Attack and Defend

Combining Game-Based Learning with Virtual Cyber Labs

Mahmoud, Rasmi-Vlad; Kidmose, Egon; Broholm, Rasmus; Pilawka, Olga Paulina; Dominika Illés, Dominika; Magnussen, Rikke; Pedersen, Jens Myrup

Published in:
Proceedings of the 14th European Conference on Games Based Learning

DOI (link to publication from Publisher):
10.34190/GBL.20.150

Publication date:
2020

Document Version
Accepted author manuscript, peer reviewed version

Attack and Defend: Combining Game-Based Learning with Virtual Cyber Labs

Rasmi-Vlad Mahmoud[1], Egon Kidmose[1], Rasmus Broholm[2], Olga Paulina Pilawka[2], Dominika Illés[2], Rikke Magnussen[2], Jens Myrup Pedersen[1]

1 Wireless Communication Networks, Department of Electronic Systems, Aalborg University, Denmark
2 Science, Policy and Information Studies, Department of Communication and Psychology, Aalborg University, Denmark

rvm@es.aau.dk
egk@es.aau.dk
rbroho18@student.aau.dk
opilaw18@student.aau.dk
dilles18@student.aau.dk
rikkem@hum.aau.dk
jmp@es.aau.dk

Keywords: Cybersecurity, Platform, GBL, Attack, Defence

Abstract: With the increasing focus on cybersecurity from both authorities and enterprises, the growing skills gap in cybersecurity is one of the biggest cybersecurity concerns. Therefore, there is an urgent need to motivate young people to choose education and careers in cybersecurity, but also to increase competencies among both students and professionals. At the same time, many of the topics of cybersecurity are well suited for gamification: This is the case for both technical topics, where Capture The Flag competitions have gained wide recognition, but also for the less technical topics such as incident-response. There are already several well-established platforms to support the former, but in most cases, the exercises offered are quite simple (find a flag and get points), and as such do not reflect the complexity of systems to attack/protect, and if more complex scenarios are covered these often are static, and it requires a significant amount of work to create new scenarios. This paper presents the overall architecture of a new platform, designed for user-friendly and automated generation of complex gaming scenarios for learning about cybersecurity. This makes it possible to create very realistic scenarios for training both technical skills and the participants' abilities to act and make decisions in stressful situations. Moreover, it offers the possibility for users to interact with each other, both within and between teams, raising their abilities to communicate and solve challenges. The platform is envisioned with both technical perspectives and game design for learning in mind. This means that the platform is not only able to create realistic virtual labs, but the labs are created based on game scenarios that are considering specific learning objectives. This also makes it possible to create games that go beyond the traditional "point collection" and engage the users in a setting that feels more realistic and absorbing.

1.Introduction

Organizations face challenges when recruiting skilled cybersecurity personnel. According to the CSIS (Center for Strategic & International Studies) report (Crumpler and Lewis 2019) the cybersecurity job market has grown with more than 50 percent from 2015. Additionally, the global gap for the cybersecurity workforce will be reaching 1.8 million unfilled positions by the year 2022 (Crumpler and Lewis 2019). Moreover, a question that was addressed by CSIS was if cybersecurity masters programs and certifications offer the training that the cybersecurity workforce needs. Unfortunately, they concluded that the requirements are not entirely met. For this reason, employers are not fully satisfied with the graduates of those programs. They require extensive training on jobs since they are lacking a fundamental understanding of important areas within the topic, as well as critical soft-skills such as teamwork, problem-solving, and communication. (Crumpler and Lewis 2019)

Nonetheless, the increase of cybercrime and the consequences raised further the necessity of cybersecurity training. There is a need also for proper learning methods to produce cybersecurity professionals that can be competent in the workforce. (Katsantonis, Fouliras, and Mavridis 2017)

Even if there has been a high engagement towards security education, there is still a long way to go since cybersecurity education needs to address a large range of roles, from technical students to high school students, but also from skilled professionals to computer users. (Idziorek, Rursch, and Jacobson 2012)

Capture-the-Flag (CTF) is a live cybersecurity competition that takes advantage of those approaches by maximizing the learning for participants by allowing them to practice finding vulnerabilities, compromising services, and also defending against attacks. Furthermore, the competitions are often happening in teams which is boosting the learning when participants learn from each other. Although these types of competitions have been known to raise interest, depending on competition's form type the difficulty can be high when someone needs to organize these types of competition. (Trickel et al., n.d.)

