The Institute of reliable Embedded Systems and Communication Electronics (ivESK) proposes a

Thesis

Implementation of a CANsec demonstrator for layer 2 protected CAN-based

The ivESK currently works on projects in the field of Controller-Area-Network (CAN) based communication. As vehicles evolve toward higher levels of automation and connectivity, in-vehicle communication networks are increasingly exposed to cybersecurity threats. Originally, CAN networks, while highly reliable and efficient, were not designed with security in mind. However, with the rise of different kinds of attacks in the recent years, novel security measures must be implemented to secure CAN-based communications.

The upcoming CAN XL bus brings higher data rates and extended payloads, opening new possibilities for advanced applications but also further increasing the attack surface. To address these risks, CANsec, a security layer inspired by the Ethernet MACsec standard (IEEE802.1AE), has been proposed to provide data integrity, authenticity, and optional confidentiality for CAN communications.

Implementing and evaluating CANsec on real CAN XL hardware is essential to validate its feasibility and assess its performance in automotive contexts. A working demonstrator, with communicating nodes and CANsec protected traffic, is therefore needed and would serve as an important step toward secure-by-design in-vehicle networks. The demonstrator also enables future performance and latency studies and provide a reference for future standardization and industry adoption.

This project includes the following tasks:

- Familiarize with MACsec to understand its architecture(control and data plane),
- concepts (CA, SA, SC, SecY, KaY) and protection mechanisms (ciphersuites).
- Identify and evaluate open-source MACsec implementations adaptable to bus-based communication model such as CAN.
- Implement CANsec.
- Validate the CANsec implementation with Network analysis tools.

The project requires good programming skills in C (or C++), ideally an understanding of CAN communication principles, first experience with real-time operating systems (RTOS) and familiarity with network security principles.

This task fosters skills in programming, secure networking and software design. Furthermore, it teaches the usage of standard security protocols and their implementation in open source frameworks.

Institute of Reliable Embedded Systems and Communication Electronics (ivESK)
Offenburg University of Applied Sciences

Prof. Dr.-Ing. Ing. Axel Sikora
Dipl.-Ing. Dipl. Wirt.-Ing.
Scientific Director

axel.sikora@hs-offenburg.de
+49 (0)781 / 205 416