Hardware as a Service (HaaS)
What if…

• I have a sensitive application I want to put in the cloud…

• …AND I want all the benefits of the OCX and MOC vision
  – Elastic access to compute, storage, and network
  – Full cross section bandwidth to other cloud services
  – Access to share and collaborate on big data
  – Rapid provisioning of cloud resources
Even the Open Cloud can be Scary

Can one exploit compromise the entire cloud?

Is this the hardware I asked for?

Give my sensitive data to whom?

With whom am I sharing this cloud?
You can... but try not to hurt yourself
R&D Challenges to Secure Multi-tenancy

- Bootstrapping trust for provisioning
- Secure delete of stored data
- Sequential versus parallel multi-tenancy
- Firmware security and integrity
Part of the solution…
Trusted Platform Module (TPM)

A hardware root of trust enables secure system identity and integrity monitoring
Linking and Layering

Bootstrapping

Software-based Cryptographic Services

Trusted Computing Services

TPM / Platform Manufacturer Enrollment

Revocation

Software ID Keys

Signed HW Certificates

Valid TPM HW?

ID key revoked?

Abstract hardware rooted security from high-level services that need it
What are we doing about it?

- BU and MIT LL are leading a consortium of players to develop and demonstrate secure multi-tenancy in HaaS
  - Gov Customers: Commonwealth of MA, United States Air Force...
  - Applying for a grant from the Commonwealth to get started

Contact us if you are interested in high security apps in the MOC