Supporting Security-Sensitive Tenants in a Bare-Metal Cloud*#

NOTE: We define security-sensitive tenants as entities, like three letter government agencies or hospitals, who are both willing to pay a significant price for security and that have the expertise, desire, or requirement to trust their own security arrangements.

Amin Mosayyebzadeh¹, Apoorve Mohan⁴, Sahil Tikale¹, Mania Abdi⁴, Nabil Schear², Charles Munson², Trammell Hudson³, Larry Rudolph³, Gene Cooperman⁴, Peter Desnoyers⁴, Orran Krieger¹

Boston University¹ MIT Lincoln Laboratory² Two Sigma³ Northeastern University⁴ (Massachusetts Open Cloud)

*Mosayyebzadeh, Mohan, and Tikale contributed equally.

#DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited. This material is based upon work supported by the Under Secretary of Defense for Research and Engineering Under Air Force Contract No. FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Under Secretary of Defense for Research and Engineering.
Security-Sensitive Organizations Detest Public Cloud Offerings
Problems with Existing Cloud Offerings

A. A Virtualization-based offering is prone to side-channel, covert-channel, hyperjacking, etc.
Problems with Existing Cloud Offerings

B. Cloud orchestration softwares have huge trusted computing base (TCB) and hence a massive attack surface.
C. **Limited visibility and control over implementation and operation** - tenants need to trust non-maliciousness and competence of the provider.
Problems with Existing Cloud Offerings

D. Adheres to one-size-fits-all security solutions for operational efficiency
Problems with Existing Cloud Offerings

Bare-Metal clouds overcome the problems faced by virtualized offerings but are prone to firmware-based attacks and data theft and still possess other public cloud problems (B, C, and D).

Data Centre → Cloud

After IBM SoftLayer fails to scrub bare-metal box firmware of any lurking spies, alarm raised over cloud server security

Don't just grin and bare it: Check your provider wipes mobo before redeployment

Bare metal cloud servers are vulnerable to attack: Eclypsium

By David Heath

Research by security firm Eclypsium shows that vacated cloud servers are not properly wiped by hosting providers and may be used as an intrusion channel by bad actors.
Is is Possible to Architect a Cloud that…

- Is appropriate for even the most security-sensitive tenants?
- Doesn’t require the tenants to fully trust the provider?
- Doesn’t impact tenants with less stringent security requirements or who are willing to trust the provider for their security?
Is appropriate for even the most security-sensitive tenants?

Doesn’t require the tenants to fully trust the provider?

Doesn’t impact tenants with less stringent security requirements or who are willing to trust the provider for their security?
Bolted: An Architecture for Secure Bare-Metal Cloud Service

- Microservice-based Architecture
  - Tailor-Made Security Solution for Each Tenant
  - Minimal Trusted Computing Base (TCB)
  - Improved Visibility and Control
Bolted: An Architecture for Secure Bare-Metal Cloud Service

Microservice-based Architecture
- Tailor-Made Security Solution for Each Tenant
- Minimal Trusted Computing Base (TCB)
- Improved Visibility and Control

Operational Efficiency vs Trust
- Security-sensitive tenants can deploy most of the microservices.
- Tenants who trust the provider can simply rely on the provider for all the microservices.
Bolted: An Architecture for Secure Bare-Metal Cloud Service

Security-sensitive tenants only need to trust the network isolation service.

- Microservice-based Architecture
  - Tailor-Made Security Solution for Each Tenant
  - Minimal Trusted Computing Base (TCB)
  - Improved Visibility and Control

~3K LOC for Bolted Prototype

Most of the microservices can be implemented by the tenant.
Bolted: An Architecture for Secure Bare-Metal Cloud Service

- Microservice-based Architecture
  - Tailor-Made Security Solution for Each Tenant
  - Minimal Trusted Computing Base (TCB)
  - Improved Visibility and Control

Tenant Implemented and Verifiable Components

Example
- Firmware
- Attestation Service
- Key Management

LinuxBoot
Prototype Evaluation

Speed, Performance, and Scalability
Supporting Security-Sensitive Tenants in a Bare-Metal Cloud

Track II (Security #2: Isolation)
Date: Thursday, July 11, 2019
Time: 2:00 pm–3:20 pm