Engaging Students in Basic Cybersecurity Concepts Using Digital Game-Based Learning: Computer Games as Virtual Learning Environments

Stylianos Karagiannis and Emmanouil Magkos

Department of Informatics, Ionian University,
Plateia Tsirigoti 7, 49100, Corfu, Greece,
{skaragiannis,emagos}@ionio.gr

Abstract. Teaching various topics using gamification elements or Game-Based Learning (GBL) methods is a top trend nowadays. Gamification has shown great results towards this direction, however, the usage of GBL methods has not been sufficiently studied for the effectiveness of the learning process. This study examines how instructional design could be applied and how computer games could be a learning environment for acquiring the basic skills and experience in fundamental cybersecurity topics. Towards this direction, this research aspires to discover how specific computer games, designed as simulations, could be converted into virtual learning environments and enhance the learning process, by increasing the levels of motivation and engagement of undergraduate students in the topics of cybersecurity. Computer games are appropriate for creating effective virtual learning environments specific to cybersecurity, providing positive learning outcomes. More specifically, in this study a commercial computer game is evaluated for the effectiveness of using GBL to the learning process. The result of this approach is a learning experience, featuring positive outcomes in terms of engagement and distinct impact in terms of perceived learning. For this study, the ARCS motivation model was used, for evaluating motivation levels and for investigating potential attributes which are related to perceived learning, knowledge and skill acquisition.

Keywords: Game Based Learning, Gamification, Cybersecurity, Instructional Design, Cybersecurity Training

1 Introduction

Playing computer games has been correlated to different behavioural, motivational, cognitive and perceptual outcomes [1,2,3]. Using computer games along with the official educational material could be a solution for maintaining self-paced learning tasks resulting in obtaining high levels of engagement and motivation during the learning process. Within a game, students are usually called to solve complex tasks and gradually acquire the desired skills. Using gamification elements in the learning process has shown great results in the past [4,5,6,7,8]. Approaches like Problem and Challenge Based Learning (PBL and CBL) [9,10,11], introduce rewarding systems and other fun elements to the teaching material [12,13]. CBL and PBL methods follow the learning by experience method, based on theories of *social constuctivism* [14,15,16,17], and often require high potential and effort from the participants in order to complete the tasks [20]. Maintaining balance between learning, competitiveness, social collaboration and creativity, while presenting sufficient academic and educational context still remains a research challenge [18]. Towards this direction, computer games could be a solution [19,20,21,22].

Gamification turns the learning process into a game by embedding various gamification elements, while *Game-Based Learning (GBL)* is using some of the elements of a game, such as a computer game as part of the learning process [23,24]. Through GBL, instructional material is able to be presented to the participants, while they experience a gamified learning experience [25]. Active participation together with fun elements are important for enhancing the learning experience in order to convert it into a more interesting and engaging process[26]. Finally, GBL has been used successfully in various knowledge topics [20].

The effectiveness of gamification and GBL in terms of skills and knowledge acquaintance has been extensively studied [20,4] with respect to how such methods could be effective in terms of the learning process [27,18,28,29]. However, maintaining the participants motivated during the learning process, while achieving high levels of engagement is usually difficult. Especially in cybersecurity topics which usually require advanced technical skills, more engaging methods are required in order to achieve the required learning outcomes. Most of the issues derive from the complex concepts that participants are called to understand and usually require strong background knowledge [30,8]. Even if it is applicable to enhance the learning experience using *virtual learning environments* [31], the set of tasks are usually difficult to be followed by undergraduate students.

Computer games have already been used for teaching various concepts in computer science. For instance, particular approaches for teaching Boolean algebra are computer games focused on hardware design such as *”MHRD”*[1] and *”TIS-100”*[2] for teaching assembly language and computer architecture [32]. Another interesting approach is *”Shenzen I/O”*[3], a circuit deisng game, focused on acquiring familiarity in various concepts of engineering and computer architecture. These approaches tend to be able to improve coding skills, however, sufficient empirical data to quantify or to evaluate the effectiveness of the learning outcomes do not exist [33]. On the other hand, regarding tabletop games, empirical data exist which usually evaluate the positive impact of these approaches in terms of general introductory knowledge [34].

[1] https://store.steampowered.com/app/576030/MHRD/

[2] http://www.zachtronics.com/tis-100/

[3] https://store.steampowered.com/app/504210/SHENZHEN$_{I}O/$

For integrating educational context and maintaining balance between acquiring knowledge while having fun, it is important to highlight specific indicators which affect the learning outcomes. It seems that using computer games as virtual learning environments could enhance the total learning experience [35,36]. One of the most popular approaches for presenting cybersecurity challenges are *virtual machines* which are based on systems that maintain various vulnerable services and technologies. These approaches are usually used in *Capture The Flag (CTF)* challenges, where participants are called to solve puzzles and try to exploit the vulnerabilities of the systems. Through CTF challenges participants can actively participate in the learning experience and achieve high levels of engagement [37]. Towards this direction, practical customized courses and exercises could be developed, in order to train people in terms of cybersecurity threats and attacks [38,39]. Cybersecurity topics often include complex processes and as an outcome, educational context must be presented as sub-tasks and reward the participants, in order to increase their motivation and persistence towards finding appropriate solutions.

Gamification and table-top games has been previously applied in education. Some of the approaches combine storytelling and puzzles [40,41], while the most popular approaches of table-tops for cybersecurity are *Control-Alt-Hack* [42,43] and *d0x3d!* [44]. However, further research is needed for providing sufficient empirical data, related to the learning outcomes and to the acquired skills. Furthermore, cybersecurity training using *serious games* is a young and developing field [45]. Serious games related to cybersecurity such as *CyberCIEGE* have been mentioned together with commercial computer games like *Hacknet-labyrinths* [46,47]. Furthermore, specific studies relate education directly to games [48]. Moverover, CTF challenges and online cybersecurity challenges have been described along with serious games in a relative context. In order to discover how to adopt real-world challenges [49,50,51] and security scenarios in a computer game, a specific learning and educational methodology is required.

Embedding computer games, gamification and GBL in cybersecurity education, will continue to evolve and the enhancement of learning processes will most probably engage students in cybersecurity topics, together with the positive outcomes of increasing security and privacy awareness [52,53]. A few studies show that empirical evidence towards this direction currently exists, however, no clear evidence is mentioned in terms of using these methods as an assessment method [54,55,38,56,25,57,58].

1.1 Our Contribution.

The main purpose of this research is to evaluate how and whether *Digital Game-Based Learning (DGBL)* could enhance the learning experience regarding cybersecurity curriculum in academia, achieving high levels of engagement and active participation. This paper seeks answers to the following questions:

1. How can education be more interesting with the adoption of gamification elements and how can DGBL could be used in order to create virtual learning environments to this aspect?

2. What are the potential benefits and limitations regarding the learning effectiveness of DGBL in conducting cybersecurity training labs?
3. Which specific attributes derive from DGBL and possibly affect positively the learning outcomes?

More specifically, in this study, the commercial computer game, Nite Team 4[4], is evaluated in terms of the effectiveness of adopting DGBL into the learning process. This study aspires to make a contribution in providing empirical data and evidence on how and whether computer games can provide sufficient background knowledge and skills acquaintance in cybersecurity courses. With the implementation and evaluation of DGBL [28] as a main virtual learning environment in cybersecurity, this study aspires to fill the gap between theory and practice presenting a self-learning experience with the option to integrate with a collaborative learning process inside the classroom [49].

Our approach is highly correlated with approaches like CTF challenges and more specific Classroom Capture the Flag Challenges [59]. Using the recommended approach, students were able to acquire technical experience and skills in basic cybersecurity topics, in ethical hacking and penetration testing. Furthermore, the students were introduced to technical skills in topics of IT, while learning by experience the concepts that were already instructed according to the official academic curriculum.

