Bootstrapping trust

Linus Karlsson[1,2]
[1]Lund University, [2]RISE SICS

Joint work with:
Nicolae Paladi

May 10, 2017

The network infrastructure for 5G networks will be shared among many tenants. To facilitate such an environment, Software Defined Networking (SDN) is a key concept. In the center of all action is the SDN controller, which manages the network. This controller communicates with other parts of the network, such as virtual switches and Virtual Network Functions (VNFs).

A malicious or compromised node in the network may, through its communication with the central network controller, affect the behaviour of the complete network. It is therefore of great importance to ensure the integrity of the entities that is part of the network infrastructure.

We utilise trusted computing techniques to ensure the integrity of components taking part in the SDN topology. More specifically, we utilise Intel SGX to provide remote attestation and isolation. This ensures that the controller can attest the integrity of VNFs before including them in the network, so that compromised or malicious entities can be detected. We also discuss how this can be achieved if the VNFs are executed in a virtualized environment.

In addition to this, we discuss how to setup an integrity and confidentiality protected connection between the VNFs and the network controller. This requires key distribution and management, and we utilise the isolation properties of Intel SGX to minimise the risk for key leakage.