

CEN 6940 Problem Understanding and Work Plan

Project Title: CyberSphere

Project Category: Innovative Product

Team Name: VR Cyber Educators

Submitted By: Thang, Taiwo, and Zoe'

Problem Statement:

The issue we aim to address is the disconnect between conventional cybersecurity education and the practical/real-world experience students require to be more proficient in the field. Common cybersecurity precepts in schools often need help engaging students and effectively training them for real-world challenges. This issue stems from the archaic practice of teaching methods needing to be more theoretical and sparsely intertwined with practical applications. Many existing programs rely largely on abstract concepts, creating a less user-friendly experience by limiting hands-on practice and real-world problem-solving opportunities. It is also through this that many students find it difficult to translate their classroom knowledge into practical skills needed in their respective fields, and with cybersecurity being heavily reliant on practical application, poses a major hindrance to the student's real-world growth.



Conclusion

The nature of this issue is born from the disparity between the structure of academic teaching and the ever-dynamic and changing requirements in the cybersecurity field. Many school modules/curricula may not effectively adapt to the ever-evolving nature and practical needs of this field, leading to many graduates feeling unprepared to enter the workforce as such, creating individuals who may have the theoretical knowledge, but lack the on-the-job training skills needed to tackle various security challenges.

The severity of this issue can be seen through the Rapidly Evolving Threat Landscape, Increased Stakes (company reputation, financial loss, etc.), and Growing Complexity of Cybersecurity. In such a field as this, Cyber threats are constantly changing with new ways of attacking and gaining access to private information coming to light. As such, the need to also evolve the ways of protecting against such threats needs to be looked at.

Presently, there are several features related to this issue. The theoretical knowledge students possess offers a strong understanding of basic cybersecurity concepts (i.e., risk management, security protocol, and network defense). Market demand also plays a role as many diverse industries are seeking skilled cybersecurity experts thus creating awareness for more individuals to pursue the field. Currently, many students report feeling unprepared to tackle real-

world challenges mainly due to their lack of hands-on training which sheds light on the existing gap many educational programs have been criticized for. Threats are also constantly evolving and due to its unpredictable nature; educational institutes presently find difficulty keeping the students' curricula to the point.

This problem relates to our cybersecurity degree because effective and efficient training in this field will develop us as more than adequate professionals who can confidently address present day-to-day security issues. Our project serves to enhance and build upon the learning provided to students such as ourselves by being placed in scenarios similar to on-the-job environments where we have to understand and tackle issues that we could encounter on a day-to-day basis.

The significance and motivation of this project is its possibility to enhance cybersecurity education by providing a more practical and engaging learning method. Our project will better link the space between theoretical knowledge and real-world practical use through its provision of a more effective educational structure thus improving student's engagement, knowledge retention, and confidence to face real-world challenges in the present digital terrain.

Key points our project aims to offer can be summarized as:

- **Active Learning & Hands-On Training:** This is a method of learning in which a student actively engages with the material while also applying theoretical knowledge. In our case, this would be achieved through simulated activities within the virtual environment that aim to reinforce the students understanding while also enhancing inherent skills such as problem-solving.

- **Simulation-Based Learning & Real-World Problem Solving:** This would involve using an interactive environment to mimic a real-world scenario. Allowing students to improve their skills (i.e., decision-making, critical thinking, etc.) while also offering an idea of what day-to-day working life would entail. Simulation-based learning can allow students to retain information better since they will be able to connect their experiences to real-life problems. An example would be allowing students to interact with a phishing email. When this incident occurs, they can remember the exact steps needed to identify if an email is a scam since they are actively identifying the threat instead of reading about it in a textbook.
- **Cybersecurity Concepts:** This covers essential topics that make up the groundwork for understanding and counteracting threats in cyberspace. It would involve reinforcing various concepts such as:
 - **Phishing:** a deceitful tactic attackers use to impersonate individuals/companies in order to retrieve sensitive information.
 - **Encryption:** the techniques of enciphering data to prevent unauthorized access.
 - **Malware:** Malicious software disguised as authorized programs designed to weaken a system.
 - **Steganography:** the process of masking information within another data to make detection difficult.
 - **Digital Forensics:** the technique of collecting and analyzing data from devices in a legal manner.

