Gamification of cyber ranges in cybersecurity education

Martin Jelo* and Pavol Helebrandt*
* Slovak University of Technology, Institute of Computer Engineering and Applied Informatics, Bratislava, Slovakia
xjelo@stuba.sk, pavol.helebrandt@stuba.sk

2022 20th International Conference on Emerging eLearning Technologies and Applications (ICETA) | 979-8-3503-2033-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICETA57911.2022.9974714

***Abstract*—There is a lack of cybersecurity experts, and this problem is getting worse with the increasing number and importance of IT systems together with rising number and sophistication of attacks. Rapid development in cybersecurity necessitates constant training and practice to keep up with the latest threats. Studying IT, and especially cybersecurity is considered difficult and there is an urgent need to encourage interest of students in this field. One promising avenue to improving the situation is gamification. Gamification has been used in education to improve enthusiasm of students, increasing their numbers, information uptake and retention. Leveraging social connections and human competitiveness can further motivate students to take part and engage in the learning activities they would otherwise not consider. Virtualized environments offer means to scale up the practical training as well as share latest teaching methods. Cyber ranges used by educational institutions often are such open platforms that provide such practical cybersecurity training. Moreover, with some thoughtful planning they can prove to be popular serious games. In this paper, we explore opportunities for hands-on cybersecurity education by using gamified scenarios in cyber range virtualized environment. We focus on cyber testing environments, what their types are, and what it includes. We place emphasis on creating basic game scenario close to real-world situations.**

***Keywords*—cyber range, cybersecurity education, virtual learning technology**

I. INTRODUCTION

There is a plethora of information freely available on the Internet on almost any topic including cybersecurity information and tools. The lowering of access bar has both positive and negative effects. Those motivated can acquire knowledge to defend complex IT systems, or how to attack them. Readily available tools and techniques to bring down systems or networks, combined with the consequences of those attacks in the real-world necessitate growing budgets dedicated to defense of these systems. To keep the ever-increasing number of IT systems functioning and protected, training more cybersecurity professionals is unavoidable.

A proper environment is needed for the training for the students and to make sure they can experiment in a safe environment. Cyber ranges were long used by industry for training and testing in isolated training networks, but they were expensive and unavailable to majority of schools and universities. Utilizing advances in virtualization, containerization, orchestration and provisioning, cyber ranges can be created more cheaply and easily. In these environments, the students can safely learn how attacks against many services work and how to defend against them.

The main contribution of this paper is a fully functional scenario for cyber range with gamification elements for teaching offensive cybersecurity and penetration testing techniques.

The rest of this paper is organized as follows. In Section 2, we discuss the current state of the art in cybersecurity training. Section 3 provides overview of cyber ranges and their taxonomy. Game scenario design is presented in Section 4, with Section 5 providing its verification and test results. Conclusions and future work are discussed in Section 6.

II. STATE OF THE ART

Cybersecurity education is gaining importance in all aspects of life. As such, it can cover a vast and various spectrum of information and skills depending on position and responsibilities. In this section, we address them from simplest cybersecurity awareness - necessary for all, moving on to more specialized knowledge and corresponding tools required by cybersecurity professionals.

A. Cybersecurity Awareness

If we want to secure people or make them feel secure in digital infrastructure, we need to train them, so they understand what they need to do in security management. They must know what threats can appear on the internet. However, they must know what they are talking about, know both theoretical principles of threats and practical skills in defense against them. If we train these people and make a new generation of professionals in cybersecurity, we can rely on them to know what they are talking about. These professionals can further lead or manage the team of cybersecurity specialists and work on, e.g., penetration tests for companies or red team attacks on companies. These people can protect companies and even people in society.

B. Methodology for Cybersecurity Education

The education methodology represents an essential role in the teaching process. When a teacher can motivate their students, to arouse their interest in the topic, they fulfil their purpose. However, how to motivate more students and not just a few of them? One education method particularly suited for cybersecurity is gamification.

According to [1] *Gamification* is the use of game mechanics and game thinking to engage users in solving problems and motivate them by introducing elements of