1.2 Outline

This paper is organized as follows: Section 2 presents the methodology used for this research. Section 3 discusses background concepts and principles that were used in our approach, while Section 4 presents our approach. In Section 5, results and discussion of this research are given. Section 6 concludes the paper.

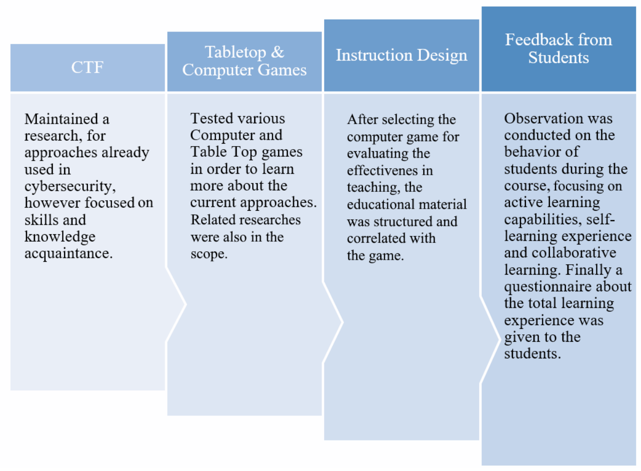
2 Methodology

For this study a few computer and tabletop games were examined outside the classroom, including Hacknet and Hacknet Labyrinths, TIS-100, Shenzen I/O, [d0x3d!] and Control-Alt-Hack [42,44,46,32,23]. The chosen approaches include attributes which focus on skills and experience acquaintance and on discovering elements which enhance the self-learning experience.

For integrating educational material while maintaining balance between fun and knowledge, it is important to specify the key-elements which might affect the learning outcomes. The specific game has been chosen to be presented in the lab in order to quantify the effectiveness in terms of the learning outcomes. To ensure that DGBL methods enhance active participation during the learning process, participants were introduced to the in-game context in order to be familiar with the main concepts. Specific directions were given before starting the learning process.

[4] https://www.niteteam4.com

In Fig.1, the main steps which were followed in our approach are presented. During our study, active learning and instructional design guidelines were first analyzed for collecting a concrete and conceptual index, in order to maintain balance between fun and learning.



CTF

Maintained a research, for approaches already used in cybersecurity, however focused on skills and knowledge acquaintance.

Tabletop & Computer Games

Tested various Computer and Table Top games in order to learn more about the current approaches. Related researches were also in the scope.

Instruction Design

After selecting the computer game for evaluating the effectivenes in teaching, the educational material was structured and correlated with the game.

Feedback from Students

Observation was conducted on the behavior of students during the course, focusing on active learning capabilities, self-learning experience and collaborative learning. Finally a questionnaire about the total learning experience was given to the students.

Fig. 1. Methodology steps

Towards this direction, a specific computer game, called NITE Team 4 was selected mostly because of the high correlation between the in-game context and of real-world tools and methods. More importantly, the computer game is presenting extra information by providing various website links.

The following principles were taken into consideration for creating our methodology [62,60] derriving from Vygotsky's theories on Zone of Proximal Development:

1. Provide related context to what have been already instructed before, in order for the participants to recall any required information [60].
2. Organize the learning process in four different stages and embed various sub-goals in order to build up gradually from simple to complex concepts [60].
3. Emphasize on team collaboration [61] and on the importance of setting questions during the learning process [62].
4. Enhance the process with self-learning capabilities, in order to bypass the knowledge and experience gap between the participants [62,60].
5. Maintain the concepts and scenarios in difficulty levels which will be comfortable and at the same time challenging [62,60].

Expected learning goals include improvement in terms of background knowledge, skills acquaintance that are mostly related to basic concepts and methods, used in ethical hacking and penetration testing. Most of the presented processes are similar to real-world processes. The presented context inside the computer game helps for creating a real-world learning environment, providing rich context and a variety set of challenges.

The experiment was conducted on undergraduate students for enhancing the learning process of a specific course in the Department of Informatics, Ionian University, Corfu, Greece. Most of the participants did not have any significant experience and knowledge in cybersecurity. Specifically the observation was focused on discovering actions that highlight attributes of collaborative learning, indicators that present self-learning experience elements and connection to theoretical concepts. During the learning process, a variety of educational and informative material according to cybersecurity concepts has also been instructed. For analyzing the motivational aspects of learning environment, *the ARCS model of Motivational Design* [63] was taken into consideration. The questionnaire was based on the four key elements of the above model, namely Attention, Confidence, Relevance and Satisfaction [63]. During the learning process other various observations were performed related to the students' behavior and are described in Section 4.

2.1 Common approaches in Cybersecurity topics

To begin with, it is important to present approaches of computer games and other gamification approaches, which were previously tested before this study, focusing on the expected learning outcomes. These approaches are worth-mentioning and were previously tested for discovering the key elements which might enhance our approach and might be used in future research.

Computer Games. Various approaches are presented on commercial computer games, mostly in the form of simulations.

1. **Hacknet Labyrinths[5]:** *Hacknet Labyrinths* is a simulation-based hacking computer game, featuring real-world networks and real-like system infrastructure. A set of tool-kits for penetration testing and ethical hacking similar to the real ones is presented [46].
2. **Uplink[6]:** The main positive learning outcomes of this game is to introduce network commands and familiarity in UNIX systems along with other basic topics of cybersecurity. However this approach is mostly a computer game featuring only themes deriving from cybersecurity [64].
3. **NITE Team 4[7]:** NITE team 4 is also a simulation computer game featuring topics of cybersecurity and adopting real terminology from NSA leaks. Tools that already exist in the real world are also presented in the computer game. The high engagement and the similarities with real ethical hacking tools

[5] http://www.hacknet-os.com/
[6] https://www.introversion.co.uk/uplink/
[7] https://www.niteteam4.com/

and methods are the main attributes of this game, as well as the ability to create custom puzzles and challenges. Related information about network protocols and topology is presented, as well as real tools and services. The main difference with Hacknet is that methods presented in NITE Team 4 are similar to the real ones and the steps are clearly stated in terms of learning basic concepts of cybersecurity. Moreover, the in-game context is enhanced with educational material regarding real-world information such as real ethical hacking tools and penetration testing methods.
4. **CyberCIEGE[8]:** CyberCIEGE focuses on cyber defense where participants access a real VPN network. The target group for this game is to prepare workforce such as system engineers, software developers, system designers and network administrators in order to increase security awareness.

Vulnerable Virtual Images. Well known approaches for enhancing the learning process include the use of virtual systems that are vulnerable. These approaches are also used on CTFs, however the challenges usually are able to be hosted individually, focusing on self-learning experiences. Some approaches are published in ***Vulnhub***[9] and others are published in official websites like the well-known virtual machine of ***Metasploitable***[10] from Rapid7. Furthermore, some other challenges are published in ***Over the Wire***[11]. Finally, various conferences publish the challenges and the solutions of conducted past CTF challenges.

1. **Vulnhub:** This website maintains various vulnerable virtual systems, focused on learning the basics in cybersecurity. Using walkthroughs the participants are able to learn and get help from others. Afterwards, it is possible to try and solve the challenges without using the walkthrough, since the website provides also vulnerable images for which the solutions are not provided.
2. **Metasploitable:** A well-known virtual image featuring various vulnerabilities. Focused on web exploitation methods this image features a large variety of vulnerabilities.
3. **Over the Wire:** This website maintains a variety of challenges which are presented and accessed mostly through SSH. Focused on step-by-step learning experience and featuring walkthroughs it is considered as a nice approach for beginners.
4. **Hack the Box[12]:** This approach is one of the most known in conducting individual CTFs. Hosting a lot of challenges, this platform maintains many vulnerable images and CTF challenges that participants can access using a VPN. This platform mostly focuses on various levels of challenges, however most of the challenges are for advanced users. This platform features options for workforce acquaintance and a large community. Moreover, this platform has been presented in various conferences for providing CTF challenges.

