The Center for Cyber Defenders

Expanding computer security knowledge

BLE Role Reversal

Caroline Kish, Georgia Institute of Technology

Project Mentor: Jeremy Giron, Org. 5867

SAND2019-8024D

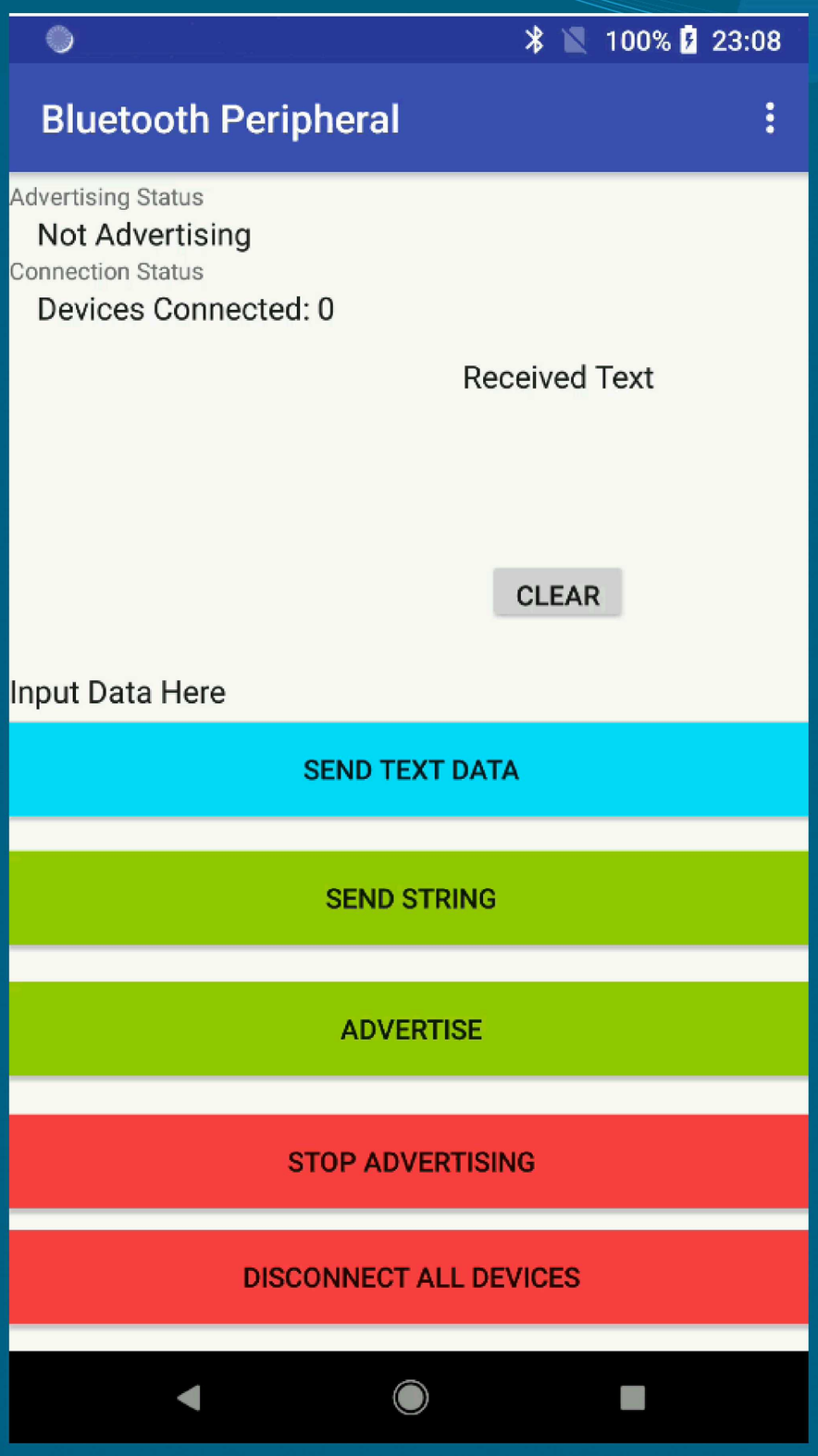
Problem Statement:

In most Android Bluetooth communications, the Android device acts as the central device, and the device it pairs with acts as the peripheral device. Our goal is to provide authentication and encryption to the reverse of this interaction (where a Pixel 2 acts as the server and an embedded system acts as the client). Implementing these security features will allow the embedded system to authenticate an advertising device before connecting to it. It will also encrypt communication between the two devices to prevent eavesdropping.

Approach:

- Gain familiarity with Bluetooth low energy (BLE) communications and Bluetooth 5 protocols.
- Explore and compare the libraries used to implement whitelisting, authentication, and encryption on the embedded system.
- Experiment with different implementations of the security features based on online forum discussions and embedded system module examples.
- Use Bluetooth sniffing device to test and confirm security features.

Android Application Design:



Results:

- Enabled whitelisting and authentication before BLE pairing and bonding occur.
- Encrypted communication between the embedded system and the Pixel 2 phone.

Impact and Benefits:

- Ensure that only trusted devices are able to connect with the embedded system, and ensure that all communication between the Pixel 2 and embedded system is protected.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.