ECE 707 Final Report

Brian Mhatre

April 2024

1 Introduction

2 Motivation

3 Bluetooth Vulnerabilities

4 Implementation

The vulnerability we targeted involves a flaw in Bluetooth implementations, allowing the establishment of new connections from devices already connected. This attack concept was inspired by the paper "Cut It: Deauthentication Attack on Bluetooth," where a deauthentication strategy was effectively implemented using this vector. Our experiment setup included an Arduino Rev equipped with an HC05 Bluetooth module and an Android device running a basic app to establish a connection and send a continuous stream of messages to the HC05. Upon securing the connection, we employed a virtual machine running Linux equipped with a wireless Bluetooth adapter to execute the attack. We utilized the Python library, Bleak Scanner, to monitor and record the device name and MAC address of each detected device. Subsequently, we used the Linux command 'spooftooph' to alter the MAC address of our Bluetooth adapter and 'l2ping' to dispatch echo requests.

Our attack followed these steps: Initially, we scanned for the MAC addresses of nearby devices. After the scan, the user selected the MAC addresses of the master (impersonator) and slave (victim) devices. The Bluetooth adapter was then reconfigured to mimic the master device. Following this setup, a barrage of pings was directed at the victim's MAC address, utilizing multiple threads spawned by Python's 'subprocess' library and the flood option in 'l2ping.

To defend against this attack we added code to the Arduino Rev to detect when spam pinging was occurring and delay the processing of requests until the pinging stopped.

5 Results

6 Next Steps