Certificate-based Security for the Internet of Things

Master Thesis project at RISE SICS, Kista.

Description of the units
This work will be carried out in the Networked Embedded Systems (NES) group at RISE SICS in collaboration with the RISE SICS Security Lab. Our current research focus is on the Internet of Things and cyber security. Among the group's key technologies are the Contiki operating system, uIP stack , ContikiRPL, SICSLoWPAN and lightweight implementations of IPsec and DTLS. We conducts projects together with industry and academic partners from Sweden and across the world.

Thesis description
In order to provide modern security solutions also for resource-constrained devices that lack traditional input such as
keyboards, new lightweight public key infrastructure solutions for the internet of things are being proposed. Still, several issues regarding certificate management remain to be solved. It is therefore needed to investigate how existing PKI standards and proposed IoT security standards best can be used to provision certificate based solutions for IoT devices.

The security architecture on the Internet, with root Certificate Authorities (CAs) and chains of delegation needs to be adapted to the constraints of IoT. This thesis will propose a chain of trust for certificate provisioning and management for IoT devices, using existing standards wherever possible. Tasks include determining which actions should best be done by cloud or edge devices.

SICS will provide both background information and a certain amount of code libraries.

The tasks of the Masters student
for this thesis are:

- Study state-of-the-art PKI technologies and protocols
- Study related proposed IoT security standards
- Learn to program a selected embedded systems platform with the Contiki OS.
- Study state-of-the-art PKI policies, procedures, responsibilities and relationships, and investigate their feasibility in resource-constrained IoT
- Specify and implement certificate management components, and evaluate them by comparing with an existing X.509-based solution in an IoT testbed
- Document the results as a thesis document.

Competence
We are looking for a bright MSc student with background and demonstrated interest in cyber security and who has fulfilled the course requirements. Good programming skills are required, as is good spoken and written English.
Applications should include a brief personal letter, CV , and recent grades . 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?

Please contact
Dr. Shahid Raza
E-mail: shahid.raza@ri.se

Joel Höglund
E-mail: joel.hoglund@ri.se

RISE SICS
Electrum Building, Isafjordsgatan 22SE-164 40 Kista, Stockholm

ID: 1575