A Secure Cloud with Minimal Provider Trust

Amin Mosayyebzadeh, G. Ravago, A. Mohan, A. Raza, S. Tikale, N. Schear, T. Hudson, J. Hennessey, N. Ansari, K.Hogan, C. Munson, L. Rudolph, G. Cooperman, P. Desnoyers, O. Krieger











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

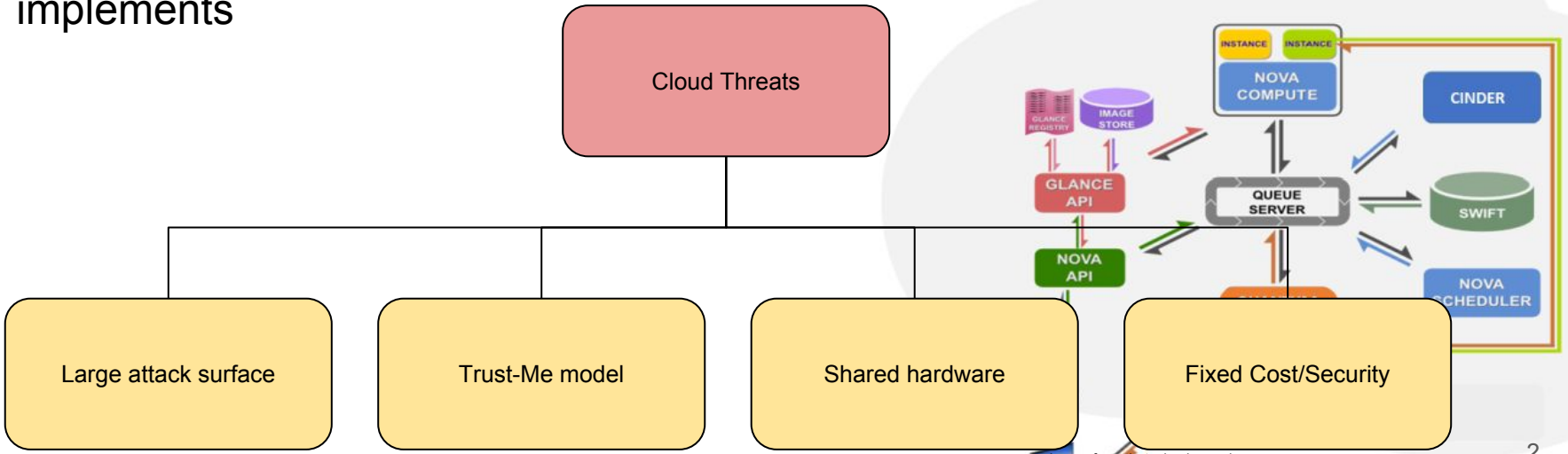
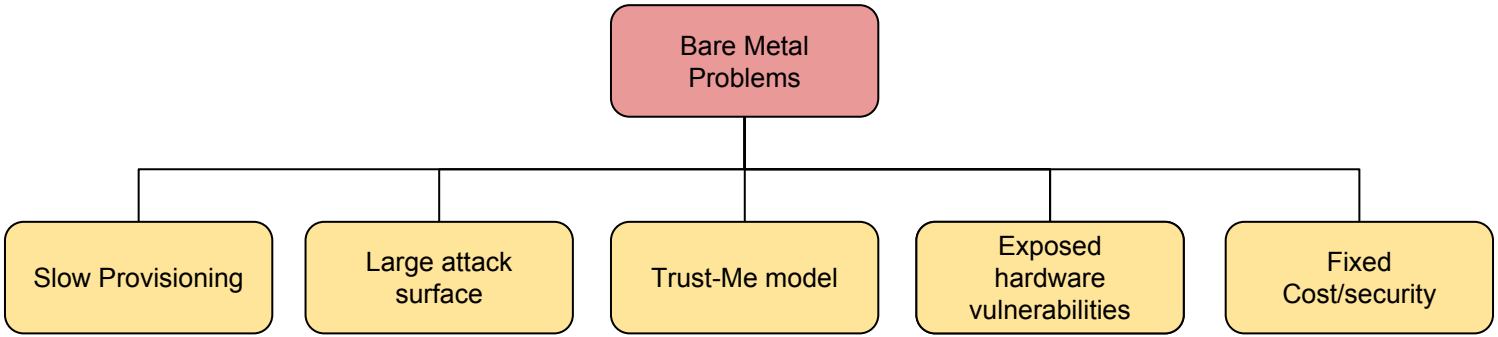


