Towards Trusted Cloud Computing

Authors: Nuno Santos, Krishna P. Gummadi, and Rodrigo Rodrigues
Introduction

- Creation of trust
  - Encryption
- Terra
  - Prevents owner of physical host from interfering with or inspecting a running computation
  - Determines if computation is running in a trusted environment.
  - Works on a VM running in a single host.
Trusted Cloud Computing Platform

Overview

- Provides abstraction of closed box execution environment

- Allows a user to check whether the virtual machine is running securely
Eucalyptus

- Manages 1+ clusters made of nodes running VMMs to host customers' VMs
- Cloud Manager
  - Image loaded into CM
  - Launched
  - Exports administrative tools
    - Adding/removing VMI's and users
- Xen supports live migration
Attack Model

- **Systems administrator**
  - Run user level processes at Dom0
  - Physical access
  - Single sysadmin with root privileges?
  - Assume they can login with root privileges
  - Physical access?
    - Divert the VM to a machine under their control, located outside the security perimeters.

- **TCCP must:**
  - Confine the VM execution inside the perimeter
  - Sysadmin can't access memory
"Trusted Computing"

- TPM chip
  - Endorsement private key (EK)
- Remote attestation
  - Measurement List (ML)
  - Nonce
Trusted Cloud Computing Platform

- **TVMM**
- **TC**
  - Manages set of nodes in security perimeter called trusted nodes
  - Attests to the node's platform
  - Located in ETE
- Trusted nodes must:
  - must be in security perimeter
  - run TVMM

- When to be wary:
  - Launching
  - Migration

- ETE
  - VeriSign
Node Management

TPM holds the public endorsement key of the node and the expected measurement list.

The ETE makes the public EK, ML, and indicated trusted keys all safely publicly available.
Launching a VM

User does not know which physical node the VM will be launched on and can only trust the TC

1. \{\alpha, \#\alpha\}_{K_{VM}}{n_U, K_{VM}}_{TK^{P}_{TC}}
2. \{\{n_U, K_{VM}\}_{TK^{P}_{TC}}, n_N\}_{TK^{P}_{N}}, N\}_{TK^{P}_{TC}}
3. \{n_N, n_U, K_{VM}\}_{TK^{P}_{N}}_{TK^{P}_{TC}}
4. \{n_U, N\}_{K_{VM}}
Migrating a VM

- $N_s$ - source node
- $N_d$ - destination node
- Both must be trusted
- VM state must remain confidential and unmodified
Questions?