On the establishment of trust in the cloud-based ETSI NFV framework

Marco De Benedictis
Politecnico di Torino
Dip. Automatica e Informatica
Torino, Italy
Email: marco.debenedictis@polito.it

Antonio Lioy
Politecnico di Torino
Dip. Automatica e Informatica
Torino, Italy
Email: antonio.lioy@polito.it

***Abstract*—This paper discusses the open issues in incorporating trust techniques in the NFV environment specified by the ETSI NFV Industry Specification Group, and analyses the available technologies to fill this gap. ETSI is developing security and trust specifications within its NFV-SEC working group, with the aim of establishing and assessing trust of both the hardware platform and the virtualised infrastructure hosting the Virtual Network Functions. Cloud computing, envisioned by ETSI as enabling technology for the deployment of the NFV infrastructure, represents a challenging environment for the establishment of trust. Open issues in this area include applicability of hardware-based trust assessment to a virtualised infrastructure, and integrity and privacy of virtual instances hosted on a multi-tenant platform. This paper discusses the challenges in applying one specific technology, Trusted Computing, to a NFV cloud-based architecture and proposes a concrete solution (based on the Intel OpenCIT framework) to address each issue. Moreover, a mapping between the ETSI NFV security and trust guidance and the OpenCIT capabilities is proposed. Finally, applicability of the solution to the NFV Management and Network Orchestration stack is discussed, with particular attention to the reference implementation promoted by the ETSI-hosted initiative Open Source MANO.**

I. Introduction

Today's ICT infrastructures are evolving towards virtualisation technologies to reduce the costs of hardware installation and maintenance, as well as to meet the ever increasing demands of flexibility and scalability for their services. Cloud computing is one of the most relevant paradigms for large scale virtualisation. It envisions several service models to abstract deployment of applications, often distributed geographically, from the underlying hardware through virtualisation techniques. Virtualisation is not only a key enabling technology for cloud-based deployments but it has recently gained momentum in networking as well, as envisioned by the *Network Function Virtualisation* (NFV) and *Software Defined Networks* (SDN) paradigms.

NFV is a relevant technology for the network of *Internet Service Providers* (ISPs) for several reasons. First of all, it lowers the overall costs for provisioning and maintenance of network appliances by moving the network functions in commodity devices. Second, it allows flexible placement and optimisation of *Virtual Network Functions* (VNFs) in the infrastructure depending on the demand at a certain point in time.

Substantial efforts in NFV standardisation have been carried out by the ETSI NFV *Industry Specification Group* (ISG). Its activities, started on November 2012, are divided among several working groups specialised on specific aspects of the environment, such as the infrastructure, interfaces, reliability, and security. The NFV-SEC working group focuses on establishing trust and security in the *NFV Infrastructure* (NFVI). The latest release of the specifications at the time of this writing, resulting from a two-year phase release management process, is named Release 2 and it is considered as reference version for this paper.

The available NFV-SEC specifications cover several aspects, such as definition of the problem statement, use cases to be addressed, and regulatory concerns with privacy and lawful interception. A security and trust guidance [1] is also available, which briefly presents different methodologies for establishing trust in the NFVI. Additional specifications for the execution of sensitive NFV components have been provided [2], focusing on both the hardware and software requirements for implementation of trust-related components, system hardening, and secure logging. Regarding the VNFs capabilities, NFV-SEC presented also the *NFV Security Management* (NSM) framework [3] to monitor and automate virtualised security functions in the infrastructure, as an addition to the intrinsic capabilities of the network services to be deployed. Specifications provide a set of recommendations on the use of and enhancements to OpenStack as pertinent to NFV [4], given the interplay between NFV and the cloud deployment model, for whom OpenStack is one of the most popular and widely used technologies.