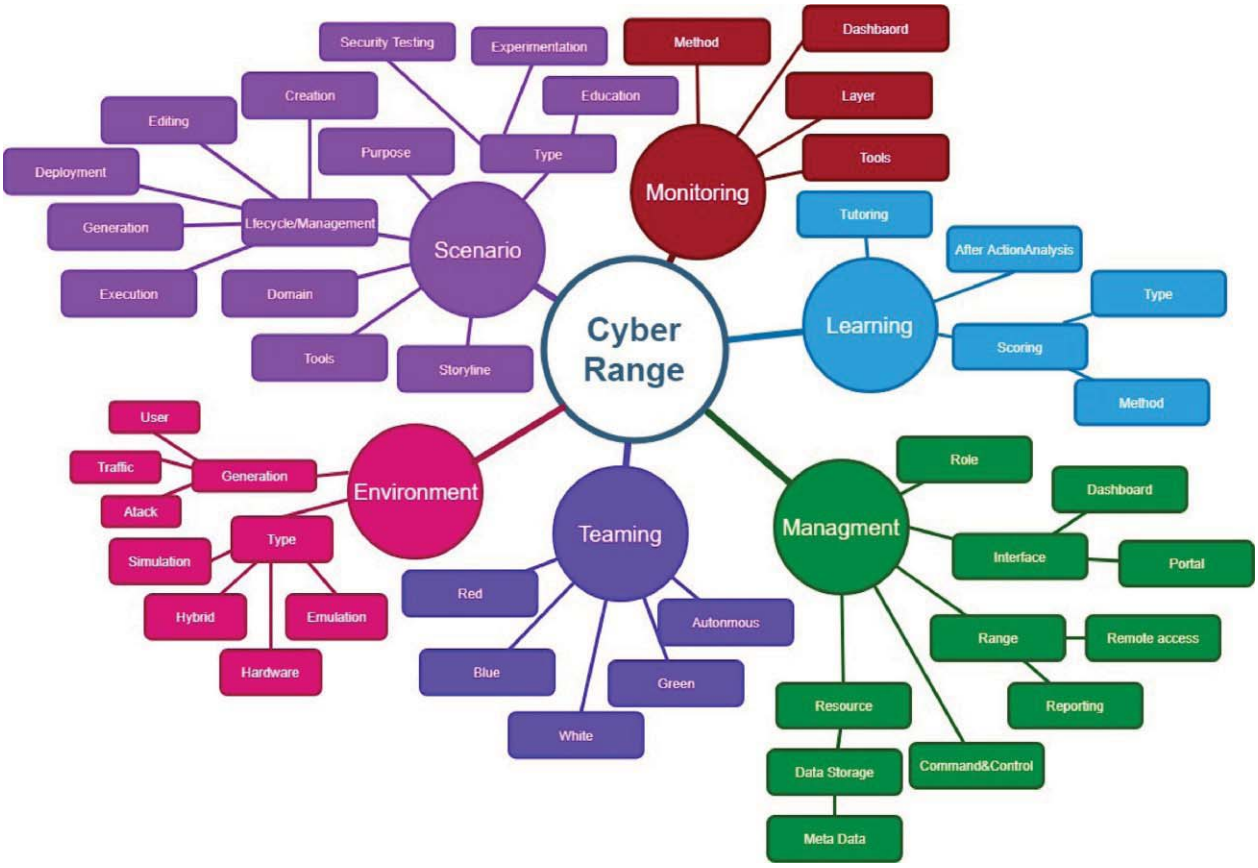


Figure 1. Cyber range taxonomy [6]

competition and reward. Many people are competitive and try to perform better, as some rivalry motivates them to challenge themselves. Furthermore, the concept of gamification can be applied in cybersecurity learning or training. This concept makes it great for learning new ideas and techniques for beginners in this field. If competitive elements along with fun are added to the learning platform, it becomes more enjoyable and brings the spirit of learning [2]. Through gamification, trainees can obtain the appropriate practical skills and the corresponding to an incident or a special cyber-attack occasion [3].

Students remember only 10% of what they read; 20% of what they hear; 30% of what they hear, if they see visuals related to what they are hearing; 50% of what they hear, if they watch someone do something while explaining it; but almost 90% if they do the job themselves, even if only as a simulation [4]. This approach is good to use because, in the cybersecurity field, there are a lot of programs and tools that students must know and use. Some of the tools we can mention are Nmap , Metasploit , Burp Suite and many others.

C. *Capture the Flag*

A cybersecurity CTF is a competition between security professionals and/or students learning about cybersecurity [5]. The key component in this type of competition is to find a flag. The flag is often hidden from the user and can be obtained after successfully completing the specific challenge. The flag can be anything we can think of, but in cybersecurity, this is often a text file, which indicates that the user has found the flag. This principle might feel easy for anyone; however, we should keep in mind that time is one of the most factors that can affect a player's actions when it comes to the competition.

The most common types of CTFs are: *Jeopardy*- teams have to solve a set of challenges from areas such as Cryptography, Forensics, Reverse engineering, or anything else; *Attack-Defense*- some teams try to attack, and the other teams try to defend from attacks; *Mixed Competitions*: change formats [2].

Cyber challenges, code sprints and other gamified activities and competitions hold enormous promise in both the public and private sectors and can be used in all phases of the employment lifecycle [7]. These activities have become more prevalent in recent years and some of the most popular online cybersecurity games are *TryHackMe*, *HackTheBox*, and *picoCTF*.

III. RELATED WORKS

Best learning results are achieved with practice, and gamification of learning through cyber ranges makes the practical learning of cybersecurity more engaging.

A. *Cyber Range Overview*

There are a lot of definitions that can describe, what a cyber range is, what it contains and what it should provide. One of the many definitions is by NIST, describing cyber range as "*interactive, simulated representations of an organization's local network,*

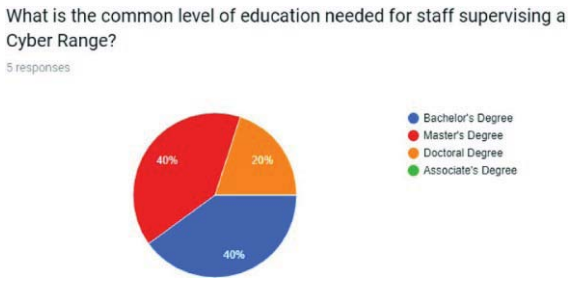


Figure 2. Education required for staff supervising a cyber range [8]

system, tools, and applications that are connected to a simulated Internet level environment." Another description of cyber range says it is just a realistic environment for cyber warfare training. These definitions may vary in some respects, but the essence is the same.

Use of cyber ranges and research in this topic is growing in cybersecurity training. They seem to offer more opportunities than just a regular CTF game. However, a cyber range can have aspects of CTF. It all depends on how the cyber range is implemented and what it can offer. Cyber ranges provide a great opportunity to simulate different scenarios, teach students and sharpen their skills, and for professionals, to strengthen their security team and try to replicate the real-world scenario for attack-defense. Cyber ranges seek to provide high-fidelity simulations of realistic networks to present practical scenarios for teams [9].

Although we provide a reason for individuals to use cyber ranges, in a way that cyber ranges are developed, their main aim is on red-blue teaming. In Chouliaras et al. [11], 10 cyber ranges were surveyed about their focus in cybersecurity, 7 out of 10 cyber ranges selected the option for red or blue teaming. The next most voted option was the SCADA system. The paper ascribes this due to the incidents at Iran's nuclear program and attack on the Ukraine power grid. While CTF is a great way for students to improve and maintain learned skills, only 2 cyber ranges have environment for this type of challenge.

Cyber ranges can be categorized in terms of their deployment. *Simulation* - recreates the core traits of a security scenario, it does not need to be in a virtual machine, it simulates the main activity of e.g. server. *Emulation* - to mirror a production network, this can be a real software that operates in e.g. web server, mobile app, *Hybrid* - combination of the previous two types. [10]

Papers [12, 13] also describe types of cyber ranges, but they might have slightly different naming convention. We should note that in some papers on cyber ranges, authors have described emulation type as a hybrid type of cyber ranges, Additionally, some authors do not distinguish between these types of cyber ranges or define them vaguely.

In [6], Yamin et al. present a new taxonomy for classification of cyber ranges, which can be seen in a Figure 1. Each cyber range can have different goals. This taxonomy provides a complex insight into cyber range, based on 6 main concepts – *scenarios*, *monitoring*, *learning*, *management*, *teaming*, and *environment*.

