Lightweight Application Layer Protection for Embedded Devices with a Safe Programming Language

Martin Andreas Disch

Master thesis in Computer Science

Securing communication in IoT devices is very important, but also difficult due to constraints in connectivity, processing power, memory size and energy usage. Several lightweight protocols have been developed for this context, among them the EDHOC key exchange and OSCORE, which provides application-layer protection of the commonly used CoAP protocol. These protocols are relatively new and few implementations exist. We implemented an open source library for OSCORE using EDHOC, targeted at embedded devices and written in Rust. This programming language is known for its memory safety, a useful guarantee in security-critical environments. The implementation was demonstrated in a test setup using real hardware, consisting of an embedded resource server, embedded client and a CoAP proxy in between. With this approach we have demonstrated the viability for embedded devices of both the proposed protocols, as well as the Rust programming language, and contributed the first Rust implementations of EDHOC and OSCORE.

Prof. Jacques Pasquier-Rocha