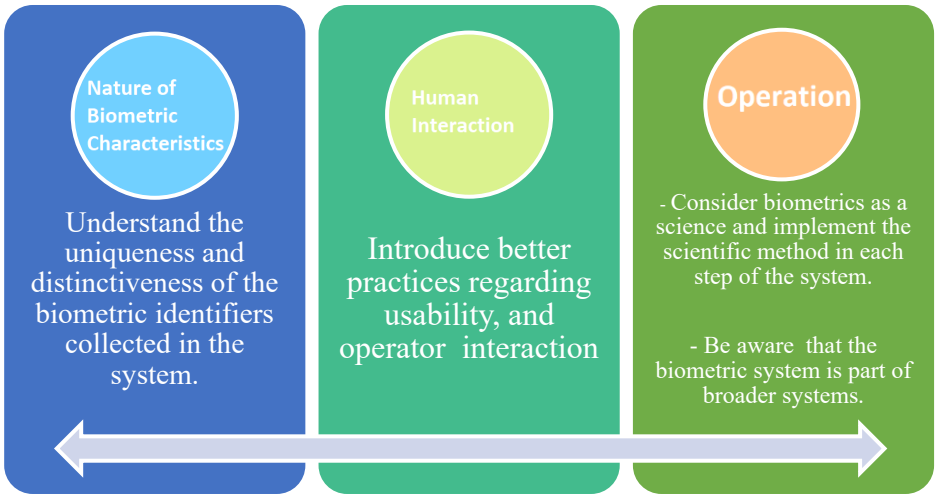
- Sensor: calibration, external noise, quality of the biometric signals, age, and sensitivity are some factors to be considered to manage uncertainty due to the biometric sensor.
- Algorithms and devices: pattern extraction, matching, and comparison algorithms are vital for biometric systems performance. Uncertainty can emerge when differences

between the different algorithms are present. Factors such as error rates, speed, cost of acquisition, operation, maintenance, and usability are also uncertain sources.

- Biometrics Integrity: Due to the nature of the data collected, this information is prone to manipulation, security breaches, transformation, privacy issues, non-proper management, and usage for another purpose than intended. It is essential to take into account that the data measured is just a proxy of the biometric trait, and the matching result is obtained within a tolerance of approximation, which can generate uncertainty to the process (Wayman et al., 2013).

Figure 3 presents a summary of the primary sources of uncertainty and ways to manage or mitigate it, taking into consideration that all of them are related to the system.

Fig. 3: Sources of uncertainty in biometric systems and management



2 Discussion

It is crucial to understand and recognize the distinctive characteristics of the biological traits collected in biometric systems and be aware that uncertainty can be present in the system. Biometric characteristics are valuable for identifying an individual in simple or complex processes in life. Nonetheless, they have their limitations that can be surpassed if the scientific method is rigorously implemented in all the processes that encompass these large systems.

Biometrics, their operation, performance, and analysis is considered a science. Hence, the principles of repeatability and reproducibility are relevant to the good development and implementation of the technology.

Uncertainty estimation in biometric systems goes beyond the recognition error rates, such as false positives and false negatives. It performs a complete analysis of all the uncertainties that could emerge in real life from the software to the environment and social factors since the system is acquiring human characteristics to identify a specific individual.

3 Conclusions

The following study analyzed in general biometric technology and uncertainty within the systems to highlight the importance of uncertainty awareness. It describes the concept and the different sources of uncertainty that could be present in the system for implementers and operators to consider and control when executing these systems. It is essential to be aware of the presence of uncertainty while planning, designing, and implementing a biometric system to have better results and protect biometric information.

Uncertainty management takes one step further into risk analysis. This approach determines other sources, such as economic or public effects, to create a robust design. The

effectiveness of a biometric system relies not only on the operational and technological process but also on the social context since it is a human recognition system.

Uncertainty is, indeed, an ongoing research topic in different technological and scientific fields. Concerning biometric systems, uncertainty estimation and management is relevant for technological success, correct performance, and user acceptability. However, further research regarding algorithms, software, human impact, uncertainty, and management related to these factors in the process is needed.

Unexpected opportunities can emerge due to uncertainties. Biometric technology is becoming ubiquitous in daily life systems such as healthcare, banking, financing, mobile applications. Furthermore, society is demanding better products and services. Hence, uncertainty should be included in biometric system design for anticipating its successful outcomes and downsides.

Biometric technology is a promising field that will ease infinite tasks if appropriately used, and uncertainties are well managed and controlled.

Resources

Ayyub, B. M. (2015). Introduction to the Aims and Scope of the Journal. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering, 1*(1), 01614001. doi:10.1061/ajrua6.0000001

Callahan, E. M. (2010, November 5). *Immigration Benefits Background Check Systems* [PDF]. Department of Homeland Security.

De Neufville, R., De Weck, O., Frey, D., Hastings, D., Larson, R., & Simchi-Levi, D. (2004). Uncertainty Management for Engineering Systems Planning and Design. *Engineering System Monograph.* Retrieved February 3, 2020, from http://web.mit.edu/deweck/www/PDF_archive/4%20Other%20Major%20Pubs/4_6_ESD2004_uncertainty.pdf

Drosou, A., Tzovaras, D., Moustakas, K., & Petrou, M. (2012). Systematic Error Analysis for the Enhancement of Biometric Systems Using Soft Biometrics. *IEEE Signal Processing Letters, 19*(12), 833-836. doi:10.1109/lsp.2012.2221701

Galbraith, J. R. (1973). *Designing complex organizations*. Reading, MA, US: Addison-Wesley.

Hummeltenberg, W. (2014). Decision Engineering. Retrieved February 18, 2020, from https://enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/daten-wissen/Business-Intelligence/decision-engineering

Jain, A. K., Ross, A. A., & Nandakumar, K. (2011). *Introduction to biometrics*. Springer-Verlag New York. https://doi.org/10.1007/978-0-387-77326-1

Milliken, F. J. (1987). Three Types of Perceived Uncertainty about the Environment: State, Effect, and Response Uncertainty. *The Academy of Management Review, 12*(1), 133. doi:10.2307/257999

Nadort, A. (2007). The Hand Vein Pattern Used as a Biometric Feature. Retrieved February 3, 2020, from https://docplayer.net/3197586-The-hand-vein-pattern-used-as-a-biometric-feature.html

Ong, M. G. K., Tee, C., & Jin, A. T. B. (2008). Touch-less palm print biometric system. *Proceedings of the Third International Conference on Computer Vision Theory and Applications, 2*, 423-430. doi:10.5220/0001073504230430

Pato, J. N., Millett, L. I., & Committee, W. B. (2010). Biometric Recognition. *THE NATIONAL ACADEMIES PRESS,* Washington D.C., US. https://doi.org/10.17226/12720

Ross, A. (2007). Human recognition using biometrics: an overview. *Annales Des Telecommunications-Annals Of*, *62*(1), 11–35. https://doi.org/10.1007/BF03253248

Szamosi, B., & Pokoradi, L. (2016). Intersubjectivity as an uncertainty source of risk assessment. *CINTI 2015 - 16th IEEE International Symposium on Computational Intelligence and Informatics, Proceedings*, (2), 35–39. https://doi.org/10.1109/CINTI.2015.7382949

Theofanos, M., Stanton, B., Micheals, R., & Orandi, S. (2007). Biometric systematic uncertainty and the user. *IEEE Conference on Biometrics: Theory, Applications and Systems, BTAS'07*. https://doi.org/10.1109/BTAS.2007.4401918

Thunnissen, D. P. (2003). Uncertainty Classification for the Design and Development of Complex Systems. *3rd Annual Predictive Methods Conference*, 16. https://doi.org/10.1.1.128.133

Watanabe, M. (2008). Palm Vein Authentication. *Advances in Biometrics,* 75-88. doi:10.1007/978-1-84628-921-7_5

Wayman, J. L., Possolo, A., & Mansfield, A. J. (2013). Modern statistical and philosophical framework for uncertainty assessment in biometric performance testing. *IET Biometrics, 2*(3), 85-96. doi:10.1049/iet-bmt.2013.0009

ANALYSIS OF ATTEMPTS TO PENETRATE INFORMATION SYSTEMS OVER THE INTERNET

Pavol Sojka[25]

Abstract
In recent years, the number of hardware and software resources has grown rapidly. The dark side of the industry is also developing fast, where the vulnerabilities of various software tools, huge leaked libraries, tools to break down the competitors' computing infrastructure, and many other illegal activities are growing. The aim of our paper is to analyze and evaluate illegal activities, which we have recorded at the level of either the University of Economics in Bratislava or on our virtual computers located on the Google Cloud infrastructure. First, we discuss the most common types of attacks, and later select data that we have collected on our servers for deeper analysis, namely ssh remote login attacks, and briefly mention attacks on Apache and MySql. In the analysis, we will focus on the frequency of attacks from specific countries, and thus the secondary objective of the paper will be to recommend how to prevent and possibly eliminate the attacks. The data used does not have a test character, but it is the real data collected from the servers used for teaching process.

Key words
software, security, leak, attack, protection

1 Introduction

In recent years, we have witnessed the rapid take-up of new technologies and the upgrading of existing ones. Each device and service we own generates some amount of data. These data become more valuable than before because of continuous migration from paper media to digital media in state service, business and so. Data are valuable for criminals for trading, espionage and racketeering. State service and also companies invest more money to strengthen security of their systems and employee' security awareness. These items in budgets are continuously growing so it is necessary to highlight the weakest spots in infrastructure. These spots should be identified individually according to needs of the company and according to services they provide. Our paper is targeted on most commonly used services, that many companies uses to administer their internal systems or to run web infrastructure like internet shops, internal systems, online presentations and alike.

1.1 Types of attacks and ways of intrusion into systems

There are several types of attacks in practice, the phising attack, which is to persuade the victim to take some action that an attacker needs to successfully penetrate the system. Such an unaware collaboration consists, for example, in deceiving a victim to trigger an attachment from mail, for example a false billing from an operator when, after running the zip archive content, files with the most known extensions were encrypted on the computer and the attacker requested a ransom for files decryption. Another type of attack is a worm that scans, for example, home and business networks, and searches for vulnerable services such as file sharing services and the like. Another type of attack is the attack through public Wi-Fi networks, where the attacker can try to capture unencrypted communication of other users. It is another popular technique, when

[25] Ing. Pavol Sojka, University of Economics in Bratislava, Faculty of Economic Informatics, Department of Applied Informatics, Dolnozemská cesta 1, 852 35 Bratislava, pavol.sojka@euba.sk.

USB keys are left in different public places, and when they are inserted into a computer, they can try to infect it and then capture user activities such as keystrokes, screen, camera and microphone to watch activity around the computer area.

In our text, we will focus only on network-based attacks that are targeted on intrusions by using port scanning tools and testing dictionaries names and passwords - dictionary-based attacks and possibly brute force attacks.

1.2 Dictionary-based attacks

A dictionary attack is based on trying all the strings in a pre-arranged listing, typically derived from a list of words such as in a dictionary (hence the phrase dictionary attack). In contrast to a brute force attack, where a large proportion of the key space is searched systematically, a dictionary attack tries only those possibilities which are deemed most likely to succeed. Dictionary attacks often succeed because many people have a tendency to choose short passwords that are ordinary words or common passwords, or simple variants obtained, for example, by appending a digit or punctuation character. Dictionary attacks are relatively easy to defeat, e.g. by using a passphrase or otherwise choosing a password that is not a simple variant of a word found in any dictionary or listing of commonly used passwords (Dictionary attack, 2019).

1.3 Brute force attacks

In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search.

A brute-force attack is a cryptanalytic attack that can, in theory, be used to attempt to decrypt any encrypted data (except for data encrypted in an information-theoretically secure manner). Such an attack might be used when it is not possible to take advantage of other weaknesses in an encryption system that would make the task easier (Brute-force attack, 2019).

1.3 Port scanning

The purpose of port scanning is finding the open ports on the computers that were found with a host scan. When a port scan is started on a network without making use of the results of a host scan, much time is wasted when many IP addresses in the address range are vacant. Most programs that communicate over the Internet use either the TCP or the UDP protocol. Both protocols support 65536 so called ports that programs can choose to bind to. This allows programs to run concurrently on one IP address. Most programs have default ports that are most often used. For example, HTTP servers commonly use TCP port 80 or secured one on port 443. Network scanners try to connect to TCP or UDP ports. When a port accepts a connection, it can be assumed that the commonly bound program is running. TCP connections begin with a SYN packet being sent from client to server. The server responds with a SYN/ACK packet. Finally, the client sends an ACK packet. When the scanner sends a SYN packet and gets the SYN/ACK packet back, the port is considered open. When a RST packet is received instead, the port is considered closed. When no response is received the port is either considered filtered by a firewall or there is no running host at the IP address. Scanning UDP ports is more difficult because UDP does not use handshakes and programs tend to discard UDP packets that they cannot process. When an UDP packet is sent to a port that has no program bound to it, an ICMP

error packet is returned. That port can then be considered closed. When no answer is received, the port can be considered either filtered by a firewall or open. Many people abandoned UDP scanning because simple UDP scanners cannot distinguish between filtered and open ports (Port scanning, 2019).

1.5 SQL Injection technique

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server (SQL injection, 2019).

1.6 Infrastructure monitoring

Our infrastructure, on which we actively monitored intrusion attempts, included several types of servers where Linux distributions were installed, namely two CentOS Linux servers, one Debian Linux server, and one Suse enterprise Linux server. All servers are used for teaching and have only those services and ports configured for the service needed. Servers are regularly updated to keep running most recent version of libraries. The author himself has been active in the field of information technology as a system administrator, so current installations can be considered as properly set up and secure as possible. In addition to known bugs in operating systems and other software products, the so-called zero-day vulnerabilities exist, where the software manufacturer has not updated the libraries yet. This type of errors are probably the most dangerous and there is no effective protection against them.

On our infrastructure, the ssh (secure shell) service is currently running, which is essential for the remote administration of Linux-based servers. Furthermore, the Apache web server service is essential for running web-based applications. Apache web server is not the only product that allows web applications to run, but is one of the most widely used. In addition, we have an Oracle database server and MySQL database server running in our environment. Database servers can run completely isolated from the Internet environment, but are vulnerable indirectly through so-called sql-injection attacks that an attacker can execute through an application running on the Apache web server while communicating with the database server.

1.7 Running services and open ports

1.7.1 Secure shell (ssh) service

Secure Shell (ssh) is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command-line login and remote command execution, but any network service can be secured with SSH.

SSH provides a secure channel over an unsecured network in a client–server architecture, connecting an SSH client application with an SSH server. The protocol specification distinguishes between two major versions, referred to as SSH-1 and SSH-2. The standard TCP port for SSH is 22. SSH is generally used to access Unix-like operating systems, but it can also be used on Microsoft Windows. Windows 10 uses OpenSSH as its default SSH client.

SSH was designed as a replacement for Telnet and for unsecured remote shell protocols such as the Berkeley rlogin, rsh, and rexec protocols. Those protocols send information, notably passwords, in plaintext, rendering them susceptible to interception and disclosure using packet analysis. The encryption used by SSH is intended to provide confidentiality and integrity of data over an unsecured network, such as the Internet.

SSH uses public-key cryptography to authenticate the remote computer and allow it to authenticate the user, if necessary. There are several ways to use SSH; one is to use automatically generated public-private key pairs to simply encrypt a network connection, and then use password authentication to log on.

Another is to use a manually generated public-private key pair to perform the authentication, allowing users or programs to log in without having to specify a password. In this scenario, anyone can produce a matching pair of different keys (public and private). The public key is placed on all computers that must allow access to the owner of the matching private key (the owner keeps the private key secret). While authentication is based on the private key, the key itself is never transferred through the network during authentication. SSH only verifies whether the same person offering the public key also owns the matching private key. In all versions of SSH it is important to verify unknown public keys, i.e. associate the public keys with identities, before accepting them as valid. Accepting an attacker's public key without validation will authorize an unauthorized attacker as a valid user (Secure Shell, 2019).

1.7.2 Web server (Apache)

The Apache HTTP Server is free and open-source cross-platform web server software, released under the terms of Apache License 2.0. Apache is developed and maintained by an open community of developers under the auspices of the Apache Software Foundation. The vast majority of Apache HTTP Server instances run on a Linux distribution, but current versions also run on Windows and a wide variety of Unix-like systems. Past versions also ran on OpenVMS, NetWare, OS/2 and other operating systems.

Originally based on the NCSA HTTPd server, development of Apache began in early 1995 after work on the NCSA code stalled. Apache played a key role in the initial growth of the World Wide Web, quickly overtaking NCSA HTTPd as the dominant HTTP server, and has remained most popular since April 1996. In 2009, it became the first web server software to serve more than 100 million websites. As of August 2018, it was estimated to serve 39% of all active websites and 35% of the top million websites. Apache supports a variety of features, many implemented as compiled modules which extend the core functionality. These can range from authentication schemes to supporting server-side programming languages such as Perl, Python, Tcl and PHP (Apache HTTP Server, 2019).

1.7.3 Database server (MySQL/Oracle)

A database is an organized collection of data, generally stored and accessed electronically from a computer system. Where databases are more complex they are often developed using formal design and modeling techniques.

The database management system (DBMS) is the software that interacts with end users, applications, and the database itself to capture and analyze the data. The DBMS software additionally encompasses the core facilities provided to administer the database. The sum total of the database, the DBMS and the associated applications can be referred to as a "database system". Often the term "database" is also used to loosely refer to any of the DBMS, the database system or an application associated with the database.

Computer scientists may classify database-management systems according to the database models that they support. Relational databases became dominant in the 1980s. These model data as rows and columns in a series of tables, and the vast majority use SQL for writing and querying data. In the 2000s, non-relational databases became popular, referred to as NoSQL because they use different query languages (Database, 2019).

MySQL is free and open-source software under the terms of the GNU General Public License, and is also available under a variety of proprietary licenses. MySQL was owned and sponsored by the Swedish company MySQL AB, which was bought by Sun Microsystems (now Oracle Corporation). In 2010, when Oracle acquired Sun, Widenius forked the open-source MySQL project to create MariaDB (MySQL, 2019).

Oracle Database (commonly referred to as Oracle RDBMS or simply as Oracle) is a proprietary multi-model database management system produced and marketed by Oracle Corporation. It is a database commonly used for running online transaction processing (OLTP), data warehousing (DW) and mixed (OLTP & DW) database workloads. The latest generation, Oracle Database 18c, is available on-prem, on-Cloud, or in a hybrid-Cloud environment. 18c may also be deployed on Oracle Engineered Systems (e.g. Exadata) on-prem, on Oracle (public) Cloud or (private) Cloud at Customer (Oracle Database, 2019).

2 Methodology

Based on literature review we have chosen some types of attacks which also occurred mostly on our operating systems. We also analyzed malicious behavior noticed in system logs. According to Pan et al. (Pan et al., 2019) attacks can have significantly different characteristics. Different types of web attacks, such as SQL injection, cross site scripting, remote code execution and file inclusion vulnerabilities, use different forms of attack vector and exploit different vulnerabilities inside web applications. These attacks therefore often exhibit completely different characteristics. For example, SQL injection targets databases, whereas remote code execution targets file systems. Our effort was targeted to prevent attacking primarily on ssh service because we used deep log files inspection before to choose which service is mostly flooded with break-in attempts.

Methodology we used in our model was as follows:

1) Manual check of chosen log files on daily basis. Log files we were monitoring was *secure* log file, which is located in */var/log* directory and *access_log* in */var/log/httpd* directory. According to Pompon and Heath (Pompon, 2020) authentication attacks belong to top ten attacks against service providers in period from the year 2017 to 2019. Our monitoring confirms that presumption and we focused on monitoring already mentioned *secure* log;
2) We used particular techniques to identify entries in *secure* log with failed login. Techniques are explained in more detail in "Results" section in this paper;
3) After identification of malicious IP addresses we took countermeasures to block them (described in "Results" section);
4) Later we monitored further failed login attempts and at the same time we monitored if banned IP addresses were still trying to connect to our systems;
5) With the tool *whois* we found out the country of origin of IP addresses.
6) Statistics calculated for the given period from 20th of March till 25th of April 2019 (Fig. 1).

For our own research it is necessary to have a server running on the public network - the Internet and enabled logging events for a particular service. We have to know how to use

available third-party tools to analyze log records, or use embedded operating system tools. We have used the built-in operating system tools for analysis as they are present in every Linux installation and are therefore immediately available.

The model for use in our work has been set up as a sequence of steps, when we provide both current and archived logging records (Hussain, 2013) for processing purposes, as a second step we have prepared a script that performed analysis on the logs, resulting in the extraction of data that contained only the failed login attempts. Since logging records contain thousands of records of both legal and illegal activities, filtering out relevant data was a necessary step. Since the newly acquired data is also in large quantities - depending on the size of the log files, it can be thousands of lines depending on the time span we choose - it is necessary to perform additional filtering according to the IP address (Adresa IP, 2019), where we get the frequency of IP addresses from which penetration attempts were made. Subsequent analysis will determine the first five most numerous attacks and from which countries, respectively networks they originated. To determine the ISP of the attacking IP address, we will use the IP address tool called whois in conjunction with the nslookup tool. Both tools will be used as needed, whois will be most used. After the main analysis, we can determine which networks are most involved in the current attempts to infiltrate our network, and we can give network administrators recommendations for taking active action. This tool is usable repeatedly without restrictions and therefore can provide recommendations on any time basis, but to reduce the load on the current server it is recommended to do once a day, or do off-line analysis, that is, on another specified server performed as needed.

The tool in the current development phase is designed to find suspicious IP addresses from which a predefined amount of penetration attempts are made and display the IP address to the system administrator after analysis. In the future, the author plans to extend the tool to include active measures in the form of direct entry of malicious IP addresses into the /etc/hosts.deny file (Understanding TCP Wrappers (/etc/hosts.allow & /etc/hosts.deny) in Linux, 2019), where we block the ability to connect to the server and in our case it will be a *ssh* service that was mentioned in the text above. The advantage of our tool is basically instant executability and minimal setup effort, as well as its currently free use.

3 Results

3.1 Obtaining data

As mentioned earlier, the operating system on which we will analyze logs is CentOS Linux version 7, which is derived from Red Hat Enterprise Linux, which itself and its derivatives are among the most widely used operating systems in the corporate area (The Red Hat Enterprise Linux Team, 2018). In this version of Linux, we are looking for log entries in */var/log/* and we will evaluate the logs of the intrusion attempts through the *ssh* protocol running on port 22 and the log file name is *secure*, the full path of the log file will be */var/log/secure*. Successful login attempts are also noted in this file, and messages such as the *crond* process that execute tasks according to their time settings are also written to this file. In other Linux operating systems, the */var/log/* location is also used, but the log file name may vary, and the internal structure of these log files may also vary. For example, in Suse Enterprise Linux, *ssh* records are stored in files named audit. We analyzed logs from 20th of March till 25th of April 2019.

Since we need to find penetration attempts, we will use the operating system tools to see if there are bad login attempts and calculate the number of attempts using another operating system tool (*wc* tool, will be mentioned later). As mentioned in the text above, we will have to set threshold value represented by the number of invalid login attempts. For our purposes, we will choose the value of 5 attempts, unless the value proves not to be accurate (for example, a legitimate user forgets a password and tests his passwords to log in), so we can adjust that

threshold. To find bad login attempts, we will use the Linux command combination within the bash (Bash (Unix shell), 2019): *cat /var/log/secure | grep -i failed*. This command combination shows (*cat*) the contents of the secure file and then executes the *grep -i* command after *cat* statement, which searches for the occurrence of the word *failed*. The *-i* switch ensures that the word *failed* can be in the form of, for example, *Failed*, that is, Linux distinguishes uppercase and lowercase letters in commands, as opposed to Windows, which does not distinguish between case letters. This property is generally referred to as case sensitivity (Case sensitivity, 2019). In a small preview, we'll show the result of this operation:

```
Apr 23 17:53:34 CentOS sshd[20497]: Failed password for invalid user pi from
135.0.47.21 port 43374 ssh2
Apr 23 17:53:34 CentOS sshd[20509]: Failed password for invalid user pi from
135.0.47.21 port 43375 ssh2
```

As shown from the example above, the attacker tried to connect to *ssh* from California's IP address 135.0.47.21 with user *pi*, where the attacker believes that he is trying to attack raspberry pi on our network (Raspberry Pi, 2019).

In the next example, we calculate the number of penetration attempts using a command combination: *cat /var/log/secure | grep -i failed| wc -l* . This command combination no longer shows the contents of the *secure* file on the screen, but directly counts the occurrence of rows with the word *failed* in the computer's memory and lists only the number of records at the end of the operation. The *wc* command means "word count" and the *-l* switch counts the number of lines. The logging record audited in the earlier period has shown that over time approx. 5:35 am to 1:00 pm during the same day, the attacker attempted to penetrate 8504 times from the same IP address, which is documented by a short log record:

```
Mar 29 05:35:27 CentOS sshd[5459]: Failed password for root from 107.0.106.213
port 49967 ssh2
Mar 29 05:35:30 CentOS sshd[5464]: Failed password for root from 107.0.106.213
port 50189 ssh2
Mar 29 05:35:34 CentOS sshd[5468]: Failed password for root from 107.0.106.213
port 50393 ssh2
Mar 29 05:35:37 CentOS sshd[5473]: Failed password for root from 107.0.106.213
port 50623 ssh2
…
…
Mar 29 13:00:36 CentOS sshd[16817]: Failed password for invalid user 4f3d2s1a
from 107.0.106.213 port 57297 ssh2
Mar 29 13:00:39 CentOS sshd[16822]: Failed password for invalid user 4l3n
from 107.0.106.213 port 57634 ssh2
Mar 29 13:00:42 CentOS sshd[16826]: Failed password for invalid user 4na2xf
from 107.0.106.213 port 57970 ssh2
Mar 29 13:00:45 CentOS sshd[16831]: Failed password for invalid user 4p4ch3
from 107.0.106.213 port 58327 ssh2
Mar 29 13:00:48 CentOS sshd[16835]: Failed password for invalid user 4r3e2w1q
from 107.0.106.213 port 58649 ssh2
```

This IP adress was banned later and we will show how in the next text.

3.2 Banning IP addresses of the attackers

Blocking addresses that try to connect to our server through *ssh* can be done in several ways. When we talk about enterprise infrastructure, the easiest solution is to ask your network administrator to activate blocking rule at the central firewall, which is a network traffic control device. This approach is the most widely used, but it has one disadvantage for our approach,

which is the constant need to contact the network administrator to block a specific address or unblock it if the situation so requires. Another option is to use a firewall on our own server to block the IP address. This service is provided, for example, by the *firewall-cmd* utility (Ellingwood, 2015) or *ufw* application (How to Configure a Firewall with UFW, 2019). However, configuring these utilities requires some experience in network administration as well as network protocol knowledge, such as which service uses which port (List of TCP and UDP port numbers, 2019) and so on.

Therefore, we will use a system service that allows us to block individual IP addresses based on the service. So we define which service is blocked for a specific IP, but other services are not covered if we don't change that setting. So in short, if we block an IP address from accessing our *ssh* service, then the *www* service, that is, the web server service providing the website does not apply the blocking. This is because access to the server management (via *ssh*) is mostly done by a few people, but virtually anyone from around the world accesses the web presentation because the web presentation is intended to be publicly accessible. The Linux operating system uses a pair of files to control the access to its services, namely */etc/hosts.allow* and */etc/hosts.deny*. The *hosts.allow* file allows addresses that are explicitly defined to access the service while a full access ban is applied, and *hosts.deny* has the opposite effect that all IP addresses are allowed to access our service except those defined in this file. For our approach, we have chosen to use the approach that all IP addresses have access to the services of our server - in our case *ssh* service - except those explicitly defined in the */etc/hosts.deny* file. The addresses in this file are to be "punished" by prohibiting access for their behavior on our server being evaluated as a penetration attempts and not standard communication.

Furthermore, another advantage of this solution is that we can disable entire IP address ranges (IP Address Ranges by Country, 2019), not just one particular IP address. From our experience, we know that attackers use thousands of IP addresses, so it is no harm to block the entire scope, especially when we know that they are locations outside Slovakia. Once the entry to this file is made and saved, the blocking of that address is activated. The address is permanently blocked until it is manually deleted. Of course, we must be careful not to block ourselves inadvertently, because then it is necessary to unblock either directly at the physical location of the server or unblocking it from another non-blocked IP address. This applies to *ssh* service. The advantage of this approach is that even a non-IT specialist is able to perform these interventions after short training. Here's a small bit of /etc/hosts.deny:

```
Sshd
 :
58.242.83.,61.177.172.56,112.115.181.187,168.195.230.82,59.45.175.,105.,203.
206.,213.248.,186.227.230.40,218.,153.,209.87.,115.249.,111.0.,123.,46.166.
185.,221.,122.,188.164.,121.,186.,181.,188.19.,31.,173.,46.,190.,124.,95.188
.,117.,49.,95.68.,175.,103.207.,113.,91.197.232.,51.
```

It can be seen from the brief illustration that we are also blocking specific IP addresses (they have the form *X.Y.Z.W* - that is, they have four octets (IP decimal notation, 2019)) or entire IP ranges, e.g. *51* (marked with bold font). This means that no IP address starting with the first octet 51 will connect to our service. Which service uses this active blocking is marked at the start of blocked IP addresses, in our case it is *sshd* (bolded), which means *ssh daemon - secure shell service (ssh)* mentioned earlier in the text.

Let us show an effect after activating blocking rules (command used to filter out *refused* connections *cat /var/log/secure|grep -i refused*). In just three days, there were 104 observations of refused IP adresses, but we show just four to demonstrate an example:

```
Apr 24 12:05:46 CentOS sshd[12011]: refused connect from 162.105.146.159
(162.105.146.159)
```

```
Apr 24 13:10:53 CentOS sshd[15969]: refused connect from 162.243.148.138
(162.243.148.138)
Apr 24 13:26:41 CentOS sshd[16876]: refused connect from 117.6.19.97
(117.6.19.97)
Apr 24 13:44:48 CentOS sshd[17922]: refused connect from 89.40.70.49
(89.40.70.49)
```

3.3 Other services (Apache web server, MySql database server)

The attackers try to find out in advance which services are running on the target server by doing portscan and test which software versions are running on them. If they find an outdated version of, for example, the Apache web server, they try to attack it and take advantage of non-updated errors in the software. They also test which web applications run on the server, for example, to view and manipulate data (via e.g. phpMyAdmin) in the MySql database and alike. Web server services are, as a matter of principle, provided as public, so activity on them does not necessarily give rise to increased attention, but from time to time it is advisable to audit the access logs and analyze whether there is any non-standard activity. If a web server is properly set up, updated, and all services outside the public zone are password protected, its operation should be relatively secure unless a new security threat or vulnerability occurs. The same is true for the database server service, which should not be available at all, but its services should be provided through a web server. Following is a sample from a web server log file showing non-standard activity, but it did not compromise the server, just shows attacker's break-in attempts:

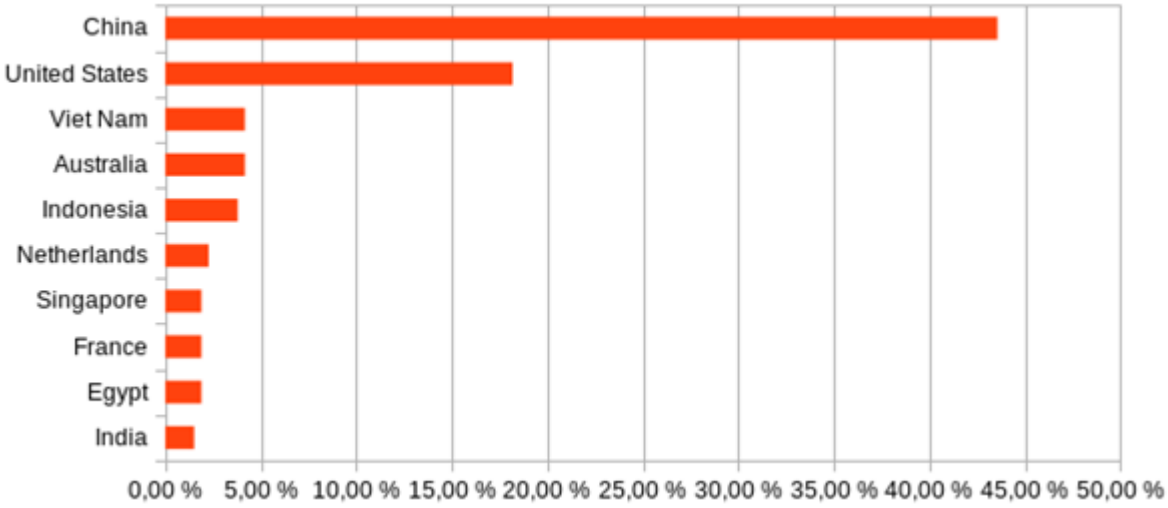
```
190.33.56.234 - - [24/Apr/2019:00:20:50 +0200] "GET /phpNyAdmin/index.php
HTTP/1.1" 404 984 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0;
Trident/4.0)"
190.33.56.234 - - [24/Apr/2019:00:20:50 +0200] "GET /program/index.php
HTTP/1.1" 404 984 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0;
Trident/4.0)"
190.33.56.234 - - [24/Apr/2019:00:20:51 +0200] "GET /shopdb/index.php
HTTP/1.1" 404 984 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0;
Trident/4.0)"
190.33.56.234 - - [24/Apr/2019:00:20:52 +0200] "GET /phppma/index.php
HTTP/1.1" 404 984 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0;
Trident/4.0)"
190.33.56.234 - - [24/Apr/2019:00:20:53 +0200] "GET /phpmy/index.php
HTTP/1.1" 404 984 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0;
Trident/4.0)"
190.33.56.234 - - [24/Apr/2019:00:20:54 +0200] "GET /mysql/admin/index.php
HTTP/1.1" 404 984 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0;
Trident/4.0)"
190.33.56.234 - - [24/Apr/2019:00:20:54 +0200] "GET /mysql/dbadmin/index.php
HTTP/1.1" 404 984 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0;
Trident/4.0)"
190.33.56.234 - - [24/Apr/2019:00:20:55 +0200] "GET
/mysql/sqlmanager/index.php HTTP/1.1" 404 984 "-" "Mozilla/4.0 (compatible;
MSIE 8.0; Windows NT 6.0; Trident/4.0)"
190.33.56.234 - - [24/Apr/2019:00:20:56 +0200] "GET
/mysql/mysqlmanager/index.php HTTP/1.1" 404 984 "-" "Mozilla/4.0 (compatible;
MSIE 8.0; Windows NT 6.0; Trident/4.0)"
190.33.56.234 - - [24/Apr/2019:00:20:56 +0200] "GET /wp-
content/plugins/portable-phpmyadmin/wp-pma-mod/index.php HTTP/1.1" 404 984 "-
" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0)"
```

It is clear from the log record text that the attacker tested whether the phpMyAdmin application is running on the server, which is used to access the MySql database, further tested whether we have any applications running in commonly called directories such as mysql, shopdb, and so on and also tried to make sure that the famous Content Management System (CMS) Wordpress is running on the server, which is often the target of attacks. In the next text we summarize the selected number of attacking IP addresses and assign them the country of origin.

3.4 Most frequently used attackers' IP addresses

After applying our new rules for blocking IP addresses attacking our server, we will review the correctness of the measures taken before in our logs to verify that our system will block the connection attempts (see logs illustration mentioned earlier with *refused connect* statement). Now we'll analyze the rejected login attempts for about one week of monitoring, from which country it was reported, the number of attempts, and the result will be displayed graphically (Fig. 1). Tool used for analysis was *whois* utility.

Fig. 1: Percent of IP addresses according to attacker's origin



Source: own elaboration

We can conclude from our calculations that over two hundred of blocked IP addresses were trying to connect to our server in about week. As we can see from the graph the most of them originated from China - 115 times, followed by US addresses - 48 times, and Vietnam, Australia, and Indonesia approximately 10 times. Note that these were connection attempts, which we refused directly at the first connection attempt. Before blocking of selected IP addresses, attempts to connect were in thousands and were made within a few hours almost every two or three days. Analyzing these penetration attempts would be enough to create a separate article and therefore will not be discussed further.