Cyber range can be focus on just one, a few or can try to cover all points of the taxonomy. However, this can be a difficult as complexity rises excessively. Identifying targets, setting goals and expectations in managing a cyber range accordingly is necessary.

Darwish et al. [8] surveyed educational cyber ranges about their experience with the new technology in teaching cyber security. While it should be highlighted that the survey had responses only from 5 educational institutions, it represents universities' perspectives and experiences on managing cyber range. They discovered that more than half of educational cyber ranges surveyed required supervising staff with at least a Master's degree, as shown in Figure 2. It reflects varying complexity of cyber ranges based on the goals. This can also be result of required knowledge for managing cyber range - cyber security, computer networks or at least the basics of computer science.

B. Game Scenarios

Game scenarios design and implementation need to be specified with respect to the goals and modified for specific audience where possible. Games started as simple and mostly static, which limited their scope and flexibility. More complexity and dynamic elements were included later. This shows an advancement in the specification and execution of scenarios in cyber ranges. According to Yamin et al. [6], these dynamic components change the environment and make the scenario more realistic.

Another approach to flexible games is automatically creating randomized scenarios, as outlined by Schreuders et al. in [14]. They present Security Scenario Generator (SecGen) – a modular framework to create *rich-scenarios* by generating a random number of virtual machines with random vulnerabilities. These scenarios are preconfigured with everything needed, e.g. scenarios can contain multiple virtual machines, random vulnerabilities in systems, configuration vulnerabilities, network configuration, anything like that. This approach is helpful when teaching students how to exploit different vulnerabilities, get system privileges on these machines or make a CTF competition for students. It also limits opportunities for students to find out the scenario write-up on the internet and defeat the purpose of the teaching method.

When planning a cybersecurity game, scenario introduction, tasks and its interconnection with the overall storyline can be crucial for player immersion. This is especially if the player is not familiar with the cyber range environment.

C. KYPO Cyber Range

KYPO cyber range [15] is an open-source cyber range that provides two related environments. First is a cloud based KYPO Cyber Range Platform (KYPO CRP) for running multiple sandboxes in parallel. Second, KYPO Cyber Sandbox Creator (KYPO CSC) is lightweight standalone environment for running the sandbox on student's own computer. Game scenarios created for KYPO CSC can be easily modified for deployment on KYPO CRP, as both use the same formats. The only difference being the underlying virtualization technology.

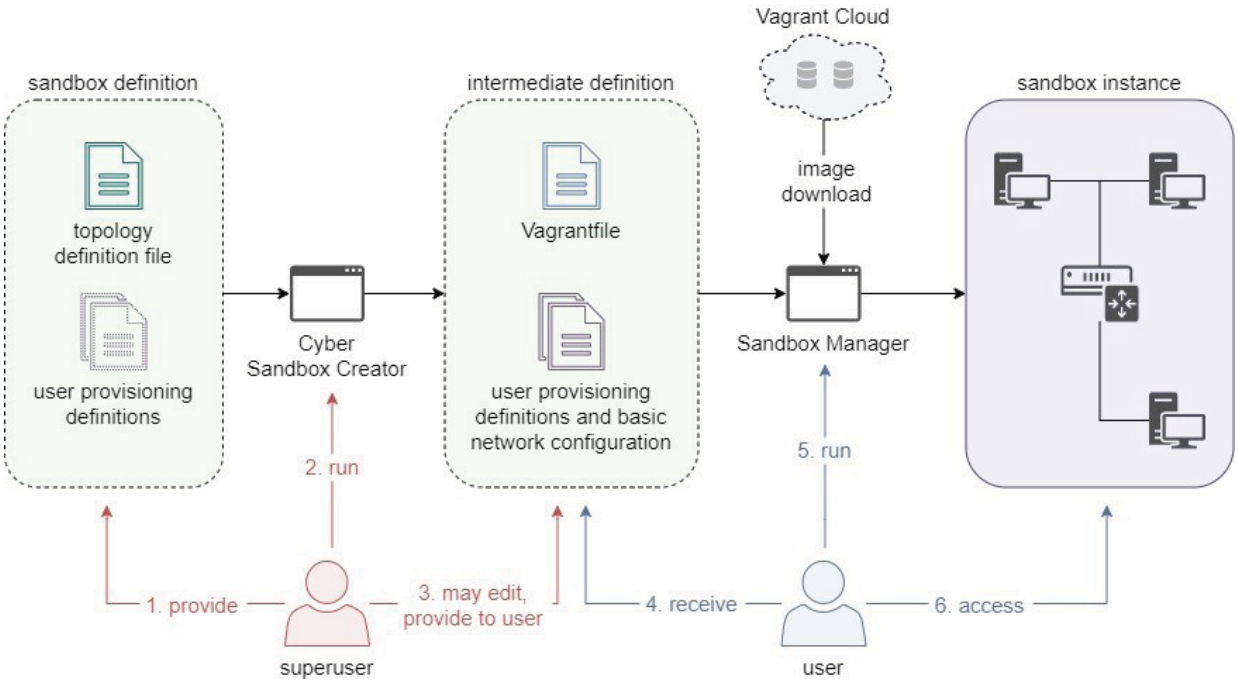


Figure 3. KYPO Cyber Sandbox Creator architecture [15]

Figure 3 depicts the architecture of the KYPO CSC together with the setup pipeline. The first step is creation of topology definition by the instructor (superuser). The topology can further be customized by additional software and/or configuration for desired sandbox in the form of *Vagrant* file. This *Vagrant* file can be distributed among students and used to recreate the sandbox on each student's computer.

IV. Game Scenario Design

Aim of the proposed game is to create a red team CTF scenario - an environment for teaching offensive techniques in penetration testing course. Our goal is to provide knowledge on specific vulnerabilities in a system and to understand the methods of exploiting these vulnerabilities. The central concept of the game is to teach students how to get into the mindset of potential attackers. Students can benefit from this understanding of offensive thinking when they are responsible for defending systems against intrusions. The techniques learned and order of actions are applicable to offensive cybersecurity in general.

The players should find 2 flags that are specific files on the target VM during the game scenario. The first flag is in file *user.txt*. This file indicates that the player successfully gained access to the target with user level privileges. This can be done after exploiting the Shellshock vulnerability. The second flag is in file *root.txt* and is accessible after indicates that the player gained access to the root account.