[8] https://my.nps.edu/web/c3o/cyberciege

[9] https://www.vulnhub.com/

[10] https://sourceforge.net/projects/metasploitable/

[11] http://overthewire.org/wargames/

[12] https://www.hackthebox.eu

Tabletop Games. Furthermore, in this study the following tabletops were also studied:

1. **Control-Alt-Hack**[13]**:** Control-Alt-Hack is a card game for increasing security awareness. The game mechanics and designed content is engaging, encouraging interest in computer security. The findings were positive in terms of increasing security awareness and it was conducted on 22 educators representing 450 students [42].
2. **[d0x3d!]**[14]**:** [d0x3d!] is an open source card game. designed for informal computer security education [44]. The game is cooperative and players assume the role of white-hat hackers, with the main task of retrieving digital assets from an adversarial network. The card game is released in three different forms[15].

Most of the table-top games focus on acquiring familiarity related to cybersecurity terminology.

3 Background: Gamification and GBL

3.1 Active Participation and high levels of engagement

A balance between challenges, instructive material and assessments together with gamification elements could result in positive learning outcomes [65,20]. GBL provides fast response between action and feedback resulting in self-learning and self-assessment elements, similar to approaches like "learning from mistakes" [20]. These attributes are important for achieving high motivation and for developing self-paced elements during the learning process. Games have been highlighted with the method of ”try and error”, which is important for motivating players to keep trying until they succeed.

As a result, computer games could provide a sufficient learning environment as already applied in serious games [1,66,67,27]. Context which is related to real-world cases and challenges could be presented inside a computer game. When carefully designed, the pedagogic content could be embedded and with the integration of quizzes and interactive exercises, computer games could provide the opportunities for achieving high levels of engagement through interaction and exploration [56,68,69,70,1].

3.2 Gamification, GBL and expected Learning outcomes

In approaches like gamification and GBL, the expected learning outcomes have to be described and specifically depicted. To enforce appropriate instructional context, the expected learning outcomes have to be specified. Entertainment elements alone could not guarantee sufficient learning outcomes. The differences between Gamification and GBL are presented in table 1 in order to distinct such indicators.

[13] http://www.controlalthack.com/

[14] http://d0x3d.com/

[15] https://github.com/TableTopSecurity/d0x3d-the-game

Gamification	Game Based Learning
Gamification is turning the learning process as a whole into a game, using gamification elements like reward system, badges, storytelling, theme-related context, different levels, Leader-boards	GBL is using a game as part of the learning process, using learning games to achieve an instructional goal. Serious games and classical computer games or table-top games might be included.
Game design and game elements in non-game context. Convert instruction to a game-like approach.	Educational content is included in the game. Play a digital or non-digital game in order to achieve the required learning outcomes.

Table 1. Differences between Gamification and GBL [82,55]

In order to be effective in terms of the learning outcomes, pedagogical principles and directive instruction material has to be carefully embedded and organized [71]. Towards this approach, implementations that provide simulations focused on network infrastructure do exist[72].

Basic Principles of Gamification. The use of digital and physical games is often presented [35] together with specific exercises from suggested gamification approaches [73]. However, in order to accept the broad use of gamification in academia, more careful approaches have to be considered as well. Gee [74], for example, indicated that 16 learning principles could be offered from games such as: interaction, well-structured problems, challenge and consolidation, pleasantly frustrating, system thinking, exploration and cross-functional teams, among other principles [74,15,75,76]. These principles are directly related to cybersecurity concepts in order for the participants to discover design and configuration flaws.

Role of Engagement. The role of engagement in the learning process is also pinpointed during the design phase of a game [77]. When playing games, participants are called to solve complex challenges and participate without experiencing fatigue, while it is a comfortable learning task [58]. For achieveing the expected learning outcomes it is important to highlight the attributes that have potential positive impact on the learning process [78,68,83]. Towards this direction, careful and comprehensive methods are required in order to introduce the instruction material and to define the learning outcomes [79].

Learning outcomes and effectiveness. Specific studies argue that not all games could be effective as a learning environment and not all the participants will accept these methods [80]. Educational games are still in early stages of evolution and even nowadays more careful approaches have to be developed in order to achieve and to accept computer games as a successful learning approach.

Main issues include difficulties in terms of integrating educational context inside games [44].

The positive impact of Games. Despite the limitations of using GBL, games in general have been associated with the benefits below which result in positive learning outcomes [23]:

1. Games can be used for examining individual characteristics such as self-esteem
2. Games are fun, which consequently leads to undivided attention and focus for long periods of time, helps developing various IT skills and engages participants to make mistakes and learn from them.

3.3 GBL and Education in Cybersecurity Topics.

Educational domains that use GBL are interdisciplinary topics where skills such as critical thinking, group communication, debate and decision making are of high importance. Such topics require high collaboration and active participation in order to achieve the sufficient learning outcomes [20]. Towards this direction computer games could enhance this perspective and improve the attributes of collaborative learning and of active participation.

4 Using a Computer Game as a Virtual Cybersecurity Learning Environment

Integrating a computer game as a virtual learning environment is difficult, especially for presenting complex topics such as that of cybersecurity. Computer games maintain the ability to create self-learning experiences, by presenting interactive walkthroughs and step-by-step guidelines. Towards this direction, students were firstly introduced to basic methods of ethical hacking and penetration testing. It was mentioned in the classroom that a computer game will be used as a virtual learning environment, highlighting the correlation between real commands and of software tools. Finally, it was mentioned that approaches such as CTF challenges already exist in official training and that this proposed approach is a gamified version similar to CTF challenges.

4.1 Introduction to the Game

Participants were guided through a structured guideline and were called to fulfill the first steps and to learn the basic tactics, tools and commands. The first directions and information were presented with the following message: “ ”*. . . some of the most advanced technology used to hack through corporate systems and networks based on Real-World Events. The world today has evolved from regular warfare, to cyberwarfare. As such, we need experienced personnel to repel attacks* *from various sources at any given time. Join us for a better world...""*. The message depicts the aspect of being involved in real-world cases and to acquire skills for repelling attacks. In each step, participants were rewarded with badges as virtual certification credits. These features are important for the participants to be motivated and at the same time important in order to control and to evaluate their own progress.

Computer games maintain the ability to present step-by-step guides. The in-game guidelines were presented in a well-structured way which was effective in terms of enhancing the self-learning experience. It is important to maintain the attribute of self-learning, in order to bypass issues deriving from knowledge and skills gap between the participants. After each set of challenges, solutions were presented in the class for those who were incapable to follow.

First Section, the Academy. This section includes practices important for learning the basic commands and to be familiar with the required tools. The basic topics are the following:

1. Basic Terminal Operations
2. Digital Forensics
3. Network Intrusion
4. Command and Control
5. Elite Training
6. Signal Intelligence
7. StingerOS Advanced

Most of the missions were highly correlated to cyberthreats and cyberattacks, encapsulating information and software tools from the real-world.

Academy Level 1 - Basic Terminal Operations. This topic includes a set of practices and missions, which helps the participants to learn the basic tools and commands and get familiar with the environment. For example, 6 training missions were included in the first academy level (Fig. 2), containing a subset of missions. More specifically the sub-modules were the following: Stinger OS Basics, Basic OSINT, Fingerprint, Advanced OSINT, Exploit Database and Foxacid. All the above tasks included a code number (ex. SOPS.01, OSINT.01). The used terminology was similar to the official cybersecurity curriculum. For example, even from the beginning the tasks and missions related to official terminology such as *Open-source Intelligence (OSINT)* methods.

