Immersive and Game-based Learning Experiences in Cybersecurity

Nicholas De Marco[1,*,†], Antonio Pisu[1,*,†], Teresa Onorati[2,*,†], Paloma Díaz[2,*,†], Ignacio Aedo[2,*,†], Paola Barra[3,*,†] and Genoveffa Tortora[1,*,†]

[1]Department of Computer Science, Universita Degli Studi di Salerno, Fisciano, Italy
[2]Department of Computer Science, Universidad Carlos III de Madrid, Leganés, Madrid, Spain
[3]Department of Science and Technology, University Parthenope of Naples

Abstract

Education in STEM disciplines, such as cybersecurity, presents several challenges due to the applied and evolving nature of these domains. Traditional methods are primarily focused on a passive approach, emphasizing theoretical knowledge and offering limited opportunities for active engagement. Consequently, students may struggle to apply the knowledge they gain to solve specific problems. In contrast, immersive learning enables active involvement with content, promoting situated and embodied learning as well as the transfer of knowledge to the real world. For cybersecurity, in particular, immersive experiences give the possibility to simulate real-world scenarios, such as network attacks, system vulnerabilities, and defensive strategies, in a safe and controlled environment. Game-based learning has also shown great potential by increasing students' focus and motivation on learning. In this paper, we propose two immersive learning experiences that introduce fundamental concepts of cybersecurity. The first one aims to offer an application for analyzing network traffic to overcome the limitations of current monitoring systems. Both experts and non-experts can interact with several immersive visualizations to, for example, check the health status of an IP address. The second one is an immersive learning game designed to introduce and practice several cybersecurity concepts. Players engage in a sequence of challenges, including decrypting messages, configuring firewalls, and recovering corrupted data.

Keywords

Immersive Learning, Virtual Reality, Education, Cybersecurity

1. Introduction

Cybersecurity is a multidisciplinary field that requires knowledge from a wide range of domains and has to deal with an ever-evolving threat landscape. Teaching technical disciplines, such as cybersecurity, involves the application of innovative pedagogical approaches that support active, experiential, and problem-solving learning. Traditional methods often rely on passive content delivery and abstract representations, struggling to promote practical understanding and adequate learning experiences that guide students toward an increased awareness of cybersecurity threats and a greater interest in the field [1].

In recent years, the advent of new technologies has significantly reshaped learning methods, promoting more interactive, focused, and engaging approaches [2, 3]. Immersive technologies, such as virtual and augmented reality, enable experiential learning by allowing users to interact actively with complex concepts in realistic environments [4], which makes them particularly suitable to learn about complex and applied STEM concepts and to improve the transfer of knowledge to real-world situations [5]. Prior work has also shown that such experiences can enhance spatial awareness, facilitate collaborative analysis, and promote data exploration, while reducing cognitive load compared to traditional 2D interfaces [6]. Young learners also tend to prefer interacting with immersive experiences over 2D

Sense-XR 2025 - The Feeling of Virtual, XR, Haptics, and 3D Graphics, a workshop co-located with CHItaly 2025 (Salerno, Italy, 6-10 October 2025)

*Corresponding authors.
†These authors contributed equally.
n.demarco4@studenti.unisa.it (N. D. Marco); a.pisu@studenti.unisa.it (A. Pisu); tonorati@inf.uc3m.es (T. Onorati); pdp@inf.uc3m.es (P. Díaz); aedo@ia.uc3m.es (I. Aedo); paola.barra@uniparthenope.it (P. Barra); tortora@unisa.it (G. Tortora)

replicas, and they also spend more time exploring the immersive information space [7]. Virtual reality environments offer users a higher level of immersion, leading to increased concentration and enhanced mental processing capacity [8]. Game-based learning is another successful approach used in many STEM areas, including cyber-security [1], due to its ability to engage learners in flow experiences [9].

In this paper, we benefit from the learning affordances of immersive technologies and game-based learning to design two experiences that support both experts and non-experts in learning the fundamentals of cybersecurity. The first experience is an immersive environment with different visualizations of network traffic data. Interacting with the visualizations, users can learn about the health status of the IP addresses in the network and analyze other aspects of the connections. Compared to the security monitoring systems currently in use, this immersive experience enables users to focus on data exploration, thereby gaining a deeper understanding of how network traffic analysis works. The second application is a game designed to introduce fundamental cybersecurity concepts, such as cryptography, firewalls, backup, and recovery. The player experiences three different scenarios with mini-games to solve. Along the journey, she can access advanced information in the form of knowledge pills, which explain the theory behind the game logic, and a digital library where she can request additional explanations from a generative AI engine.

