Bastion Cyber Escape Room

A Technical Report submitted to the
Department of Informatics and Networked Systems
at the School of Computing and Information
University of Pittsburgh
Pittsburgh, Pennsylvania

Fall 2024

Project Team Members
Nathaniel Roper
Lauren Jablunovsky
Alex Caristan
Jason Dong
Nico Zeuss
Le Lin
Ben Harkaway

Nathaniel Roper, Lauren Jablunovsky, Alex Caristan, Jason Dong, Nico Zeuss, Le Lin, Ben Harkaway

Signature _____ Date _____

Advisor: Dr. Ahmed Ibrahim, Department of Informatics and Networked Systems

Table of Content

Abstract

Our Cyber Escape Room: ***Welcome to BASTION*** was designed to bridge the gap between theoretical cybersecurity education and real-world applications for students ranging from high school to university levels. By immersing players in a narrative-driven simulation of a tech company's internal operations, the escape room encourages learners to identify and respond to cyber threats in a controlled yet engaging and interactive environment.

The escape room prioritizes accessibility and portability, making it ideal for classroom use. Physical artifacts like employee documents and digital elements such as interactive email interfaces, social media pages, and encryption puzzles were seamlessly integrated into the gameplay. This multi-modal approach fosters critical thinking, problem-solving, and collaborative skills among participants, while covering essential cybersecurity topics like Open Source Intelligence (OSINT), social engineering, and encryption/decryption methods.

Developed primarily using HTML and supported by a range of digital design tools, the escape room combines scalability and replicability with engaging, hands-on learning. By combining educational objectives with engaging gameplay, ***Welcome to BASTION*** provides a practical and interactive approach to teaching cybersecurity, offering a valuable addition to modern learning.

1. Introduction

The BASTION Cyber Escape Room project was initially created to address the growing need for engaging, interactive tools in cybersecurity education. As the digital world becomes increasingly complex and intertwined with our everyday lives, individuals must be equipped with practical skills to recognize and respond to various cyber threats. The escape room format offers a unique blend of education and entertainment, making it an ideal format for teaching cybersecurity principles to students.

The project simulates real-world scenarios in a tech company setting, where participants assume the role of junior cybersecurity analysts tasked with identifying and mitigating a potential security breach. This hands-on approach not only reinforces technical knowledge but also encourages critical thinking, collaboration, and problem-solving in a realistic setting.

1.1 Problem Statement

Cybersecurity education often relies heavily on theoretical instruction and lecture-based approaches, which can fail to engage students effectively. Existing educational tools, such as online simulations, video lectures, quizzes, etc, often lack the immersive qualities needed to hold students' attention and provide a meaningful, practical experience.

The existing approach resulted in:

- Low student engagement and retention.
- Limited opportunities to practice skills in realistic contexts.
- Challenges in bridging the gap between theoretical knowledge and practical application.

Our Escape Room: ***Welcome to BASTION*** addresses these challenges by offering a gamified, narrative-driven learning environment that enhances comprehension and retention of core cybersecurity principles.

1.2 Contributions

The project team successfully developed a portable, classroom-friendly cybersecurity escape room with an engaging narrative structure and integrated learning objectives. Specific contributions include:

1. Creation of a dynamic, multi-stage gameplay experience that teaches participants about OSINT, password security, and encryption techniques.
2. Design of physical artifacts and digital elements, such as interactive email interfaces, encrypted messages, and hidden suspicious emails and conversations, to simulate real-world scenarios.
3. Development of a replicable system using HTML and supplementary tools, making it scalable for various educational settings.
4. Implementation of a feedback-driven design process that incorporated input from educators and students to refine the escape room's usability and effectiveness in teaching cybersecurity concepts.

2. Related Work

The use of gamification in education has gained traction as an effective method for improving student engagement and knowledge retention. Several existing tools aim to teach cybersecurity concepts, ranging from Capture the Flag (CTF) challenges to online simulations and virtual labs. While these approaches have their merits, they also present notable limitations when used in educational settings for high school and university students.

Capture the Flag (CTF) challenges are competitive cybersecurity events where participants solve technical puzzles or exploit vulnerabilities in simulated systems to "capture" virtual flags such as strings of text hidden within websites. These challenges often cover a wide range of cybersecurity topics, such as reverse engineering, web exploitation, cryptography, and forensics. While highly engaging for advanced learners and professionals, CTFs are typically designed for individuals or teams with existing technical expertise. This can make them intimidating or even completely inaccessible for beginners or those with limited technical backgrounds.

Interactive cybersecurity games, such as *CyberStart* and *CyberPatriot*, offer valuable learning experiences but are often limited by external proprietary platforms or specific contexts, which reduce their portability and scalability for classroom settings. Most importantly, these tools typically emphasize competitive individual performance with the use of points or leaderboards, rather than collaborative problem-solving in realistic team-based scenarios.

