PhD Student: Rikard Höglund, RISE Cybersecurity, Kista Stockholm <rikard.hoglund@ri.se>
Main Supervisor: Shahid Raza, RISE Cybersecurity

Title: Lightweight and robust end-to-end security solutions for the IoT

Abstract:
Many IoT devices are constrained in terms of energy, bandwidth, or computing resources. IoT devices frequently employ intermediary device such as proxy servers in their network topology. The focus of this work is designing, developing, and evaluating a comprehensive solutions toolbox to provide methods for secure communication targeting IoT devices. Considered solutions cover secure communication end-to-end, also for group environments, which should be lightweight and feasible for use in resource-constrained devices. These solutions will cover both actual message exchange, as well as administrative aspects such key management and access control. Furthermore, scenarios involving (untrusted) intermediaries and non-conventional communication patterns will be explored. One target of this work is application scenarios involving IoT devices organized into groups, where they engage in one-to-many communications. Special focus will be on the CoAP (Constrained Application Protocol) protocol which is widely deployed in IoT scenarios, including security protocols building on CoAP such as OSCORE, Group OSCORE, ACE and EDHOC. Lastly, some of these activities are input to standardization activities in the IETF (Internet Engineering Task Force).