Leveraging Software Integrity Verification in the Cloud

The *Remote Attestation Service* is a cloud subsystem responsible to assess the integrity of nodes in the cloud infrastructure through techniques introduced by the Trusted Computing technology.

This service gives significant advantages in the cloud environment. First, it allows cloud users to deploy their virtual machines on a physical host that satisfies desired security requirements, represented by integrity levels.

Secondly, this service allows cloud administrators to monitor the status of the nodes in an efficient way and to take appropriate countermeasures once a compromised host has been detected. For instance, administrators can isolate the host such that it can not attack other nodes of the infrastructure.

Architecture

The *Remote Attestation Service* consists of two components:

OpenAttestation: this framework, developed by Intel [1], enables *OpenStack Nova Scheduler* to retrieve and verify the integrity of cloud nodes such that the former can select a host that meets users' requirements. The framework, as depicted in Figure 1, handles the Remote Attestation protocol through two submodules

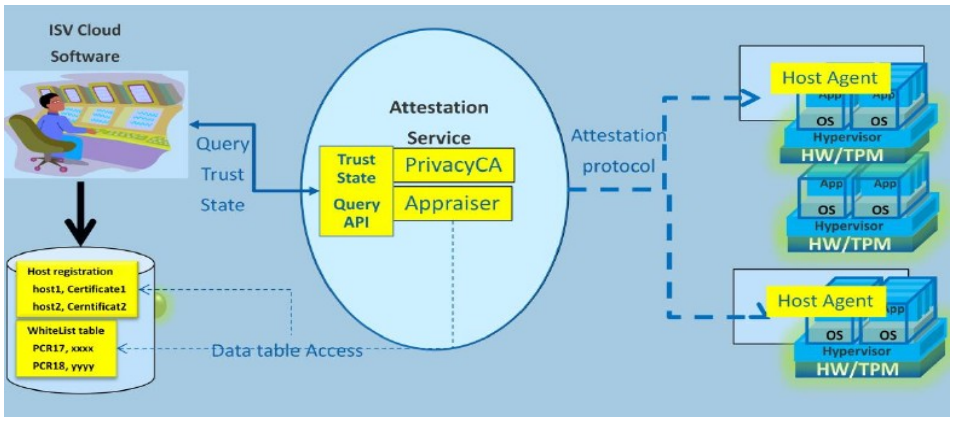

Figure 1: OpenAttestation architecture - taken from documentation

that act as the endpoints:

- **Host Agent:** collects the measurements done by the cloud node being attested, generates and sends the integrity report to the verifier;
- **Appraiser:** verifies the integrity report received from a cloud node and assigns to the latter an integrity level.

RA Verifier: this component analyzes the measurements performed by the Integrity Measurement Architecture (IMA), a subsystem of the Linux Kernel, running on cloud nodes. In particular, it verifies whether the digests of binaries and shared libraries are present in a database of known values and whether the packages these files belong to are up to date. The first check allows to detect possibly malicious software that may have been executed before verification, while the second check allows to identify loaded applications with known vulnerabilities that may be exploited by an attacker.

Integrity Levels

As said before, users can specify integrity requirements through levels. An integrity level is a numeric representation of the integrity status of a system and allows to determine whether the host which the system is running on will perform its task, e.g executing a virtual machine from an user, as expected. Since integrity levels are progressive, requiring a higher level will give more confidence and trust into the hosts.

In the current version, five integrity levels have been defined:

1. *boot_untrusted*: invalid integrity report;
2. *ima_digest_not_found*: unknown digests;
3. *ima_pkg_security_updates*: packages with security vulnerabilities;
4. *ima_pkg_not_security_updates:* packages with other vulnerabilities;
5. *ima_all_ok*: all digests recognized and packages up to date.

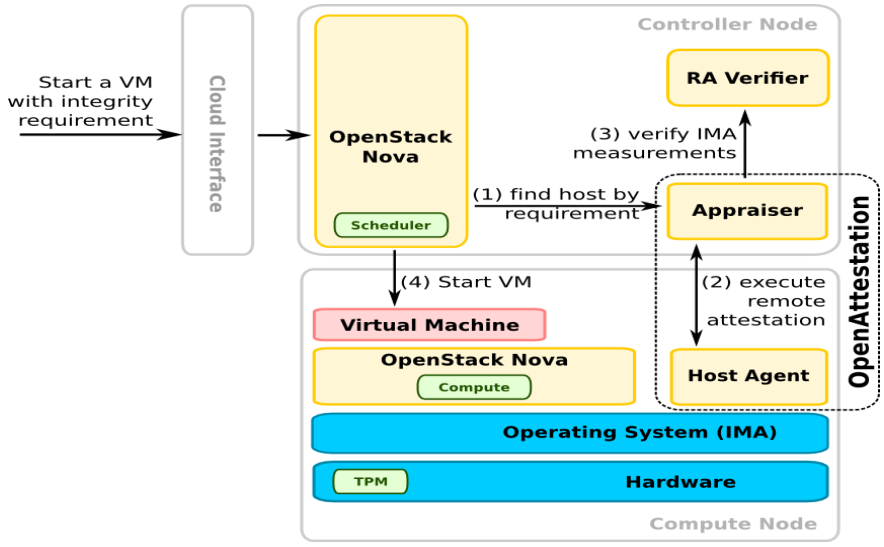

Figure 2: Remote Attestation with Trustworthy OpenStack

Integration with Trustworthy OpenStack

Trustworthy OpenStack allows users to specify an integrity requirement for the hosts where their VMs will be deployed on. Currently, there are two ways to supply this type of requirement: by extending the extra specifications of a VM instance type (also called flavor) with the key-value pair *trusted_host - <desired integrity level>* or by providing this information directly when a VM is being instantiated. It is also possible to specify *min_trusted_host* as a key to select a host whose integrity level is greater or equal to the value specified.

As depicted in Figure 2, when a user instantiates a VM while providing an integrity requirement (e.g. through the *Dashboard*), *Trustworthy OpenStack Scheduler* tries to find a host that meets this requirement by requesting to the *Remote Attestation Service* the current integrity level for each available host. Then, the *OpenAttestation* component executes the Remote Attestation protocol between the Controller node and the Compute Node (the queried host) and, if the integrity report is valid, passes IMA measurements to *RA Verifier,* which determines the host integrity level, and returns that level back to the caller. Lastly, the *Scheduler* requests a host that satisfies the integrity requirement to start the VM as requested by the user.

References

[1] Intel, OpenAttestation SDK (OAT) A SDK for Remote Attestation, https://github.com/OpenAttestation/OpenAttestation.

Where To Find Remote Attestation Service?

RA Verifier is available at http://security.polito.it/tc/ra

Further Information

Further information about *Remote Attestation Service* can be found under Deliverable „D2.4.2—Initial Component Integration, Final API Specification, and First Reference Platform".

Disclaimer

The TClouds project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement number ICT-257243.

TClouds at a glance

Project number:
257243

TClouds mission:
- Develop an advanced cloud infrastructure that delivers computing and storage with a new level of security, privacy, and resilience.
- Change the perceptions of cloud computing by demonstrating the prototype infrastructure in socially significant application areas.

Project start:
01.10.2010

Project duration:
3 years

Total costs:
EUR 10.536.129

EC contribution:
EUR 7.500.000

Consortium:
14 partners from 7 different countries.

Project Coordinator:
Dr. Klaus-Michael Koch
coordination@tclouds-project.eu

Technical Leader:
Dr. Christian Cachin
cca@zurich.ibm.com

Project website:
www.tclouds-project.eu