Security and trust in a Network Functions Virtualisation Infrastructure

Marco De Benedictis

Modern digital infrastructures are undergoing a significant evolution thanks to the advantages offered by virtualisation techniques in terms of flexibility, scalability and the overall reduction of hardware-related costs. More specifically, the Cloud computing paradigm foreshadows large scale virtualisation as a viable technology to manage on-demand allocation and distributed deployment of computing resources in a dynamic environment. More recently, virtualisation has gained momentum in the networking domain as well, where network operators are exploring technologies to enhance the flexibility of their infrastructure and to reduce the overall provisioning, maintenance and upgrade costs associated to traditional appliances. In this regard, the latest trend concerns the implementation of networking functions (i.e. routers, switches, Network Address Translation boxes) in softwarised instances that run on top of commodity hardware in a data-center. This aims to achieve a higher degree of scalability of network functions when compared to traditional hardware-based infrastructures, wherein each topology change and service deployment typically imply a physical manipulation at the appliance level. Moreover, the operators are interested in reducing the vendor lock-in, which often leads to substantial upgrade and maintenance costs.

From a security perspective, virtualisation exposes network infrastructures to different families of threats. In particular, software modules may include vulnerabilities that can be exploited remotely, compromising both the network itself and its clients' privacy, both at virtualisation and networking level. Additionally, the softwarisation of the network makes it more prone to software bugs introduced by the developers. Given the privacy sensitive nature of public networks, security and trustworthiness of the platform are considered paramount. Because of this, network virtualisation should be supported by appropriate means to ensure that the software domain is protected against manipulations and that an attack can be detected by the monitoring systems.

In this thesis, we propose a platform to assess the trustworthiness of a softwarised network infrastructure. This offers a generic approach to integrity verification so that heterogeneous virtualisation platforms can be protected. This is particularly relevant in today's cloud infrastructures, that adopt different virtualisation strategies ranging from traditional virtual machines to more light-weight forms of virtualisation (i.e. containers). In the proposed approach, adherence to existing standards on network softwarisation and hardware plat-

form trust is considered paramount to ensure market readiness of the solution, and ease its application by existing frameworks. We have developed the system within the SHIELD Horizon 2020 project, that aimed to the definition of a secure platform based on an interplay of network softwarisation, trusted computing, and artificial intelligence to both support the deployment of networking functions in a operator network and to monitor their life-cycle against external attacks or malfunctions. Compared to existing approaches, the system offers a generic approach to network integrity verification, making it applicable to heterogeneous hardware platforms. Moreover, it targets elements acting both at the physical and virtual level to protect the entire cloud software stack. This work addresses the current limitations in the state of the art in the field of security and trust of a virtualised network infrastructures with the following contributions: (1) a trust architecture tailored for a highly-virtualised environment that targets both the physical and the virtual domains of execution; (2) an integrity verification technique that enables run-time attestation of lightweight virtualised instances against manipulation by external attackers; (3) a monitoring process that enhances the threat response capabilities in a softwarised network infrastructure by integrating the previous contributions in a cloud practical scenario.