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

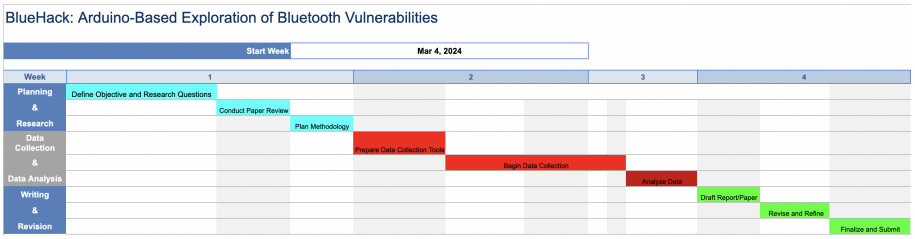

Figure 1: Weekly Project Timeline Over A One Month Period

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.

Project Schedule

	ASSIGNED TO:	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
Week 1	Ryan Usher	Research and Document on Exisiting Papers			Plan Methodology	
	Brian Mhatre	Research Papers for Literature Review				
	Brandon Cegelski	Literature Review				Compile literature review for related work section
	ASSIGNED TO:	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
Week 2	Ryan Usher	Develop a basic Arduino program to initiate Bluetooth pairing				
	Brian Mhatre	Determine Bluetooth Vulnerability to Attack and Detail Plan				
	Brandon Cegelski	Compile literature review for related work section	Help solve any technical problems. If none then start working on getting threat model into paper			
	ASSIGNED TO:	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
Week 3	Ryan Usher	Test Bluetooth Paring		Analyze Data		Record Results/Vunerabilities
	Brian Mhatre	Implement Attack and Test it Against App Arduino Connection				
	Brandon Cegelski	Help solve any technical problems. IF none then start work on writing project attack section of paper, results, and conclusions section				
	ASSIGNED TO:	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
Week 4	Ryan Usher	Create Draft Project		Finalize Project and Prepare for Presentation		
	Brian Mhatre					
	Brandon Cegelski					

Figure 2: Individual Project Timeline Over A One Month Period

3 Team Member Roles

Ryan Usher: Project Lead

- Oversee project kickoff and ensure team alignment with project objectives
- Manage the setup for data collection tools and resources.
- Ensure the methods are correctly applied.

Brian Mhatre: Research Analyst

- Find papers and write summaries for literature review.
- Implment man in the middle attack for BLE.
- Test implmentation and collect data on the attacks effectiveness.

Brandon Cegelski: Technical Specialist

- ...
- ...
- ...