CTF competitions have shown to be effective by offering a degree of hands-on experience and entertainment. There are different types of CTFs, however, most of them vary from three principal themes: attack-defend, attack-only, and defend-only. (Katsantonis, Fouliras, and Mavridis 2017).

In attack-defence, CTFs participants are required to firstly operate some of their services and after that to start attacking other team's setups. The teams are rewarded with points when both their services are running and/or they manage to compromise other teams' services. On the other hand, attack only CTF or Jeopardy CTF are designed to learn only attacking tactics. The players receive points based on the complexity of the attack that they need to use to successfully exploit a system. The last type of CTF is Defend-Only where players need to only secure their environments and services, and they are ranked based on this.

Using CTF competitions in an educational context ensures a high degree of motivation and commitment between the participants, while they also have shown effectiveness in demonstrating what incident handling can be like. However, they have limitations in the pedagogical context (M. Katsantonis, Fouliras, and Mavridis 2017).

Nonetheless, creating a virtual environment plays an important role in many parts of cybersecurity training. Having virtual environments that can replicate real IT infrastructures as realistically as possible offers a lot of comfort both for users and organizers in testing new approaches to a problem (Furfaro et al. 2016). Some virtual environments support only static, pre-build scenarios set up by the developers. Such scenarios do not allow modification or adding e.g. network traffic generators.

One approach that can enhance the learning process in cybersecurity is "game-based-learning" which includes virtual reality games, multi-user virtual environments, and simulations (Kumar et al. 2013) where students can experience aspects of games and learn in a context already designed. The students can perform actions and experiments based on the consequences while they actively learn in a safe environment. Game-based learning can be used as an innovative method for training cybersecurity skills due to its strong ability to attract and engage the learners (M. N. Katsantonis, Fouliras, and Mavridis 2017).

Even if this is a young field some argue that the non-game-based learning approaches have different short-comings in their methods. Some of their improvements can be made on the educational impact and their entertainment level (Nagarajan et al. 2012). Furthermore, students are learning only 20 percent of what they hear and read but learning up to 90 percent if they practice something (Findley 2011).

The main contribution of this paper is the design of a platform that will facilitate both training cybersecurity technical skills in complex training scenarios and offer users the possibility to work in teams to develop their soft skills. The rest of the paper is organized as follows: Section 2 describes the background of the study by presenting the elements of game design, Section 3 presents the motivation of creating a new platform for cybersecurity training. Next, section 4 introduces the scenarios for the new platform and the design, section 5 describes how a new scenario can be created on the presented structure and the future steps in the development. Finally, the paper ends with the conclusion section.

2.Background

This section summarizes the findings of (Broholm, Pilawka, and Illes 2020). Please refer to this for further details.

The concept of games can be used for many purposes, not only for fun, excitement, and leisure. For instance, applying game elements into a genuine setup to raise the experience has already taken place in the military. We adopt the definition that gamification is the "usage of game elements into non-game context", moreover game design elements that are used in serious games are important when it comes to making a difference between what is a game and what represents a gamified application

Gamification has shown to be effective by leading to changes in attitude, behavior, and knowledge within the learning process. Furthermore, a study made by (Fujimoto, Fukuyama, and Azami 2015) revealed that games are not limited to raising knowledge absorption but have also shown to be effective in broadening social interactions. Learning by playing is an approach valuable to understand how players learn while playing serious games. Moreover, players can increase their motivation if the failure is less harmful while they can learn new skills in safer environments. (Broholm, Pilawka, and Illes 2020)

Another aspect of gamification that can increase the learning experience is competition. Assessing the progress in comparison with others is helping increase the level of motivation and engagement towards the learning process. To achieve competition, framework tools such as leaderboards and rankings are used. It is worth emphasizing that e-learning approaches towards competition and progress are required to be implemented through gamification by certain graphics, visuals, and authentic animations which helps the user getting involved in the gamification experience. (Broholm, Pilawka, and Illes 2020)

Cybersecurity is a highly specialized field and demands certain methods to be applied for learning. One possible approach can be to use techniques of gamification to increase the learning experience, but also to understand what motivates the users.