Academy Level 2 - Digital Forensics. Topics like intelligence gathering, directory enumeration and password attacks were presented. Moreover, concepts such as Xkeyscore (used from NSA) were mentioned deriving from elements of *Alternate Reality Games (ARG)* and in order to present real-world context.

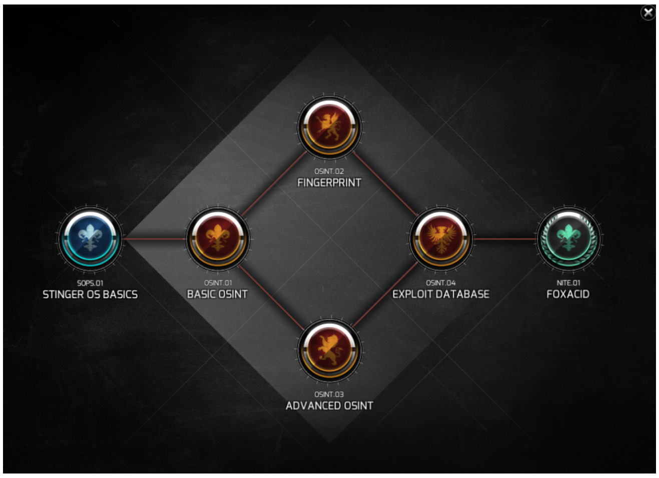


Fig. 2. Academy Level 1 – Steps and Progress Tracking

Academy Level 3 - Network Intrusion. Tools like Intelligence gathering focused on network infrastructure and exploitation tools were introduced. Concepts like *Man In The Middle (MITM)* were introduced, together with the Social Engineering Toolkit (SET Toolkit[16]).

4.2 Game Components

NITE Team 4 maintains a variety of tools, software components, modules and submodules in order to create more engaging and customized experience.

Information Gathering	Network Intrusion
Host Fingerprint	Phone CID Backdoor
Exploit Database	Password Attack
WMI Scanner	MITM
Air Crack	Social Engineering Toolkit
Active Directory	Hydra Terminal

Data Forensics	Advanced Tools
Xkeyscore Forensics	Turbine C2 Registry
File Browser	Satellite Feed
TBW Archive	Hivemind Network
Notepad	Command Center

Table 2. Main tools and software components

[16] https://github.com/trustedsec/social-engineer-toolkit

Gameplay Option - Section 1: Basic Software and Tools. The main tools and software components of the game are presented in table 2. The following tools were available for further processes:

- Stinger OS Cluster
- Satellite Feed (Drone and Geolocation Intelligence)
- Hivemind Network

Gameplay Option - Section 2: Missions. Using elements of storytelling which derive from real-world events and cases, the learning process could be transformed in an immersive and educational process. Missions are divided into four different sections. Every section and topic included a different set of challenges, featuring storytelling and multimedia elements. Every scenario or story, is called as *Operation*, maintaining sub-set of challenges and sub-tasks. The attributes of every mission are the following:

1. **Type:** The type of mission such as *Basic OSINT, enumeration or exploitation.*
2. **Real Life:** Correlation with real-world cases.
3. **Level:** Level of difficulty.
4. **Ambiance:** The role of the player in each mission.

Each mission has a unique name and a description. For example, a specific operation has the name *Operation Castle Ivy* and the description is the following: *"Military grade malware was stolen from NITE Team 4 as of yet unknown means. Assess the scope of the leak"*[17].

Gameplay Option - Section 3: Multiplayer/Hivermind Network. *Hivemind Network* is a module which includes challenges and puzzles created from other users, using an extra feature/software of Nite Team 4, called *"Network Administrator"* (Fig. 3). At the time we conducted this research, 51 different challenges were presented in NITE Team - Hivemind Network. Users are able to execute network mapping processes similar to *arp-scan* or *netdiscover.* Through this process, the user is possible to extract information related to network topology and discover the running services. Focusing on methods of reconnaissance, enumeration and OSINT the participants are able to get familiar with network topology and services. Every time a user discovers some information, using tools like *sfuzzer* or *fingerprint*, the discovered information is included in the network topology.

Custom challenges could integrate storytelling elements including interesting names and other related information and context. Every challenge is hosted in a virtual domain *".hvm".* which includes multiple services and assets. Subdomains and other system resources could be enumerated using reconnaissance methods in order to exploit the vulnerabilities and attack the systems. Each

[17] NITE Team 4 - In-game statement

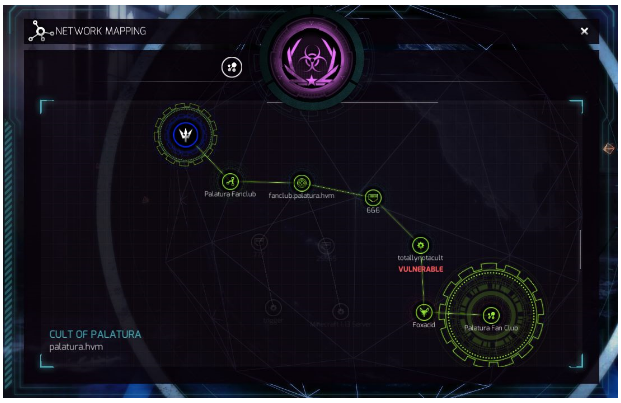
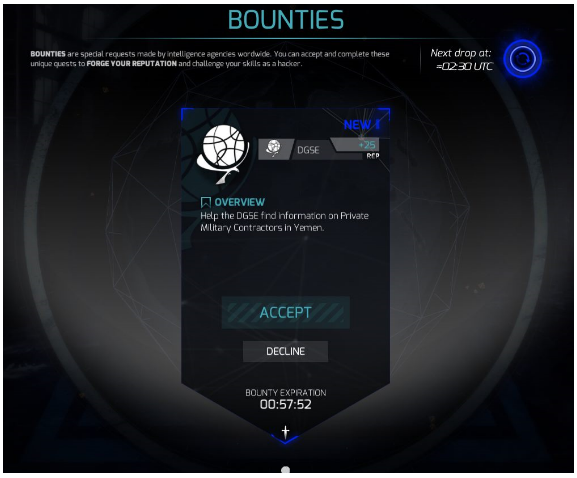


Fig. 3. Custom challenge created by another player

challenge holds information related to the duration of time needed for solving the challenge and indicators related to content quality, fun and difficulty level among others.

Gameplay Option - Section 4: Bounties. Participants were called to test their skills (Fig. 4 through challenges that have a time limit, maintain a rewarding system and give reputation points. This set of challenges are very similar to official CTF challenges.


BOUNTIES

BOUNTIES are special requests made by intelligence agencies wordwide. You can accept and complete these unique quests to **FORGE YOUR REPUTATION** and challenge your skills as a hacker.

Next drop at: ≈02:30 UTC

NEW !

DGSE +25 REP

OVERVIEW

Help the DGSE find information on Private Military Contractors in Yemen.

ACCEPT

DECLINE

BOUNTY EXPIRATION 00:57:52

Fig. 4. Special challenges with time expiration

Gameplay Option - Section 5: Open WorldCampaign. This option is a combination of ARG elements and of NITE Team 4 challenges. The potential of creating a real-world puzzle combined with storytelling elements could create real-world challenges and enhance the learning curve, since the engagement levels might increase.

Extra Module: Network Administrator. This is an extra software component, where users are able to create their own challenges and puzzles in order to make them public to the NITE Team 4 network universe. Network Administrator is still in beta version, however it is already up and running. All services, port numbers and other network and application components are highly correlated to real software components. Through this option, users are free to create a network topology and actually get familiar with threat modelling tools. Towards this direction, this tool could help the participants in terms of acquiring basic knowledge in topics of security modelling and systems' design. Moreover, this could be very important in terms of getting familiar with threat modelling tools and methods.

