Enabling Cloud Customers to Trust the Cloud

CSC574 – Fall 2011

(Course Project)

Ashwin Shashidharan (ashashi3)

Jitesh Shah (jhshah)

Instructor: Prof. William Enck

Motivation & Problem

- **Adoption of IaaS providers on the rise**
  - Cheap infrastructure, quick scaling up

- **What are we trusting the cloud for?**
  Protection of business critical data
  - Secure computation
  - Secure storage

- **What do we trust?**
  - Cloud provider : Limited (TCB setup & Physical security)

- **What do we protect against?**
  - Cloud provider compromise: Remote Shell (root) access to Management node.

Concepts

- **Notion of security**:
  - Avoid break-ins. Hosed if broken-in

- **Different requirements**: Need to protect data in the face of break-ins

- New technologies **enable confinement**
  - SELinux: “root” is not special. MAC access control.
  - TPM: Cannot be re-programmed even by root without presence of AuthData.

Guest VM

Guest VM

Launcher (Sandboxed)

VMM

Cloud Infrastructure

TPM

SSL-based Mutual Authentication

Data

Customer Infrastructure

But where to store the private key?!

Evaluation Approach (Attacks)

- Cannot re-program the TPM (AuthData)
- Cannot steal encryption keys. No access to SSL private key
- Cannot modify the kernel (Encrypted and HMAC-ed)
- Cannot use a customized kernel (No keys)
- No use hexdump-ing the guest Image
- Cannot attack the launcher process : SELinux sandboxing

Evaluation Approach (cont..)

- Cannot access the running guest VM from the management node – sshd on guest VM can explicitly deny that.
- Can destroy data, but cannot access – OK because there will be backups.
- Side-channel attacks : Securely clean RAM before shutting down.

Preliminary Results

- TPM seal/unseal data works. SSL private key protected.
- Kernel encryption/integrity protection done. Decryption done in Trusted Launcher.
- Need to figure out a way transfer encryption key to the Guest VM (Shared page? Fake driver?)