4 Discussion

Aim of our paper was to identify IP addresses with malicious intent to break into our systems. For this purpose we chosed Linux based servers, which are being used in teaching process for students to save their papers and to make e-tests. One of these servers is located inside University of Economics in Bratislava as virtual server and the another one was located as virtual server in google cloud platform infrastructure. Both servers underwent similar type of attacks. The intended purpose of attackers was to find out, which services are published into the internet network and subsequently to adapt the type of attacks. In our servers there are

configured world wide web (www) service (Apache server), secure shell service (ssh) and indirectly can also be accessed database server (MySql). Therefore we described in the text before the main type of attacks, that we can await. By observing log files we identified an often attempts to break-in to our systems via secure shell by technique that can be either dictionary attack or brute force attack. We took measures to stop these activities by blocking particular IP address or whole address block if attacker came from suspicious IP addresses outside european countries. Our security countermeasures approach has main flaw, that in our solution the user is banned forever to access the service. This can cause problem with accessing www service from these addresses for regular users, but it could be treated by time-limited blocking. Users accessing ssh service are mostly administrators, so access to this service can be blocked for everybody outside the whitelisted IP addresses.

5 Conclusion

As we have seen in the analysis on real world data, the problem of security issues and system hacking is more relevant than ever and it can be assumed that similar scenarios are taking place on all available operating systems throughout the Internet. Thanks to the mass scale of internet attacks these lead to relatively successful system penetrations. Based on the public database lustration (RIPE Database, 2019) it is possible to find out IP addresses owners, but it is not possible to determine who is really behind these addresses. It is obvious that the owners of these addresses are not going to reveal the holders of these IP addresses without state authorities' cooperation.

Of course, to gain more precise data, it would be useful to analyze log records for a period of at least half a year and ideally on at least ten and more involved operating systems. This can be a subject of future research.

Resources

Bandel, D. A. (2000). *Linux security toolkit*. Foster City, CA: M & T Books.

Beaver, K. (2018). *Hacking for dummies*. Hoboken, NJ: For Dummies, a Wiley brand.

Blank, A. G. (2004). *TCP/IP foundations*. San Francisco, CA: SYBEX.

Bresnahan, C., & Blum, R. (2015). *Linux essentials*. Indianapolis: Sybex.

Collins, M. (2014). *Network security through data analysis: Building situational awareness.* Beijing: O'Reilly.

Ellingwood, J. (2015, June 18). How To Set Up a Firewall Using FirewallD on CentOS 7. Retrieved February 26, 2019, from https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-using-firewalld-on-centos-7

Hussain, S. (2013, December 17). How To View and Configure Linux Logs on Ubuntu and Centos. Retrieved March 1, 2019, from https://www.digitalocean.com/community/tutorials/how-to-view-and-configure-linux-logs-on-ubuntu-and-centos

Krout, E. (2019, October 1). How to Configure a Firewall with UFW. Retrieved February 26, 2019, from https://www.linode.com/docs/security/firewalls/configure-firewall-with-ufw/

Kultan, J., & Schmidt, P. (2019). *Pokročilé využitie databáz pre ekonomické školy: vybrané otázky*. Vydavateľstvo EKONÓM.

Michael, R. K. (2008). *Mastering Unix shell scripting: BASH, KORN Shell, and KORN 93 Shell scripting for programmers, system administrators and UNIX gurus*. Indianapolis, IN: Wiley.

Pan, Y., Sun, F., Teng, Z., White, J., Schmidt, D. C., Staples, J., & Krause, L. (2019). Detecting web attacks with end-to-end deep learning. *Journal of Internet Services and Applications, 10*(1). doi:10.1186/s13174-019-0115-x

Pompon, R., & Heath, M. (2020, February 6). Top Attacks Against Service Providers 2017-2019. Retrieved April 18, 2020, from https://www.f5.com/labs/articles/threat-intelligence/top-attacks-against-service-providers-2017-2019

Russell, J., & Cohn, R. (2012). *List of Tcp and Udp Port Numbers*. Book on Demand.

Schmidt, P. (2017). *Základy informačných sietí* (1.st ed.). Nové Zámky, Slovakia: AZ Print. pp.91-93

Schmidt, P., & Bandurič, I. (2015). *Úvod do tvorby webu.* Bratislava, Slovakia: Vydavateľstvo Ekonóm.

The red hat enterprise linux team (2018, October 3). Red Hat continues to lead the Linux server market. Retrieved February 23, 2019, from https://www.redhat.com/en/blog/red-hat-continues-lead-linux-server-market

Upton, E., & Halfacree, G. (2016). Raspberry Pi user guide. Chichester, West Sussex, UK: John Wiley & Sons.

CYBER STRATEGY AND FRAMEWORK OF INTERNATIONAL ORGANIZATIONS

Eva Beke[26], Zoltan Rajnai [27]

Abstract
This article focuses on the existing international cybersecurity frameworks, pointing out the various efforts they make at the international organizations. It also examines the directions in the legal and policy framework for global cybersecurity. The goals that international agencies aim to reach, the law and policymaking potentials and the role of both international organizations. As cyber-attacks continue to increase in frequency and in size yearly, the importance and need for better cyber security resilience, mitigation and defence policy would be an equally concerning matter. To improve the present situation and enhance cybersecurity a comprehensive and clearly defined approach and international agreement is necessary. The NATO can set global measure because the influence of their member states while the Organization for Security and Co-operation in Europe (OSCE), is for a regional guideline. Both take initiatives that recognize the full spectrum of cyber threats, crimes and attacks and set frameworks for global, regional and national level. For research method, I have used content analysis, desktop research and secondary data analysis.

Key words
NATO, OSCE, cyber strategies, positions of international organizations, challenges

1 Introduction

The past couple of years have been very productive as far as cyber space concerned. It was a "two-way productivity": in one hand the cyber-attacks against whole nations, like Estonia and Taiwan or against critical infrastructures, like health care institutions, still mills or even governmental domains, throughout the entire globe. On the other hand cyber defence, resilience and mitigation progress were initiated on the global and national level as well. In the 21st century, the cyber space became the new territory for opposition parties to measure the balance of power. Nowadays cyber-attacks happen very fast and can cripple thousands if not millions of electronic devices, and harm organizations' systems and private users' data. They can also compromise governments' order or can try setting a new order from outside or influencing election or even discrediting governments' officials in place. Where the attack is coming from also varies, as much as it can be an outside attack, there is a growing number of insider attacks from employees accessing classified data. In order to see both international organizations' responsibility and the action they authorized to take it would be mandatory clarifying the different cyber conflicts and attacks by legal terms. As we go through each group, we are not only trying to defy the major differences in between cyber conflicts but also giving examples of each. (Jahankhani, 2014)

Internet governance: means a set of collectively agreed initiatives and activities by international organizations, governments, NGOs, and/or public and private sectors, to institute a global-regulation structure that freely supports the geographical, financial, and social use of

[26] Óbuda University / Doctoral School on Safety and Security Sciences H-1089 Budapest, Népszínház utca 8, beke.eva@bgk.uni-obuda.hu

[27] Óbuda University / Doctoral School on Safety and Security Sciences H-1089 Budapest, Népszínház utca 8, rajnai.zoltan@bgk.uni-obuda.hu

the ICT infrastructure among nations. It also aims to establish standards for security and policies for vigilance, defense and control. (Benrik, 2014)

Cyber threats by incidents: not all cyber experts who caused accidents are criminals. They can be either enthusiasts who "just for fun" wants to gain control, or many times like the below examples show a simple error causing a rather dangerous data exposition. (Pires, 2008)

Third party vendor error happened in 2018 in Orlando's Orthopedic Center where 19.000 patients' data been posted

Misconfigured FTP server caused in 2018 at the Med Evolve in Arkansas , USA that 205.000 records were exposed

Cybercrime: is the use of ITC to carry out criminal and harmful acts in cyber space. The person or groups behind these kind of attacks are usually those, whose general intent to generate profit illegally. Most of the times they use different targets; however, they cannot keep control for a prolonged time over the servers as the risk of detection increases accordingly. They do not necessarily want to destroy the systems, hoping that they can receive more information from it.

Because of *Cyber Espionage* in 2019 in the US, stolen medical records were on sale on the Dark Web

Data Breach targeted LinkedIn users in 2019 worldwide, focusing on those associated with financial, energy, and government entities operating in the Middle East

Ransomware attacked in 2019 the Quest Diagnostic, US nationwide and 7.7 million consumers' data were exposed

Cyber terrorism: considered an organized attack, using ICT in cyberspace to strike on other information-communication systems with the aim of causing disruption or destruction with the consequent panic or large-scale public response, mainly in the economic-finance field or often against critical infrastructures.

Wannacry in 2017 worldwide attacked in 99 countries, critical infrastructures, universities, financial institutions with 230.000 computers compromised and demanded ransom in 28 languages

Around 800 various cyber-attacks happened in 2019 *against* Microsoft worldwide targeting think tanks, NGOs, and other political organizations

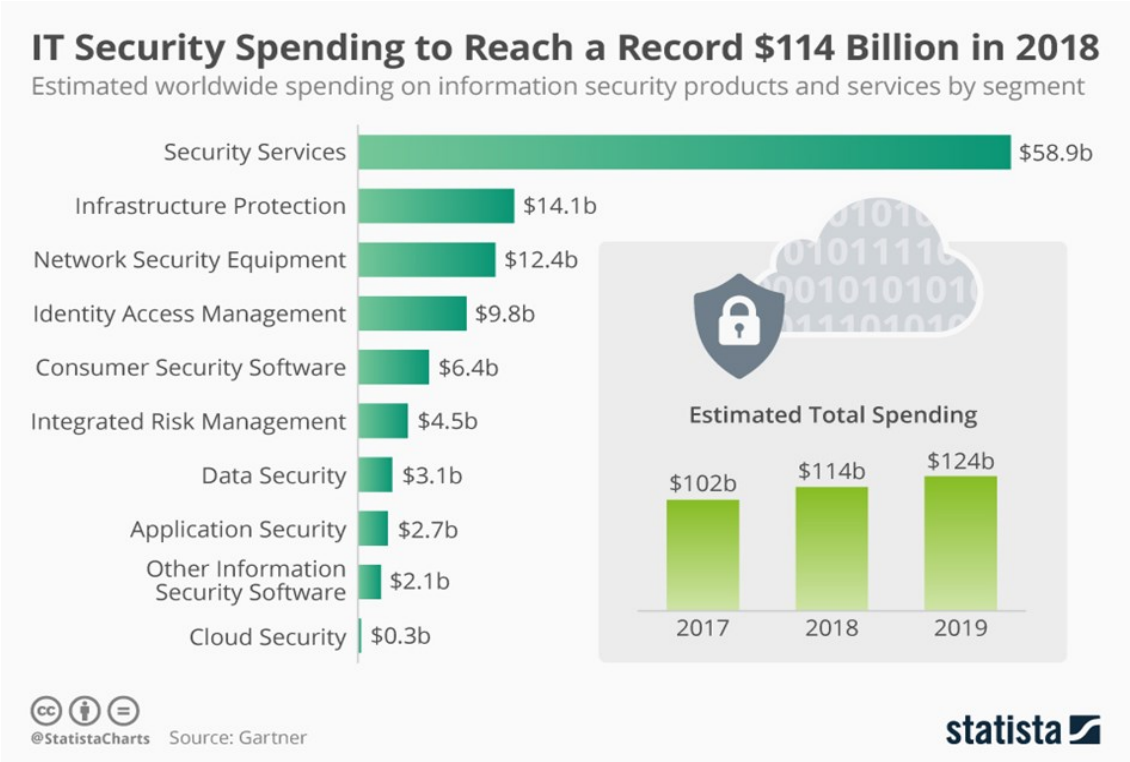
Cyber warfare: can be a conflict between two nations, or even non-state actors and the target generally military, industrial or sometimes civilian. Almost all of them politically motivated acts, "state actors or groups attempt to disrupt the activities of organizations or nation-states, especially for strategic or military purposes and cyberespionage." (Brenner 2006)

In 2020 China *espionage group* (assumed) *attacked Malaysian Government* and stole data about government-backed projects in the region

In 2010, *Stuxnet* caused substantial damage to the Iranian Nuclear Program and effected further India and Indonesia among other nations.

To show relevant data of security measure we chose Gartner's latest estimates, of worldwide spending. It displays how much was the worldwide expenditure on IT Security by segments. The first and second place are representing the highest costs for security services and infrastructure protection. Also amongst the first ten, most secured assets are the data security as well as cloud security. The forecast was for 2019 $124 Billion and one can easily assumes that this number will be higher by the end of 2020, although there is no data as of yet.

Chart 1. Information Security Spending to Reach a Record $114 Billion in 2018



Source:https://www.statista.com/chart/15198/estimated-worldwide-spending-on-information-security/ (Richter, 2018)

After the general overview of the different cyber conflicts, there is a summary in Table 1. (Below) to show the responsibility of each international organizations. It is clear that the UN alone authorized by member states to act on the full spectrum of cyber conflicts, while the NATO can step up only when warfare is the case. Regional or EU organizations can act on various levels which responsibility highly depends on the number of the member states and on their agreements as well. Many like-minded nations within the EU have the same agenda and principles as far as cyber security concerned, unlike the UN where in 2017 and since then there were not any common consensus in this matter ratified and accepted by all nations. That is why regional organizations input, laws and considerations can set further agreements for international cyber security standards, framework and stability.

Table 1. International organizations' positions for cyber defence

	OSCE	UN	OECD	CoEu	EU	G8	NATO	CECSP	ENISA
Internet Governance		•	•	•	•			•	•
Cyber Crime	•	•	•	•	•	•		•	•
Cyber Terrorism	•	•				•			
Cyber Warfare		•					•		

Source: https://www.researchgate.net/publication/236808768_Global_Cybersecurity-Thinking_About_the_Niche_for_NATO (Tikk, 2020)

2 The North Atlantic Treaty Organization's role (NATO) in cyber defence

NATO has a distinctive role in the field of cyber security. Its challenge will be to both integrate with and take advantage of the existing, somewhat fragmented cybersecurity frameworks of its member nations. NATO needs a practical and structured coordination mechanism with national authorities to respond cyber incidents and national security-relevant attacks. To discuss NATO's relevant role in the field of cybersecurity, there are some corner stones to focus on, mainly because other international organizations have so far failed to implement it effectively. The first is an adequate response mechanism for cyber-attacks, which would include proper information exchange, without jeopardizing any allies' territorial integrity, political independence or national security. This role of NATO is different comparing to those, which are governing Internet and information society issues. The current policy framework focuses on the security of NATO's systems and the assistance to allies in case of a cyber-attack. With this in mind, NATO is starting to combine political, military, industrial, and technological approaches to cybersecurity. NATO could also make a significant contribution in the field of concept development. By formulating, testing and implementing responsible, coherent and effective cyber security concepts will be a challenging task. Responding to cyber-attacks in combination with possible other threat scenarios becomes an even more demanding task, which requires better coordination and agility. NATO's position allows necessary steps in two different phases. (Efthymiopoulos, 2019)

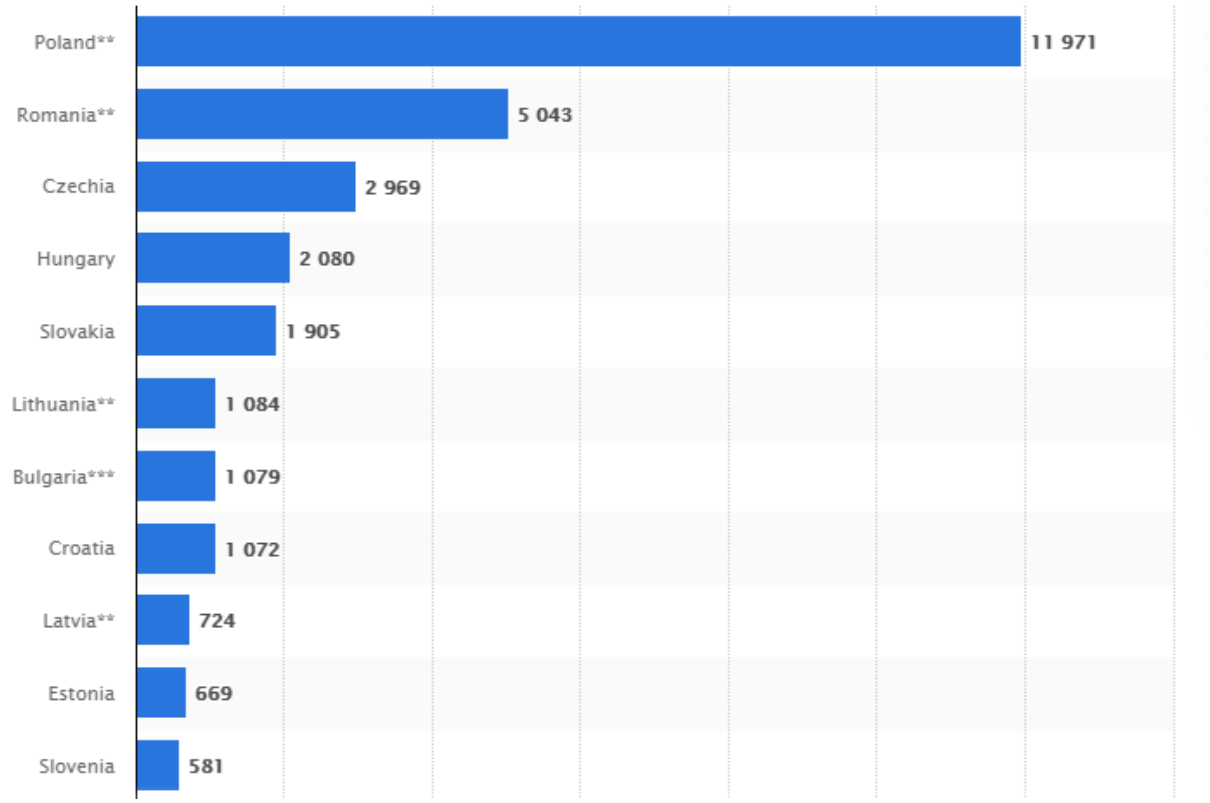
Cyber resilience: the main aim is to provide military resilience and business continuity. NATO as a global player is encouraged by member states "(1) to protect NATO's operational information systems, and (2) to protect its allied countries from any e-, or in other words cyber-attacks…" (Efthymiopoulos, 2019)

Smart defense: meaning the use of new technology, the latest cyber defense method and having a wider knowledge about the insecurities of cyber environment. The basic purpose was to „rethink present strategies and identify urgent measures to be taken in order to minimize the strategic and economic impacts of cyber-attacks". (Efthymiopoulos, 2019)

NATO more and more observes that organized cyber-attacks aim to exhaust the "gaps" in the "system social and market matrix". Consequently, member states should enhance the necessity for coordination of human resources in connection with IT warfare, operational network, counter intelligence, and cyber-defense, in the field of practicalities, such as trainings and operation practices, and in the scientific field as well, for technological and innovation exchange. (Shen, 2016).

Traditional security affairs require both a careful defense planning and resilience. Although cyber security defined as an e-dimensional effort to protect our IT systems, critical infrastructures or governmental institutions the same rules apply there too. Cyber security at NATO level is a strategy, just like on a traditional battlefield preventive and operational. Require interdisciplinary methods such as political-military coalition as well as technological and innovation development. Global framework is necessary in our interconnected and rather "creative" operational world, because only national level security measures might not be enough to mitigate or protect nations. "In 2019, considering the risk assessments on hybrid threats and challenges, the need for better civil awareness and readiness, at a time of much needed cooperative defense, allies have to decide for a robust long-term planning innovative and entrepreneurial strategy for current and future operations of NATO. Keeping in mind the need for strong success in field operations, including success in and at a multi-dimensional level of operations against all threats while making operations to be cost efficient with minimum human casualty numbers." (Efthymiopoulos, M., 2019) As the chart shows below, the estimated military expenditure of NATO, countries reached over 1 billion US$ in 2019, what is clear sign that security including the new threat of cyber security became an ever-important issue in the international arena.

Chart 2. Defence expenditure in the current prices and exchange rates in the Central and Eastern European (CEE) countries in 2019(in million U.S. dollars)

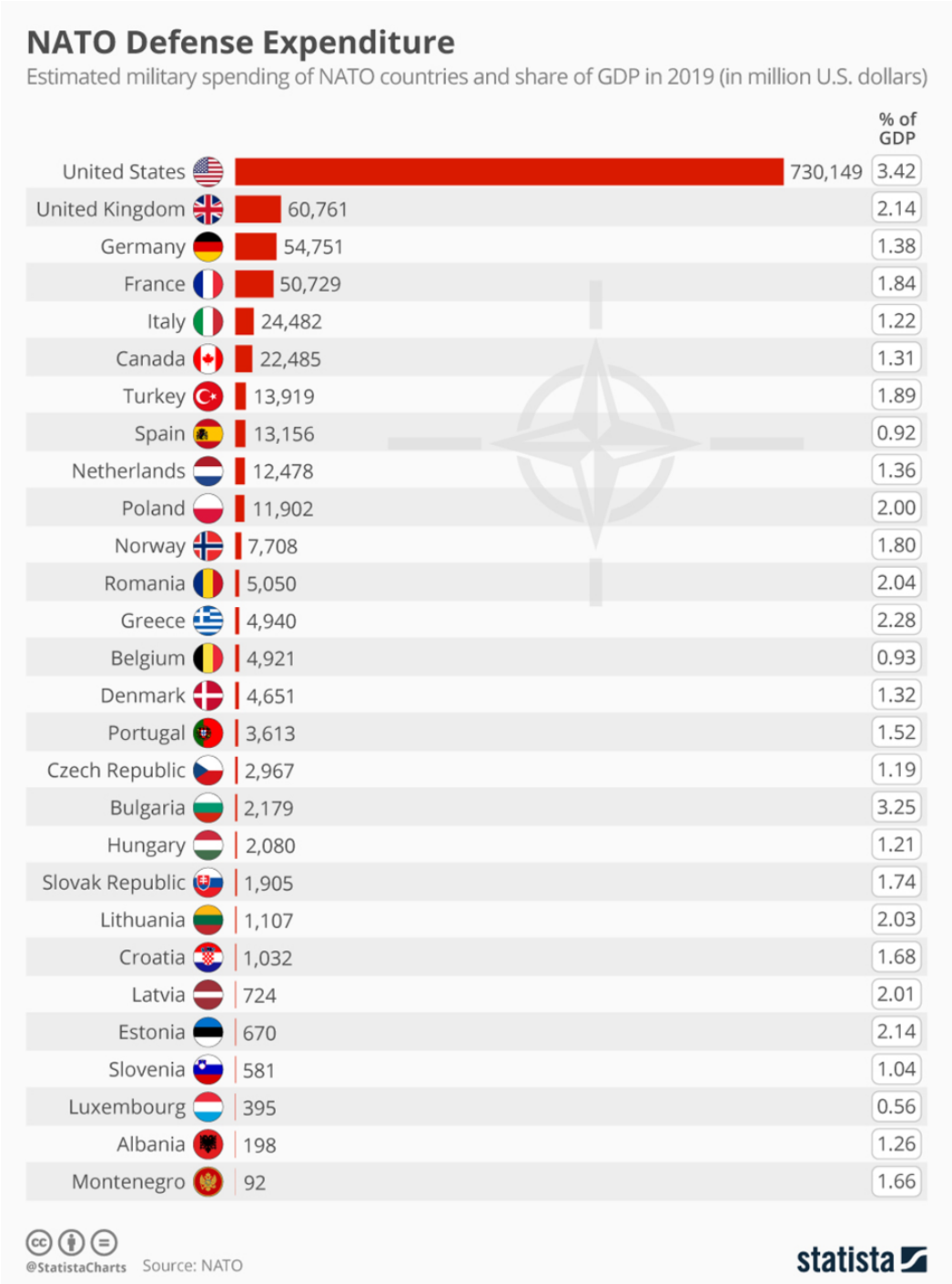


Source: https://www.statista.com/statistics/1085713/cee-military-expenditure-in-current-prices/ (Sas, 2020)

In 2017, - by statistical data – only five countries met the goal of spending 2 percent of their GDP on defense and that has now increased to nine according to the alliance's latest budgetary data. The U.S. is set to spend over $730 billion on its military this year and it's joined above the 2 percent threshold by Bulgaria (3.25 percent), Greece (2.28 percent), the United Kingdom (2.14 percent), Estonia (2.14 percent), Romania (2.04 percent), Lithuania (2.03 percent), Latvia (2.01 percent) and Poland (2 percent). (McCarthy, N, 2019)

"Poland incurred the highest defense spending from NATO member states in the region of Central and Eastern Europe in 2019. Almost 12 billion dollars are expected to be allocated for this purpose. It is also likely that in 2019, in the region of Central and Eastern Europe, the NATO-recommended allocation of two percent of GDP to defense will be exceeded by Estonia, Romania, Poland, and Latvia." (Adriana Sas 2020)

Chart 3. NATO defense expenditure



Source: https://www.statista.com/chart/14636/defense-expenditures-of-nato-countries/ (McCarthy, N, 2019)

3 The Organization for Security and Co-operation in Europe (OSCE) as a regional player in cyber defence

Cyber threats are, by their very nature, global. Effective defence therefore requires coordination among nations. Securing the flow of information — from critical to economic and social life —requires a balance between national and international measures. Despite somewhat differing national views on cybersecurity measure cooperation has proved successful among

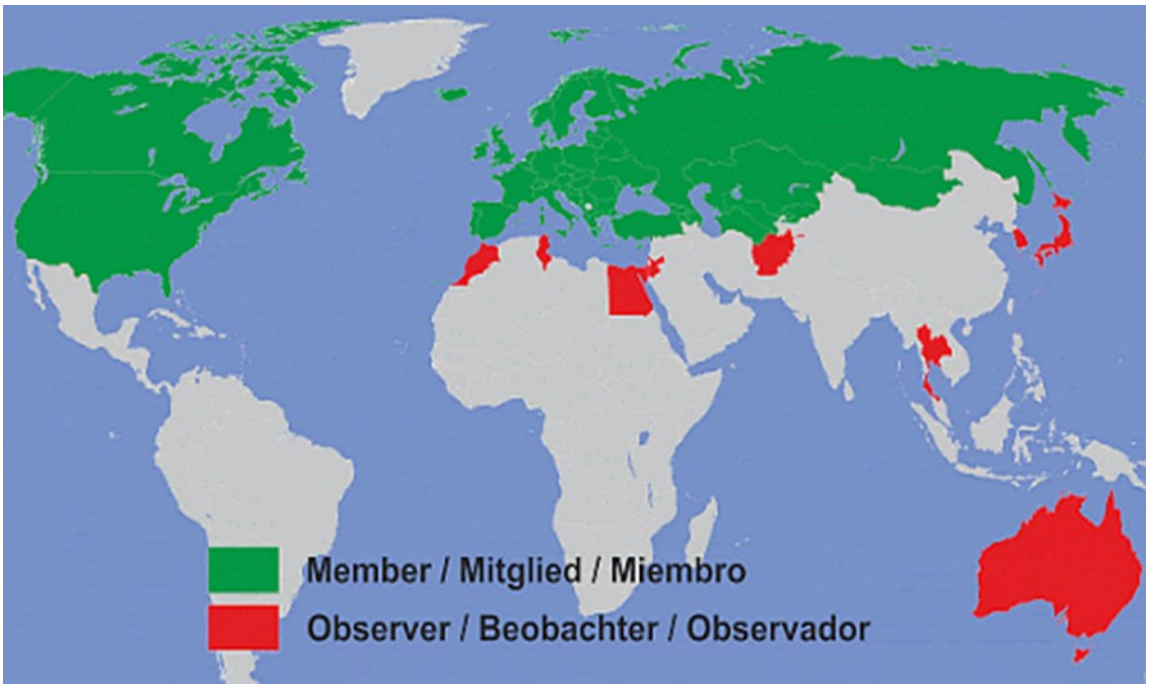
like-minded partners, and there are signs of emerging cyber-coalitions. Thus, the task of securing the cyber domain and information society must truly be both a national and international one.

Besides the United Nations and The European Union, several regional organizations and fora have developed working agendas on cybersecurity and ICTs in the context of international and regional security, particularly through the lens of confidence-building and cooperative measures. The OSCE, for example, commenced its work in this area in 2011, resulting in the establishment, by the OSCE Permanent Council. The Organization for Security and Cooperation in Europe (OSCE, 2020) is one of the most important security institutions in the pan-European region since the end of the Cold War. (Biscop 2006)

The OSCE is counting 57 member states, what makes it the largest security-oriented international organization. Unlike NATO, what has 30 member states, which out of 28 are also in Europe, excluding Canada and USA from North America. OSCE members cover most of the Norther Hemisphere and established in in 1975 August 1st as a forum for the East-West talks.

OSCE is often referred to as a 'soft' security organization, because a political agreement rather than a formal international treaty established it and because it does not have its military forces to deploy, unlike NATO. In order its decisions, to come into force depends heavily upon the powers of its participating states, on the diplomatic skills and on cooperation with other international or even regional institutions.

Fig.1. Member States of OSCE

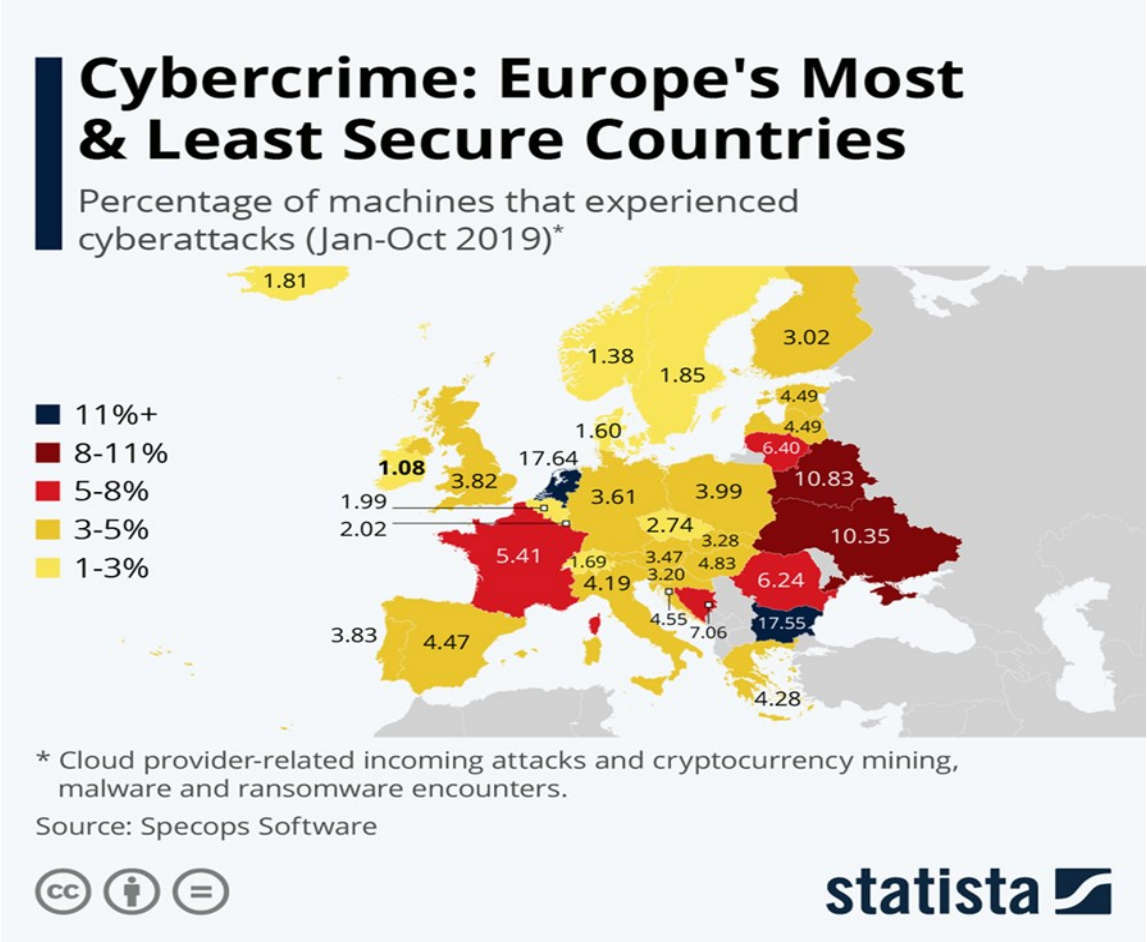


Source: http://www.geo-ref.net/en/t-osce.htm (OSCE, 2020)

OSCE cyber security framework and directives' main aim is to improve security of all levels. The objective includes changes in behavior towards cyber security, driving investments and using the already existing tools for defense and mitigation. (Carrapico, 2016). In Vienna in 2016 with the agreement of all 57-member states, they came to a groundbreaking list concerning OSCE confidence-building measure to enhance cyber stability and reduce the risk, primarily stemming from the use of ICT systems. (Bossong 2016)This practice would further include reducing or in any case, to cooperate when cross-border attacks or incidents involved, providing more information and data through a trusted electronic communication networks, dependence

on advancement of technologies, even on those developed outside of the EU, critical infrastructure protection against cyber-attacks. (Fransen, 2015)This agreement is still in effect, however a new set of directives are also ready covering the coming years of 2021-2027. This is a so-called "five-pillar policy" framework, with an attached budget of 2 Billion EUR. (The draft proposal at EU's future budget agreement) (Mitrakas, 2019)The five key area would include best use of Digital Capacities and Interoperability, Cybersecurity, Artificial Intelligence, High Tech performance Computing and Advanced Digital Skills. The reason for enhanced alliance and defense shows in the map below. "Specops Software has released data showing the countries in Europe most and least susceptible to cybercrimes. The company analyzed the total number of cloud provider related incoming attacks as well as cryptocurrency mining, malware and ransomware encounters on machines in each country. The Netherlands has the highest rate of machines that experienced one of the above attacks at 17.64 percent while Ireland had the least at 1.08 percent." (McCarthy, N, 2019)

Fig. 2. Cybercrime: Europe's Most & Least Secure Countries

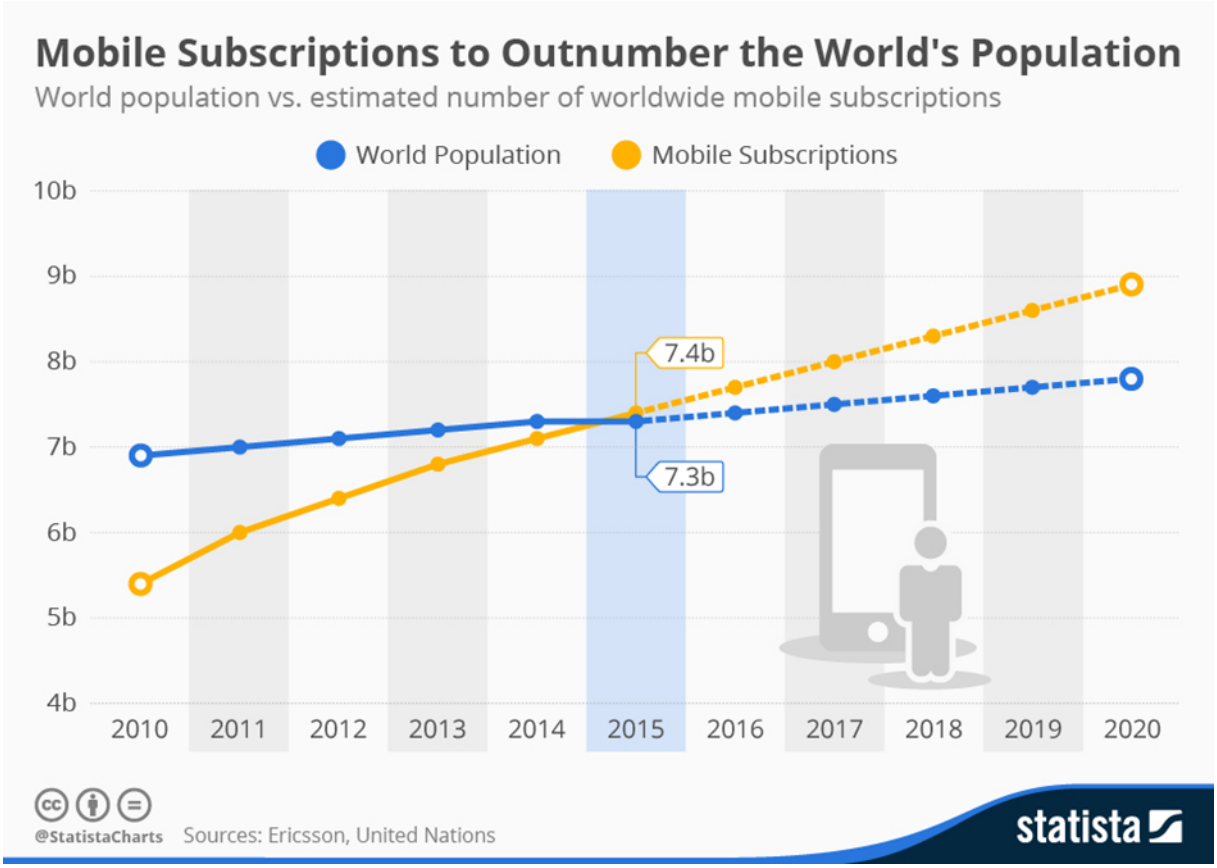


Source: https://www.statista.com/chart/20914/share-of-european-computers-that-experienced-cyberattacks/ (McCarthy, N, 2019)

In 2017, member states agreed on protecting national critical infrastructure systems, as the most validated future attacks against national wellbeing and safety. The OSCE also serves many political agenda focusing on European and world citizens as well to achieve a better and more secure place. More and more reports suggest that half of the cyber-attacks caused by human errors whether of malicious or incautious reasons should be another discussion. That is why OSCE decided to promote and implement some necessary changes and training in human behavior and habits when it comes to information security. On the other hand, OSCE is also a

first-runner promoting fundamental human rights, such as freedom of expression and securing private data without any compromises. As the chart below shows that by 2015, the mobile subscription outnumbered the world's population. As a forecast, we can also see that by the end 2020 this number will exceed the population by a billion, so the necessity to train future generation is imperative in this fully interconnected era.