Image from thetechsolo.wordpress.com

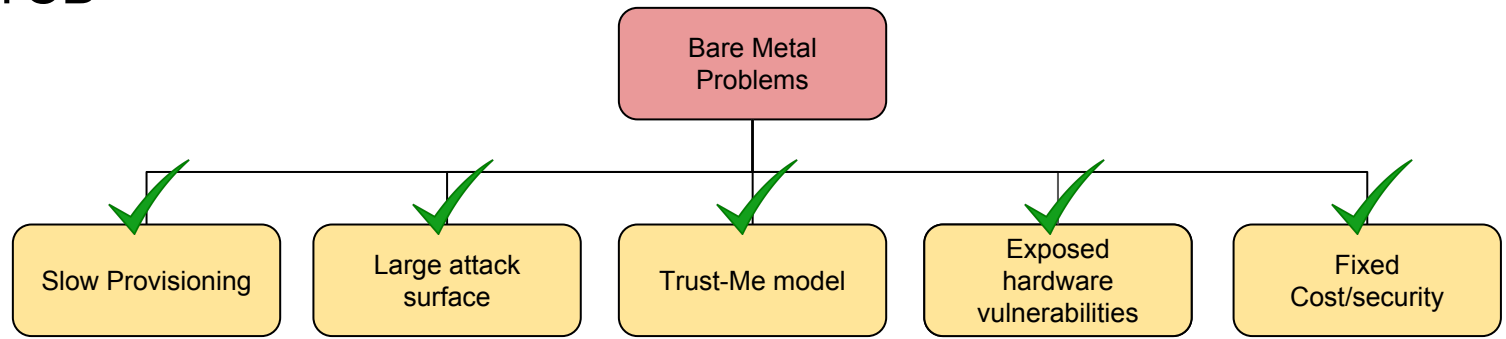
Today's Bare Metal Clouds

- 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

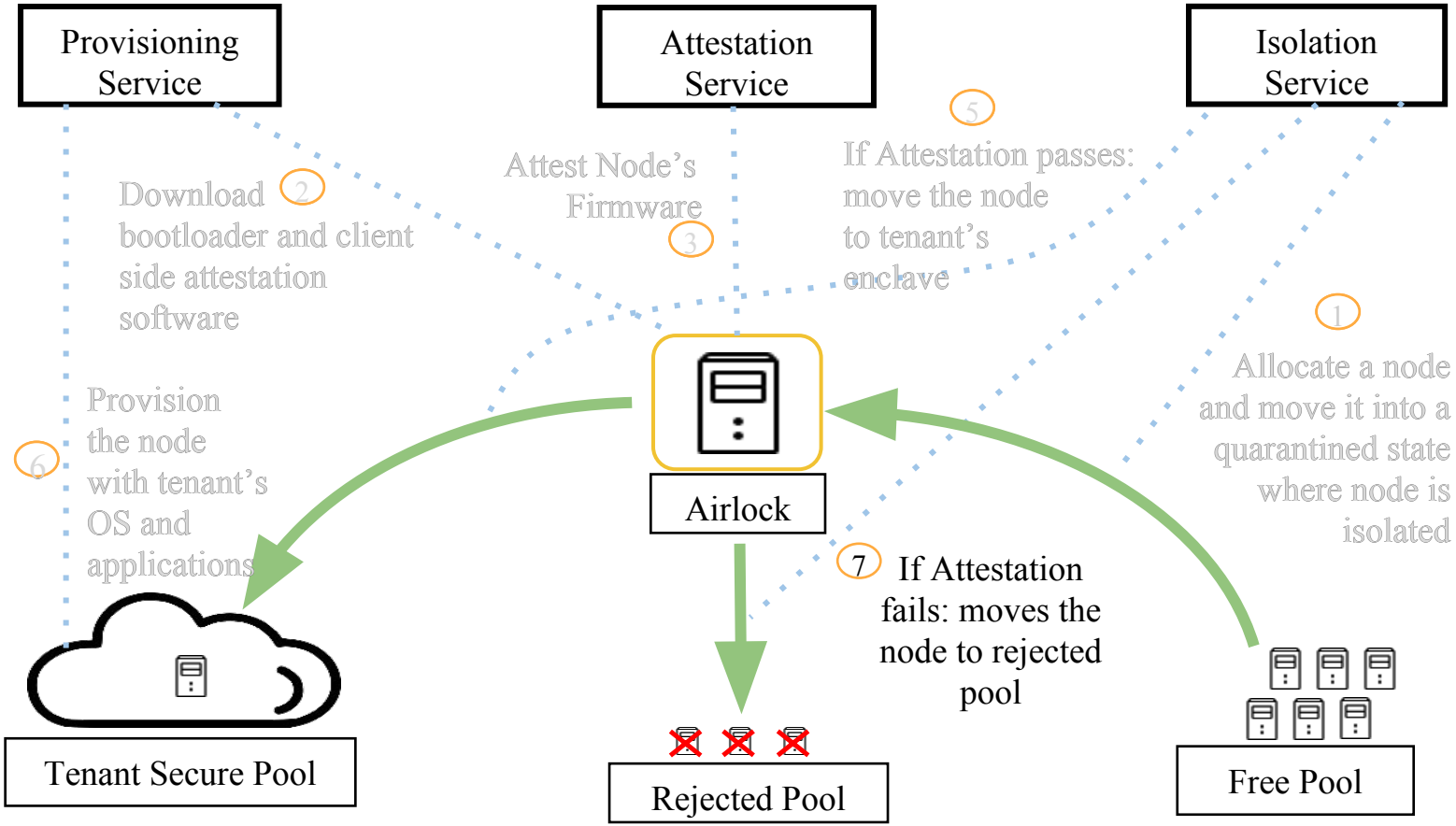
- Minimizing trust in the provider
- Supporting even the most security sensitive tenants
- Tenants can make the cost/performance/security tradeoff
- Provisioning time as fast as virtual
- Small Microservices; most can be deployed by tenants and not in TCB



