POLITECNICO DI TORINO

Dipartimento di Automatica e Informatica

PhD in Computer and Control Engineering

XXXII cycle

Supervisor

Prof. Antonio Lioy

Security and trust in a Network Functions Virtualization infrastructure

PhD Candidate: *Marco De Benedictis*

1. Context

Network Functions Virtualization (NFV) proposes a shift from the hardware appliances to softwarised ***Virtual Network Functions*** (VNFs):

- networks can be easily deployed and adjusted to traffic needs thanks to cloud computing
- more flexible and scalable, no vendor lock-in

NFV networks introduce security risks due to the interplay of networking and virtualisation.

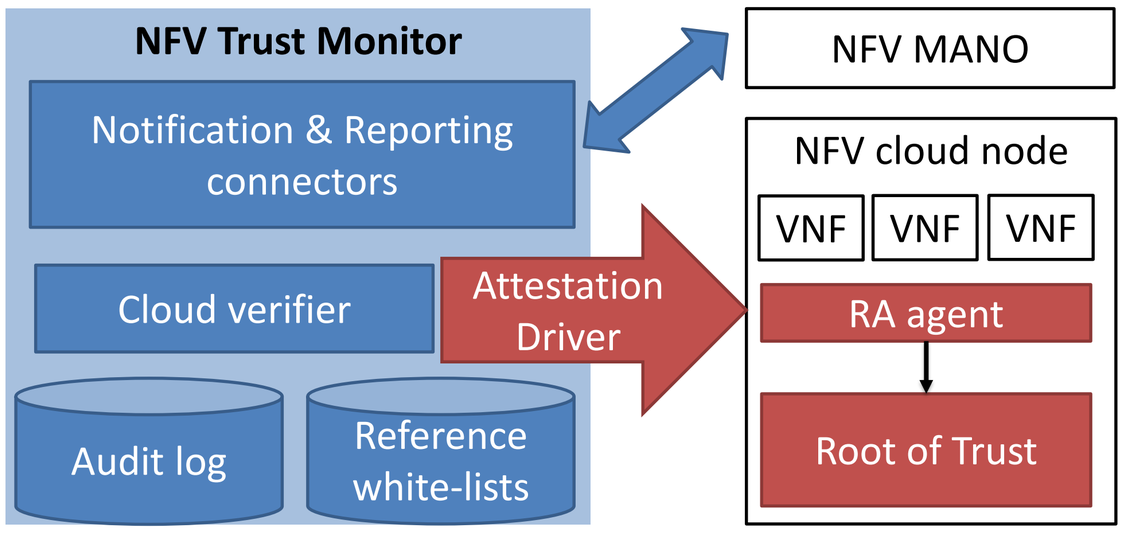
2. Objectives

- Protect NFV networks against manipulations
- Enhance orchestration with reaction to threats

3. Trust architecture and technique

I designed the NFV ***Trust Monitor*** (TM) [1], based on Trusted Computing methods:

- ***Remote Attestation*** (RA) to verify the integrity measurements against known-good values
- ***Trusted Platform Modules*** (TPMs) are Roots of Trust for authentication and secure storage



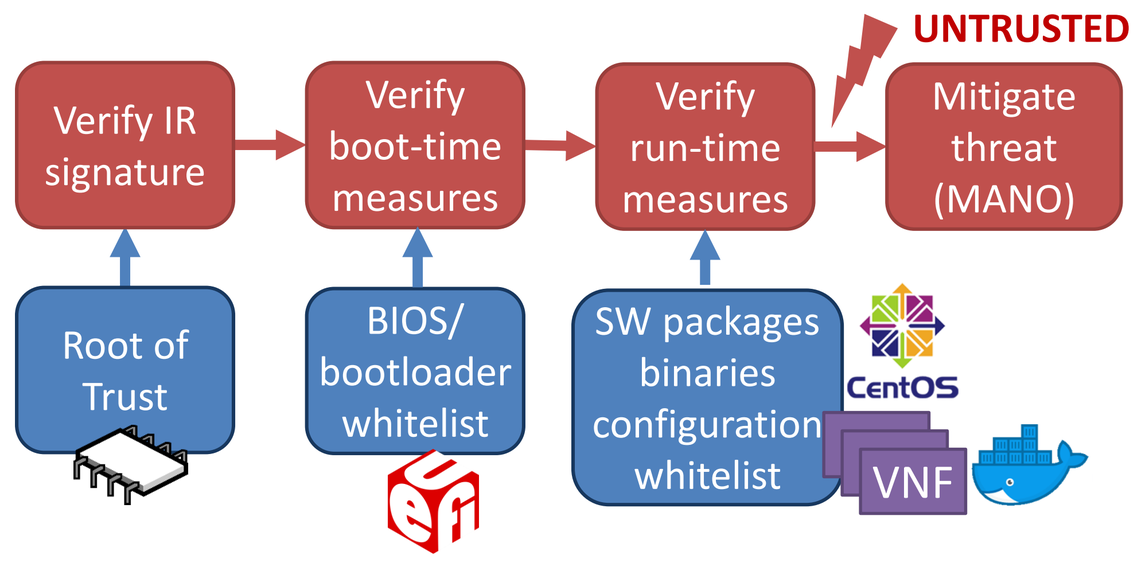
A measure is a **cryptographic hash** of a software event (e.g. binary, file open for read).

Key aspects of our solution:

- verification of the boot (BIOS, bootloader) and the run-time events against manipulations
- integration within the ETSI NFV ***Management and Orchestration*** (MANO) domain
- **generic approach** to attestation to support different *Trusted Execution Environments* (TEEs)

I developed a **container-based** VNF attestation technique [2] as *Attestation Driver* for the TM:

- leveraging container share of the host kernel
- Linux ***Integrity Measurement Architecture*** (IMA) kernel-level system hooks to measure containers
- a proof by a single physical TPM can be used to validate all measurements (host + containers)



4. Validation

Proof-of-Concept based on Docker and Open Source MANO Release 5 as part of the **SHIELD** H-2020 project [3].

Runtime VNF attestation requires a non-negligible overhead in the order of seconds, due to

- TPM signing latency (~ 2 s)
- size of the IMA event log

5. Conclusions

- Platform attestation can support the orchestration towards a secure NFV
- Open challenges exist in applying trust to full virtualisation and supporting different TEEs

6. References

1. De Benedictis M. and Lioy A., A proposal for trust monitoring in a Network Functions Virtualisation Infrastructure, IEEE NetSoft 2019, DOI: 10.1109/NETSOFT.2019.8806655
2. De Benedictis M. and Lioy A., Integrity verification of Docker containers for a lightweight cloud environment, Future Generation Computer Systems, DOI: 10.1016/j.future.2019.02.026
3. De Benedictis M. *et al*, NFV-based network protection: The SHIELD approach, IEEE NFV-SDN 2017, DOI: 10.1109/NFV-SDN.2017.8169869