Chart 4. Mobile Subscriptions to Outnumber the World's Population



Source: https://www.statista.com/chart/4022/mobile-subscriptions-and-world-population/ (Richter, 2015)

OSCE relationship with the above-mentioned NATO is also a main point in its agenda. Out of the two international organizations only NATO is authorized to have military deployment against cyber warfare acts, however other military issues such as enhancing not only the protection phase, but actively cooperate in the field of anticipation and preparation can be a common goal. OSCE's other particularly important focus is on cybercrime and the use of info communication systems by terrorists. The strategy includes the potential countermeasure acts, to exchange best practices between member states and at the same time to recognize the private sector's partnership and effective technology-driven involvements. (Van Puyvelde, 2018)
As Michael Linhart said in his opening remarks in 2017 in Vienna,

"Uncertainty about the origin of hostile cyber action is a common characteristic of cyber incidents and introduces a further element of potential instability into international affairs. Furthermore, the protection of human rights 'online' as well as 'offline', in particular the right to privacy, needs to be guaranteed as well in order to rebuild confidence between states and their citizens. Faced with these challenges, we need to come together to do three things: work towards a common understanding of the rules for responsible state behavior in cyber space; promote confidence and trust between states; and strengthen our efforts to increase cyber resilience by promoting capacity building." (Michael Linhart, Austrian Deputy Foreign Minister, 2017 OSCE Chairmanship Conference, Vienna).

4 Conclusion

At this critical point for global cyber security, international organizations have recently reinforced their agendas to tackle cybersecurity in a more comprehensive setting. However, how single states choose to take part will greatly influence the future of collective success.

At present, both international organizations along with others set to introduce legal, operational and technical framework to protect cyberspace. Once they worked out an essentially acceptable position, and then have the capability to decide when meaningful and applicable international agreement will come into force to achieve a comprehensive and effective cybersecurity framework.

Despite having developed extensive and thorough information security and policy-, frameworks the regional, European organizations are not able to build global information security alone. Global commitment for strategies has utmost importance too.(Dijkstra,2018)However by staying with regional agreements can result varying normative depth, which – considering the global nature of the Internet, IoT, AI and their relevant agents and systems – does not seem the most efficient approach. As for the advantages, regional guidelines could show a faster way to operational and legal norms on a larger, global scale as well.

Resources

Bernik, I. (2014). Cybercrime and cyber warfare. Retrieved April 04, 2020, from https://www.amazon.com/Cybercrime-Cyber-Warfare-Focus-Wiley/dp/1848216718

Biscop, S. (2006). The EU, the OSCE and the European security architecture: Network or labyrinth? *Asia Europe Journal, 4*(1), 25-29. doi:10.1007/s10308-006-0044-8

Bossong, R., & Wagner, B. (2016). A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime, Law and Social Change, 67*(3), 265-288. doi:10.1007/s10611-016-9653-3

Brenner, S. W. (2006). Cybercrime, cyberterrorism and cyberwarfare. *Revue Internationale De Droit Pénal, 77*(3), 453. doi:10.3917/ridp.773.0453

Carrapico, H., & Farrand, B. (2016). 'Dialogue, partnership and empowerment for network and information security': The changing role of the private sector from objects of regulation to regulation shapers. *Crime, Law and Social Change, 67*(3), 245-263. doi:10.1007/s10611-016-9652-4

Dijkstra, H., Mahr, E., Petrov, P., Đokić, K., & Zartsdahl, P. H. (2018). The EU's partners in crisis response and peacebuilding: Complementarities and synergies with the UN and OSCE. *Global Affairs, 4*(2-3), 185-196. doi:10.1080/23340460.2018.1530572

Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship, 8*(1). doi:10.1186/s13731-019-0105-z

Fransen, F., Smulders, A., & Kerkdijk, R. (2015). Cyber security information exchange to gain insight into the effects of cyber threats and incidents. *E & I Elektrotechnik Und Informationstechnik, 132*(2), 106-112. doi:10.1007/s00502-015-0289-2

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. *Cyber Crime and Cyber Terrorism Investigator's Handbook,* 149-164. doi:10.1016/b978-0-12-800743-3.00012-8

McCarthy, N., & Richter, F. (2019, December 03). Infographic: NATO Defense Expenditure. Retrieved April 04, 2020, from https://www.statista.com/chart/14636/defense-expenditures-of-nato-countries/

McCarthy, N., & Richter, F. (2020, February 21). Infographic: Cybercrime: Europe's Most & Least Secure Countries. Retrieved April 01, 2020, from https://www.statista.com/chart/20914/share-of-european-computers-that-experienced-cyberattacks/

Mitrakas, A. (2018). The emerging EU framework on cybersecurity certification. *Datenschutz und Datensicherheit - Dud*, 42(7), 411-414. doi: 10.1007/s11623-018-0969-2

OSCE (2020).ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE. Retrieved 3 May 2020, from https://www.osce.org/

Pires, H. F. (2008). Global Internet Governance: The Representation Of Country Toponyms In Cyberspace. Retrieved April 20, 2020, from http://www.ub.edu/geocrit/sn/sn-270/sn-270-151b.htm

Richter, F. (2018, August 23). Infographic: Information Security Spending to Reach a Record $114 Billion in 2018. Retrieved January 13, 2020, from https://www.statista.com/chart/15198/estimated-worldwide-spending-on-information-

Richter, F. (2015, November 17). Mobile Subscriptions to Outnumber the World's Population [Digital image]. Retrieved May 02, 2020, from https://www.statista.com/chart/4022/mobile-subscriptions-and-world-population/

Sas, A.(2020). Defense expenditure in the current prices and exchange rates in the Central and Eastern European (CEE) countries in 2019* [Digital image]. Retrieved May 02, 2020, from https://www.statista.com/statistics/1085713/cee-military-expenditure-in-current-prices/

Shen, Y. (2016). Cyber Sovereignty and the Governance of Global Cyberspace. *Chinese Political Science Review,* 1(1), 81-93. doi: 10.1007/s41111-016-0002-6

Tikk.E.(2020). Global Cybersecurity–Thinking About the Niche for NATO. *SAIS Review of International Affairs,* 30 (2), 105-119. doi: 10.1353/sais.2010.0012

Van Puyvelde, D. (2015). Hybrid war – does it even exist? NATO REVIEW. Retrieved April 04, 2020, from https://www.nato.int/docu/review/articles/2015/05/07/hybrid-war-does-it-even-exist/index.html

DESIGN A PROTECTED ROOM FROM INFORMATION SECURITY ASPECT, A PERSONAL APPROACH

Gábor Bréda[28]

Abstract

In today's information world owning and using information in the right place and time will provide its owner with benefits. Obtaining and transmitting information is not as difficult as in recent historical periods. When it comes to infocommunication systems, the digital recording and flow of data and information is the basic function of these communication technologies, it is difficult to prevent the selective entry and spreading of information. According to my research, there may be an increased need for personal communication where it can be ensured that the subject matter of the discussion will remain between the parties present, and the information provided remains within the confines of the communication environment, excluding the theoretical information security gaps.

One way to create verbal and visual information security is to conduct the interaction between the walls of a protected meeting room. Creating such a space in today's environment of wireless information and communication technology is a special task, as in my opinion the entire set of telecommunication achievements of the information society should be excluded from the protected environment. The physical security of protected conference rooms also requires the constant monitoring and protection of the live radio environment.

By continuously operating a radio monitoring system in the environment, you can obtain a picture of the characteristics of the radio ether and the presence of the radio communication devices present. The emergence of a new frequency may pose a security risk. The source of the new signal needs to be identified.

In this paper, I intend to outline the physical design of the protected meeting room I consider appropriate.

Keywords

Protected room, information security, RF shielding, acoustic shading,

1 Introduction

In today's information society, information is generated 24 hours a day, whether open or non-public. The data is usually stored on a storage medium or IT system to achieve the appropriate quality and capacity. Data must be processed to obtain information. Data processing and result storage nowadays is carried out almost exclusively on computing devices, which significantly increases the relevance of creating security designs to protect non-public data. (Act on the Protection of Classified Data, 2009) At the legislative level, data protection is addressed by development and research teams, as well as international and national organizations, dealing with the protection of IT assets and networks, as the basic information sharing environment of the information society. (Government Decree on the procedure for the operation of the National Security Inspectorate and the handling of classified data, 2010) However, the scope of this article does not allow a detailed presentation of these. (Government Decree on the detailed rules for industrial safety inspection and the issuance of site safety certificates 2010) (Act on Electronic Information Security of State and Local Government Bodies, 2013) (Government Event Management Center) (ISO, 2013)

[28] Óbuda University , Doctoral School on Safety and Security Sciences , bredagabi@freemail.hu, ORCID ID:0000-0001-7868-6637

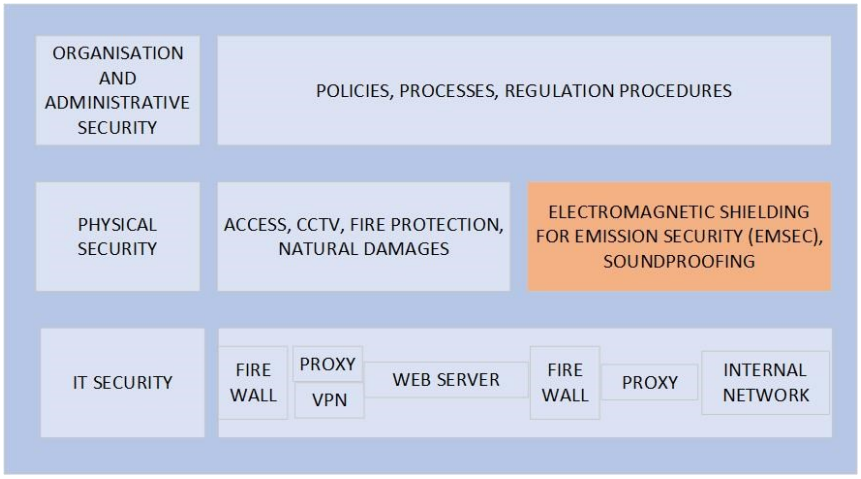
2 The emerging breach in information security

Focusing on the subject of the research, it can be declared that to ensure that non-public information is protected (be qualified or sensitive) several criteria has to be met. The confidentiality, integrity, credibility, and availability of data, as well as the necessity and proportionality of the protection, and the principle requirement of knowledge must not be violated. (Act on the Protection of Classified Data, 2009) In order for a dataset to be interpretable by a human being, one has to elaborate it, learn it, and share it with others (Act on Electronic Information Security of State and Local Government Bodies, 2013). The information should continue to comply with the criteria wich apply to data (Ackhoff, 1989). The processing of protected information usually takes place in a delimited system, in an environment protected by engineering and the previously mentioned laws and organizations. (IBM Global, 2010) Cognition and sharing in a human-human context require new physical and protective measures to achieve a consistency in the level of protection. Human cognizance is carried out with the help of sensory organs, especially through hearing and vision. The presentation of information in a form that is directly understandable to humans involves new media, of which protection cannot be ignored in the processing, storage, and transmission chain, which, until now, has been well protected. These media include the space in which the information is displayed acoustically and visually. Cognition requires interfaces. The physical phenomena appearing in voice-based transmission are either the vibrations of the voice generated by human communication or the sound of a speaker from an IT media player. During visual transmission, the physical phenomena are either the paper with the written information or the information content of the various monitors and projectors. There are several physical phenomena in the chain that need to be investigated from an information security point of view, and security steps may be needed to be taken to block a certain channel in case of a theoretical emergence of an information security breach (Ványa, 2001) (Vadász, 2014) . If stored and transmitted information are provided with a high level of protection in IT and storage systems, then beside the protection of legal, theoretical and IT elements, the physical design of the environment compliant to information security also cannot be neglected, as data and information is displayed there in their purest, most human-close form. (Rajnai &Fregan, 2016) (Varga, 2008) With regards to its notion, I call a protected room a demarcated area where the exchange of data and information on data carrier devices, and human-to-human communication can be realized in accordance with the criteria for classified information. (Haig, 2006) (Haig, 2007) Problem: During cognition and communication, primary and secondary physical phenomena are created that carry the information itself, thereby opening up the theoretical possibility of information leakage. (Kerti, 2010) (Muha, 2007) (Keszthelyi, 2012)

3 Complex protection strategy

The specific procedures used in case of protected rooms are illustrated in Figure 1 below, based to their position in the complex security strategy. The model, based on an individual approach, can be divided into three groups: Organization and administrative control, Physical security, and IT security. Organizational and administrative measures determine the rules, processes, and regulations governing data management, thereby providing basic policy measures to ensure the protection of information. IT security implements the secure design of IT systems and the storage of data on IT systems by developing hardware and software components for the security strategy. In the process of creating physical security, traditional physical protection components include elements for the magnetic and radio attenuation of the environment and the acoustic attenuation of the protected space.

Fig. 1: Developing complex information security (own figure)



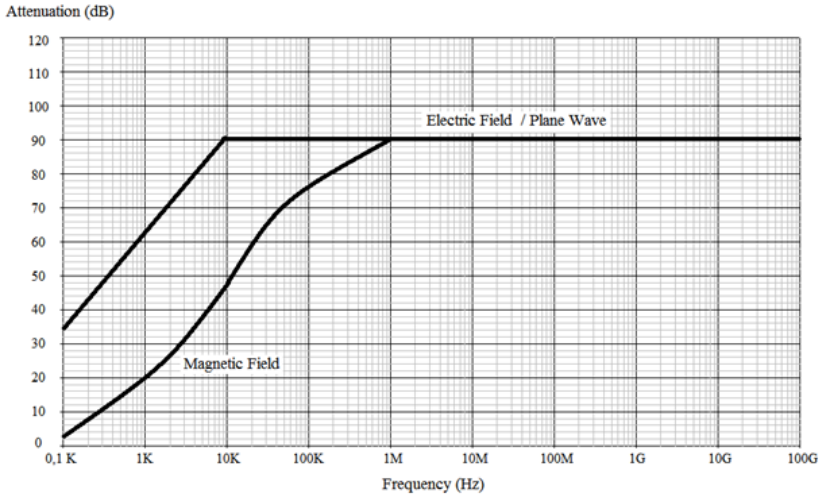
A primary phenomenon is the sound that makes use air pressure waves as a transmission channel to make the eardrum of nearby communicators and the surface of nearby objects vibrate. In the case of visual communication, photons of light are reflected by the written media and are directly emitted by the monitor or projector and travel through the air into the eyes of the participants. Secondary phenomena are magnetic fluxes that correlate with the appearance of information resulting from the operation of equipment used in communication, additional vibrations in the sound generated by the sound, and scattered beams during the reflection of light. In addition, further information security problems may be posed by controlled, but not always reliable telecommunication devices at the site of communication, whose networks now provide almost complete geographical coverage. (Haig, 2006) Based on the data protection criteria and considering the possibilities of technology, it can be stated that, Thesis: the primary and secondary physical phenomena that occur at the site of an interaction during human-to-human communication and information from a technological device can, in principle, be intercepted without adequate protection, thus preventing the protection criteria from being met. Sensitive data and information must be processed and distributed to the right holders within the walls of a room, a protected area in which they are secure. The physical phenomena resulting from the various forms of communication and the contributing additional information must remain in the confines of the protected space.

4 The protected room

Designing a protected room, in this case a protected meeting room, is hardly conceivable without the use of defence resources, following a security strategy. Resources, by their very nature, can have powerful solutions and technical protection tools. My research focuses on the development of physical and technical protection solutions. When establishing a protected room, placement is the first step. The location of such a room should, as an autonomous space, be positioned as an interior space of a building group, with a complete horizontal and vertical interconnection. The physical security of the protected room can be further enhanced by surrounding it with a fully controlled space. The design proposal is the realization of a shell model, according to which a new autonomous space is created within the designated space, with the realization of special needs. The masonry, the floors, and ceilings of this new space must be made of a material with sufficient strength to support the carrying capacity of an interior space's design. In terms of material, breakdown and restoration should not be possible without traces. The space between existing and formed spaces must be permeable from all directions due to the feasibility of subsequent checks. The inner side of the confining outer space has to be shielded

in order to dampen the radio signals originating from within the inner space and to prevent access to the communication channels from the outside. (Standard No.IEEE-299-2006) After analysing the literature, it appears to be a good solution to implement a magnetic and electric field shielding surface with 90 dB attenuation, the theoretical damping curve of which is shown in Figure 2. (Catrisse, Vanhee & Pissort, 2015)

Fig. 2: Dampening characteristic curve (own figure)



By shielding magnetic and electrical fields, it is possible to eliminate the theoretical information security vulnerability arising from the operation of various electronic devices. (Standard No. MIL-STD 285) The ventilation of the inner room must be solved from the outside room so that the flow of fresh air arrives indirectly to the inner compartment's airspace to avoid contact with the direct outside space. In the space between the two rooms and in the engineering channels, noise has to be generated to prevent the transmission of sound vibrations and secondary mechanical vibrations from the interior room. The masonry of the exterior surrounding room shall be designed with a degree of attenuation relative to the sound produced inside the room, so that the vibrations of the human voice produced in the room cannot pass through the walls nor be detectable by instrumental testing. Table.1 shows a subjective summary of sound attenuation value and speech intelligibility.

Tab. 1: Understandability of speech in relation to the sound dampening between two areas

Sound dampening between two areas (dB)	Evaluation on subjective basis
25dB	Normal speech can be heard
30dB	Loud speech is clearly heard
35dB	Loud speech is understandable in case of no other noise
40dB	Loud speech can be heard, but it is not understandable or hard to understand
45dB	Loud speech can barely be heard, not understandable
>50dB	Loud speech can be heard only in a very quiet environment and can not be understood

According to the table, a sound attenuation of more than 50dB is required between a protected room and the outside. (Standard No. MSZ 15601-1:2007) (Standard, MSZ 15601-2:2007) The lighting of the meeting room should also be provided with light sources on the walling of the surrounding room, thus reducing the number of technical installations used in the inner space of the protected room. (ISO, 1998) Considering the furnishing of the meeting room,

simplicity should be sought after. Furniture items should contain as little metal as possible, relying mainly on glass- and transparent plexiglas furniture, if possible. When designing the security, the room complex must be secured with proper locking and access control system. When constructing the electronic property protection, it is recommended to create an autonomous camera surveillance system and electronic property protection that is separate from the central defence system. When discussing the comprehensive design of the complex security of protected premises, the monitoring of the radio environment of the room cannot be neglected. In the vicinity of a protected room, it is necessary to know the characteristics of the radio spectrum and the origin of the frequencies found therein, in order to detect newly emerging signals. The radio monitoring system is used for this purpose. (Vaszari, 2007) Despite the shell model, an emerging radio signal may pose a security risk, and its origin must be identified. (Kuris, 2009) (NBF, 2019) A visualisation of such a room, based on the results of the research, is shown in Figure 3.

Fig. 3: Possible design of a protected room (own figure)

Prom a design perspective, the interior walling of the room is made of glass. The material and the transparent structure of the masonry greatly determine the simple exclusion of a conceptual vulnerability that would require the presence of equipment on or inside the walling, capable of generating information leaks. Inside the room there is a ventilation device to ensure the possibility of continuous human presence, which must be specially designed, while keeping the radio and acoustic damping at the appropriate level. The interior must rest on support legs for the complete accessibility of the perimeter. Lighting is provided from the outside. This eliminates a further theoretical vulnerability. In my opinion, it is expedient to create artificial acoustic signals in the space between the two rooms, thus increasing the suppression of the vibrations generated in the external masonry during the protected communication. In my opinion, the same level of attenuation should apply to windows and doors as to the walling for the sake of consistency in security levels, so I do not consider the placement of a door or window to be practical. (Berek, 2014)

The internal power supply's circuits should preferably be provided with a filter that only allows 50 Hz of the mains current through, thus preventing radio waves from appearing in indoor equipment in the direction of the power supply, and the transmission of external radio and telecommunication radio signals from the interior of the protected room. This is crucial for maintaining the consistency of security strength of the magnetic and electric attenuation devices. (Berek, Berek & Berek, 2016)

5 Conclusion

Based on my research and my personal concept, this paper outlines the definition of a protected space from the research aspect of the topic. The potential information security problems are presented, alongside with a proposition on how to eliminate them. The security solutions are placed in the defence model based on individual ideas. Finally, the design ideas can serve as a model for the design of a protected room.

Resources

2009. CLV. Act on the Protection of Classified Data. (n.d.). Retrieved April 10, 2019, from http://njt.hu/cgi_bin/njt_doc.cgi?docid=126195.383725

90/2010. (III. 26.) Government Decree on the procedure for the operation of the National Security Inspectorate and the handling of classified data. (n.d.). Retrieved April 10, 2019, from http://njt.hu/cgi_bin/njt_doc.cgi?docid=132266

92/2010. (III. 31.) Government Decree on the detailed rules for industrial safety inspection and the issuance of site safety certificates. (n.d.). Retrieved April 10, 2019, from http://njt.hu/cgi_bin/njt_doc.cgi?docid=132295.387559

2013. L. Act on Electronic Information Security of State and Local Government Bodies. (n.d.). Retrieved April 10, 2019, from http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.383761

A Nemzeti Biztonsági Felügyelet feladatairól és az elektromágneses kisugárzás elleni védettség minősítéséről. (n.d.). Retrieved April 10, 2020, from http://www.nbf.hu/tempestmer.html

Ackhoff, R. L. (1989). From Data to Wisdom. Journal of Applies Systems Analysis, 16, 3-9.

Berek, L. (2014). Biztonságtechnika - ÁROP 2.2.21 Tudásalapú közszolgálati előmenetel. National University of Public Service.

Berek, L., Berek, T., Berek, L. (2016). Személy és vagyonbiztonság. Óbuda University.

Catrysse, J., Vanhee, F., Pissoort, D., Celozzi, S. (2015). Differences between NSA 94-106 and IEEE 299 LF magnetic shielding measurements. 2015 IEEE International Symposium on Electromagnetic Compatibility (EMC), Germany, 13-16, https://doi.org/10.1109/ISEMC.2015.7256124

Haig, Zs. (2006). Az információbiztonság komplex értelmezése. Hadmérnök, különszám Robothadviselés 6, 1-9.

Haig, Zs. (2007). Az információs társadalmat fenyegető információalapú veszélyforrások. Hadtudomány, 17(3), 37-56.

Hungarian Standard. (2007). Building acoustics. Part 1: Sound insulation requirements inside building (Hungarian Standard No.15601-1:2007).

Hungarian Standard. (2007). Building aciustics. Part 2. Sound insulation requirements of facades (Hungarian Standard No.15601-2:2007).

Nemzetbiztonsági Szakszolgálat. (n.d.). Retrieved April 10, 2019, from http://www.cert-hungary.hu/

IBM Global Business Service (2010). Smarter cities for smarter growth - How cities can optimize their systems for the talent-based economy. IBM.

IEEE. (2019). Method for Measuring the Effectiveness of Electromagnetic Shielding Enclosures (IEEE Standard No. 299-2006). https://standards.ieee.org/standard/299-2006.html

ISO. (1998). Acoustic, Measurment of sound insulation in buildings and of buildings elements Part 4: Field of airborne sound insulation between rooms (IEEE Standard No. 140-4:1998). https://www.iso.org/standard/2210.html

ISO. (2013). Information technology — Security techniques — Information security management systems — Requirements (ISO Standard No. 27001:2013). https://www.iso.org/standard/54534.html

Kerti, A. (2010). A vezetési és információs rendszer technikai alrendszerének vizsgálata különös tekintettel a minőségbiztosításra és az átvitel biztonságra. [Doctoral dissertation, Miklós Zrínyi University of National Defense].

Keszthelyi, A. (2012). Információbiztonság, technikai alapismeretek. In Vállalkozásfejlesztés a XXI. században. Óbudai University.

Kuris, Z. (2009). Komplex információbiztonság megvalósítási lehetőségeinek megközelítése. Hadmérnök, 4(2), 311-318.

Military Standard. (1956). Attenuation Measurements for Enclosures, Electromagnetic Shielding, For Electronic Test Purposes Method Of (Military Standard No. MIL-STD-285).

Muha, L. (2007). A Magyar Köztársaság kritikus információs infrastruktúráinak védelme. [Doctoral dissertation, Miklós Zrínyi University of National Defense].

Rajnai, Z., Fregan, B. (2016). Kritikus infrastruktúrák védelme. Proceedings of the XXI-th International Scientific Conference of Young Engineers. Romania, 349–352. https://doi.org/10.33895/mtk-2016.05. 78

Vadász, P. (2014). Információkeresés a gazdasági hírszerzésben. Hadmérnök, 9(2), 343-357.

Varga, P. J. (2008). A kritikus információs infrastruktúrák értelmezése. Hadmérnök, 3(2), 149-156.

Ványa, L. (2001). Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre. [Doctoral dissertation, Miklós Zrínyi University of National Defense].

Vaszari, Á. (2007). Üzleti hírszerzés a multinacionális cégeknél és a kis és közép vállalkozásoknál. Budapest Business School.

ASSESSING RISKS IN MOBILE DEVICES BY USING FMEA

Esmeralda Kadena[29]

Abstract
During the last years, mobile device usage has been raised significantly. Due to technological advances, it offers better convenience. Services like (video) calling, messaging, chatting, etc., can be done anywhere as long as network connectivity is available. On the other hand, many risks related to security and privacy have been present.

The objectives of this research are to give a general overview on mobile devices risks and to identify the need for improvement by applying the Failure Mode Effects Analysis (FMEA). To accomplish the objectives, frequent mobile devices failures were determined by using focus group technique. Then the potential failure modes are explained and analysed. The findings of this work support the idea that needs, capabilities and behaviours of people should be considered from manufacturer side in a serious way.

Key words
Mobile Devices, Risks, FMEA.

1 Introduction

Mobile devices provide users with a wide range of services like phone calls, Internet services, sharing and keeping data, on/off-line games, entertaining applications, etc. Due to these services, a mobile device is faced with challenges like security and privacy. Recently, appreciation of the mobile device has been lower than for desktop PCs (PCMagStaff, 2011), and it is more seen as a disposable item (Chin, Felt, Sekary, & David, 2012). Thus, the security awareness can be considered lower than for PCs as well. Now, smartphones pair mobile phones with other devices such as PDAs, HD camera, media player, GPS navigation units and other data storage and processing devices. Even before mobile devices came with 3G and 4G compatibilities, but right now such devices transformed into mobile computers with smart options like touch screen and laptop capabilities, can easily browse the Internet and third-party applications using wireless network.

But while considering security on this field we have to put human- factor in the first line. The user can influence over the mobile device. In most cases he can harm or prevent from harming himself. For an average user it is very important to understand some basics regarding the security risks of his mobile device that might not be properly understood.(Schmidt, Pittner, & Krauspe,. 2014) According to past researches, privacy and security play roles in users' installation decisions. In an experiment realized by Good et al., was found that people preferred applications with better privacy policies if the privacy is included in the cost of application functionality (Good, et al., 2005). On the other hand, there are many cases in which user is not directly involved. Check Point, discovered a "severe infection" in 38 new Android smartphones where the malware were not downloaded into the devices but they arrived with pre-installed malware (Mamiit, 2017).

[29] Óbuda University, Doctoral School on Safety and Security Sciences, Budapest (Hungary)
kadena.esmeralda@phd.uni-obuda.hu

Human factor is the weakest link in the interfacing process and keeping secure information with machines that they interact (Metalidou, et al., 2014). The errors to hardware or software Human factor is the weakest link in the interfacing process and keeping secure information with machines that they interact (Metalidou, et al., 2014). The errors to hardware or software can be unintentional because of the lack of training or intentional violation of guidelines (Beatty & Beatty, 2004). Information security loss comes also because of the corporations; the reactive management approaches that they use in security incidents (Qian, Fang, & Gonzalez, 2012). Maxion and Reeder found that undependable user interfaces are more prone to the flaws in design and they can be a significant factor in the human error that cause security breaches (Maxion & Reeder, 2005). Before developing new devices, engineers can consider human behaviour as accepted in the way it is. A solution might be the approach of human-centred design which puts on first line human needs, capabilities and behaviour and then start designing to accommodate them (Norman, 2013). In order to assess the risks associated with mobile devices, compatible with risk assessment guidelines, Theoharidou et. al, introduced and explained a tailored risk assessment method (Theoharidou, Mylonas, & Gritzalis, 2012). This compatible method with risk assessment guidelines of ISO/IEC (Humphreys, 2007), provided a better evaluation by considering threats and security model of smartphones in Android platform (Šrekl & Podbregar, 2014).

In this paper the focus is on hardware and software failures occurring in mobile devices in general. The work is orientated through the potential failures that might occur from manufacturer, users' practices or both by applying FMEA method.

2 Failure Mode Effects Analysis (FMEA)

FMEA was developed and implemented for the first time in 1949 by U.S. Army and later executed in Apollo space programme to temperate the risk (Carlson, 2012). As a significant method for an engineering design, production process, product planning and so on, should be engaged in companies. Its object is to find links between causes and effects/defects, searching and solving and drawing the decisions based on the requirement of applicable action.

FMEA is a methodology designed for (Stamatis, 2003):

- Identifying potential failure modes for a product or process;
- Assessing risk associated with the identified failure modes;
- Ranking the problems by considering the importance;
- Identifying and counteracting the most serious concerns.

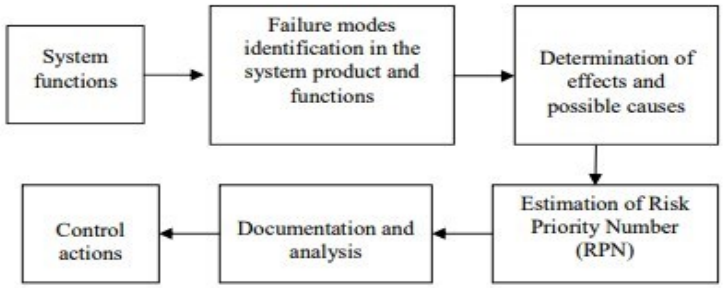
It is a step by step tactic and tends to identify all possible failure throughout the processes and studying the consequences of these failures (Mhetre & Dhake, 2012). The point of applying FMEA is to continuously develop products and process in consistence with consumers' satisfaction (Johnson & Khan, 2003). FMEA method can be used in (Dudek-Burlikowska, 2011):

- Formation of the product concept, to check if the customer prospects are taken in consider.
- Product defining, for checking if projects, service, supplies are appropriate and controlled in the right time.
- Process of production, in order to check if documentation primed by engineers is fully carried out.
- Assembly, for checking whether the process of the assembly is compatible with documentation.
- Organization of the service, in order to check whether the product or the service is pleasant with recognized criteria.

The indicator used for determining right corrective action on the failure modes is RPN, formula of which is: RPN = Severity (S) × Occurrence (O) × Detection (D). Ranking levels of S, O and D result in a scale from 1 to 1000. After calculating RPN by engineering teams it is easy to identify the areas of greatest problem. Then the focus shifts to the solution of failure modes (McDermott, Mikulak, & Beauregard, 2017).

The good of FMEA is that can be used in all phases of the system lifecycle from requirement specification to design, implementation, operation and maintenance (Stamatis, 2003). Major benefit from FMEA can be achieved at the early design phases because the weakest point in the structure of the system can be revealed and addressed prior doing expensive design changes in later phases. As it is shown in fig. 2 (Vijayalakshm, 2014), the process of FMEA starts from the identification of scope of the system and its functions. The technique of brainstorming can be a useful method for finding failure modes. Later, the effects and the causes of potential failures are determined. Risk analyses is done after detecting these possible causes and effect. Final phase consists on documenting the process and taking actions to reduce the risks.

Fig 1: Phases of FMEA



Source: (Vijayalakshm, 2014)

Marques analysed FMEA with specific emphasize on hardware (Marques, 2010). RPN was found for different kind of hardware and failure was found on phone shell. The result showed that top priority should be given to this failure by manufactures when designing a smartphone. Two other researchers were focused on the weakest point of a mobile device on design stage by using ANSA and LS_DYNA (Liu & Li, 2011). The tests consisted on dropping from 1m height a mobile phone on a granite floor and did face drop, corner drop and edge drop. It was found that the impact of stress increase in cover glass and other glass layers. They found the shock absorbing pad which is attached to the camera is reducing the impact load on lens of the cameras.

According to analyses of performance of mobile devices terminals from Tay, R et.al by using FMEA, was found the Radio Frequency (RF) performance using SEMCAD X software (Tay, Chavannes, Futter, G.II, & Kuster, 2006). The authors state that effects of component changes, metallic coating, materials parameters and interconnections are affecting the performance of Radio Frequency distribution. They concluded that in order to receive the proper expectation of the device is very important the knowledge on the performance reliability. Cinque et.al (Cinque, Cotroneo , Zbigniew , & Iyer, 2007) in an article about the failure data analyses on Symbian OS, analysed the software failures such as freeze, self-shutdown, unstable behaviour, output failure and input failure. Failure data were collected from 25 phones in 14 months. It was found that major problems are coming because of the memory access violation errors and heap management. Moreover, in 2011, Cinque, studied enabling online dependability assessment of Android smartphone (Cinque, Cotroneo , Zbigniew , & Iyer, 2007) . The logging platform for the collection of failure data was discussed.

Usually exist two types of failure in mobile devices. One is due to accident and another is due to malfunction of hardware or software and this failure is a matter of concern for all users. Vijayalakshmi studied the FMEA in Android OS (Vijayalakshm, 2014). According to his findings top priority should be given for hardware (devices' shell with the highest RPV number) while in software side the problem of self-shut down was most dangerous as can contribute to data loss or failure of OS.

3 FMEA in Mobile Devices

In this study, was applied focus group technique (Morgan, 1997) in order to determine most frequent mobile devices failures. As a result, six most frequent failure modes related to hardware and three most frequent software failure modes were emphasized. Later, the FMEA method was conducted based on the next steps.

Step1: Identification of potential failures and effect: The most problematic components that were found out in a mobile device are classified as follows:

Hardware Failure Modes: Touchscreen; Battery; Device Shell; Front-facing camera; Rarefacing camera; Microphones.

Software Failure Modes: Freeze; Self-shutdown; Output failure

Step 2: Determining severity: Severity (S) is a rating of the seriousness of the effect of a failure mode to the system, assembly, product, customer or government regulation (Stamatis, 2003). It is related to the Failure effect. Severity rates on a scale of 1 to 10 where 1 is the lowest and 10 is the highest. In the following table are showed typical FMEA severity ratings and their meanings:

Tab. 1: Severity rankings and meanings

Effect	Rank	Criteria
None	1	No effect
Very Slight	2	Customer not annoyed. Very slight effect on product or system performance
Slight	3	Customer slightly annoyed. Slight effect on product or system performance
Minor	4	Customer experience minor nuisance. Minor effect on product or system performance
Moderate	5	Customer experience some dissatisfactions. Moderate effect on product or system performance
Significant	6	Customer experiences discomfort. Product performance degraded but operable and safe
Major	7	Customer dissatisfied. Product performance severely affected but functional and safe. System impaired.
Extreme	8	Customer very dissatisfied. Product inoperable but safe. System inoperable.
Serious	9	Potential hazardous effect. Able to stop product without mishap - time depended failures. Compliance with government regulation is in jeopardy.
Hazardous	10	Hazardous effect. Safety related- sudden failure. Non-compliance with government regulation.

