# A game-based learning experience for improving cybersecurity awareness*

Silvestro Veneruso, Lauren S. Ferro, Andrea Marrella, Massimo Mecella, and Tiziana Catarci

Sapienza Universitá di Roma, Rome, Italy
veneruso.1461229@studenti.uniroma1.it,
{lsferro,marrella,mecella,catarci}@diag.uniroma1.it

**Abstract**

The use of videogames is an established tool to train a systematic way of thinking that allows users to learn by gaming. In this paper, to address the increasing need of awareness in cybersecurity related issues, we present the realization of a Virtual Reality (VR) videogame targeted towards educating users in the context of cybersecurity.

## 1 Introduction

Over the last years, videogames have been offering solutions to educate users in ways that traditional methods cannot afford, more so in a consequence free environment where players can succeed, being rewarded for solving a problem or completing a task, or fail, and by doing so can reflect, understand, and try again [9]. So, videogames train a systematic way of thinking that allows players to learn by gaming [10]. In many traditional settings (e.g., in classrooms) receiving feedback is often a delayed event. Conversely, in videogames, it is possible for the player to receive feedback immediately, by highly reducing the time span between learning and practising. In addition, videogames that challenge players can also result in better learning outcomes [4], and therefore, improving acquisition of learning content. Videogames and other types of interactive learning experiences can encompass a variety of different experiences such as serious games[1], gamified experiences[2], and simulations[3]. In each of these genres, different approaches for integrating educational content afford the possibility for players to not only engage in an enjoyable experience, but also to learn something valuable from it.

Based on the foregoing considerations, we present in this paper the realization of a Virtual Reality (VR) First-Person videogame, called CyberVR, targeted towards educating users in the context of cybersecurity, a research and practical field that has been attracting considerable interest in recent years [1, 2, 3]. The player, that acts as an IT technician, explores a fictitious post-apocalyptic world where IT systems are designed as virtual environments, and IT technicians have the possibility to setup them directly from the inside. The player can progress in the game by interacting with an invisible entity, called the "Administrator", which supports the player in the proper execution of tasks, presented to the player in the form of mini-games. Each mini-game covers a relevant and contemporary topic related to cybersecurity, from highlighting



[1]Representations of reality without the consequences of reality that a player would find in a simulation.

[2]Gamification is not a game per se, rather an application with game elements that encourage certain behaviours.

[3]Representation of reality where actions have the same (simulated) consequences as they would have in reality.

the importance of keeping updated a software (SW) system, to requiring the player to handle a communication between two subjects, using the "public-key cryptography".

The rest of the paper is organized as follows. In Section 2, we introduce the technical features related to the development of CyberVR, and we discuss its novelty with respect to state-of-the-art existing games for learning cybersecurity aspects. Then, in Section 3, we present a walkthrough of CyberVR describing in detail the structure of any cybersecurity-related mini-game. Finally, Section 4 concludes the paper.

## 2 Game Development and Related Work

The development of CyberVR was was performed through the Unreal Engine 4 with the use of the Oculus Rift and Leap Motion. The Oculus Rift allowed us to develop an experience that was set in VR, and the Leap Motion allowed players to use their hands to interact with in-game objects and throughout the mini-games. In addition, the player also used an xBox controller for some parts of the interaction, specifically to advance the dialogue with the Administrator.

To develop a videogame that was specifically focused on educating users in the context of cybersecurity, we needed the understanding of what was currently available in the research literature. Specifically, we found (academic) games such as CyberCIEGE [5], PhishGuru [6], Anti-Phishing Phil [12] and Phish Phinder [8], frameworks like [7] for designing cybersecurity focused games, and mainstream videogames such as Overwatch and Hacker Evolution Duality.

The development of CyberVR has resulted in many elements and features that differentiate the game in comparison to those that already exist. First of all, the main difference is that CyberVR does not just focus on a single cybersecurity issue, but rather on several, thus making it a complete introduction to the most relevant cybersecurity aspects. The second difference is that CyberVR actively involves the user in every aspect of the game as opposed to traditional participation such as moving a mouse or typing on the keyboard, as found with games such as Anti-Phishing Phil or PhishGuru. Since this experience utilises the Oculus Rift with the Leap Motion device as well as an xBox controller, the player is encouraged to "interact" with the security issues rather than more traditionally and passively by clicking or typing responses. Another important characteristic of CyberVR relies in its contemporary nature, as the game challenges and pushes the barrier of educational game design further with the use of modern technology. In this way, CyberVR is novel in both its approach and representation of cyber-security topics, raising the bar on educational games and interactive learning experiences, and therefore aligning with more contemporary and relevant technology and interactive design.