Among the aforementioned standards, the NFV-SEC working group has put significant effort in proposing *Trusted Computing* (TC) technologies, as defined by the *Trusted Computing Group* (TCG), to protect the integrity of sensitive components in the NFV environment. A fundamental principle of TC is the *Chain of Trust*, an extension process that ensures trustworthiness of a computing system by transitive measurements. This methodology requires the introduction of an implicitly trusted entity, comprising a minimal combination of both hardware and software, that is called *Core Root of Trust for Measurements* (CRTM). Starting from it, each software component extended in the Chain of Trust is responsible of

measuring and storing the integrity value of the next element. The establishment of the CRTM requires a dedicated hardware chip, called *Trusted Platform Module* (TPM) [5]. This module, standardised by the TCG, stores the integrity measurements in specific protected *Platform Configuration Registers* (PCRs), that can be written only by the TPM. Integrity evidence is provided by listing the PCRs values digitally signed with an *Attestation Identity Key* (AIK), generated by the TPM itself. *Remote Attestation* (RA) is a specific work-flow defined by TCG that allows a *Trusted Third Party* (TTP) to remotely verify the integrity of a computing system, by checking the measurements stored in the PCRs against a white-list of known-good values. Different frameworks have been proposed for establishing trust in a distributed environment by exploiting a RA-based work-flow, the latest one being Intel *Open Cloud Integrity Technology* (OpenCIT) [6].

The paper discusses the challenges in managing trust in the ETSI NFV framework, and focuses on the open issues in trusting a virtualised environment. Moreover, we propose the OpenCIT framework as enabling technology for trust in a cloud-based deployment of the NFVI, and analyse its capabilities in respect to the requirements set by the NFV-SEC working group.

The rest of the paper is structured as follows. Section II presents the related work on the topic. In Section III, we present the motivation behind our proposal, highlighting the peculiarities of the NFV scenario with respect to the traditional trust problem for computing systems. Section IV addresses the specific problems to be considered in the design of a solution for trust establishment in the ETSI NFV framework. Section V presents the OpenCIT technology and discusses its integration within the NFV administrative domain. Finally, future work on the proposed solution is presented along with the authors' conclusion in Section VI.

II. Related work

The establishment of trust in the NFV environment, as envisioned by the ETSI NFV ISG, has been already discussed in scientific literature. Jacquin *et al.* [7] have discussed the problem of trust in modern network infrastructures, with respect to both SDN and NFV. The authors propose the inclusion of a TC-compliant verifier in the SDN management infrastructure that could interact with both the SDN controller and the SDN network elements to retrieve their network flow tables and exchange attestation data. The attested elements are equipped with an hardware *Root of Trust* (RoT), such as the TPM, and measure their boot process to enable remote verification. The authors also focus on the applicability of TC methodologies to NFV, proposing the use of *virtual TPM* (vTPM) to address access and resource allocation by multiple *Virtual Machines* (VMs) running in the same host equipped with a physical TPM. Finally, the authors propose Linux *Integrity Measurement Architecture* (IMA) [8] as enabling technology to measure executables and configuration files running in the VMs, whose initial state should be known a priori. Jaeger [9] has presented the architecture of a *Security Orchestrator* for trust management and automated control of deployment and configuration of virtual security functions within the network services in the NFVI. The proposed architecture is suitable for hybrid networks where both physical and virtual network functions are deployed, and it is meant to interact with the NFV *Management and Network Orchestration* (MANO) entities as an external set of components to the standardised NFV ecosystem. The same problem has been discussed by Ravidas *et al.* [10], whose work focuses on incorporating trust in a telecommunication cloud platform by proposing an architecture, comprising a security orchestrator and an attestation server, based on the OpenCIT framework, to be included in the NFV MANO infrastructure. The proposed architecture is meant to bind trust verification and life-cycle management of the computing nodes in the cloud platform. The authors also propose image integrity verification and binding to a specific platform configuration for the VNFs, as crucial to establish trust between the VNF and the NFVI. Yan *et al.* [11] have proposed a framework for security and trust to be applied on 5g networks, for whom the authors consider both SDN and NFV as enabling technologies. A *NFVI Trust Platform* (NFVI-TP) is envisioned for platform layer security, where a *Root Trusted Module* (RTM) is used to ensure trustworthiness of each component built on top of it. The TPM is considered as one specific implementation of the RTM. The NFVI-TP is also in charge of ensuring Quality of Service of VNFs, identifying and authenticating VNFs and monitoring the execution of VNF Forwarding Graph by a third party, such as the NFV Orchestrator.