Incorporating these key points into the overall education of students helps address the gap between theoretical knowledge and practical application, and with these tools in hand, students could confidently engage in real-world scenarios, make use of data analytics to understand key information, and have a comprehensive understanding of popular threats as well as protection against them.



Visual Aid

Work to be performed:

Project Scope/Purpose

The purpose of Cybersphere is to aid and improve cybersecurity education by linking the gap between theory and practice through the use of an immersive and simulated experience that will enhance student engagement, improve knowledge retention, and make them ask questions and want to explore further, overall making them better future cybersecurity professionals.



Objectives

- All Team Members

- To facilitate active learning methods to ensure students engage with the material. Each member will contribute their area of expertise to offer exercises that promote critical thinking and problem-solving.
- Allow frequentative improvements through continuous testing and gathering of feedback to improve the curriculum and simulation so as to ensure the project evolves based on the user and real-world demand.
- Zoe'
 - Improving threat analysis skills by providing students with the resources to retrieve and understand data manipulation as well as an understanding of the dangers of malware.
- Thang
 - To provide enhanced practical skills through user/student engagement in realistic incident response scenarios and escape room simulations for handling real-world challenges.
- Taiwo
 - To give a stable balance of offense and defense by assisting students in identifying phishing attacks as well as methods of countering them.

Activities need for project completion

- Virtual Environment Development: This would involve building the virtual-reality space for use. Using the Unity Engine as well as several assets we intend to incorporate, we aim to offer an immersive experience that allows for user interaction as well as providing feedback based on actions performed.

- Curriculum Development: Creation of a diverse set of learning segments that cover essential topics can be achieved through the understanding of the present-day student curriculum in the university. This can be achieved through working with professors and experts in the field.
- Common Threat Analysis Research: Conduct extensive research on current cyber threats which entails analyzing recent attacks, and taking note of attack patterns, trends, and vulnerabilities exploited.
- Testing and Improvement: Organizing meetings for beta testing in order to take note of user feedback for further improvements. This will aid in analyzing the strengths and weaknesses present and allow for further iterations to be made prior to final delivery.`
- Incorporation Within Educational Institutes: Ensuring our project aligns with the existing cybersecurity curriculum through partnering with educators as well as offering training sessions.

List of required resources - Thang, Taiwo, Zoe':

Thang:

- Google Doc: For Report management and collaboration.
- GitHub: For version control and collaborative coding.
- Unity (Cross-Platform Game Engine): For developing the virtual environment.
- C# (Code Blocks): For programming various mechanics of the simulations.
- ACM Digital Library: For access to research papers and digital resources to aid members area research

- Asset Store (Unity asset store, GameDev Market, OpenGameArt.org, etc.): For the provision of pre-made assets for enhancing the development process.
- VR headset (Oculus Quest 3): For testing the virtual environment firsthand.

Taiwo:

- Google Doc: For Report management and collaboration.
- Unity (Cross-Platform Game Engine): For developing the virtual environment.
- C# (Visual Studio Code): For programming various mechanics of the simulations.
- Academic Search Complete: For access to research papers and digital resources to aid members area research
- 3D Modeling Suite(Blender): For creating 3D models and assets that will be used in our environment.
- Asset Store (Unity asset store, GameDev Market, OpenGameArt.org, etc.): For the provision of pre-made assets for enhancing the development process.
- VR headset (Oculus Quest 3): For testing the virtual environment firsthand.

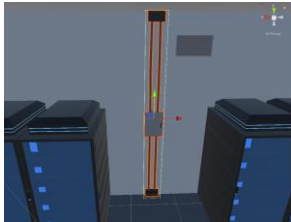
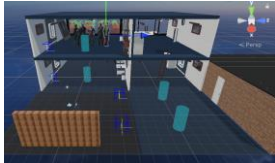

Zoe':

- Google Doc: For Report management and collaboration.
- Unity (Cross-Platform Game Engine): For developing the virtual environment.
- Unity Learn: For tutorials and resources on Unity development.
- C# (Visual Studio Code): For programming various mechanics of the simulations.
- IEEE: For access to research papers and digital resources to aid members area research
- Asset Store (Unity asset store, GameDev Market, OpenGameArt.org, etc.): For the provision of pre-made assets for enhancing the development process.
- VR headset (Oculus Quest 3): For testing the virtual environment firsthand.

