Experiential Learning Through Immersive XR: Cybersecurity Education in Water Treatment Plants

Yeana Lee Bond, Anthony Lee, Fatemeh Sarshartehrani

1 Topic and Goals of Our Project

In this project, we address the impacts of cybersecurity attacks in critical infrastructures such as the water treatment plant facilities in Roanoke, Virginia. We propose a Virtual Reality (VR) application that can assist users with the process of learning and training about three different attack scenarios that could disrupt the normal water treatment procedure in the plant as well as the consequences that could severely affect our daily lives. The goal of our project is to promote awareness of the cyberattacks that could negatively impact our vital resources and to provide a viable solution in the form of an effective and affordable cyberattack education and training platform in an institution or workplace.

2 Experiential Learning: Scenario-Based Training Strategies

The effective learning facilitation factors focus on the trainee and training design [4]. The training system should provide learners (employees) with the talent (attitudes, knowledge, and skills) needed to perform more effectively [4]. Experiential learning is shown to have transformational effects on learners as it constructs knowledge and meaning from real-life experience [3]. Dewey (1938) discoursed this aspect of experiential learning when conceptualizing experience as an organizing focus for lifelong learning and development [6]. His work, along with the insights of others regarding necessary cognitive, affective, and environmental conditions needed for adults to constructively and effectively learn [6]. Imagine that someone 'fails' to perform a task. Then, we need to know what their reasoning and explanation is for their actions/inaction that led to the failure [6]. This is why our team took a reverse approach where we began thinking about what we could do to promote cybersecurity awareness in general to how we could evaluate what users learn using our application first. We employed a bottom-up strategy and Task Analysis [8] in coming up with three cyberattack scenarios and ideas of how users will be tested after experiencing the "before" and "after" in each attack scenario. This strategy also helped us determine what to evaluate: After reviewing more literature [7] we decided to include the component of transfer learning in the evaluation of our effectiveness because what was previously acquired can influence subsequent learning and performance [9]. In other words, it is ideally the improvement of learning in a new task through the transfer of knowledge from a related task that has already been learned [6]. In our application, while a user learns through three types of cyberattacks, of which each is mapped to one scenario, we will assess if the user can apply each type of cyberattack to the other scenarios in terms of predicting the consequence of it via the post-testing module. We expect that users will apply relevant knowledge from previous learning experiences when given new scenarios, which is the result of positive transfer learning according to learning theories [7]. Table 1, 2, and 3 offer detailed descriptions of evaluation in terms of the transfer learning aspect as well as the objective, task, goals, results, and methods in each scenario in terms of the experimental learning aspect. Lastly, the tables show our compact version of Task Analysis we customized due to the page limit.

The first scenario we propose is a Denial of Service attack. This attack portrays a scenario where a user attempts to perform a specific action on the water treatment plant computer system but is unable to due to an overload of requests on the computer system that cause it to become unresponsive. Table 1 provides a breakdown of what the scenario consists of and our learning goals.

The second scenario we plan to demonstrate is a scenario where data that is sent to the plant operator is manipulated by an attacker. This is known as an Output Manipulation Attack. Various gauges are used in the water treatment process that provide critical information for ensuring proper cleansing of the wastewater. An example of this is a meter providing the current pH level in the water. Maintaining the proper pH level for the

Objective: Users will learn what a DoS attack is and how it affects them in the context of controlling the wastewater intake rate by using a turn-style knob.	
Before the Attack	**After the Attack**
Task Goal: Users can decrease the wastewater intake rate.	**Task Goal:** Users are unable to decrease the wastewater intake rate successfully.
Action result: The flood gauge sign will reflect the correct water height in feet. Users feel satisfied. The surrounding environment remains undamaged.	**Action result:** No action could be taken at all. Users feel frustrated, stuck, and/or lost. The surrounding area becomes damaged due to flooding.
Action method: A knob mechanism taken from the Unity tutorial	**Action method:** A knob mechanism that is unresponsive from user adjustment.
Evaluation: Users are able to apply learned knowledge from this scenario in terms of how the DoS attack affects other scenarios. Users learn how cybersecurity attacks can impact their ability to make necessary modifications to the system.	