2.1 Gamification in Cybersecurity

Traditional learning schemes are not applicable for cybersecurity, due to rapid changes, however, simulations and game designs are. Gamification can be used in designing a cybersecurity platform to enhance knowledge retention and to evoke perishable skills. Gamification can also be used to avoid endangering production systems, but instead test and train in closed environments. The initiative of using gamification in cybersecurity training is already known since the National Initiative for Cybersecurity Education (NICE)(Amorim, Joni A., et al., 2013) states that "gamified ranges for cybersecurity" are principles that cybersecurity platforms need to include. When designing a cybersecurity platform, it is important to define exactly what competencies are required, because the aspect of competence in gamification and cybersecurity training requires individuals with different skills and knowledge to team up. Additionally, to maintain the game balance it is important that the learner competencies match the game objectives. In the study "On the design of security games: from

frustrating to engaging learning" (Vykopal and Barták 2016) stated that the learning game should be divided into levels to help accomplish individuals' learning goals. (Broholm, Pilawka, and Illes 2020)

A cybersecurity crisis simulation consists of different types of roles such as attackers, defenders, and users interacting with a system. These roles resemble real-life situations as each one's aim is to win over the other. A pilot study was defining 3 key components of how human behavior is monitored during simulations within the cybersecurity domain and these are Motivation, Opportunity, and Ability.

Motivation is driven by how the individual reacts to a scenario, emotional response, and their habits. Opportunity is oriented towards achieving a goal by making use of the external background, while the ability is defined by the skills an individual can use during a simulation.

2.2 Cyber Attack crisis simulation

According to (Granlund, Berglund, and Eriksson 2000) a resourceful method to positively accomplish the learning goals of students is to use web-based simulations. Moreover, this method is also keeping their motivation high. However, the usage of web-based simulation has its drawbacks when it is used constantly to teach a big audience due to the expensiveness of the scenarios in terms of computing power. Still, scenarios have a high importance in the context of a crisis simulation. (Broholm, Pilawka, and Illes 2020)

A crisis represents an unforeseen event that is modifying the stability of a system and requires a fast reaction to stabilize that specific system. Although a crisis can vary, a person that has already experienced one simulation has grown and he/she is capable of following a specific cycle, which consists of initial response, time of consolidation and restoration. (Broholm, Pilawka, and Illes 2020)

Human behavior during a crisis is different than the everyday one, and therefore further research is needed in the field of cybersecurity to determine how individuals react in such circumstances. There is a tendency to become irrational in stressful situations, and in cybersecurity human's behavior is playing a key role. Therefore, it is important to determine what factors during a simulation have positive or negative influence over a decision that a certain person is making. However, when a simulation is constructed, it is important to consider realism of the environment, tools that are available for the situation but also the timing of a simulation, to not overload the users and impact his/her decision and fatigue. (Broholm, Pilawka, and Illes 2020)

Therefore, we conclude that there is a need to introduce more realism in cybersecurity, to accustom the rapid changes of this field, and we conclude that gamification can have a positive impact in the learning process. The next section will present how previously presented elements will be integrated in the new cybersecurity platform.

