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 Mosayyebzadeh[1], **Apoorve Mohan**[4], Sahil Tikale[1], Mania Abdi[4], Nabil Schear[2], Charles Munson[2], Trammell Hudson[3], Larry Rudolph[3], Gene Cooperman[4], Peter Desnoyers[4], Orran Krieger[1]

Boston University[1] MIT Lincoln Laboratory[2] Two Sigma[3] Northeastern University[4]

(Massachusetts Open Cloud)

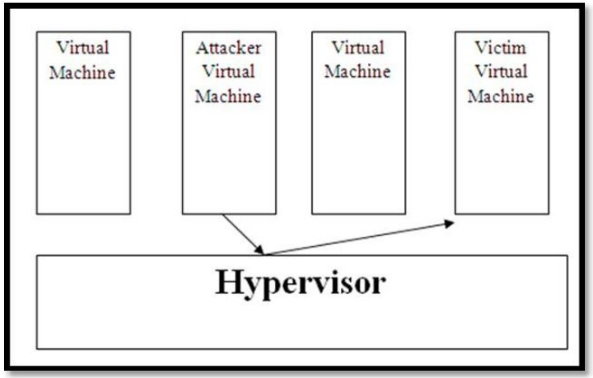
*Mosayyebzadeh, Mohan, and Tikale contributed equally.

#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

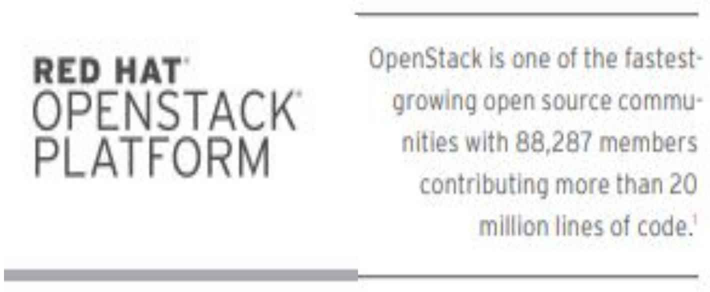
Problems with Existing Cloud Offerings

A. A Virtualization-based offering is prone to side-chanel, covert-channel, hyperjacking, etc.



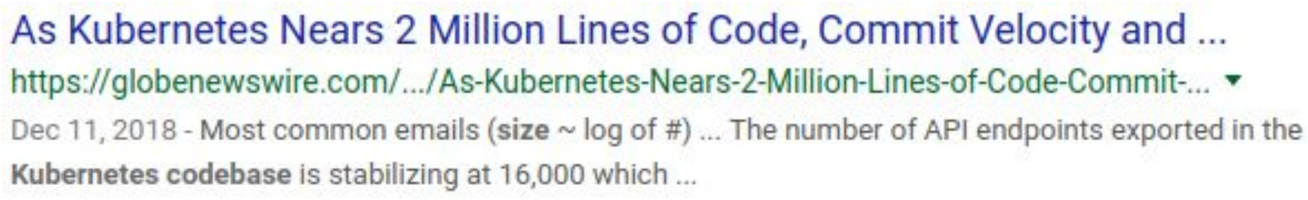
Problems with Existing Cloud Offerings

B. Cloud orchestration softwares have huge trusted computing base (TCB) and hence a massive attack surface



RED HAT OPENSTACK PLATFORM

OpenStack is one of the fastest-growing open source communities with 88,287 members contributing more than 20 million lines of code.[1]



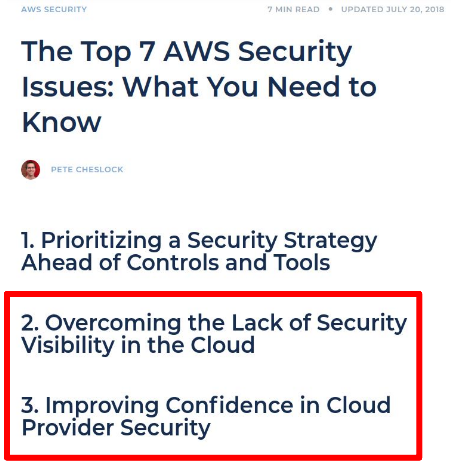
As Kubernetes Nears 2 Million Lines of Code, Commit Velocity and ...

https://globenewswire.com/.../As-Kubernetes-Nears-2-Million-Lines-of-Code-Commit-... ▾

Dec 11, 2018 - Most common emails (**size** ~ log of #) ... The number of API endpoints exported in the **Kubernetes codebase** is stabilizing at 16,000 which ...