Table 1: Scenario 1 - DoS Attack Scenario in Water Treatment Plant VR Experience

Objective: Users learn how to check the current chlorine level in the water system. Users will learn to map each watercolor to the defined level. Post-attack, the user will realize the impact of output data manipulation and how they were tricked into making improper adjustments.	
Before the Attack	**After the Attack**
Task Goal: Users can control the chlorine level so that the correct watercolor is reflected.	**Task Goal:** Users are unable to see the correctly reflected water color mapped with the ppm level.
Action result: The chlorine level sign will reflect the correct watercolor and ppm level. Users feel satisfied. Water is deemed safe for use.	**Action result:** User thinks that they correctly controlled the chlorine level, but saw an unexpected watercolor. The user feels frustrated, confused, and/or stuck. Water becomes dangerous for human consumption.
Action method: A slider mechanism taken from Unity tutorial.	**Action method:** A slider mechanism works as intended, but the result of using it shows the incorrect water color due to meter data manipulation.
Evaluation: Users are able to apply learned knowledge from this scenario in terms of how output manipulation affects other scenarios. Users learn how cyberattacks can be used to trick them into performing an incorrect action. Users learn why chlorine level is important in water plant facilities.	

Table 2: Scenario 2 - Chlorine Level Monitoring Scenario in Water Treatment Plant VR Experience

Objective: Users learn what an input manipulation is in the scenario of checking and controlling the water temperature. Users learn how cybersecurity can affect their ability to maintain a certain temperature level when treating the water.	
Before the Attack	**After the Attack**
Task Goal: Users are able to change the actual water temperature to the intended value.	**Task Goal:** Users are unable to change the water temperature to the desired value.
Action result: Users are able to become familiarized with the thermal interface and make proper adjustments.	**Action result:** Users are unable to adjust the temperature as intended. Resulting in improper water treatment and unintended functionalities to be activated which may cause harm/damage.
Action method: A knob mechanism taken from the Unity tutorial and a thermometer showing the correct water temperature.	**Action method:** The knob mechanism is not working the way it is supposed to, and the temperature remains unchanged.
Evaluation: Users are able to apply learned knowledge from this scenario in terms of how an input manipulation affects other scenarios. Users learn how cybersecurity attacks can impact their ability to make necessary modifications to the system.	

Table 3: Scenario 3 - Water Temperature Control Scenario in Water Treatment Plant VR Experience

water is important for the water quality and taste. Lower pH levels introduce toxic metals into the water which cause infrastructure damage and health concerns [2]. Table 2 goes into detail about the scenario.

Our final proposed scenario is Input Manipulation. Instead of the operator being deceived through the presentation of false data, the commands that the operator inputs will be manipulated to perform an unintentional action. Users will attempt to perform a task such as increasing the water temperature based on accurate temperature readings, but none of the button mappings will match with their corresponding action, causing mass confusion and making the system unusable. Table 3 describes the scenario in more detail.

These three scenarios only portray a subset of the capabilities that cyberattacks can perform. Within these scenarios, we will present dialog boxes along with audio narration that guides the users through the scenarios and provides educational context for the scenarios being portrayed. This will enrich conceptual understanding by providing immersive experiences and demonstrations, truly embodying the essence of experiential learning. Furthermore, to evaluate our design's initial effectiveness, we will conduct an informal user study with Virginia Tech students so that polishing can be done before presenting it to the plant workers.