3. The network analysis platform

Universities' curriculum follows a strict path of teaching students into adversarial thinking, by learning about different types of past attacks without taking into consideration that a static approach cannot give the best overview. Nonetheless, training only the defensive side is not the key either since this cannot defeat the ingeniousness of the attackers, so it is essential to train simultaneously in both attacking and defending (Roschke, Willems, and Meinel 2010). Once the minimum knowledge and skills are developed, it is desired to move away from static computer-based scenarios to real human interaction and construct scenarios where a group of users can compete with each other for different objectives (Roschke, Willems, and Meinel 2010). Additionally, it is not sufficient to study vulnerabilities and abstract patterns, hands-on experience is needed to understand the complex concepts required by cybersecurity. As it was previously presented in section 2, gamification is a good framework that can be used for the learning process, but allowing users to team up and solve problems in a group have produced good results (Trickel et al., n.d.)

There exist a large number of platforms that support different types of CTFs based competitions, but one major drawback is that they are not open source which makes them less suitable for educational purposes. Moreover, even if some of them are open source their configuration is not trivial, and a lot of work is required for organizers (Panum et al. 2019).

The existing platforms are not supporting the exact purpose and therefore, Aalborg University started this journey by firstly creating Haaukins (Panum et al. 2019) for having a virtualized fully automated jeopardy CTF engine. However, Haaukins cannot adapt to attackers' creativity since there is no interaction between the users (Panum et al. 2019). Moreover, Haaukins was designed as an open-source platform for beginners to get an introduction to cybersecurity, but there is a need to play more advanced scenarios, where users can experiment various networks scenarios that are designed in a virtualized environment.

Therefore, a new platform for training cybersecurity is needed, which allows for improved realism, better gamification and the possibility for participants and teams to work either with or against each other. The target group of this new training platform is to provide advanced training for students that have a certain knowledge of cybersecurity. The project is a collaboration between three educational institutions from Denmark, Aalborg University, Technical University of Denmark and Business Academy Aarhus. The platform will assist students in learning by offering a training environment and a series of simulated scenarios that will be further explained in the next section.

The novelty of the new platform represents the facts that will allow users to interact with each other and to form teams or to use the environment as a single user and train some of the skills that are necessary in the team-based games. Moreover, the platform will be created in a virtualized environment that is capable of automatically creating the required conditions for the simulation. This automatized approach not only takes the additional work from the instructor, but also ensures that the system is easy to get started with and use, and the organizer can fully focus towards the educational process.

During the development, but also the design phase, scalability and realism were taken into consideration. The platform should support a high degree of scalability while the realism is not limited. Besides, the users' ease of access has to be high.

4. Design of Platform

4.1 Training Scenarios

Training cybersecurity skills require different settings which are not limiting the learning. The platform is expected to support the following scenarios, and the design of the platform can allow to either play these scenarios one by one or to build on knowledge from a previous module that was played. Throughout the description of the scenarios two types of roles, *Attacker and Defender,* will be used. An attacker is the user that performs offensive maneuvers to gain information from other systems, while a defender is the user that tries to counteract the attacker's moves or to set up defensive systems.

4.1.1 Network Analysis Scenario

In this scenario, the students are expected to learn/train their defensive capabilities by detection. They are expected to understand/analyze network traffic, logs and/or to organize security information and events management (SIEM). On the side of the training, students to be defenders will be provided with access to the environment and tools which are pre-installed, but particular configurations are to be made by them. Students are expected in this scenario to determine which tools are best to configure, and to determine based on traffic, logs, and alerts if a malicious activity is happening in the network.

4.1.2 Network Configuration Scenario

Students will learn/train network security skills by learning how to configure intrusion detection systems (IDS) and firewalls in a network, as well as getting to experiment with network segmentation capabilities. For students to train as defenders they are, for instance, expected to write their own firewall rules, attach a component to a specific network, or determine the best position for an IDS.

4.1.3 Attack - Defense Scenario

The goal of this scenario is for the student to train/learn attacking capabilities while consequently learning how to defend their environments. The main differences of this scenario, compared to the previous scenarios, are that students can work in teams, while they experiment at the same time being an attacker and/or a defender. The platform supports this type of activity by providing the teams two symmetrical environments and allows them to compete with their opponents (the other team) following a set of established rules. Attackers' objective is to find pieces of information called *Flags*, that can either be short fragments of text or random numbers, in opponents' setup while defenders' goal is to limit their capabilities and to ensure that their systems are running.