4.3 Comparison between Game and Real-world

In conclusion, it seems that correlation exists between the in-game concepts and real-world information. Towards this direction, it is important to mention that some users mentioned that some challenges, required skills in cryptography in order to complete the missions. This issue could be solved and enhance the learning experience in terms of real skills, if the users were introduced to basic principles and set of challenges between the main challenges. Basic methods and tools for executing the attacks are presented in Table 3.

Action	NITE Team 4	Real-world
Port Scanning	Fingerprint	Nmap
DNS Enumeration/ Sudomains (OSINT)	Osintscan	The Harvester, sublist3r
DNS Enumeration/ Sudomains (Wordlist)	Sfuzzer	Dirb, Dirbuster, DNSRecon
Search vulnerabilities	Searchsploit	Searchsploit
Discover running services	Netscan	Nikto, Wpscan
Packet Capturing (802.11)	Airodump	Airodump-ng

Table 3. Comparison between in-game commands and real commands

NITE Team 4 has been already announced as a partnership with the *International Air Transportation Association (IATA)* for setting practices in order to improve skills related to the topics of cybersecurity. Featuring real cases including modern cyberthreats, the main focus is to maintain threat cases for educational purposes. Moreover, showcases related to the game are also presented in events such the RSA Conference, The Black Hat convention and SecTor conventions[18].

Real-world Cases. The following methods are presented and are highly correlated to real cases used in ethical hacking and penetration testing:

1. Reconnaissance and Intelligence Gathering: Processes related to network scanning, sub-domain enumeration and network mapping using in-game tools such as *sfuzzer* and *OSINTscan.* Afterwards participants are invited to execute port scanning and vulnerability analysis using the related software components and tools.
2. Network Infiltration: Participants are called to attempt connecting to the network using various rootkits and exploits.
3. Network Scanning (Insider): Participants have to execute commands such as *netscan* and *airodump* for discovering any devices connected to the network and also for discovering and enumerating folders across the network, such as shared folders.
4. Password Attacks: Participants have to launch password attacks in order to access services and enumerate devices in the network. Basic tools are introduced which are similar to the real ones. Generic tools like *John the Ripper* and text files such as *RockYou.txt* are presented in this section. For example RockYou.txt is a popular wordlist used for bruteforce attacks and John the Ripper is a well-known software tool for executing password attacks.

Moreover, basic malware, hacking tools and exploits such as rootkits *Assassin* and *AfterMidnight* are presented. An in-game software tool called *Foxacid Server* is mostly used for exploits like *Metasploit.* Furthermore, commands such as *searchsploit* is presented in order to discover information related to exploits and vulnerabilities known as *Common Vulnerabilites and Exposures Exploits(CVEs).*

Finally, the game provides more information regarding each concept and tool, redirecting the user to various websites, blogs and Wikipedia pages in order to learn more information regarding to real commands and software tools. For instance, information is provided related *Kali Linux* and *Metasploit* during the in-game exploitation phases. It is considered important for the students to follow such links, in order to learn more about the type of attacks and to understand the tools.

5 Results and Discussion

The learning outcomes from our approach were evaluated using the following indicators [63]:

1. **Attention:** Refers to elements of perceptual stimulation, active participation and the ability to present similar context to the participants' interests.

[18] https://aliceandsmith.com

2. **Relevance:** Includes elements which help the participants understand the relevance between past knowledge and includes specific goal orientation, familiarity and context related to the learner's needs and motives.
3. **Confidence:** Attributes which enhance the learners' positive expectation for success, personal responsibility and self-control elements, that participants have during the learning process.
4. **Satisfaction:** Enjoyable and fun elements, and features such as extrinsic rewards while enhancing the extrinsic and intrinsic reinforcement related to the effort.
5. **Perceived Learning:** Refers to attributes like self-report capabilities, knowledge acquaintance or more accurately as *"Self-report of knowledge gain, generally based on some reflection and introspection"* [81].

For each of indicator, participants were called to answer in a 7-point Likert scale if they disagree (grade-1) or totally agree (grade-7). Deriving from Keller's model of Motivation (ARCS), the concepts of Attention, Confidence, Relevance and Satisfaction [63] are presented, along with the statements which were included in this research. The indicator of actual learning is not evaluated, since specific assessment methods have to be integrated in order to achieve such results.

Attention. The main objective is to achieve high attention levels, in order to increase levels of engagement during the learning process. In Table 4 the statements related to the element of Attention are presented.

Item Code	Statement
ATT1	The presented process included various self learning capabilities.
ATT2	During the lab I was focused and absorbed in the process.
ATT3	It is an "eye-catchy process".
ATT4	The way in which learning objectives were presented helped me focus.
ATT5	Storytelling is exciting and it helps me to go on.

Table 4. Questionnaire items to evaluate "Attention"

During the process, participants indicated high levels of attention, active participation and collaborative learning, achieving high levels of engagement. Regarding the statements in Table 4, average score for ***Attention* was 73.46%.** Some participants scored very low in evaluating the total process as a good approach for cybersecurity training and it was mentioned that approaches like CTF would be more appropriate. However, it was highlighted that gamification elements would enhance the approach, for instance if gamification elements were embedded in a specific CTF challenge.

Relevance. In Table 5, it is perceived that participants which have strong background knowledge would understand most of the presented cybersecurity topics. As a result participating in such challenges could improve skills related to other IT topics such as Databases and Operating Systems. Therefore, it is still difficult to understand how this process could result in achieving better grades in terms of evaluation processes such as exams. However, acquiring skills and background knowledge through this method may eventually have a positive impact in other topics of IT. The average score for ***Relevance*** **was 76.40%.**

Item Code	Statement
REL1	It reflects, to a good extent, possible real case scenarios.
REL2	I can correlate the content with concepts that I am already familiar with such as Databases, Networks, Programming, and Operating Systems.
REL3	The content is related to my general interests in the scientific field.
REL4	This methodology corresponds to my IT needs.
REL5	I am awareof most topics and I can discover related information in topics of Programming, Databases, Network and Web Infrastructure.

Table 5. Questionnaire items to evaluate "Relevance"

Confidence. Participants mentioned that self-learning features are very helpful and improves their ability to maintain control during the entire process (Table 6). Towards this direction, computer games could be used as self-assessment methods in evaluating every step of each challenge. Elements of high interactivity enhance participants' confidence and together with elements of collaborative learning, the learning process achieve high engagement levels. Most of the participants wanted to continue the process after acquiring sufficient familiarity related to basic basic in-game concepts. The average score for ***Confidence*** **was 74.76%.**

Item Code	Statement
CON1	How much despite the difficulties this methodology increases the feeling of perseverance in order to discover the solution.
CON2	I want to finish the lab (to see everything - it is interesting).
CON3	I would like to explore hidden sub-challenges or optional context.
CON4	Gradually and during the lab, I think I can cope better and I feel self-confident.
CON5	This methodology does correspond to my IT needs.
CON6	During the process I feel I have the control.
CON7	Using this method as an assessment method is a good idea. I am not scared of that as much as of the exams.

Table 6. Questionnaire items to evaluate "Confidence"

Satisfaction. Some participants mentioned that this process was the best and most enjoying process they ever had during their undergraduate studies (Table 7). Collaborative learning could enhance the engagement levels and make the learning environment more entertaining. Average score on ***Satisfaction*** **was 78.47%.**

Item Code	Statement
SAT1	I would like to repeat this process without caring for academic rewards and marks. I would like to learn more.
SAT2	Really, I had a lot of fun.
SAT3	I did not feel tired when I played.
SAT4	I feel satisfied after the lab.
SAT5	I really enjoyed this process as a virtual learning environment.
SAT6	I felt that time passed very quickly.
SAT7	I felt happy during the process.