Some terminology

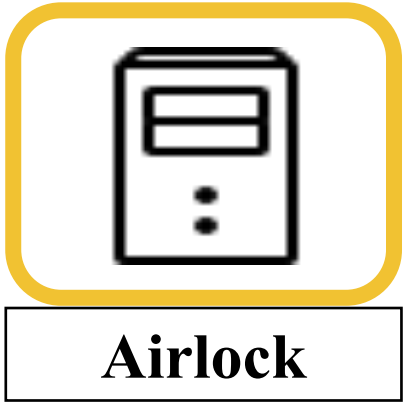
- Attestation
- Trusted Platform Module (TPM)

Bolted architecture

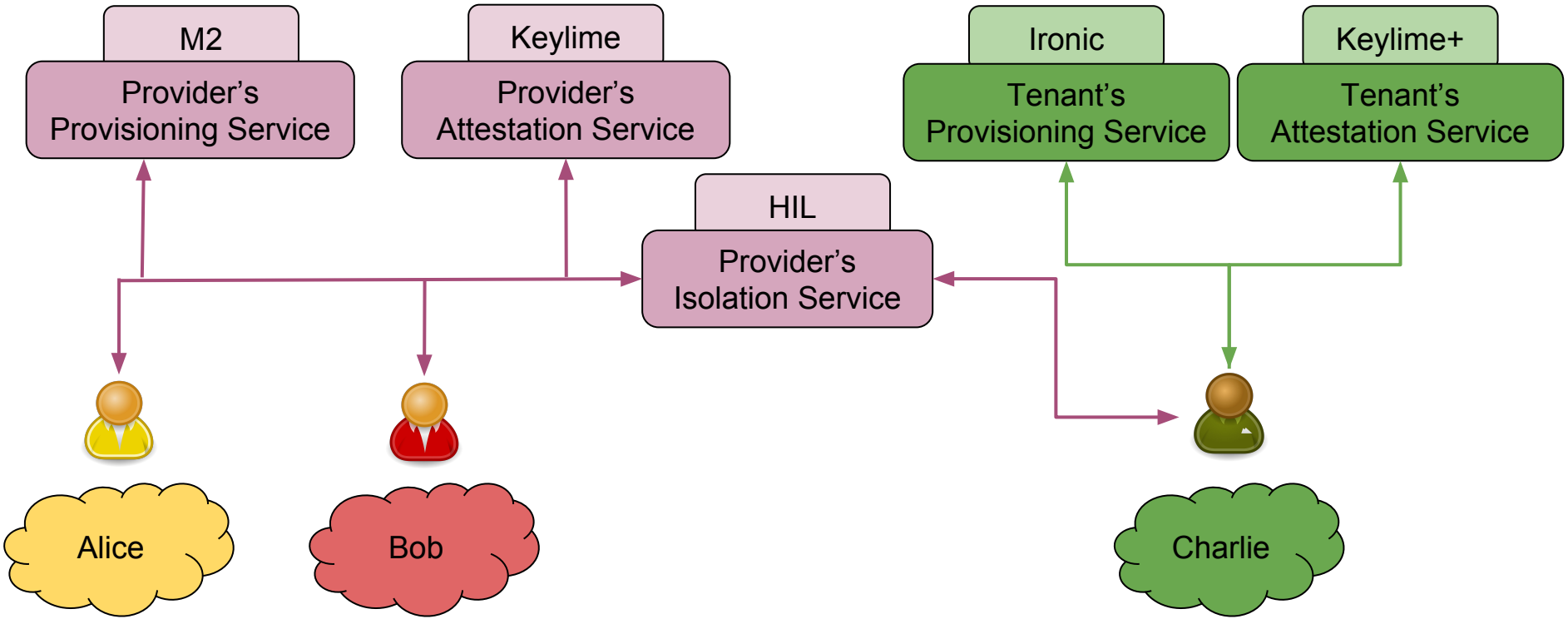


How do we attest a node?