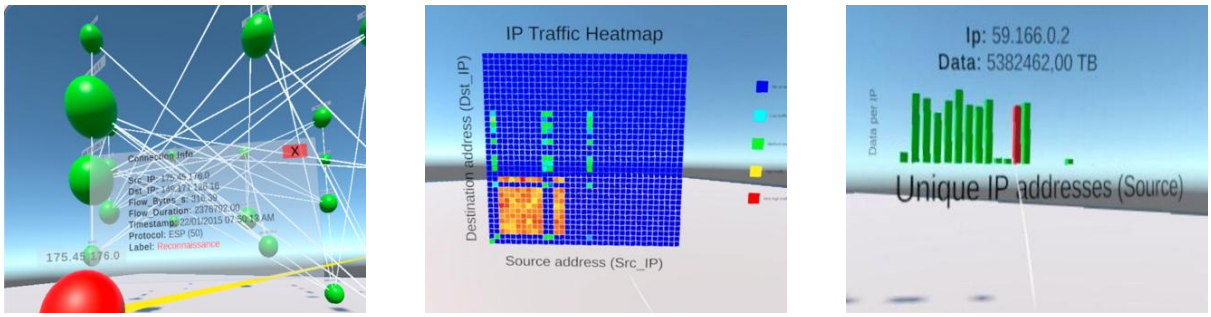
2. Related works

From the very first attempt to build virtual environments in the 1990s, it was clear that there was a valuable application of this technology in education, with a shift towards more active participation, where students do not stand in front of a monitor, but wear the device and interact with an immersive interface through multimodal stimuli [10]. Immersive Learning refers to creating engaging experiences through artificial environments perceived as non-mediated to facilitate learning through a sense of presence and immersion to give students the feeling of being physically present in the virtual space and immersed in the interaction with the digital objects around them [11, 10, 12, 5]. A strong sense of presence and immersion is crucial for influencing how students learn from the elements in the scene.

The application of an immersive approach to building learning experiences can be associated with various pedagogical strategies, including active, experiential, and game-based, where the primary focus is on learning to solve complex problems through a "learning by doing" paradigm [13]. This approach can impact the interest and curiosity of students, improving their motivation and leading to better academic performance and results [14, 13]. Immersive technologies can be beneficial for building representations and simulations that facilitate a deeper understanding of complex concepts. This leads to a shift from processing definitions and symbols in traditional educational methods to interacting with visual models and images [10, 5]. In this way, students can easily apply the knowledge they have gained to real-life situations. For example, to learn how to change a component of a car engine, it would be more effective to interact with a virtual model of a car rather than relying on physical elements or multimedia descriptions [15]. Immersive learning experiences are also safer and more sustainable than real-world ones, since learners can repeat actions as many times as needed without facing any risk or consuming or damaging physical materials.

Immersive learning experiences are often combined with game-based learning to leverage the intrinsic motivation features of video games. Digital educational games, frequently referred to as serious games, engage learners in gaming experiences with a learning purpose [16]. Their success strongly relies on the intrinsically motivational features of video games, including the intense involvement of learners and their exposure to continuous challenges that require the application of skills, all of which contribute to creating flow experiences [9].

Immersive experiences can provide significant educational benefits, particularly in STEM (Science, Technology, Engineering and Mathematics) disciplines, such as cybersecurity, where it is crucial not only to have an understanding of the main concepts and topics but also to know how to apply them to real-world cases. One of the characteristics of the cybersecurity field is the complex and ever-evolving nature of cyberattacks, which require robust and effective strategies. Immersive applications can help



(a) Interacting with a connection (b) IP traffic heatmap (c) Histogram of IP traffic

Figure 1: Three views of the immersive visualizations for Network Traffic Analysis

support the learning of these strategies and their applications [17]. Virtual environments can provide a safe and controlled space to simulate real-world hazards and attacks, and analyze the effectiveness of various strategies [18]. In this way, students can acquire knowledge and skills to handle similar situations in reality. Moreover, these experiences are designed to be interactive and engaging, enhancing students' motivation and, consequently, their interest in the disciplines [17].