Table 7. Questionnaire items to evaluate "Satisfaction"

Perceived Learning. For ***Perceived Learning*** **the average score was 78.70%.** The statements for assessing perceived learning are presented in Table 8.

Item Code	Statement
PER1	Could create the right environment for learning more information and acquire skills.
PER2	It is like a virtual learning environment, however it requires customization.
PER3	It might help me to improve my grades (as a result of familiarity with other fields).
PER4	It is perceived by me that I have developed some skills.
PER5	I can perceive that through this methodology I acquired knowledge and skills.

Table 8. Questionnaire items to evaluate "Perceived Learning"

Real-world tools and case scenarios. It is important to mention the importance of including real-world scenarios, tools and commands during the learning process. Towards this direction the virtual learning environment is important to be a representation of real cases and scenarios [4]. Since in this study a computer game was used, it is important to compare it with the commands and tools used in the real world. In Table 9 the statements for evaluating how much the computer game matches reality are presented.

Item Code	Statement
REA1	The presented challenges were similar to real-world incidents.
REA2	This method is good for acquiring basic familiarity with some of the real penetration tools.
REA3	Multi-faceted learning, helps me to understand most of the methods
REA4	It is possible that the presented scenarios and cases could be real cases.
REA5	Cases are very real. If I did not know that the system is a game i would possibly think that this is real.

Table 9. Questionnaire items to evaluate "Real-world tools and case scenarios"

From the participants' responses on the statement of how much the the process reflects a real case scenario, the answers were positive. However it was mentioned that some commands and software tools do not exist in reality. High correlation was indicated with Kali and other penetration tools and methods. The **correlation between real-world software tools and cases in contrary to the in-game context scored 72.20%.**

Related topics and Perceived learning. Since topics of cybersecurity require strong background knowledge in other IT topics, it is inevitable that we have to identify if perceived learning is achieved in other topics as well. Towards this direction it is important to identify any direct or indirect impact to the learning outcomes in general.

Item Code	Statement
REL1	It would be nice to have similar learning processes with the right customization context in other courses as well.
REL2	After my participation, my learning ability in other fields seems to improve.

Table 10. Questionnaire items to evaluate "Impact on other related fields"

In Table 10 the statements which declare if this approach would have a positive impact in other related topics are presented. **The possibility for our approach to present other IT topics which are relevant to cybersecurity scored 80.51%.**

5.1 Summary

The ARCS model itself provides information about the impact of the process on the engagement levels during the learning process. In our research high levels of students' engagement were achieved during the learning process. The average scores are summarized in Table 11.

Attribute	Average Score(%)
Attention	73.46%
Relevance	76.40%
Confidence	74.76%
Satisfaction	78.47%
Perceived Learning	78.70%
Relevance with other Topics	80.51%
Real-world	72.07%

Table 11. Summary scoring table

Our approach takes into account the ARCS model [63] for evaluating motivation levels and for discovering the elements which are related to perceived learning. Most of the participants scored this method sufficient in terms of using this method as a learning process. Attributes such as actual learning and the usage of this method as an assessment method are not evaluated. Towards this direction more work is required regarding the impact of the specific approach in other I.T topics. **Total score of this approach acceptance from students indicates 76.49% acceptance as a sufficient learning method.**

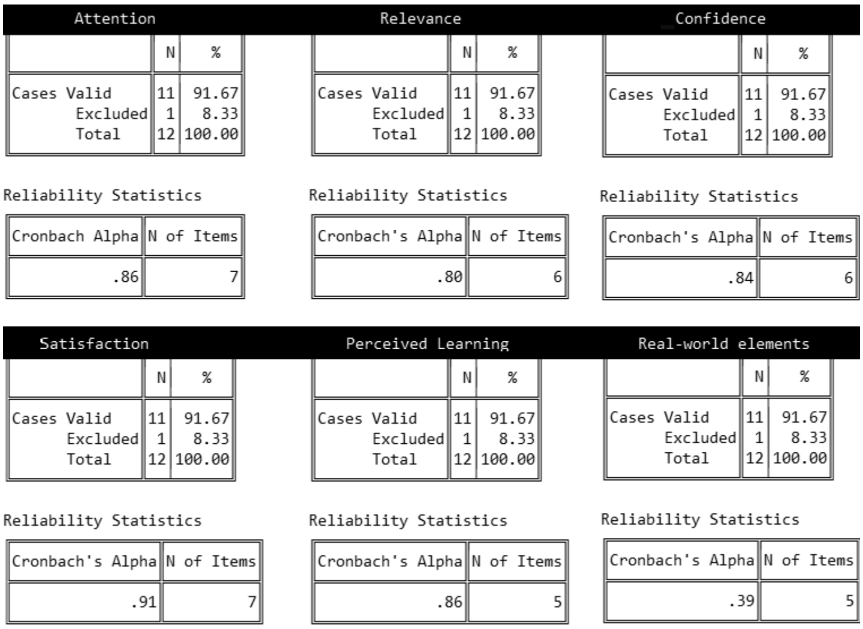
Reliability check for each construct is presented in Fig. 5. Most of the constructs achieve sufficient reliability scores, except for the construct related to the ability of this approach to present Real-world events and incidents or to be used to teach other IT topics.

Considering the answers related to the acceptance of this approach in other topics, it is clear that it might be difficult to accept it as an official assessment method in academia. Students for example are confused in how this method could enhance their skills and knowledge in matters of the official academic curriculum.

6 Conclusions

In this study, a method for introducing students to the basic concepts of cybersecurity was proposed. The impact of GBL on the learning outcomes was also discussed, focused on the ARCS motivation model [63] and how it applies to our approach. The main purpose was to increase the engagement levels of the academic course and to maintain balance between fun, engagement and perceived learning in the complex topics of cybersecurity.

The in-game challenges and software tools are compared with tools and ethical hacking methods that exist in reality, in order to uncover the potential of computer games as virtual learning environments. In our proposal we mentioned



Attention

		N	%
Cases	Valid	11	91.67
	Excluded	1	8.33
	Total	12	100.00

Reliability Statistics

Cronbach Alpha	N of Items
.86	7

Relevance

		N	%
Cases	Valid	11	91.67
	Excluded	1	8.33
	Total	12	100.00

Reliability Statistics

Cronbach's Alpha	N of Items
.80	6

Confidence

		N	%
Cases	Valid	11	91.67
	Excluded	1	8.33
	Total	12	100.00

Reliability Statistics

Cronbach's Alpha	N of Items
.84	6

Satisfaction

		N	%
Cases	Valid	11	91.67
	Excluded	1	8.33
	Total	12	100.00

Reliability Statistics

Cronbach's Alpha	N of Items
.91	7

Perceived Learning

		N	%
Cases	Valid	11	91.67
	Excluded	1	8.33
	Total	12	100.00

Reliability Statistics

Cronbach's Alpha	N of Items
.86	5

Real-world elements

		N	%
Cases	Valid	11	91.67
	Excluded	1	8.33
	Total	12	100.00

Reliability Statistics

Cronbach's Alpha	N of Items
.39	5

Fig. 5. Reliability check - Cronbach's Alpha

the importance of presenting real software tools used for ethical hacking and penetration testing in contrary to the in-game context.

High correlation levels are indicated regarding the relevance between in-game context and real-case scenarios. It is perceived that the skills were gradually developed, enhanced with the self-learning elements which computer games could provide. Basic concepts and methods were presented in the game and even participants with insufficient knowledge in ethical hacking could follow the procedure.

Finally, through this research, we were able to extract empirical data on how Gamification or GBL could enhance the learning process. By focusing on GBL, we combined the fun elements deriving from computer games with an actual learning process enhanced by gamification elements.