The solutions proposed in literature lack a direct mapping with the ETSI NFV standardisation work in security and trust and they don't discuss integration with the rest of the NFV ecosystem. Furthermore, the referenced papers do not address NFV deployments based on lightweight virtualisation techniques, such as *Linux Containers* (LXC) and, more recently, Docker [12]. Nevertheless, these technologies may be a valuable alternative to traditional virtualisation for the NFV scenario, because of their lower memory footprint, faster deployment and focus on application-layer processes.

III. Motivation

Trust establishment in the NFV environment is a challenging problem that can't be addressed by the traditional hardware-based attestation scheme envisioned by TCG, because of the peculiar demands in terms of flexibility, scalability and privacy implied by the NFV environment. Cloud computing is referenced as enabling technology for the provisioning of NFV services in the ETSI NFV White Paper [13], because of its advantages in abstracting hardware resources and providing on-demand computational power. Although being more flexible than traditional distributed architectures, the cloud service model heavily relies on virtualisation, which still is a challenging domain for applying TC technologies. Whilst there are technological proposals for attesting traditional VMs, such as the vTPM proposed by the TCG, this work also focuses on more recent virtualisation technologies, such as containers

(e.g. Docker), which are gaining momentum because of their lighter memory footprint and faster deployment time. Although the need for trust in the NFV has been already foreseen by the ETSI ISG, there is still an unresolved gap between specifications and a reference technical solution. This paper aims at filling the gap by proposing a concrete, available technology that enables sustainable Trusted Computing methodologies in a cloud infrastructure and may be integrated with the NFV Management and Network Orchestration architectural framework (MANO). The extension of Trusted Computing techniques to SDN network infrastructure, when exploited for traffic flow control in the NFV environment, is not covered here.

IV. Open issues in security and trust in the NFV

The NFV framework is composed by different sub-systems that run on a virtualised execution environment, namely the *Management and Network Orchestration* (MANO) stack, the NFVI infrastructure, and the VNFs deployed on top of it. The Security and Trust Guidance [1] mentions attestation of the nodes in the NFVI as a key technology to establish trust in the NFV environment. The *Trust Manager* entity is introduced as part of the MANO administrative domain, outside of the NFVI, to implement the trust logic for the framework. This section focuses on the open issues when trusting virtual instances in a cloud-based platform. It also discusses the relationship between trust management and the MANO stack and scalability issues raised by its operations.

A. Attestation of virtual instances in a cloud solution stack

The implementation of Trusted Computing methodologies by the Trust Manager should be assessed because of the extensive use of virtualisation in NFV. Traditional RA procedure requires the attester to have direct access to the TPM device in the host system for *measurement* and *attestation* of the platform, whose result is provided to a remote party in charge of the *verification*.

NFV-SEC introduces *Trustworthy Boot* [1] as a concept for validating boot integrity of the components in the NFVI, inclusive of the hardware platform, firmware, hypervisor, and Operative System. Moreover, the need for a *Hardware-based Root of Trust* (HBRT) [2] in the NFVI is envisioned by the standards as a foundation for the Chain of Trust. Trustworthy Boot specification references *Secure Boot*, *Measured Boot* and Intel *Trusted Boot* as non-exclusive implementation technologies. The first focuses of validating the integrity of the firmware at boot time via digital signatures, acting as a local verification process for each NFVI node. Both Measured Boot, proposed by TCG, and Intel Trusted Boot focus on measurement of the running software at boot time, starting from an hardware RoT, which is implicitly trusted. The measurement log is the evidence that will enable remote verification by a TTP via RA. Trustworthy Boot also lists the architectural layers affected by trust verification during the execution of VNFs, including the hardware platform, hypervisor, virtualisation container, VNF operative system and the VNF application. The standard also specifies that a TTP may require a specific Level of Assurance (LoA) regarding the VNF trust, depending on the security requirements on the infrastructure and on the purpose of such network function.