3. Two Immersive Learning Experiences in Cybersecurity

In this paper, we describe two immersive experiences designed to support users while learning and practicing cybersecurity concepts. Both use a virtual reality environment, but each offers a different experience. The first one is an immersive visualization space for analyzing network traffic datasets. The second one is a game designed to introduce fundamental concepts, such as cryptography, firewalls, backup, and recovery.

3.1. Immersive Visualizations for Network Traffic Analysis

The security of the network traffic is a key issue for many businesses and companies [19]. Actual network security monitoring systems offer several key operations, such as intrusion detection, real-time alerts, and policy enforcement, to detect threats early and respond promptly [20, 21]. Often, these systems can be challenging to interact with, failing to provide a clear understanding of what is happening in the network [6].

The first immersive experience we propose enables both students and system analysts to monitor network traffic through various visualizations. By interacting with them, users can, for example, determine whether an IP address is in a healthy state or is experiencing issues due to excessive incoming traffic. In this way, they can learn from exploring the dataset in a space that encourages information retention and pattern recognition.

The system has been designed to analyze network traffic in real-time; however, for testing purposes, we have used a dataset containing real network traffic data. The design of the immersive experience is based on a modular structure in five steps:

1. **Data Collection**: The system has been designed to analyze network traffic in real-time; however, to test the prototype under realistic but controlled conditions, we utilized the CIC UNSW-NB15 Augmented Dataset [22], which contains traffic generated in a simulated enterprise-like network environment. The dataset includes both realistic normal behavior and various types of synthetic cyberattacks collected over a two-day period. It provides 47 features per connection and consists of eight types of attacks: Fuzzer, Analysis, Backdoor, Exploit, Generic, Reconnaissance, Shellcode, and Worm.
2. **Data Preparation**: To make the dataset compatible with the system, it was necessary to identify and extract only the features required for the visualizations, specifically to define the nodes,

(a) Ceaser Chipher (b) Configuration Firewall (c) Backup and Recovery

Figure 2: The three scenes in the cybersecurity learning game

establish the links based on data exchanges, and display meaningful statistics for each connection.

3. **Immersive Network Graph**: The main visualization created in the VR environment is the network graph, where each node represents an IP address in the network, with different colors indicating its health status: green for regular traffic, orange for potentially anomalous behavior (used to anticipate possible DoS attacks [23]), and red for nodes identified as malicious. The links between nodes represent the information exchanged between two IP addresses at a given instant in time. As shown in Figure 1a, the VR environment displays the 3D network graph with color-coded nodes and visible connections. The user can activate a timeline on her left arm to display the evolution of the network traffic over time, observing how the colors and the connections change. The user can also interact with the network by grabbing and moving nodes, as well as by clicking on a link to display information related to the specific connection (Figure 1a).
4. **Query Menu**: Users can access a menu to select one of three predefined queries, each designed to provide targeted insights into network activity. The first query displays a histogram representing the total amount of data generated by each source IP address, helping analysts quickly identify the most active nodes. The active nodes may indicate legitimate high-traffic sources or potentially compromised systems involved in data exfiltration or denial-of-service attacks. The second query utilizes an interactive bubble graph to display the distribution of protocols (e.g., TCP, UDP, ICMP) employed for the connections. The bubble size indicates usage frequency, and it can help detect abnormal protocol usage, such as unexpected encrypted traffic or unusual reliance on uncommon protocols. The third query generates a heatmap that visualizes the traffic intensity between source and destination IP pairs using a color gradient: blue indicates no or very low traffic, cyan indicates low traffic, green represents medium traffic, yellow shows high traffic, and red signals very high traffic. This visualization facilitates the detection of communication bottlenecks, suspicious peer-to-peer patterns, or lateral movement within the network. Each query activates the tailored 3D visualization in the VR environment when selected, as shown in Figure 1b and Figure 1c.
5. **System Tutorial**: The users accessing the system for the first time can explore a tutorial to familiarize themselves with the different options offered by the system, including the visualizations and the controllers to interact with them.

3.2. An Immersive Cybersecurity Learning Game

The second immersive experience we propose is CyberSecVR, a learning game to support students and non-experts in exploring fundamental concepts in cybersecurity. CyberSecVR is structured as a sequential journey through three virtual environments, each representing a key topic in cybersecurity. The aesthetic of the scenes incorporates several cyberpunk-inspired elements, including neon-lit scenes, stylized terminals, and digital overlays, to enhance user immersion in the game's dynamics.