- Software hash measurements are stored in TPM
- Attestation client side sends these measurement ro server side
- Attestation server side check them against a whitelist

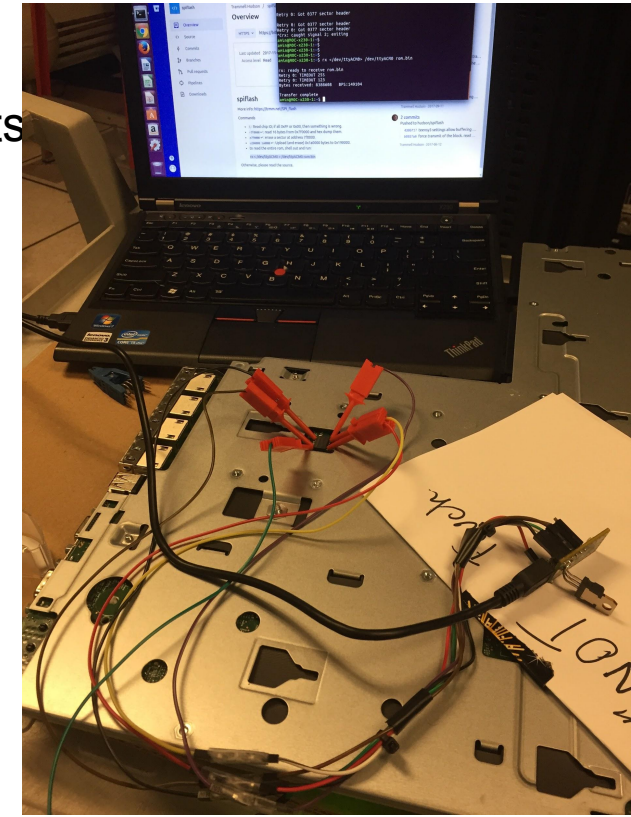


Answering different needs of different tenants



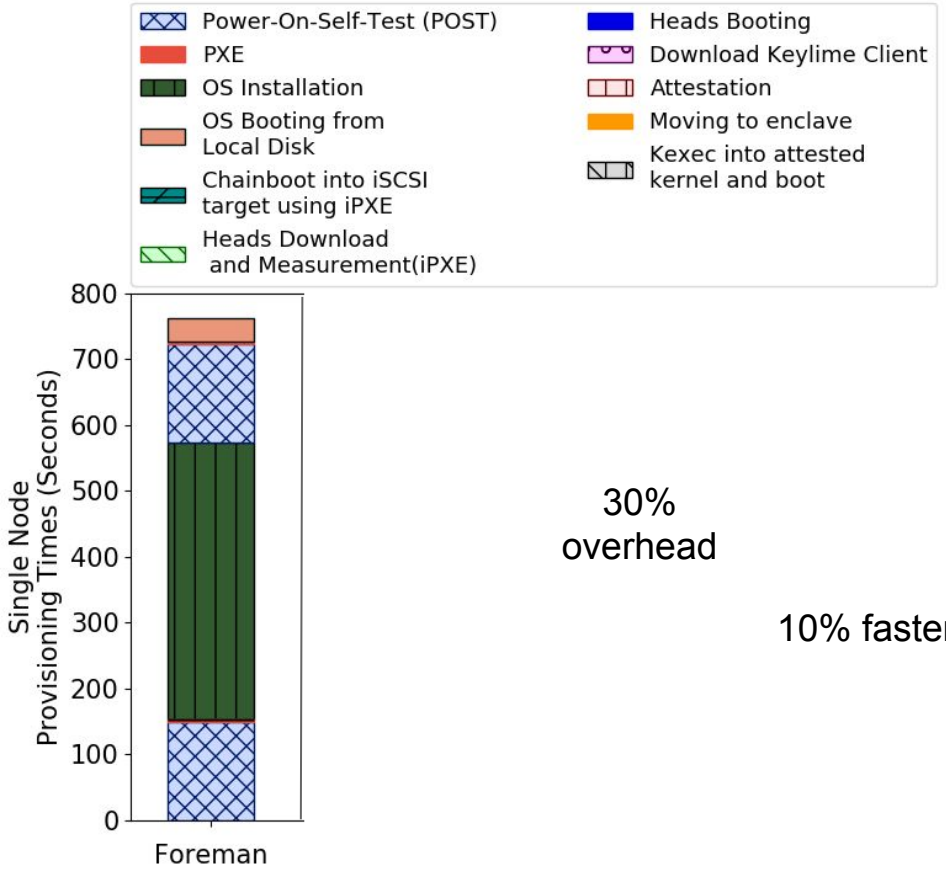
What about the firmware?