Problems with Existing Cloud Offerings

C. Limited visibility and control over implementation and operation - tenants needs to trust non-maliciousness and competence of the provider



AWS SECURITY

7 MIN READ • UPDATED JULY 20, 2018

The Top 7 AWS Security Issues: What You Need to Know

PETE CHESLOCK

1. Prioritizing a Security Strategy Ahead of Controls and Tools

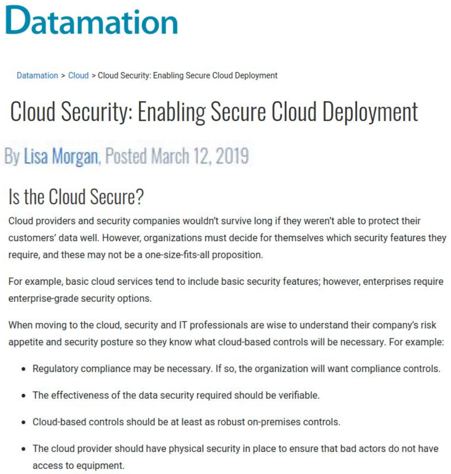
2. Overcoming the Lack of Security Visibility in the Cloud

3. Improving Confidence in Cloud Provider Security

Problems with Existing Cloud Offerings

D. Adheres to one-size-fits-all security solutions for operational efficiency

Why the Cloud Cannot be treated as a One-size-fits-all when it comes to Security


Datamation

Datamation > Cloud > Cloud Security: Enabling Secure Cloud Deployment

Cloud Security: Enabling Secure Cloud Deployment

By Lisa Morgan, Posted March 12, 2019

Is the Cloud Secure?

Cloud providers and security companies wouldn't survive long if they weren't able to protect their customers' data well. However, organizations must decide for themselves which security features they require, and these may not be a one-size-fits-all proposition.

For example, basic cloud services tend to include basic security features; however, enterprises require enterprise-grade security options.

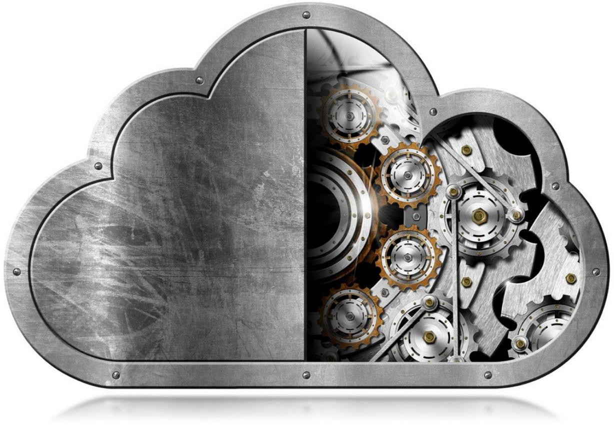
When moving to the cloud, security and IT professionals are wise to understand their company's risk appetite and security posture so they know what cloud-based controls will be necessary. For example:

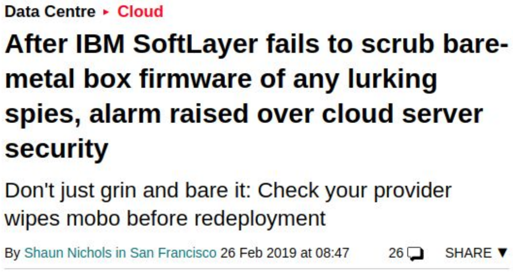
- Regulatory compliance may be necessary. If so, the organization will want compliance controls.
- The effectiveness of the data security required should be verifiable.
- Cloud-based controls should be at least as robust on-premises controls.
- The cloud provider should have physical security in place to ensure that bad actors do not have access to equipment.

