Corporate Research Norway is offering the following Master Thesis

Performance evaluation of customized opensource SSL/TLS solutions in resource constrained environment

Recently, embedded systems (ES) have advanced considerably in terms of processing capabilities, memory support~~s~~, operating system capabilities and tools support. However, until now, relevant systems mostly contain legacy ESs for which resource constraints limit the adoption of advanced applications such as enhancements for cyber security. It is both expensive and time consuming to replace hardware from the legacy ESs with hardware that has been enhanced with advanced capabilities (processing power, memory etc…). As a first step to integrate advanced security functionalities within the legacy embedded systems, one needs to investigate the performance of the available solutions in a resource constrained environment. In this context, this research would target open-source SSL/TLS solutions. Often in order to fit these solutions into such an environment, it is required to look for a custom-made solution as well. In this thesis, the targeted open-source candidates for providing SSL/TLS are openSSL, GnuTLS, PolarSSL, SharkSSL, nanoSSL-mocana. The research will most likely use Linux-based source code and target ARM-based hardware settings.

The thesis will start with a comprehensive study of the SSL/TLS protocol and algorithm in terms of message exchanges during session establishment, key generation processes and optional and mandatory parts of the algorithm. The capabilities of the open-source solutions for SSL/TLS will be briefly studied and most of the time will be spent on testing the performance of these solutions in a real hardware setting. Before starting the performance evaluation, one should also study the hardware platform to be used. It is expected that the performance measurement would allow us to choose the best possible candidate/candidates and the reasons such choice. In the investigations of the performance of SSL/TLS, we are looking for the following answers:

- How do the solutions perform with encryption and without encryption (e.g., authentication and integrity protection only)?

- How long it takes to establish a session?

- How do the solutions perform if we increase the size of the keys?

- How do the solutions perform for different cipher suites (a representative selection of cipher suites should be used)?

- Analysis of flexibility/usability of library: How modular is the candidate library? Is it easy to manage which parts are needed and use only these?

- Which one is the best candidate compared with the size of the solution and above performance criteria?

Requirements:

- Relevant knowledge on Security (e.g. SSL/TLS protocol)
- Good knowledge on C++ programming language
- Knowledge on Linux OS

Interested and competent students are asked to send in CV with necessary competence details as soon as possible to:

Judith Rossebø, Judith.rossebo@no.abb.com

Mohammad Mushfiqur Rahman Chowdhury, mohammad.chowdhury@no.abb.com