Attestation of both physical and virtual instances are to be addressed in NFV. In this context, attestation of VNFs is a more relevant topic from the research perspective as it encompasses the challenges into establishing trust for different virtualisation technologies, namely *hardware virtualisation* and, more recently, *OS virtualisation*. Although not being specific on the virtualisation layer solution, NFV-SEC working group foresees the deployment of both VM-based and container-based VNFs [2]. The first, also known as *full virtualisation*, enables the execution of a full guest Operative System (OS) on top of the host OS by emulating the hardware resources of the execution environment. This solution requires the host system to run an hypervisor, whilst the guest OS does not require any modification from a *vanilla* version. Technologies like XEN, KVM, VMWare Server or ESX implement hardware virtualisation.

In case of VM attestation, an alternative to physical TPM has been proposed, consisting of a software implementation of the device, known as vTPM. This technology emulates the capabilities of the physical device (e.g. secure storage, cryptographic operations) with a custom software module, without violating the requirement of an hardware RoT. Each VM is given access to a client TPM driver, which replicates the standard TPM commands. A special VM runs a server TPM driver, which receives commands from the other VMs and forwards them to a manager which has visibility on the physical TPM in the host platform. The NFV-SEC standards refer to vTPM as an alternative to physical device when its use would not be feasible for attestation. However, the vTPM solution introduces the problem of binding the attestation results provided by a VM and its hypervisor, in order to assure that the host platform has actually started the vTPM instances.

In case of OS virtualisation, the virtual instances are named *containers*. Container-based virtualisation does not run a full guest OS inside a host OS, instead it leverages Linux kernel functionalities, namely Control Groups (*cgroups*), *Namespaces*, *copy-on-write storage*, to isolate processes running in each container from the others and from the host system. Differently from VMs, containers are based on the host's kernel (which has to be patched) and their processes are visible on the host machine. Although they provide less isolation than traditional VMs, they have advantages in terms of performance and scalability, both of which are relevant to the NFV environment. Attestation of container-based VNFs is a promising area for further research because of the lack of production-ready solutions that apply to different OS virtualisation technologies.

B. VNF image integrity and confidentiality

The NFV environment may be suited for open innovation scenarios where the infrastructure's maintainer would allow VNF developers to upload their applications to a shared catalogue, to build competition and enhance the platform's

capabilities. Hence, protection mechanisms for the VNFs packages should be applied, as also specified by the ETSI VNF Packaging Specification [14].

The VNF package is defined as a set of files and descriptors that provide the means for validating and instantiating the VNF. Both encryption and digital signature techniques could be applied to the VNF package in order to enable confidentiality, authenticity and data integrity for the VNF images. The use of cryptographic operations implies the need for managing keys in the NFV infrastructure. Such capability should be managed by the platform in an automated way, as to reduce the impact on scalability. This issue is addressed by the NFV-SEC family of standards [2] by introducing a *Key Management System* (KMS) entity for key generation, storage, deletion and cryptographic processing within the framework.