- 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

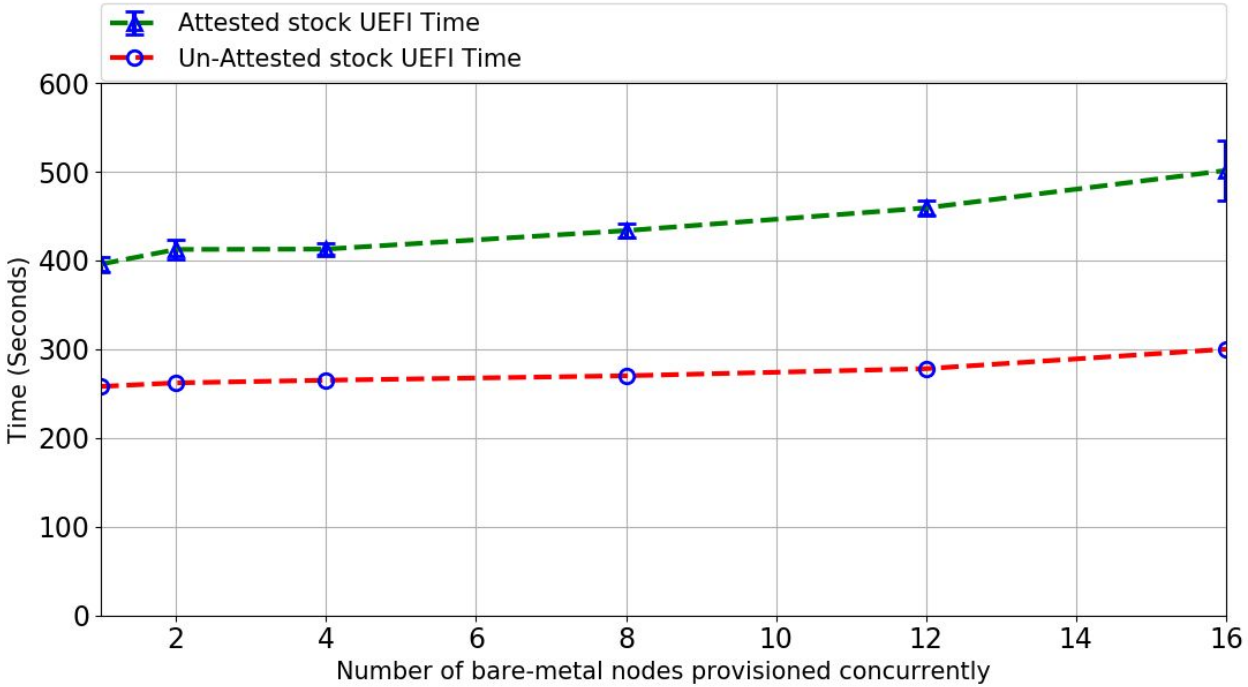
Dell R630
20 cores - 256GB RAM



30% overhead

10% faster

Scalability



50 seconds additional overhead

Dell M620 - 10 cores - 64GB RAM

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

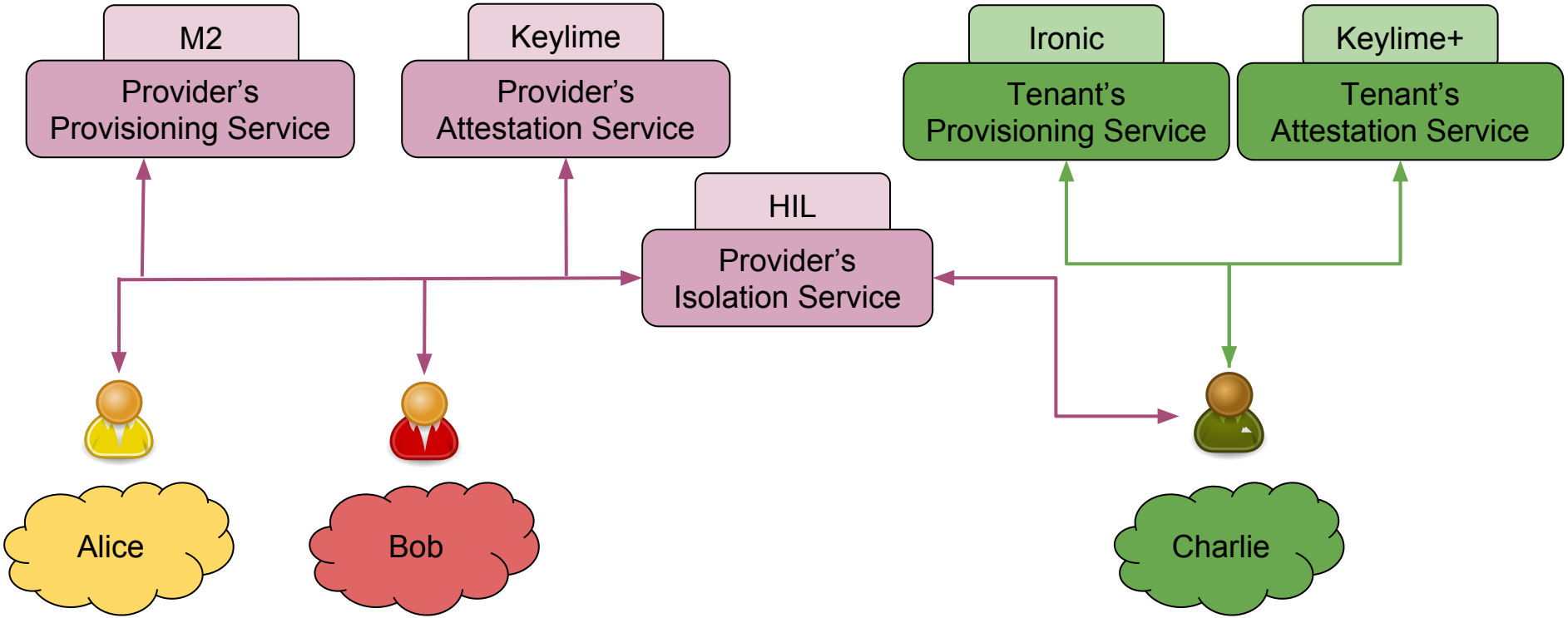
- Minimizing trust in the provider
- Supporting even the most security sensitive tenants
- Tenants can make the cost/performance/security tradeoff
- Provisioning time as fast as virtual
- Small Microservices; most can be deployed by tenants and not in TCB