The scenario objectives map onto standard real-world intrusion actions. First, the *reconnaissance* and finding the target server on the network, followed by *target scan* of open ports. *Enumeration* on detected open ports to find a way in. *Exploitation* of vulnerable service, in this case *shellshock* in old version of bash to gain access to the system. After gaining initial access as a normal user, explore the system or try brute-force for *privilege escalation* to gain root access.

The game scenario was implemented in KYPO CSC, using a standard Kali Linux VM and a modified target VM - customized by installing applications and changing setting to include the desired vulnerabilities. As scenario storyline and tasks are not delivered by KYPO CSC, these are provided by a standalone webpage. The walkthrough webpage for players includes 6 interconnected levels, with tasks that take the player logically through the intrusion process to gain access and get the 2 flags on target system. Additionally, there is an optional *spoiler* for each level with specific instructions how to complete the level. This was added so that players can continue the game when they might get stuck on a specific task.

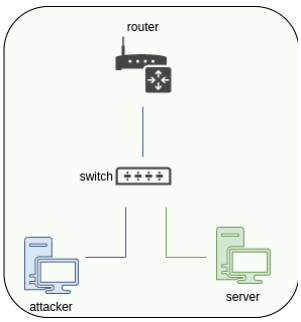


Figure 4. Designed scenario topology

V. VERIFICATION AND TEST RESULTS

Functioning of the game scenario was continuously checked during the whole development process by its creators. The correct behavior of the game final version was verified by an independent teaching assistant before start of testing and gathering feedback by a small group of volunteer students.

The final game scenario was tested by a total of 6 volunteer participants, who were mostly IT students. Although this was a small sized test pool, participants had different levels of offensive techniques knowledge beforehand. Thus, the feedback provided was representative of introductory course students.

The participants filled in a feedback form documents, with questions focusing on three areas. First, clarity of the tasks and walkthrough instructions. Secondly, the game itself, achieved outcomes, and the participant engagement with the scenario. Thirdly, to provide any general notes and comments. The feedback from participants was beneficial to improving the game - to see how users understood the walkthrough and judge the difficulty sufficient.

A. Walkthrough Instructions Feedback

The first two questions in feedback form were multichoice and focused on the state of the game completion by players, and use of the walkthrough instructions and spoilers. Test players were representing almost the whole skill spectrum, missing only those able

Figure 5. Test players responses on game completion

Figure 6. Test players responses on spoiler usage

to complete the scenario by themselves without using walkthrough instructions, as can be seen in Figure 5. By investigating answers to the second question, seen in Figure 6, we observed that two thirds of test players used spoilers a few times, except one skilled player who used it only once and one beginner who use them many times.

The following questions were for the participants concerning the walkthrough instructions and were open ended. *If you used the walkthrough instructions, was there something not explained enough? Did you find anything difficult to understand?* Most users replied that the level 5 (Python Library Hijacking privilege escalation method) was not written well, or they found it difficult to understand and follow the instructions. Instructions for Level 5 were considered too vague by the users and most had problems completing it. Even though references to similar examples were included, students seem to have overlooked them.

Based on the feedback, the walkthrough instructions were improved by including more details and changing formatting with more emphasis on references.

B. Game Outcomes Feedback

Feedback questions on the game outcomes were open ended, as we looked for test players own opinions and ideas for improvement.

Have you learned anything new?

All participants learned something through the game. Half of the players responded they learned about the Python Library Hijacking privilege escalation method. This was probably because of the disproportionate time they spent on this task. Two replied that they learned what privilege escalation is and why is it important. One increased familiarity with the tools used.

Have you experienced any problems with the game?

Most participants mentioned level 5 Python Library Hijacking, but these were caused by not actually understanding the walkthrough instructions. One participant noted crash of the VMs during enumeration, but as the problem was reappear, it was probably a random occurrence not caused by the scenario or cyber range environment.

Did you enjoy the game?

All answers were positive, with one participant noting they hope to have more course assignments use this form of environment.

Based on the responses, the continuous checking during development of the scenario and its verification before the start of the testing with volunteer players prevented any technical problems during testing.

C. Test Results Summary

We received differing opinions on the game from the test participants. The thinking was that the game scenario design is well made overall, but the thing that needs improvement is the walkthrough instructions. The descriptions of the task levels are acceptable. The problem is that the expectation for the interest of users and the time they spent on later and more difficult tasks would be higher.

Overall, we evaluated that this game is suitable to be included in cybersecurity course with a focus on penetration testing. The results are encouraging and after

minor modification, the game can be included into education process. Results of the evaluation show that the students learn new and valuable practical skills for cybersecurity in general and penetration testing in particular.

VI. CONCLUSIONS

We set out to improve practical cybersecurity training with realistic game scenarios. In this paper, we presented offensive cybersecurity game scenario for KYPO cyber range together with results from its preliminary testing and feedback. The designed game scenario was implemented and functionally verified utilizing KYPO Cyber Sandbox Creator. A small group of participants with various levels of subject matter knowledge tested the game scenario by playing it and provided feedback.

The scenario was judged by the players to be beneficial, engaging, and sufficient to be used for education of basic offensive techniques for penetration testing. The practical experience and knowledge of offensive techniques gleaned from the game prepares players for the role of penetration tester. Furthermore, understanding of the offensive techniques also improves awareness of how to defeat them when protecting a system.

The walkthrough instructions were improved based on the student feedback because the beginners did not fully understand everything as expected. Some misunderstanding might be expected, but players should fully understand what they are doing to get the best learning results.

The main contribution of this paper is a fully functional CTF-based game named Unpleasant, published at *https://gitlab.fiit.stuba.sk/xjely/unpleasant*. This repository contains everything that a user needs to set up the game scenario environment.

Next step in our research would be to conduct a larger scale testing not just with volunteers, but with all students of a penetration testing course. The larger sample size might reveal further ideas for improvement as well as optimization for further use.

In the future, the game may be improved and extended to include web-based vulnerabilities that may not lead into the Shellshock vulnerability, but to other vulnerabilities that can be exploited. This requires more effort in web development, such as creating a vulnerable web application. No matter what web-based vulnerability it can be, an Apache server is already installed on the server that future editors can take advantage of and create their own web page to create a vulnerability.

In the presented game scenario, we included multiple privilege escalation techniques and the Shellshock vulnerability exploitation. The editor should not continue creating more privilege escalation techniques. We think that the game provides enough privilege escalation techniques. Instead, a few techniques can be removed, and new techniques can be created, such as looking at the */etc/crontab* file.

