Protection of Client Keys Against Internal and External Attackers

Moving to the cloud also means to relinquish physical control over the own data and computations. As a consequence of the loss of physical control over computations in the cloud, the client faces limitations concerning the security in cloud computing and in particular regarding the protection of deployed high-value cryptographic credentials. For instance, clients may deploy a web-service that uses SSL/TLS to secure the communication with its end-users requiring an asymmetric key-pair. Specifically, potential attacks (cf. Figure 1) that compromise the security of these high-value credentials, like the SSL/TLS private key, might originate from

- External Attackers which exploit vulnerabilities in the deployed web-service
- Malicious co-located Clients which might compromise the isolation between Virtual Machines
- Insider Attackers at the provider side which exploit their privileges

In presence of these shortcomings and threats, we introduce *Cryptography-as-a-Service* (CaaS), a technology that allows for establishing secret-less client VMs and securely separating client's cryptographic primitives and credentials.

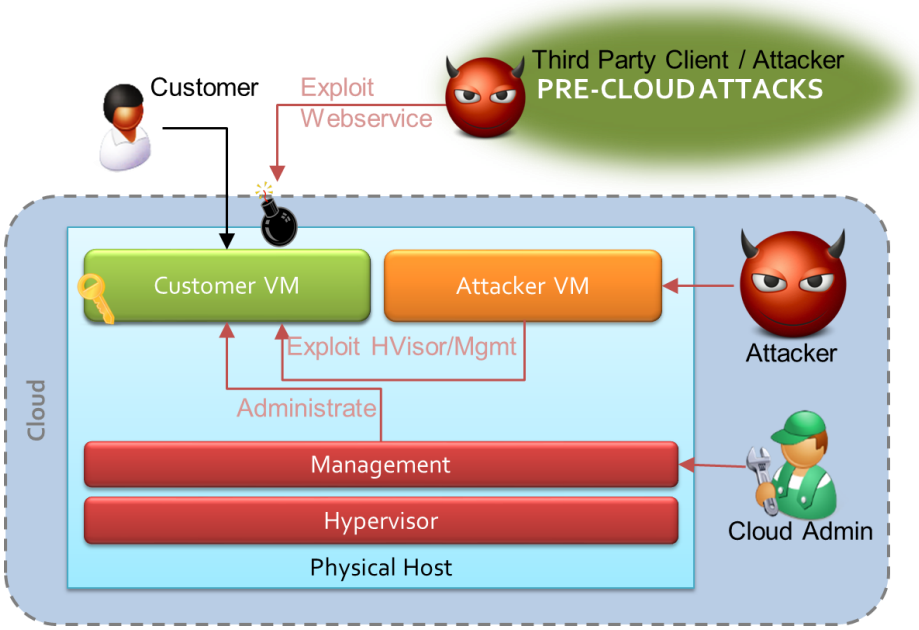

Figure 1: Potential attackers against Customer Virtual Machines

Benefits of Cryptography-as-a-Service

Cryptography-as-a-Service empowers the cloud clients to be in control of their cryptographic operations and keys that they deploy in the cloud, independently of the cloud provider. They can leverage CaaS in two different usage modes (cf. Figure 2):

Virtual Security Module emulates a virtual hardware security device, like an HSM, attached to the client VM. The client's workload can leverage this security module as a secure credential storage to protect his high-value cryptographic keys from unauthorized access by external attackers or insider attacks. Additionally, the client can also load custom trusted code into the security module and leverage it as a customized crypto engine, e.g., to securely maintain SSL/TLS communication channels by outsourcing the security-sensitive key management operation into the isolated Virtual Security Module.

Secure Virtual Device forms a transparent layer between the client VM and peripheral devices (storage disk or network card) and encrypts all I/O data streams to/from those devices similar to full-disk encryption or Virtual Private Networks (VPN). We also use this layer as a convenient building block to protect the VM images and VM states during provisioning to the cloud (i.e., the client uploads only encrypted images to the cloud), migration between cloud nodes (i.e., the VM state is transferred only in encrypted form between cloud nodes), and storage.

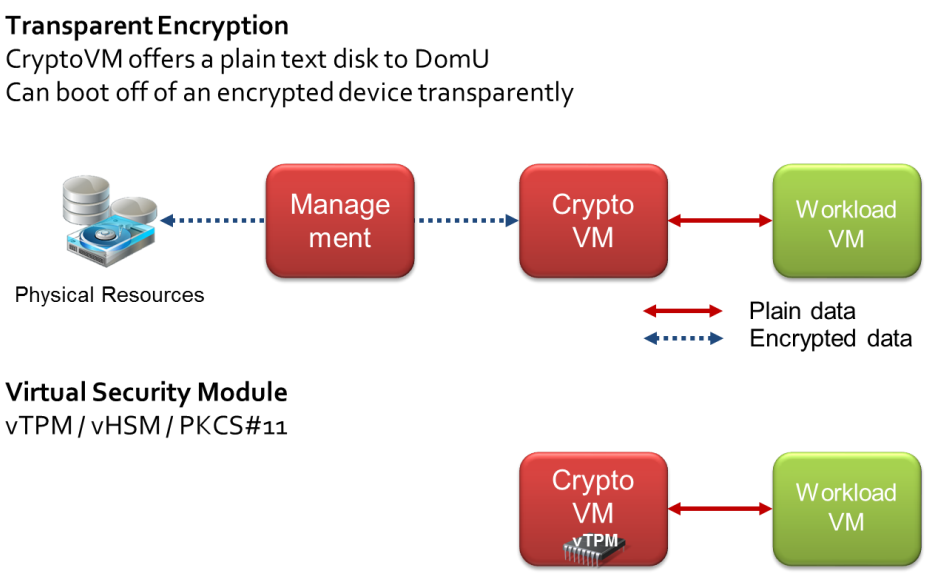

Figure 2: Modes of operation of Cryptography-as-a-Service

Integration with Trusted OpenStack

All cryptographic operations of the service are executed in a specially protected virtual machine called CryptoVM. We secure the high-value cryptographic assets in the CryptoVM through isolation provided by our trusted hypervisor. Moreover we remove privileges from the omnipotent management domain, in which insider attackers could operate. Leveraging standardised Trusted Computing technology, the client can verify prior to deployment of high-value credentials that the cloud indeed provides a trusted CaaS platform and thus protects these credentials.

CaaS is implemented at the lowest level of the cloud software stack, beneath the virtual machines, at the hypervisor level. Consequently, it is independent of the management software running in Dom0 of Xen. However, the Trustworthy OpenStack platform of TClouds is aware of CaaS and supports the provisioning of keys and encrypted images in the user interface. These keys can only be decrypted by the CaaS Trusted hypervisor in a known, secure state.

In Trustworthy OpenStack, CaaS further leverages other components of TClouds. For instance, the Remote Attestation Service is used prior to migration of VMs to verify that the target cloud nodes of the migration are running the CaaS Trusted Hypervisor. On the other hand, concepts like TVDs can leverage the transparent encryption layer of CaaS as convenient building block to transparently encrypt the network and storage data of VMs.

Further Information

Further information about Cryptography-as-a-Service can be found under Deliverable „D2.1.2— Preliminary Description of Mechanisms and Components for Single Trusted Clouds".

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