Novelty comes in this scenario when the act starts, since both teams prepare their environment by making sure that the services are up running and by setting up log management capabilities in the allocated timeframe. Once the game starts everyone can attack each other and get "flags" from the available environments. Every team will have an environment with vulnerable machines, and the complexity of the necessary exploits will vary from easy to hard.

4.1.4 Red - Blue Team Scenario

The purpose of this scenario is for the students to train/learn to be an attacker and/or a defender. The scenario starts with asymmetric labs, one of the teams is in an attack position (Red) the second one is in defense (Blue). Attackers, in this scenario the Red Team, are performing offensive attempts to infiltrate and retrieve information from the opposite team while the defenders, Blue Team, are acting against their tactics.

The advantage of this type of scenario is that the learners can specialize in either the attacking or defending position once they have previously experienced both situations. It is a scenario that allows the user to play the role, attacker or defender, he/she considers to be the most interesting and challenging.

4.2 Platform Architecture

To accustom some of the ideas presented in section 3 here the overall architecture of the platform will be presented while some of the concepts will be explained. The platform architecture will be designed based on Microservices, which is a software development technique used to design an application as a collection of small systems that each has a limited functionality, which can be seen in figure 1.

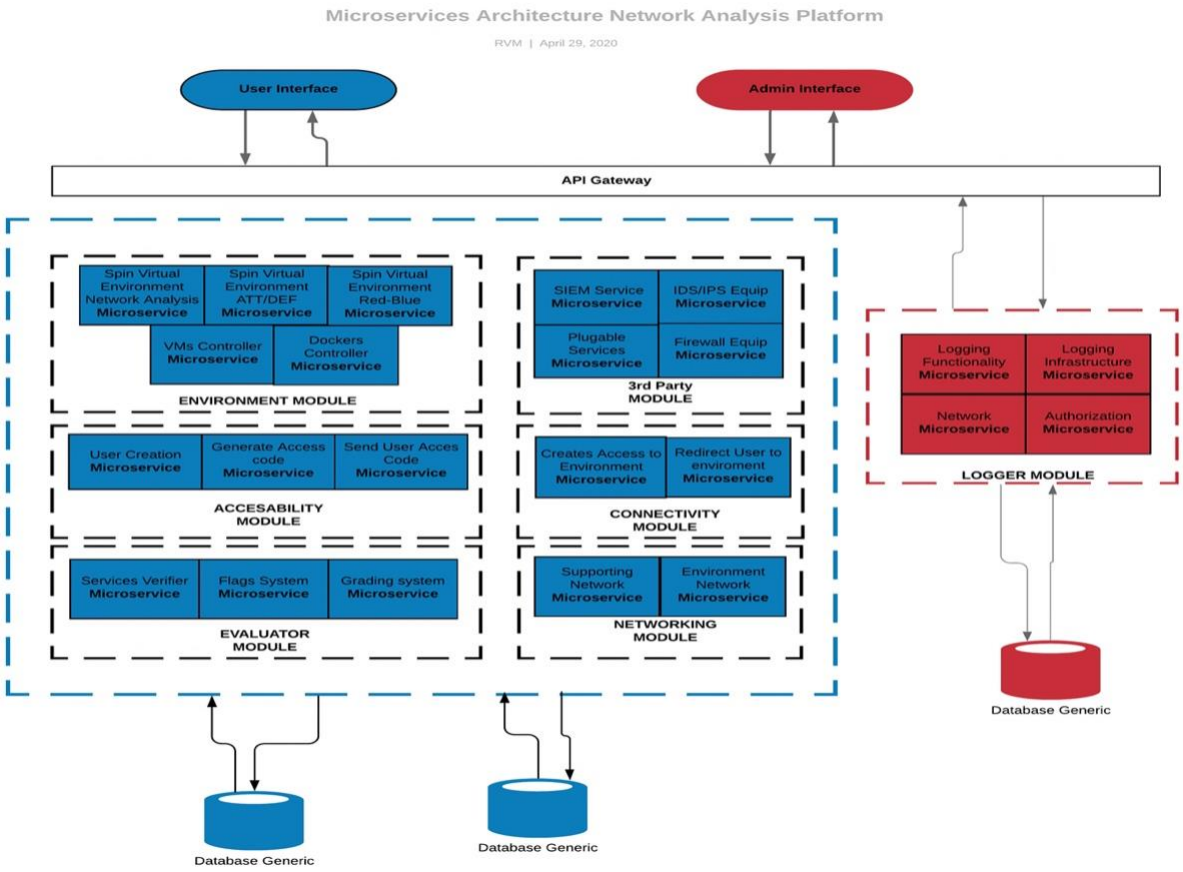

Figure 1: *Network Analysis Platform Architecture Diagram. The platform consists of an administrative and an infrastructure part. Various modules in each part cover different aspects of the whole platform and are implemented with a collection of microservices, which provides scalability, among many other benefits.*

Some of the core advantages for using microservices are *Isolation* - if some of the functionalities during the existence of the project might need to be maintained this can be done locally with having a major impact on the whole system. As it was already mentioned in section 3, *Scalability*, is a crucial aspect both in regard to the product lifecycle by allowing to easily add new components and features, but also to help the development. A Microservice architecture permits that different microservices will be replicated and divided across different servers, providing scalability. This not only facilitates the load balancing but allows multiple small instances of the platform to run different activities. Moreover, microservices allow for multiple development choices now and in the future, which ensures a high degree of *Flexibility*. Finally, Microservices guarantee rapid development by their *Agility*, since they are strongly related to common practices of software development and information technology operations.

