Securing Bare Metal Clouds

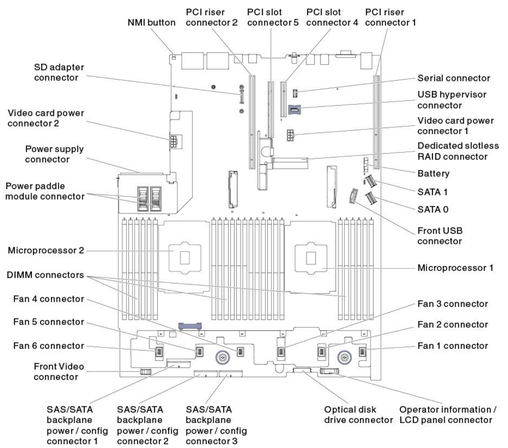
Jason Hennessey[1], Nabil Schear[2], Trammell Hudson[3], Orran Krieger[1], Gerardo Ravago[1], Kyle Hogan[1], Ravi S. Gudimetla[4], Larry Rudolph[3], Mayank Varia[1], Peter Desoyers[4], and Manuel Egele[1]

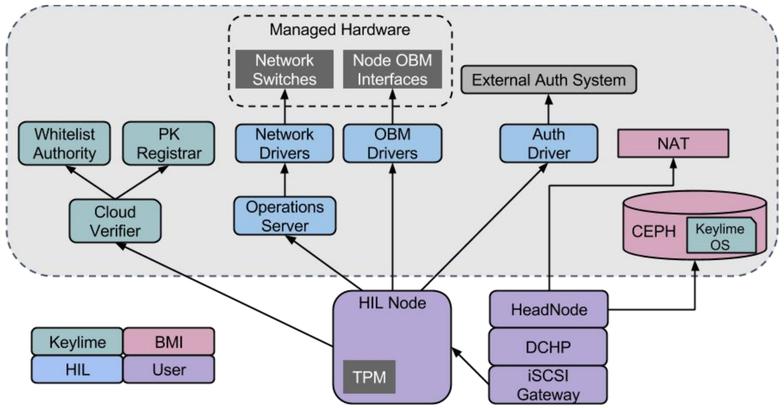
Bare Metal Clouds & Trusted Hardware

Bare metal nodes provide performance and privacy advantages over virtual machines, but the direct hardware access they give opens up new attack vectors that must be addressed.

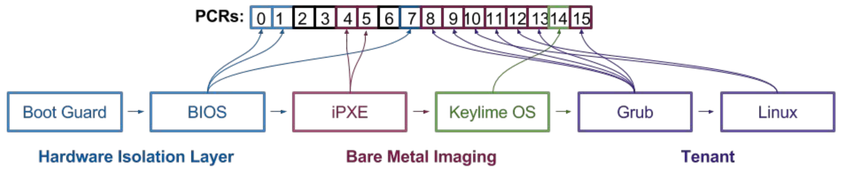
As a mitigation, we demonstrate a complete chain of measurements rooted in a hardware TPM. A user is then able to attest to the boot time integrity of their node.

This removes the need for much of the trust that traditional clouds require tenants to place in the provider and their fellow clients.





Interactions of HIL, BMI, and Keylime with tenant nodes



Arrows indicate the PCR in which each component is measured

Hardware Isolation Layer (HIL)

- provides clusters of bare metal machines to tenants
- network separation isolates tenant's machines from those belonging to other tenants

BMI

- provides images to bare metal nodes and PXE boots them

Keylime

- provides an attestation infrastructure for the trusted computing layer
- novel key bootstrapping protocol rooted in hardware identities
- tenants are able to verify the integrity of their provisioned node before enabling higher level security services using whitelist authority

PCR	Usage	PCR	Usage
0	S-CRTM, BIOS, Host Platform Extensions	8	TrustedGRUB2 kernel (diskboot.img)
1	Host Platform Configuration	9	TrustedGRUB2 kernel (core.img)
2	Option ROM Code	10	GRUB Loader Measurements (Linux Kernel)
3	Option ROM Configuration	11	GRUB Commands
4	IPL Code	12	LUKS-header
5	IPL Code Configuration and Data	13	GRUB Modules
6	State Transitions and Wake Events	14	Keylime OS
7	Host Platform Manufacturer Specific	15	TrustedGRUB2 MBR (boot.img)

Threat Model

- Bare metal clouds expose the tenant to new attack vectors:
  - Embedded firmwares run early in the boot sequence (BIOS), are rarely updated, difficult to inspect, and persist between tenants
  - Tenants could flash malware into the firmware of a machine before returning it to the pool, affecting all future users of the machine
  - Any persistent state left on a machine by a tenant can be exploited by future attackers seeking to scrape secrets from disk or memory

Chain of Trust

- prior component measures each subsequent link in the chain before chainloading into it
- measurements are stored inside the PCRs of the TPM
- contents of TPM can be queried and signed with a hardware rooted key (EK)
- tenant can fetch known good PCRs and the public signing key for the node to compare the PCR values and validate the signature.

Future Directions

- adapt current Keylime architecture to be bootable OS
- increase the amount of firmware that is measurable
- open source, minimal firmware
  - even measured firmware can contain bugs/backdoors
  - proprietary firmware stops receiving updates before product end of life
  - open source firmware is auditable & can be updated by community effort

1. Boston University , 2. MIT Lincoln Laboratory, 3. Two Sigma, 4. Northeastern

http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.5462.doc/c_internal_connectors.html