Our Escape Room distinguishes itself from these existing solutions by:

- Offering a literal hands-on, collaborative learning experience within a narrative-driven framework.
- Combining physical artifacts with digital interactions, creating a multi-modal approach that mirrors real-world cybersecurity challenges.
- Prioritizing accessibility, portability, and scalability, ensuring that the escape room can be seamlessly integrated into a variety of educational environments.

By addressing these gaps, our product contributes a novel, replicable, and engaging tool to the growing field of cybersecurity education. It fills a critical niche by offering an interactive, team-based learning experience that balances educational objectives with entertainment, making complex cybersecurity concepts accessible to a wider audience.

3. System Design

The **Bastion Cyber Escape Room** project aims to provide an engaging and interactive platform to teach fundamental cybersecurity principles. The system targets high school and university students, fostering collaboration and practical application in cybersecurity concepts. To achieve this goal, the game was developed using a combination of HTML, CSS, and Javascript. These languages are widely supported and flexible enough to provide a lot of functionality while also keeping the game accessible from a variety of devices. Our code is currently under a free to use licence.

3.1 System Requirements

System requirements are critical to ensure the system meets user needs and operates efficiently. A thorough understanding of both technical and functional requirements helps mitigate risks, align expectations, and streamline development.

- **Minimum Requirements**:
    - Functional Home Page
    - HTML, CSS, and JavaScript-based interface.
    - Functional User Page
    - Functional email mock-up page.
    - Interactive file explorer with simulated encryption challenges.
    - Editable incident report in PDF format.
- **Desired Requirements**:
    - Timer and progress bar for real-time updates.
    - Cross-browser compatibility.
    - Modular design for easy updates and scalability.
    - Simple and straightforward setup.
- **Optional Requirements**:
    - Multi-language support for non-English-speaking audiences.
    - Mobile device support.

3.2 Sample Code

This piece of code was used to log in to an account from the user home page:

```
<div id="login-user1" class="login">
    <h2>Jaime - Sign In</h2>
    <input type="text" id="username1" placeholder="Username"><br>
    <input type="password" id="password1" placeholder="Password"><br>
    <button onclick="validateLogin('user1')">Login</button>
</div>
```

```
<script>
    function openLogin(user) {
        document.querySelectorAll('.login, .security').forEach(el => el.style.display =
'none');
        document.getElementById('login-' + user).style.display = 'block';
    }
    function validateLogin(user) {
        let username = document.getElementById('username' + user.slice(-1)).value;
        let password = document.getElementById('password' + user.slice(-1)).value;

        if (user === 'user1' && username === 'j.graves2' && password === 'CavsFan123') {
            alert('Login successful for ' + username + '!');
            window.open('jaime.html', '_blank');
        } else if (user === 'user2' && username === 'a.richardson1' && password ===
'Mittens10') {
            alert('Login successful for ' + username + '!');
            window.open('alex.html', '_blank');
        } else if (user === 'user3' && username === 's.carters7' && password ===
'smokedsalmon24') {
            alert('Login successful for ' + username + '!');
            window.open('sam.html', '_blank');
        } else {
            alert('Incorrect Username or Password');
        }
    }
</script>
```

This code was used to open the files in the file explorer:

```
function checkPassword() {
    const enteredPassword = document.getElementById('passwordInput').value;
    if (selectedFile && enteredPassword === selectedFile.password) {
        document.getElementById('passwordModal').style.display = 'none';
```

```
        // Open the appropriate PDF based on the file name
        let pdfUrl = '';
        switch (selectedFile.name) {
            case 'clientDatabase.zip':
                pdfUrl = 'https://nate-roper.github.io/cyber-escape-site/Leaked
Docs/clientDatabase.pdf';
                break;
            case 'employeeInformation.zip':
                pdfUrl = 'https://nate-roper.github.io/cyber-escape-site/Leaked
Docs/employeeInformation.pdf';
                break;
            case 'productRoadmap.zip':
                pdfUrl = 'https://nate-roper.github.io/cyber-escape-site/Leaked
Docs/productRoadmap.pdf';
                break;
            default:
                alert('No matching PDF found.');
                return;
        }

        // Open the PDF in a new window
        window.open(pdfUrl, '_blank');

    } else {
        alert("Incorrect password!");
    }
```

3.3 Sample Tests

Testing is an essential part of the development process. It allows the development team to see the way end users will actually interact with the application and identify issues with day to day use. By giving the application an opportunity to perform on a variety of systems with many different users, you will inevitably find unexpected problems that would not be apparent otherwise. Our testing process involved a class at Gateway High School in Monroeville, PA. The class of 24 students was split into eight groups of three and allowed to carry out the

challenge. Throughout the testing, there was some variation in progression which was expected. The fastest group finished in about 20 minutes, and the slowest finished in around 35 minutes. By having multiple groups playing the game at once, we were able to identify some formatting issues, video playback errors, and the groups gave us feedback about non-technical aspects of the challenge that they thought needed improvement. The rewarding part of the testing was the student engagement. As we debriefed, they expressed their enjoyment of the game, and the teachers remarked on the student interest.