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

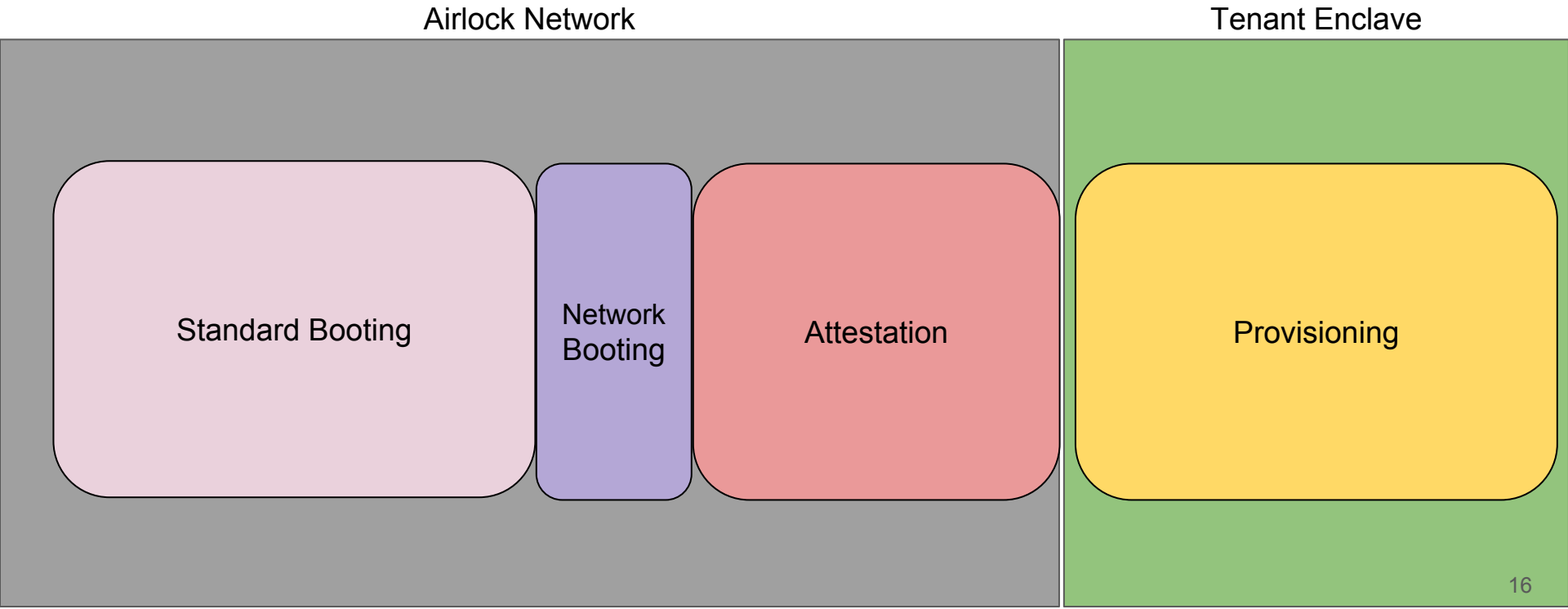
Open Source Code

- https://github.com/cci-moc/hil
- https://github.com/cci-moc/ims
- https://github.com/mit-ll/python-keylime
- https://github.com/osresearch/heads

