Max
Planck
Institute
for
Software Systems

Towards trusted cloud computing

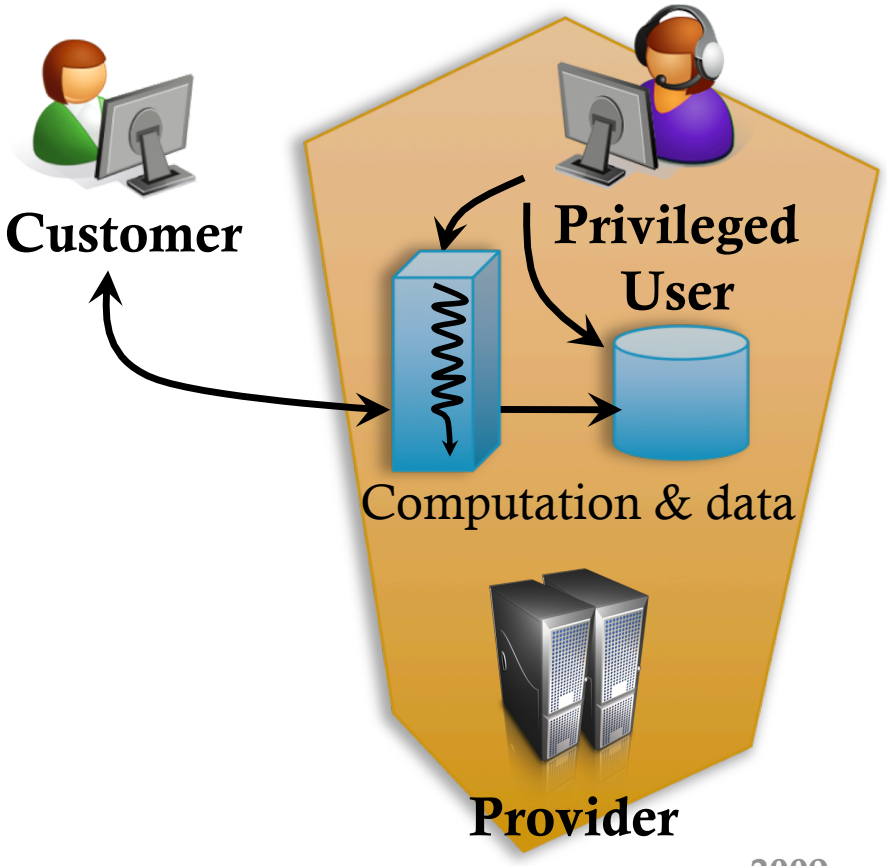
Nuno Santos, Krishna P. Gummadi, and Rodrigo Rodrigues
MPI-SWS

Cloud computing appealing but still concerns

- Many companies can reduce costs using CC services
- But, customers still concerned about security of data
- Data deployed to CC services can leak out

Potential data leakage at the provider site

- Customer pay virtual machine (VM) to compute data
  - E.g., Amazon EC2
- Privileged user with access to VM state can leak data
  - Accidentally or intentionally



Need solution to secure the computation state

- Encryption can secure communications and storage
- But, encryption *per se* is ineffective for computation
  - Raw data kept in memory during computation
- Provider benefits from providing a solution

Trusted Cloud Computing Platform

- **Goal: Make computation of virtual machines confidential**
- Deployed by the service provider
- Customer can verify that computation is confidential