The platform consists of two parts: The *Infrastructure* (Blue part of Figure 1) and the *Administration* (Red part of Figure 1). The two parts are made from modules which are made from several microservices that aid in serving the different functionalities. The Administration microservices are responsible for managing, for instance, errors and information from the platform, but also for providing a method of accessing the platform as an administrator. The Infrastructure part is supporting the scenarios presented in section 4. To create a structure between the different microservices that will be used, they are grouped into different modules and the following main modules can be depicted based on the main functionalities that they will serve: *Environment Module, 3rd Party Module*, *Accessibility Module, Connectivity Module*, *Evaluator Module*, and *Networking module*. Therefore, in the remaining part of the section, the main modules will be explained based on the functionality they intend to serve and how they are connected with the rest of the blocks.

Starting from the *Accessibility Module* which is responsible for user-related functionalities, such as creating an account to the platform and providing access to the platform, then *Connectivity module* it is involved by creating the connection link and by taking the user to the correct environment. Context is created with the Environment module, by generating the necessary virtual components that are used for the scenarios. Moreover, in setting up the context the *3rd Party Module and Networking Module* are involved, the first can integrate already existing libraries into the environment, while the Networking Module will take the responsibility for creating the necessary networks both inside an environment but also for

the platform itself. Lastly, the game design is implemented through the *Evaluator module*, which provides a method to assess the players' progress, also using the *Environment module* to verify during a scenario if certain services are running.

5. Discussion and Conclusion

This paper covers a wide range of cybersecurity trainings by including both a defense perspective, as well as an attacking one. Furthermore, the base structure of the platform allows the creation of new scenarios based on the existing ones. For instance, a possible new scenario that can be created is a *Decoy* one where students can learn/train their techniques of a cyber incident containment. First, they can identify the source of the threat and then use proper techniques to isolate it. This new scenario can be created based on the existing development by taking advantage of the existing labs and virtualization and by modifying some of the already established networks and connections between labs. However, it is still an ongoing challenge to observe how the described scenarios perform in maintaining user motivation and entertainment level while the learning process is maximized.

Creating proper cybersecurity education represents a challenge for many organizations, both from the private sector but also universities. Many approaches have been taken towards creating a proper training framework and the most widely used method were in terms of CTF competitions. Even if CTFs represent a great approach towards learning cybersecurity it is necessary to focus the training towards the learning process in these competitions. For this reason, the principles of game design can be integrated with cybersecurity training for enhancing the learning and motivation for the users. Nonetheless, the learning is effective if it can be done progressively, by building up on knowledge from the previous levels before the whole picture of a game is formed. Moreover, designing training solutions that do not require extensive work from the organizers is desired, since it facilitates to run in different settings with different types of audience. Automated and virtualized environments can be used by many people while their focus remains on the learning process.

