Creating Isolation in the Cloud

Nabil Schear
nabil@ll.mit.edu

Massachusetts Open Cloud Workshop

30 October 2018
CLassified-as-a-Service (CLaaS) Concept

- **Current:** classified workloads in physically isolated copies of commercial clouds
  - Sacrifice: scalability, flexibility, cost, latest technology advances

- **Alternative:** strongly *isolate* classified workloads in the public cloud
  - Need secure integrated hardware and software implemented by cloud providers and IC customers

The IC needs flexible and substantial cloud resources to maintain US intelligence advantage.
How do We Protect Classified Clouds Today?

Physical Isolation

NSA Certified Network Encryption

Policy and Certification

FedRAMP

National Institute of Standards and Technology
U.S. Department of Commerce
What We Want to Enable
What We Want to Enable
Why Isolation is So Hard

Server Motherboard

- Storage Channel
- Comm Channel
- Flash Chips
- Storage Channel
- Comm Channel
- Storage Channel
- Comm Channel
- Comm Channel
- Storage or Comm Channel
- Storage or Comm Channel
- Storage or Comm Channel
- Storage or Comm Channel
- Comm Channel
- Comm Channel
- Comm Channel
- Comm Channel
- Comm Channel
CLaaS Development and Transition Model

**CLaaS Prototype System**
- System Analysis
- Experimentation
- Verification and Validation

**Evaluation Methodology**
- Metrics
- Test Harness

**Rapid Prototyping**
- Requirements for secure cloud HW/SW

**Government Users**
- Cyber Threats
- Capability Advances
  - Commercial
  - DoD Industrial Base
  - DoD Labs
  - FFRDCs/UARCs
  - Academia
- Updated Cyber Threats
- New Capabilities
- Capability Gaps

**Commercial Public Cloud**
- Updated Cloud Computing System
- Cloud Infrastructure
- Networking
- Sensors
- Compute
- Storage
- Energy
- Rapid HW / SW refresh (12-18 mo)
- Testing

**Public Cloud Computing System**
- Applications
- Amazon Web Services
- Microsoft Azure
- Google Cloud

**Capability Advances**
- Commercial
- DoD Industrial Base
- DoD Labs
- FFRDCs/UARCs
- Academia

**Capabilities**
- Commercial
- DoD Industrial Base
- DoD Labs
- FFRDCs/UARCs
- Academia

**CLaaS Prototype System**
- System Analysis
- Experimentation
- Verification and Validation

**Evaluation Methodology**
- Metrics
- Test Harness

**Government Users**
- Cyber Threats
- Capability Advances
  - Commercial
  - DoD Industrial Base
  - DoD Labs
  - FFRDCs/UARCs
  - Academia
- Updated Cyber Threats
- New Capabilities
- Capability Gaps

**Commercial Public Cloud**
- Updated Cloud Computing System
- Cloud Infrastructure
- Networking
- Sensors
- Compute
- Storage
- Energy
- Rapid HW / SW refresh (12-18 mo)
- Testing

**Public Cloud Computing System**
- Applications
- Amazon Web Services
- Microsoft Azure
- Google Cloud
Summary

• CLaaS has the potential to revolutionize secure cloud in the 2020s
  – Commercial cloud providers interested
  – Technology to implement CLaaS is maturing: bare metal clouds are a reality
  – Assessment based on:
    • Isolation mechanism assurance
    • Bandwidth of covert storage and communication channels

• Current status:
  – Beginning initial study to flesh out initial design for prototype and assessment methodology
  – Building a community of interested partners including
    • Major cloud providers
    • Massachusetts Open Cloud partners

We are seeking your ideas for technical solutions to strong isolation in the cloud