The first scene, where the game begins, is an outdoor courtyard in front of a futuristic laboratory with various environments designed to simulate increasingly complex cybersecurity scenarios. In the same courtyard, a digital library is also available, where players can find more information about the concepts encountered during the game. The game is organized into three environments:

1. **Cryptography**: This is the first level of the game, and it is set in a closed courtyard outside a high-tech laboratory building. The player has to decrypt a short sentence encoded with a Caesar cipher [24] to unlock the doors and enter the laboratory. As shown in Figure 2a, a stylized terminal displays the encrypted phrase, while a holographic interface allows the user to type the decoded version using a virtual keyboard. After a few seconds of inactivity, the system displays a clue as a visual representation of the alphabet to the player. This level introduces the concept of symmetric encryption and logical pattern recognition through simple interaction. The correct answer triggers visual and audio feedback, giving interesting information about the Caesar cipher and granting access to the laboratory.
2. **Firewall Defense**: The second level takes place inside a high-security network control room in the laboratory. The player is tasked with configuring a firewall system to defend against an ongoing DoS attack [23]. Using gesture-based and controller inputs, the player observes streams of incoming packets rendered as colored orbs flying toward a server terminal. Each packet includes visual cues such as IP address labels, protocol icons, and, most importantly, color coding: green orbs indicate legitimate packets, and red ones indicate malicious ones. The player can manually shoot unwanted packets using a handheld device or, as shown in Figure 2b, configure an autonomous turret based on a whitelist and blacklist mechanism: the whitelist contains benign IP addresses, and the blacklist contains malicious ones. This dual mechanic introduces players to both manual and rule-based filtering, mirroring real-world intrusion prevention techniques.
3. **Backup and Recovery**: The third level places the player in a simulated server room. The space is filled with large holographic drives and blinking storage bays, evoking the interior of a futuristic data center. Players must solve a series of mini-puzzles, similar to those shown in Figure 2c, to restore corrupted data from backups. This includes visual sorting tasks and interactive diagrams that illustrate the differences between full, incremental, and differential backups. A damaged virtual disk must be repaired by dragging and placing encryption pieces and selecting the correct recovery paths. Feedback is provided through visual light signals and narrator cues, helping players understand not only what backup strategies exist but also when and why each is appropriate.

In another building, adjacent to the laboratory, a library is located that hosts a virtual assistant terminal, accessible after completing the game's three levels. This assistant appears as a floating holographic AI situated in a quiet digital room filled with virtual books and glowing panels. Players can grab a virtual microphone and start speaking directly to the assistant to ask questions or clarify concepts encountered during the game. The assistant utilizes various generative AI models to provide dynamic and context-aware responses, speech-to-text transcription, and in-game narration.

4. Conclusions and future works

The proposed immersive experiences have significant potential for offering an innovative approach to learning cybersecurity fundamentals from both theoretical and practical perspectives. They have been designed to leverage immersive learning, supporting both expert and non-expert users as they explore topics such as network traffic analysis, firewalls, and data recovery. The results are more engaging and practical experiences that can increase users' motivation and interest in the cybersecurity domain. Both experiences can be employed to train users with the simulation of real-world scenarios and encourage long-term knowledge retention.

The experiences are currently being evaluated to assess their efficacy as learning tools, particularly in terms of learners' engagement and transfer of the acquired knowledge to the real world.

Acknowledgments

This work has been supported by the Madrid Government (Comunidad de Madrid-Spain) under the Multiannual Agreement with UC3M (IRIS-CM-UC3M) and the Institute of Women (Ministry of Health, Social Services and Equality) under the InfoIA project (2024/00647/001).

Declaration on Generative AI

During the preparation of this work, the authors used Grammarly in order to: Grammar and spelling check, Paraphrase and reword. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] T. W. J, Addressing cybersecurity challenges in education, International Journal of STEM Education for Sustainability 3 (2023) 47–67.

[2] T. Marko, Neil selwyn: Education and technology: Key issues and debates, International Review of Education (2022). doi:10.1007/s11159-022-09971-9.

[3] K. Klein, M. Sedlmair, F. Schreiber, Immersive analytics: An overview, it - Information Technology 64 (2022) 155–168. doi:0.1515/itit-2022-0037.

