CCS Lab Internship opportunity

1. Summary

- Advisor: Prof.Heejo Lee
- Working period: 2 months (October – November 2021, can be extended)
- Required people: 1 person
    - Certain amount of wage as a lab intern will be provided

2. Work description

1. Develop a Bluetooth fuzzing tool

(bfuzz, see https://www.iotcube.net/process/type/bf1)

- Bluetooth fuzzer is a tool for discovering implementation error of Bluetooth-enabled devices with mutated wireless packets.
- Specific works
    - Analyze bfuzz's fuzzing algorithm and suggest new fuzzing algorithm
    - Develop Bluetooth RFCOMM protocol fuzzer
    - Research Bluetooth protocol stack fuzzing test (papers, commercial tools)

2. Fuzzing Test on Bluetooth-enabled devices.

- Test Bluetooth fuzzing tool on the Android devices, automotive AVN(Audio Video Navigation) system and laptops.
    - Test host Bluetooth drivers (e.g. Bluez, Bluedroid…) on the variety of Bluetooth-enabled devices
    - Collect crashes and analyze vulnerable crashes through Android Debugging Bridge (ADB) and hcidump.

3. Requirements

- Passion for improving programming skills

- Interest in Bluetooth and security
- Smooth communication

4. Contact

Please contact Haram Park (freehr94@korea.ac.kr) if interested!