3 Design Process

Reflecting Dr. Bowman's feedback that we should focus on the design of the experiential learning experience rather than three-dimensional modelling of the water treatment plant, the team decided to brainstorm potential scenarios and interactions that could effectively simulate cyberattack experiences. Through collaborative ideation, three distinct scenarios were conceptualized, Denial of Service Attack, Output manipulation, and Input manipulation. These scenarios were chosen for their relevance to real-world cyber threats and their potential to foster an immersive learning experience.

To bring the envisioned scenarios to life, the team researched different VR development platforms. They specifically looked into Unity, which is widely used, has thorough documentation, and a strong support community. Furthermore, we found Unity's compatibility with Meta Quest 2 to be beneficial for the project due to the device's accessibility and immersive capabilities. Leveraging Unity's vast tutorial resources, the team extracted applicable methodologies and techniques that could be customized to meet the project's unique requirements. This exploration facilitated the conceptualization of interactive elements and environments suitable for simulating the selected cyberattack scenarios. Our team started having a clear understanding of the project's scope and its technological framework by setting milestones, setting up the virtual environment, integrating basic interactive components, and developing and refining the cyberattack scenarios through an iterative process.

In the project's hands-on stage, we made a basic virtual environment and added interactive elements. We successfully built an initial scene for the Water Treatment Plant simulation in virtual reality. Users can enter, and move around using teleportation. The key highlight is the interactive display with buttons, each serving a unique function to improve the user's learning. You can see a video of our prototype **here**. [1]

The "Instructions" button is crucial as it provides essential information about the simulation's objectives and offers guidance on how to use the VR controllers. It acquaints users with the operational aspects of the simulation, ensuring they are well-prepared to engage with the content meaningfully.

The interface has buttons that are intended to start the learning process for each of the three cyberattack scenarios specifically designed for the education framework of the project. These scenarios are still in the conceptual stage with detailed interactivity and functionality planned for future development.

Our team has planned to enhance the scenario-specific buttons with comprehensive functionalities in the future. This will allow users to actively engage with and explore the intricacies of the Water Treatment Plant. The development is aimed at providing a hands-on learning experience for the users. They can interact with the plant's components, simulate responses to cyberattack scenarios, and gain a deeper understanding of cybersecurity principles in the context of critical infrastructure.

4 Major Design Decisions

The team made important design decisions for the VR experiential learning platform based on a combination of academic research, user-centered design principles, and the practical limitations of VR technology. In this section, we will provide more information about the key choices that were made during the development process.

As part of the educational objectives of the project, it was essential to select cyberattack scenarios that accurately represented real-world threats while also enabling immersive learning. These scenarios were specifically designed to capture the complex nature of cybersecurity within the context of Water Treatment Plants. They were carefully crafted to simulate the cognitive dissonance and challenges that are commonly encountered during real cyberattacks. This approach helped to improve the learners' comprehension and resilience.

We started focusing on some scaled-down, scenario-based training modules as Dr. Bowman advised. For CS 5754 Virtual Environment, our design project is more about the VR learning experience. Hence, our design project's overarching question is how we could facilitate effective experiential learning using an immersive VR for cybersecurity training.

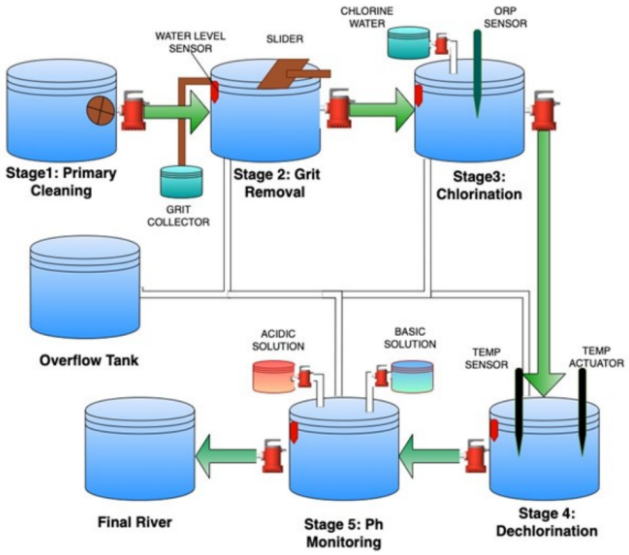

Figure 1: Five general stages for water treatment procedure [5]