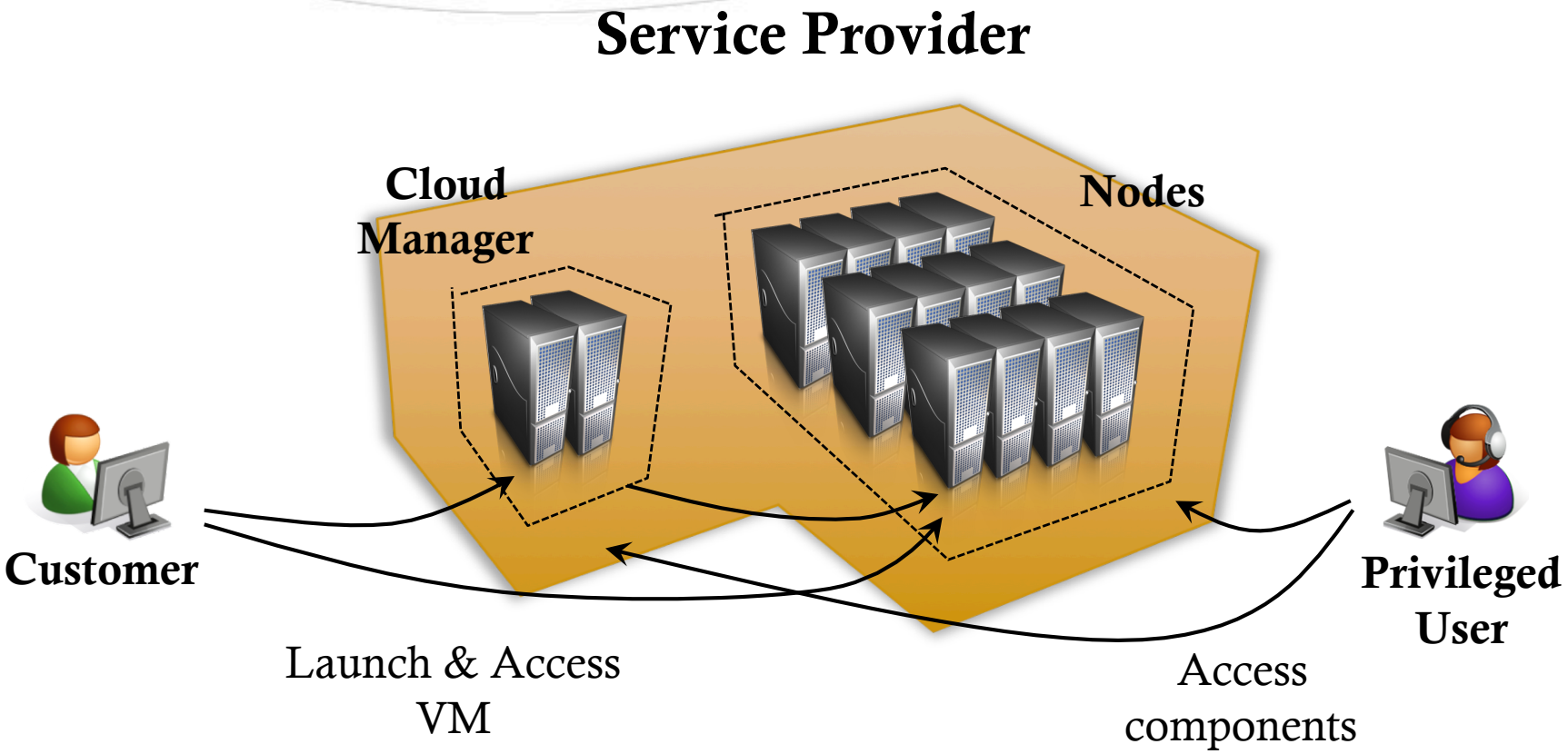
The threat model: User with root privileges

- Providers require staff with privileged access to the system
  - E.g., maintenance of software and workload
- **User with full privileges on any machine**
  - Configure, install and run software, remotely reboot
  - Setup attacks to access VM state

Rely on provider to secure the hardware

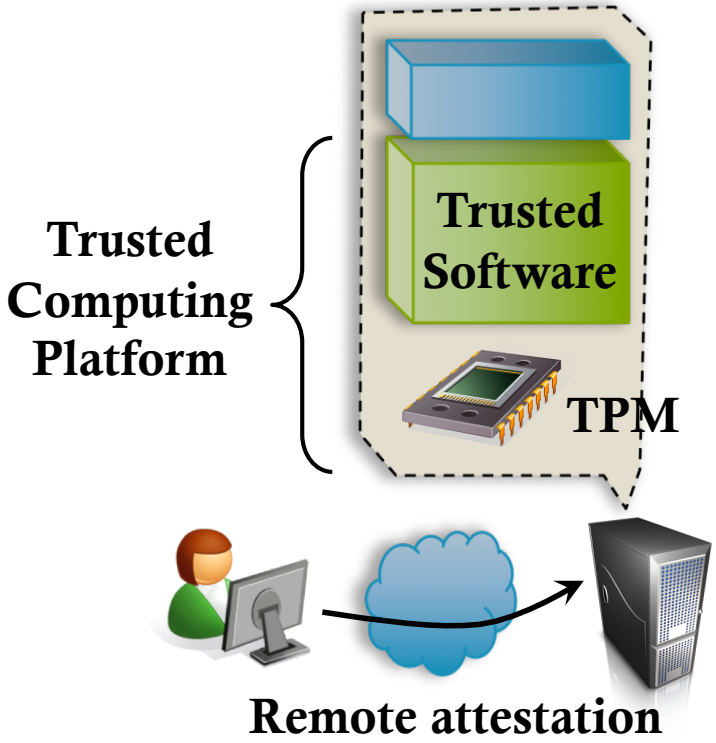
- Access to hardware can bypass any sw-based protections
  - E.g., cold boot attacks
- Leverage security protections deployed by providers
  - E.g., physical security perimeter, surveillance
- These protections can mitigate hw-based attacks

