



Student Assistant (m/f/) in cooperation with Fraunhofer AISEC*

Network protocol fuzzing of embedded devices

Fuzzing is a popular technique to automatically discover bugs in a given software by mutating a given input such that the new input crashes the target. However, fuzzing embedded IoT devices poses unique challenges as resources on these systems are usually scarce.

Task Description

We are looking for a student assistant (m/f/*) helping us implement model-based fuzzers for network protocols found in embedded devices.

Your duties include:

- Researching protocol specifications (e.g. Wifi/802.11, Bluetooth, ...)
- Implementing a fuzzer for selected protocols using a python based fuzzing framework
- Evaluation of these fuzzers on selected IoT devices
- Building ontop prior work, further development of a repeatable, generic test setup these fuzzers can run on

Requirements

- High motivation and ability to work independently
- Good programming skills in Python3
- Familiarity with IoT platforms (ESP8266, ESP32, ...) is beneficial
- Experience programming embedded C and debugging embedded code is preferred

Contact

Please send your application with current CV and transcript of records to:

Katharina Bogad

Fraunhofer Institute for Applied and Integrated Security (AISEC)

Secure Operating Systems

Lichtenbergstr. 11, 85748 Garching near Munich

Mail: katharina.bogad@aisec.fraunhofer.de

Phone: +49 89 322 9986-1020

Publication Date: 15.09.2022