Source: (Stamatis, 2003)

Step 3: Estimating Occurrence: Occurrence (O) is a rating responding to cumulative numbers of failures that could occur over the design life of a system or component (Stamatis, 2003). Occurrence is related to the Failure Cause and CNF stands for Cumulative Number of Failures. In the table below are presented typical FMEA Occurrence ratings:

Tab. 2: FMEA Occurrence rankings and meanings

Effect	Rank	Criteria	CNF/100
Almost never	1	Failure unlikely. History of similar design shows no failures	<0.0058
Remote	2	Rare number of failures likely.	0.0068
Very slight	3	Very few failures likely.	0.063
Slight	4	Few failures likely.	0.46
Low	5	Occasional failures likely.	2.7
Medium	6	Medium number of failures likely.	12.4
Moderately high	7	Moderately high number of failures likely.	46
High	8	High number of failures likely.	134
Very High	9	Very high number of failures likely.	316
Almost certain	10	Failure almost certain to occur. History of many failures with previous or similar designs.	>316

Source: (Stamatis, 2003)

Step 4: Failure Detection: Detectability (D) is a rating of the ability of the proposed design control to detect a potential failure mode or occurrence (Stamatis, 2003). Detectability is related to Failure Control. The higher the value of D, the more likely the failure will not be detected. In the following table, the respective values of Detectability and their meanings are listed:

Tab. 3: FMEA Detectability rankings and meanings

Effect	Rank	Criteria
Almost certain	1	Proven detection methods available in conceptual design.
Very High	2	Has very high effectiveness.
High	3	Has high effectiveness.
Moderately High	4	Has moderately high effectiveness.
Medium	5	Has medium effectiveness.
Low	6	Has low effectiveness.
Slight	7	Has very low effectiveness.
Very Slight	8	Has lowest effectiveness in each applicable category.
Remote	9	Unproven or unreliable, or effectiveness is unknown.
Almost impossible	10	No technique is available or known, and/or none is planned.

Source: (Stamatis, 2003)

Step 5: Calculating Risk Priority Number: Risk Priority Number (RPN) is calculated based on the three above explained criteria:

1- The severity of the effect on user and mobile system itself.
2- How frequently the problem is likely to occur.
3- How easily the problem can be detected.

$$RPN = S * O * D \quad (1)$$

4 Results

At first, the FMEA form was filled by taking into account the above-mentioned steps. The potential causes of failure occurrence for each failure mode and effects have been determined by considering the influence they have on the component and the whole system of mobile device. To eliminate/reduce the potential causes of failures, recommended actions are given for each of the defined failure modes. The application of FMEA on hardware and software components on mobile devices is presented in the following table:

Tab. 4: Application of FMEA in Mobile Devices

No	Failure mode	Function	Potential Failure Mode	Effects	Potential Causes	Current Design / Process Control	Recommendations
HARDWARE							
1	**Touchscreen**	To interact with the user. It is a display that can recognize a touch to its surface area (works as an input), either with a finger or a stylus.	Unresponsive: stops responding to users' touchinputs.	Not able to execute actions.	Hardware fault: User's carelessness; Physical damage (broken screen); Damaged by frequent touch (dirt and grease); Software issue: Operation and system problems.	Tests and inspections	More supervision; Selection of more resistant material; Improve sensitiveness; Improve the quality design of apps that come from manufacturer - here should be taken in consider responsive design.
2	**Battery**	Provides energy and sustainability to the mobile device.	Not functional; Incapability of charging; Low durability; Overheating.	Dissatisfaction by the user; Durability of the battery too insufficient for a correct utilization of mobile device; Constant shut down; Explosion risk.	No proper batteries type; negligent utilization by user.	Tests and inspections	Continuous work on making chips and Operating Systems more efficient to save power; Manufacturer should think seriously about replacement of lithium batteries with more effective ones.

3	**Device Shell**	Covers and protects the internal elements of device	Easily damaged after falling	Dissatisfaction by the user; Over the time, device becomes more exposed and can be more damaged.	User's negligence; Low material quality; Manufacturing design errors	Tests and inspections	More supervision; Selection of appropriate and more resistant material.
4	**Frontfacing camera**	Taking selfies	Not working	User get dissatisfied and annoyed.	Application issue	Tests and inspections	More supervision; Improving default camera app.
5	**Rarefacing camera**	Taking pictures	Not working	Users get very dissatisfied.	Application issue	Tests and inspections	More supervision; Improving default camera app.
6	**Microphones**	Transmitting user's voice over a digital network to the other person on the phone. Voice in voice and video recording; Taking voice as an input in dictation, voice commands, voice assistants, music recognition apps.	Static audio output; Noisy background during phone calls; Audio cut offs; Distant sound; Not working at all.		Software malfunctions: software bugs or system glitches; files and apps get corrupted; wrong configuration of audio settings; third party accessories. or Hardware damage: when the physical microphone component gets damaged and stops working. Hardware damage can be due to physical or liquid damage.	Tests and inspections	More supervision; Improving the quality.
SOFTWARE							
7	**Freeze**		Malfunction	Unable to operate the required function; Inappropriate output.	Due to the increase on operations; insufficient memory capacity; less software quality.	Tests and inspections	Selection of proper and reliable software; more supervision

8	**Selfshutdown**		Sudden or frequent shut down accidently	Inconvenience for the user; Problems for various hardware and malfunctions of software	Poor battery; Software problem; or Memory access violation error.	Tests and inspections	Batteries should be checked; more supervision.
9	**Output failure**		No output after giving input	Inconvenience for the user; malfunction	Hardware problem because of the touchscreen or software issue.	Tests and inspections	More cautiousness from manufacturer side; more supervision.

In accordance with FMEA steps, values of Severity, Occurrence and Detectability have been estimated and RPN is then calculated. Tab. 5 indicates the findings:

Tab. 5: Collection of evaluated S, O, D and RPNs values

COMPONENT	S	O	D	RPN
Touchscreen	9	6	3	162
Battery	9	7	4	252
Shell	4	8	4	128
Front-facing camera	4	2	8	64
Rare-facing camera	3	2	7	42
Microphones	5	6	3	90
Freeze	8	6	5	240
Self-shutdown	8	5	4	160
Output failure	7	4	5	140

According to the details and results from FMEA method, the RPNs values were analysed to get into conclusions. The results highlight that the critical failures on battery (RPN=252) followed by mobile device freeze (RPN=240) show that they should be the ones with high priority. Their severity values are high as well and they pose a high risk. Severity criteria should be prioritised as it is related to failure effects in the whole system. Thus, touchscreen and selfshutdown components have to be considered as well. Authors suggest that when conducting FMEA it is very important to understand and decide which failure modes are more significant than others by extending this method with an additional weighting factor (Ványi & Pokorádi, 2018).

Moreover, by considering the potential causes, many of them are closely related to users' practices and behaviours in mobile devices. Digital habits of users and their unconsciousness about potential online threats pose a high risk in mobile device systems (Holicza & Kadena, 2018). As the human error is inevitable, two options can be seen. One is related with the acceptance of the current level of harm and the other one is to start viewing the current failures as a result of the present conditions of the system. Putting continuously effort on training, education and programs about users' awareness is a good measure but still it does not promise the wanted results (Tick & Tick, 2013).

5 Conclusion

In this paper were presented risks associated with the usage of mobile devices. Later, FMEA Risk Matrix Methodology was applied in mobile device systems and nine failure modes were considered. The RPNs results revealed that a failure on battery, followed by freeze of mobile device are the ones with high priority. On the other hand, touchscreen and self-shutdown failures have also high severity and even though their RPNs are not the highest, they should be considered with high priority as well.

In addition, an extension of FMEA method that takes into account weighting factors, should be considered for future work. Moreover, considerable attention should be paid to human errors in mobile device and more concentration on human-centred design is needed by taking into account needs, capabilities and behaviours of people. Therefore, on the extension of FMEA, considerable attention must be paid to human errors. Putting more effort and focus on the design of elements in mobile device systems would be a good attempt to reduce and (or) eliminate the potential failure effects.

Resources

Beatty, P. C., & Beatty, S. F. (2004). Anaesthetists' intentions to violate safety guidelines. *Anaesthesia, 59*(6), 528-540. doi:10.1111/j.1365-2044.2004.03741.x

Carlson, C. S. (2012). Chapter 3: Understanding the Fundamental Definitions and Concepts of FMEAs. In *Effective FMEAs: Achieving safe, reliable, and economical products and processes using failure mode and effects analysis* (pp. 21-55). Hoboken, N.Y: Wiley.

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012). Measuring user confidence in smartphone security and privacy. *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12,* 1-16. doi:10.1145/2335356.2335358

Cinque, M., Cotroneo, D., Kalbarczyk, Z., & Iyer, R. K. (2007). How Do Mobile Phones Fail? A Failure Data Analysis of Symbian OS Smart Phones. *37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07),* 585-594. doi:10.1109/dsn.2007.54

Dudek-Burlikowska, M. (2017). Monitoring of the Production Processing in a Metallurgical Company Using FMEA Method. *Archives of Metallurgy and Materials, 62*(4), 2089-2094. doi:10.1515/amm-2017-0309

Good, N., Dhamija, R., Grossklags, J., Thaw, D., Aronowitz, S., Mulligan, D., & Konstan, J. (2005). Stopping spyware at the gate. *Proceedings of the 2005 Symposium on Usable Privacy and Security - SOUPS '05,* 43-52. doi:10.1145/1073001.1073006

Holicza, P., & Kadena, E. (2018). Smart and Secure? Millennials on Mobile Devices. *Interdisciplinary Description of Complex Systems, 16*(3), 376-383. doi:10.7906/indecs.16.3.10

Humphreys, E. (2007). *Implementing the ISO/IEC 27001 information security management system standard*. Boston: Artech House.

Johnson, K., & Khan, M. (2003). A study into the use of the process failure mode and effects analysis (PFMEA) in the automotive industry in the UK. *Journal of Materials Processing Technology, 139*(1-3), 348-356. doi:10.1016/s0924-0136(03)00542-9

Liu, W., & Li, H. (2011). IMPACT ANALYSIS OF A CELLULAR PHONE. Retrieved 2018, from https://pdfs.semanticscholar.org/5c6f/614a6f958fdf6cad965eb0c92714e4eb3931.pdf?_ga=2.27565500.1496686248.1598012123-1719538615.1574936450

Mamiit, A. (2017, March 13). New Android Smartphones Found To Be Already Infected By Malware: Are You At Risk? Retrieved August 21, 2020, from http://www.techtimes.com/articles/201326/20170312/new-android-smartphones-found-to-be-already-infected-by-malware-are-you-at-risk.htm

Marques, L. M. (2010, May 26). *FMEA – Mobile Phone*. Lecture presented in University of Ljubjana, Faculty of Computer and Information Science, Ljubljana.

Maxion, R. A., & Reeder, R. W. (2005). Improving user-interface dependability through mitigation of human error. *International Journal of Human-Computer Studies, 63*(1-2), 25-50. doi:10.1016/j.ijhcs.2005.04.009

McDermott, R. E., Mikulak, R. J., & Beauregard, M. R. (2017). *The basics of FMEA*. New York, New York: Productivity Press.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia - Social and Behavioral Sciences, 147*, 424-428. doi:10.1016/j.sbspro.2014.07.133

Morgan, D. L. (1997). *Focus groups as qualitative research* (Second ed.). Thousand Oaks: Sage Publications. doi:https://dx.doi.org/10.4135/9781412984287

Norman, D. A. (2013). *The design of everyday things*. New York, NY: Basic Books.

PCMagStaff. (2011, February 8). Smartphone Shipments Surpass PCs for First Time. What's Next? Retrieved August 21, 2020, from https://www.pcmag.com/archive/smartphone-shipments-surpass-pcs-for-first-time-whats-next-260337

Qian, Y., Fang, Y., & Gonzalez, J. J. (2012). Managing information security risks during new technology adoption. *Computers & Security, 31*(8), 859-869. doi:10.1016/j.cose.2012.09.001

Schmidt, P., Pittner, J., & Krauspe, K. (2019). Apple iCloud security and data theft. *Trends and Innovation in E-Business, Education and Security: Proceedings, 4(1)*, (pp. 60-67).

Stamatis, D. H. (2003). *Failure mode effect analysis: FMEA from theory to execution*. Milwaukee, Wisc.: ASQC Quality Press.

Tay, R., Chavannes, N., & Futter, P. (2006). Failure Modes and Effects Analysis (FMEA) on the RF Performance of Mobile Device Terminals. In *Proc. EUCAP, Nice*. Retrieved

2018, from https://www.semanticscholar.org/paper/Failure-Modes-and-Effects-Analysis-(FMEA)-on-the-RF-Tay-Chavannes/e95c5bd0506fbd2d6cac9f11722d863b137d9ee6

Theoharidou, M., Mylonas, A., & Gritzalis, D. (2012). A Risk Assessment Method for Smartphones. *IFIP Advances in Information and Communication Technology Information Security and Privacy Research,* 443-456. doi:10.1007/978-3-642-30436-1_36

Tick, J., & Tick, A. (2013). Business process modeling — Simulation of administrative activities. *2013 IEEE 9th International Conference on Computational Cybernetics (ICCC),* 345-348. doi:10.1109/icccyb.2013.6617616

Ványi, G., & Pokorádi, L. (2018). Sensitivity analysis of FMEA as possible ranking method in risk prioritization. *U.P.B. Scientific Bulletin. Series D: Mechanical Engineering, 80*(3), 165-176.

Vijayalakshmi, K., Dr. (2014). Analysis of Android OS Smart Phones Using Failure Mode and Effect Analysis. *International Journal of Latest Trends in Engineering and Technology (IJLTET), 4*(4), 11-18. Retrieved June, 2018, from https://www.ijltet.org/wp-content/uploads/2014/11/2.pdf

Šrekl, J., & Podbregar, A. (2014). Enhancing Safety Information Systems With The Use Iso/iec 27000. *Safety Engineering, 4*(1). doi:10.7562/se2014.4.01.03

PASSWORD SELECTING HABITS

Esmeralda Kadena[30]

Abstract
In the information age we live in, every person is split into entities: the real & material part and the part of data and/or information that are stored in databases and servers on the internet. The connection between the two parts is realized by accounts and authentication, which are presumed to be secret. Nowadays every person has a lot of accounts, a webmail, a profile on a social network or an online banking account, etc. All of these accounts perform user authentication by entering passwords. Password safety is essential for protecting personal information, bank details virtual identities as well.

Passwords have been the target of much criticism. For many users, it is simpler to choose passwords that can easily be guessed by attackers. Every day an enterprise employee uses multiple passwords in order to use all applications and systems provided by his employer. Enterprises spend significant resources to deploy authentication mechanisms and policies, which are then compromised due to password leaks or abuse. On the other hand, attackers have automated software that can guess typical passwords with success.

The aim of this paper is to investigate the password selecting and using habits of university students, to see whether they apply the correct theoretical knowledge correctly – or not quite.

Key words
Passwords, Attacks, Users, Habits.

1 Introduction

The password cracking act has been closely connected to the field of Information Security because passwords were the first means of keeping data safe and restricting access to it (O'Gorman, 2003). Nowadays passwords are still commonly used and stay the most standard way of adding security to private information. Therefore, there is a wide-ranging of passwords attacks.

Passwords are one of the methods of authentication. Authentication can be realized in many ways: based on knowledge, possession and biometric methods. Maybe selecting a correct and suitable authentication method is the most crucial decision to design secure systems mechanism. Authentication has developed gradually during the past years but there is still no way to completely avoid user complicity. The one which is based on something you know is password and the human factor is usually responsible for the choice of an insecure or foreseeable password both on user and system administrator side. Encryption algorithms are usually widely tested and those that are used have been proven to be secure. Because of this, an attacker will almost always attempt to attack the predictability to the human factor and not trying to break the encryption.

Due to the current increase in incidents involving public expose of personal information (including here passwords), it is now easier to gather extremely accurate statistical information to identify most used passwords and the reasons that lead of the selection of those passwords. It was of interest to investigate the level of information about this field. Therefore, a study was conducted among university students in Albania. Research questions:

[30] Óbuda University, Doctoral School on Safety and Security Sciences, Budapest (Hungary)
kadena.esmeralda@phd.uni-obuda.hu

- How the university students select passwords?
- Do they apply the correct theoretical knowledge correctly?

2 Methodology

To investigate the password selecting and using habits, a survey about user behavior on password selecting was used. It conducted a brief self-administered demographics questions that collected basic information including gender, age, study level, place of residence, father's and mother's highest educational degree, and if they owned a laptop and a mobile smart device with a network connection (smartphone, tablet). It was mostly intended to give a better understanding of the respondent included in the study.

The questionnaire was developed around the idea of exploring the user's password habits and knowledge. Through this questionnaire, the participants were asked about password usage and habits, including questions about how many hours they spent on internet in the school day and during the weekends, the most important accounts they had, whether they reused passwords about these important accounts, and how they kept track of their passwords for these important accounts. The other set of questions asked about the average length of passwords for their important accounts and what kind of characters were included in their passwords in these accounts. No question to participants was about what their passwords were. The participants in this study were conducted from Albania and all of them were students.

The questionnaire was chosen to encourage students to easily answer about the ways in which they approach the task of password selecting and management. That's why the questionnaire was focused around topics of interest to study; to investigate the way in which they choose passwords, why they make their decisions and to see whether they apply the correct theoretical knowledge correctly. The quantitative collected data helped in evaluation because it provides quantifiable and easy to understand results.

3 Background and Reviewing Literature

Nowadays there are several studies about password habits and user knowledge on password selecting. According to this, a survey from CSID in collaboration with Research Now in 2012 was made among American users (CSID & Research Now, 2012). According to their findings, 61% of them reuse passwords among multiple websites; 54% of users have only five passwords or less; 44% change passwords only once a year; 89% of them feel secure with their password management and use habits and 21% had an online account compromised. Another study shows that students in higher and further education are aware of the importance of cybersecurity, with 77% said that it as a growing threat but only 35% think it is their obligation to learn about cybersecurity, and less than 20% say they are concerned about it (McDonald, 2016). While 90% of them were more interested in their marks than cybersecurity field. Only 35% did not know what security was available on university computers. 24% of students think that university network is more secure than their home network. But 16% have had their personal details hacked online, while 4% have experienced a hack on their college/university emails. It is clear that more efforts need to be done to educate students about security, responsibility and why not how can they help to reduce threats of cybersecurity at their institutions?

In the fifth annual "Worst Passwords List" of SplashData about password habits of Internet users, people are putting themselves at risk continuously (TeamsID, 2016). The most used passwords from 2011 to now remained "123456" and "password. It is clear that the way in which people select passwords remain continuously at risk. Although this it is shown from the study that, CEO of SplashData Morgan Slain said: "We have seen an effort by many people to be more secure by adding characters to passwords, but if these longer passwords are based on simple patterns they will put you in just as much risk of having your identity stolen by hackers".

Consequently, from the user point of view, the question is: What should we take into consideration to create a strong and secure password that we can keep in mind as well?

In 2014 a data breach affected the Internet Corporation for Assigned Names and Numbers (ICANN). Some unknown attackers used spear-phishing and had access to some of the organization's systems. They use this campaign to a sensitive group system operated by ICANN and sent spoofed emails to members of staff. The staff entered their usernames and passwords with the keys to email accounts. The hackers then accessed several systems within ICANN: The wiki pages of the Governmental Advisory Committee (GAC), Centralized Zone Data System (CZDS), the domain registration Whois portal, and also the blog. It was reported that passwords couldn't be hacked because they were cryptographic hashes but anyway the corporation advised the users to change their passwords (Khandelwal, 2014).

Also, in 2014, a hacker with nickname Kuroi SH hacked certain domains of the United States, based Uniformed Services University (USU). He also leaked login credentials online (Waqas, 2015). The problems for USU: 1) Plain-text passwords which can be further used for phishing scams and/or for hacking the social media accounts, but only in case the same email and passwords. 2) The mirrors of all targeted websites are on hold on Zone-h, once accepted it will be impossible for the university to hide the leaked data from the eyes of the public. Another case is the "1.2 Billion Shades of Grey". It was reported that FBI linked a hacker known as Mr. Grey to 1.2 billion stolen credentials and 500 million email addresses for websites like Facebook and Twitter (Raymond, 2015). It found posts by "Mr. Grey" who wrote in November 2011 that he could locate the records, if anyone wanted information about user's account on Facebook, Twitter and a Russian Social network VK. Hold Security's chief information security officer (Alex Holden), who reported to Reuters, showed that the hacker had access to a database and stolen data via malware and viruses (botnets) looking for SQL injection flaws.

In information security, confidentiality is a key element. User authentication is the main mechanism to obtain this (Parker, 1991). There are two different stages in which authentication procedures have traditionally been divided. The first is User identification (User ID) that identifies the user interacting with the system and as it simply specifies who the user is, this id does not have to be secured. The second stage is user authentication; when a user tries to access a resource, he/she has to be checked from the authorization process as the legitimate user to use that resource. Usually, the system administrator is responsible for defining permissions in the access control list form, for each resource. There are several authentication technologies available in the market over the years (Duncan, 2001). To understand them, everyone should be familiar with the standard authentication factors such as something you know, something you have, something you are and how each technology contributes to giving strong authentication capabilities.

4 Passwords

The most common examples of authentication: using a username and password (something you know). Firstly, passwords were system-generated to guarantee users employed "secure" combinations of characters. For some users they cannot be remembered and therefore they write them down. What is more, security risks were identified in the distribution of system generated passwords. Both of these reasons have brought to user-generated passwords as the most commonly used process for password creation.

Types of attacks on passwords: Password cracking is the process of either guessing or recovering a password from stored locations or from a data transmission system (Shankdhar, 2018). Security analysts and experts suggest different approaches when it comes to password cracking (Weir, Aggarwal, Medeiros, & Glodek, 2009). Attack selection depends on the hashing algorithm used and the speed of the hash calculation. To evaluate the efficiency of password recovery methods we can base on:

- The time that will take for the attack to try one password. Based on password policies, usually, passwords have an expiry date, as a result, will not be considered an attack that takes too much time.
- Which is the number of resources that the attacker has? In the cases of organized crime and industrial espionage, the attacker might have the facility to use multiple processors, data canters, or botnets for the attack. This reduces the needed time for an attack and might result in making another attack that was thought impossible.
- The success probability of the specific attack or approach.

Whether the attacker wants to crack one password, or a group of passwords must be taken into account. If the attacker has one password, then the goal is to crack it within a reasonable amount of time. If the attacker has many passwords then the goal might be to crack any of the passwords, a substantial amount of the passwords, or as many passwords as he can within a reasonable amount of time and given the resources he has. In order to accomplish the best possible result, it is essential to make the attack as targeted as possible for a better success rate within the available time. The main categories of password cracking techniques are online and offline attacks.

Online attacks: are attacks that are performed on a live host or system by either using an exhaustive search (brute-force) or wordlist attack against a session, login form, or any type of authentication technique used. Online attacks are not as popular as offline attacks because they are often not possible. Various protection mechanisms like Captcha images and maximum unsuccessful authentication attempts are employed that made the online attacks difficult and dangerous to realize. Usually, few very common or probable passwords can be tried online but sometimes that may be enough for a successful attack. Sometimes, it is still possible to launch online attacks if the security measures above can be avoided, there is enough bandwidth to perform the attack, and other contributing factors make it possible such as IDS evasion. An example of a tool that can be used for an online attack is Hydra (Lee, 2015). Hydra is a network login cracker that supports several online services, for example: POP3, HTTP, LDAP, IMAP etc.

Offline attacks: can be executed without the need to interact with the victim host and they can be performed on hashed passwords at a different location. This is done by extracting the hash (or hashes) stored by the victim and attempting to crack them or a special rig or remote machine. This can be done without alerting the target host. This type of attack is quite popular because they are easier to realize and are often possible due to various vulnerabilities in the victim's infrastructure. Offline attacks can be further distinguished depending on the type of resources that are needed to execute the attack. In specific, there are CPU based attacks and GPU based attacks that can be used in combination with pre-computed hash tables (rainbow tables), dictionaries, or brute-force techniques. Additionally, other attack types exist such as a simple Google search or combinations of attacks mentioned. Depending on any additional information and/or suppositions the attacker may have they can optimize their attack. The main cracking techniques are represented as below (Cross & Shnider, 2008).

4.1 Deffault passwords

Several system administrators leave their devices and applications with default usernames and passwords combinations. In this way, an attacker can break into the network and then easily can gain access. The reasons for doing so are the lack of knowledge or the "laziness" of system administrators that a password must be changed or supposing that their perimeter firewall will protect from unauthorized access. Thinking that the first thing an attacker will do is to try the most used passwords (i.e.: 1111, letmein, qwerty, hello, 123456, etc.), definitely, this practice is not a good idea. Which is more, some worms are configured to automatically search for

systems with a default username and password. This is realized by running a vulnerability scanner on your network which can identify systems and services using default passwords. Just now, at our Óbuda University, a new service was introduced to inform employees online about their salary and tax deductions. The default password is 123456, and the site does not force users to change the default password at their first login.

Some software, systems, and services that commonly use default passwords (US-Cert CISA, 2016):

- Routers, access points, switches, firewalls, and other types of equipment
- Web applications
- Databases
- Industrial Control Systems (ICS) systems
- Administrative web interfaces
- Other embedded systems and devices

Guessing based on the connection between the password and the user(name) (Keszthelyi, 2013)*:* The predictability of the user is the password crackers best friend. It is a fact that our brain is emotionally attached to things related to our interests, such as animals, hobbies, family or even conversations on social networks and so on. Regarding this, there are large chances for password crackers to look at this information and make some guesses when trying to crack a password without referring to dictionary or brute force attacks. For example, they can take in consider the relationship between the password and the date of birth of a person, login name as strings or derivation from the name (myname1), login name as logical (Ronaldo -- CR7), phone number, pet name, etc., and that's enough.

Using these kinds of passwords is fatal. Some of them may be used even in an online attack and they need no more than a few extra time. In 2010 a Frenchman was convicted by successfully hacking into accounts of president Obama, singers Britney Spears and Lilly Allen by this method (Mesquita, 2010).

4.2 Dictionary attack

As the dictionaries are raw text files, they consist of one word/phrase per line where each line is a candidate match in which each hash is computed and compared to the hashes to be recovered. A Dictionary contains a list of possible matches rather than all possible string combinations (the difference between brute force attacks). As it contains a limited number of words (compared to brute force), a dictionary attack needs just a little time. It needs to be well optimized for example it should contain the most probable passwords for the given situation. And at this point attacker must suppose the language. Frequently they contain known and popular passwords, words from the English and/or other languages, ID numbers, phone numbers, phrases from books etc.

Considering a system that runs normally, a simple dictionary attack cannot be used online. That's because of the time delay between the failed login attempts and too many attempts will cause a security alert for the administrator of the system. Who thinks that grouping words together such as 'beyourself' or 'superadminguy' will prevent your password from being cracked is wrong? It can be cracked but it needs a few extra seconds.

c. Brute force attack

This technique seems to be similar to the dictionary attack, but it has an extra bonus, for the hacker, of being able to identify words that are not in the dictionary. It consists of working through all probable alpha-numeric combinations from aaa1 to zzz10. The cracking time depends on the speed of the computer and how complex is the password. In theory, a complete brute-force attack that tries out all the possible character combinations can guarantee a 100%

success rate. However, when attempting a brute-force attack on passwords longer than 10 characters the time needed to perform it becomes unrealizable. You can see below Gosney case. Brute force attacks can be shortened by throwing more computing horsepower in terms of both processing power - including using the power of your video card GPU - and machine numbers, such as the use of distributed computing models and zombie botnets.

At the end of 2012 Jeremi Gosney demonstrated the unbelievable cracking speed of a special hardware-software platform he had developed. It consisted of five servers containing 25 AMD Radeon GPUs and communicating to each other at 10 Gbps. On NTLM hashes he could reach a 348 billion tries/sec cracking speed and it means that a 14-character long Windows XP password could have been cracked in not more than six minutes (Roberts, 2017). Gosney indicated that his system was scalable up to 128 GPUs but, unfortunately, he had no more financial background than what was enough for that 25 GPUs.

Supposing this cracking speed rounded up a little to 1012 tries/sec we get these results (number of possible char combinations are charsetlength, combinations/speed=cracking time):

Tab. 1: Password's cracking time

Char set	Length	Cracking time (rounded)
80	8	28 min
100	8	2.7 hours
80	10	124 days
80	16	10^{11} years

These results show us the very big difference between polynomial functions (xa) and exponential functions (ax). In other words: the length of a password is significantly more important factor from the point of view of security than the character types it consists of (Keszthelyi & Kadena, 2016).

d. Advanced dictionary attack

Hybrid dictionary attack: A hybrid dictionary attack is a combination of a brute-force attack and a dictionary attack. A hybrid dictionary attack takes a dictionary as input and appends brute-forced strings to each entry of the dictionary. Therefore, for each string in the dictionary, this attack produces several other strings such that a dictionary entry

“apple” produces “111apple”, “112apple” up to “999apple” for a brute-force that pre-pends three numbers to each entry. A hybrid dictionary attack results in a polynomial increasing amount of computation and time based on the amount of characters to be concatenated with the dictionary entries.

Rule-based dictionary attack: A rule-based dictionary attack is similar to a hybrid dictionary attack with the difference that instead of appending a string in all its possible combinations, the rule-based dictionary attack uses rules to transform each dictionary entry or concatenated it with commonly used prefixes and postfixes. The difference is whether you put the appended strings into the dictionary, or the cracking program generates them online – I think there will be no measurable difference between the two methods in cracking time. In any kind of dictionary, attacks you use a simple and short dictionary (short at least comparing it to the brute force).

Phishing: This is an easy way: Ask the user for his/her password. A phishing email leads the unsuspecting reader to a faked online website, payment, social network, etc. in order to login

and put right some terrible problem with their security. Why bother going to the trouble of cracking the password when the user will happily give it to you anyway?

e. Social Engineering

This technique is based on the "ask the user" concept. It takes this concept outside of the inbox that phishing tends to stick with and into the real world " (Anderson, 2008). A favorite of the social engineer is to phone a business office pretending to be as an IT security tech guy and ask for the password of network access. You'd be amazed how often this works (Krombholz, Hobel, Huber, & Weippl, 2015). Some of them take the "risk" to wear a suit and name badge before going into a business to ask the receptionist for the same question face to face.

A young guy who was claimed to have successfully attacked the private mailbox of John Brennan director of the Central Intelligence Agency in last October told the press that "he was a high school student, claimed that he social engineered a customer service agent into giving up access to Brennan's AOL account" (Farivar, 2015).

f. Malware

Malware can install a key logger or screen scraper and it can record everything that user type or it can take screenshots during a login process (Felt, Finifter, Chin, Hanna, & Wagner, 2011). Then it forwards a copy of this file to hacker central. Some malwares look for the existence of a web browser client password file and copy this which, unless properly

encrypted, will contain easily accessible saved passwords from the user's browsing history. Other roundabouts may also occur, such as a hidden camera in the ceiling, but these kinds of roundabouts have nothing to do with the quality of the passwords, naturally.

Nowadays there are several options that are thought to offer more protection, particularly when have to do with important data. Smart Cards, Tokens, Biometrics, etc. are some of them.

5 Results of the study

There were 93 participants for the study, and all were students from the university community. There was no exception about the type of university or study program, so both public and private and any kind of their field of studies were taken in consideration.

General data collected:

- 64.5% (60 students) of respondents study at European University of Tirana while 25.5% were from other Universities.
- 35.5 % of them (33 students) were males and 65.5% females (60 students).
- 72% live in Capital City, whereas 7.5% in a big city, 11.8% in a city, 3.2% in a small city and the rest (3.2%-3students) in a village. • 90 of them owned a computer/laptop while only 3 students didn't.
- Also 90 (96.7%) of them had a mobile smart device with the network connection (smartphone, tablet) and only 3 (3.3%) hadn't.
- 64.5% were interested in science and the rest in humanities.

Students Habits: Because of a significant scale of spending time on the internet during the school day and weekends it is faced, most of them every day are exposed to the risks on the internet. About 38.7% of them are active 2-5 hours on the internet on an average school day and only 15.1% spend less than an hour. While this number is higher on weekends and holidays on long hours, where 45.2% are active 2-5 hours, 33% more than 5hours and only 6.5% (6students) less than an hour.

Maybe is just interest the above-mentioned percentage regarding their interest (humanities or science). But according to their field of study, actually most of them are enrolled in IT studies or similar. Which it means that maybe they have the knowledge but do not apply it. ECDL exam is not too common in Albania. “Most of them asked me directly, what does it mean?” and results that only 19 students had one.

The questionnaire contained a question about the importance of some systems such as: Facebook, Google Drive, Email account, School Information System, Intavideo, Twitter, Vimeo, Ustream, Spotify, Tumblr, MySpace, iTunes, Snapchat, Foursquare, Blogspot.com, Hotdog, Meetup, Miutcánk, Waze.

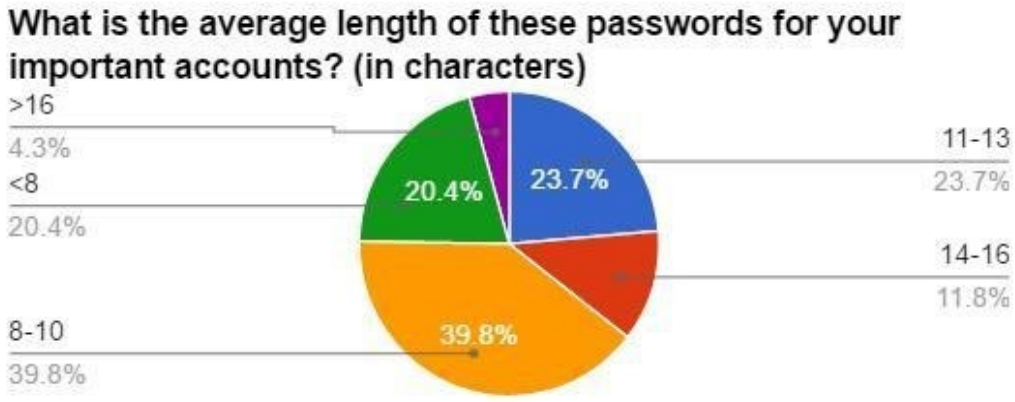
For most respondents (64.5%) their email account is the most important system. It is followed by the school information system (41.9%), YouTube (28%), Google Drive (22.6%) and Facebook (9.7%) that actually means quite a low significance. Most of them have given an importance 2 (28%) and 3 (27%) (from 1 to 5 scale) to Facebook what is interesting. While some systems were unknown for this country and that’s why they had the lowest importance. Twitter, of course is not included in this group but surprisingly it has also insignificant importance which led to poor usage from Albanian students (82% don’t use it).

Password Creation: As you can see from the following charts, students were asked about the length and characters of passwords of their important accounts. It is not clear if they meet the requirements of some systems in password creation or they really apply their knowledge. Results show that most students use passwords that contain mixed char types.

The length as the most important factor in creating a password can indicate how good it is. In this case, the large length (>16) present the lowest percentage which means only 4 students. On the other hand, the most frequent length is 8-10 characters (37 students) followed by 11-13 characters (22students).