ACKNOWLEDGMENT

This publication has been written thanks to the support of the Operational Programme Integrated Infrastructure for the project: International Center of Excellence for Research on Intelligent and Secure Information and Communication Technologies and Systems (ITMS code: 313021W404), co-funded by the European Regional Development Fund (ERDF).

This work was supported by Cultural and Educational Grant Agency (KEGA) of the Ministry of Education, Science, Research and Sport of the Slovak Republic under the project No. 026TUKE-4/2021.

REFERENCES

[1] Moore, M.: “Bringing Gamification to Cyber Security Training”. url: https://onlinedegrees.sandiego.edu/bringing-gamification-to-cyber-security-training/ (Accessed 2022-03-01).

[2] Li, C., & Kulkarni, R.: “Survey of cybersecurity education through gamification.” In: *2016 ASEE Annual Conference & Exposition.*

[3] Athanasios Grigoriadis et al. “Cyber Ranges: The New Training Era in the Cybersecurity and Digital Forensics World”. In: *Technology Development for Security Practitioners*. Springer, 2021, pp. 97–117.

[4] Findley M. R.: “The relationship between student learning styles and motivation during educational video game play”. In: *International Journal of Online Pedagogy and Course Design (IJOPCD) 1.3* (2011), pp. 63–73. https://doi.org/10.4018/ijopcd.2011070105

[5] Tim Harmon. “Cyber Security Capture The Flag (CTF): What Is It?” url: https://blogs.cisco.com/perspectives/cyber-security-capturethe-flag-ctf-what-is-it/ (accessed 2022-03-01).

[6] Yamin, M. M., Katt, B. and Gkioulos, V.: Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. In: *Computers & Security*, 88, 101636. https://doi.org/10.1016/j.cose.2019.101636

[7] Wolfenden B: “Gamification as a winning cyber security strategy”. In: *Computer Fraud & Security* 2019(5), pp. 9–12.

[8] Darwish, O. et al.: “Survey of Educational Cyber Ranges”. In: *Workshops of the International Conference on Advanced Information Networking and Applications*. Springer. 2020, pp. 1037–1045.

[9] Brunner, R., et al.: “Design for an educational cyber range”. In: *Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security*. 2019, pp. 1–2.

[10] Messina, G.: “Types of cyber ranges compared: Simulations, overlays, emulations and hybrids”. Feb. 2021. url: https://resources.infosecinstitute.com/topic/types-of-cyber-ranges-compared-simulations-overlaysemulations-and-hybrids/ (Accessed 2022-03-01).

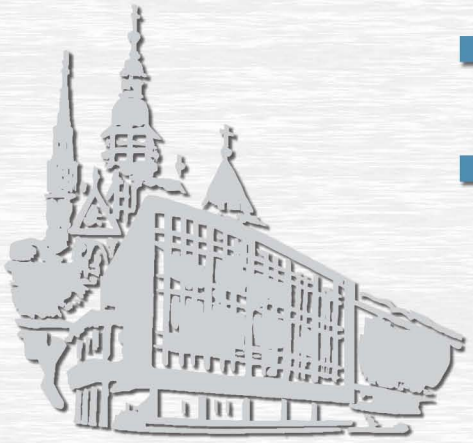
[11] Nestoras Chouliaras et al.: “Cyber ranges and testbeds for education, training, and research”. In: *Applied Sciences* 11.4 (2021), p. 1809.

[12] Davis, J., & Magrath, S.: "A survey of cyber ranges and testbeds." (2013).

[13] Ukwandu, E. et al.: “A review of cyber-ranges and test-beds: Current and future trends”. In: *Sensors* 20.24 (2020), p. 7148.

[14] Schreuders, Z. C. et al.: “Security Scenario Generator (SecGen): A Framework for Generating Randomly Vulnerable Rich-scenario VMs for Learning Computer Security and Hosting CTF Events”. In: *2017 {USENIX} Workshop on Advances in Security Education* ({ASE} 17). 2017.

[15] Vykopal, J., Čeleda, P., Seda, P., Švábenský, V., & Tovarňák, D. (2021, October). Scalable learning environments for teaching cybersecurity hands-on. In: *2021 IEEE Frontiers in Education Conference (FIE)* (pp. 1-9). IEEE. https://doi.org/10.1109/FIE49875.2021.9637180



ICETA 2022

International Conference

20th Anniversary of IEEE International Conference on Emerging eLearning Technologies and Applications

IEEE Czechoslovakia Section

PROCEEDINGS

Information and Communication Technologies in Learning

October 20-21, 2022
Grand Hotel Starý Smokovec, High Tatras
Slovakia

2022 20th International Conference on Emerging eLearning Technologies and Applications (ICETA) | 979-8-3503-2033-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICETA57911.2022.9974615

ICETA 2022

20th Anniversary of IEEE International Conference on Emerging eLearning Technologies and Applications

PROCEEDINGS

October 20 – 21, 2022

Grand Hotel Starý Smokovec, High Tatras, Slovakia

2022 20th International Conference on Emerging eLearning Technologies and Applications (ICETA) | 979-8-3503-2033-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICETA57911.2022.9974883

COMMITTEES

Honorary Committee Chair

Kmeť Stanislav, Technical University of Košice

Honorary Committee

Molnár Ľudovít, Slovak University of Technology, Bratislava
Newman B. Harvey, California Institute of Technology, Pasadena
Rudas Imre, Óbuda University, Budapest