## 3 Game structure

The game consists of two main levels. The first one is set outside a building (see Figure 1), which the Administrator refers to be as his *non-secure IT system*, and is thought as a tutorial that enables the player to learn how to move/interact in/with the environment. Then, the second level takes places inside the building, and consists of six mini-games that the player has to complete (in any order) to *secure the IT system*.

Before entering into the building, i.e., into the IT system that has to be secured, the player is asked to "scan" the surface of the system (see Figure 2). The rationale for this is to introduce the concept of performing a NMAP[4] (network mapper) scan via a terminal command. Once the player has completed the scan, s/he must "ask for permission" from the Administrator of

[4]Nmap is a open-source network scanner. See https://nmap.org

Figure 1: The environment when the player begins the game.

the system to gain access. Once access has been granted to the player, s/he proceeds to enter the building, where the player is immediately confronted with a dark space - a metaphoric


Figure 2: NMAP scanning.

"Black Box". Here, the player performs a "Black Box Analysis" through VAPT (Vulnerability Assessment and Penetration Testing). Once the analysis is completed, the player can then proceed to playing the six available mini-games, which are described below.

**Information Flow**: It requires a player to scan data packets, which are represented by cubes. The aim of this mini-game is to find out if the data packets are "Sensitive Data" or "Public Data". Once the player has properly identified the data packet type, s/he redirects the data packet towards the correct information flow using buttons, as shown in Figure 3.

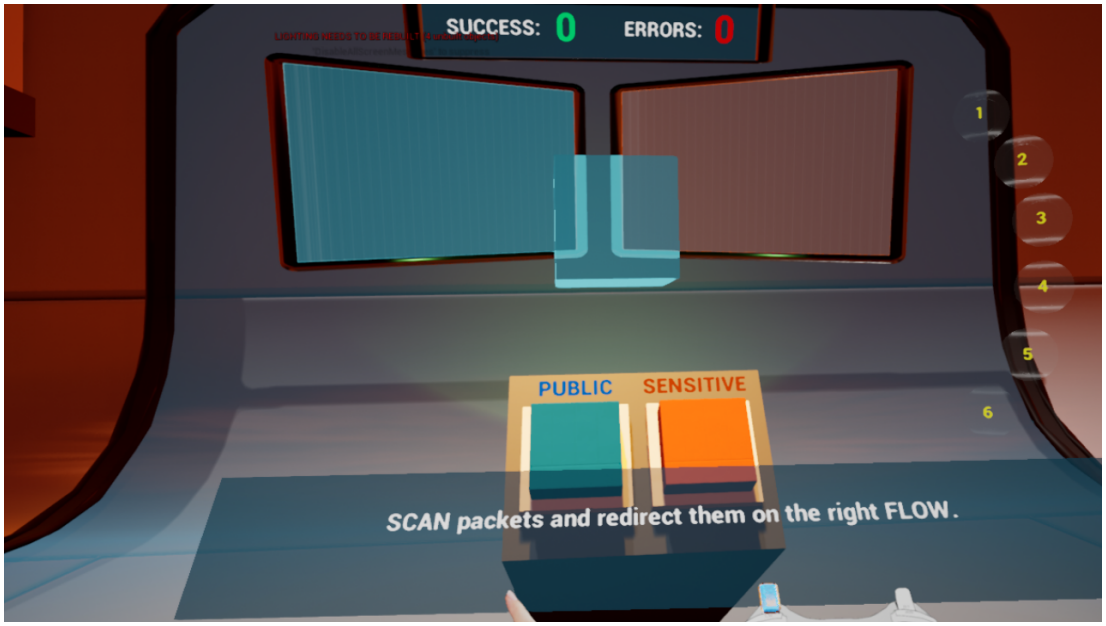


Figure 3: Information Flow mini-game.

**Code Injection**: It requires the player to scan the source code to locate dangerous/malicious pieces of code. Once the player has identified the dangerous code, s/he must destroy it using a "fire" gesture, as shown in Figure 4.

