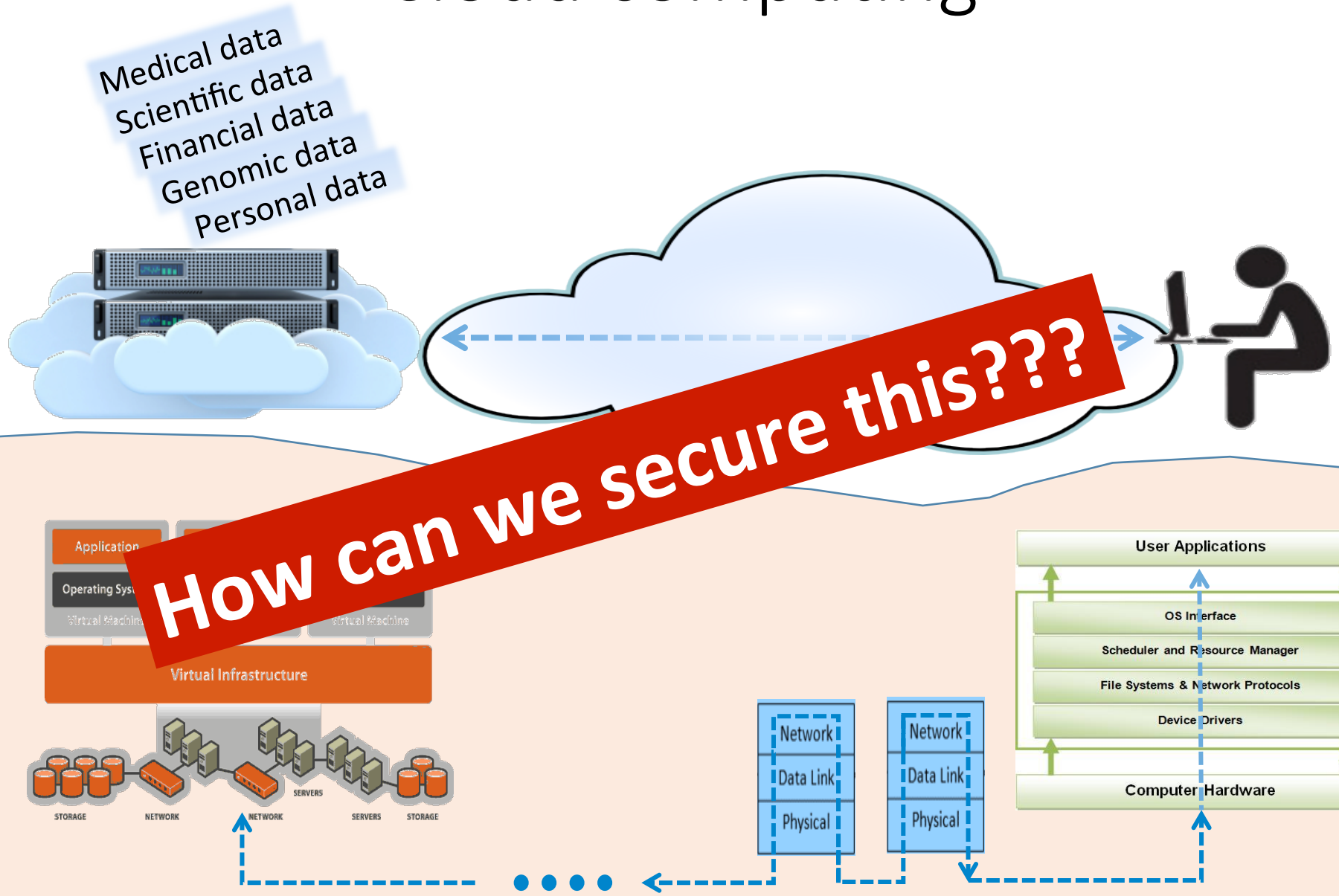
Modular Approach to Cloud Security (MACS)