C. Relationship between trust and the MANO stack

The Trust Manager is envisioned as part of the MANO stack, so it should be placed in an administrative area along with the other components implied in the life-cycle management of the NFVI. The traditional cloud deployment platform, representing the underlying infrastructure for NFV, should be extended to support trust monitoring within the life-cycle management of the NFV infrastructure, comprising both the physical computing nodes and the running VNFs. Both NFVI nodes and VNFs should be attested at load time prior joining the infrastructure. This capability would require interaction and possible synchronisation between the Trust Manager and the *VNF Manager*, to prevent deployment of an untrusted instance. It is to be noted that the NFV environment may host several tenants, such as the different clients of a ISP network. Hence, the Trust Manager should be able of providing limited visibility of attestation reports to the other components of the MANO stack depending on the assignment of hosts to specific tenants.

D. Impact on performance and scalability of trust operations

The *measurement* and *attestation* phases of RA are affected by the latency introduced locally by the attester when issuing commands to the TPM. Moreover, the *verification* phase requires a remote verifier to retrieve the attestation data via a secure channel (e.g. TLS) and then to check the validity of these data against a white-list. The latency of this process might not be critical for a traditional client-server scenario with a single attester, but should be carefully investigated when moving to a cloud deployment scenario with several instances (both physical and virtual) to be attested periodically. Work in progress by the NFV-SEC group is tackling different workflows for attestation that should scale better for deployments with large number of VMs on a single compute node, but no public standard is yet available in this regard.

V. Available technologies

In this section, available technologies for providing security and trust in NFV are proposed. More specifically, the applicability of a technology for ensuring privacy and integrity of a cloud platform in the NFV scenario is discussed as follows, as well as its interoperability with the MANO stack.

OpenCIT [6] is a framework proposed and maintained by Intel, that aims at protecting integrity of a virtualised infrastructure managed by a *Cloud Service Provider* (CSP). OpenCIT is tightly bound to the hardware platform of the CSP, as it leverages Intel processors with *Trusted Execution Technology* (TXT) to establish an hardware RoT for the cloud computing nodes. OpenCIT is a successor to the *OpenAttestation* (OAT) project, which implemented the concept of a Remote Attestation framework for assessing the trust of TPM-equipped computing nodes in a cloud infrastructure. In the NFV environment, trust capabilities are tightly coupled with the management and orchestration of the infrastructure. As already discussed, NFV-SEC envisions the addition of a long-lived entity in the MANO administrative domain, namely the Trust Manager, to manage trust related operations and interact with the other components of the MANO stack. *Open Source MANO* (OSM) [15] is an open-source project hosted by ETSI and, therefore, is considered as the reference implementation for the NFV MANO sub-system.

Figure 1 depicts the links between the architectural components of OpenCIT and the high-level domains of the NFV framework [16]. Core components of the OpenCIT framework include:

- Intel-based hardware architecture with TXT enabled on the computing node and physical TPM (both versions 1.2 and 2.0 are supported);
- Trust Agent that enables both RA and the extended chain of trust capabilities on the computing node;
- Attestation Server that performs RA, comparing Intel TXT measurements against a white-list;
- Key Management System that leverages platform trust for distribution of cryptographic keys to encrypt/decrypt virtual images;
- Attestation Reporting Hub that decouples trust assessment and reporting, as performed by the Attestation Server, from any third-party Scheduler Service interested in retrieving trust-related information;
- Trust Director that defines trust policies for verification of hosts and virtual instances and also manages decryption of virtual images to be on-boarded, by interacting directly with the CSP Image Management Service.

The contributions of OpenCIT to the NFV trust establishment and the interoperability with OSM are discussed later in this paper, and are based on the latest version of the frameworks released at the time of writing, namely OpenCIT 3.2.1 and OSM Release Two.

A. Integrity of the NFVI host platform

The OpenCIT chain of trust starts from Intel TXT, the hardware RoT that measures the first code executed in the boot process, which in turn will measure other software transitively. This technology allows measurement of BIOS, SINIT ACM, OS kernel and hypervisor during the boot process, whose digests are stored in the TPM internal registers, the PCRs.