**Patch Management**: It is a mini-game about keeping a SW system (e.g., a program, server, etc.), which is represented by a cube. Specifically, the system needs to be updated and patched. This is a typical and needed security requirement when it comes to protecting a SW system and the data/applications that it uses to manage. Patches and updates can solve a critical problem of the SW, such as a security flaw that may have been introduced during the development phase. The player needs to "scan" all layers of the SW (cube) and apply the correct patch, from the ones that are visually available to her/him, using buttons (marked A, B, C). A screenshot of this mini-game is shown in Figure 5.

**Dynamic SW Analysis**: It is a testing technique based on observing the behaviour of a SW during its running phase. First of all, this mini-game requires the player to run the SW by pressing a button "Run Code". At this point, the player will notice that several security issues appear in the code in the form of orange poles that protrude out towards the player. Each of the orange poles is provided with a yellow label with the "issue" name, as shown in Figure 6. These are typical and popular issues that may arise for a SW at run-time (e.g., SQL Injection and Buffer Overflow). It is up to the player to then "Reject" these issues by physically pushing


Figure 4: Code Injection mini-game.

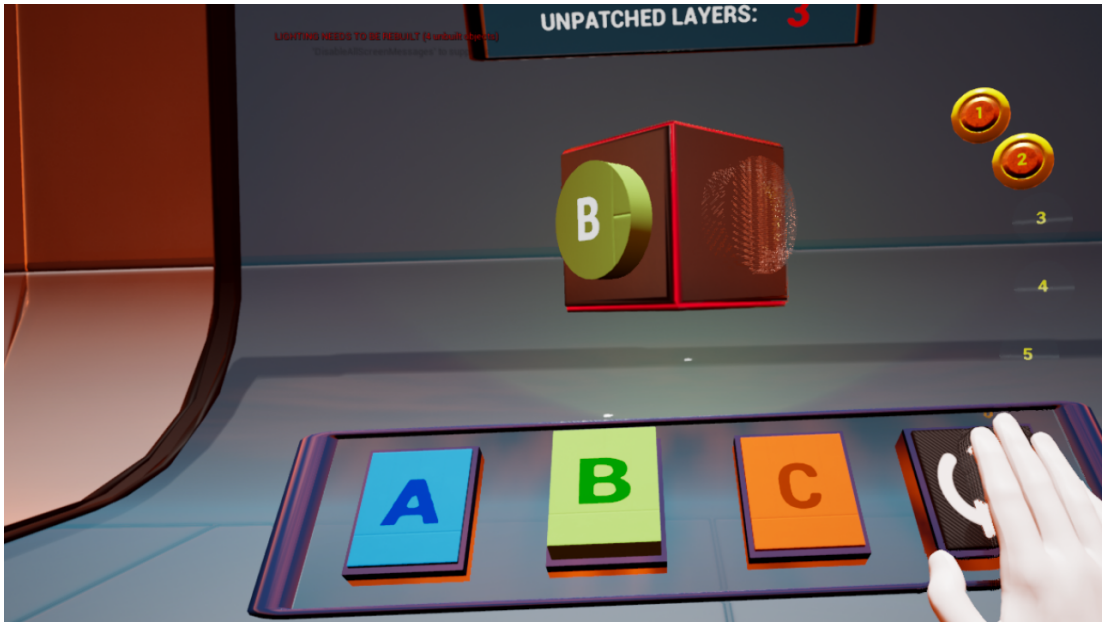


Figure 5: Patch Management mini-game.

them with her/his hands. Once the player has performed this task for ten issues, s/he can destroy them with the fire gesture, and the mini-game can be considered as completed.

**Privilege Escalation**: The system to be secured may have intruders inside it. Therefore,


Figure 6: Dynamic SW Analysis mini-game.

in this mini-game, the player must "scan" the users that acceded into the system to find out which ones have reached the "Root", i.e., a restricted area of the system that typically requires that the users have specific privileges or permissions to access to it. In this mini-game, the player will find that some users (i.e., the intruders) have utilised a flaw in the security (e.g., a weak password) to obtain permissions. Hence, to solve the problem, the player must fix the security flaw by removing permissions to unauthorized users, and therefore implementing stronger passwords. A screenshot of this mini-game is shown in Figure 7.

**Public-Key Cryptography**: It is a mini-game about two users - Alice and Bob - who want to exchange messages in a secure way, as show in Figure 8. The player achieves this by using "Public key" cryptography. First, the player encrypts the message by using a "Public key", which is known by both the sender and the recipient of the message. Then, on the other side of the communication, the player decrypts the message using a "Private Key", which is known only to the recipient of the message. To encrypt the message, the player needs to physically grab keys from Alice and Bob. Once the player has successfully allowed four messages to be exchanged, the mini-game is complete.