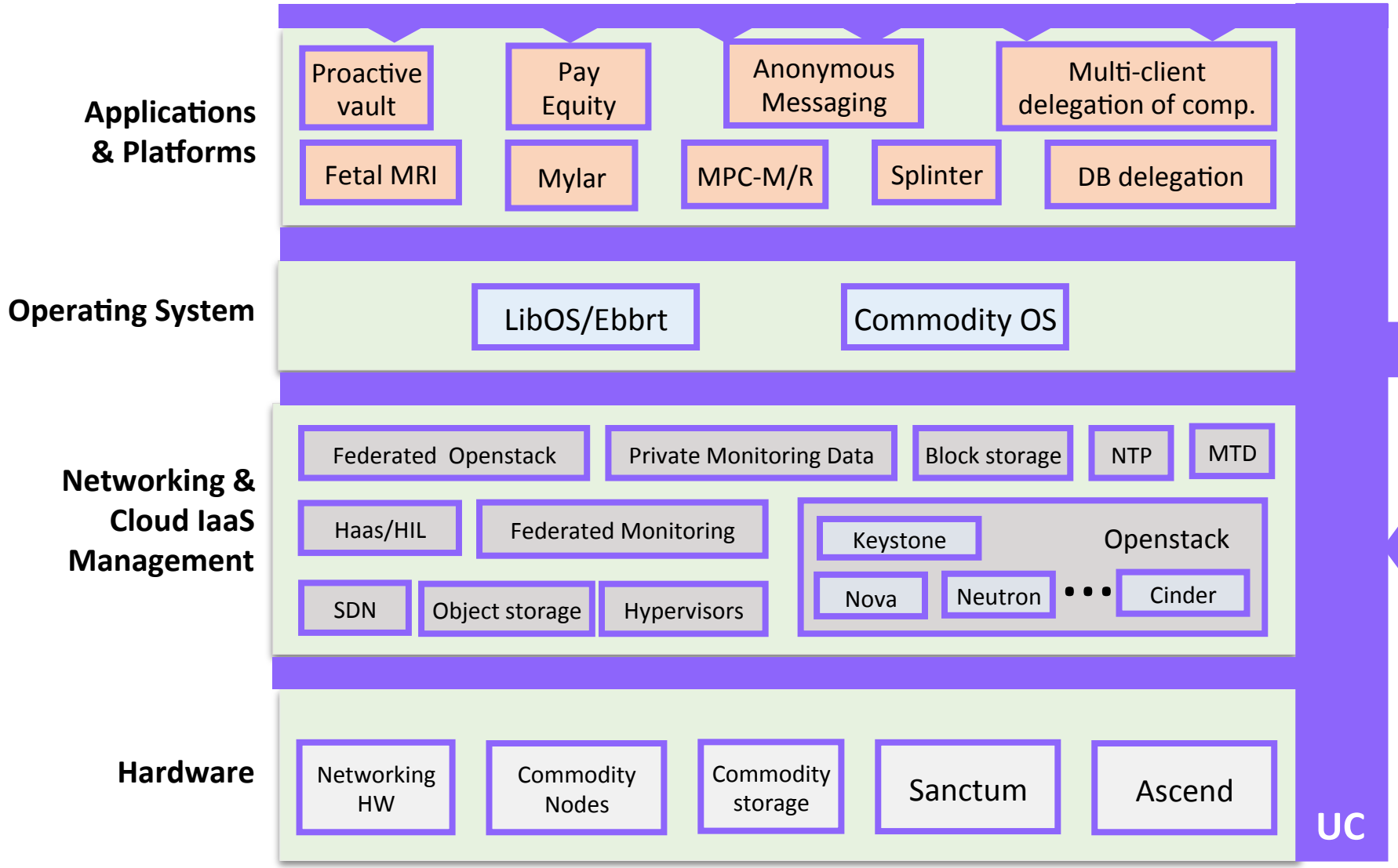
Mayank Varia, Boston University (varia@bu.edu)

