Open Thesis / Project

Using UWB Channel Impulse Responses as Physical Unclonable Function

Thesis Type

Master Project / Master Thesis

Motivation

Conventional embedded devices rely on hardware security modules for security-related operations. However, such security modules can be expensive and might not be suitable for constrained Internet of Things (IoT) devices. Modern research focuses on novel physical unclonable functions (PUFs), which have gained a lot of prominence in the last couple of years. PUFs rely only on the already integrated physical features of the targeted device and are designed to be nearly impossible to replicate or clone, making them ideal for security operations such as key generation or authentication.

Our aim is to explore the potential of PUFs in conjunction with low-power wireless communication technologies, in particular with systems based on ultra-wideband (UWB) radio. UWB has become increasingly popular thanks to its high time-domain resolution and multipath resilience, which allows to estimate the distance between two devices with centimetre-level accuracy. Among others, UWB radios allow direct access to the estimated channel impulse response (CIR) with sub-nanoseconds resolution. The CIR contains information about the propagation paths taken by the signal transmitted by a device. In the presence of static devices and stationary environments, we hypothesize that the information contained in a CIR should be sufficiently unique and unclonable among different pairs of UWB transmitters. The goal of this work is to verify this hypothesis and to experimentally prove (i) whether the CIR estimated by off-the-shelf UWB devices can be used as PUF and (ii) whether it can provide sufficient security for real-world IoT applications.

Goals and Tasks

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

- Gain an understanding of PUFs and how they can be used with wireless and constrained embedded devices;
- Explore the characteristics of UWB CIRs and investigate their suitability as PUF;
- Develop a model for extracting a unique PUF from off-the-shelf UWB radios and evaluate its effectiveness;
- Evaluate the use of the UWB CIR for PUF use cases in relation to the achieved security strength and performance requirements.

Target Group

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

Required Prior Knowledge

- Basic knowledge of wireless communication;
- Basic knowledge of signal analysis;
- Experience with embedded systems;
- Understanding of basic security concepts.

Contact Person

- Dipl.-Ing. Fikret Basic
  basic@tugraz.at
- Assoc.Prof. Carlo Alberto Boano
  cboano@tugraz.at