The Center for Cyber Defenders

Expanding computer security knowledge

BLE Role Reversal

Mia Wilson, Ohio University

Project Mentor: Jeremy Giron, Org. 5867

SAND2018-7370D

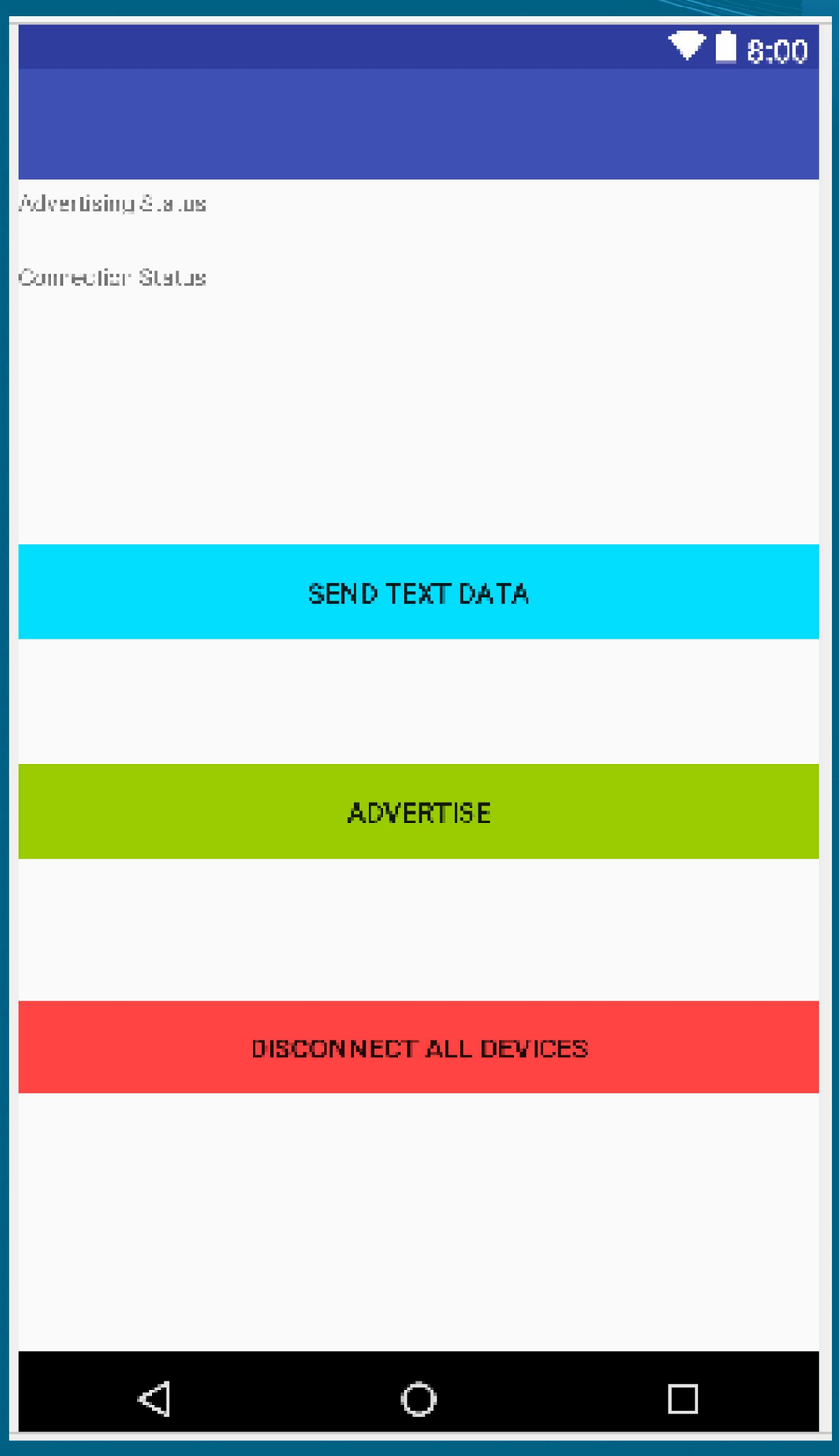
Problem Statement:

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 reverse this interaction allowing for a Pixel 2 to act as the server and an embedded system to act as the client. Implementing this role reversal will allow the phone to advertise for a connection, while the embedded system listens for a device to connect to. This allows a connection to be made between the embedded system and the phone, without advertising packets being transmitted from the embedded system when the phone is not present.

Approach:

- Gain familiarity with Bluetooth low energy (BLE) communications and Bluetooth 5 protocols.
- Learn the software development kit libraries for client set up on the embedded system side. Create source code with IAR IDE to allow listening, connection, data transfer, and disconnect for the Rigado module.
- Learn APIs used in Android Studio to enable peripheral mode. Develop an application for the Pixel 2 to allow advertising, connection, data transfer, and disconnect.
- Create Bluetooth sniffing device to monitor and validate data transmission.

Android Application Design:



Results:

- Enabled advertising on the Android and listening on the Rigado. From there we were able to get the devices connected.
- We plan to have data transmission between the two devices by the end of the summer.

Impact and Benefits:

- Keep the embedded system from advertising itself, in contrast to the typical situation where it acts as a peripheral.

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.