Open Thesis / Project

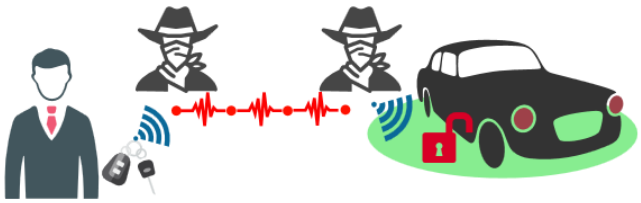
Securing UWB-based IoT Localization Systems

Thesis Type

Master Project / Master Thesis

Motivation

Ultra-wideband (UWB) has become one of the most promising technologies for indoor positioning thanks to its robustness and high time-domain resolution. Big players such as Apple and Samsung have started to include UWB radios into their smartphones, whilst car manufacturers such as BMW, Volkswagen, and Tesla will soon rely on this radio technology to enable **secure access** to their vehicles. The range of UWB-based applications is not limited to mobile and automotive systems, but extends to asset tracking, building control, factory automation, and other location-aware IoT use cases. The next generation UWB devices are finally offering *secure physical layer extensions* to prevent malicious entities from manipulating the distance and position estimation process, which is indeed an important requirement in safety-critical applications. A not yet investigated problem is how to exchange keys and how to coordinate secure distance estimation when these secure physical layer extensions are enabled. In this project, you will get familiar with these topics and investigate how to incorporate the UWB security physical layer extensions into modern and state-of-the-art IoT localization systems.



Goals and Tasks

Within this context, the student can explore several directions and perform different tasks, such as:

- Get to know UWB systems and their security features for secure key exchange;
- Get familiar with state-of-the-art UWB based localization systems;
- Explore the design of protocols for the exchange of security tokens in scalable UWB-based localization systems. The exploration can also consider the use of other out-of-band technologies (e.g., BLE v5.2);
- Build a demonstrator where several low-power devices perform secure localization.

Target Group

- Students of ICE/Telematics;
- Students of Computer Science;
- Students of Electrical Engineering.

Required Prior Knowledge

- Knowledge of networked embedded systems;
- Excellent C programming skills;
- Experience with embedded platforms is a plus;
- Background on computer systems security.

Contact Person

- DI Michael Stocker
  michael.stocker@tugraz.at
- Assoc. Prof. Carlo Alberto Boano
  cboano@tugraz.at

Institute for Technical Informatics
Networked Embedded Systems Group