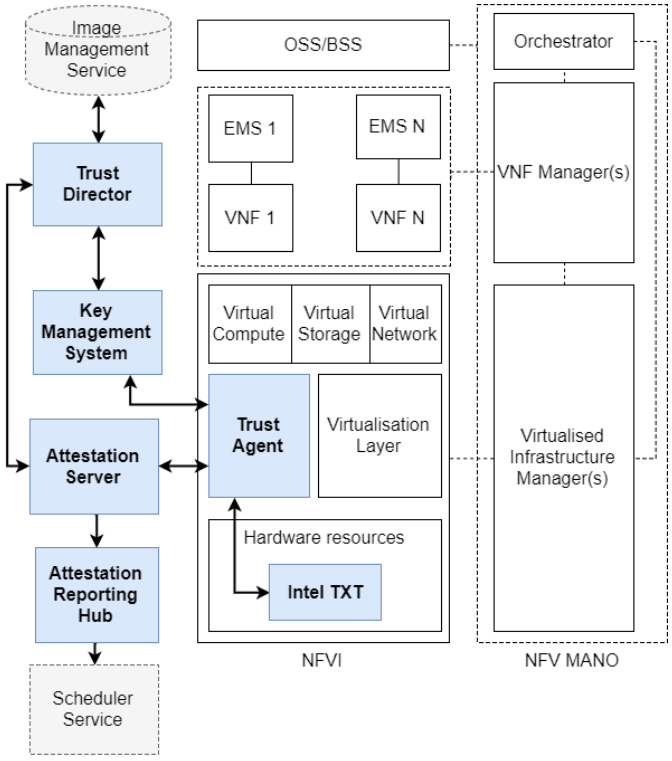

Figure 1. Integration of OpenCIT components in the NFV architecture.

The Trust Agent, executed within the host OS, maintains the ownership of the TPM and is in charge of collecting such measurements and securely providing a proof, i.e. the *TPM quote*, as a response to a RA request. The Attestation Server is in charge of initiating the RA procedure and verifying the measured host components against known-good values, that need to be previously stored. OpenCIT allows the measurements to be imported by a reference server or manually inserted in the white-list. Each NFVI node to be attested should execute the Trust Agent and be registered with the Attestation Server, to set the reference values for future attestations and to generate a AIK to digitally sign the attestation evidence.

Moreover, OpenCIT implements an additional step for attestation of Linux hosts, allowing a customization of the list of files and directories to be measured during the boot process. Such capability, named Trust Policy, enables remote integrity verification at application level, similarly to the Linux Integrity Measurement Architecture proposed by Jacquin *et al.* [7]. Both executables and configuration files are extended into the chain of trust of the host platform into a specific PCR by a component of the Trust Agent. The generation of Trust Policies is handled by the Trust Director entity, which will require access to mount the host file system in order to allow the infrastructure's maintainer to select the files to be measured. Each policy is digitally signed by both the Trust Director and the Attestation Server to ensure its integrity and authenticity, and stored in the host (e.g. the NFVI node) file system, where it is extended into the chain of trust. The same Trust Policy can be even copied on different nodes if their configuration is expected to be identical, such as the different computing nodes in the NFVI.

Both TXT and Trust Policies can be leveraged to achieve NFVI host attestation, functioning as an implementation of the ETSI Trustworthy Boot definition [1]. Local enforcement of execution policies depending on the firmware integrity, as envisioned by Secure Boot, is not addressed by OpenCIT. Moreover, extending host attestation with Trust Policies is currently supported only on Linux hosts, running Ubuntu 16.04 or Red Hat Enterprise Linux 7 distributions.

