



Security and **Privacy** in **Cloud Computing**

Ragib Hasan

Johns Hopkins University
en.600.412 Spring 2010

Lecture 5
03/08/2010

Securing Clouds

Goal: Learn about different techniques for protecting a cloud against insider adversaries

Reading

Santos et al., [Towards Trusted Cloud Computing](#), HotCloud 2009

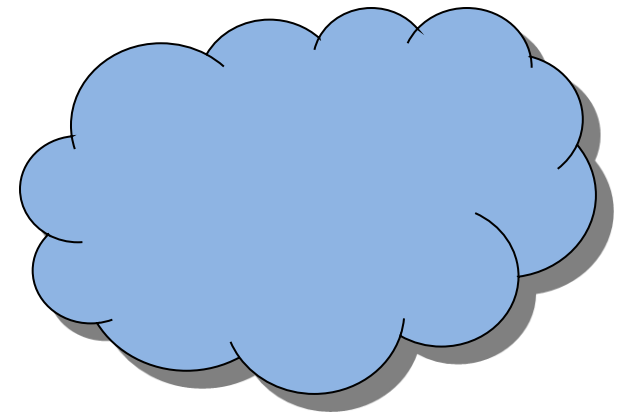
Krautheim, [Private Virtual Infrastructure for Cloud Computing](#), HotCloud 2009

Wood et al., [The Case for Enterprise-Ready Virtual Private Clouds](#), HotCloud 2009

The IaaS security problem

The cloud acts as a big black box, nothing inside the cloud is visible to the clients

Clients have no idea or control over what happens inside a cloud



Even if the cloud provider is honest, it can have malicious sys admins who can tamper with the VMs and violate confidentiality and integrity

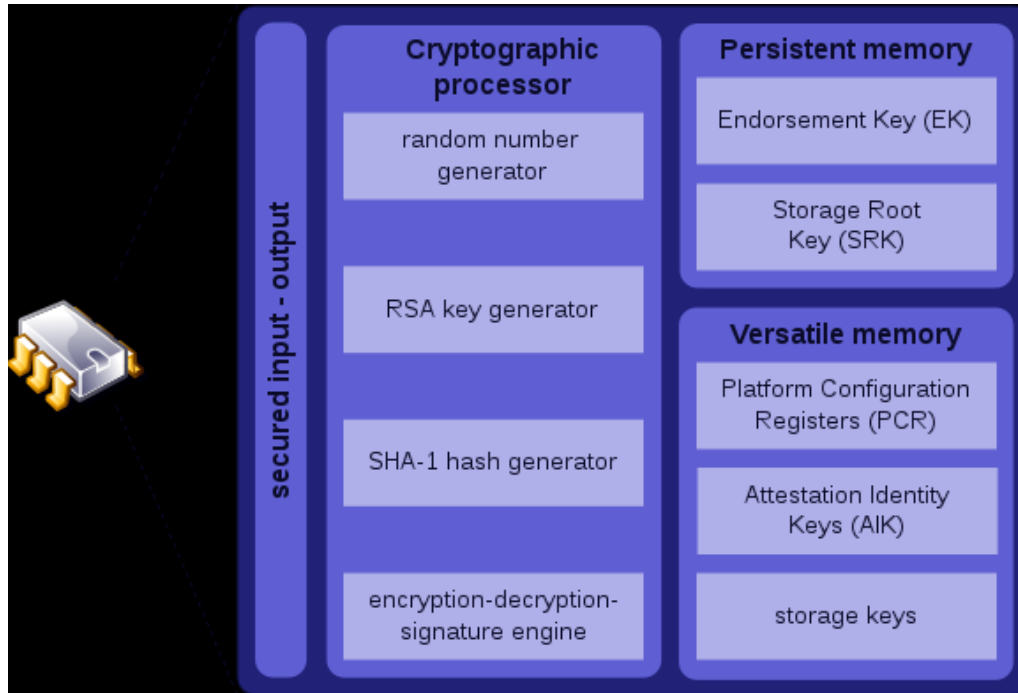
How to ensure that the cloud is not tampered with?

- **Naïve Approach 1:** Just trust the cloud provider
 - Why won't work: Provider may be honest, sys admins may not be so
- **Naïve Approach 2:** Ask the cloud provider to allow auditing of the cloud by the client
 - Why won't work: Providers are not willing to open their system to outside audits
- **Workable Approach 3:** Ask cloud provider for unforgeable proof/attestation
 - Why may work: A third party proof not revealing other information may be enough for both client and provider

How to audit with a third party?