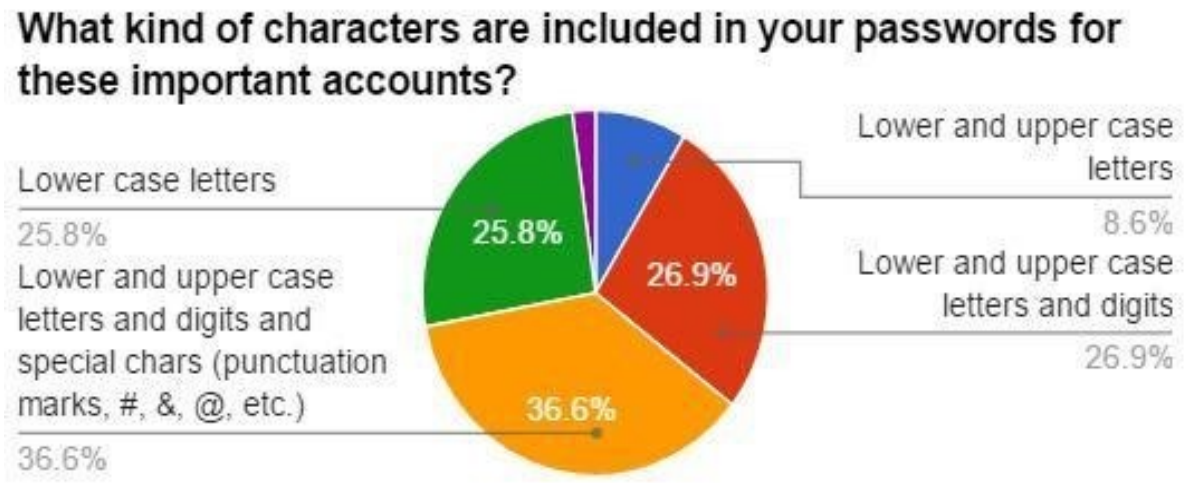
Supposing the cracking speed of 1012 tries/sec on the basis of Gosney's experiment 16 char long passwords are secure enough (8.93*1010 year for brute force, approximately the age of our universe) while 8-10 char long ones are considered to be problematic (half an hour – four months) and 11-13 char long passwords may be problematic (27-17,000 years) may be considered as possibly problematic.

Fig. 1: The average length of passwords for their important accounts



As we can see in fig.2, most of them include in their passwords lower, upper cases, digits and special punctuation marks. This shows that for them, a secure password (because we are talking about important accounts), must contain these characters. Which is not true, because security depends more on length than on characters. This result is significant to think that exist a lack of knowledge.

Fig. 2: Types of characters included in their passwords



Password Management and Security: Fig. 3, demonstrates the frequency in changing passwords for their important accounts.

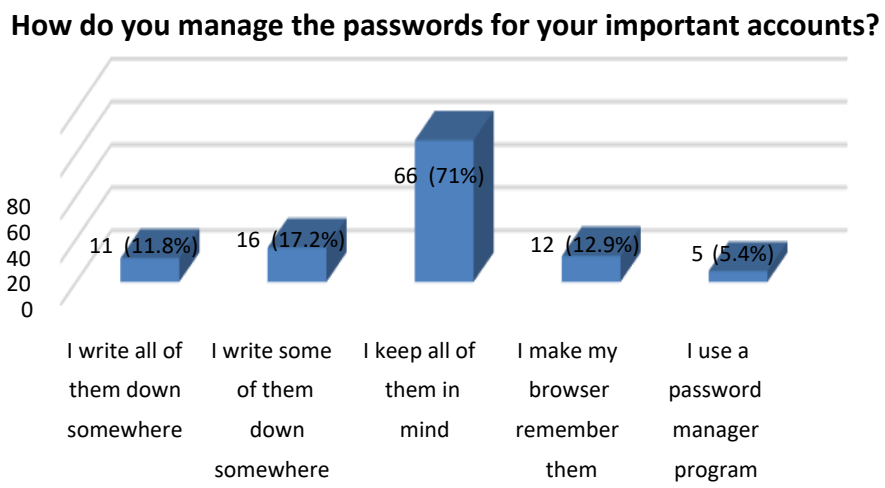
Fig. 3: The frequency of changing passwords

The reasons for changing passwords (frequent answers): "When someone might have learnt/learns it"; "When someone learns this password"; "To have more security for my important files"; "To be secure"; "I change just the school's email , because I have to once a year"; "For fun"; Because some other people try to login in my account"; etc. So, it seems that some of them have the intention (Tick, 2011).

The reasons for not changing passwords: "Why to?!"; "Why I need?"; "Too troublesome"; "Too lazy, Usually make a change only if I have to.."; "It takes me a lot of time"; "No reason"; "Just habit"; "I think that is secured enough even without changing them repeatedly"; "I have never had problems before"; "I am not obsessed with security"; etc.

As it is shown some of them prefer laziness instead of security, I think that they aren't enough informed about the risks.

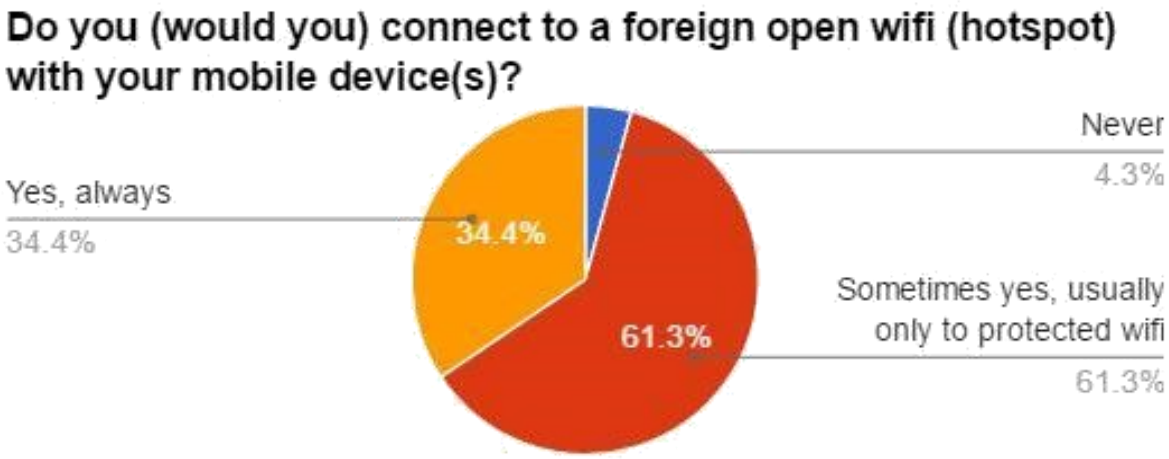
Fig. 4: Password management



The chart in fig. 4, illustrates the way that they manage passwords of their important accounts. As it is shown the critical point is the large part (71%) that keep all the passwords in their mind and only 5 of them use a password manager program. It is unclear if some of them really change the default passwords provided by the system administrator of SIS (it has only 2 years that is implemented in our university and some friends of mine keep in mind that password).

More than half of the students, (62.4%) approve that (would) log in into their important accounts from a foreign device such as a computer in a netcafé or in a library. Fig. 5 shows the results about connecting or not to a foreign open Wi-Fi with the mobile device. Approximately one-third should be more careful.

Fig. 5: Connecting to a foreign open Wi-Fi



6 Conclusion

This paper was based on the review of the literature and some latest news to give a wide background about the authentication types and most common risks related to passwords. As it was discussed, password breaches are gaining popularity and still exist problems in password selecting compared with times ago (Beke, Kovács, & Rajnai, 2019). The amount of our

important data stored in the computer are extremely increased. Thus, everyone must be careful in selecting passwords. It was shown that the type and mixture of characters are not the most important factor in creating passwords but the length. The survey about password selecting and users' habits on Albania has led to conclude that the password selecting and using habits of university students are better than expected, but far from being perfect.

This is a good basis to build up a security training to make them more conscious. We also may take into consideration the fact that the most important account is the mailbox and perhaps students have not very important stuff in their mailboxes. So, the value they could assign to their important accounts may be not too high. If this is the real situation it means that their security consciousness is better.

Resources

Anderson, R. J. (2008). *Security engineering: A guide to building dependable distributed systems* (2nd ed.). New York, NY: John Wiley & Sons.

Cross, M., & L. Shinder (2008). Chapter 11 - Passwords, Vulnerabilities, and Exploits. In *Scene of the cybercrime* (pp. 467-503). Burlington, MA: Syngress Publishing, Elsevier. doi:https://doi.org/10.1016/B978-1-59749-276-8.00011-X

CSID, & Research Now. (2012, September). *CONSUMER SURVEY: PASSWORD HABITS* (Rep.). Retrieved March, 2016, from CSID website: https://www.csid.com/wp-content/uploads/2012/09/CS_PasswordSurvey_FullReport_FINAL.pdf

Duncan, R. (2001). *An Overview of Different Authentication Methods and Protocols* (Working paper). Retrieved 2016, from SANS Institute website: https://www.sans.org/reading-room/whitepapers/authentication/overview-authentication-methods-protocols-118

Farivar, C. (2015, October 19). Hacker releases new purported personal data for top CIA, DHS officials [Updated]. Retrieved November, 2019, from http://arstechnica.com/tech-policy/2015/10/hacker-releases-new-purported-personal-data-for-top-cia-dhs-officials/

Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011). A survey of mobile malware in the wild. *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices - SPSM '11,* 3-14. doi:10.1145/2046614.2046618

Keszthelyi, A. (2013). About Passwords. *Acta Polytechnica Hungarica, 10*(6), 99-118. doi:10.12700/aph.10.06.2013.6.6

Keszthelyi, A., & Kadena, E. (2016). Misunderstanding how Passwords Work. In *Management, Enterprise and Benchmarking in the 21st Century* (Vol. III, pp. 83-92). Budapest, Hungary: Óbuda University, Keleti Faculty of Business and Management.

Khandelwal, S. (2014, December 18). Global Internet Authority ICANN Has Been Hacked. Retrieved March 21, 2016, from http://thehackernews.com/2014/12/ICANN-Hacked.html

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113-122. doi:10.1016/j.jisa.2014.09.005

Lee, S. (2015, December 29). Top 10 Password Cracking Tools. Retrieved February 17, 2020, from https://www.wondershare.com/password/password-cracker-tools.html

McDonald, C. (2016, March 18). Most students say cyber security is a growing threat. Retrieved March 29, 2016, from http://www.computerweekly.com/news/4500278781/Most-students-say-cyber-security-is-a-growing-threat?utm_medium=EM

Mesquita, R. (2010, June 25). Frenchman convicted for hacking Obama's Twitter. Retrieved March 20, 2016, from http://archive.boston.com/business/technology/articles/2010/06/25/frenchman_convicted_for_hacking_twitter/

O'gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE, 91*(12), 2021-2040. doi:10.1109/jproc.2003.819611

Parker, D. B. (1991). Restating the foundation of information security. *Computer Audit Update, 1991*(10), 2-15. doi:10.1016/0960-2593(91)90013-y

Raymond, N. (2015, November 24). FBI has lead in probe of 1.2 billion stolen Web credentials: Documents. Retrieved April 01, 2016, from http://www.reuters.com/article/us-usa-cyberattack-russia-idUSKBN0TD2YN20151124?feedType=RSS

Roberts, P. (2017, November 09). New 25 GPU Monster Devours Passwords In Seconds. Retrieved March 28, 2016, from http://securityledger.com/new-25-gpu-monster-devours-passwords-in-seconds/

Shandkhdhar, P. (2019, November 15). 10 Most Popular Password Cracking Tools [Updated for 2018]. Retrieved August 21, 2020, from https://resources.infosecinstitute.com/10-popular-password-cracking-tools/

TeamsID. (2016, January 19). Announcing Our Worst Passwords of 2015. Retrieved February 18, 2016, from https://www.teamsid.com/worst-passwords-2015/

Tick, A. (2011). A new direction in the learning processes, the road from eLearning to vLearning. *2011 6th IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI),* 359-362. doi:10.1109/saci.2011.5873029

US-Cert CISA. (2016, October 7). Alert (TA13-175A) Risks of Default Passwords on the Internet. Retrieved November 2, 2016, from https://us-cert.cisa.gov/ncas/alerts/TA13-175A

Waqas. (2015, October 12). Someone Hacked Uniformed Services University and Leaked Their Credentials Online. Retrieved March, 2016, from https://www.hackread.com/uniformed-services-university-domain-hacked/

Weir, M., Aggarwal, S., Medeiros, B. D., & Glodek, B. (2009). Password Cracking Using Probabilistic Context-Free Grammars. *2009 30th IEEE Symposium on Security and Privacy,* 391-405. doi:10.1109/sp.2009.8

VULNERABILITIES, IDENTIFICATION AND DETECTION OF UNMANNED AERIAL VEHICLES

Attila Máté Kovács[31], Zoltán Rajnai[32]

Abstract
Drones and other unmanned aerial vehicles (UAV) are widely developed and deployed for different applications ranging from agriculture monitoring, commercial aerial surveillance, disaster relief, package delivery and motion picture filming. The growing use of drones represents a threat to personal privacy as well as safety for the aviation and regulation authorities around the world. There is an increasing necessity to have external systems for UAVs to be detected and located. It is necessary to identify them because drones will soon become part of our daily lives.

Key words
unmanned aerial vehicle, UAV, drone, risk, aviation, flight, pilot, vulnerability, threat, attack, vector

1 Introduction

When a new technology emerges, new rules and technical arrangements are needed to facilitate and regularise the smooth running of this technology without disrupting people's lives. This is the case with UAV/drone technology. Unmanned aerial vehicles will soon fill cities and airspace will be occupied by drones, resulting in more air traffic. Thus, more sophisticated methods of detecting and identifying drones will be required.

With the growing need to regulate unmanned air traffic, a mechanism for all drone operators and manned aviation to be able coordinate with one another will be needed to ensure conflict resolution, approvals of flights, and compliance with local airspace boundaries.

Many organisations are testing beyond the line of sight and autonomous flight. This is a call to all regulators and aviation authorities to develop a comprehensive system for monitoring and tracking unmanned aerial vehicles.

The wide use of UAVs requires their accurate control and real-time monitoring. Cooperative UAVs are those which transmit their location themselves while non-cooperative UAVs need some kind of external system to be detected and located. It is necessary to identify them because drones are becoming part of our daily lives.

UAVs are currently used for a wide range of missions, for example, outskirts observation, surveillance, transportation and attacks. The administration of UAVs should be reliable, robotised and self-ruling.

Thus, political and military administrations have the expectation towards UAVs to protect national security via reconnaissance or even battle missions. In order to meet these expectations and succeed in these missions, UAVs must gather and process information extensively.
Because of the above factors, UAVs may also have to process and store a wide array of data, ranging from troop moves and developments to information on nature or environment and key tasks. The quantity and range of data covered lead to UAVs to become a particularly attractive target for secret activities and therefore make them susceptible to being stolen, controlled or attacked. An example of this is the loss of an RQ-170 Sentinel to Iranian military authorities on

[31] Óbudai University, Doctoral School for Safety and Security Sciences, kovacs.attilamate@phd.uni-obuda.hu
[32] Óbudai University, Doctoral School for Safety and Security Sciences, rajnai.zoltan@bgk.uni-obuda.hu

4 December 2011. This demonstrates that past attempts to recognise opportunities and strengthen UAVs have been lacking.

2 The importance of analyzing UAV vulnerabilities

Due to the increasing dependence on UAVs to ensure national security realized by administrative and military powers, it is inevitable to have a systematic, solid investigation of vulnerabilities is necessary.

Cyber conflicts often target civilian infrastructures or even military infrastructures or computer systems. The increasing level of improvement in present day tactics and strategies and the reliance on these specific tools require the assessment of the vulnerability of cutting edge military systems and assets to specialized assaults.

Meanwhile, previously predominately used by military administrations, UAVs are becoming progressively important for more common applications. UAVs may depend on in-built computers or be controlled remotely by pilots at ground stations. Various episodes relating to automatons have been reported on by the general media in the last seven years, which evidences and increases the public's enthusiasm for military and non-military personnel drone applications (Baldor, 2012).

It is both captivating and abnormal that more research is done into the security of present day vehicles uniting vehicle-to-vehicle and vehicle-to-framework correspondence than investigation into the security of UAVs. It is indistinct whether this is because of the shut source legislative issues coming about because of UAVs' military causes or whether these gadgets are essentially viewed as secure as a result of their one of a kind assignments.

Framework security ought to never be considered as a state, yet rather as a system. So as to help this technique, it is significant to be prepared to portray and survey the present security status. Besides, it is fascinating to have the choice of examining framework arrangements as respects security levels.

Knowing the vulnerabilities of a system is essential in determining how secure it is. In fact, the actual vulnerability of a system is the part that is most likely to break down as a result of certain events. Depending on the seriousness of the breakdown, ranging from the total loss of control or destruction of the system to minor errors, such vulnerability may pose a risk to the system's security. In other words, a risk is a conceivable event with a major impact on the system's security. An event may either be an attack or an occasion (Bishop, 2004).

As it concerns system security, a risk is a combination of the seriousness of the effect of an attack on the security systems, increased by the likelihood of the event. Subsequently, risk evaluation measures the conceivable severity and probability of attacks. It is a key incentive for any significant level security system (Jaquith, 2010).

Interestingly, attackers scanning for targets follow a similar path to system designers planning a protected system. An attacker scans for a system weakness implying a great danger or inferring a high risk. A system planner attempts to remove vulnerabilities implying serious dangers and strengthens the system through a combination of ways of dealing with stress.

To improve the system's security, it is essential that the system planner find vulnerabilities before attackers do. This is accomplished by consistent risk investigation, which is rather appraisal. There are risk evaluation plans for most types of software and equipment components. Nevertheless, no such risk evaluation plot or rule for UAVs was found. Alarmingly, the revealed events relating to UAVs demonstrate that risk appraisal for UAVs – whenever used – is certainly inadequate.

3 Identification and detection methods

Every UAV needs to be identified individually and registered in local airspace control to avoid any unwanted problems. This identification has to be indisputable. Therefore, various ways to detect, track, and interdict potentially unauthorized drones carries critical importance for surveillance and ATM applications. Two categories should be considered. Firstly, the identification of the signal being sent from a drone which can be read in the area where the drone is operating. Secondly, registration of the UAV on the air traffic control system server (Tejedor, 2018).

Drones increasingly need a communication channel to communicate seamlessly. Thus, a method for incorporating the detection and identification of drones is necessary. Every time there is a new drone in an area, it should be detected with drone detection technologies and registered in the local air traffic control system.

A geographical map can be added to the drone identification system to locate it more accurately. This facilitates the identification and location of a drone in a given geographic area as well as sharing it with the responsible authorities.

Some key detection technologies:

1. Wave Radar - mmWave radars are compact devices used for surveillance in conditions of poor visibility. These radars demonstrate low absorption due to rain, fog, smog and dust. They are active sensors. SSRS are radar sensors operating at 94GHz with 750 MHz bandwidth and 20 cm resolution (Caris et al., 2019). High RF bandwidth and resolution enable them to detect and identify UAVs at a range of 10 m to several hundred meters. They provide 1.25°azimuth for cross-section resolution. The power of RF waves used is below the range of that of mobile phones, making it less dangerous. Doppler characteristics assist in differentiating and following the target UAV (Guvenc et al., 2019).
2. UWB Radar - UWB radars use pulse modulation where very narrow bursts are modulated and sent. UWB devices are used for communication, detection and location of objects. In (Nakamura & Hadama, 2017), authors have studied the feasibility of using UWB for drone detection and measured the radar cross-section of a typical drone to be used for detection.
3. Doppler spectrum plays a vital role in analysing the signatures of identification and classification of drones. In (Harmanny et al., 2015), authors have recorded the micro-Doppler ‘signatures’ of various models of drones and also differentiated between drones and birds. While in (Ritchie et al., 2017), authors have analysed the ‘signatures’ of drones with different payloads and without payloads. Short-time Fourier transform was used to analyse the characteristic ‘signatures’ of different drones without payloads. The experimental setup involved three static radars operating at 2.4 GHz frequency.

Other techniques involve visual sensors, acoustic sensors and RF signals being transferred between UAV and controller. In (Nguyen et al., 2016), two possible scenarios for UAV identification are described, namely sniffing of the signal between controller and UAV and reading the reflection from the drone’s propellers.

4 Role of cyber, security, safety and resilience

UAVs are exceptionally uncovered in specialised systems. To investigate UAV vulnerabilities, it is crucial to understand what components a UAV is made of and how these parts work together. To break down UAVs on a typical premise, we depicted UAVs as component models.

The UAV’s foundational, core or base system" is the foundation of the UAV connecting relevant UAV components. The action or whole process of this synthesization and connection allows inter-component communication and provides wider control of the sensor, route,

aeronautical and correspondence system. The more efficient the process, the more the UAV can be defined as an UAV operating as a "working system."

Furthermore, this foundational base system enables the synchronization of other components, like additional sensors or weapon systems. These UAV sensor systems may actually mean the tactile hardware itself of the UAV together with incorporated pre-processing capabilities and functionalities. In case of basic military UAVs, these sensors are frequently cameras with various capacities. UAVs may be fitted with further sensors, for example INS, GPS and radar.

The focus on defence, security and resilience, additionally strengthened by such organisations' and platforms' activity, will provide a deeper understanding of a wide array of areas that include state security, cybersecurity and disaster resilience.

These involve highly novel applications of system analysis in enhancing security and resilience. The importance of such endeavours is to measure the possible effect that dangers pose to how communities adapt to their changing social, industrial contexts and environments.

The UAV avionics system is able to transform received control signals into engine, flaps, rudder, stabiliser and spoiler commands. UAV in-flight communication is always remote and can be divided into two types:

a) direct, line-of-sight (LOS) communication and
b) indirect, mostly–satellite communication (SATCOM).

One example of such a UAV, the RQ-170 Sentinel, can run autonomously. They can also be equipped to hold and operate weapons just like weapon support systems (for example, the MQ-9 Reaper).

The all-encompassing UAV component model's information flow inside may differ according to UAV type. Internal communication may be significant for an attacker if the attacker has access to the internal system (Torun, 1999).

Unless physical access to the UAV is available, an attacker must access and influence the UAV remotely. Making action easier for an attacker, UAVs are profoundly influenced by external input and thus provide different input channels.

Considering the "remote nature" of UAVs, their channels are remote and hence difficult to strengthen. There are a few information flows between a UAV and its environment. The two most significant operational associations are:

1) the bidirectional information flow between the communications system and the ground control station (GCS)
2) the information flow from the environment to the sensors.

However, further impacts of nature on the UAV must be considered. These are the changes in the UAV's altitude actuated by aeronautics, the consequence of weapons on the earth and the impact of the environment on communications.

The dependence of sensors and system components are, for the most part, explored during system planning; consideration of the responsiveness of a sensor or system part to control is not normal. What should be considered regarding unauthorised control of a UAV is information on the receptiveness of the system parts to control. Receptiveness must be considered during system planning to prevent third parties exploiting this information.

5 Vectors and attacks

The inclusion of UAVs into military operation was accompanied by a succession of mishaps broadly affecting the general security of UAVs. One of the most intriguing incidents was the alleged theft of an RQ-170 Sentinel.

It is generally acknowledged that Iranian forces are in the ownership of the RQ-170 Sentinel. This case was confirmed by a press release by US President Obama, requesting the return of the UAV (Bishop, 2004). Nonetheless, the circumstances under which the UAV came into the possession of the Iranian forces are open to dispute. There are two famous hypotheses which clarify how the RQ-170 Sentinel may have been lost.

The principal hypothesis speculates that a weakness of the UAV sensor system with impacts on the routing system was used to attack the GPS system (Torun, 2000).

In general, such an attack theoretically uses relies on knowledge regarding GPS usefulness or its limitations. This makes it simple to attack the GPS arrangement of a UAV by a "GPS spoofing" attack. The satellite signal of the GPS is covered and disturbed by a spoofed GPS signal sourcing from a transmitter with a stronger signal nearby. The spoofed GPS signal recreates the GPS satellite signal, driving on a distorted estimation of the UAVs current position.

A supporter of the hypothesis can actually reason that Iranian forces have successfully attacked the satellite correspondence of the drone and spoofed the GPS signal to have the drone land securely on an Iranian airfield. While this attack is difficult to execute, it is not inconceivable. Yet, the capability of Iranian forces to have enough information and methods to accomplish a GPS spoofing attack remains debatable.

The other hypothesis connects the loss of the UAV due to a specialised error. The hypothesis proposes that the UAV may have landed in an Iranian area because of a specialised breakdown. This may have enabled Iranian forces to retrieve the UAV. Both hypotheses demonstrate security issues.

The GPS spoofing hypothesis underscores the need to incorporate further, unusual components in UAV risk evaluation. Partially efficient systems like UAVs rely on their sensor systems to work accurately. Moreover, the sensor system must be assessed as a constantly open information channel, which may subsequently be susceptible to attacks.

6 Risk assessment framework

When surveying the risk of UAV security violations based on the below introduced component models, the general risk appraisal of a UAV is the summation of its components risk evaluation.

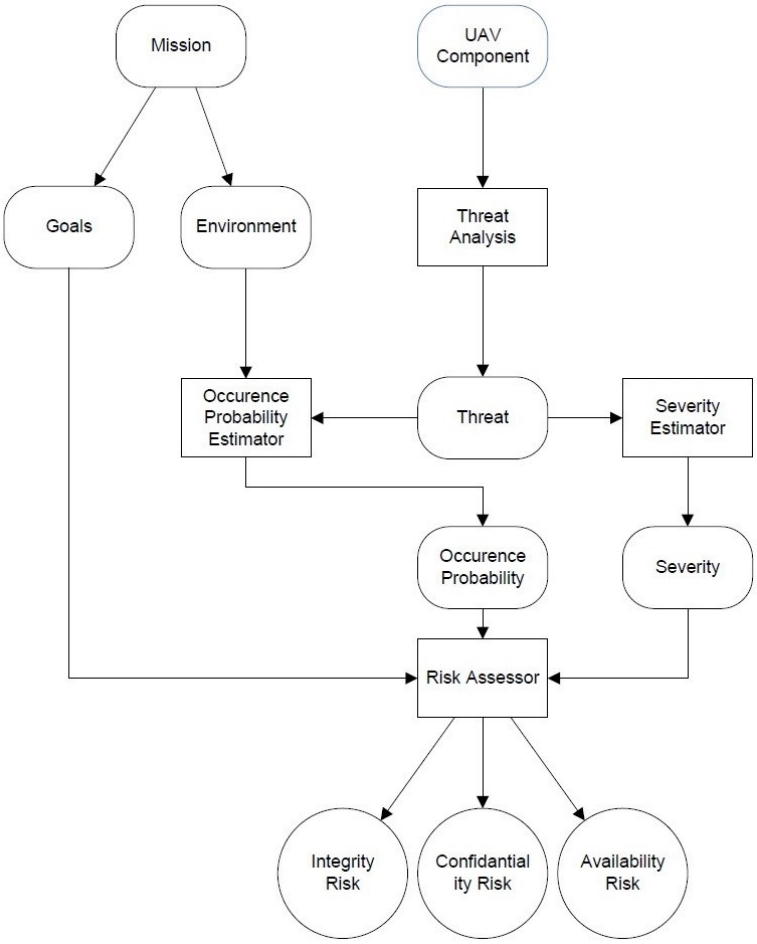
The risk evaluation context, inputs and results have a multi-dimensional. This defines or influences the risk evaluation depending on the type and power of security required. Thus, the result is a component-focused yet insightful, probability-based assessment of integrity, confidentiality and availability of the UAV (Jaquith, 2000).

An output meaning a high score for example in the risk evaluation framework correlates with high risk concerning the loss of confidentiality, integrity or availability. The process overall provides data on the susceptibility of parts to attacks and on the integrity, confidentiality or availability of each part of the UAV.

Values in the range of 0 and 1 are assigned to the part (0 - “not susceptible,” 1 - “highly susceptible”) depending on the degree of susceptibility.

The values are assigned by the framework in accordance with the vulnerability of the analyzed part to attacks affecting integrity, confidentiality or availability. The particular probabilities of the event of an attack are increased with the importance of the weakness in order to compute the risk (Young, 2010).

Fig. 1. Overview of the introduced UAV risk assessment framework.



The outcome should be assessed in accordance with the severity of the loss of integrity, confidentiality or availability of the explored part of the UAV. Security parts may be in conflict. The multi-dimensional analysis of risk explores the various requirements of UAVs. As indicated by the general assignment of the UAV, various security parts play different roles and should be weighted accordingly. Hence, the risk evaluation of UAVs is always alignment (to context and mission) focused and mission-specific.

7 Conclusion

UAV risk evaluation is a complex task comprising vulnerability and threat analysis; moreover, it is mission-specific. The UAV related episodes examined suggest that risk evaluation plans for UAVs are lacking or deficient. The proposed framework is an attempt to depict and formalise UAV risk evaluation.

The component model of UAVs was intended to order and characterise a component-based risk assessment. The components “communication system,” “data storage” and “sensor system” were examined depending on the innovation employed and its known vulnerabilities. Ecological factors and issues relating to maintaining devices were may also be examined.

The qualities determined may give an indication of the susceptibility of an UAV explored to attacks affecting availability, integrity or confidentiality.

In the described framework and its theoretic and practical context, the risk was defined as the output of the susceptibility of a UAV compounded by the probability of occurrence of a particular attack on a component's vulnerability and increased by the severity of the attack.

Resources

Baldor, L. C. (2012, August 12). Flashy drone strikes raise status of remote pilots. *The Boston Globe*.

Bishop, M. (2008). *Introduction to computer security*. Boston: Addison-Wesley.

Guvenc, I., Ozdemir, O., Yapici, Y., Mehrpouyan, H., & Matolak, D. (2017). Detection, localization, and tracking of unauthorized UAS and Jammers. *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*. doi:10.1109/dasc.2017.8102043

Harmanny, R. I., Wit, J. J., & Premel-Cabic, G. (2015). Radar micro-Doppler mini-UAV classification using spectrograms and cepstrograms. *International Journal of Microwave and Wireless Technologies, 7*(3-4), 469-477. doi:10.1017/s1759078715001002

Jaquith, A. (2010). *Security metrics: Replacing fear, uncertainty, and doubt*. Upper Saddle River, NJ: Addison-Wesley.

Nakamura, R., & Hadama, H. (2017). Characteristics of ultra-wideband radar echoes from a drone. *IEICE Communications Express, 6*(9), 530-534. doi:10.1587/comex.2017xbl0079

Nguyen, P., Ravindranatha, M., Nguyen, A., Han, R., & Vu, T. (2016). Investigating Cost-effective RF-based Detection of Drones. *Proceedings of the 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use - DroNet '16*. doi:10.1145/2935620.2935632

Ritchie, M., Fioranelli, F., Borrion, H., & Griffiths, H. (2017). Multistatic micro-Doppler radar feature extraction for classification of unloaded/loaded micro-drones. *IET Radar, Sonar & Navigation, 11*(1), 116-124. doi:10.1049/iet-rsn.2016.0063

Takacs, A., Lin, X., Hayes, S., & Tejedor, E. Takacs, A. (2018, November). *Drones and networks: Ensuring safe and secure operations. Ericsson white paper GFMC-18:000526* [PDF]. Ericson.

Torun, E. (2000). *UAV Requirements and Design Consideration* (Tech.). (NTIS No. 200026)

Young, C. S. (2010). *Metrics and methods for security risk management*. Burlington: Syngress.

WHICH ONE OF US IS THE 'PHISHERMAN' AND WHICH ONE IS THE TROUT?

Tamás Kun[33]

Abstract
Can we influence national elections? Can we gather money for military purposes through the cyber field? Can we cripple economies through cyber-attacks? The answer is yes, we can. In this paper I highlight events occurred in the recent months. Influence in national election could be interfering, but not in the way of altering the polls data, but the events under the campaign. This last motive usually has not been discussed in social discussion.

Keywords
social engineering, cyber activity, phishing, cyber-attacks, financial gain

1 Introduction

This paper aims to draft the situation what is around the topic of social engineering and cyber activities. In the 19th century, from on technological point of view, the Morse code was a big breakthrough and changed the shape of warfare in common. Later, the communication speed accelerated with the radio, the radar and other devices even better. In our century, the IoT devices (the primitive Internet has been founded around 1968) head on tech, with more and more integrated and linked systems. Enormous resources are on the road, what attackers can exploit easily. Coordinated attacks now are available nearly any corner of the world, so tracking these has become a serious problem. If you ask me, the real deal is not just altering the results anymore. The main goal is to change the process as it goes. National governments have been challenged by non-state actors from the shadows, with new tools for influencing. Social engineering is probably a real risk factor for politics, economics and for military as well. In the following, I mention some of these in brief, a review how cyber activities went in the recent months and years.

2 Literature review

2.1 Targets and motives

An article in (Dcomisso, 2020) presents our starting point. Which are the most relevant targets? Almost every business could be a **potential target**. That is coming from stored data. Cybercriminal activities circles around **common motives**: sensitive data what can be personal information, credential information, contact info (email address, cell phone number etc.) or the business infrastructure itself. Generally, cyber-attack activities are motivated by **financial gain**, but other motivation could be arising just as: political purposes, espionage (gaining illegal industrial advantage) or intellectual challenge.

Authors in (Trendmicro.com, 2015) states, that targeted attacks often concentrate on the following:

Information Theft – in this type, attackers are aiming at the owner of the information, whom could hold customer information, business secrets or intellectual property. The effectiveness of this attacking method relies on that quarter of all data breaches since 2005 were on information theft.

[33] Óbuda University Doctoral School of Safety and Security Sciences, 1081 Budapest, Népszínház str. 8., e-mail: kun.tamas@phd.uni-obuda.hu

Espionage – monitoring the victims' activities and steal information that these targets may have

Sabotage – the main goal for the hacker is destruction, defamation or blackmailing targets

Author in (Alder, 2016) says the following: "Cybercriminals were after their account information due to the higher level of privileges they had. 44% of attacks were taking place on the IT department. The financial departments were targeted in 43% of attacks. The CEO was next in line, being the target of 27% of attacks."

I think this is obvious that IT Department is on the top of the charts, because it is the most authorized department in business with tech support background. The following one is Finance Dpt., which underlines the financial gain motive. And as the third in the row is the CEO, who is the top decision-maker person in the company. Statistics are logical and relevant.

Authors in (Eide, 2019) says "Financial services firms are 300 times as likely as other companies to be targeted by a cyberattack—and dealing with those attacks and their aftermath carries a higher cost for banks and wealth managers than for any other sector." Financial firms will be more and more crucial in the future (and they are important in the present as well) when the digitalization process continues in the sector.

2.2 Most common types of attacks

Since the internet is conquering meantime day by day, the types and methods of the attacks on the new battlefield called 'Cyber field' are various and inexhaustible. But these attacks are costing billions for economies around the globe.

Author in (Melnick, 2020) describes the most common types of cyber-attacks:

- Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
- Man-in-the-middle (MitM) attack
- Phishing and spear phishing attacks
- Drive-by attack
- Password attack
- SQL injection attack
- Cross-site scripting (XSS) attack
- Eavesdropping attack
- Birthday attack
- Malware attack

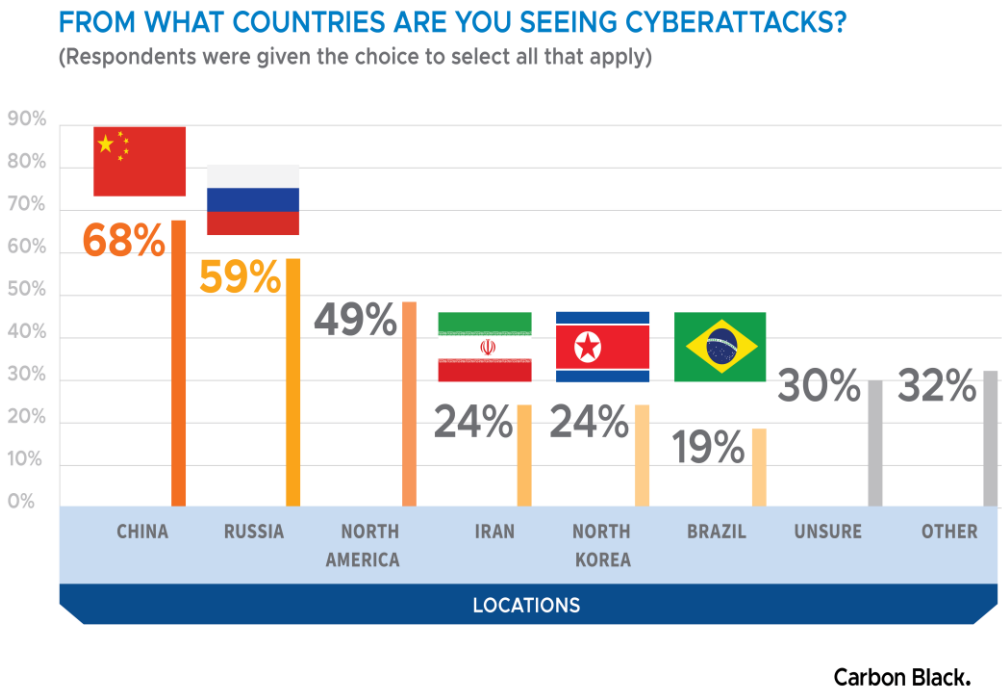
There is a phenomenon, what is not an attack type, but fueling power: **Botnets**. These are mostly hundreds, or thousands of computers infected with malicious code (malwares) which are in sleeping state and generally the malwares undetected by anti-virus software or by the owners. These networks can be used not just to bring enough power source to launch a distributed attack, and hide the attacker, but could be multiply the number of calculations. There are several topographies of its connections: star-model, multi-server, hierarchical and it can be peer-to-peer.