Program Committee Chair

Jakab František, Technical University of Košice

Program Committee

Babič František, Technical University of Košice
Bauer Pavol, Delft University of Technology
Bederka Andrej, Slovak National Coalition for Digital Skills and Jobs, Bratislava
Behun Marcel, Technical University of Kosice
Berke József, John von Neumann Computer Society, Budapest
Bieliková Mária, Slovak University of Technology, Bratislava
Bours Patrick, Norvwegian University of Science and Technology
Brestenská Beáta, Comenius University Bratislava
Cehlar Michal, Technical University of Košice
Chovanec Martin, Technical University of Kosice
Čičák Pavol, Slovak University of Technology, Bratislava
Čižmár Anton, Technical University of Kosice
Dado Milan, University of Žilina
Doboš Ľubomír, Technical University of Košice
Dolnák Ivan, University of Žilina
Doroshenko Anatoliy, Institute of Software Systems of NASU, Kiev
Drozdová Matilda, University of Žilina
Dzupka Peter, Technical University of Košice
Feciľak Peter, Technical University of Kosice
Galgoci Gabriel, AT&T Bratislava
Gavurova Beata, Technical University of Košice
Genči Ján, Technical University of Košice
Haľama Marek, Technical University of Košice
Hämäläinen Timo, University of Jyväskylä
Hautamaki Jari, University of Appl. Science
Hluchý Ladislav, Slovak Academy of Sciences, Institute of Informatics
Horváth Pavol, SANET - Slovak Academic Network, Bratislava
Huba Mikuláš, Slovak University of Technology, Bratislava
Hudak Radoslav, Technical University of Košice
Hvorecký Jozef, Vysoká škola technická a ekonomická in České Budejovice

2022 20th International Conference on Emerging eLearning Technologies and Applications (ICETA) | 979-8-3503-2033-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICETA57911.2022.9974915

Jelemenská Katarína, Slovak University of Technology, Bratislava
Juhár Jozef, Technical University of Košice
Juhas Gabriel, Slovak University of Technology in Bratislava
Kainz Ondrej, Technical University of Košice
Kess Pekka, University of Oulu
Kireš Marian, University of Pavol Jozef Šafárik
Klačková Ivana, University of Žilina
Klimo Martin, University of Žilina
Korshunov Alexander, Kalashnikov Izhevsk State Technical University of the name M.T. Kalashnikov
Kotuliak Ivan, Slovak University of Technology
Kováčiková Tatiana, COST Office, Brusel
Kovács Levente, Óbuda University, Budapest
Kyselovič Ján, Slovak Centre of Scientific and Technical Information, Bratislava
Lavrin Anton, Technical University of Kosice
Lelovsky Mario, Slovak IT Association Bratislava
Levický Dušan, Technical University of Košice
Lumnitzer Ervin, Technical University of Kosice
Mesaroš Peter, Technical University of Košice
Meško Dušan, Jessenius Faculty of Medicine, Martin
Michalko Miroslav, Technical University of Kosice
Modrak Vladimir, Technical University of Kosice
Mulesa Oksana, Uzhorod National University
Mytnyk Mykola, Ternopil National Ivan Pul`uj Technical University
Nakano Hiroshi, Kumamoto University
Pavlik Tomaš, Technical University of Košice
Pietrikova Alena, Technical University of Kosice
Pisutova Katarina, Comenius University
Piteľ Jan, Technical University of Košice
Poruban Jaroslav, Technical University of Košice
Radács László, University of Miskolc
Restivo Maria Teresa, University of Porto
Ristvej Jozef, University of Zilina
Salem Abdel-Badeeh M., Ain Shams University of Cairo
Semanišin Gabriel, University of Pavol Jozef Šafárik
Simonics István, Obuda University, Budapest
Šimšík Dušan, Technical University of Košice
Sinčák Peter, Technical University of Košice
Sobota Branislav, Technical University of Košice
Sovak Pavol, University of Pavol Jozef Šafárik
Stopjakova Viera, Slovak University of Technology in Bratislava
Strémy Maximilián, Slovak University of Technology in Bratislava - Advanced Technologies Research Institute – University Science Park CAMBO, Trnava
Stuchlikova Lubica, Slovak University of Technology
Šveda Dušan, UPJŠ Košice
Szabo Stanislav, Technical University of Košice
Szentirmai László, University of Miskolc
Turna Jan, Comenius University, Bratislava

Usawaga Tsuyoshi, Kumamoto University
Vagan Terziyan, University of Jyvaskyla
Vasková Iveta, Technical University of Košice
Vokorokos Liberios, Technical University of Košice
White Bebo, SLAC National Accelerator Laboratory, Stanford University
Zivcak Jozef, Technical University of Košice
Zolotová Iveta, Technical University of Košice

Organizing Committee Chair

Jakab František, Technical University of Košice

Organizing Committee

Fejedelem Štefan, elfa, s.r.o., Košice, Conference Manager
Rakoci František, elfa, s.r.o., Košice, Webmaster
Zámečníková Iveta, elfa, s.r.o., Košice, Finance Chair

TABLE OF CONTENTS

Committees **4**

Table of Contents **7**

Contract Cheat Detection using Biometric Keystroke Dynamics **15**
N. Agarwal, N.F. Danielsen, P.K. Gravdal, P. Bours

A study on the methodology of Software Project Management used by students whether they are using an Agile or Waterfall methodology **22**
E.M.M. Alzeyani, C. Szabó

How (not) to regulate automated vehicles: lessons from Slovakia **28**
J. Andraško, M. Mesarcík

Education challenges after Covid-19 ..... **34**
V. Bakonyi, Z. Illés

Enhancing Education Process Supported by Virtual Reality **40**
A. Behúnová, L. Knapcíková, M. Behún

Workstation with speed servo drive **46**
I. Bélai, I. Bélai

Algorithmic difficulty of solving examples from Slovak language **53**
M. Beno

On the simulation of electric scooter crash-test with the hybrid human body model **59**
T. Bonkowski, J. Špicka, L. Hyncík

Handover strategies simulations in IEEE 802.11 based on Artificial Intelligence **66**
A. Brezáni, R. Bencel

Impact of electromagnetic radiation – research **73**
I. Bridova, M. Moravcik

Flip Learning: A New Paradigm **79**
P. Campanella

LMS: Benchmarking ATutor, Moodle and Docebo **85**
P. Campanella

School web portal as a means of parent-teacher communication **91**
I. Cernák, P. Sitiarik, M. Rojcek

Using BBC Micro:bit in University Environment **97**
M. Cernanský, J. Jurinová

2022 20th International Conference on Emerging eLearning Technologies and Applications (ICETA) | 979-8-3503-2033-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICETA57911.2022.9974730

Development of a Multifunctional Micro-mobility Unit with Autonomous Mode **103**
D. Chikurtev, P. Stoev, R. Ficherov, M. Stoeva

Methodology for successful spin-off creation in academic setting **109**
P. Cižmár, H. Dunne, V. Fedák, R. Hudák, F. Jakab