- Allow third party access to cloud?
- Use trusted hardware

Trusted Platform Module (TPM)



TPMs are inexpensive chips now included in most laptops

Can be the building block for a trusted computing base

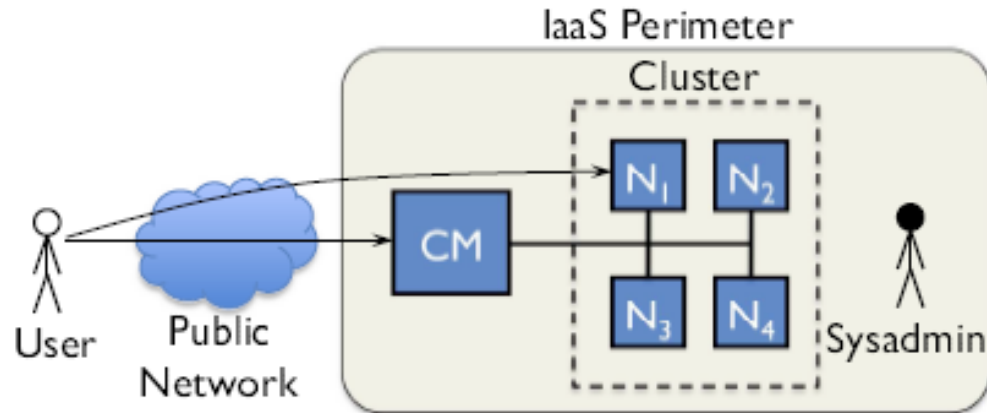
Can bootstrap trust in a system

Cannot (easily) be compromised to get the keys

Endorsement Key: A private (RSA) key that identifies the chip

Platform Configuration Register (PCR) : Can contain hashes of system configurations

Trusted Cloud Computing Platform by Santos et al., HotCloud 09



Problem Insiders with root access can compromise confidentiality of client virtual machines

Possible solution?: Encrypt virtual machines, but sooner or later, it has to be decrypted to run

Possible Solution?: Only allow nodes running trustworthy software to decrypt the VM

Threat Model



Attacker

- A malicious insider with root level access to cloud nodes (i.e., can install new software, modify existing software etc., inspect VMs running on a node)
- Does not have physical access to machine

How determine if a node is trustworthy?

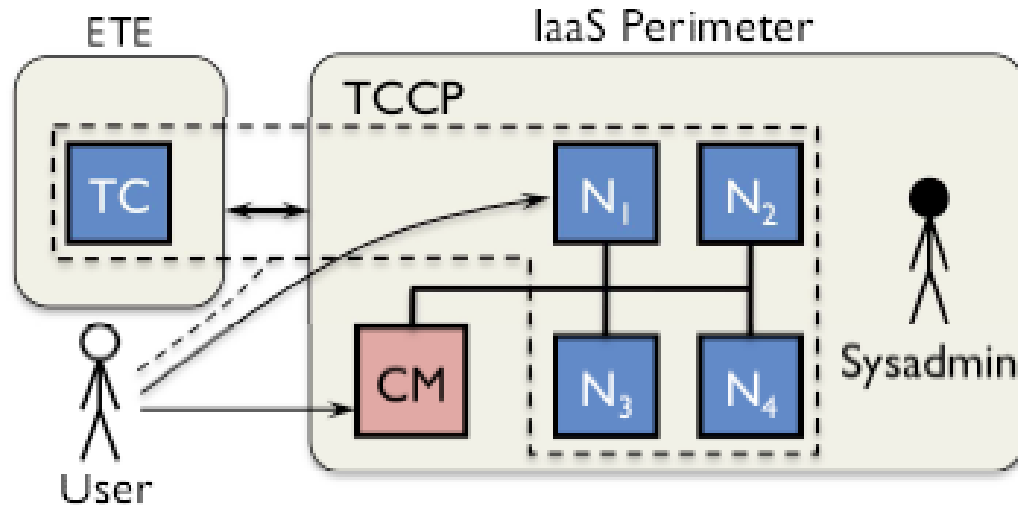
Major events that causes changes

- Node start, VM Launch, VM migration

How to determine trustworthiness?