Model of elastic virtual machine services



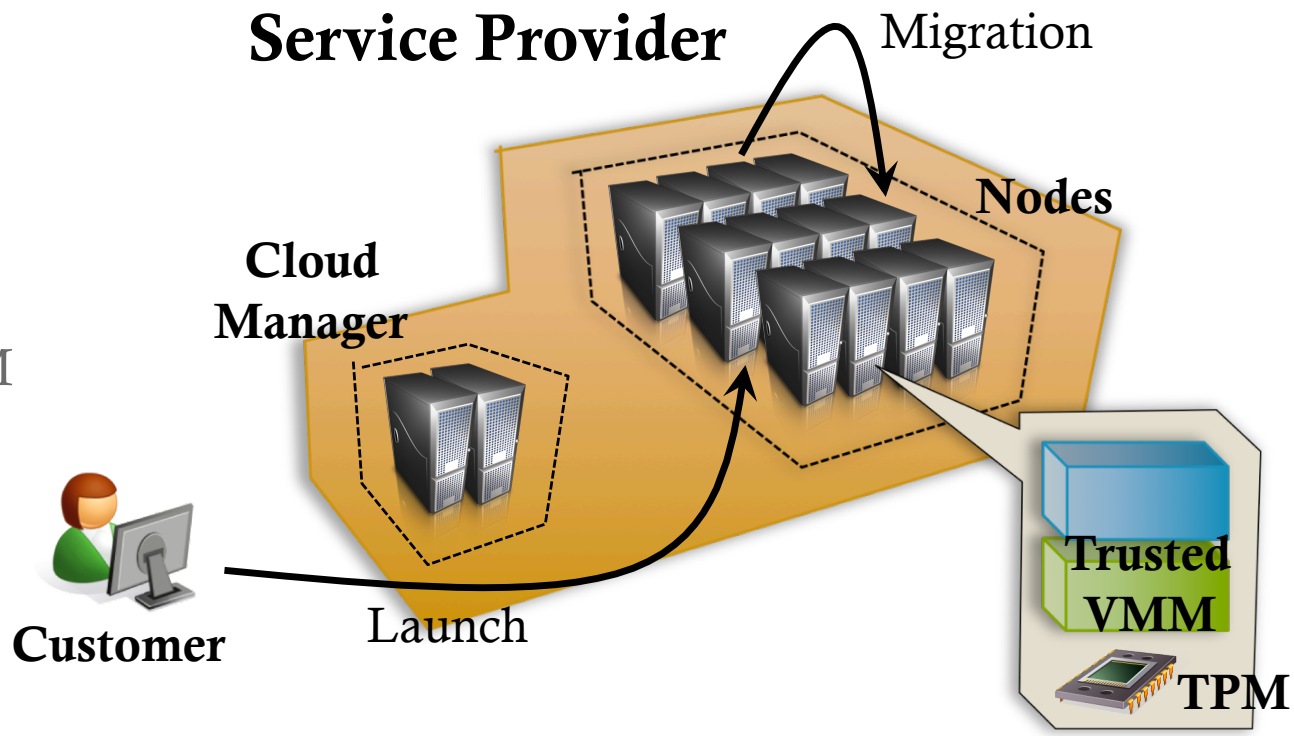
Trusted computing techniques are a good start

- Trusted computing platforms
  - Remote party can identify the software stack on host
- Trusted Platform Module (TPM)
  - Secure boot
  - Remote attestation



