A Secure Cloud with Minimal Provider Trust

Today’s cloud security problems

- Massive trusted computing base (TCB) and huge attack surface
- Trust-Me model: Tenant needs to trust provider for security
- Shared hardware: vulnerability for co-location based attacks
- Fixed security: all tenants get the same security procedures provider implements
Today's Bare Metal Clouds

- Don't share machines between tenants: no co-location attacks
- Still have:
  - Large TCB & attack surface
  - "Trust-me" model
  - Fixed security
- Introduce new problems:
  - Hardware vulnerabilities is exposed to the tenants: firmware
  - Provisioning is slow
BOLTED: a new architecture for bare metal cloud

- Minimizing trust in the provider
- Supporting even the most security sensitive tenants
- Tenants can make the cost/performance/security tradeoff
- Provisioning time as fast as virtual
- Small Microservices; most can be deployed by tenants and not in TCB

---

Bare Metal Problems

- Slow Provisioning
- Large attack surface
- Trust-Me model
- Exposed hardware vulnerabilities
- Fixed Cost/security
Some terminology

- Attestation
- Trusted Platform Module (TPM)
Bolted architecture

1. Allocate a node and move it into a quarantined state where node is isolated.
2. Download bootloader and client side attestation software.
3. Attest Node’s Firmware.
4. Provision the node with tenant’s OS and applications.
5. If Attestation passes: move the node to tenant’s enclave.
6. Provision the node with tenant’s OS and applications.
7. If Attestation fails: moves the node to rejected pool.

Service Providers:
- Provisioning Service
- Attestation Service
- Isolation Service
How do we attest a node?

- Software hash measurements are stored in TPM
- Attestation client side sends these measurement to server side
- Attestation server side checks them against a whitelist
Answering different needs of different tenants

- **M2**
  - Provider’s Provisioning Service

- **Keylime**
  - Provider’s Attestation Service

- **HIL**
  - Provider’s Isolation Service

- **Ironic**
  - Tenant’s Provisioning Service

- **Keylime+**
  - Tenant’s Attestation Service

Alice

Bob

Charlie
What about the firmware?

- Legacy BIOS, UEFI, … are huge
  - Vulnerable to attacks; potentially enabling tenants to modify FW
  - No way for tenant to inspect FW
- Heads: A stripped down linux firmware
  - Small, Open source
  - Deterministically built
- Bolted works with either UEFI or Heads
  - With UEFI, download Heads as execution environment for Keylime client
  - We have burned Heads into a small number of servers
Bolted - Performance/Security tradeoff

Dell R630
20 cores - 256GB RAM

30% overhead
10% faster
Scalability

Dell M620 - 10 cores - 64GB RAM

50 seconds additional overhead
Final Thoughts

● Future Directions
  ○ We are working with the open compute project to integrate Heads
  ○ We are working with RedHat to upstream technologies (HIL, M2 and Keylime) into Foreman, Ansible Networking and Fedora.
  ○ DoD and Medical use cases.

● Feedback: We would like to get suggestions about more Use Cases

● Open issues:
  ○ Measuring other firmwares (disk, power supply, and etc.)
Concluding remarks

- Minimizing trust in the provider
- Supporting even the most security sensitive tenants
- Tenants can make the cost/performance/security tradeoff
- Provisioning time as fast as virtual
- Small Microservices; most can be deployed by tenants and not in TCB

Real implementation, portions being used in production today in the Mass Open Cloud
Open Source Code

- https://github.com/cci-moc/hil
- https://github.com/cci-moc/ims
- https://github.com/mit-ll/python-keylime
- https://github.com/osresearch/heads
Panel kick off slide: Bolted

M2
Provider’s Provisioning Service

Keylime
Provider’s Attestation Service

Keylime+
Tenant’s Provisioning Service

Ironic
Tenant’s Provisioning Service

Provider’s Isolation Service

Tenant’s Attestation Service

Alice

Bob

Charlie
: Secure Boot of a node

Airlock Network

Standard Booting  Network Booting  Attestation

Tenant Enclave

Provisioning
Implementation - Stock UEFI

1. Moving to Airlock
2. Power cycle

TIME

HIL

OS + Applications running Kernel Boot Tenant Script

Keylime

Client

Power On BootGuard

stock UEFI

iPXE

PXE

TFTP Server

HTTP Server

Attestation Ack

Kernel image + script

Moving to Tenant Enclave

M2

Ping Request

Ping Ack

Provisioning

Heads

Node Verification Request

TPM

Measurements

Standard Booting

Network Booting

Attestation

Provisioning

Network Booting

Attestation

Provisioning
Implementation - Burned Heads

1. Moving to Airlock
2. Power cycle

TIME

HIL

Power On → BootGaurd

HTTP Server → Keylime Server → Kernel Boot

Keylime Client

Kernel image + script

Attestation Ack

Moving to Tenant Enclave

Node Verification

TPM Measurements

Provisioning

OS + Applications running

Standard Booting

Attestation

Provisioning
Implementation - Stock UEFI

1. Moving to Airlock
2. Power cycle

Airlock Network

- Power On
- Bootguard
- stock UEFI
- PXE
- iPXE
- iPXE Server
- HTTP Server
- Keylime Server
- Keylime Client
- Kernel image + script
- Tenant Enclave
- Moving to Tenant Enclave
- Ping Ack
- Provisioning
- Node Verification
- Kernel Boot
- OS + Applications running

Tenant Enclave

- Kernel Guard
- Tenant Script
- Heads
- TPM
- Measurements
Using Microservices to Reduce Attack Surface

- HIL has 3000 LoC
- M2 has 3500 LoC
- Keylime has less than 7000 LoC including server and client sides
Bolted system with more security

- We are measuring Bolted with secure deployment of real applications:
  - Network encryption
  - Remote Disk encryption & Memory scrubbing
  - Continuous attestation