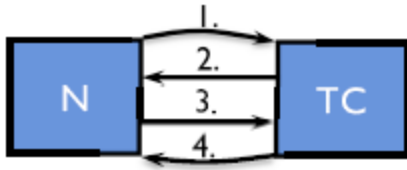
- A node is trustworthy if it has a trustworthy configuration (e.g., h/w, software etc.)
- Remote attestation can help in verifying configurations

TCCP Architecture



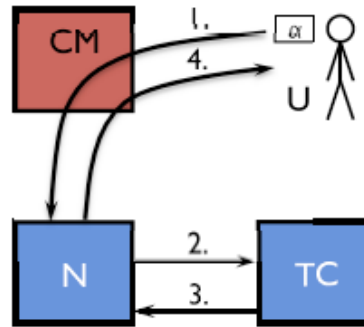
- Nodes run **Trusted Virtual Machine Monitors** (TVMM), and TVMM configuration can be certified by TPMs
- External Trusted Entity (ETE) or the **Trusted Coordinator** (TC) is the trusted third party that verifies the node

TCCP Protocols



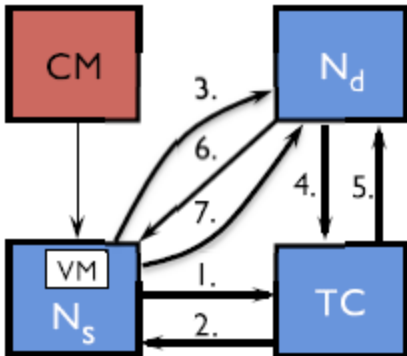
1. n_N
2. $\{ML_{TC}, n_N\}_{EK_{TC}^P}, n_{TC}$
3. $\{\{ML_N, n_{TC}\}_{EK_N^P}, TK_N^P\}_{TK_{TC}^P}$
4. $\{accepted\}_{TK_N^P}$

Node registration



1. $\{\alpha, \#\alpha\}_{K_{VM}} \{n_U, K_{VM}\}_{TK_{TC}^P}$
2. $\{\{n_U, K_{VM}\}_{TK_{TC}^P}, n_N\}_{TK_N^P}, N\}_{TK_{TC}^P}$
3. $\{\{n_N, n_U, K_{VM}\}_{TK_N^P}\}_{TK_{TC}^P}$
4. $\{n_U, N\}_{K_{VM}}$

VM Launch



1. $\{\{N_d, n_{s1}\}_{TK_N^P}, N_s\}_{TK_{TC}^P}$
2. $\{\{n_{s1}, TK_{N_d}^P\}_{TK_{N_s}^P}\}_{TK_{TC}^P}$
3. $\{\{K_S, n_{s2}\}_{TK_{N_s}^P}, N_s\}_{TK_{N_d}^P}$
4. $\{\{N_s, n_d\}_{TK_{N_d}^P}, N_d\}_{TK_{TC}^P}$
5. $\{\{n_d, TK_{N_s}^P\}_{TK_{N_d}^P}\}_{TK_{TC}^P}$
6. $\{n_d\}_{K_S}$
7. $\{VM_{id}, \#VM_{id}\}_{K_S}$

VM Migrate

TCCP limitations

- Any single point of failure?
- Will it increase the attack surface?
- How about cost-effectiveness?

Private Virtual Infrastructure

Krautheim, HotCloud09

Problem The abstraction of a cloud hides the internal security details from clients, which in turn causes them to mistrust the cloud.

Idea

- Cloud provider and client collaborate to create a trusted system.
- Separate the different clients through their exclusive private virtual infrastructures
- Give more control to the cloud clients

Separating the Fabric from the Cloud

- Cloud provider owns and operates the underlying fabric of the cloud (e.g., h/w and minimal amount of software)
- Clients own the virtual data center infrastructure
- Resource provisioning and management is done by the client using a “Factory” (which can be off the cloud)

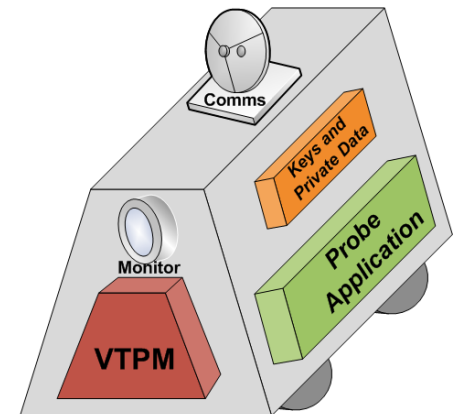
5 Tenets of Cloud Computing Security

- Provide a trusted foundation
- Provide a secure provisioning factory
- Provide measurement and attestation mechanisms
- Provide secure shutdown and destruction of VMs
- Provide continuous monitoring and auditing

