Champion TLS Library for Isolated Enclaves

A security evaluation for cloud orchestration platforms.
Master Thesis project at the Security Lab of RISE SICS in Kista or Lund.

Background
Cloud orchestration is steadily gaining importance along with the increase in the complexity of systems deployed in cloud environments. The complexity of deployed systems has in many cases passed well beyond the comprehension of human operators. This carries the risk of introducing misconfigurations leading to security vulnerabilities and potentially affecting system availability. The currently available cloud orchestration platforms focus on supporting scalable system deployment over an easy operator interface using either declarative or imperative commands. However such cloud orchestration platforms provide only limited and often inadequate security features when it comes to protecting the configuration of deployed systems verifying target cloud resources or protecting tenant authentication credentials.

Objectives
Within the framework of the COLA project the Security Lab at RISE SICS is working on developing a secure and robust cloud orchestration platform. One way to achieve this is by placing authentication credentials in trusted execution environments (TEE and attesting their integrity before provisioning security-sensitive data. TEEs with strong security guarantees can be built using Software Guard Extensions (SGX – a set of recently introduced extensions to the x86 instruction set architecture and related hardware. The current effort aims to make a performance comparison of several TLS libraries that currently support for Intel SGX.

Briefly the thesis consists of the following items:
1. Identify TLS libraries that support Intel SGX.
2. Identify a comprehensive set of relevant tests to evaluate TLS performance in SGX enclaves.
3. Implement a TLS benchmark using the TLS libraries that support Intel SGX.
4. Analyse the performance evaluation and the performance trade-offs.
5. Provide a written report on the findings.

Implementation will be carried out on x86 platforms provided by RISE SICS. The SGX enclaves will be based on original Intel hardware. The master project will be carried out at RISE SICS and will be supervised by researchers at RISE SICS.

Competence
We are looking for one or two bright MSc students in Kista or Lund who meet the following requirements:
1. Knowledge in C (advanced skills are a bonus)
2. Interest in performance evaluation
3. Interest in isolated execution environments
4. Good spoken and written English

Applications
Applications should include a brief personal letter your CV with your education professional experience and specific skills and recent grades. In your application make sure to give examples of previous programming or other projects that you consider relevant for the position. Candidates are encouraged to send in their application as soon as possible in paper form or via eK mail. Suitable applicants will be interviewed as applications are received.

Contact
Nicolae Paladi | nicolae.paladi@ri.se | PGP 0xE2616E7D
Security Lab
RISE SICS

1 http://projectKcola.eu/