Adaptation of Multisource Video Streaming in Heterogenous Environment of National Telepresence Infrastructure with Advanced Elements of Processing Visual Recordings to Multimedia Archive **117**
D. Cymbalak, F. Jakab, R. Vápeník, M. Murín, M. Korének, P. Hrcka

Intelligent road recognition system for an autonomous vehicle **122**
M. Dlugosz, M. Brodzicki, P. Skruch, M. Szelest, D. Cieslar

BIMI specification as another technical approach in the fight against e-mail phishing **129**
I. Dolnák, K. Kampová

Assessing expectations and potential of domain independent corporate learning chatbots **135**
F. Dopler, B. Göschlberger

Information System for Asset Management in Buildings **141**
M. Durneková, M. Kvet

Moving beyond dual education framework for the skill development of ICT potentials **147**
M. Dzbor, M. Cicvara

Best Practice for Boosting Innovation in the HEI through the Initiative of European University Alliances **153**
V. Fedák, R. Hudák, F. Jakab

Solving the QoS Issues of Video Streaming in IP Networks **159**
M. Fendek, M. Michalko, O. Kainz, P. Fecilak, K. Fecilaková

Importance of Human Skills and "Fun" in Education of Project Leaders **165**
M. Filipová, P. Balco

Issues and methodology of teaching automation using intelligent information technologies **172**
D. Gabriska

Interactive Jupyter Notebooks with SageMath in Number Theory, Algebra, Calculus, and Numerical Methods **178**
A. Gajdoš, J. Hanc, M. Hancová

Social Micro-Learning and Student Performance **184**
B. Göschlberger, F. Dopler, G. Kotsis

The Dynamics of Regulation of Automated and Autonomous Vehicles 190
Z. Gyurász

Open R and Python-based Digital Tools in Statistics, Random Processes, and Metrology 196
J. Hanc, M. Hancová, A. Gajdoš

Future Lower Primary School Teachers Taking an Online Algorithmization and Programming Course and Self-Assessing their Performance 202
T. Havlaskova, T. Javorcik

Optimisation of Algorithms Generating Pseudorandom Integers with Binomial Distribution 209
R. Horváth

Serious games in sciences, humanities, and arts: examples from a practical perspective 214
M. Hostovecký, K. Pribilová

How to teach, design and program robotic and IoT systems 219
J. Hrbácek, M. Binas, J. Strach

Should We Forget the PID Control? 225
M. Huba, P. Bisták

The current state of ICT security at Czech primary schools 231
J. Hubert, M. Dosedla, K. Picka

Digital Escape Room for computer network mechanic students 236
L. Huraj, M.S. Hudáková

Teachers' interdisciplinary cooperation triggers students' transferable competencies and intensifies the process of internationalisation of Higher Education 243
L. Hurajová, G. Chmelíková, J. Luprichová

Virtual Reality Environment as a University Online Education Platform 250
J. Hvorecký, P. Rozehnal

On Supporting the Effective Use and Transfer of Outputs from Research Projects 256
F. Jakab, A. Lavrin, B. Bonk, M. Tomasko

Aggregation and Evaluation of Communication Data of Large Telepresentation Infrastructure based on Computing Nodes on Critical Endpoints 260
F. Jakab, J. Molitorisová, R. Vápeník, D. Cymbalák, J. Kovácová

Traffic signs detection, recognition and tracking for roads mapping 266
M. Janeba, K. Balaj, M. Galinski

The Incorporation of Digital Technology into Education from the Point of View of School Principals and ICT Coordinators 273
T. Javorcik, T. Havlaskova

Gamification of cyber ranges in cybersecurity education 280
M. Jelo, P. Helebrandt

Low-code platforms and languages: the future of software development 286
G. Juhás, L. Molnár, A. Juhásová, M. Ondrišová, M. Mladoniczky, T. Kovácik

Development of a desktop application for a complex heterogeneous evaluation system 294
J. Jurinová, J. Miština

Monitoring of parking space occupancy via UAVs 300
O. Kainz, K. Briškár, M. Michalko, F. Jakab, I. Nováková, P. Fecilak

An innovative multidisciplinary approach to the teaching computer networks and cybersecurity 306
E.A. Katonová, R. Petija, F. Jakab, O. Kainz, M. Michalko, J. Džubák

Examination of Average Consensus with Maximum-degree Weights and Metropolis-Hastings Algorithm in Regular Bipartite Graphs 313
M. Kenyeres, J. Kenyeres

Ubiquitous Art: Hybrid Aspects of Technology-Oriented Art (Part 1) 320
R. Kitta

Mechatronic Systems in Mechanical Engineering 324
I. Klacková, D. Wiecek, T. Dodok

Evaluation of containerized cloud platform for education and research 332
M. Kontsek, M. Moravcik, P. Segec, D. Cymbalak

Do Neural Networks Recognize Patterns as well as Students? 338
J. Kopcan, M. Klimo, O. Škvarek

Design of a Final Thesis Proposal Module 344
J. Kostolny, V. Salgova, S. Kvietkova

Application of the Simulation Tools in the Educational Process 348
R. Králiková, E. Lumnitzer

Implementation of elements of the Industry 4.0 concept and its impact on employees in line with Human Resource Management in industrial organisations in Slovakia 352
E. Kubišová, L. Grajzová, M. Cambál, D. Babcanová

The Informatics 2.0 Approach in Relation to the Digital Skills Test 358
N. Kvassayova, M. Kvassay, M. Bendikova, E. Dusekova, S. Stankevich

Concept of Hybrid Temporal Architecture 364
M. Kvet

Design of an Intelligent Vehicle Accident Detection System 371
P. Lehoczký, F. Caplák, D. Cok, R. Križan, L. Šoltés

Employers and Academia must communicate! For the sake of successful graduates and happy future employers 377
M. Lelovsky

Use of gamification in the teaching process of solving logistic tasks 382
O. Lohaj, J. Paralic, M. Stašš

Implementation of Substandard Acoustics in Education Processes 388
E. Lumnitzer, E. Jurgovská, A. Yehorova

Phishing as a Cyber Security Threat 392
M. Madlenák, K. Kampová

Creating an overtaking maneuver in the Prescan virtual environment 397
L. Magdolen, J. Danko, T. Milesich, I. Kevický, L. Hanko

Key Performance Indicators and Managerial Competencies and Effectiveness Developed by BIM Technology in Construction Project Management 404
T. Mandicák, P. Mésároš, L. Zemanová, R. Rucinský

