Master thesis project (30hp) Linköping University / Ericsson Research

Contact: Prof. Christoph Kessler, LiU; Prof. Ben Smeets, Ericsson Research, Lund

Performance optimization of security functions in IoT devices

The vision of having billions of devices that will improve our personal life and the functioning of business and society in general can only be realized when these devices can operate and be managed in a trustworthy manner. Although the understanding of the importance of this is not really materialized in all IoT (*Internet of Things*) technologies, we see that already today certain commercial products for IoT, such as *wirelesshart* and *Zigbee*, have security features. Also in standardization the importance of security is recognized, and improved standards for IoT are being developed, such as object security in IETF instead of TLS. Discussions around the design of security functions for IoT circle much around making them more fit for the constrained usage conditions of IoT, typically being power consumption and size of required hardware. Optimizations take place by looking at very specific security functions, e.g. secure communication protocol or a signature scheme, and trying to optimize this. In practice these security functions are only one part of the application of the service the IoT device has to deliver. It would be more natural to aim for a more global optimization so that, for example, the total power consumption is kept small for the entire service. However developers may not have the means to perform such an optimization. Specifically, developers lack tools and methodology to optimize the power consumption of their application on the device. While this is true in general, it is also specifically valid when it comes to choices of security functions that work optimally together with the application.

This master thesis project will, in close cooperation with Ericsson Research in Lund, investigate how we can develop a framework for developers to implement applications that optimally use the available security functions to perform their task, by suitable coordination (e.g., software caching, adaptation of buffering scheme, degree of parallelism, resource management) at the application/library/OS level, also taking possible trade-offs between power usage and quality of service into consideration (e.g., by adapting encryption levels). Here we primarily investigate power consumption and execution time.

[x] Wirelesshart Security, http://en.hartcomm.org/hcp/tech/wihart/wihart_security.html

[x] Zigbee, http://www.zigbee.org/zigbee-for-developers/applicationstandards/zigbeehomeautomation/

[1] G. Selander *et al*., Object Security of CoAP (OSCOAP), draft-selander-ace-object-security-04, March 2016, IETF. https://datatracker.ietf.org/doc/draft-selander-ace-object-security/

[2] Bootstrapping Security: The Key to Internet of Things Access Authentication and Data Integrity. Ericsson White Paper 284 23-3284 Uen, February 2016. https://www.ericsson.com/res/docs/whitepapers/wp-iot-security.pdf