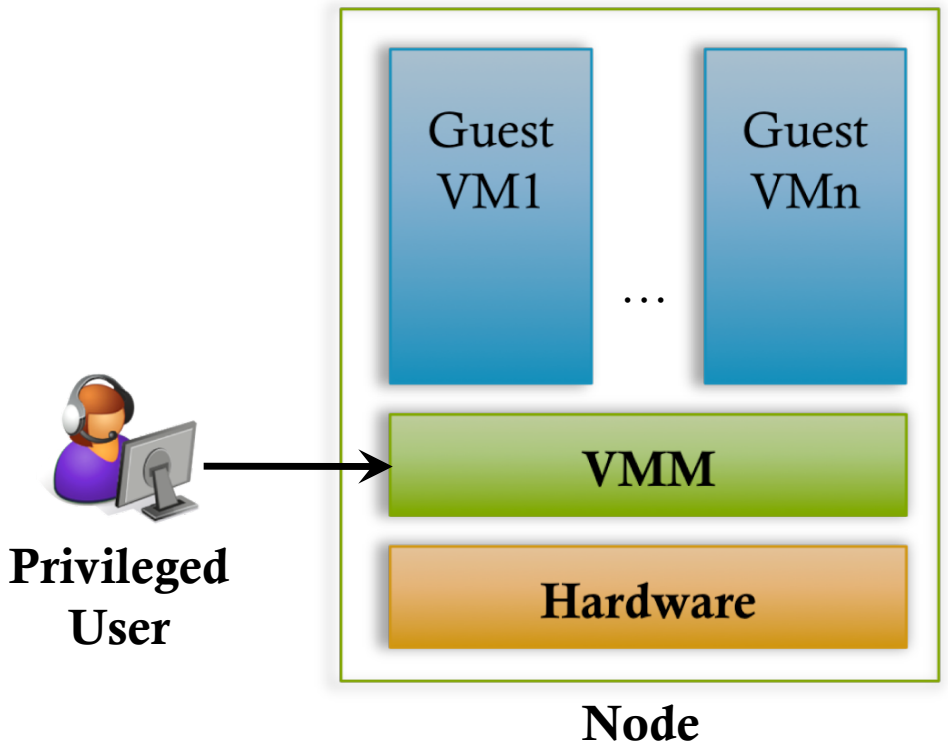
Our proposal: Trusted Cloud Computing Platform

- Trusted VMM
- Guarantee that VMs only run on nodes
  - With trusted VMM
  - Within security perimeter
- Secure launch & migration



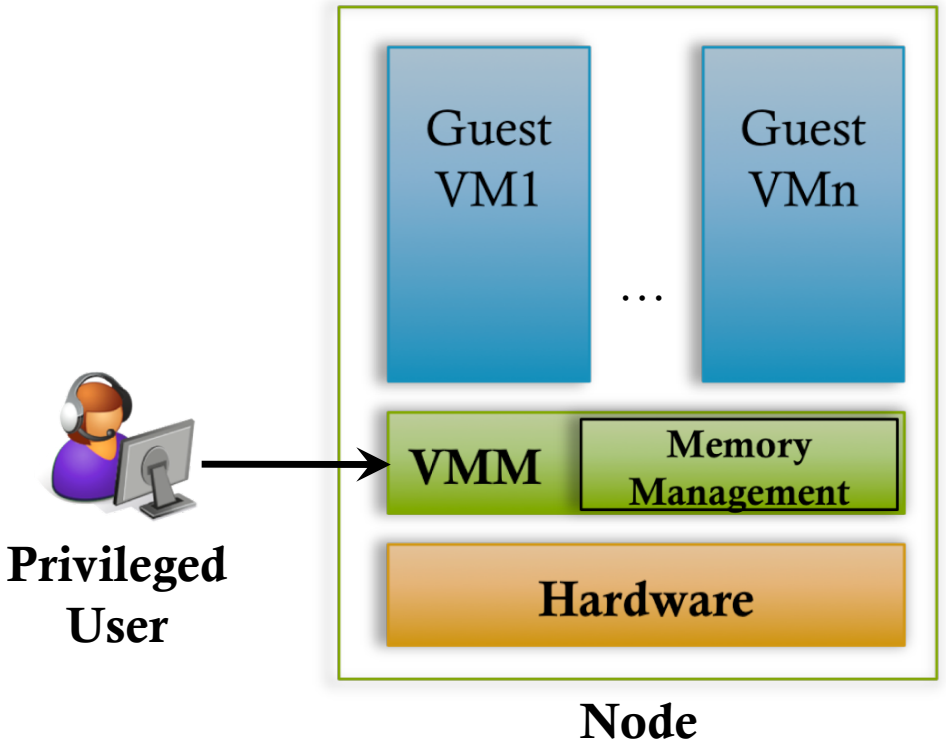
Issues with current VMMs

- No protection from privileged user
  - E.g., XenAccess
- Support operations that export VM state
  - Migration, suspension, etc.
- Large trusted computing base (TCB)



Challenges: Secure memory management

- Prevent guest VM inspection & keep TCB small
- Provide narrow interface for launching, migration, etc.
- Migration ensure destination is trusted
- Efficient
- Possible research: limit TCB to memory management



Summary: Trusted Cloud Computing Platform

- Prevent inspection of computation state at the service provider site
- Allows customers to verify that computation is secure
- Deployed with cooperation of the cloud provider

Thanks! Questions?

Contact:

Nuno Santos

nuno.santos@mpi-sws.org