References:

Amorim, Joni A., et al. "Gamified training for cyber defence: Methods and automated tools for situation and threat assessment." NATO Modelling and Simulation Group (MSG) Annual Conference 2013 (MSG-111), 2013. 2013.

Broholm, Rasmus, Olga Paulina Pilawka, and Dominika Illes. 2020. 'Development of a Training Platform for Cybersecurity Crisis Simulation'. Work under submission; To be submitted in June 2020.

Crumpler, William, and James A. Lewis. "The cybersecurity workforce gap." Center for Strategic and International Studies, Washington, DC. [Online]. Available: https://www. csis. org/analysis/cybersecurityworkforce-gap (2019).

Findley, Michael R. 2011. 'The Relationship between Student Learning Styles and Motivation during Educational Video Game Play': International Journal of Online Pedagogy and Course Design 1 (3): 63–73. https://doi.org/10.4018/ijopcd.2011070105.

Fujimoto, Toru, Yuki Fukuyama, and Tomoko Azami. 2015. 'Game-Based Learning for Youth Career Education with the Card Game "JobStar"', 8.

Furfaro, Angelo, Antonio Piccolo, Domenico Saccà, and Andrea Parise. 2016. 'A Virtual Environment for the Enactment of Realistic Cyber Security Scenarios'. In 2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech), 351–58. https://doi.org/10.1109/CloudTech.2016.7847720.

Granlund, Rego, Erik Berglund, and Henrik Eriksson. 2000. 'Designing Web-Based Simulation for Learning'. Future Generation Computer Systems 17 (2): 171–85. https://doi.org/10.1016/S0167-739X(99)00112-0.

Katsantonis, Menelaos N., Panayotis Fouliras, and Ioannis Mavridis. 2017. 'Conceptualization of Game Based Approaches for Learning and Training on Cyber Security'. In Proceedings of the 21st Pan-Hellenic Conference on Informatics - PCI 2017, 1–2. Larissa, Greece: ACM Press. https://doi.org/10.1145/3139367.3139415.

Kumar, Abhishek, Subham Kumar Gupta, Animesh Kumar Rai, and Sapna Sinha. 2013. 'Social Networking Sites and Their Security Issues' 3 (4): 5.

Nagarajan, Ajay, Jan M. Allbeck, Arun Sood, and Terry L. Janssen. 2012. 'Exploring Game Design for Cybersecurity Training'. In 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 256–62. Bangkok: IEEE. https://doi.org/10.1109/CYBER.2012.6392562.

Panum, Thomas Kobber, Kaspar Hageman, Jens Myrup Pedersen, and René Rydhof Hansen. 2019. 'Haaukins: A Highly Accessible and Automated Virtualization Platform for Security Education'. In 2019 IEEE 19th International Conference on Advanced Learning Technologies (ICALT), 2161-377X:236–38. https://doi.org/10.1109/ICALT.2019.00073.

Roschke, Sebastian, Christian Willems, and Christoph Meinel. 2010. 'A Security Laboratory for CTF Scenarios and Teaching IDS'. In 2010 2nd International Conference on Education Technology and Computer, 1:V1-433-V1-437. https://doi.org/10.1109/ICETC.2010.5529213.

Trickel, Erik, Francesco Disperati, Eric Gustafson, Faezeh Kalantari, Mike Mabey, Naveen Tiwari, Yeganeh Safaei, Adam Doupe, and Giovanni Vigna. n.d. 'Shell We Play A Game? CTF-as-a-Service for Security Education', 10.

Vykopal, Jan, and Miloš Barták. "On the design of security games: From frustrating to engaging learning." 2016 {USENIX} Workshop on Advances in Security Education ({ASE} 16). 2016.