3 The tools of the trade

3.1 Interfering elections

Authors in (Kellermann, 2018) shows that for the midterm election 2018 in the US freelancer hackers offered voter databases on the dark web from 20 different states, where personal information just as IDs, full names, contact info (phone numbers, addresses), gender and even nationalities. This can be a good starting point for direct marketing campaign. Furthermore, the report goes in details with social media sites hacking, offering followers in numbers, what could be used to influence public opinion. And last, they offer DDoS attacks, email list extraction, banking and governmental database hacking, but they underline, that they do not accept social media account hacking offers.

Figure 1 Incident Response firms' investigation



Source: Kellermann, 2018

Interesting thing, that on the figure that North America on the charts has no flags. An explanation for that would be, that NA can be the United States and Canada in common. In summary, we can note that the full arsenal of cyber-attacks is available for business. In Fig.1 we can see that on the top, most of them are Nuclear Power States, which means there must be massive military or economic issues with these attacks.

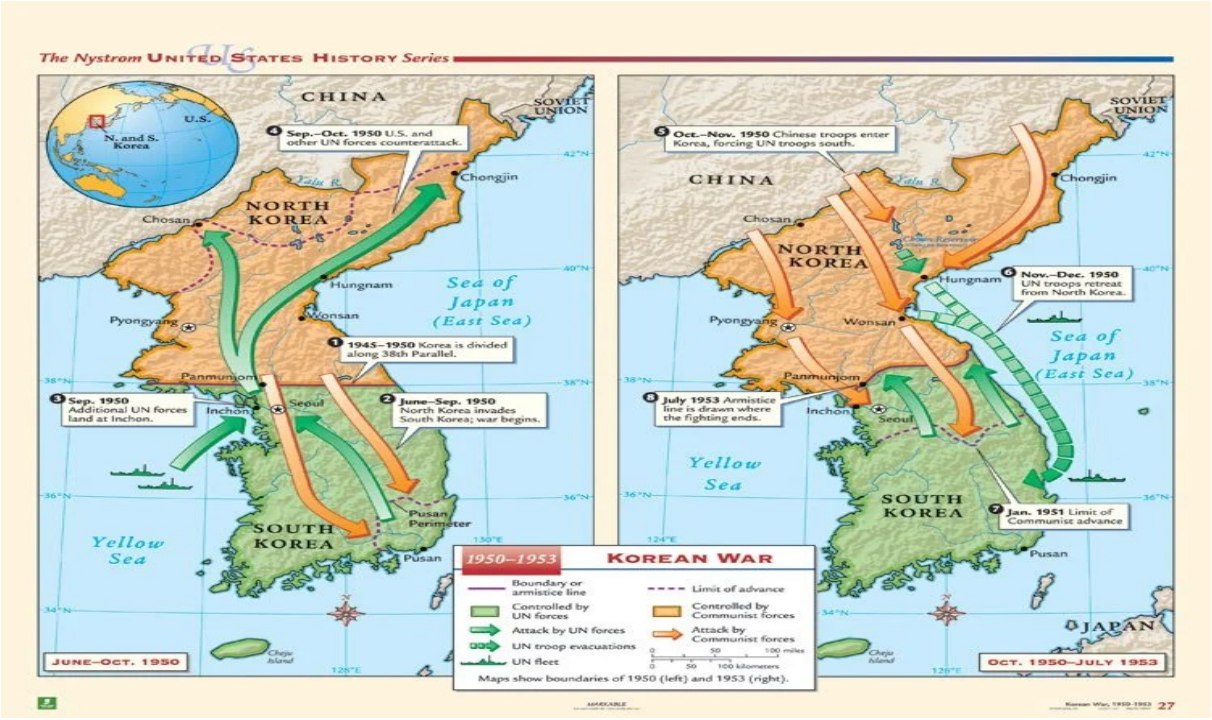
3.2 North Korea's growing cyber activity

North-Korea has invested 2 billion US dollars in cyber-attacks according to United Nations' confidential report (Nichols, M., 2019) says Reuters. The article describes that Pyongyang continued the enhance of ballistic missile and nuclear program but did not make test firing since February. The money comes from cybercriminal activity, where the funds were collected from cryptocurrency exchange and thieving from financial institutions.

Authors in (Kim & Polito, 2019) write about the North Korean army's hacker department. "North Korea's cyber army consists of approximately 7,000 hackers, performing a wide range

of activities including theft, denial of service (DDoS), espionage and sabotage." The point is, not only the DPRK has cyber military personnel in their ranks.

Figure 2 Korean War Alliance Systems

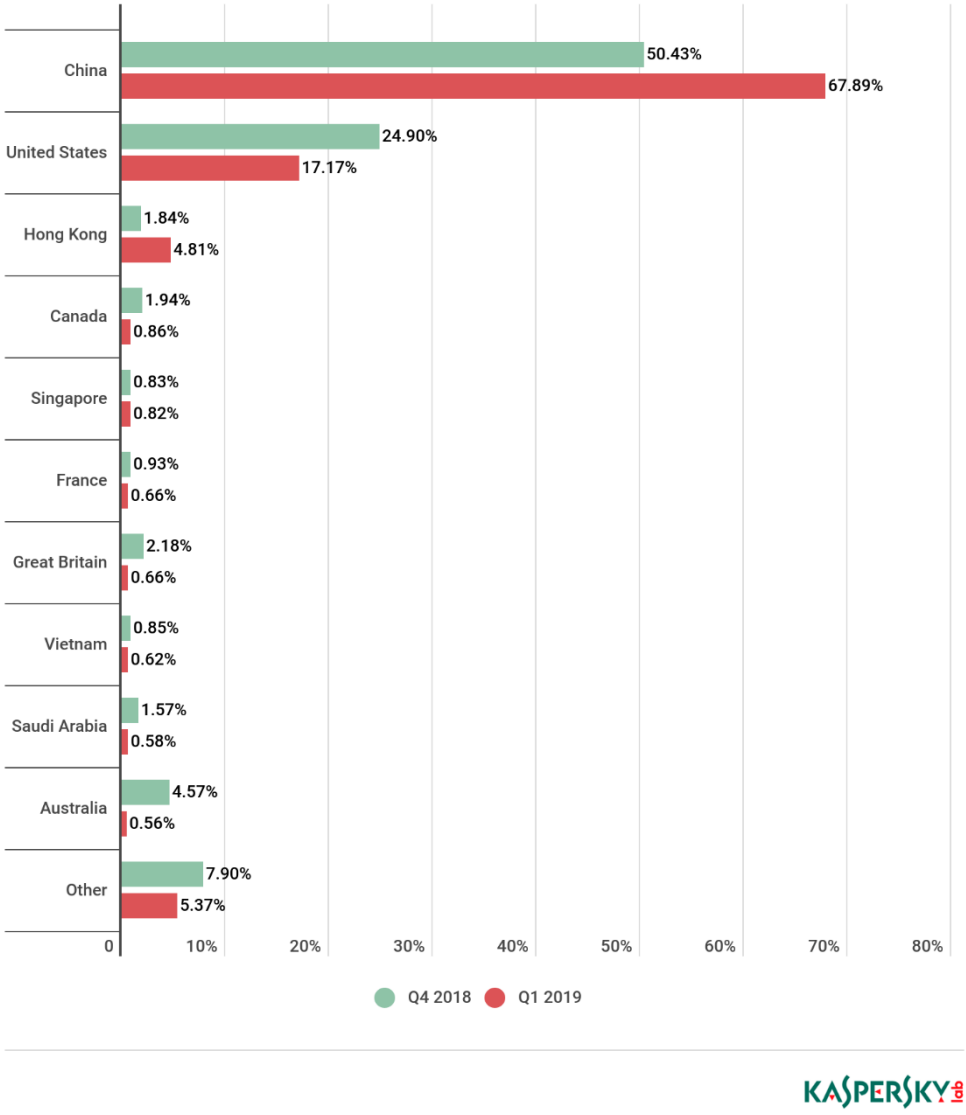


Source: Yao, Z, 2018

What could be the motives are for cyber-attacks? It is known, that the Regime and the US has conflict on Korean-Peninsula since 1953, the end the Korean War. In Fig.2 the alliance between the fighting parties are the same. On U.N. Forces South-Korea, the United States and their allies, facing The Soviet Union (what is today mostly the Russian Federation) and China. Nowadays common interests are replicating the old systems, but with up-to-date challenges. Sanctions against the DPRK is generating the need for reaction, that is the reason why North Korea targets mostly US firms in any way.

3.3 Crippling the routine: DDoS

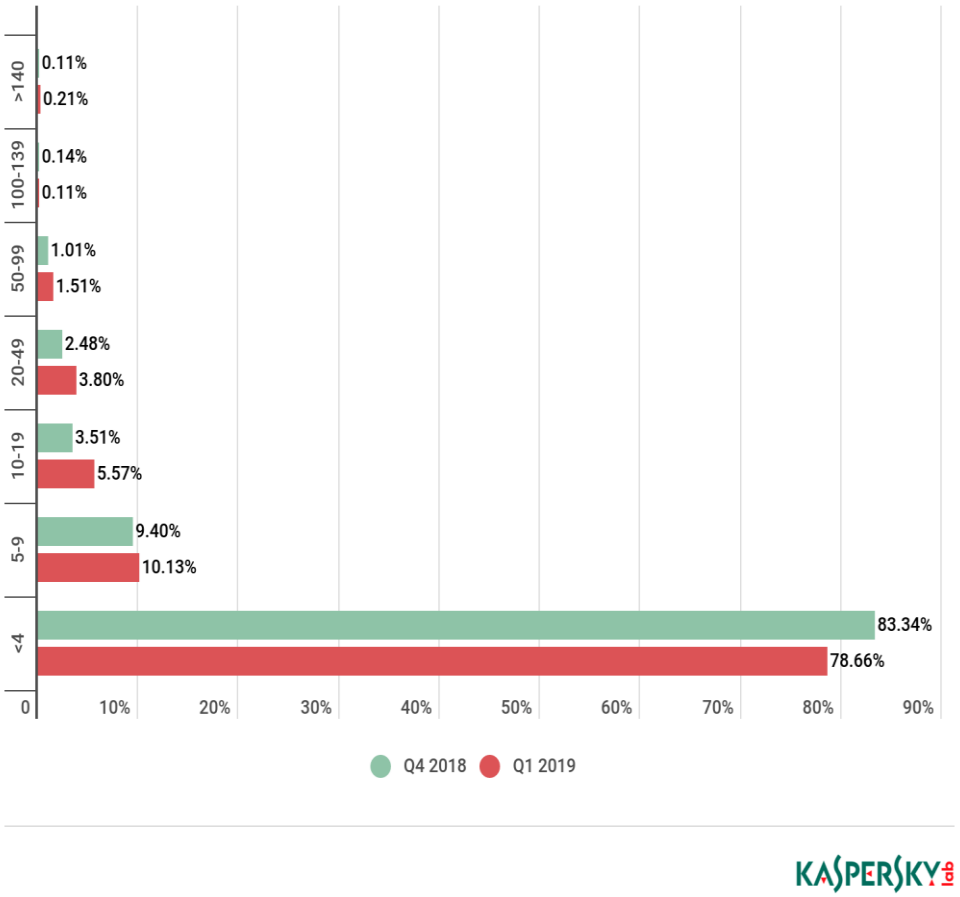
Figure 3 Distribution of DDoS attacks by country, between Q4 2018 and Q1 2019



Source: Kupreev, Badovskaya, & Gutnikov, 2019

First, I spotlight the fact, that Russia is not in the top chart. In Fig.3 there is an increase in China and Hong Kong, while in the other countries we can see a reduction in the attacks. The top two country is an interesting result, because between these two giants there is a modern trade war, which seems to be as real in the cyber as it is in commerce.

Figure 4 Distribution of DDoS attacks by duration (hours), Q4 2018 and Q1 2019



Source: Kupreev, Badovskaya, & Gutnikov, 2019

On the other hand, the length of an attack is a reasonable mention as well. In Fig.4 the chart is beautifully asymmetric, there is an exponential descent. Why DDoS attacks durations tends to only a couple of hours? The answer is simple. The main goal is crippling businesses not destroying them. While businesses are delayed, industrial advantages can be deducted and positions on the markets are changing. In IT services industry, SLA-s (Service Level Agreement) are crucial. Nowadays real-time availability is a must and their denials could be a huge problem. Consumers/customers/clients behavior is important, and we cannot have (we shouldn't) the luxury to let them away to another company. So, there is a race between companies, and there are new tools in the competition, for instance cyber-attacks. However, if these events can go so far, that could be decay homeland security.

3.4 On troubled waters: Phishing

I have met with this at my workplace: **phishing**. Phishing emails usually easily noticeable ones with critical thinking, because they lack the general appearance in a mailbox environment. But, a well-prepared one, for example a **spear phishing** email (which is prepared with an investigation on the target before launching the attack) could be distract a senior employee either. Luckily, the last type requires more time and effort, so these in numbers are not typical.

On mobile devices (Aonzo, Merlo, & Tavella, 2018) phishing activities can be relying on 'secure' forms. The attacker fakes input sites, and the user asked for to give credential information. The fake social media application suggests an easy way to log in, for exchange personal information. Authors highlight an important warn: *"... password managers do not ease phishing attacks, but quite the opposite. In fact, web password managers check the current website domain name to determine whether to auto-fill (or auto-suggest) credentials: if the domain name does not match the expectations, no credentials are suggested. Thus, an attacker that uses Unicode characters to create a facebook.com-looking domain name* ***may fool a human****, but not a password manager: the malicious domain name will be different from the legitimate one, and the password manager suggestion will not trigger."* According to that, the main reason, that phishing could be such as effective, because it is relying on the factor of gullibility. I think the bottleneck of every business organization since the appearance of world-wide internet from a cybersecurity aspect is the human factor. The lack of thoughtfulness, skills or qualified workforce, defense systems are won't be able the hold an attack, so we must inform, train our environment to build up our resistance, in order to make business effective and stable. Experts often say, that security levels can be raise by improving standards. It is obvious, because attacks will be always differing from a daily routine, they are mostly special, one-time only incidents.

Mobile devices have a potential growth in numbers, and practically they benefit from mobility, which allows hackers gather information flexible and with quick changes (in the methods and the victims). Furthermore, this elasticity can be used to connect infected devices on different places and different times, open Wi-Fi platforms with low security protocols, the sky is the limit.

4 Discussion

We can summarize, that in connection with cyber-attacks there are several issues. We cannot state that the main goal is only financial gain. We can see that military motives are also behind these events and remote-controlled devices, IoT technologies, smart devices are also on the field. Economic interests will be on the plate and non-state actors will be also interested in financial matters in the future. Speaking for myself, interfering in the media and social platforms are common things today, but calculating with risk and opportunities are differing from the previous decade. Political and business leaders have been realized that there is so much resource in these tools and methods, and they started to use them in a professional way. I would like to underline, that for this research the gathered data is barely enough, but, the cyber filed is more likely filled with summed numbers and rarely with statistics and long-lasting trends. Cybersecurity today more likely busy with advertising in opposite with prevention and cybercriminals on the dark web are also familiar with marketing strategies. Business is in the focus now, and regulators are running behind the results.

5 Conclusion

The research has been showed, that both social engineering and cyber activities has key potential in the events happening around the world. In the future, this study will continue in my thesis, on a more scientific approach. In my opinion, the common failure on cyber-attack lies on naivety on both sides. The attacker writes a text about asking personal information but, lacks basics like efficient grammar. The victim usually gives away data willingly (like contact info and passwords) which is fundamentally held in the example company's database, what the attacker wants to hijack. We can agree on that we have to train our employees and our private individuals in order to prevent these events. Critical thinking is a must for any cybersecurity or IT professional, because they are the ones whom meeting first with the attacks. The cost of

cybercriminal activity is rising by the with tens of percentage per year, which commemorates well the need for these professionals. In my opinion, today the hackers have the upper hand in the cyber field, but I see potential in regulators, whom has finally understood, that cyber-attacks have critical impact on daily basis. The solution for these is not just making standards for appropriate function, but the conviction of masses that they must be deliberate with these risks and hazards. In the approaching future critical infrastructures will be the key elements in these events.

Resources

Alder, S. (2019, July 15). Calculating the Cost of Spear Phishing. Retrieved December 8, 2019, from https://www.hipaajournal.com/cost-of-spear-phishing-8268/

Aonzo, S., Merlo, A., Tavella, G., & Fratantonio, Y. (2018). Phishing Attacks on Modern Android. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 1788-1801. doi:10.1145/3243734.3243778

Eide, N. (2019, June 21). Cyberattacks hit financial services 300 times more than other sectors. Retrieved January 23, 2020, from https://www.ciodive.com/news/cyberattacks-hit-financial-services-300-times-more-than-other-sectors/557372/

Kellermann, T. (2018, October 13). Carbon Black Report: Destructive Cyberattacks Increase Ahead of 2018 Midterm Elections. Retrieved February 14, 2020, from https://www.carbonblack.com/blog/carbon-black-report-destructive-cyberattacks-increase-ahead-of-2018-midterm-elections/

Kim, C. W., & Polito, C. (2019). The Evolution of North Korean Cyber Threats. The Asan Institute for Policy Studies, Issue Brief, 3, 1-12. Retrieved January 23, 2020, from http://en.asaninst.org/contents/the-evolution-of-north-korean-cyber-threats/

Kupreev, O., Badovskaya, E., & Gutnikov, A. (2019, May 21). DDoS attacks in Q1 2019. Retrieved January 23, 2020, from https://securelist.com/ddos-report-q1-2019/90792/

Melnick, J. (2020, March 10). Top 10 Most Common Types of Cyber Attacks. Retrieved August 24, 2020, from https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

Dcomisso (2020, May 26). Reasons behind cyber attacks. Retrieved August 24, 2020, from https://www.nibusinessinfo.co.uk/content/reasons-behind-cyber-attacks

Yao, Z. (2018, September 30). Why would we not expect the same outcome in the Vietnam War as the Korean War? Retrieved 10 01, 2019, from https://www.quora.com/Why-would-we-not-expect-the-same-outcome-in-the-Vietnam-War-as-the-Korean-War

Thomson Reuters. (2019). North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report. Retrieved January 28, 2019, from https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX

Nichols, M. (2019, August 05). North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report. Retrieved January 17, 2020, from

https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX

Trend Micro.com. (2015, October 22). Understanding Targeted Attacks: Goals and Motives. Retrieved January 24, 2020, from https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/understanding-targeted-attacks-goals-and-motives

LINKS AND VULNERABILITIES OF CYBER-PHYSICAL SYSTEMS - TWO APPROACHES' CONTEXT AND RELEVANCE: SPAEVI AND SCyPH

Zoltán Rajnai[34], Attila Máté Kovács[35]

Abstract
Cyber-physical systems (CPS) interact with infrastructure networks. Other types of networks such as industrial control systems are also linked with cyber-physical systems. In this study, the focus is on the issues and their possible solutions to mitigate malicious attacks on a CPS. To provide better control systems, trust management is promoted across various industries. SPAEVI and SCyPH have been used to explore the possibilities of providing a link between a cyber-physical system and the infrastructure in fields like the automotive industry. Furthermore, contextualizing embedded cyber-physical system malwares' physics impact does not have any formal methodologies and may even be seen as an art.

Keywords

Cyber-physical systems, risk assessment, industrial control system, malware, infrastructure, internet of things, IoT, virtualization

1 Introduction

During the past few decades, with the advancement of IT technologies, the critical infrastructure, and cyber-physical systems have changed a lot. Nowadays, research on cyber-physical system security focuses on the challenges related to the interaction with infrastructure systems like electric grids, oil pipelines or natural gas systems.

Malware and forensic analyses of embedded cyber-physical systems are tedious, manual processes that testbeds are commonly not designed to support. Researchers explored a few main issues of cyber-physical systems. The key focus is on cyber-physical system security and its contribution to vulnerability research, issues and conclusions (Ang Cui et al., 2013). Furthermore, not like existing hardware-based testbeds, the resulting soft industrial control system testbeds are portable, distributable and expandable by design.

On the other hand, this embedded system virtualization itself is non-trivial, especially at the firmware level, and solutions vary widely depending on the embedded system architectures and operating systems. Below are given some key points for cyber-physical systems (Bodenheim et al., 2014).

In large downward systems of critical infrastructure, there are relays built into the trust management system that provides effective support and controlled access to the security system. A trust management infrastructure supports many programs such as security control in a production department, historical logs, databases, operator networks, engineering configuration files, and many other data files belonging to the organization (Barbosa, 2014). Trust management gives key position holders access to a language program so that policy accesses are static to specific personnel. The system is based on cryptographic mechanisms able to communicate credentials, requests, and decisions across the organization. (Huitsing et al., 2008).

[34] Óbudai University, Doctoral School for Safety and Security Sciences, rajnai.zoltan@bgk.uni-obuda.hu

[35] Óbudai University, Doctoral School for Safety and Security Sciences, kovacs.attilamate@phd.uni-obuda.hu

However, you can change any of the decisions or policies at any time manually. Trust management systems mitigate the risk of cyber attacks such as the stealing of important documents (Gilles, 1974).

It is also of utmost importance to explain the patterns of trust management decisions and language as well as calling attention to the risks of policy breaches and data loss caused by postponed security updates (Henry et al., 2010). Rollback access control mechanisms regulate user tasks, which further reinforces the significance of network behavior in a dynamic trust management system (Redwood, 2016). Some of these systems may even be capable of managing all utility networks. Although, if such a utility network is managed by a trustable third party, its chances of being hacked may as well be lower. (Dondossola et al., 2011). The third party is liable for the installation, maintenance, and monitoring of the networks. However, hackers target these third-party services and that is where trust management becomes useful in cyber-physical systems.

2 Literature review

Authors consider and highlight three basic areas such as the identification of vulnerabilities, exploit development, and exploit mitigation. Hackers target the system via vulnerability research using their skills and expertise. The developer of a cyber-physical system should block unauthorized access to the system and rule out the possibility of exploiting the system's vulnerability e.g. by pushing unique characters.

The vulnerability of large-scale applications are of more complex nature, therefore, it gets increasingly difficult to find and fix all of them. A defender always tries to mitigate the risk of being hacked and find and fix all vulnerability points. That leads to the framing of offensive and defensive motivation and as part of this process, development should always use the latest technology. IT security systems such as DEP/NX, ASLR, PIE, RELRO have been revolutionary in this regard. Cyber-physical systems can be evaluated based on three key aspects: threat information, complexity, and the esoteric nature of the CPS (Sridhar et al., 2012).

CPS systems with complex nature deduct problems that provide greater IT security. IT security is the main contributor to the esoteric nature of a CPS. Industry standards and other specifications that protect the firewall against harmful attacks are often restricted by security reviews. A former study suggests that these firewalls and signature-based instructions are ineffective (Liu et al., 2012).

3 Cyber-Physical systems

Cyber-physical systems are sensor-based systems that monitor and control physical systems. That means that the systems in self-automotive sensors, robotic control security system, data acquisition SCADA, process control systems (PCS), industrial control systems (ICS), or distributed control systems (DCS) consist of applications that vary industry by industry based on how they get utilized.

Self-sensors, activators, automotive control systems come complete with terminal units (RTUs), programmable logic controllers (PLC), and intelligent electronic devices (IEDs) that are the basic components of a cyber-physical system. Most of the CPS systems are connected to the internet (Bodenheim et al., 2014). The general breakdown of the layers of a system like that as used by many operational networks such as SCADA, ICS is as follows (Thornton and Morris, 2015).

1. Sensors and actuators;
2. Distributed controllers, including:

- programmable logic controllers (PLCs)
- intelligent electronic devices (IEDs)
- programmable automation controllers (PACs)

3. Supervisory and control systems
4. Human machine interfaces (HMIs)

Firewalls are responsible for the breaking or blocking traffic as soon as possible after an incident report has been received. Firewalls block specific components of the protocol in use.

The developers must have a clear understanding of the specific protocol to be able to detect the problems. Cyber-physical systems are esoteric in nature, which makes it very important for a CPS designer to use protocols when developing a firewall. In most systems, the firewall limits the ports ranges and the cyber security systems developed physical system.

For defensive and offensive points in cyber-physical security many tools such as attack trees, unique languages, Markov chains, expensive real-world testbeds, layered static models, etc. are used to analyze the CPS. The past literature puts a strong emphasis on limiting the protocol, and system control unit logics for CPS attacks.

Faults in the cyber-physical security and control systems are identified by recognized organizations in the U.S. Department of Energy and Institute of Standards and Technology (Guidry et al., 2013). Reliable computation-heavy infrastructure models were designed to guarantee high-level security (Burmester et al., 2013). Other developers use reverse engineering approaches for the investigation of target systems (Liu et al., 2013).

4 Framework design and methodology

Attack, exploitation and post-attack actions and their consequences for the CPS are visible and tracked in SCADA HMIs and PLCs. The honeypot technologies available today provide attackers with data that is often static or pseudo-random data. This will most probably not force attackers to use high value or zero-day attacks.

Yet, this problem may be tackled by a symbolic cyber-physical honeynet framework, enhancing the screening and coalescence of attack events for analysis, providing attack introspection down to the physics level of a SCADA system and enabling forensic replays of attacks.

Honeynet methodologies shall and can also be extended. This extension may cover the application of integrated physics simulation and anomaly detection relying on a symbolic data flow model of system physics. Attacks triggering anomalies in the physics of a system can thus be captured and organized via a coalescing algorithm for efficient analysis.

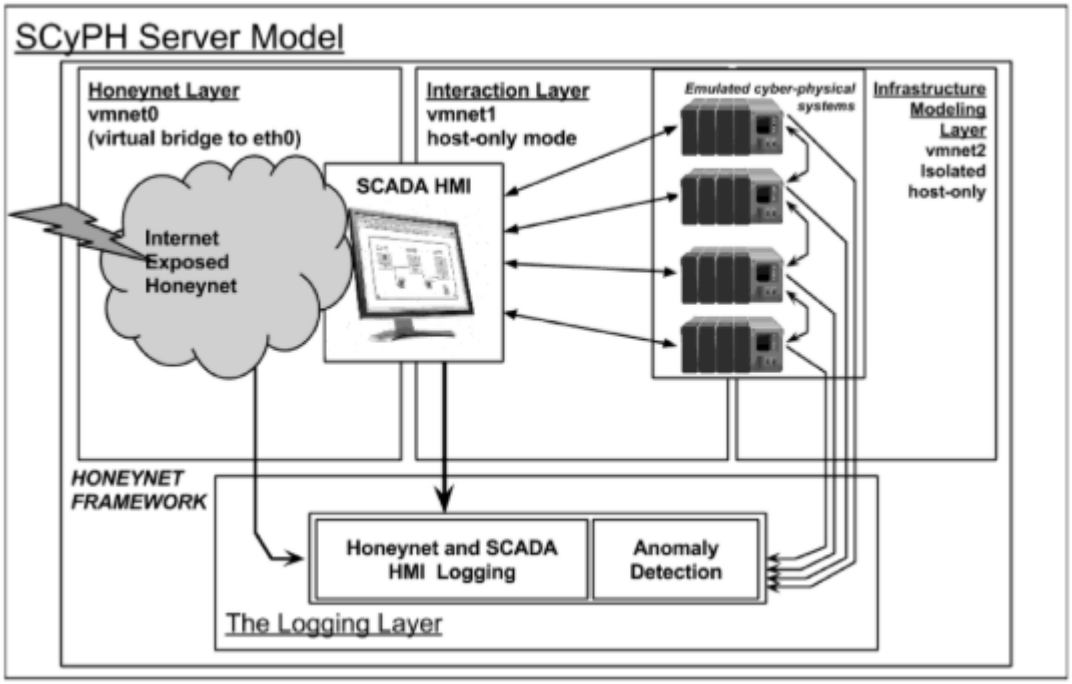
Experimental results have already demonstrated the effectiveness of the approach in research. A symbolic simulation in a CPS can be used to monitor the device display and visualize the monitoring process.

It is true however, that HMIs allow hackers an easy opportunity to access critical parts of a system. In some instances, the phase angle and voltage fluctuations may be problematic for an electric grid.

To detect the problems, a CPS should have the following three features:

- All components should be modular
- HMI interaction should be coupled with the simulated physical model
- Layers should be strictly partitioned

Figure 1: A general architecture for the SCyPH framework



Source: Rice & Shenoi, 2015

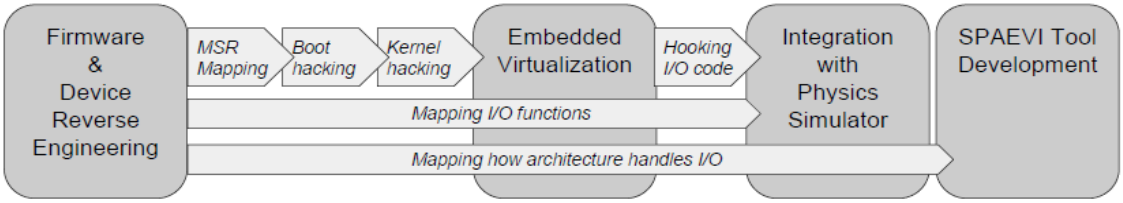
It is also important to note that in spite of decades-long support by experts and government authorities, the so-called "air-gaps" are not used and managed properly. This phenomenon is especially dangerous as they are supported by vendors and are relied upon to safeguard industrial control systems and operational technology and utility networks.

In 2011, the Director of the U.S. Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) testified that: "In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network" (Subcommittee on National Security, 2011). This situation is not unique to the U.S. power grid and there is compelling evidence that industrial control system vendors have been intentionally moving away from the traditional airgap advice (Byres, 2012).

These reports and experiences lead directly towards the research and application of a wide array of tools and methodologies to measure or simulate threats.

Past studies suggest that the Simulated Physics and Embedded Virtualization Integration methodology (SPAEVI) is a valid design for the implementation of portable, expandable, and distributable technologies. The stated technology is used for the detection of malware, reverse-engineering, and distributive systems.

Figure 2: The SPAEVI methodology workflow



Source: Rice & Shenoi, 2015

i. Results, conclusion and recommendations

The SPAEVI methodology covers the analysis of the malware, automotive weapons, even drones as part of Layer 2. However, in the case of a high-level data scam, in Layer 3 and 4, the SCyPH technique may fail and even physical data can be damaged as the results of a malicious attack on the cyber-physical system.

The referred studies explain the problems and analysis of the cyber-physical system. The researcher contributes to the identification of the control system problems limiting trust management. The vulnerability research is typically covered in or at least closely related to threat intelligence. Cyber-physical system malware analysis results in the restriction of certain protocols in the physical control system. On Layer 4, the chance of cyber attacks is increased and it is quite easy to compromise system security. While on Layer 3, it is relatively complex in nature. The protocol is quite complex in different computer systems. The above techniques may even cause the device to reboot. The results show that Layer 3 and 2 are trustable protocols for cyber attacks even in the event of recurring attacks.

At the initial stages, CPS malware was designed to limit physical devices. Then with the development of systems and techniques, later experiments illustrate that a cyber attacker can control the physical device with little effort. 'Little effort may mean, that the attacker can access the physical system with CPS-embedded malware by using approximately 8 bytes.

Resources

Ang Cui, A., Costello, M., & Stolfo, S. J. (2013, April 23). *When firmware modifications attack: A case study of embedded exploitation.* [PDF].

Barbosa, R. R. (2014). Anomaly detection in SCADA systems: A network based approach. doi:10.3990/1.9789036536455

Bodenheim, R., Butts, J., Dunlap, S., & Mullins, B. (2014). Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices. *International Journal of Critical Infrastructure Protection, 7*(2), 114-123. doi:10.1016/j.ijcip.2014.03.001

Burmester, M., Lawrence, J., Guidry, D., Easton, S., Ty, S., Liu, X. . . . Jenkins, J. (2013). Towards a secure electricity grid. *2013 IEEE Eighth International Conference on Intelligent Sensors, Sensor Networks and Information Processing*. doi:10.1109/issnip.2013.6529819

Dondossola, G., Garrone, F., & Szanto, J. (2011). Cyber risk assessment of power control systems — A metrics weighed by attack experiments. *2011 IEEE Power and Energy Society General Meeting*. doi:10.1109/pes.2011.6039589

Gilles, K. (1974). *The semantics of a simple language for parallel programming. Information processing* [PDF].

Guidry, D., Burmester, M., Liu, X., Jenkins, J., Easton, S., & Yuan, X. (2013). A Trusted Computing Architecture for Secure Substation Automation. *Critical Information*

Infrastructures Security Lecture Notes in Computer Science, 130-142. doi:10.1007/978-3-642-41485-5_12

Henry, M. H., Layer, R. M., & Zaret, D. R. (2010). Coupled Petri nets for computer network risk analysis. *International Journal of Critical Infrastructure Protection, 3*(2), 67-75. doi:10.1016/j.ijcip.2010.05.002

Huitsing, P., Chandia, R., Papa, M., & Shenoi, S. (2008). Attack taxonomies for the Modbus protocols. *International Journal of Critical Infrastructure Protection, 1*, 37-44. doi:10.1016/j.ijcip.2008.08.003

Liu, C., Stefanov, A., Hong, J., & Panciatici, P. (2012). Intruders in the Grid. *IEEE Power and Energy Magazine, 10*(1), 58-66. doi:10.1109/mpe.2011.943114

Liu, S., Mashayekh, S., Kundur, D., Zourntos, T., & Butler-Purry, K. (2013). A Framework for Modeling Cyber-Physical Switching Attacks in Smart Grid. *IEEE Transactions on Emerging Topics in Computing, 1*(2), 273-285. doi:10.1109/tetc.2013.2296440

Redwood, W. O. (2015). Cyber Physical System Vulnerability Research. Retrieved from http://purl.flvc.org/fsu/fd/FSU_2016SP_Redwood_fsu_0071E_13190

Rice, Mason & Shenoi, Sujeet. (2015). *Critical Infrastructure Protection IX* : 9th IFIP 11.10 International Conference, ICCIP 2015, Arlington, VA, USA, March 16-18, 2015. 10.1007/978-3-319-26567-4.

Sridhar, S., Hahn, A., & Govindarasu, M. (2012). Cyber–Physical System Security for the Electric Power Grid. *Proceedings of the IEEE, 100*(1), 210-224. doi:10.1109/jproc.2011.2165269

Thornton, Z., & Morris, T. (2015). Enhancing a Virtual SCADA Laboratory Using Simulink. *IFIP Advances in Information and Communication Technology Critical Infrastructure Protection IX,* 119-133. doi:10.1007/978-3-319-26567-4_8

A SENSE OF SECURITY AND SECURITY AWARENESS

Lajos Szabó[36]

Abstract
The lack of a definition of a sense of security makes it difficult to compare common language and scientific interpretation. I present the possibilities of defining subjective and objective sense of security based on the results achieved in psychology and sociology, criminology, and law enforcement. Analysis of the emotional and intellectual content of a sense of security. Criteria for safety-conscious activity.

Keywords
Safety, Security, sense of security, objective sense of security, subjective sense of security, safety consciousness

1 Introduction and literary review. (The practice of using terms of security and security awareness.)

Again, I would like to address some of the terms that we believe are scientifically defined concepts, but they are not. We like to say that we are representatives of homo sapiens, we always know exactly what is happening around us. In addition, because of our conscious activity, forward-thinking planning and conceptual capacity, we are able to influence future events. This is partly true, but in many cases it is not true. It's not even true that we perceive our environment with the right accuracy. As Donald D. Hoffman, a professor in the department of cognitive sciences at the University of Irvine, California, points out, it is preferable to adapt to perceptions than to use energy to develop and analyze them; "*Organisms that accurately detect reality are destroyed by non-realities but adaptive organisms*" (Hoffman, 2015).

It is important for many disciplines to define what we mean by a sense of security. Since we not clarify this, we can't really talk about what can be called safety-conscious behavior. Until we find a connection between the factors that triggered our sense of security and the activity and behaviors that we do, can we not be sure whether what we are doing is a conscious, instinctive, or emotional approach. I have already explained part of the topic in my presentation on the relationship between security and a sense of security (Szabó, 2016), but the three years that have passed have strengthened my urge to coincide with the very widely used term 'security awareness' today. In doing so, I will use part of the material from my aforementioned lecture.