6.1 Limitations

Students were informed that the main virtual learning environment would be a computer game and not a real platform. As a result, some participants did not directly correlate the process with a real virtual learning environment. The second limitation was the small set of participants. However, using the correct methodology, this method could be used in order to enhance the learning process in the official academic curriculum and to collect more empirical data. Finally, this approach could be an appropriate method for conducting assessments and exams. However not sufficient empirical data are presented in this research in order to support this approach and to create an appropriate assessment method.

6.2 Future Work

More work is required in terms of analyzing the features which affect attributes such as perceived learning, actual learning and skills acquaintance. In order to convert a computer game into a virtual learning environment more customization and research is required. We plan to study the interconnections and possible extensions of the proposed method, using real-case scenarios and defining specific learning goals.

We recognize the importance of increasing the data-set of this research in order to better investigate the impact of this approach on the learning outcomes. Towards this direction we plan to create attack scenarios, both inside the computer game and also in the lab, in order to collect more details. Scenarios might be created using the software component of Nite Team 4 - *"Network Administrator"* in order to create custom challenges deriving from real-case scenarios. Furthermore, the potential of Gameplay Option - Section 3: Multiplayer/Hivemind Network (presented in chapter 4.2) has to be further analyzed in order to highlight the importance of creating custom challenges which are highly related to real-world infrastructure and acquiring familiarity related to threat modelling tools.

References

1. T.M. Connolly et al., A systematic literature review of empirical evidence on computer games and serious games. Comput. Educ. 59(2), 661–686 (2012)
2. B. Bediou et al., Meta-analysis of action video game impact on perceptual, attentional, and cognitive skills. Psychol. Bull. 144(1), 77 (2018)
3. B.D. Coller, D.J. Shernoff, Video game-based education in mechanical engineering: a look at student engagement. Int. J. Eng. Educ. 25(2), 308 (2009)
4. K. Kiili, Digital game-based learning: towards an experiential gaming model. Internet High. Educ. 8(1), 13–24 (2005)
5. P. Buckley, E. Doyle, Gamification and student motivation. Interact. Learn. Environ. 24(6), 668 1162–1175 (2016)
6. J. Hamari et al., Challenging games help students learn: an empirical study on engagement, flow and immersion in game-based learning. Comput. Hum. Behav. 54, 170–179 (2016)
7. K. de Beer, M. Holmner, The design of an alternate reality game as capstone course in a 685 multimedia post-graduate degree (2013)
8. R.M. Felder, R. Brent, Navigating the bumpy road to student-centered instruction. Coll. Teach. 44(2), 43–47 (1996)
9. R.E. Gewurtz et al., Problem-based learning and theories of teaching and learning in health professional education. J. Perspect. Appl. Acad. Pract. 4(1) (2016)
10. . L.F. Johnson et al., Challenge-Based Learning: An Approach for Our Time (The New Media Consortium, 2009)
11. D.K. Meyer, J.C. Turner, C.A. Spencer, Challenge in a mathematics classroom: students' motivation and strategies in project-based learning. Elem. School J. 97(5), 501–521 (1997)
12. S. Cass, Some assembly (language) required-Three games that make low-level coding fun [Resources-Geek Life]. IEEE Spectr. 54(5), 19–20 (2017)

13. G. Surendeleg et al., The role of gamification in education-a literature review. Contem. Eng. Sci. 7(29), 1609–1616 (2014)
14. J.M. Pittman, R. Pike, An observational study of peer learning for high school students at a cybersecurity camp. Inf. Syst. Educ. J. 14(3), 4 (2016)
15. L. Cifuentes et al., An architecture for case-based learning. TechTrends 54(6), 44–50 (2010)
16. A. Bruckman, Community support for constructionist learning. Comput. Support. Coop. Work (CSCW) 7(1–2), 47–86 (1998)
17. D.H. Jonassen, Instructional design models for well-structured and III-structured problem solving learning outcomes. Educ. Technol. Res. Dev. 45(1), 65–94 (1997)
18. P. Fotaris et al., Climbing up the leaderboard: an empirical study of applying gamification techniques to a computer programming class. Electr. J. E-learn. 14(2), 94–110 (2016)
19. Šakić, Mateja, and V. Varga, Video games as an education tool, in The Sixth International Conference 807 on e-Learning. eLearning-2015 (2015)
20. M.Pivec, O.Dziabenko, I.Schinnerl, Game-based learning in universities and lifelong learning: UniGame: social skills and knowledge training game concept. J. Univ. Comput. Sci. 10(1), 14–26 (2004)
21. R.Ibrahim, A.Jaafar, Educational games (EG) design framework:combination of game design, pedagogy and content modeling, in 2009 International Conference on Electrical Engineering 733 and Informatics, Vol. 1 (IEEE, 2009)
22. K. Squire et al., Electromagnetism supercharged!: learning physics with digital simulation games, in Proceedings of the 6th International Conference on Learning Sciences (International Society of the Learning Sciences, 2004)
23. R. Al-Azawi, F. Al-Faliti, M. Al-Blushi, Educational gamification vs. game based learning: 646 comparative study. Int. J. Innov. Manage. Technol. 7(4), 132–136 (2016)
24. C.I. Muntean, Raising engagement in e-learning through gamification, in Proceedings of 6th International Conference on Virtual Learning ICVL, Vol. 1 (2011)
25. C. Cheong, F. Cheong, J. Filippou, Quick quiz: a gamified approach for enhancing learning. 672 PACIS (2013)
26. M. Prensky, The games generations: how learners have changed. Dig. Game-based Learn. 1 (2001)
27. R.N.Landers,Developing a theory of gamified learning: linking serious games and gamification of learning. Simul. Gaming 45(6), 752–768 (2014)
28. S. Maraffi, F.M. Sacerdoti, E. Paris, Learning on gaming: a new digital game based learning approach to improve education outcomes. US-China Educ. Rev. 7(9), 421–432 (2017)
29. M. Prensky, Digital game-based learning. Comput. Entertain. (CIE) 1(1), 21–21 (2003)
30. V. Vbensk, J. Vykopal, Challenges arising from prerequisite testing in cybersecurity games, in Proceedings of the 49th ACM Technical Symposium on Computer Science Education (ACM, 2018)
31. P. McClean et al., Virtual worlds in large enrollment science classes significantly improve authentic learning, in Proceedings of the 12th International Conference on College Teaching and Learning, Center for the Advancement of Teaching and Learning (2001)
32. C. Johnson et al., Game development for computer science education, in Proceedings of the 2016 ITiCSE Working Group Reports (ACM, 2016)
33. F. Agalbato, D. Loiacono, Robo 3: a puzzle game to learn coding, in 2018 IEEE Games, 644 Entertainment, Media Conference (GEM) (IEEE, 2018)

