Improving Over-The-Air Fuzzing against WLAN Firmware in Android (Bachelor/Master Thesis)

Background

Fuzzing is a software testing method that is based on providing inconsistent or invalid input to the software under test and observing its behavior. This can reveal implementation issues leading to crashes, denial of service or even security issues. Fuzzing is generally applied to software, but can also be used to test the implementation of firmware running on radio chips (e.g. WLAN chips). This is done by sending invalid or incomplete WiFi frames to the device over radio (over-the-air fuzzing). The fuzzer then observes if the device responds normally, returns an error message or crashes entirely, giving it information into possible implementation flaws and protocol adherence.

Objectives

The objective of this project is to build on previous work on over-the-air fuzzing and improve the fuzzer by improving the fuzz test generation and/or improving the fuzzer's introspection into the targeted device. This can be done, respectively, by modifying the fuzzer or installing additional tools on the targeted device.
This includes:

- Literature Review: In-depth examination of the current state of research into over-the-air fuzzing and possible improvements of an existing fuzzer
- Prototyping: Implementation of one of several improvements to the fuzzer
- Evaluation: Evaluation of the performance of the improved fuzzer in comparison to the original
- Documentation: Thoroughly documenting the research process, findings, and strategies employed to navigate and resolve challenges encountered during the study.

The exact scope of the project depends on the thesis type (Bachelor/Master).

Requirements

Candidates should be interested in wireless networking and security analysis in general, and in fuzzing in specific Experience in setting up and using DIY home automation (e.g. Home Assistant) is a benefit.

Application Process

All applications must be submitted through the application website INTERAMT:
https://www.interamt.de/koop/app/trefferliste?partner=339
(Abschlussarbeiten Bachelor / Master)
Carefully note the information provided on the site to avoid any issues with your application.
Your application should include

- a short CV
- a current transcript of records
- the keyword "T3-SC-OTAFUZZ" as a comment

For any questions or further details regarding this thesis and the application process, please feel free to contact ZITiS T3 (t3@zitis.bund.de) or PD Dr. Corinna Schmitt.