Thesis title: Efficient redistribution of cryptographic group keys in the Internet of Things

Thesis description

Multicast group communication is typically secured by means of one cryptographic group key, commonly shared among all group members. It is vital to efficiently renew and re-distribute the group key if it gets compromised, as well as upon joining and leaving of group members. The goal of the project is to implement and evaluate an already well-defined security protocol defined at SICS, aimed at efficiently revoking and re-distributing a cryptographic group key. The implementation will be done on real IoT devices, taking into account their constraint nature.

SICS will provide background information, necessary guidance during the course of the thesis, and the hardware for evaluation (for example the ones shown in the picture below). The tasks of the Masters student for this thesis are:

- Study the novel IoT technologies and the considered group key management protocol.
- Learn to program the selected embedded system platform with the Contiki OS.
- Implement and experimentally evaluate the key management protocol on IoT devices. Performance analysis will include evaluation of memory usage, communication overhead, and energy consumption.
- Document the activities and results as a thesis report.

Competence

We are looking for a bright MSc student who has fulfilled the course requirements. Good C programming skills are required, as is good spoken and written English. Experience with network and communication security is a plus.

Applications should include a brief personal statement, CV, and a list of grades. In the application, make sure to mention previous activities or other projects that you consider relevant for the position. Candidates are encouraged to send in their application as soon as possible. Suitable applicants will be interviewed as applications are received.

Start time: As soon as possible
Location: SICS Swedish ICT AB, Kista, Stockholm

About SICS

SICS Swedish ICT is a leading research institute for applied information and communication technology in Sweden. SICS is a part of Swedish ICT Research AB, a non-profit research organization owned by the Swedish government and industry. SICS’ mission is to contribute to the competitive strength of Swedish industry by conducting advanced and focused research in strategic areas of computer science, and actively promote the uptake of new research ideas and results in industry and society at large. SICS is an active participant in collaborative national, European, and other international R&D programs.

Contact person
Dr. Marco Tiloca, SICS Swedish ICT AB, Security Lab (marco@sics.se)
Dr. Shahid Raza, SICS Swedish ICT AB, NES Lab (shahid@sics.se)
Electrum Building, Isafjordsgatan 22, SE-164 40 Kista, Stockholm