Evaluating Privacy Risks from Fingerprinting Network Traffic in IEEE 802.15.4/ZigBee (Bachelor/Master Thesis)

Background

ZigBee is a radio technology based on the IEEE 802.15.4 standard and is widely used in home automation (e.g. in almost all smart lightbulbs). Consistent with other networking technologies, devices are addressed using unique identifiers. Each ZigBee device is permanently and uniquely identified by a 64-bit Extended Address (MAC address) that never changes during its lifetime. However, when a device joins a ZigBee network (e.g. a local home automation system), it is additionally assigned a 16-Bit Short Address, which is unique within the network and used for all communication with that network. Another device in a different ZigBee network may use the same short address, and the address may change during the next join procedure. Beyond static identifiers used for addressing, dynamic properties of device behavior, such as transmission schedules and endpoint activity, can reveal the intended role and operational function of end devices in the network.

Objectives

Detecting ZigBee networks and passively analyzing their wireless data traffic can reveal the what devices are present in home automation network. Furthermore, by injecting fake frames and commands into a ZigBee network, it is possible to force devices to send messages within the current ZigBee network. This allows attackers to learn about devices transmit only infrequently, or even obtain permanent and unique identifiers of ZigBee devices nearby. This thesis aims to evaluate the practical feasibility of passive and active ZigBee network and device fingerprinting attacks in order to assess impacts on user privacy.

Objectives of a possible thesis includes:

- Literature Review: In-depth examination of the current state of research into ZigBee Anonymity/Privacy, Passive/Active Fingerprinting and ZigBee identifiers
- Prototyping: Implementation of an attack prototype that is able to inventory ZigBee devices from active networks using passive and/or active fingerprinting
- Evaluation: Evaluation of the attack's performance with regard to information obtained, effort required, success rate and resulting privacy threat
- 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 focusing on network protocol and security analysis. 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; Pflichtpraktika)
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-ZIGBEE" 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.