Introduction

Hosting resources in the cloud results into a shared responsibility between cloud provider and customer. In particular the responsibility for all security aspects is now shared. Moreover, as all cloud customers use the same resources, the infrastructure is shared among multiple tenants, which may be competitors. Hence proper isolation of cloud customers becomes of crucial importance for acceptance of cloud offerings.

With the TrustedInfrastructure Cloud we provide the following key properties:

Trust in remote resources is established by building on top of Trusted Computing technologies, providing verifiable integrity of the remote components.

Protection against insider attacks is achieved, as the administration is completely controlled by the infrastructure itself. All data is encrypted and there are no administrators with elevated privileges.

With **Trusted Virtual Domains (TVD)** we provide trustworthy isolation of virtual computing, storage and networking resources as well as pervasive information flow control. TVDs are employed for isolation of tenants and for separation of security domains of a single tenant.

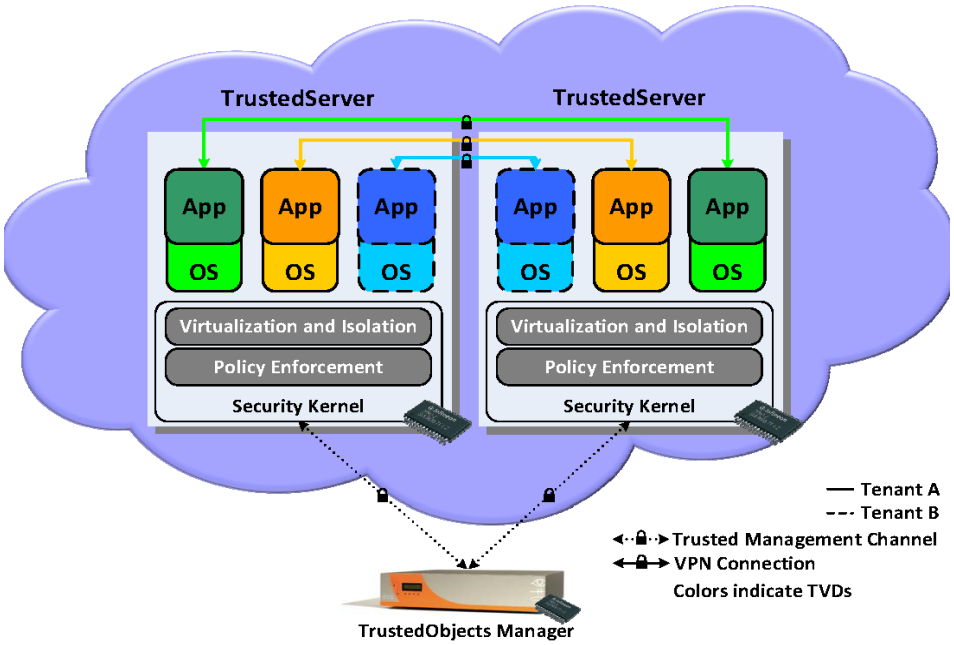

Figure 1: A TrustedInfrastructre Cloud running VMs of different tenants TVDs

Architecture

In the TrustedInfrastructure Cloud (cf. Figure 1) a central management component, called TrustedObjects Manager (TOM), manages a set of TrustedServers (TS) which run a security kernel, which in turn run the virtual machines (VM) of the users. A virtual machine consists of the operating system (OS) and applications (App).

TS as well as the TOM, are equipped with a hardware security module (HSM) [1]. When started, the HSM is employed for secure boot, ensuring the integrity of the software (in particular of the security kernel). Moreover, the hard drives are encrypted by a key that is stored within the HSM. Via this sealing, the local hard drives can only be decrypted in case the HSM has crosschecked the integrity of the component. Hence only an untampered security kernel can be booted and can access the decrypted data. The security kernel enforces the security policy and the isolation.

The TOM is in charge of deploying configuration data (including key material and security policies) and VMs on the TrustedServers. Security services within the security kernel handle the configuration and ensure that the security policies are properly enforced. Encrypted communication of TOM and TrustedServer is via the Trusted Management Channel (TMC) which ensures the integrity using remote attestation before transmitting any data. All administrative tasks on the TrustedServer are performed via the TMC, there is no other management channel for an administrator (like an ssh-shell). In Figure 2 the

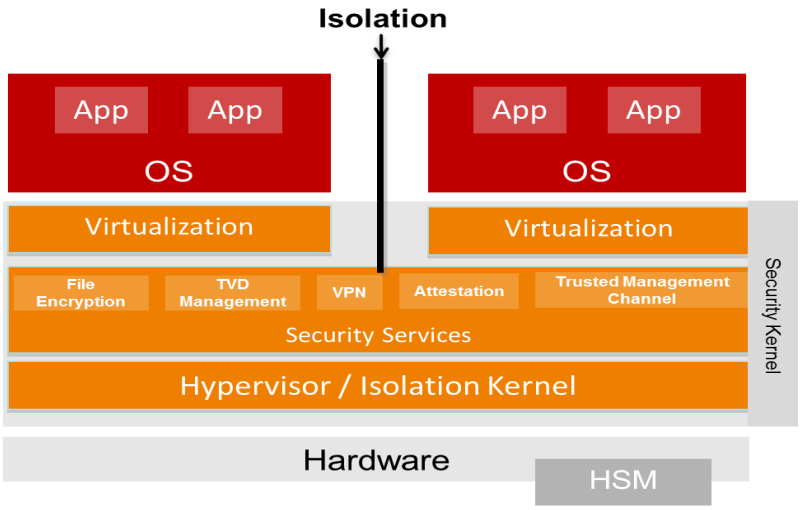

Figure 2: Architecture of a TrustedServer

architecture of a TrustedServer is presented in more details. The security kernel comprises the isolation kernel and the hypervisor to provide isolation between virtual machines and a set of security services managing TVDs, file encryption, VPN, remote attestation and the TMC.

Trusted Virtual Domains

Trusted Virtual Domains (TVD) [2] allow the deployment of isolated virtual infrastructures upon shared computing and networking resources. By default, different TVDs are isolated from each other.

Communication is restricted to virtual machines within the same TVD and data at rest is encrypted by a TVD specific key. Remote communication between components of the same TVD over an untrusted network are secured via virtual private network (VPN). Only virtual machines of the same TVD, which have access to the same TVD key, are able to communicate and decrypt data.

A TrustedServer can simultaneously run various VMs attached to different TVDs. Figure 1 illustrates that each tenant runs his own set of TVDs, ensuring isolation of tenants. A single tenant can also run distinct TVDs (cf. Tenant A), to isolate domains within an organisation.

References

[1] Trusted Computing Group (TCG). TPM Main Specification, Version 1.2, Revision 116, March 2011.

[2] CDE+10 L. Catuogno, A. Dmitrienko, K. Eriksson, D. Kuhlmann, G. Ramunno, A.R. Sadeghi, S. Schulz, M. Schunter, M. Winandy, and J. Zhan. Trusted Virtual Domains–Design, Implementation and Lessons Learned. Trusted Systems, pages 156–179, 2010.

Disclaimer

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

Where To Find TrustedInfrastructure Cloud?

http://www.sirrix.com

Further Information

Further information about TrustedInfrastructure Cloud can be found in "D2.1.1—Technical Requirements and Architecture for Privacy-enhanced and Resilient Trusted Clouds" and "D2.3.1— Requirements, Analysis, and Design of Security Management".

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