Cloud Security Does one size fits all - YouTube
https://www.youtube.com/watch?v=f5QaP8GBahQ
Jun 29, 2017 - Uploaded by MetricStream

Problems with Existing Cloud Offerings

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



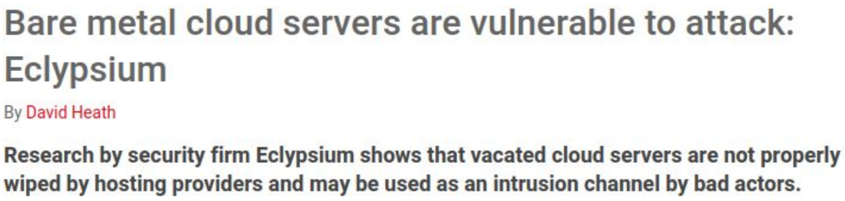


Data Centre ▸ Cloud

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

By Shaun Nichols in San Francisco 26 Feb 2019 at 08:47 26 SHARE ▼



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.

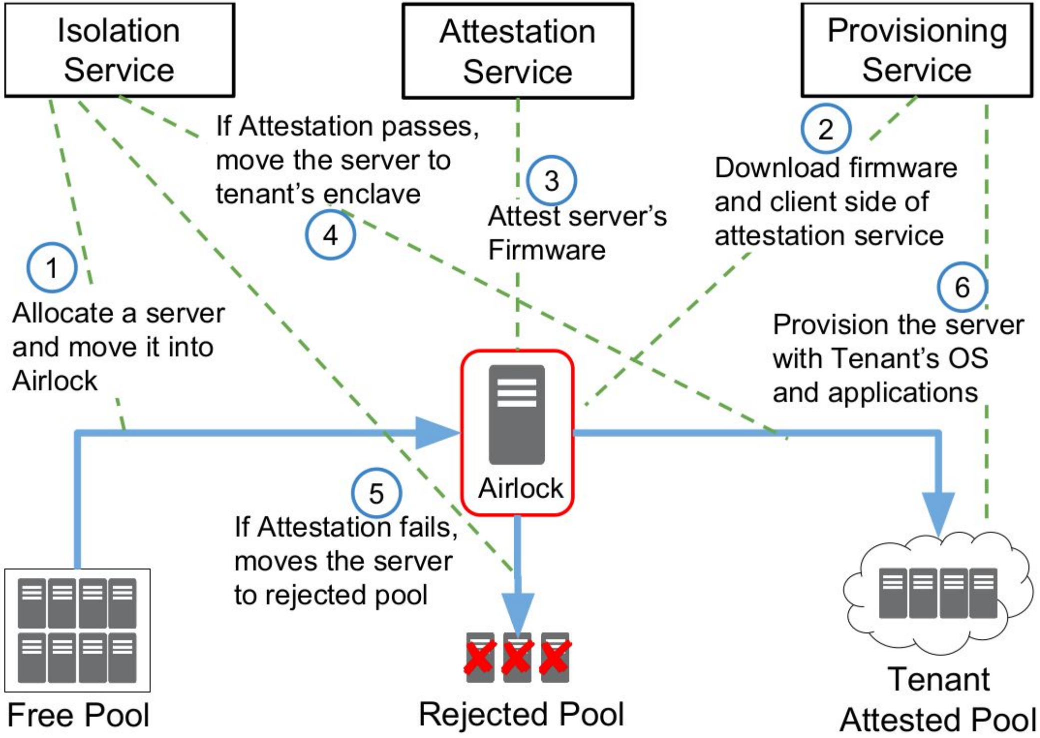
Is is Possible to Architect a Cloud that…

❑ 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?

