BlueHack: Arduino-Based Exploration of Bluetooth Vulnerabilities

Brian Mhatre, Ryan Usher, Brandon Cegelski

February 2024

1 Problem

Bluetooth Low Energy (BLE) is a low cost a easy to implement technology that enables efficient communication between small devices. Despite its widespread use, its susceptibility to security breaches such as spoofing and unauthorized access raises substantial concerns. These vulnerabilities not only compromise the integrity and privacy of data exchanged between devices but also pose risks to users' security, especially in applications involving sensitive information such as health monitoring devices. Our proposed project will involve researching the vulnerabilities in BLE, implementing a specific hack and finally researching new security measures used to safeguard the Internet of Things infrastructure against potential attacks.

2 Project Timeline

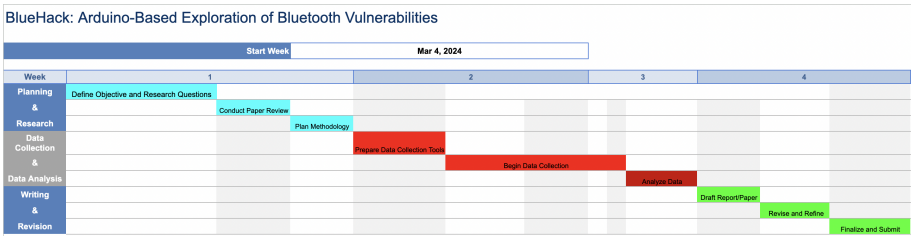

Figure 1: Weekly Project Timeline Over A One Month Period

The image identifies the Project timeline. The first week is dedicated to planning and research, which includes defining objectives and research questions, conducting a paper review, and planning methodology. In the second week, the focus shifts to preparing data collection tools and beginning the actual data collection. The third week is centered around continuing the data collection and analyzing the gathered data. The fourth and final week is reserved for drafting

the report or paper, revising and refining the draft, and ultimately finalizing the document and submitting it.

3 Team Member Roles