Lehrstuhl für Sicherheit in der Informatik
Prof. Dr. Claudia Eckert

Fraunhofer AISEC

HiWi-Job *in collaboration with Fraunhofer Research Institute AISEC*

Black-Box Fuzzing of Wi-Fi Chip Firmware

Date: *8. Juli 2019*

Motivation

The ESP8266 and ESP32 are broadly used Wi-Fi chips in IoT deployments. Their firmware implements, amongst others, a networking stack which eases developers from the burden of implementing/integrating their own stack into their IoT applications. The integrity of such firmware, possibly deployed in millions of existing, geographically dispersed devices, is decisive for their availability. While the source code of embedded firmware is often not available open source, identifying bugs and vulnerabilities becomes difficult. For this purpose, we are implementing a (black box) firmware fuzzing testbed for embedded equipment, such as the ESP Wi-Fi chip.

Task Description

The task is to extend the testbed's fuzzing engine (based on boofuzz) with support for the fuzzing of layer 2 Wi-Fi protocols (802.1X). The current fuzzing engine only allows the fuzzing of higher-layer protocols. The task includes testing the extended fuzzing setup with the Wi-Fi chip firmware, and analyzing fuzzing results regarding possible bugs and vulnerabilities.

Requirements

- Good C programming skills and basic experiences with microcontroller programming
- Basic experience with fuzzing
- Optional: Experiences with Wi-Fi chips, binary exploitation

Contact

Manuel Huber (manuel.huber@aisec.fraunhofer.de) or
Fraunhofer Research Institute AISEC
Parkring 4, 85748 Garching (bei München)
Phone: 089/3229986165