B. Integrity and confidentiality of VNFs

As previously discussed, the latest release of OpenCIT introduces the Trust Policy as a measurement architecture for files and directories executed within a target host. Apart from physical machines, this capability has been extended to virtual instances instantiated in the CSP infrastructure. More specifically, Trust Policies are available for Linux KVM machines and Docker instances running on a Linux host machine, whose chain of trust is inclusive of the Trust Agent itself. Differently from host policies, the virtual instances policies are stored along with the images in a *Image Management Service* (IMS), owned by the CSP, by the Trust Director. Execution of virtual instances can be prevented if their attestation result does not match the predefined Trust Policy. Also, their trustworthiness may depend on the trust status of the underlying host platform, regardless of their internal status. Overall, the extended chain of trust proposed by OpenCIT, from the hardware RoT to the application layer of virtual instances, can be mapped on the different Levels of Assurance envisioned by NFV-SEC. Integrity of VNFs can be achieved with a combination of load-time measurements and image validation via digital signatures, the latter being performed by the IMS.

Confidentiality of virtual images is another relevant security property relevant to the NFV scenario, considering the multi-tenancy and privacy concerns of cloud deployments. OpenCIT introduces a *Key Management Service* (KMS) to generate cryptographic keys for encryption of virtual images. Encryption of images is performed by the Trust Director at on-boarding time, which also stores metadata to identify the KMS instance that issued the key. Decryption is performed by the Trust Agent, whose AIK is cryptographically bound to the decryption key by the KMS itself. Moreover, the key is retrieved by the KMS only if the target host is trusted. Because of the binding between the decryption key and the TPM which generated the AIK, the virtual instance is launched on a trusted host only.

Although promising, the OpenCIT proposal for integrity verification and confidentiality of virtual instances is still far from a production-ready environment. First, it does not support popular virtualisation technologies, such as VMware. Moreover, both VM snapshots and migrations are not supported by either integrity or privacy work-flows.

C. Integration of trust with the MANO stack

OpenCIT framework consists of a number of stand-alone modules integrated with the standard components of an OpenStack-based CSP infrastructure. Modifications are applied to the OpenStack controller, *Nova*, and to the dashboard, *Horizon*, by specific extensions provided by OpenCIT itself. These modification enable visualisation of trust-related information in the OpenStack user interface. Moreover, a specific filter is added in the OpenStack scheduler to perform attestation of computing nodes before deploying virtual instances on top of them.

OpenStack is also supported by the OSM implementation of the NFV MANO stack, acting as underlying *Virtual Infrastructure Manager* (VIM) for the NFVI. Integration of the OpenCIT-based trust solution with OSM would benefit from the built-in support for OpenStack by both the frameworks. Differently from OpenCIT, OSM does not require any customisation to the underlying OpenStack deployment, as it interacts with such infrastructure through built-in APIs. Hence, the abstraction model adopted by OSM decouples its architecture from the underlying VIM, easing integration with custom deployments, such as the one required by OpenCIT.

Moreover, OpenCIT integrates trust assessment with the life-cycle management of computing nodes and running instances of a CSP. This capability is relevant for the NFV scenario, which envisions attestation as part of VNFs execution process and therefore implies an interaction between the trust management framework (e.g. OpenCIT) and the MANO stack. Apart from VNF instantiation, periodic attestation of both NFVI nodes and VNFs could enhance the level of trust by providing constant monitoring of platform trust. Regarding privacy issues, The Attestation Reporting Hub in OpenCIT is designed to provide results of attestation to external Scheduler Services by limiting their visibility to specific nodes of the infrastructure.

VI. Conclusion

Future work will focus on the integration of the OpenCIT framework with the ETSI-hosted initiative Open Source MANO, both leveraging OpenStack as VIM. Whilst OpenCIT has built-in support for deployment and life-cycle management of virtual instances, its implementation is not compliant with VNF on-boarding and execution and, therefore, such functionality should be delegated to OSM. Moreover, scalability issues in trust-related operations will be addressed by investigating alternative attestation work-flows, such as the currently drafted NFV-SEC proposals, and evaluating their performance with respect to the synchronous attestation work-flow employed by the Attestation Server. The resulting infrastructure will be evaluated with experimental measurements, in a real world scenario. Moreover, additional technologies for the protection of NFV cloud deployments will be investigated, such as TrustZone [17] for the Arm hardware platform.

