CyberBlock README Document

Overview

What if I told you that your pacemaker could be hacked at any moment? Medical device manufacturers, healthcare providers, and regulators are increasingly facing issues with the security of medical devices. While it can be simple to make medical devices more secure, the trade-off is the loss of efficiency. CyberBlock started as a card game created by Ben, Tram, and Jeannine who are members of Medtronic. The purpose of the game is to train people in the medical device industry in cybersecurity and improve their strategic decision making used to defend against real world cyber-attacks. The team at Medtronic tasked us with creating a web-based version of CyberBlock. Our digital version expands on the physical card game with new features and the ability to play remotely, allowing people all over the world to participate. Without the limitation of physical cards, the attacks and defenses can be kept up to date with current real-world cyber threats. The computer-based game will have features to allow teams to purchase security defenses for their devices using limited resources. Hosts will create game lobbies that users will be able to join using a game code. The users will then face off against cyber-attacks with their purchased defenses. If the team can fend off the attack, whether from eliminating or remediating the attack, they will be awarded points. At the end of the game, the team will be able to view the number of points received through a scoreboard.

Purpose

The purpose of the CyberBlock game is to engage students and workers involved in the medical device security field by having users purchase upgrades and defenses in a game environment that could potentially stop cyber-attacks similar to situations that they would face in the real world. With a web-based version of the game, participants will learn how to counter cyber-attacks using defenses that could be implemented into medical devices and from the interactions, we hope to provide an enjoyable experience for the players.

Technology Used

- Frontend
    - React
        - Free to Use
        - Most used framework
        - Great for frequently changed web state
    - Socket.IO
        - Allows live communication between the client and the server
- Backend
    - Node-JS
        - Open source and cross-platform
        - Enable developer to create both front and back end with JS
    - Socket.IO
        - Allows live communication between the server and the client

    - MySQL
        - This database is widely supported on many types of hardware
        - Mature Relational Database System
- CSS
    - Material-UI
        - React UI library that allows us to easily create a responsive user interface
- Hosting Platform for Development
    - Heroku
        - Faster and Easy Deployment
        - Low computational demand
    - CyberBlock was moved to Medtronic Servers to be internally hosted

Target Audience

The game is designed for students learning cybersecurity principles and cost-effectiveness of defenses in relation to modern cyber-attacks. The CyberBlock game is independent and self-contained. Cyber security instructors will be able to create game lobbies where users can join the game and play along. The game's purpose is to train students or employees how to manage and prepare for cyber security risks via defenses and learn which defenses work well against which attacks.

The users for the game are divided into two categories: beginner, intermediate and advanced players. The beginner's category will have reduced card sets based on the attack score below five. The difficult mode will have all the cards set. The beginner user's interface will have the least number of cards sets and the advanced level users will have the greatest number of cards. The attacks will have difficulty as attribute to determine whether the attack is beginner, intermediate or advanced level attack.

Cautions

A few precautions that all users can take while playing this game are as follows:

Refrain from refreshing the game while in session as it disconnects you from the game.

In any case of disconnection, the player is unable to rejoin.

The game is not immune to any SQL injections.

The app is vulnerable to any web attacks overall.

References

"Mitre ATT&CK." MITRE ATT&CK, The MITRE Corporation, 2021, https://attack.mitre.org/.

"D3fend Matrix: Mitre D3FEND." D3FEND Matrix | MITRE D3FEND, The MITRE Corporation, 2021, https://d3fend.mitre.org/.

"General Cyber Security Taxonomy", University of Kent, 2021, https://cyber.kent.ac.uk/research/cyber_taxonomy/app/taxonomy/visualization?t=space_tree&n=Cyber%2BSecurity&st=true&nid=39.

"Common Attack Pattern Enumeration and Classification." CAPEC, The MITRE Corporation, 25 Feb. 2021, https://capec.mitre.org/.Tram-Anh Cai."CyberBlock Components", Medtronic, 09/09/2021

Contacts

Benjamin Pope (benjamin.pope@medtronic.com)

Tram-Anh Cai (tram-anh.cai@medtronic.com)

Jeannine Looney (jeannine.looney@medtronic.com)

Debra Parcheta (debra.parcheta@ucdenver.edu)