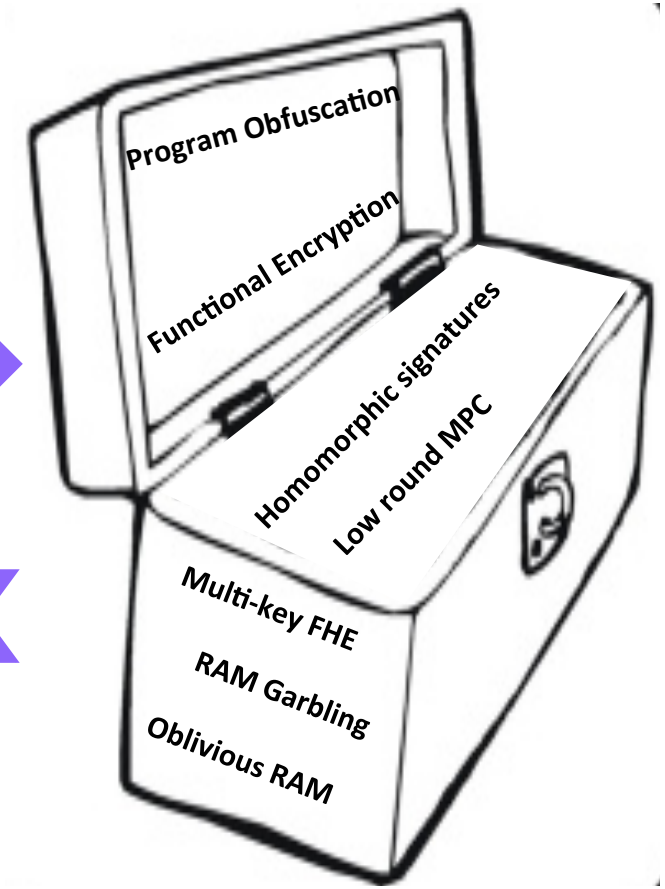
bu.edu/macs

Cloud computing



MACS Architecture





Algorithms & Techniques

BOSTON UNIVERSITY · MIT · Northeastern · University of Connecticut

Research Team with Broad Expertise

Algorithms & Techniques	Applications & Platforms	Operating System	Networking & Cloud Management	Hardware

Basic research

Transition to practice


Goldwasser


Wichs


Vaikuntanathan


Canetti


Zeldovich


Kollios


Bestavros


Kaashoek


Appavoo


Goldberg


van Dijk

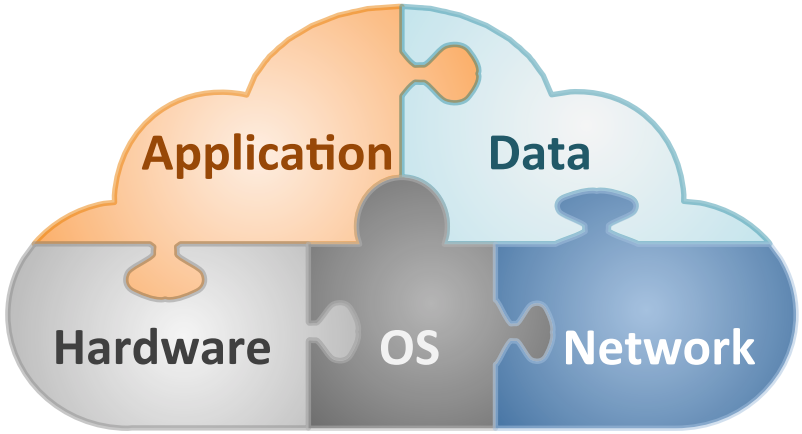

Devadas


Krieger

BOSTON UNIVERSITY · MIT · Northeastern · University of Connecticut

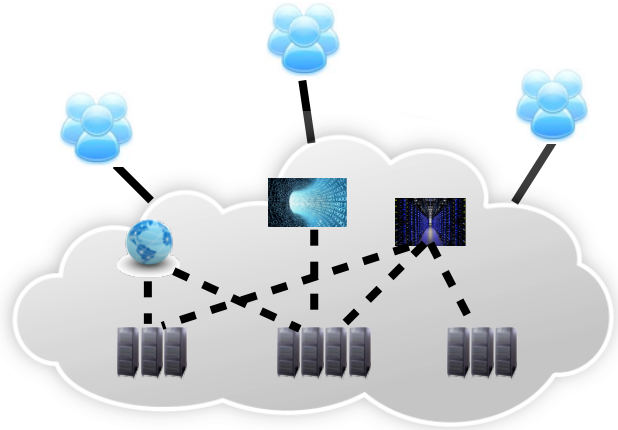
Talk Outline

1. Value of composable security



2. Collaboration with a production cloud

3. Potential of a multi-provider cloud



Value of Composable Security

In security, the sum of the parts is often a *hole*.