[4] R. Villena-Taranilla, S. Tirado-Olivares, R. Cózar-Gutiérrez, J. A. González-Calero, Effects of virtual reality on learning outcomes in k-6 education: A meta-analysis, Educational Research Review 35 (2022) 100434. doi:10.1016/j.edurev.2022.100434.

[5] C. Dede, Immersive interfaces for engagement and learning, science 323 (2009) 66–69.

[6] C. Marco, D. Mishal, H. Matous, O. Kenneth, P. Mark, Immersive insights: A hybrid analytics system forcollaborative exploratory data analysis, in: Proceedings of the 25th ACM Symposium on Virtual Reality Software and Technology, VRST '19, Association for Computing Machinery, New York, NY, USA, 2019. doi:10.1145/3359996.3364242.

[7] T. Onorati, P. Diaz, T. Zarraonandia, I. Aedo, Exploring a multi-device immersive learning environment, in: Proceedings of the 2022 International Conference on Advanced Visual Interfaces, 2022, pp. 1–3.

[8] Z. Xiaoyan, B. A. Ufuk, W. A. Sinclair, S. Dylan, O. F. Raul, I did not notice: A comparison of immersive analytics with augmented and virtual reality, in: Extended Abstracts of the CHI Conference on Human Factors in Computing Systems, CHI EA '24, Association for Computing Machinery, New York, NY, USA, 2024. doi:10.1145/3613905.3651085.

[9] M. Csikszentmihalyi, Play and intrinsic rewards, in: Flow and the foundations of positive psychology: The collected works of Mihaly Csikszentmihalyi, Springer, 2014, pp. 135–153.

[10] D. Andreas, M. Jutta, Immersive learning explored: Subjective and objective factors influencing learning outcomes in immersive educational virtual environments, in: 2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE), IEEE, 2018, pp. 608–615.

[11] B. Dennis, M. Leonel, O. Patrick, Educational practices and strategies with immersive learning environments: Mapping of reviews for using the metaverse, IEEE Transactions on Learning Technologies 17 (2023) 319–341.

[12] D. Andreas, What is immersive learning?, in: 2022 8th international conference of the immersive learning research network (iLRN), IEEE, 2022, pp. 1–5.

[13] K. M. Amin, E. Areej, F. Shahbano, A. Ahlam, Exploring immersive learning experiences: A survey, in: Informatics, volume 9, MDPI, 2022, p. 75.

[14] M. Stylianos, L. Vangelis, Immersive learning, Encyclopedia 3 (2023) 396–405.

[15] D. Paloma, Z. Telmo, S.-F. Mónica, A. Ignacio, O. Teresa, Do low cost virtual reality devices support learning acquisition? a comparative study of two different vr devices, in: Proceedings of the xx international conference on human computer interaction, 2019, pp. 1–8.

[16] D. W. Shaffer, K. R. Squire, R. Halverson, J. P. Gee, Video games and the future of learning, Phi delta kappan 87 (2005) 105–111.
[17] A. A. M, H. Shabana, I. Muhammad, A. H. Saleh, W. Muhammad, Exploring cybersecurity education and training techniques: a comprehensive review of traditional, virtual reality, and augmented reality approaches, Symmetry 15 (2023) 2175.
[18] L. Anthony, K. Kenneth, G. Denis, A. Mohamed, Experiential learning through immersive xr: cybersecurity education for critical infrastructures, in: International Conference on Human-Computer Interaction, Springer, 2024, pp. 56–69.
[19] F. M. Cremer F, Sheehan B, K. AN, M. M, M. F, M. S., Cyber risk and cybersecurity: a systematic review of data availability., National Library of Medicine (2022).
[20] K. Scarfone, P. Mell, Guide to intrusion detection and prevention systems (idps), 2007.
[21] FireMon, Top 10 network security monitoring tools, 2024. URL: https://www.firemon.com/blog/network-security-monitoring-tools/#best-network-security-monitoring-tools.
[22] C. I. for Cybersecurity, Cic unsw-nb15 dataset, 2015. URL: https://www.unb.ca/cic/datasets/cic-unsw-nb15.html.
[23] C. Glenn, K. George, B. R. R, R. Suresh, Denial-of-service attack-detection techniques, IEEE Internet computing 10 (2006) 82–89.
[24] J. Andress, Chapter 5 - cryptography, in: J. Andress (Ed.), The Basics of Information Security (Second Edition), second edition ed., Syngress, Boston, 2014, pp. 69–88. doi:10.1016/B978-0-12-800744-0.00005-1.