Deconstructing Open vSwitch for Isolated Enclaves

An enabler for secure cloud orchestration platforms.
Master thesis project at the Security Lab of RISE SICS.

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 and networks verifying target cloud resources or protecting authentication credentials.

Objectives
Within the framework of the COLA project the Security Lab at RISE SICS is working on creating secure cloud orchestration platforms that are capable of implementing security and isolation in cloud network infrastructure. One way to achieve this is by confining select SDN components to 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 port core functionality of a popular virtual switch implementation – Open vSwitch – in an SGX enclave supporting isolated execution.

The thesis consists of the following items:

1. Analyse the architecture of Open vSwitch and identify security sensitive components which can be ported to one or more SGX enclaves.
2. Describe a detailed implementation design suggestion.
3. Implement the chosen system design approach and evaluate it from a security and performance points of views.
4. Provide a written report on the findings.

Implementation will be carried out on x86 platforms. The TEE will be based on either original Intel hardware or emulation software. The master project will be done at RISE SICS and will be supervised by researchers at RISE SICS.

A successful project can lead to
• a valuable open-source contribution
• a peer-reviewed publication presented at a prestigious conference or workshop.

Competence
We are looking for one or two ambitious 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 eM mail. Suitable applicants will be interviewed as applications are received.

Please contact
Nicolae Paladi | nicolae.paladi@ri.se | PGP

1 http://www.cola-project.eu/