Planning and Implementation of a Secure Wireless Communication System for an IoT Sensor Installation

Ferdinand Keil, April 2022

1. Introduction

As part of a recently started project, a custom communication platform will be installed in LED street lights. This platform will monitor important parameters of the electronic components inside the street light with the goal of identifying their degradation over time. The platform will have access to the DALI bus controlling the driver of the street light which can be used to turn the light off. Thus, it is considered a safety-critical application.

As the street light is installed on a mast at a substantial height, the data captured over the course of the project will have to be retrieved wirelessly. To prevent attackers from seizing control over the custom platform its communication has to be thoroughly secured.

2. Tasks

In this work a systematic approach for securing the aforementioned communication channel should be developed and the proposed scheme implemented.

A threat model will be laid out as a foundation for the planning of the system. This threat model is created according to current best practices in information security. It will identify the possible threats, rate them and suggest counter measures.

The implementation of the communication system will be based on Linux and standard software packages. The final solution will demonstrate communication with an ESP32 microcontroller board as a stand-in for the communication platform. The access point will be implemented on a Raspberry Pi single-board computer.

3. Required Skills

- Linux (bash, systemd)
- Networking
- Certificate-based encryption
- Basics of information security
- Embedded development with C/C++

4. Keywords & Ideas

- hostapd
- OpenSSL
- WPA2 EAP-TLS
- Radius
- Certificate Authority
- LetsTrust TPM
- Hardware RNG
- …