When the player completes one of the six mini-games, s/he is rewarded with a coin, which represents her/his awareness of the analyzed cybersecurity threat. An example of coin can be seen in the top right-hand corner of the screen in Figure 8. Once the player has obtained six coins (i.e., the IT system has been secured), s/he will unlock the last part of the game, which consists of updating the database of threats using the experience/awareness achieved by completing each mini-game. The underlying message is that a proper knowledge of existing cybersecurity threats may allow to prevent future threats and protect better an IT system. After this, the player can return into the starting environment, which has changed in terms of a more positive aesthetic, and it is now possible for the player to conclude the learning experience.

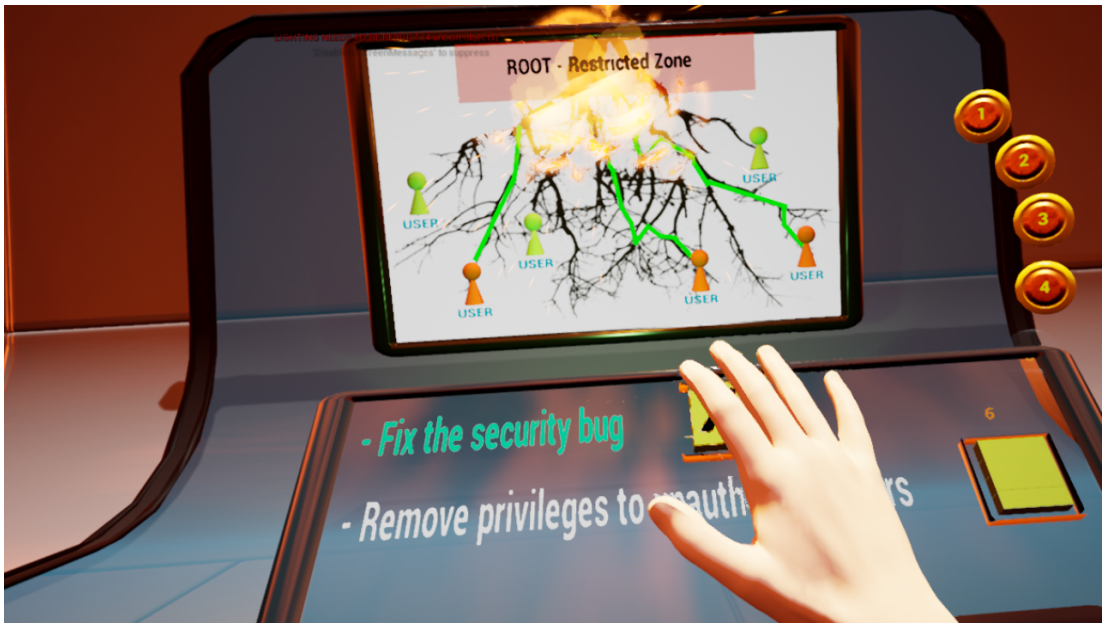


Figure 7: Privilege Escalation mini-game.