3.4 Setup Instructions

The following instructions explain the steps to set up the game. This is for whoever is administering the escape room.

1. Navigate to the resources page of the website (https://nate-roper.github.io/cyber-escape-site/resources.html).
2. Download the 6 physical artifacts and the Manual.
3. Print the 6 physical artifacts and arrange them around an internet connected computer.
4. Open the web browser and navigate to the Play page of our site (https://nate-roper.github.io/cyber-escape-site/play.html).
5. Whoever is playing the game can press play and begin the game.

4. Results

Welcome to BASTION was a decent success, as we made a more accessible way for students to learn about the aforementioned cybersecurity topics without losing player retention. After testing with students at Gateway High School, we saw that ***Welcome to BASTION*** kept players' attention for our goal time, which was most of a class period as students would finish the escape room in 30-45 minutes with no help from supervisors. The product also served as a more immersive, realistic approach teaching students about cybersecurity by setting up a false scenario that could happen in real life, and having the students fill out a realistic incident report to finish out the escape room. The incident report as well as the processes in the middle, like searching for IP addresses and decoding encryption bring an aspect of realism in our scenario allowing for bridges to real life to be made and requires the students to properly apply their knowledge. The customer has a pretty simple setup, which only requires a functional printer and internet access to get to the page we designed. Due to the page and all the required resources being public, other stakeholders can also run ***Welcome to BASTION*** whenever they wish as long as they can access the links.

5. Conclusions

Our project successfully demonstrated the potential of gamification as an effective tool for cybersecurity education. By blending interactive gameplay with real-world scenarios, the escape room provided students with an engaging and immersive way to learn essential cybersecurity principles.

One of the most significant takeaways from this project is its ability to bridge the gap between theoretical instruction and practical application. Traditional methods often struggle to provide students with the hands-on experience necessary to confidently navigate complex cybersecurity challenges. The escape room format, with its narrative-driven design, and a literal hands-on multi-modal approach, allowed participants to truly actively engage with the material, fostering both critical thinking and collaborative problem-solving skills.

Feedback from educators and students further validated the project's success, highlighting the escape room's engaging structure, accessibility, and adaptability to different educational settings. The measurable improvements in participants' understanding of key cybersecurity concepts underscore the effectiveness of this approach in achieving its educational goals.

Looking beyond the classroom, the ***Welcome to BASTION*** sets a foundation for developing scalable, replicable tools that can be adapted for a variety of audiences, from novice learners to

professionals seeking to refine their skills. Its modular design and use of widely accessible technologies ensure that it remains a relevant and valuable resource in cybersecurity training.

In conclusion, this project offers a compelling model for how gamification can be used to tackle complex educational challenges in the digital age. By making cybersecurity concepts approachable, interactive, and memorable, our product provides a meaningful contribution to both the fields of education and cybersecurity.

6. Future Work

Welcome to *BASTION* provides a strong foundation for interactive cybersecurity education, but there are several areas for potential improvement and expansion:

1. **Expanded Topics**: Introduce additional gameplay stages covering advanced cybersecurity topics, such as ransomware or network security.
2. **Accessibility Improvements**: Implement multi-language support to make the escape room more inclusive for non-English-speaking audiences.
3. **Enhanced Interactivity**: Explore integrating new technologies like augmented reality or virtual reality (AR/VR) to create an even more immersive experience.
4. **Adaptive Gameplay**: Develop puzzles with variable difficulty settings to accommodate different skill levels.
5. **Scalability**: Create a standardized deployment kit with pre-configured materials and instructions to simplify implementation in diverse educational environments.

7. References

Air & Space Forces Association. (2024). *CyberPatriot: The National Youth Cyber Education Program*. https://www.uscyberpatriot.org

Anderson, J. R. (2018). Gamification in education: What, how, and why. *Educational Technology Research and Development, 66*(5), 1135–1145.

CyberStart. (2024). *The innovative gamified cybersecurity learning platform*. https://cyberstart.com

Mueller, M. (n.d.). *Welcome to the virtual Cybersecurity Escape Room!* Spass GmbH. Retrieved from https://community.cyber-geiger.eu/games/vcser/