Bolted: An Architecture for Secure Bare-Metal Cloud Service


Isolation Service
Attestation Service
Provisioning Service
1
Allocate a server and move it into Airlock
2
Download firmware and client side of attestation service
3
Attest server's Firmware
4
If Attestation passes, move the server to tenant's enclave
5
If Attestation fails, moves the server to rejected pool
6
Provision the server with Tenant's OS and applications
Airlock
Free Pool
Rejected Pool
Tenant Attested Pool

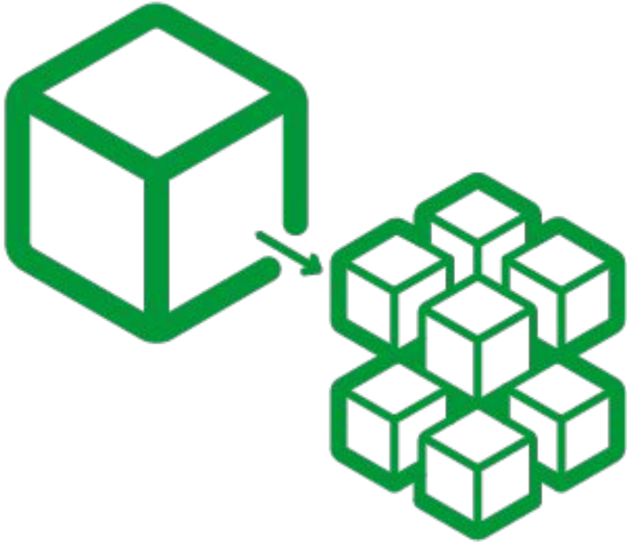
Bolted: An Architecture for Secure Bare-Metal Cloud Service

❑ Microservice-based Architecture

  ○ Tailor-Made Security Solution for Each Tenant

  ○ Minimal Trusted Computing Base (TCB)

  ○ Improved Visibility and Control

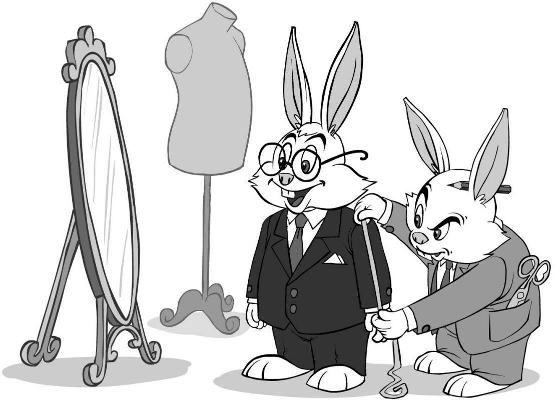


Bolted: An Architecture for Secure Bare-Metal Cloud Service

- 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 reply of provider for all the microservices.