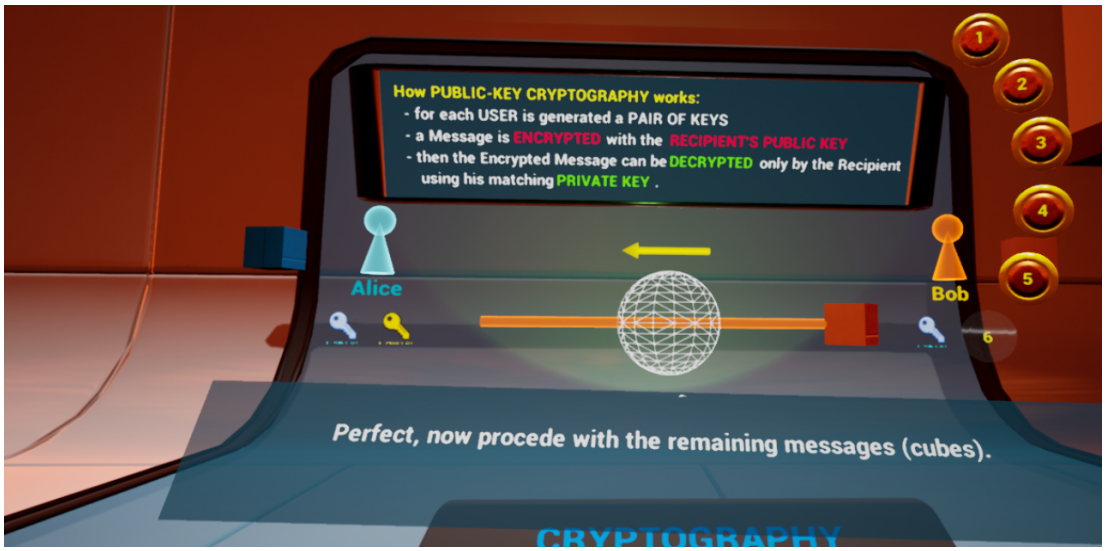


Figure 8: Public-Key Cryptography mini-game.

## 4 Concluding Remarks

In this paper, we have presented CyberVR, a videogame based on an immersive approach (leveraging VR features) that focuses on making users aware of cybersecurity issues. The videogame consists of six mini-games, whose target is to introduce the player with some of the most relevant existing cybersecurity issues, together with a way to resolve them or at least

understand their working and dangerousness in more detail. In this way, the players have the opportunity to extend or consolidate their knowledge of these issues.

Interested readers can also refer to an extended version of this short contribution [11], which provides more discussion and a large user evaluation demonstrating that CyberVR is equally effective but more engaging as learning method toward cybersecurity education than traditional textbook learning.

**Acknowledgments.** This research work has been partly supported by the "Dipartimento di Eccellenza" grant, the H2020 project DESTINI, the Sapienza grants IT-SHIRT and BPBots, the Lazio regional initiative "Centro di eccellenza DTC Lazio" and the project ARCA.

# References

[1] Simone Agostinelli, Fabrizio Maria Maggi, Andrea Marrella, and Francesco Sapio. Achieving GDPR Compliance of BPMN Process Models. In *Information Systems Engineering in Responsible Information Systems*, pages 10–22, Cham, 2019. Springer International Publishing.

[2] Simone Coltellese, Fabrizio Maria Maggi, Andrea Marrella, Luca Massarelli, and Leonardo Querzoni. Triage of IoT Attacks Through Process Mining. In *On the Move to Meaningful Internet Systems: OTM 2019 Conferences*, pages 326–344, Cham, 2019. Springer International Publishing.

[3] Giuseppe Desolda, Francesco Di Nocera, Lauren Ferro, Rosa Lanzilotti, Piero Maggi, and Andrea Marrella. Alerting Users About Phishing Attacks. In *International Conference on Human-Computer Interaction*, pages 134–148. Springer, 2019.

[4] Juho Hamari, David J. Shernoff, Elizabeth Rowe, Brianno Coller, Jodi Asbell-Clarke, and Teon Edwards. Challenging games help students learn: An empirical study on engagement, flow and immersion in game-based learning. *Computers in Human Behavior*, 54, 2016.

[5] C. E. Irvine, M. F. Thompson, and K. Allen. CyberCIEGE: Gaming for information assurance. *IEEE Security Privacy*, 3(3), 2005.

[6] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. School of phish: A real-world evaluation of anti-phishing training. In *5th Symposium on Usable Privacy and Security*. ACM, 2009.

[7] Alexis Le Compte, David Elizondo, and Tim Watson. A renewed approach to serious games for cyber security. In *2015 7th Int. Conf. on Cyber Conflict: Architectures in Cyberspace*, pages 203–216. IEEE, 2015.

[8] Gaurav Misra, Nalin Gamagedara Arachchilage, and Shlomo Berkovsky. Phish Phinder: A Game Design Approach to Enhance User Confidence in Mitigating Phishing Attacks. *arXiv:1710.06064*, 2017.

[9] Kurt D Squire. Video game–based learning: An emerging paradigm for instruction. *Performance Improvement Quarterly*, 21(2), 2008.

[10] Nick Tannahill, Patrick Tissington, and Carl Senior. Video games and higher education: what can "Call of Duty" teach our students? *Frontiers in psychology*, 3:210, 2012.

[11] Silvestro Veneruso, Lauren S Ferro, Andrea Marrella, Massimo Mecella, and Tiziana Catarci. CyberVR - An Interactive Learning Experience in Virtual Reality for Cybersecurity Related Issues. In *2020 International Conference on Advanced Visual Interfaces (AVI '20)*. ACM, 2020.

[12] Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, and Erik Andersen. What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game. In *2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, 2019.