The general flow of the water treatment procedure implemented in a cyber-physical system is shown in Fig. 1. Out of these five stages illustrated above, we picked three stages, Stage 1, 3, and 4, and chose one cyberattack scenario for each stage. Thus, we aim to provide users with three learning modules. Our decision to utilize Unity and Meta Quest 2 as the primary development platform and hardware was predicated on several factors, including the robustness of Unity's development environment, its extensive support for VR applications, and the immersive capabilities of Meta Quest 2. This combination was considered optimal for creating a realistic and engaging virtual environment that is accessible to a broad user base.

Recognizing the importance of user interaction in experiential learning, the team decided to prioritize the development of intuitive controls and realistic simulations. The interactive design needs to be carefully planned to ensure that users can navigate the virtual environment, manipulate objects, and respond to simulated cyberattack scenarios. This emphasis on user-centric design is instrumental in achieving a balance between educational efficacy and user engagement.

5 UX Design Challenges

As training content provided through Extended Reality is not very common yet, the majority of people most likely do not have any experience using VR. This brings up some challenge of how we can provide an interface that allows users to become familiar with the controls and interaction capabilities within the virtual environment. To overcome this challenge, our team plans on discussing the idea of providing an interactive tutorial when users first enter the environment. The tutorial will walk the users through the basic steps of using their controller to perform various actions.

To provide a realistic training experience, we need to ensure that the water portrayed in the environment possesses realistic physical properties. These consist of showing the direction of the water flow, the water wave patterns, and the changing of the watercolors based on user input/manipulation. Although our team possesses programming experience, we are all new to the Unity Development platform. Hence we do not possess experience in programming various physical properties of the Unity game objects we intend to incorporate. But we look forward to overcoming this challenge as this will be a beneficial learning experience for everyone on the team.

Some limitations of experiential learning include cybersickness and age/generational differences [4]. Some users are more sensitive to cybersickness than others which can prevent them from engaging in the learning experience. In addition, a generational gap may reduce the effectiveness of this experiential learning platform. Certain generations may struggle to use VR technology as people from different generations grew up with different types of technologies.

References

[1] Our Prototype Video. Feb 27, 2024.

[2] pH of Drinking Water and Water Contamination Corrosion Scale, 2024. Feb 16, 2024 3:33 PM.

[3] J. Balaisis. *The potential for experiential learning in the transformation of young adults.* PhD thesis, 1999.

[4] P. N. Blanchard and J. W. Thacker. *Effective training: Systems, strategies, and practices.* SAGE Publications, 2023.

[5] N. D. Chandrashekar, K. King, D. Gračanin, and M. Azab. Design & development of virtual reality empowered cyber-security training testbed for iot systems. In *2023 3rd Intelligent Cybersecurity Conference (ICSC)*, pages 86–94. IEEE, 2023.

[6] V. E. Cree and C. Macaulay. *Transfer of learning in professional and vocational education.* Psychology Press, 2000.

[7] S. Hajian. Transfer of learning and teaching: A review of transfer theories and effective instructional practices. *IAFOR Journal of education*, 7(1):93–111, 2019.

[8] B. Xie, H. Liu, R. Alghofaili, Y. Zhang, Y. Jiang, F. D. Lobo, C. Li, W. Li, H. Huang, M. Akdere, et al. A review on virtual reality skill training applications. *Frontiers in Virtual Reality*, 2:645153, 2021.

[9] S. Yardley, P. W. Teunissen, and T. Dornan. Experiential learning: transforming theory into practice. *Medical teacher*, 34(2):161–164, 2012.