Master Thesis: Design and implementation of TLS v1.3 suited for embedded devices

Motivation
- SSL/TLS is probably the most prominent security internet protocol. With version 1.3, this protocol has been re-designed to enhance security, but many libraries still do not support this version. TLS also plays an important role in securing the internet of things which is based on embedded devices. Analogously, many embedded devices still do not use TLS v1.3.

Goals
- The goal of this master thesis is to design and implement a TLS v1.3 library suited for embedded devices. This can be achieved by adapting an existing library. First experiments to integrate post-quantum algorithms into TLS v1.3 are desired but not necessary. The thesis is conducted at MTG AG, located in Darmstadt. MTG AG is among the leading experts in sophisticated encryption technologies in Germany.

Tasks
- Specification of evaluation criteria and evaluation of existent libraries [e.g. mbedTLS, fleATLS, BearSSL, wolfSSL]
- Design of the software.
- Implementation of the designed software in a language suited for embedded devices [e.g. C, Rust].

Prerequisites
- Good knowledge in IT-security and cryptography.
- Good knowledge of Software-Design.
- Very good knowledge of C and/or Rust.
- Thesis language can be English or German.

Literature

Start:
- Right away or by arrangement

The Cyber Security Research Group’s work includes security and privacy in IT systems and IoT settings, long-term security, and offensive security. The Group is affiliated with ATHENE, the National Research Center for Applied Cybersecurity.

MTG AG, located in Darmstadt, is among the leading experts in sophisticated encryption technologies in Germany.

Interested?
Please contact us via email or personally.

Contact
alexander.wiesmaier@h-da.de
ekaratsiolis@mtg.de

Website
https://fbi.h-da.de/personen/alexander-wiesmaier/
https://www.mtg.de/en/start/