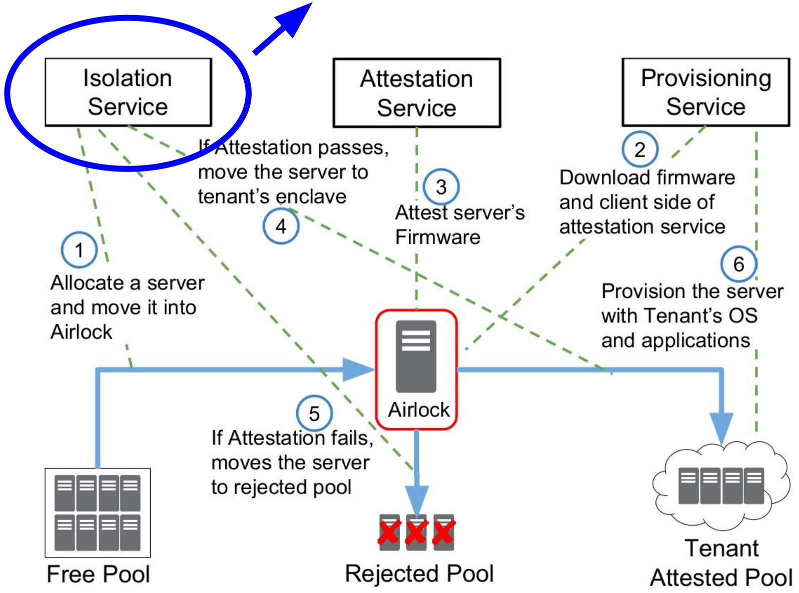


Bolted: An Architecture for Secure Bare-Metal Cloud Service

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

~3K LOC for Bolted Prototype

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



1 Allocate a server and move it into Airlock

2 Download firmware and client side of attestation service

3 Attest server's Firmware

4 If Attestation passes, move the server to tenant's enclave

5 If Attestation fails, moves the server to rejected pool

6 Provision the server with Tenant's OS and applications

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

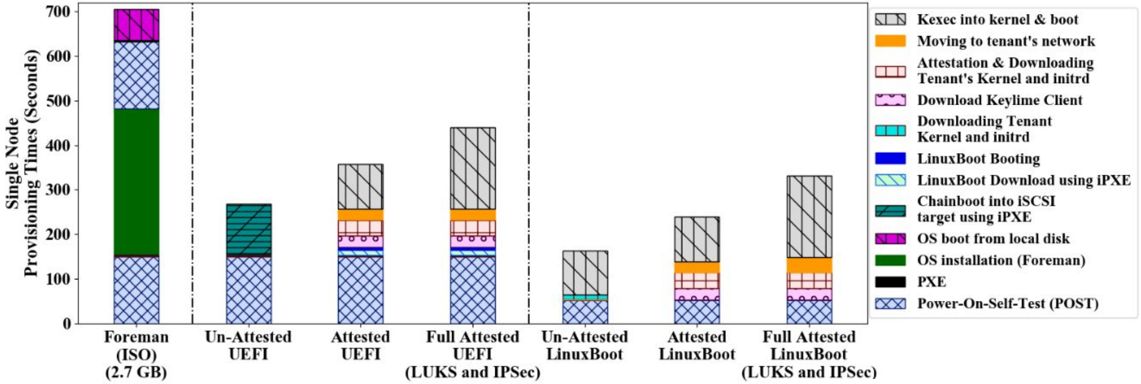
Example

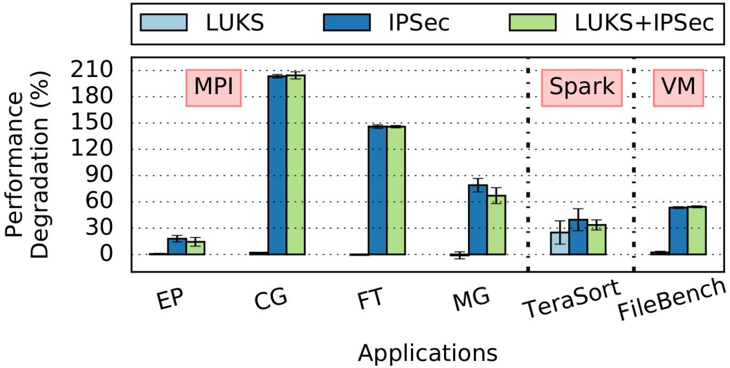
- Firmware
- Attestation Service
- Key Management

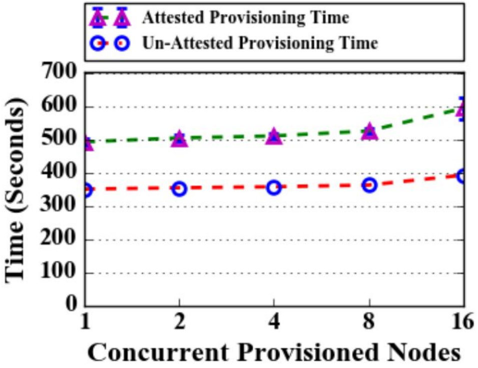
LinuxBoot

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