Object interaction in virtual school environment 410
M. Mattová, L. Murínová, B. Sobota, Š. Korecko

Cluster application in a virtual CAVE computing environment 416
M. Mattová, B. Sobota, M. Duratný, Š. Korecko

Circadian Rhythm and Skin Conductivity, Their Measurement and Use of Obtained Data to Plan Daily Activities 422
M. Miklošíková, L. Tomaszek, M. Malcík

The Role of Workforce agility in the acceptance of Information Systems: Evidence from Serbia 428
A. Milicevic, T. Lolic, S. Sladojevic, D. Krstic, D. Stefanovic

Sectoral Strategy for Human Resources Development in the Information Technologies and Telecommunication Sector by 2030 434
A. Minns

New Public Dataset for Classification of Inappropriate Comments in Slovak language 437
J. Mojžiš, M. Kvassay

ICT Literacies in the Context of Some Anniversaries 442
L. Molnár, G. Juhás, M. Ondrišová, A. Juhásová, T. Kovácik, M. Mladoniczky

Modern methods of projection as a tool for attractive education in museums 448
M. Molokác, G. Alexandrová, D. Tometzová

Kubernetes - evolution of virtualization 454
M. Moravcik, M. Kontsek, P. Segec, D. Cymbalak

Decision-Making Modeling in Educational Process Organization Under the Conditions of Crisis Situations Forecasting **460**
O. Mulesa, I. Myronyuk, O. Kachmar, F. Jakab, O. Yatsyna

Methodical procedure for creating content for interactive augmented reality **466**
I. Nováková, F. Jakab, M. Michalko, O. Kainz

Control Engineering and Industrial Automation Education using Out of the Box Approaches **472**
P.M. Oliveira, D. Vrancic, M. Huba

Children-robot spoken interaction in selected educational scenarios **478**
S. Ondáš, M. Pleva, J. Juhár

Fully Integrated On-Chip Inductors: An Overview **484**
R. Ondica, M. Kovác, R. Ravasz, D. Maljar, A. Hudec, V. Stopjaková

Covert Channel Detection Methods **491**
A. Ondov, P. Helebrandt

The Interactive Educational Course of Block Programming for Primary Schools **497**
M. Paralic, D. Jarinová, L. Smatanová

Potential Areas of the V4 to Improve Its Position in the European Innovation Ecosystem **502**
T. Pavlik, F. Jakab, V. Fedák

Universal GUI for Easy and Fast Analysis of Dynamical Systems Performance **508**
D. Perdukova, V. Fedak, D. Hanecak

Requirements to SMART Services for Education and Management of services at Universities in Slovakia **515**
N. Pinterova, P. Balco, M. Filipova

Student Satisfaction with Online Learning During Pandemic and After **523**
K. Pišútová, K. Kánová, E. Benová, A. Juhásová

Handwriting Data Analysis from Crayonic KeyVault Smart Security Device **531**
M. Pleva, S. Ondáš, D. Hládek, J. Bucko

Teaching cloud computing at The Technical University of Kosice – design, experiences, and extensions **537**
L. Pomsar, D. Hladek, A. Brecko, I. Zolotova

Application of path planning algorithms in the MATLAB environment using Lego Mindstorms **543**
K. Pribilová, Z. Mäsiarova

Introduction to Teaching the Digital Electronics Design using FPGA **549**
R. Ravasz, A. Hudec, D. Maljar, R. Ondica, V. Stopjakova

Diversity and Gender Equality as a key factor for industrial companies 555
V. Sabolová, L. Cuninková, M. Cambál

Safety of Perception Systems in Vehicles of High-Level Motion Automation..... 561
P. Skruch, M. Szelest, M. Dlugosz, D. Cieslar

A system for tracking people in a confined space..... 567
E. Skýpalová, I. Dolnák

Digital tool for designing and education in the field of sustainable and circular construction 572
J. Smetanková, P. Mésároš, A. Behúnová, L. Zemanová, K. Krajníková

Experimental multimodal user interface 578
B. Sobota, Š. Korecko, D. Bélla, M. Mattová

Therapist-patient interaction in virtual reality at the level of the upper limbs..... 584
B. Sobota, Š. Korecko, J. Gvuščová, M. Mattová

Impact of hybrid teaching methodology during COVID-19 pandemic on Operating systems course..... 589
M. Solanik, M. Nguyen, D. Gecášek, J. Genci

Design of algorithms for automated collection of IT assets 595
M. Šterbák, P. Segec, J. Jurc

Tools for automatic collection of IT assets supporting information security process 601
M. Šterbák, P. Segec, J. Jurc

Educational design for building the competence "Dealing with conflicts" in the learning process through projects in technical subjects 607
M. Stoeva

Academy Phoenix: Will Universities Reborn in Industry 5.0 Era, or Will They Lie Down in Ashes?..... 613
L. Stuchlikova, J. Marek

Non-Contact Detection of Vital Parameters with Optoelectronic Measurements under Stress in Education Process..... 620
J. Sturekova, P. Kamencay, R. Vrskova, M. Labuda

Introducing students to out-of-distribution detection with deep neural networks 627
O. Šuch, R. Fabricius, P. Tarábek

The Research on Controlling Virtual Reality by EEG Sensor 634
S. Suchalova, M. Benco, R. Hudec

Digital transformation of education with the support of the national project IT Academy..... 640
D. Šveda, V. Hubenáková, M. Babincáková, M. Kireš, K. Kozelková, K. Lukácová, A. Mišianiková, V. Ondová

Mobile technology as a tool to support the enhancement of students' communicative competence 647
D. Tran, K. Kostolányová

Creation of students' self-assessment forms using information technologies 654
M. Václavková, D. Maceková, M. Kvet

Artificial Intelligence and the criminal responsibility - challenges, obstacles and possible solutions 660
F. Vojtuš, M. Kordík, P. Dražová

Comparative Analysis of Algorithms for Mobile Robots in Performing Certain Tasks 673
S. Yovkov, N. Chivarov, S. Shivarov, P. Stoev

Personalized e-Coaching as a Support in the Social Inclusion Process 679
L. Zemko, K. Jelemenska, P. Cicak, T. Mifkovic

Assignments in Information Science Subject Aimed to Improving Pupils' Spatial Imagination 685
R. Žitný, T. Szabó

Author Index 691