1.1 A sense of security.

It is clear that the existence of some sort of orderly relationship reduces the possibility of manifesting threats and makes security, predictable, or at least estimated, by public policy at some level, and thus a sense of security in citizens.

"Scientific thinking is therefore characterized by thinking in abstract concepts." Scientific concepts are some tools of scientific thought. Through them, the scientist reaches to understand complex phenomena, to recognize their mutual relationships, and to their depiction in a telling form." (Szilágyi, 2014, p. 4.)

[36] Head of curators – REMOK Foundation -1037 Budapest Orbán B. út 37. e-mail: elnok@remok.hu

It would follow from all this that scientific thinking is based on conception and definition, after which "scientists who speak a common language" can truly understand each other and interpret the same term in no other way. So, if a science creates a concept and always does it definitively, then maybe another science would use it in the same sense, with content. However, this is not the case, it is regularly the case that the same term is used in a very different interpretation in different disciplines, and as found at that conference, they form or use terms without a formal definition.

And that's confusing. It also disturbs the researcher, the instructor and the student who are trying to learn the new ones. And in people who are uneducated on the subject, it creates such a misconception that he know what the others are talking about, and as soon as someone realizes his mistake, everything that relates to the term in question becomes meaningless to him. As I would like to say in the title, I would like to interpret the relationship between two concepts. One of the concepts in one of the titles is a sense of security.

It's a term that's confusing to me for a number of reasons. On the one hand, I didn't find its definition, even though it's used by a lot of psychological textbooks and scientific work. Abraham Maslow, the creator of the famous Pyramid of Need, did not define it either, and his explanatory syllables seek to illuminate the elements of security-need without any definition.

On the other hand, it contains a self-contradiction when the term is used in definite psychological concepts.

" By sensing we mean the uptake of stimuli by means of receptors in our sensory organs and their conversion into stimuli, i.e. electrical impulses. "*Sense in the biological sense, in the body, is a physiological change caused the a stimulus.*" (Varga et al. 2018) The sensation can be linked to other vascularizations and can generate cognitive processes that can result in a direct response to sensation (reaction) or a perceptivness with other sensations. Perception by psychology concept

"- Perception is the set of psychological processes through which we recognize, organize, and give meaning to perceptions from environmental stimuli.
- Our perception is significantly influenced by our prior experience, knowledge, current mood, needs, interests, and the particular culture in which we live. Learning also plays a very important role in perception. " (Varga et al. 2018)

So, the sensation is the trace of a signal coming through a particular receptor, if the traces of multiple sensation are combined as a result of some process, a new quality is created and we are talking about perception.

"Physiological variation in the body, in a biological sense, caused by stimulus." The sensation can be linked to other vascularizations and can generate cognitive processes that can result in a direct response to sensation (reaction) or a perceptive ness with other sensations.

Although some sightings may carry information about our own personal safety, such as feelings of balance, organs, pain, etc. We respond to these with immediate reactions and only supplement the other perceptions to identify the threatening circumstances, the lack or existence of our safety, that is the conscious activity becomes possible only with the creation of perception. Of course, I am also aware that there are perceptions that do not reach the level of consciousness when we act. These are most typically corrections made during movement, such as cycling, where due to the multitude of incoming stimuli, the brain would simply be unable to "elevate" the speed of response to a conscious level. There is a narrow range that is conscious, and "below" one that is completely unconscious.

A very interesting work, " What Is the Duration of a Percept?" (Herzog, Kammer, & Scharnowski, 2016) Is a very visual indication of this. The uniform sense of the discrete senses (3-10 ms) calculated in milliseconds shows a severe delay that can result in data loss and false

perception, which can have a direct consequence of a faulty reaction. The researchers accurately measured how unconscious the processing of perceptions into sensitized, as expected by the input of additional information in subsequent processing. The conscious detection only occurred after 400 ms, according to the experiments. For example, why someone becomes sympathetic or unsympathetic, right after we get to know them. It is a similar situation with factors affecting our security, which are largely unconsciously processed and responded.

In other words, in my view, the word 'sense of security' is not an appropriate term, if we consider the basic concepts adopted by psychology, and instead 'safety detection' would be the scientifically sound term.

However, since we do not use scientific concepts in colloquial practice, the term "feeling" usually means our idea of something (which psychology defines as perception). Certainly, the term "sense of security" emerged long before psychology developed the definite concept of "feeling and perception." Changing an expression rooted in the public consciousness and vernacular and interpreted equally by all makes no sense. It can only be a problem for those who, for some reason, are forced to thoroughly analyze and reflect on its true content.

2 Material and method. (Element-specificing of the definitions used to define a sense of security.)

Most recently, securities market III. Conference 2016. Budapest - I sat and listened to the moderators' questions, where the term "subjective sense of security" was audible. I was so confused by the term at the time that I said it, before, among others, about how meaningless the composition was.

"Behind countless human actions, we can find the issue of a sense of security as a motivating factor. The phenomenon can be described on the one hand, at the level of feelings, and on the other hand, with more tangible, concrete realities. As a feeling, we can talk about a psychological category that may be contrary to the expected behavior predicted by real, supported data." (Tóth, & Horváth, 2014)

Therefore, as the above study states, the "sense of security" is undoubtedly a subjective thing that arises in one's consciousness and can show a formation completely independent of reality and facts. In other words, the "subjective sense of security" corresponds to the unnecessary word compositions of the type "dwarf minority or metal-containing ore, etc.".

I should already apologize in advance for my statement at the end of my previous sentence from Dr. Péter Tóth, assistant professor of the university and doctoral student Helga Horváth, who are noting the study entitled 'Factors influencing a subjective sense of safety in Hungary' (Tóth, & Horváth, 2014), since I claim that there is already a meaningless word in the title in their study. What is a fact, if for some reason the term 'subjective' was added to the term 'sense of security', they certainly had a reason, so in their study, I was therefore obviously looking for the first time to see if it contained an 'objective sense of security'. Unfortunately, the term 'objective' is not included in the study at all times, so it is not possible to know from this paper what the authors might consider an 'objective' sense of security.

For example, a criminologist, describes the objective sense of security in a study by Dr. Vince R. of NKE Rtk. (Vári, 2014) „It can be concluded from research that the possibility of victimization meaning objective safety, and subjective sense of security are not only linked, but the reverse is true,... " (Vári, 2014, p. 14). It follows that, obviously, from the point of view of the criminologist, it chooses a particularly effective solution and indirectly forms an objective safety category of public safety from the number of offences committed.

The UN World Happiness Report takes on other aspects in its "well-being" examination, where it clearly matches "well-being" to a sense of security, since anyone who does not feel threatened by their workplace, their education, identity, property, sees their way of life, the

social care system, clearly feels safe. Another volume of studies presenting the results of the research, (Bugovics & Tóth, 2015), which is noted by sociologists, also explores the "well-being" issue, helps in what sociologists mean by objective safety; *'It is not only a cross-check of subjective and objective elements relating to crime, where subjective elements are data on municipalities in population questionnaires, while objective elements represent averages from territorial statistics*' (Bugovics & Tóth, 2015, p. 16.)

Some changes in the threshold (it has been increased three times since 2000) is enough, and there is already a significant reduction in the number of crimes, since if, say, an illegal act of more than 20,000-ft was considered a criminal offence, once the threshold had been changed to 50,000, it would no longer appear in the criminal statistics. It's true that they steal, vandalize, etc. still below 50,000-ft, but, logically, the crime statistics cannot be mentioned, and the citizen can already feel more safer when looking at crime statistics.

As some of the offense are thus no longer a criminal offense, many no longer even report breaches to the offense threshold, so latency usually increases after such changes.

Not only against property, but also, e.g., there are also latencies in the statistics of crimes / offenses against a person, not even a small one, such is typically bodily injury cases, in a significant part of which the victims do not want a lengthy court procedure. But even in the case of traffic crime / violation statistics, distortions and problems of interpretation can occur, as the driver is legally "drunk," with air alcohol probing showing alcoholism, since even a very small amount of consumption is considered a crime, e.g., In Hungary. However, the alcohol content of the consumed glass / mug of beer may not have appeared in the blood when the driver becomes a party to the accident or perpetrators, ie medically, alcohol consumption does not play a role in the accident, legally and statistically.

As András László Papp puts it in a study, in perfect accordance with the above, "… society's sense of security does not change objectively, depending on statistics on crime or terrorism, but changes as a result of many socio-psychological coefficients, not least information to citizens." (Papp, 2012, p. 30) Interestingly, not only information, but also our qualifications and abilities are considered as influencing factors when we perform a "safety analysis." For example, if someone is unable to perform mathematical calculations that are more complicated than the addition-subtraction operation, or only with difficulty, their sense of security may even be good in financial terms, even though they are in a catastrophic financial situation. The financial - "broker" - scandals following the change of regime show exactly how well the "average citizen" can perceive financial risks. The politician, the trader, the service provider is able to perceive exactly what can cause a sense of security in the target audience and act accordingly. We experience the same thing when a trader, insurance or financial consultant, or just some kind of craftsman offers us his portfolio, his services, with overwhelming expertise, references, data. Most people try to ensure their IT security based on various articles and sit back contentedly. Few people know that, e.g., they do not have exclusive rights over their router leased (received) from the service provider, on which their TV, radio, telephone and Internet traffic now operate. Among the employees of the service provider, those who are engaged in the installation and management of the network are able to connect to the device at any time, even completely unnoticed. Over the past decades, our computers and related hardware components have received numerous "security fixes," both in terms of firmware and software, which mean they were did not secure until then. Not even now, they have a myriad of known and as yet undiscovered vulnerabilities. By now, everyone is communicating with a smart phone whose innumerable apps have been found to be infected with malware, even though they were available in "official" iOS or Android "stores".

Obviously, the sense of security is a very complex thing to assess, perceive something, but if we know the inputs and the evaluation (average) schemes associated with receptors, we can influence the "average" sense of security of the vast majority of the population, or even a person or a smaller group.

It is also obvious that in addition to psychological readiness (or sensation), there is a need for expertise related to the given topic, or at least its appearance. Yes, apparently. I do not want anyone to confuse the persons engaged in the occupations and activities listed above with the criminals, but the perpetrators of the fraud crime defined in the Hungarian Penal Code are only able to complete the crime - the result is a crime and the damage is a necessary factual element, as well as charlatan, fortune tellers, etc. In the course of their activities, they assess the level of knowledge and intellectual abilities of their victims, and they commit the act in accordance with them. It's true that they typically have to strive for personalized solutions, but they have a lot of practice with specific schemes that they apply to a manual worker, or a high school teacher, or a businessman.

If the circumstances are such that the citizen is afraid of acts of violence, a large number of police forces will appear in the public area, and from time to time most will report a significant increase in security. Of course, there will be someone who, with the right training and information, will immediately realize that a "demonstrative public presence" is completely ineffective and / or unjustified. They are the statistically almost negligible proportion who are not interested in politics, as they read not only headlines and up to 10 lines of news, but also longer studies and are able to draw conclusions. András László Papp expresses a rather polar opinion on this issue; "*Ultimately, we can also say that if crime (more precisely, the fear of it) exists primarily in our minds, feelings, anxieties, then the state is actually doing the right thing by treating us with psychological placebos and it would be unnecessary to bother with certain security measures. Practical impact assessment.* " (Papp, 2012, p. 31) We can agree with the opinion in the fullest possible way, even if we extend it not only to crime, but to all other factors without! This can be the case, for example, when we meet a need that did not exist before, thereby gaining customers and satisfied, happy, safe customers. Well, the subject is almost unavoidable. It follows from the above that a sense of security is a state of consciousness (belief) that arises when our perceptions of the environment, which we pass through the filter of our own knowledge, suggest to us that we are safe there and then, in that activity, situations, circumstance. It is obviously subjective, as it develops within us, based on our knowledge and in many cases our emotions.

2.2 Security awareness

Over the past decade, the term "awareness" has become increasingly important in at least two word combinations. Environmental-awareness, safety-awareness, the terms are familiar to all of us, they appear in the media on a daily basis. On a daily basis, news makers are pushing these two terms and content into us. But what happens when are you looking for the term „security awareness", on the Internet? Most of our first hits are information technology articles, followed by documents on occupational safety, fire protection, accident prevention and transport. We do not find an exact definition or, if so, it is not suitable for all situations. In my opinion, the Glossary of Law Enforcement established by the Hungarian Society of Law Enforcement contains a definition that describes as accurately as possible what we mean by the term. "*Security awareness is based on security sense. It presupposes that in the context of the interested party he or she knows the value of the interest, objects, system of relations that is important to him / her, and him or she is aware of what this may mean for the opposing party. Also, that a positive relationship may cease to be transformed if no activity is done in order. Security awareness prefers the emotional side in the case of the individual, while the organization and institution prefer the rationality that maintains the system of relationships.* " (Sallai et al., 2008) Examining the definition, it is clear that it explains the concept in relation to a particular person and an organization, so it has very limited applicability.

It is unfortunate that the basis indicated in the first sentence of the term, "safety or security awareness," has not been defined in this glossary. The word security-consciousness most likely covers the state of consciousness that we call security. Security awareness depends on our perceptions and the quality of our knowledge, practice and experience in the same way as I explained in connection with the feeling of security. In the case of security awareness, however, something new emerges, which probably does not appear in the slightest in the sense of security. The sense of security is basically a perception and the formation of consciousness, emotional relationships, while security awareness already presupposes some active behavior.

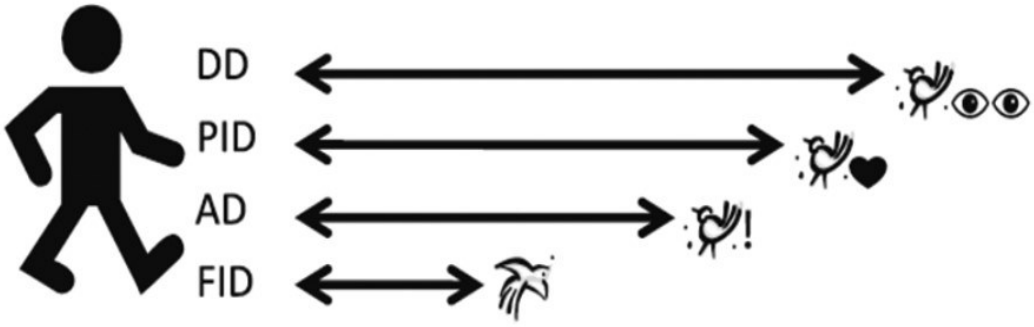
It can be an evaluation analyses, a verbal or specific physical activity, the transmission of information, or an intervention in the variables of our environment in order to maintain a state or change it in a way that is positive for us. The more in-depth knowledge we have, the more practice we have in different activities, the more accurate information we have, then the more effective solutions we can apply when needed. The extent to which we do not pay attention to this and do not form the basis of our daily lives is exemplified by the system of transport safety expectations. As long as - in Hungary - we transport a child in a car, we have to meet incredibly strict criteria. On the other hand, with regard to the safety of a child transported on a bicycle, the regulation is exhausted by determining the age of the transporter, without any technical, occupational or accident protection regulations!

The more thoroughly we are trained on something, the more practice we have gained in an activity, the more accurately we know the boundaries beyond which our safety is endangered.

A "simple" driver starts with a serious handicap against a driver with special driving skills in the same situation, but the same can be said for any profession or activity. It does not matter whether, from an ethological, sociological, occupational safety, fire protection or any other point of view, we examine the sense of security of the individual or group and its environment, as well as the adequately certified safety-conscious activity.

The best example of this is the ethological concept known as "flight distance." What is called take off distance? Flight initiation distance (FID) is the distance that, when a predator is detected, causes the prey animal to flee or take on a protective formation. (Fernandez-Juricic, Jimenez, & Lucas 2001, pp. 30-31) The terms' personal space and intimate zone used for people describe the same distance that varies from individual too individual when we begin to certify defensive behavior. Due to the plethora of ethological and psychological publications on the subject - Google Scholar gave 162,000 hits to the English search term and its notoriety, and I omit further explanations. Of course, as ethology further explored the issue of FID, more and more related concepts emerged, which are illustrated in Figure 1 (Weston, M. A., McLeod, E. M., Blumstein, D. T., & Guay P.-J., 2012, p. 2).

Fig. 1: DD detection distance, PID psychological response (identification) distance, AD alarm distance and FID take-off distance.



Explanation of Figure

- First, it is important to detect changes in the environment (detection distance = DD), even when only the fact of the change can be identified, but we do not yet know exactly what we have noticed. This is called Detection Distance.
- This is followed by the identification of the object of change that needs to develop a psychological initiation distance (PID) that is adequate to our relationship to the object of identification. This is exactly how friend-enemy identification systems work in modern weapon systems! This is called Psychological Response Distance.
- If identified as an enemy, the alarm level (AD) is reached with a very small time difference. This is called the Alarm distance.
- This is followed by the specific physical reaction (Flight initiation distance = FID), which can be escape, preparing for defense, taking on a defensive formation, and many other options until the start of the preventive attack. This is the Flying Distance, which may mean not just escaping, but even attacking or taking another safe-feeling distance. The phenomenon of FID thus accurately demonstrates that a sense of security is also present in the consciousness of animals. The activity of embarking on an escape or maintaining a distance (increasing the level of safety or maintaining an existing level) can be assessed as a safety-conscious behavior.

The existence of FID also proves that safety-conscious behavior cannot be linked solely to humans, to human behavior, but not even to the family of primates, we must go far beyond the time line of tribal development. Of course, this does not mean that animals and humans are similarly safety-conscious, but it does mean that the urge to do so is much more deeply embedded in our behavior.

3 Results and their evaluation. (Is there an accepted sense of security, a concept of security awareness, and can these concepts be characterized by subjective and objective adjectives?)

As I mentioned in my introduction, we are happy to deceive ourselves by knowing what and why we are doing, as a meaningful person, the facts, objectivity, influence us. Previous analyses do not fully support this. I begin by saying that the interpretation of the term 'sense of security' has shown that the term itself is scientifically incorrect. It has also been shown that the concept itself is little filled with content, not described in a definitive way. In the same way, so far no one defines what is meant by the term “security awareness.” The root of the problem, I believe, can be found in what I have uncovered in my work on the concept of security. A sense of security, a state of consciousness or behavior that can already be discovered in the animal kingdom. During evolution, nothing has changed on this issue when we consider McLean’s (Bárdos, 2012) theory of the three levels of the human brain. An essential element of this theory, which is now increasingly accepted, is that a significant part of human behavior is outside the zone that can be called consciousness.

Regarding human behavior, I would quote Carl Sagan’s statement (Sagan, 2000, p. 36) “*The human race is many hundreds of thousands of years old (and the family of humanoids is many millions of years old). In only three percent of this period did we pursue a settled lifestyle, farming and domesticating the animals. It is by this time that all written history falls. In the first ninety-seven percent, almost everything we consider a human trait is created.* ” Since the feeling of security and security awareness is not fundamentally human behavior, its awareness and

objectivity could be excluded from the outset. However, it cannot be completely ruled out that we can determine whether we are safe in a given place, times, circumstances by means of an analysis based on intellectual - objective experience, knowledge, practice?

Limits, factors and descriptions in regulations, standards or other suitable documentation, for example, can help us with this. This can even be automated when the sensor emits ionizing radiation outside the human detection zone, enrichment of gases, or any other emergency -, e.g., gives an alert in case of a virus attack threatening the software or operating system we use. So we can conclude that there are criteria by which our sense of security can be analyzed on an objective basis, obviously only on specific issues. It has been proven so far that the activities learned and practiced by the learned knowledge and experience significantly influence the efficiency and effectiveness of safety-conscious behaviors. It is clear, then, that fundamentally instinctive or emotional-based behavior can be increasingly taken in a conscious direction as knowledge expands.

4 Conclusions, suggestions

The only question left is how to make a general, all-applicable objective sense of security calculation (estimate)? The answer, that it is almost impossible, since the sense of security is almost completely inseparable from the subject, where you live - property relations - social status, - education - level of general and specific knowledge - cultural attachment - etc... However, when some existing danger, threats, risk arises, decision-makers always begin an assessment before taking the interventions that are really needed. In doing so, they determine;

- For what purposes, what forces and means should be used, - How long they must be kept ready and / or operated, - What results are they able to achieve in the given period with the forces and means at their disposal. That is, they designate the privileged elements of the system, determine the expected duration, and determine the lower and upper limits of the response in order to make the system sustainable and operable, adaptable to changes in the environment. In this way, the target level of security is maintained in spite of the expected losses and damages, and the system can be considered stable and predictable.

If anyone is familiar with the concept of system-based security I have formulated, it has already been discovered in the previous lines that I am using only this concept again: *The state of a system, interpreted in relation to one or more designated elements, which can be considered stable and predictable in terms of its components and the relationship between the environment and the system when examined over a certain period of time and within certain limits.* (Hoffman, 2015) In other words, an objective safety assessment can be produced if we manage to omit the emotional charge and perform only professional evaluation. To do this, we need to define limit values, describe processes and systems that we need to regulate. We need to lay down rules, standards, principles, practices between which we can operate and then adhering to them creates a sense of security, the activity that takes them into account can be security-conscious - and truly conscious -. In other words, an objective sense of security can only be (not) measured by taking into account metrics and limits defined by rules and standards, and the same can be said with regard to security awareness. The cybersecurity or information technology standards was made on this base.

The president of the Hungarian Professional Chamber of Personnel, Property Protection and Private Investigators, György Fialka, has been propagating the way to this for a long time with his lecture entitled "*Tasks of Creating Conscious Security."* (Fialka, 2019)

As he writes; "Security can be created as a result of a non-existent and non-exist process, conscious planning, and ongoing resource-intensive maintenance. Safety awareness is a learnable skill, and knowledge is the key to planning optimal defense. It can only be interpreted as a predefined target area. " (Fialka, 2019) With regard to the factors influencing security and the feeling of security, it does not reduce - as I have shown above with regard to criminology or

the United Nations - but expands the number of factors to be taken into account; “Natural risk factors (weather, flood, earthquake, etc.). Environmental risk elements (electro smog, radiation, smoke, heat, etc.) Industrial risk factors (energy supply, installed plants, infrastructure facilities,) Traffic risk elements (vehicles, roads, propellants) Criminal risk factors. (Theft, robbery, extortion, violence, industrial espionage, terror,) Social risk factors. (Because we are on the way to each other. Migration, socialization, religion, culture).

Stress effects as risk elements. .” "(Fialka, 2019) In practice, law enforcement and private security professionals are aware of the specific set of criteria that need to be assessed, analyzed and addressed in order to create security and create a sense of security in each of their activities.

The cybersecurity or information technology standards was made on this base. However, outside of a narrow group of professionals, this should be taught. However, it is not enough to create appropriate normative and other rules and standards for almost every area of life and system of relationships. Somehow we should teach everyone these, which is an exaggerated expectation given the multitude of life situations. The aim can only be to increase the general education of the average citizen through thorough teaching and educational work in this field. The level of awareness does not correlate with the population, the level of education or any other objectively measurable parameter. However, the present experience does not show that general literacy would increase, despite the fact that the availability of information in the XX. it has been growing since the end of the century. Or maybe that's why, people are reluctant to note various things that are uninteresting to them - an emotional relationship! - knowledge. In case of emergencies, sometimes it is possible to turn human behavior and attitude toward some activity more or less toward one goal. Of course, this is not easy to implement, as perhaps one of the most illustrative examples of this was when the evaluation was carried out on a professional basis in Annex II. the future prime minister's staff, which he hopes will take office in World War II. Excluding the emotional relationship, he made a decision, taking into account the material and human sacrifices. The decision to take office as prime minister has been legendary ever since - "I can't promise anything but blood, effort, sweat and tears!" - told the people in a sentence whose members were emotionally attentive to their situation, both individually and nationally. It also shows how impossible it is to separate the emotional relationship from the sense of security and security awareness of individuals and groups.

Resources

Bárdos, G. (2012). A neuronális-, az endokrin- és az immunrendszer (NEI) kölcsönhatásai. Retrieved January 24, 2020, from https://docplayer.hu/15187886-A-neuronalis-az-endokrin-es-az-immunrendszer-nei-kolcsonhatasai.html

Bugovics, Z., & Tóth, P. (2015). *Gazdasági és társadalmi konfliktusok a szubjektív jóllét és biztonságérzet megközelítésében: Tanulmánykötet*. Budapest, Hungary: L'Harmattan.

Fernandez-Juricic, E., Jumenez, M. D., & Lucas, E. (2001, May 3). Alert distance as an alternative measure of bird tolerance to human disturbance: Implications for park design. Retrieved February 25, 2020, from https://www.bio.purdue.edu/people/faculty/faculty_files/publications/36199_1492081880.PDF

Fialka, G. (2019). A Tudatos biztonság létrehozása - ppt letölteni. Retrieved January 30, 2020, from http://slideplayer.hu/slide/17564231/

Herzog, M. H., Kammer, T., & Scharnowski, F. (2016). Time Slices: What Is the Duration of a Percept? *PLOS Biology, 14*(4). doi:10.1371/journal.pbio.1002433

Hoffman, D. (2015, March). Do we see reality as it is? Retrieved January 28, 2020, from https://www.ted.com/talks/donald_hoffman_do_we_see_reality_as_it_is

Papp, A. L. (2012). Biztonság és hatékonyság: a rendészeti (állam)hatalom alkotmányos és társadalmi felfogásának átalakulása a digitális társadalomban. Retrieved January 15, 2020, from http://pecshor.hu/periodika/XIII/papp.pdf

Sagan, C. (2000). *Milliárdok és Milliárdok*. Budapest, Hungary: Akkord kiadó 2000. ISBN 963-7803-74-2 (pp. 36.)

Sallai, J., Bardósz, C., Beregnyei, J., Fórizs, S., Kökényesi, J., Lakatos, G., … Beregnyei, J. (2008). Rendészettudományi szószedet. (J. Beregnyei, Ed.). Budapest: Magyar Rendészettudományi Társaság.

Szabó, L. (2016). A biztonságérzet és a biztonság viszonya (The relation betweeen sense of security and safety security). In *XVIII. Tavaszi biztonságtechnikai szimpozium 2016* (pp. 1-12). Budapest, Hungary: Óbuda university.

Szilágyi, P. (2014). *Jogi alaptan*. Budapest, Hungary: ELTE Eötvös Kiadó. ISSN 2060 5986

Tóth, P., & Horváth, H. (2014). A szubjektív biztonságérzetet befolyásoló tényezők magyarországon. Retrieved January 13, 2020, from https://kgk.sze.hu/images/dokumentumok/kautzkiadvany2014/TothP_HorvathH.pdf

Varga, M., Dávid, M., Hatvani, A., Héjja-Nagy, K., & Taskó, T. (2018). Pszichológia elméleti alapok. Retrieved February 8, 2020, from https://uni-eszterhazy.hu/hefoppalyazat/pszielmal/index.html

Vári, V. (2014, May). Bűnüldözési statisztika a hatékonyság tükrében. Retrieved February 25, 2020, from https://adoc.tips/bnldzesi-statisztika-a-hatekonysag-tkreben.html

Weston, M. A., Mcleod, E. M., Blumstein, D. T., & Guay, P. (2012). A review of flight-initiation distances and their application to managing disturbance to Australian birds. *Emu - Austral Ornithology, 112*(4), 269-286. doi:10.1071/mu12026

OVERVIEW OF THE INTERNET OF THINGS SECURITY RELATED THREATS AND POSSIBLE MITIGATIONS

Gellért Miklós[37]

Abstract

This paper analyses the biggest security issues concerning the Internet of Things, while also giving a high-level overview of the possible mitigations. For this I have compared the different recommendations, frameworks, guidelines and best practices issued by governments, industrial bodies and sectoral non-profit organizations aiming to prevent and mitigate the before mentioned cybersecurity threats. The results showed, that there are several overlapping mitigations, which are included in the different recommendations. The reason is that some of these mitigations are very basic, like protecting the IoT device with secure credentials. Despite this, currently most of the IoT devices are not, or has only minimal mitigations. From a security perspective, this paper emphasizes the need to raise the security level of IoT devices and the need for cybersecurity and privacy standards for IoT devices.

Key words

Internet of Things, IoT, cybersecurity, privacy

1 Introduction

In today's digital age, IoT devices are no more considered to be rare novelties, as there are more than over 23 billion IoT connected devices worldwide. The number of IoT devices are exponentially growing, as the forecasts project the total number of connected IoT devices to amount to 75.44 billion in 20252025 ("IoT: number of connected devices worldwide 2012-2025 Statista," 2012).. Worldwide technology spending on the Internet of Things is estimated to reach $1.2T in 2022 (Colombus, 2018). IoT devices are equally present in the households – as consumer IoT – serving everyday needs as household appliances and gadgets as well as in industrial and agricultural facilities as sensors and smart meters. Connected devices are intertwined more and more with our everyday lives, but as great are the opportunities and benefits, so are the associated security threats as well.

Industry stakeholders and scientists from academic and industrial sectors define IoT differently. For the purpose of the present article, we will use the definition used by the International Telecommunication Union published in their overview, according to which the Internet of Things (IoT) means a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (International Telecommunication Union (ITU), 2012).

2 High level overview of the minimum requirements

a. Easy installation and maintenance

Poorly designed user interfaces and complex installation processes could result in misconfiguration of the devices, which could provide route for adversaries to compromise the device. Therefore, the installation and maintenance of the devices should follow easily

[37]Óbuda University, Doctoral School for Safety and Security Sciences, H-1034 Budapest, Bécsi út 96/b, miklos.gellert@phd.uni-obuda.hu

understandable steps with clear guidance and detailed instructions to users of the device on the configuration (European Telecommunications Standards Institute, 2019) (Department for Digital, Culture, Media & Sport, 2018) (Communications Authority, Hong Kong, 2019). The product should be designed in such a way, that the end user installation and maintenance process has the least possible effect on the security.

b. Default passwords

The proliferation of connected devices in the near future would drastically increase the amount of data produced and would cause severe security and privacy concerns. One such security concern arises from universal default usernames and passwords set by the manufacturer. A weak root password can be cracked by utilizing a dictionary attack, or a brute force attack. A dictionary attack is a form of attack, where the attacking party tries to determine the decryption used by the manufacturer by trying a list of prearranged character combinations. During a brute force attack, the attackers try to overcome the encryption by raw computing force and try to systematically check all possible character combinations in order to find the correct password. This method of attack is computationally much more intensive; therefore, it needs high performance hardware such as modern graphics processing units (GPU). Manufacturers can defend the connected devices against brute force attack and repeated logins by implementing exponentially increasing delays between retry attempts or by blocking the device after a number of invalid login attempts.

The Mirai malware attack in 2016 exploited zero-day flaws, when turned Linux operated connected devices into a part of a larger botnet and used them in large scale distributed denial of service (DDoS) attacks (Wikipedia Contributors, 2019).. The malware scanned the internet for known IP address of IoT devices, and then used a table of commonly known factory default login credentials to log in and infect the devices. The infected devices continued to function normally, except for sluggishness and increased use of network bandwidth resulting from being part of a botnet network.

All the reviewed sources are aiming to enhance device security and mitigate risks associated with no or weak passwords. The most concise wording of this objective is, that all IoT device passwords shall be unique and shall not be resettable to any universal factory default value (European Telecommunications Standards Institute, 2019) (Department for Digital, Culture, Media & Sport, 2018). Unique system-generated passwords or single use passwords are a convenient way to bypass threats arising from weak passwords (The Internet Society (ISOC), 2017). Weak passwords as null or blank passwords should be not accepted, while a password security bar could be an effective way to show the complexity of the password, if there is a visual interface for the users. Manufacturers should follow accepted industry standards and recommendations on password length and character composition. In case the password is stored in a local file on the device, the file should be only accessible and writable by the by the Devices' OS's most privileged account (IoT Security Foundation, 2018). Taking into consideration other threats connected to credentials and access management, password concealment could also be an effective way to prevent password theft.

There are additional methods to further increase device security. Device manufacturers could adopt additional measures to mitigate the risks of the connected devices by implementing elements of strong user authentication (Communications Authority, Hong Kong, 2019), based on knowledge (something only the user knows eg. single use passwords etc.), possession (something only the user possesses e.g. specific electronic tokens provided by the manufacturer) or inherence (something the user is e.g. biometrics). It can be argued however, that strong customer authentication may be inconvenient in a number of use cases, where the additional layer of security would negate the benefits of the connected device. Why would a connected

water heater, a smart air conditioner or a household thermostat need multi-factor authentication anyway? The answer is that even one compromised IoT device can have serious impact on their owners' life and could be used to force them to do something they normally wouldn't do. The various scenarios depend on the nature of the compromised device, but theoretically, a compromised smart lock can be used by an attacker to build a profile of its user and some of the user's habits and determine whether the user is at home (Wurm, Hoang, Arias, Sadeghi, & Jin, 2016).

However, adversaries could use compromised connected devices on a much larger scale. Researchers have previously demonstrated, that an Internet of Things (IoT) botnet of high wattage devices–such as air conditioners and heaters–gives a unique ability to adversaries to launch Manipulation of demand via IoT (MadIoT) attacks on the power grid, which can result in overload, equipment failure, power outages or large-scale black outs (Soltan, Mittal, & Poor 2018)..

c. Software integrity

Adversaries, when successfully compromised a device, often induce small changes in the device's behavior. Integrity monitoring can be used as an effective control to prevent unauthorized third party changes to a device's software. Integrity monitoring is an automated process validating software by comparing the current state to a known, good baseline, which is used to monitor the device behavior, to detect malwares and to discover integrity errors (European Union Agency For Network and Information Security (ENISA), 2017). Monitoring by integrity checking mechanism can be either performed regularly at pre-defined times or randomly. In case the integrity monitoring process detects an unauthorized change in the software, the device should be able to alert both the user and the device manufacturer, while only connecting to networks to perform the alerting function, while all other functions should be disabled (European Telecommunications Standards Institute, 2019)(Department for Digital, Culture, Media & Sport, 2018) (Communications Authority, Hong Kong, 2019). A locally stored known good version of the software would enable safe recovery functions and avoid denial of service attacks.

d. Software updates

Regular and timely update of IoT devices is fundamental in keeping the devices secure. Many IoT device currently do not have the ability to be updated or patched, which can have serious consequences, once critical vulnerabilities became known by adversaries. Different update processes can be applied for different categories of software, as firmware, operating system, services and applications. Software updates should be provided throughout the device lifetime, however manufacturers often decide not to support devices after their end-of-life (Nguyen, 2019), despite the critical vulnerabilities identified by security experts. The user should be clearly notified of the software update period (Department for Digital, Culture, Media & Sport, 2018) and it should be made clear, (i) whether the device is capable of receiving security related updates, (ii) if the device can receive security updates automatically and (iii) what user action is required to ensure the device is updated correctly and in a timely fashion. Device manufacturers should implement safe and secure mechanisms for automated updates, which are independent of any user action. These automatic updates should not modify previously configured user preferences or privacy settings without prior user notification and updated devices should continue to operate during the whole update process. The updates should be verified by a trusted source and encrypted using accepted encryption methods, and has digital signature, signing certificate and signing certificate chain before the update process begins

(European Union Agency For Network and Information Security (ENISA), 2017). Otherwise, adversaries could attack the device with modified update files to gain access and take control of the device. Despite the secure transmission and the applied encryption, no sensitive data should be included and transmitted during the update process.

