www.sics.se

Thesis Title: *Software and Firmware Updates for Internet of Things*

Description of the units:

The Security Lab group at RISE SICS is among the largest cybersecurity research groups in Sweden. The current research focus is on IoT security, cloud security, software security, formal methods, cryptography, standardization, privacy (technical and social aspects), and virtualization. Currently, the lab is involved in 15 research projects, funded by EU H2020, VINNOVA, Eurostars, Celtic-Plus, ECSEL, EIT, SSF, VR, and Swedish industry.

Thesis description:

The state-of-the-art in present IoT deployments is still no security or fixed security based on static PINS and password. Our current and previous research focus on new communication security protocols and intrusion detection systems for IoT. These works have already enhanced the IoT security state-of-the-art and made it practical for low-end devices. However, current solutions rely on symmetric cryptography that has no support for digital signatures, hence there are no practical solutions for software or firmware updates (to patch vulnerabilities). For sustainable security in IoT, software updates are inevitable. In our recent work, we have already shown the feasibility for asymmetric cryptography for IoT, which support full certificate-based digital signatures. [Ref: VINNOVA CEBOT and Eurostars SecureIoT projects].

This thesis will define novel lightweight ways for software/firmware updates for IoT. It is important that these mechanisms are interoperable across different IoT providers. IETF has started a working group for the standardization of software updates for IoT, which relies on public key cryptography (PKI) and is a natural fit for our ongoing PKI work. This thesis is expected to exploit (i) our current work on asymmetric cryptography for IoT and (ii) the current proposals in the IETF SUIT working group and design, implement, and evaluate lightweight software and firmware updates for battery powered-IoT devices.

RISE SICS will provide both background information and a certain amount of code libraries. The tasks of the master's student for this thesis are:

- Study state-of-the-art IoT protocol and existing software updates proposals for IoT
- Study our current asymmetric security solutions for the IoT
- Learn to program a selected embedded systems platform with the Contiki-NG OS.
- Specify and Implement lightweight end-to-end secured protocols for software updates and evaluate them in an IoT testbed
- Document the results as a thesis document.

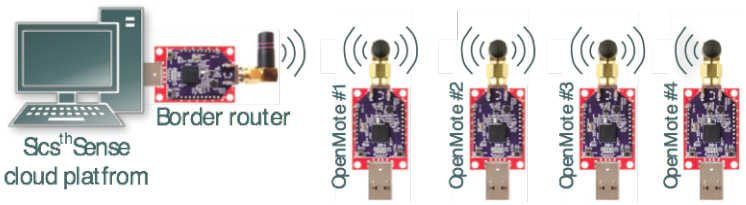
Competence:

We are looking for a bright MSc student with a background interest in cyber security and who has fulfilled the course requirements. Good C 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

City: RISE SICS Kista, Stockholm



Contact person:

Dr. Shahid Raza
Director Security Lab & RISE SICS
E-mail: shahid.raza@ri.se

Joakim Ericsson