Timeline:

Weekly Goals for Each Individual

Weekly Outcomes

	Thang	Taiwo	Zoe'
Week 3 (Sep 5 - Sep 11th) Organization of Overall Project and Goals	Focus: Incident Response and Interactive Training.	Focus: Cybersecurity Techniques & Threats	Focus: Threat Analysis
Week 4 (Sep 12 -Sep 18) Kick-off Meeting (Finalize roles. Responsibilities, Setup communication options and Project Management Tools, Role Research)	-Incident Response Scenario - Escape Room	-Phishing -Encryption	-Malware -Digital forensics
Week 5 (Sep 19 - Sep 25) Identify needed assets & material needed.	- Unity - VS code - UNF Library Database -VR Headset	-Unity -VS Code -UNF Library Database -VR Headset	-Unity -VS Code -UNF Library Database -VR Headset
Week 6 (Sep 26 - Oct 2) Design Drafts for simulator, puzzle, scenario, etc.	The room will focus on a Server breach with flashing lights and require the user to navigate through traps to disconnect power (Incident Response)	-Interactive puzzle-based scenario. (Encryption) - Encryption key using hidden messages (Phishing)	- Data extraction and analysis through photo (Digital Forensics) -Allow users to encounter malware through the system. (Malware)
Week 7 (Oct 3 - Oct 9) Initial Prototype			
Week 8 (Oct 10 - Oct 16) Feedback and Interaction of prototype	Receive feedback on the Escape Room environment.	Receive feedback on the Phishing and Encryption environment	Receive feedback on the Malware and forensics environment

Week 9 (Oct 17 - Oct 23) Update designs based on feedback received	-Incident Response Scenario - Escape Room	-Phishing -Encryption	-Malware -Digital forensics
Week 10 (Oct 24 - Oct 30) VR Integration and testing	Will be incorporating VR integration to allow users to navigate through the escape room. Examples include Dodge traps and interacting with server breach.	Integrate VR into the Phishing and Encryption environment by requiring users to move around the environment. Users will be able to climb ladders, interact with doors and objects.	Users will be required to move around rooms, climb ladders, and interact with keys in the threat analysis environment. These keys will be used to unlock doors through VR.
Week 11 (Oct 31 - Nov 6) Controlled user testing feedback	Send out announcement requesting for volunteers to come in and test the room and have volunteers who did the training to fill out a survey to give feedback.	Reserve room in the computing building for individuals to test. (VR lab)	Request VR headset to use during the test.
Week 12 (Nov 7 - Nov 13) Fine tuning and potential system enhancements	Determine if changes need to be applied to the project based on feedback received.	Improve the environment based on feedback from controlled user testing on phishing and encryption material.	Change or incorporate new mechanisms depending on feedback received.
Week 13 (Nov 14 - Nov 20) Finalized system/quality assurance	Update and finalize needed parts of the Incident Response Scenario and escape room.	Finalize the creation and system of the phishing and encryption room.	Complete any needed parts of the malware and digital forensics room setup.
Week 14 (Nov 21 - Nov 27) Project documentation/Presentation	Complete Project documentation for Incident Response and escape room. - Include	Complete Project documentation for Phishing and encryption. - Include	Complete Project documentation for Malware and Forensics. - Include

	<p>experiences dealt with while creating and testing the escape room.</p> <ul style="list-style-type: none"> - prepare for Final Presentation. 	<p>feedback based on the puzzle-based scenario and encryption with hidden messages</p> <ul style="list-style-type: none"> - prepare for Final Presentation. 	<p>feedback about the interaction of users with their ability to analyze the photos provided.</p> <ul style="list-style-type: none"> - prepare for Final Presentation.
Week 15 (Nov 28 - Dec 4) Rehearsal & Final Report	Rehearse material on the escape room environment and prepare the final report section.	Rehearse material on phishing and encryption room environments and prepare the final report section.	Rehearse material on the malware and forensics room environments and prepare the final report section.
Week 16 (Dec 5 - Dec 10) Final Product Delivery	Present Final Product	Present Final Product	Present Final Product