In conclusion, the OpenCIT framework is considered highly promising because it has built-in support for attestation of both physical platforms and virtual instances in a cloud environment. Moreover, the recent addition of Trust Policies for both physical servers and virtual instances would extend the chain of trust to application-layer of both NFVI host platform and VNFs, providing a concrete mapping between attestation capabilities and the different Levels of Assurance defined in the ETSI standard. The support of OpenStack by both OpenCIT and OSM is an additional advantage of the proposed solution, which may ease trust integration with the de-facto standard for ETSI NFV MANO deployment.

Acknowledgment

The research described in this paper is part of the SHIELD project, co-funded by the European Commission (H2020 grant agreement no. 700199).

References

[1] "ETSI GS NFV-SEC 003 Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance," ETSI NFV ISG, Dec. 2014.

[2] "ETSI GS NFV-SEC 012 Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components," ETSI NFV ISG, Jan. 2017.

[3] "ETSI GS NFV-SEC 013 Network Functions Virtualisation (NFV) Release 3; Security ; Security Management and Monitoring specification," ETSI NFV ISG, Feb. 2017.

[4] "ETSI GS NFV-SEC 002 Network Functions Virtualisation (NFV); NFV Security; Cataloguing security features in management software," ETSI NFV ISG, Aug. 2015.

[5] Trusted Platform Module. [Online]. Available: https://trustedcomputinggroup.org/work-groups/trusted-platform-module/

[6] Open Cloud Integrity Technology (Open CIT). [Online]. Available: https://01.org/opencit

[7] L. Jacquin, A. Lioy, D. R. Lopez, A. L. Shaw, and T. Su, "The trust problem in modern network infrastructures," in *Cyber Security and Privacy: 4th Cyber Security and Privacy Innovation Forum, Brussels (Belgium), April 28-29, 2015, Revised Selected Papers*, F. Cleary and M. Felici, Eds. Springer International Publishing, 2015, pp. 116–127.

[8] Integrity Measurement Architecture. [Online]. Available: https://sourceforge.net/p/linux-ima/wiki/Home/

[9] B. Jaeger, "Security Orchestrator: Introducing a Security Orchestrator in the Context of the ETSI NFV Reference Architecture," in *TRUSTCOM'15: 14th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications - Vol. 1*, Helsinki (Finland), August 20-22, 2015, pp. 1255–1260.

[10] S. Ravidas, S. Lal, I. Oliver, and L. Hippelainen, "Incorporating trust in NFV: Addressing the challenges," in *ICIN-2017: 20th Conference on Innovations in Clouds, Internet and Networks*, Paris (France), March 7-9, 2017, pp. 87–91.

[11] Z. Yan, P. Zhang, and A. V. Vasilakos, "A security and trust framework for virtualized networks and software-defined networking," *Security and Communication Networks*, vol. 9, no. 16, pp. 3059–3069, 2016.

[12] Docker. [Online]. Available: https://www.docker.com/

[13] "Network Functions Virtualisation - An Introduction, Benefits, Enablers, Challenges & Call for Action," White Paper, ETSI, Oct. 2012.

[14] "ETSI GS NFV-IFA 011 Network Functions Virtualisation (NFV); Management and Orchestration; VNF Packaging Specification," ETSI NFV ISG, Oct. 2016.

[15] "Open Source MANO," White Paper, ETSI OSM Community, Apr. 2017. [Online]. Available: https://osm.etsi.org/images/OSM-Whitepaper-TechContent-ReleaseTWO-FINAL.PDF

[16] "ETSI GS NFV 002 Network Functions Virtualisation (NFV); Architectural Framework," ETSI NFV ISG, Dec. 2014.

[17] ARM TrustZone. [Online]. Available: https://www.arm.com/products/security-on-arm/trustzone