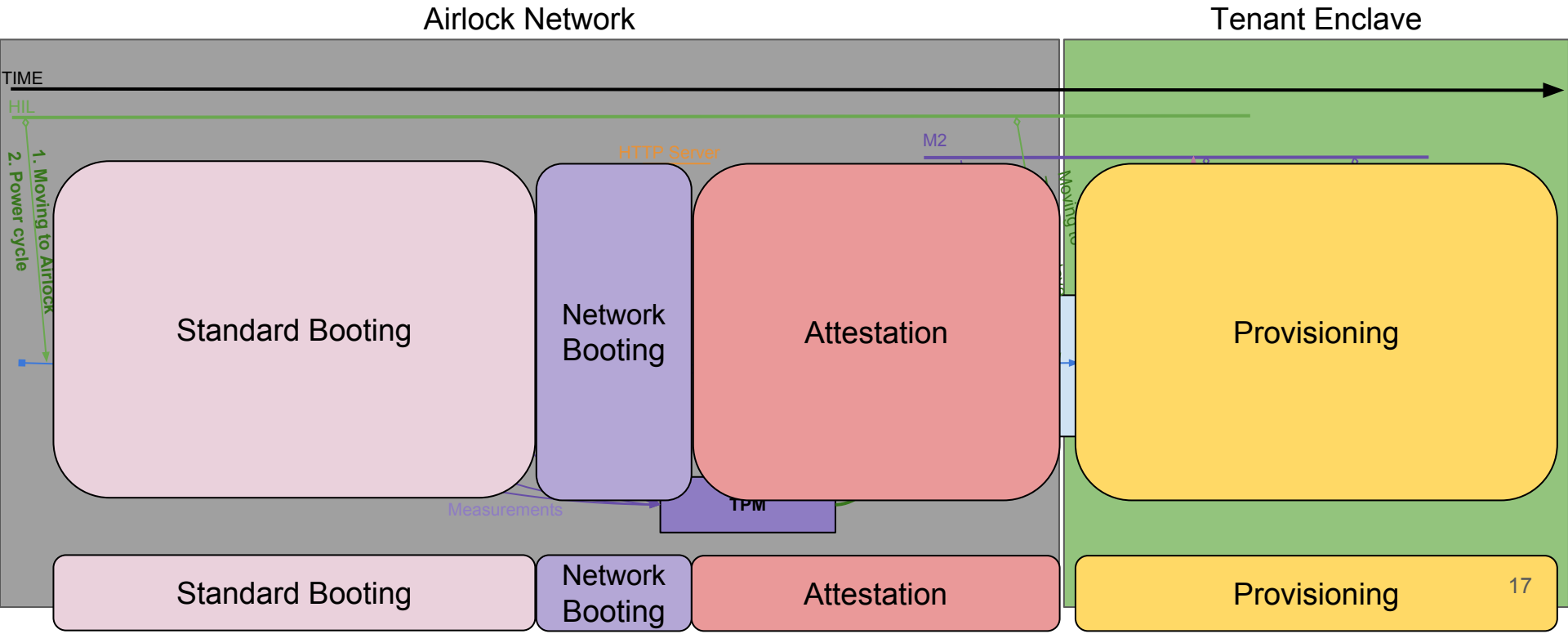
Panel kick off slide: Bolted



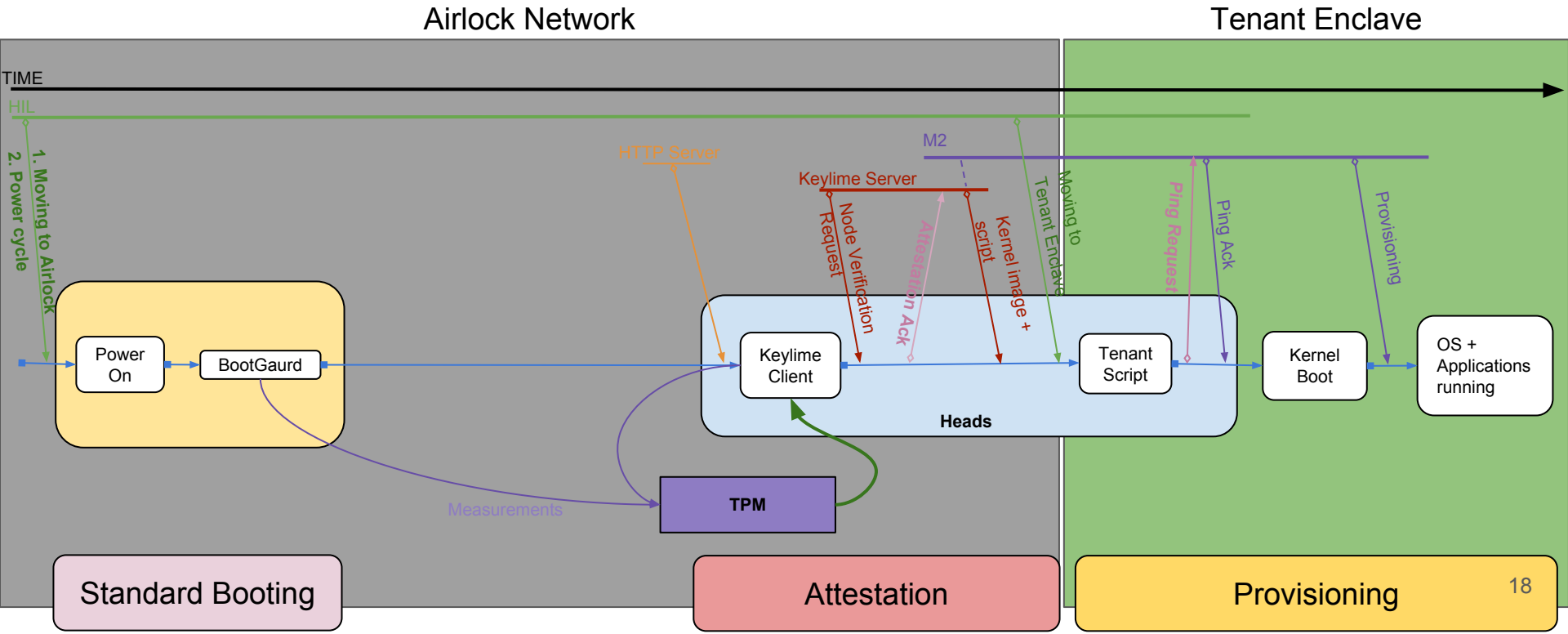
: Secure Boot of a node



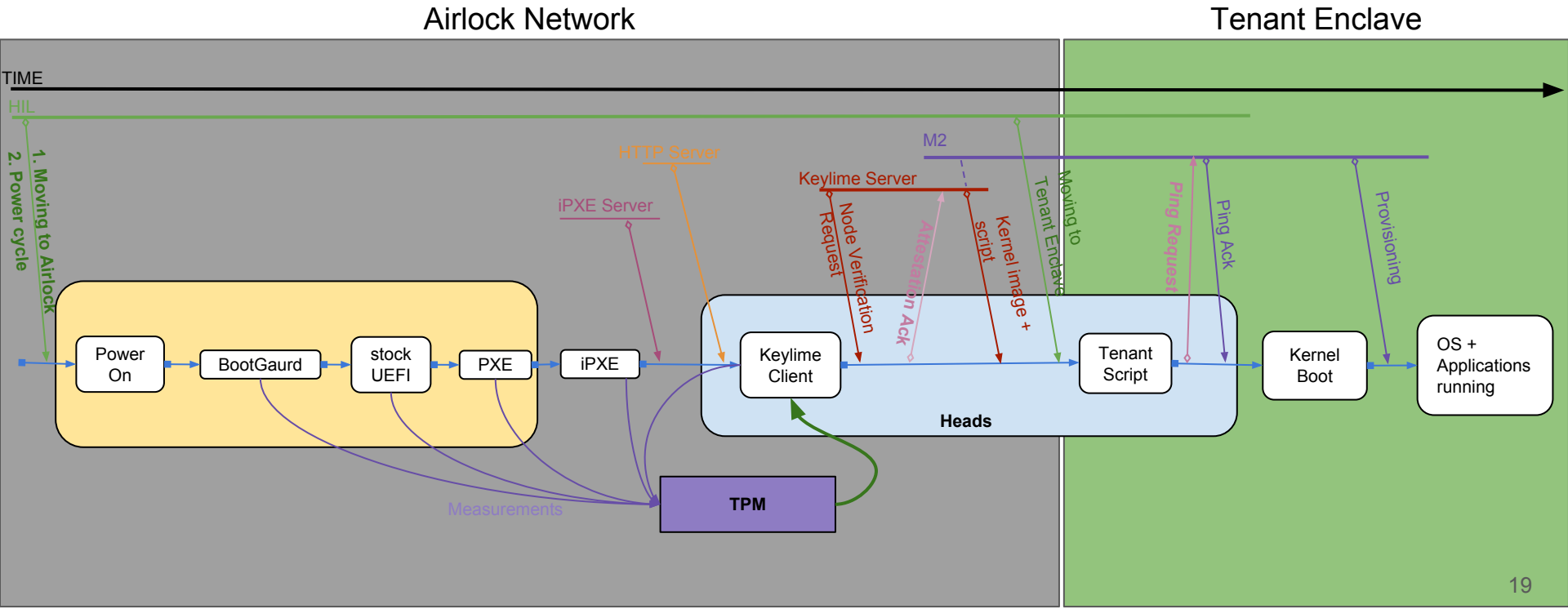
Implementation - Stock UEFI



Implementation - Burned Heads



Implementation - Stock UEFI



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

