Rikard Höglund
RISE Research Institutes of Sweden / Uppsala University

End-to-end, lightweight and robust security solutions for the low-power IoT

My name is Rikard Höglund, working at RISE Research Institutes of Sweden, and I am enrolled as a PhD student at Uppsala University at the Department of Information Technology, Division of Computer Systems. I formally started as a PhD student during March this year, the thesis title "End-to-end, lightweight and robust security solutions for the low-power IoT".

The focus of my PhD project is designing, developing and evaluating a comprehensive solutions toolbox to provide methods for secure communication targeting IoT devices. In this respect, considered solutions will cover secure communication end-to-end, also for group environments, will aim to be lightweight and feasible for resource-constrained devices, as well as robust against network attacks. In particular, they will cover both actual message exchange, as well as administrative aspects such key management and access control. Special focus will be on the CoAP protocol which is widely deployed in IoT scenarios, including security protocols building on CoAP such as OSCORE, Group OSCORE and EDHOC.

Some available building blocks could be eligible as a starting point to build on. However, most require significant further design work to achieve satisfactory functionalities and performance. In particular, advanced scenarios involving intermediaries and non-conventional communication patterns have not been properly explored and addressed. Furthermore, design space is open in application scenarios involving IoT devices organized into groups, where they engage in one-to-many communications. In fact, it is especially challenging to design solutions that are not only secure and correct, but that also remain efficient and scalable with the number of communicating devices. At the same time, other aspects such as enabling advanced performance optimizations are also left open to research, in terms of design, feasibility assessment and evaluation.

During this first year of my PhD, specific topics I will work on include the existing challenges of secure (group) communication, (group) key management and robustness against network attacks. In addition to this, one area I will explore further is how to provide efficient and secure rekeying solutions for secure communications protocols for the IoT such as OSCORE. The performance of protocols for secure group communication, such as Group OSCORE, will also be considered. For the OSCORE protocol, certain limits must be considered as to how many times a certain key is used for encryption or failed decryptions. If these limits are exceeded, further use of the keys can allow breaking the security properties of the algorithms.

One particular topic I am focusing on now is providing robustness against denial-of-service attacks to constrained IoT devices. In IoT scenarios where devices are often constrained in terms of resources and power, DoS attacks can be particularly effective. It relies on a reactive, adaptive and host-based approach that takes as input information about ongoing attacks from communication layers like DTLS. By understanding when an attack is in progress including its severity, the victim device can react by trading service availability and quality of service for attack exposure. Under severe attack conditions, this can involve an intermediary device holding and relaying messages, and the usage of low-power modes of operation to limit the impact on energy consumption.