Security Analysis of the ESP Wi-Fi Chip

Date: 8. Februar 2019

Motivation
The ESP8266 is a widely used Wi-Fi chip in IoT deployments. The ESP implements a networking stack, easing developers from the burden of implementing/integrating their own networking stack into their IoT application. The integrity of the firmware on the ESP is decisive for the availability of IoT devices, possibly deployed in millions of existing, geographically dispersed devices.

Task Description
The first step of this work is to develop a good understanding of the Wi-Fi chip and to compare it with similar chips on the market. The next step is to conduct a thorough security analysis of the firmware to assess possible vulnerabilities. The analysis includes an evaluation of vulnerabilities, and should propose concepts and solutions on how to protect the firmware. The proposed topic is in general not limited to the herein described tasks and allows for several similar follow-up activities.

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

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