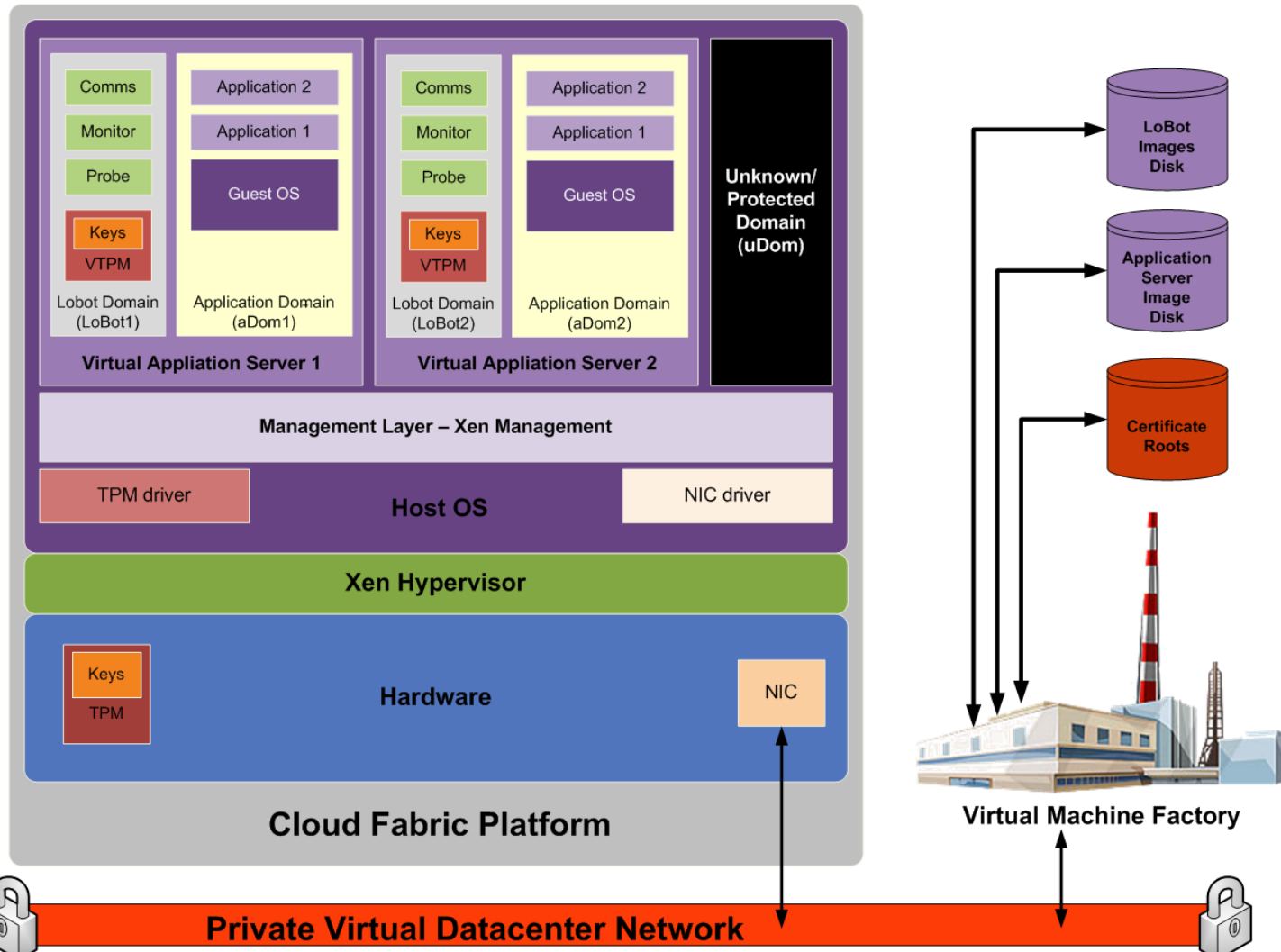
LoBots

LoBots

- Secure VM Architecture and transfer protocol
- Act as the trusted agent of the PVI factory inside a cloud
- Can measure and monitor cloud on behalf of the factory



PVI Model



CloudNet

Wood et al., HotCloud 09

Problem: Migrating to cloud is difficult for enterprise applications

Opening up network to outside access can expose system to outsider attacks

Solution:

- Merge VPN technology with clouds
- Network provider collaborates to set up a VPN link between enterprise and cloud



Further Reading

TPM Reset Attack <http://www.cs.dartmouth.edu/~pkilab/sparks/>

Halderman et al., **Lest We Remember: Cold Boot Attacks on Encryption Keys**, **USENIX Security 08**, <http://citp.princeton.edu/memory/>