34. R. Van Solingen, K. Dullemond, B. Van Gameren, Evaluating the effectiveness of board game usage to teach GSE dynamics, in 2011 IEEE Sixth International Conference on Global Software Engineering (IEEE, 2011)
35. P.D. Allen, K.A. Straub, Using games to enrich continuous cyber training. Johns Hopkins APLTech. Dig. 33(2) (2015)
36. A.V. Kirillov et al., Improvement in the learning environment through gamification of the educational process. Int. Electr. J. Math. Educ. 11(7), 2071–2085 (2016)
37. R.S. Cheung et al., Effectiveness of cybersecurity competitions, in Proceedings of the International Conference on Security and Management (SAM). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp) (2012)
38. A. DomNguez et al., Gamifying learning experiences: practical implications and outcomes. 698 Comput. Educ. 63, 380–392 (2013)
39. J. Mirkovic et al., Evaluating cybersecurity education interventions: three case studies. IEEE Secur. Priv. 13(3), 63–69 (2015)
40. M. Schiffman, Hackers Challenge: Test Your Incident Response Skills Using 20 Scenarios (McGraw-Hill Inc, New York, NY, USA, 2001)
41. Z.C. Schreuders, E. Butterfield, Gamification for teaching and learning computer security in 811 higher education, in 2016 USENIX Workshop on Advances in Security Education (ASE 16) (2016)
42. T. Denning et al., Control-Alt-Hack: the design and evaluation of a card game for computer 692 security awareness and education, in Proceedings of the 2013 ACM SIGSAC conference on 693 Computer Communications Security (ACM, 2013)
43. T. Denning, A. Shostack, T. Kohno, Practical lessons from creating the control-alt-hack card 695 game and research challenges for games in education and research, in 2014 USENIX Summit 696 on Gaming, Games, and Gamification in Security Education (3GSE 14) (2014)
44. M. Gondree, Z.N.J. Peterson, Valuing security by getting [d0x3d!]: experiences with a network security board game, in Presented as part of the 6th Workshop on Cyber Security Experimen719 tation and Test (2013)
45. M. Hendrix, A. Al-Sherbaz, B. Victoria, Game based cyber security training: are serious games suitable for cyber security training? Int. J. Ser. Games 3(1), 53–61 (2016)
46. H. Gonzalez, R. Llamas, F. Ordaz, Cybersecurity teaching through gamification: aligning training resources to our syllabus. Res. Comput. Sci. 146, 35–43 (2017)
47. R. Raman, A. Lal, K. Achuthan, Serious games based approach to cyber security concept learning: Indian context, in 2014 International Conference on Green Computing Communication 803 and Electrical Engineering (ICGCCEE) (IEEE, 2014)
48. J.-N. Tioh, M. Mina, D.W. Jacobson, Cyber security training a survey of serious games in cybersecurity, in 2017 IEEE Frontiers in Education Conference (FIE) (IEEE, 2017)
49. G. Barata et al., Engaging engineering students with gamification, in 2013 5th International Conference on Games and Virtual Worlds for Serious Applications (VS-GAMES) (IEEE, 2013)
50. M. Denk, M. Weber, R. Belfin, Mobile learning-challenges and potentials. IJMLO 1(2), 122–139 (2007)
51. L.M. Kinczkowski, Hacker's challenge: test your incident response skills using 20 scenarios. Secur. Manage. 47(1), 108–108 (2003)
52. F. Alotaibi et al., A review of using gaming technology for cyber-security awareness. Int. J. 650 Inf. Secur. Res. (IJISR) 6(2), 660–666 (2016)

53. K. Boopathi, S. Sreejith, A. Bithin, Learning cyber security through gamification. Indian J. Sci. 664 Technol. 8(7), 642–649 (2015)
54. Rice, J.W. Rice, The gamification of learning and instruction: game-based methods and strategies for training and education. Int. J. Gaming Comput. Med. Simul. 4(4) (2012)
55. K.M. Kapp, What is gamification, in Game-Based Methods and Strategies for Training and Education, The Gamification of Learning and Instruction (2012), pp. 1–23
56. L.A.Annetta et al.,Investigating the impact of video games on high school students engagement 654 and learning about genetics. Comput. Educ. 53(1), 74–85 (2009)
57. R.S.N.Lindberg,T.H.Laine,L.Haaranen,Gamifying programming education in K12: a review of programming curricula in seven countries and programming games. Br. J. Educ. Technol. 50(4), 1979–1995 (2019)
58. P. Fotaris et al., From hiscore to high marks: empirical study of teaching programming through gamification,in European Conference on Games Based Learning. Academic Conferences International Limited (2015)
59. C. Eagle, J.L. Clark, Capture-the-Flag: Learning Computer Security Under Fire (Naval Post703 graduate School Monterey CA, 2004)
60. B.C. Dunphy, S.L. Dunphy, Assisted performance and the zone of proximal development 700 (ZPD); a potential framework for providing surgical education. Aust. J. Educ. Dev. Psychol. 701 3(2003), 48–58 (2003)
61. L. Lin, Exploring collaborative learning: theoretical and conceptual perspectives, in Investigating Chinese HE EFL Classrooms (Springer, Berlin, Heidelberg, 2015), pp. 11–28
62. V.P. Dennen, Cognitive apprenticeship in educational practice: research on scaffolding, model689 ing, mentoring, and coaching as instructional strategies. Handb. Res. Educ. Commun. Technol. 690 2(2004), 813–828 (2004)
63. J.M. Keller, Development and use of the ARCS model of instructional design. J. Instr. Dev. 10(3), 2 (1987)
64. A.D.E. Le Compte, T. Watson, A renewed approach to serious games for cyber security, in 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace (IEEE, 2015)
65. D.I. Cordova, M.R. Lepper, Intrinsic motivation and the process of learning: beneficial effects 683 of contextualization, personalization, and choice. J. Educ. Psychol. 88(4), 715 (1996)
66. M. Kebritchi, A. Hirumi, H. Bai, The effects of modern math computer games on learners math achievement and math course motivation in a public high school setting. Br. J. Educ. Technol. 38(2), 49–259 (2008)
67. J. Lee et al. More than just fun and games: assessing the value of educational video games in the classroom, in CHI'04 Extended Abstracts on Human Factors in Computing Systems (ACM, 2004)
68. K. Becker, Video game pedagogy, in Games: Purpose and Potential in Education (Springer, 660 Boston, MA, 2009), pp. 73–125
69. A.C. Siang, R.K. Rao, Theories of learning: a computer game perspective, in Proceedings of Fifth International Symposium on Multimedia Software Engineering, 2003 (IEEE, 2003)
70. K. Siau, H. Sheng, F.F.-H. Nah, Use of a classroom response system to enhance classroom interactivity. IEEE Trans. Educ. 49(3), 398–403 (2006)
71. F.L. Greitzer, O.A. Kuchar, K. Huston, Cognitive science implications for enhancing training effectiveness in a serious gaming context. J. Educ. Resour. Comput. (JERIC) 7(3), 2 (2007)

72. F. Gilberg, Using games to improve network security decisions (2006)
73. M.N. Katsantonis, P. Fouliras, I. Mavridis, Conceptualization of game based approaches for learning and training on cyber security, in Proceedings of the 21st Pan-Hellenic Conference on Informatics (ACM, 2017)
74. J.P. Gee et al., Playing to learn game design skills in a game context, in Proceedings of the 8th International Conference on International Conference for the Learning Sciences-Volume 3 (International Society of the Learning Sciences, 2008)
75. D.R. Krathwohl, A revision of Bloom's taxonomy: an overview. Theory Pract. 41(4), 212–218 (2002)
76. D.R. Krathwohl, L.W. Anderson, A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives (Longman, 2009)
77. A. Nagarajan et al., Exploring game design for cybersecurity training, in 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER) (IEEE, 2012)
78. A. Amory, R. Seagram, Educational game models: conceptualization and evaluation: the prac652 tice of higher education. South Afr. J. High. Educ. 17(2), 206–217 (2003).
79. A.Hirumi,C.Stapleton,Applying pedagogy during game development to enhance game-based learning, in Games: Purpose and Potential in Education (Springer, Boston, MA, 2009), pp. 127–162
80. D. Oblinger, Games and learning. Educ. Q. 3, 5–7 (2006)
81. D.R. Bacon, Reporting actual and perceived student learning in education research, pp. 3–6 (2016)
82. S. Isaacs, The difference between gamification and game-based learning. ASCD In Service (2015), http://inservice.ascd.org/the-difference-between-gamification-and-game-based-learning
83. P. Moreno-Ger et al., Educational game design for online education. Comput. Hum. Behav. 24(6), 2530–2540 (2008)
84. S. Papert, I. Harel, Situating constructionism. Constructionism 36(2), 1–11 (1991)