Constrained IoT devices are usually not designed in a way that would enable software update or security patching. Various design considerations could result in constraints, as cost, physical size, processing power, available power source or data throughput. According to the Internet Engineering Task Force (IETF), a constrained node is "*a node where some of the characteristics that are otherwise pretty much taken for granted for Internet nodes at the time of writing are not attainable, often due to cost constraints and/or physical constraints on characteristics such as size, weight, and available power and energy. The tight limits on power, memory, and processing resources lead to hard upper bounds on state, code space, and processing cycles, making optimization of energy and network bandwidth usage a dominating consideration in all design requirements. Also, some layer-2 services such as full connectivity and broadcast/multicast may be lacking*" (Bormann et al, 2014)

For these constrained IoT devices, manufacturers should make available a clear and transparent replacement plan, detailing a schedule for end of hardware and software support and a replacement date.

e. Securely stored credentials and sensitive data

Manufacturers should ensure that the connected devices guarantee the confidentiality, integrity, availability and authenticity of the credentials and security sensitive information stored within. This is important from two perspectives. Firstly, from an information security perspective, the use of hard coded credentials in the device software shall be avoided, as they pose serious threat to the users of the device as they allow the attackers to gain unauthorized access by reverse engineering and compromise the device. Hard coding is a software development process, where the developers embed data directly into the source code of a software. Secondly, from a data protection perspective, existing and emerging data privacy and protection laws have stringent data security requirements, when it comes to storing personal data. Article 32 of the GDPR[38] – the new European data protection law – formulates one such requirement when requires data controllers and processors to implement appropriate technical and organizational measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

Storing special categories of personal data, as data concerning the health or sex life and sexual orientation of the data subject on connected devices could be prone to hacking and used for extortion by adversaries. There are numerous reports on data leakage from both healthcare (Cybersecurity and Infrastructure Security Agency (CISA), 2017) and adult toy devices (Hay, 2018), which indicates, that these devices and any devices which stores personal data, might be target for hacking attacks. Infringement of the applicable data protection rules may result in significant administrative fines for the manufacturers, beside the reputational damage.

f. Protection of personal data

IoT device manufacturers and service providers are expected to comply with applicable privacy and data protection regulations and therefore process gathered personal data fairly,

[38] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

lawfully and in a transparent manner. The concepts of data protection by design and data protection by default should be followed. Such measures could consist, inter alia, of minimizing the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing and designing IoT devices or applications, which are processing personal data or process personal data to fulfil their task, manufacturers and developers should take into account the right to data protection and implement measures to protect personal data. Such measures could consist, inter alia, of minimizing the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features (REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 2016).

The principle of data minimization requires, that personal data processed by the devices or the applications should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The definition of processing includes storing, therefore devices or applications should store the minimum amount of personal data on the device (IoT Security Foundation, 2018).

Manufacturers and application developers are required by the storage limitation principle to ensure, that their products keep personal data in a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed and have data retention policy available for the users. Personal data that are no longer necessary should be deleted or anonymized.

Lawfulness and transparency of the data procession forbids any unauthorized data process, as passive video or voice recording. Users should have a clear and transparent guidance on how the device shall be setup to maintain the end user's privacy and security and on how to dispose it securely and delete personal data (Department for Digital, Culture, Media & Sport, 2018) (European Telecommunications Standards Institute, 2019).

Communication regarding the data processing should be clear and transparent to the users, in which the manufacturers and IoT service providers describe in a clear, transparent, intelligible and easily accessible form, in plain language the information required by the applicable data protection legislation. The users should be also informed transparently about their rights to information, access, erasure, rectification, data portability, restriction of processing, objection to processing, and their right not to be evaluated on the basis of automated processing.

IoT devices – especially consumer IoT devices – just as smart phones or computers often change ownership or provide temporary service to a number of users. In these cases, the manufacturer or the IoT service provider should provide an option, which enables the user to delete all processed personal data from the device, while the device retains its function (European Telecommunications Standards Institute, 2019) (Her Majesty's Government Department for Digital, Culture Media & Sport, 2018), such as a factory or master reset function.

g. Secure communication

Connected devices, which form the Internet of Things, are connected for a reason, as they are producing, storing and exchanging data with other devices, or central servers. Therefore, security sensitive data should be encrypted at all times, including transition on networks, as the internet (European Telecommunications Standards Institute, 2019) (Department for Digital, Culture, Media & Sport, 2018). The encryption used in the device should be appropriate to the properties of the technology and usage. However, even a minor flaw in the communications architecture can result in a compromised device, which is unacceptable in safety-critical

environments (Department for Digital, Culture, Media & Sport, 2018). Devices operating in critical infrastructures, such as healthcare, should use state of the art, standardized security protocols, such as Transport Layer Security (TLS) for encryption (European Union Agency For Network and Information Security (ENISA), 2017). Currently TSL is one of the most widely used cryptographic protocol to secure data, but there are other widely recognized and used standardized security protocols as well.

h. Minimize exposed attack surfaces

Device manufacturers should apply information security and computer science principles, as the principle of least privilege (PoLP), when designing connected devices. PoLP is a basis of security engineering, as it requires that every module must be able to access only the information and resources that are necessary for its legitimate purpose. This principle should be applied during the design phase of the device, resulting in devices that run on minimum requirements, thus enhancing the protection of data and functionality of the device. Practically it means that no extra ports or hardware slots should be built into the device, if they are not needed for the operation and maintenance. Every unused port must be closed and only essential network interfaces should be open for access. Components of the IoT device, as camera, microphone or loud speakers should be disabled by default (Communications Authority, Hong Kong, 2019). Services should not be available if they are not used and code should be minimized to the functionality necessary for the service to operate (European Telecommunications Standards Institute, 2019) (Department for Digital, Culture, Media & Sport, 2018). Software and applications should run with the lowest privilege level possible (European Union Agency For Network and Information Security (ENISA), 2017).

i. Resiliency

Connected devices and IoT systems have an increasingly important role, in which the device should be running even in case of network loss or system failure. Such use cases could be health or safety related devices, where system failure means serious health or safety hazards for the users. An example could be a smart lock that turns off because of loss of network connection. The resiliency of the devices should be appropriate for their intended use and the relying systems. Power outage, sudden loss of data or network connection are just some of the threats, which should be mitigated by the implemented resilient measures. As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power. Devices should be able to return to a network in an expected, operational and stable state and in an orderly fashion, rather than in a massive-scale reconnect (European Telecommunications Standards Institute, 2019) (Department for Digital, Culture, Media & Sport, 2018). Manufacturers should implement suitable testing processes, which could verify the functions and features of the devices under duress, during recovery and during normal operations (Communications Authority, Hong Kong, 2019)(Boeckl et. al., 2019).

j. Examine system telemetry data

IoT devices collect and process telemetry data including usage and measurements and user related data. For example, adversaries could use a compromised smart meter to send false telemetry data to launch a false data injection attack (FDIA) on the power network. Another example would be a compromised industrial smart meter, which could communicate significantly higher falsified usage data resulting in higher costs for the user. Manufacturers and

IoT service providers should implement monitoring measures to examine telemetry data for anomalies (e.g. unscheduled transmission of data or extreme value measurements). If the security evaluation identifies unusual circumstances, a mitigation process should be executed in order to minimize security risks (Cyber Security for Consumer Internet of Things, n.d.) (Department for Digital, Culture, Media & Sport, 2018) (Communications Authority, Hong Kong, 2019). Users should have knowledge and information on the telemetry data collected by the device.

k. Vulnerability report

Industrial bodies, IoT device manufacturers and service providers should provide public vulnerability disclosure points, with the appropriate processes, systems and policies to receive, track and promptly respond to external vulnerability reports from third parties, including but not limited to users, academia and the research community. Knowledge about a security vulnerability allows manufacturers and providers of IoT service should act as soon as practicable to minimize the adverse impact brought about by the disclosed vulnerabilities. This is especially important as certain vulnerabilities, as hardware related ones are much more time consuming to fix. Additionally, companies should implement means to monitor and identify previously unknown vulnerabilities. Device users and industry professionals can be involved in the process, by bug bounty programs or crowdsourcing methods (The Internet Society (ISOC), 2017), which is a common practice that is used by biggest companies in the industry.

j. Conclusion

The rapid development and innovation of the IoT sector pose specific challenges for the countries and the national regulators. Privacy and security are among the biggest concerns regarding IoT as there are growing fears that individual users will become more and more transparent for manufacturers and IoT service providers alike, while they lose control over the data. Users often considered to be the weakest link in the chain, as they lack technological understanding and are not aware of the risks associated with information technology. The usage of IoT devices creates previously nonexistent attacking scenarios, where adversaries could exploit vulnerabilities to gain control over or manipulate the systems. User's security awareness is an important factor, but it is not enough in itself to mitigate security and privacy risks, especially in case of poorly designed IoT devices or services. Therefore, the responsibility should fall on the shoulders of the manufacturers and developers to design and produce secure devices and applications for the users. Unfortunately, many manufacturers and developers simply overlook or just not aware of the risks during product development and pressurized to launch new products to out-innovate or simply outgrow competitors in a rapidly growing market and thus commercial goals dominate security considerations.

Currently, most of the national frameworks are only covering parts of the IoT ecosystem from different perspectives, such as privacy and data protection, consumer protection or information security, but there are no legislative instruments detailing the specific information security minimum requirements. There are non-binding guidelines, frameworks and best practices developed by industry bodies and non-governmental organizations, but so far governments stayed away from the topic. However, more and more governments realize the importance and the possible benefits of the Internet of Things, which encourages them to regulate the field. A good example would be the above review Secure by Design Report issued by the UK government. It fits into the wider strategy to regulate the IoT ecosystem, while it was developed after thorough consultation industry, academia, and civil society more broadly, and international partners. Its recommendations are largely the same as those issued by ETSI, which

shows, how industrial bodies could influence national legislative processes. There is also noticeable international interaction and cooperation around the world. For the first, the Code of Practice issued by the Hong Kong Communications Authority would be a good example, which builds upon the recommendations formulated by the UK Secure by Design Report and also the relevant industrial guidance and frameworks. For the second, a good example would be how countries monitor other countries regulatory actions. Germany banned smartwatches aimed for children based on security and privacy concerns, after the Norwegian Consumer Council (NCC) reported the issues.

As more and more countries will enact binding legislative instruments to regulate IoT security, others will follow. This trend could lead to different mandatory applicable security standards in different jurisdictions, rising the overall security of the IoT devices and services at the expense of the fragmentation of the IoT industry. One of the problems with binding legislative actions in the technology sector is, that if a legislative instrument is too specific, it could quickly became obsolete, while if the wording is too high level or general, then it could miss its intended purpose. The other problem is that introducing a new legislation from a draft is a time consuming process, with preparatory debates, committee readings and public consultations, which could result in that the legal framework will lag behind the rapid technological advancement. However, as the proliferation of inadequately protected IoT devices continues and threats to the safety and privacy of users continue to exist, security considerations must be taken into account, whether through governmental pressure or industry incentives.

Resources

Bormann, C., Ersue, M., & Keranen, A. (2014). Terminology for Constrained-Node Networks. *Internet Engineering Task Force,* 1-17. doi:10.17487/rfc7228

Columbus, L. (2018, December 18). 2018 Roundup Of Internet Of Things Forecasts And Market Estimates. Retrieved October 10, 2019, from https://www.forbes.com/sites/louiscolumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/#e93985a7d838

Communications Authority. (2019). *Code of Practice on the Operation and Management of Internet of Things Devices.* [PDF]. Hong Kong: Communications Authority.

Cyber Security for Consumer Internet of Things. (n.d.). Retrieved January 14, 2020, from https://itlaw.wikia.org/wiki/Cyber_Security_for_Consumer_Internet_of_Things

European Union Agency for Network and Information Security. (2017). Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures. doi: 10.2824/03228

IoT Security Guidelines for IoT Service ecosystems. (2019). Retrieved from https://www.gsma.com/iot/wp-content/uploads/2019/10/CLP.12-v2.1.pdf

Hay, M. (2018, October 15). How Companies (And Hackers) Can Cash In On Smart Sex Toy User Data. Retrieved October 2, 2019, from https://www.forbes.com/sites/markhay/2018/10/15/how-companies-and-hackers-can-cash-in-on-smart-sex-toy-user-data/

Wikipedia Contributors. (2019, April 7). Mirai (malware). Retrieved from Wikipedia website: https://en.wikipedia.org/wiki/Mirai_(malware)

Department for Digital, Culture, Media & Sport. (2018). Secure by Design Report Secure by Design: Improving the cyber security of consumer Internet of Things Report Secure by Design Report 1. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775559/Secure_by_Design_Report_.pdf

IoT: number of connected devices worldwide 2012-2025 | Statista. (2012). Retrieved from Statista website: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

International Telecommunication Union (ITU). (2012). Overview of the Internet of things. Retrieved October 26, 2019, from ITU website: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

IoT Security Foundation. (2018). IoT Security Compliance Framework. Retrieved November 19, 2019, from iotsecurityfoundation.org website: https://www.iotsecurityfoundation.org/wp-content/uploads/2020/05/IoTSF-IoT-Security-Compliance-Framework-Questionnaire-Release-2.1.zip

Wurm, J., Hoang, K., Arias, O., Sadeghi, A.-R., & Jin, Y. (2016). Security analysis on consumer and industrial IoT devices. 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC). https://doi.org/10.1109/aspdac.2016.7428064

Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K. N., Nadeau, E., … Scarfone, K. (2019). Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks. https://doi.org/10.6028/nist.ir.8228

Nguyen, T. (2019, October 03). Multiple D-Link Routers Found Vulnerable To Unauthenticated Remote Code Execution. Retrieved August 25, 2020, from https://www.fortinet.com/blog/threat-research/d-link-routers-found-vulnerable-rce

The Internet Society (ISOC). (2017). IoT Security & Privacy Trust Framework v2.5. Retrieved from https://www.internetsociety.org/wp-content/uploads/2018/05/iot_trust_framework2.5a_EN.pdf

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (2016).

Soltan, S., Mittal, P., & Poor, H. V. (2018). BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid. Retrieved August 25, 2020, from www.usenix.org website: https://www.usenix.org/conference/usenixsecurity18/presentation/soltan

Cybersecurity and Infrastructure Security Agency (CISA). (2017, September 17). Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump Vulnerabilities (Update A). Retrieved November 18, 2019, from us-cert.cisa.gov website: https://www.us-cert.gov/ics/advisories/ICSMA-17-250-02A

THE USAGE OF THE OPEN-SOURCE PLATFORM ARDUINO TO TEACH IOT

Peter Procházka[39]

Abstract

The contribution deals with the use of the open-source Arduino platform, based on the ATMega microcontroller from the Atmel company and a graphical development environment based on the Wiring environment in the development of a specific device. It represents the whole process of design, construction, programming and testing, taking into account the possibilities of teaching, as well as creating a specific product for a specific business plan. Using this technology, it is relatively easy for students to approach the IoT area.

Key words

Arduino, IoT, Wiring, smart home,

1 Introduction

The Internet of Things (IoT) is now widely known to the general public and is generally used to refer to any device connected to the Internet, where each device can communicate with others via the Internet and store feedback information to a central node. The history of IoT is debatable, no one can tell for certain where and when it started, but today we see it in everyday life in the form of smart phones, computers and we can also find it in smart refrigerators, or in the home, for example, simply turning on the lights. Basically, if something works on electricity, it can be connected to the web. To sum up, the Internet of Things is now being found from households to all sectors of the economy and is still expanding as more and more companies realize the great benefits of this technology.

With the increasing availability of faster and more reliable broadband, many devices will be equipped with a standard WiFi connection. The Internet of Things is already penetrating our daily lives and changing our habits. Cars are able to sync with appointment and scheduling calendars, and smart assistants turn shopping into conversations.

So far, the most engaging application of the Internet of Things can be found in an industry where artificial intelligence (AI) is fundamentally changing ways of doing business. Smart cities help reduce waste and energy consumption, and manufacturers can improve the production process and the entire logistics. Several different sensors help in monitoring production processes, early detection of errors, etc.

IoT devices also have many uses for consumers. We can use smart TV to share, for example, videos from our mobile phone. But the house can also be connected to a mobile phone for other reasons. For example, it can be used as a remote control and user interface to adjust heating, heat recovery, fire warning, or to control lights, dim-outs, or other devices.

The scope of the Internet of Things is constantly expanding, and smart home assistants are experiencing a literal boom. It is for this reason that we decided to create a teaching tool, through which students can get acquainted with this issue and transform their knowledge into practice.

[39] University of Economics in Bratislava / faculty of Economic Informatics, department of Applied Informatics, Dolnozemská cesta 1/b, 852 35 Bratislava 5, Slovakia, e-mail peter.prochazka@euba.sk

2 Selected technology

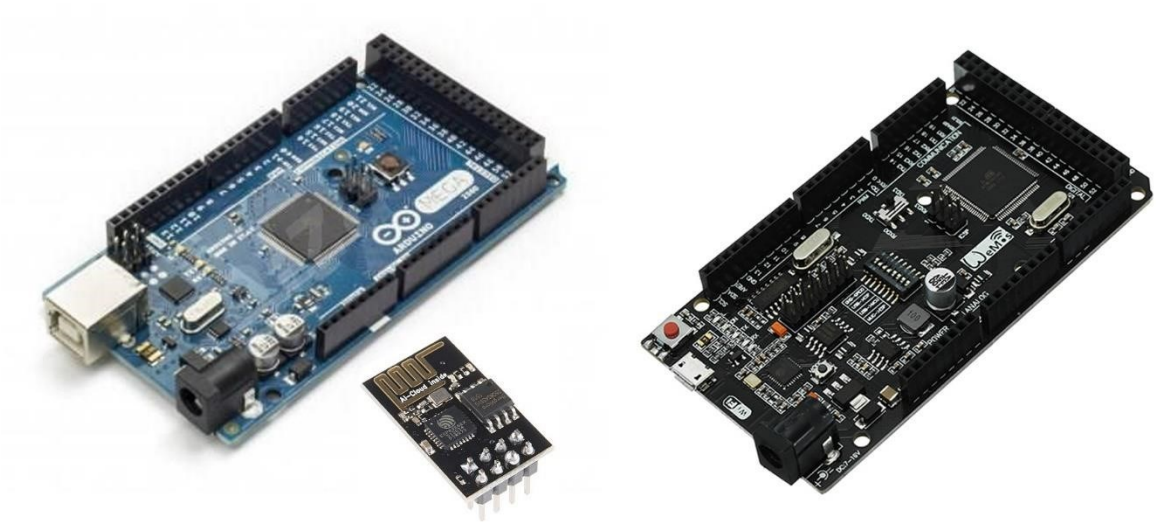
Arduino is an open-source electronic platform based on Atmel's ATMega microcontroller and a graphical development environment based on the Wiring platform. This platform was created at the Ivrea Interaction Design Institute as a simple tool for rapid prototyping aimed at students without deeper knowledge of electronics and programming. Using Arduino, it is possible to read inputs from various sensors, send messages, display measured data, or activate them on the device outputs, set their values, or publish them on a suitable operator interface.

Thanks to these features, this platform has attracted a lot of fans who bring new ideas and solutions every day, which also makes it easier for beginners to develop their devices. A very rich source of information is the website arduino.cc (Team Arduino, 2020), which is a homepage of all Arduino enthusiasts, interested people will find a lot of tutorials, training, community forum and last but not least, Arduino IoT Cloud, whose use could be a continuation of this project. This project is also inspired and draws on a wealth of published ideas.

From the point of view of students' teaching there is a lot of literature available in English, but also two very good publications in Czech. The first is: "Arduino – Uživateľská příručka" (Selecký, 2016) and the second, which is additionally free to download in pdf format, is: "Průvodce světem Arduina", 2nd edition (Voda, 2017). These publications have also served in the development of the teaching aid.

As Arduino became a phenomenon among developers, it began to change to accommodate new needs and challenges, offering a variety of clones from simple 8-bit boards to products for IoT applications. In this work, we experimented with the Arduino Mega2560, which we connected with the WiFi module ESP8266-01 and the WeMos board, which includes both of these devices on a single board (Fig. 1).

Fig. 1: Arduino Mega2560, ESP8266-01 and WeMos Arduino MEGA2560 with built-in WiFi ESP8266



Source: own archive

The big advantage is also the development environment, which works on various operating systems from Windows OS, through Mac OS to Linux. For complete beginners, there are even puzzles-like development environments that enable even a child learn to program Arduino easily. In addition, the open-source platform allows you to create your own Arduino clone with additional modules to create a target device, which can significantly reduce project

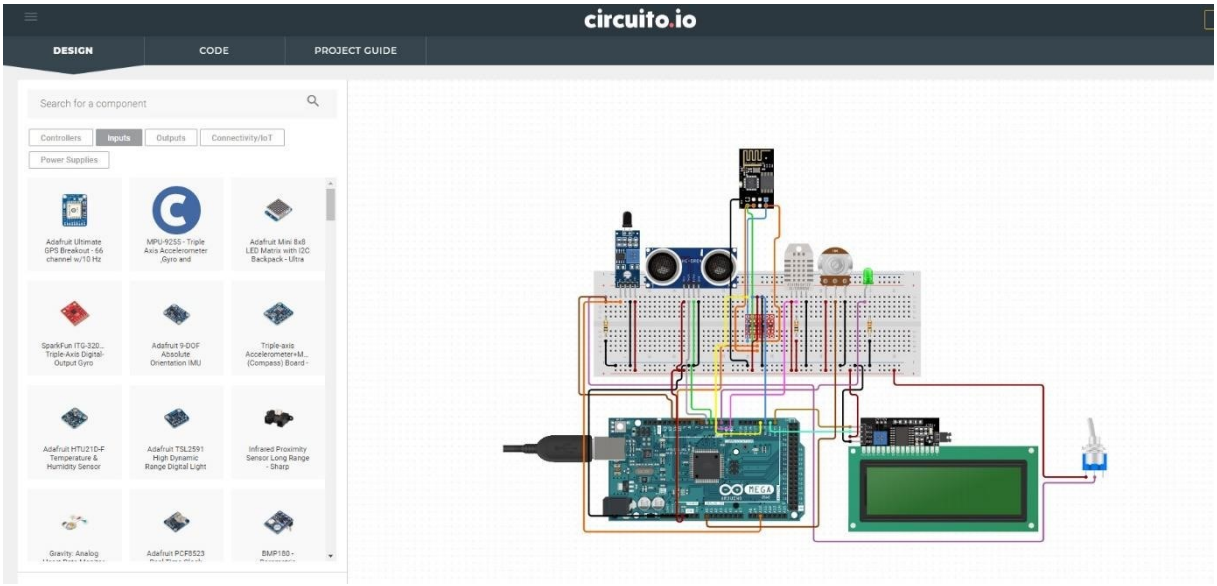
costs. But even if the developer will use Arduino, or its countless clones, it will still be a very cheap platform, costing a few tens of euros at the most.

3 Device development

To develop the teaching tool for IoT, we used the online development environment on the domain https://www.circuito.io/ (Team CIRCUITO.IO, 2020). to test its advantages and the possibility of its use in further expansion with new modules. Working with it is very simple. The user only chooses the type of Arduino and from the number of available modules he chooses the ones he wants to use. For demonstration for the purposes of this article (Fig. 2) the following modules have been added to the Arduino Mega2560:

- Infrared flame sensor
- ultrasonic sensor
- humidity and temperature sensor
- rotary potentiometer
- green led diode
- lcd display 20x4 I2C
- power switch
- WiFi ESP8266-01

Fig. 2: Circuit diagram display created on circuito.io

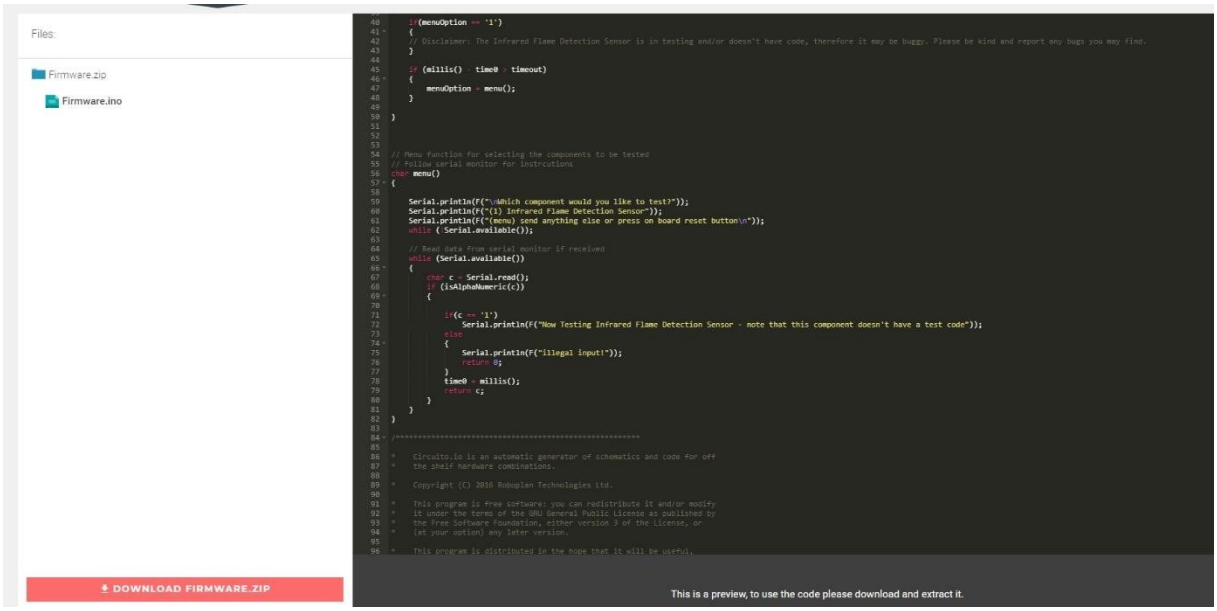


Source: https://www.circuito.io/

We designed the learning tool to be variable and easy to change and add modules, so the software contains parts of the code for more of them. By simply uncommenting and loading the code to Arduino and connecting the module, it becomes functional.

The online development environment is also very helpful in creating sample codes, as it immediately creates sample code for each added module that a person simply downloads and edits with the Arduino IDE. (Fig. 3)

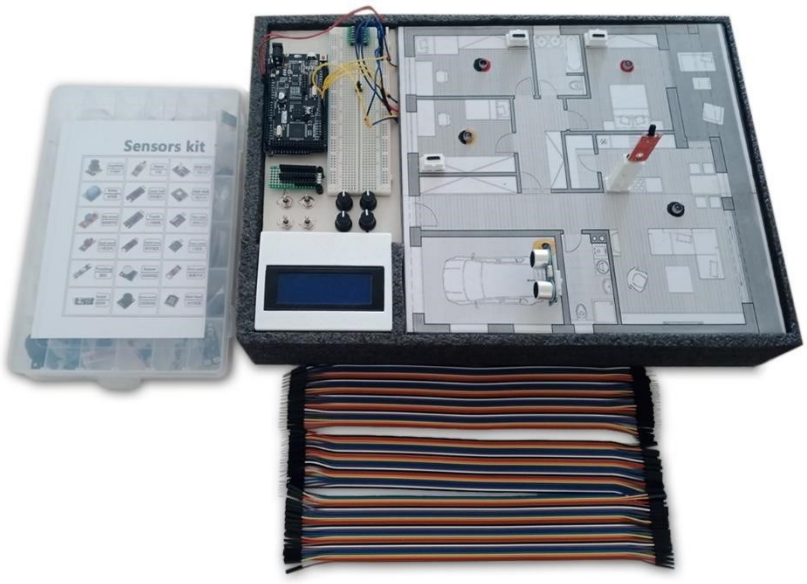
Fig. 3: Sample code display generated on circuito.io



Source: https://www.circuito.io/

We have designed the prototype of the teaching aid itself (Fig. 4) to show a plan view of an imaginary house with an LED in each room. They are lights that can be controlled remotely via a web interface or also switched using a sensor in automatic mode. They can be supplemented with other elements such as various motors, relays, solenoids, etc. A 20x4 I2C LCD display is also added to the set to add functionality.

Fig. 4: Prototype of the teaching tool

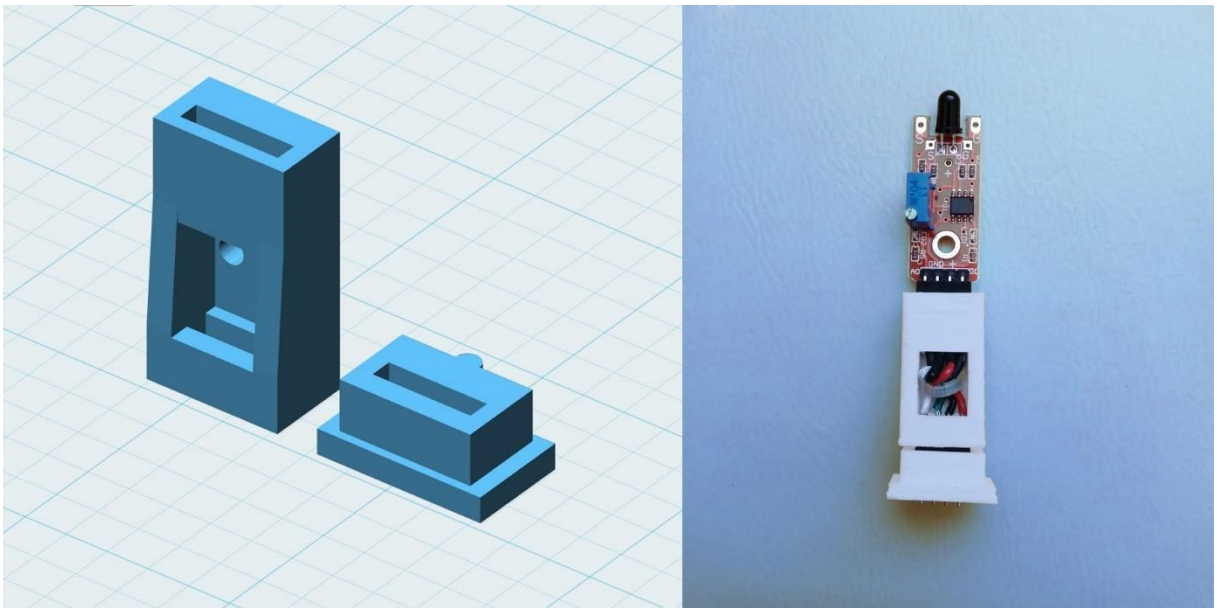


Source: own archive

To simplify the work with sensors or other input devices, we created a universal connector (Fig. 5) using 3D printing consisting of a socket, which has power terminals connected to 5V and GND and the rest are connected either directly to Arduino or via breadboard. Since most input devices have 3-4 pins, the top of the connector is always equipped with 4 pin female headers that are wired to a 4 pin male header for a specific sensor so that they can be plugged into the socket, and 5V and GND are always on the same place. This adapter must be used precisely because the terminals of the different sensors are in different order. For routine testing, 10K OHM linear potentiometers can be used instead of sensors.

In order to distinguish which sensors, LEDs, potentiometers or switches we connect, the rooms are marked with a color code that corresponds to the color codes on the connecting cables, the color of the cables for sensors, LEDs, etc. is also color-coded, so that it is always clear what module we are linking to Arduino. The cables that we do not currently use are hidden under the board, which represents the floor plan of the house. Permanent connections that do not change, such as power or display connections, are routed through the bottom and soldered to Arduino, or an auxiliary printed circuit board.

Fig. 5: Universal connector



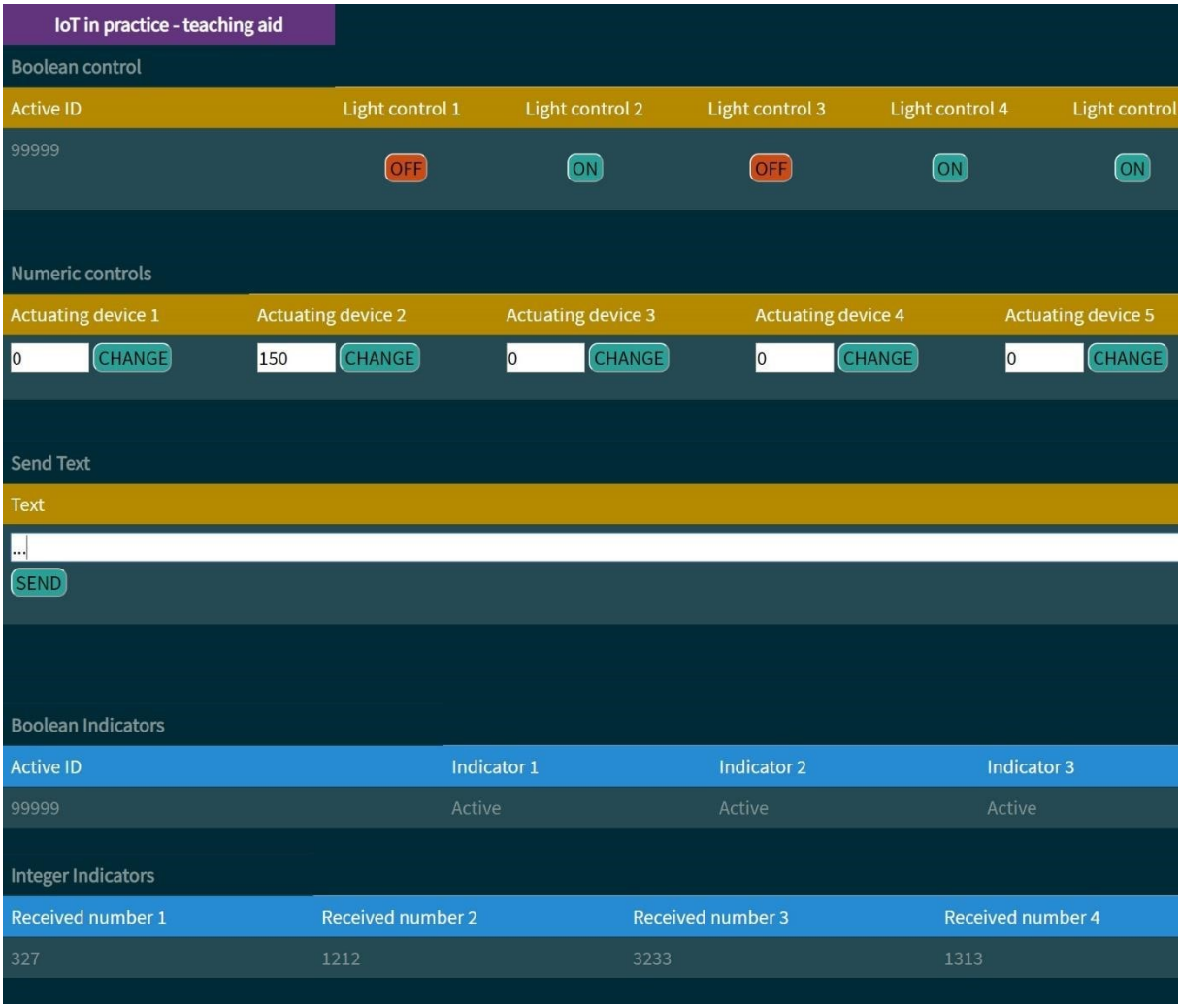
Source: own archive

Some modules do not use 5V for their power supply, but only 3.3V. For this reason, we have added another female pin header that is linked to this power supply on the Arduino board. A typical example of such a module is WiFi ESP8266-01. If it was connected incorrectly and 5V was applied instead of 3.3V, it would be damaged.

In order to control and monitor the learning tool wherever there is an internet connection, we have created a simple PHP website using MySQL, which records sensor values and displays them in the "operator panel" while it also enables setting up devices, switch on or off and also send a message to the lcd display (Fig. 6).

To connect to the database, a simple database_connect.php file is created, in which we must enter the database server address, user name, password, and database name. This information is usually obtained from the hosting provider for our domain. Depending on the location of the teaching aid, we need to change the Arduino file, where it is necessary to define the WiFi SSID and its password.

Fig. 5: Web *interface* – control panel



Source: own archive

4 Conclusion

Nowadays, there are many technologies that are part of the Internet of Things, such as self-driving cars, smart homes, smart cities and various artificial intelligence applications. They simplify our lives and bring us luxury, but at the same time they are becoming a threat to Internet security. Many devices have default passwords that cannot be changed because these devices have only basic controls, but no interface to change settings. Such elements of the Internet become a potential back door to the entire local network to which they are connected. Tighter regulations and tighter security controls will play an important role in our future of the Internet of Things. There are also ethical questions about the use of IoT. The more devices we use for our activities, the more sensors that will monitor our ways and habits, the more privacy will be compromised.

In any case, the Internet of Things is becoming an integral part of our everyday life and needs to be addressed, hence we have created this learning tool to help students try out different

input and output modules, discover weaknesses and imperfections, design new solutions and investigate their impact and threats on users themselves.

Resources

Arduino. (24.3.2020). *Arduino.* Retrieved from: Arduino: https://www.arduino.cc/

Selecký, M., & Herodek, M. (2016). Arduino: Uživatelská příručka. Brno, Czech Republic: Computer Press.

Team Arduino. (2020). Arduino. Retrieved February 24, 2020, from https://www.arduino.cc/

Team CIRCUITO.IO. (2020). How to wire to Arduino Mega. Retrieved April 13, 2020, from https://www.circuito.io/app?components=512%2C11061

Voda, Z. (2017). *Průvodce světem Arduina.* Bučovice, Czech Republic: Nakladatelství Martin Stříž.

Notes

ISBN 978-963-449-206-1