– Dave Safford, circa 2000

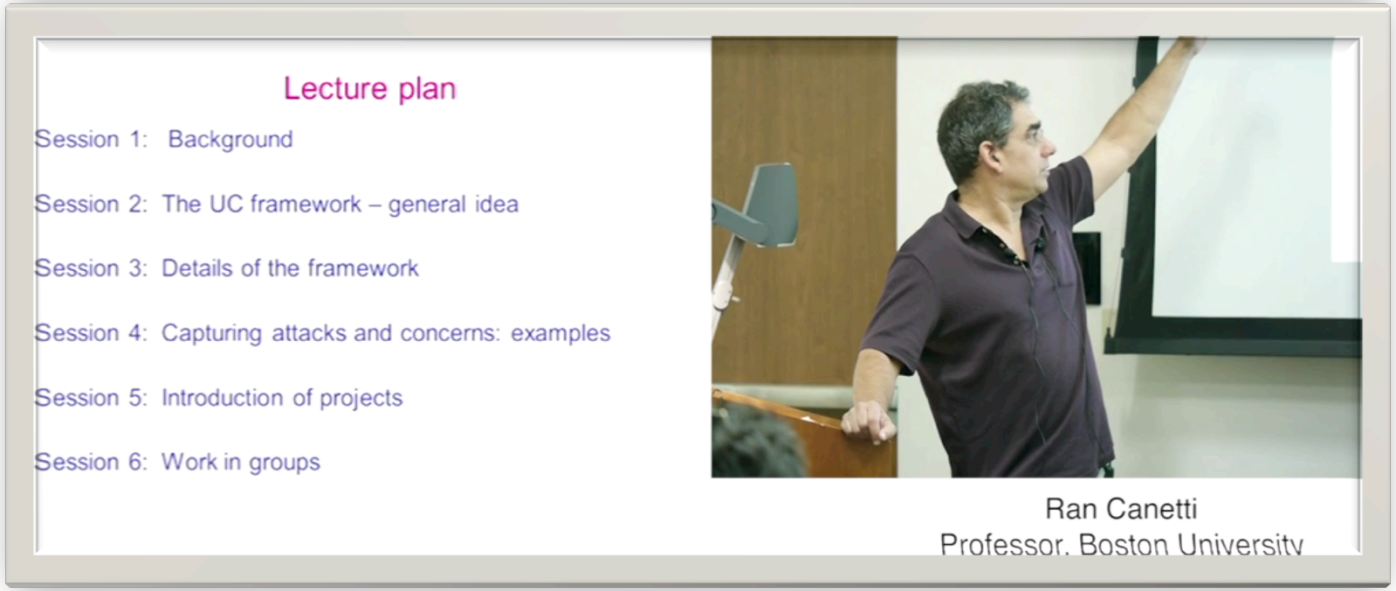
Our goal is to build security systems so that the sum of the parts is a *holistic security guarantee*.

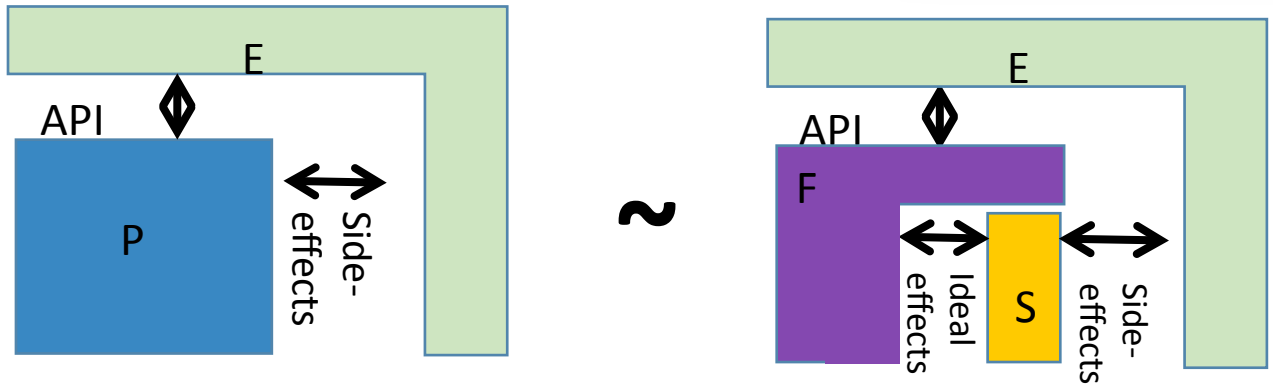
– Ran Canetti, 2016

Universal Composability

3 hours of video introducing the essential concepts of UC to a general computer science audience.

Search for “composable security” on YouTube.





P $\rightarrow_{UC^{\perp}}$ **F** if there exists **S** such that for all **E**, $Exec_{E,P} \sim Exec_{E,S,F}$

BOSTON UNIVERSITY MIT Northeastern University of Connecticut

Modularity and Composition

- **New security models**

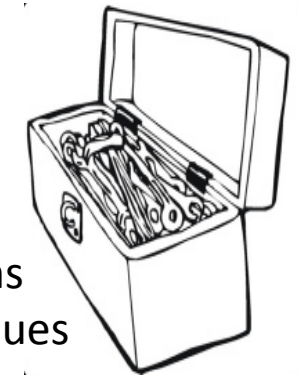
  Put trust in the forefront: Who do you trust and for what?

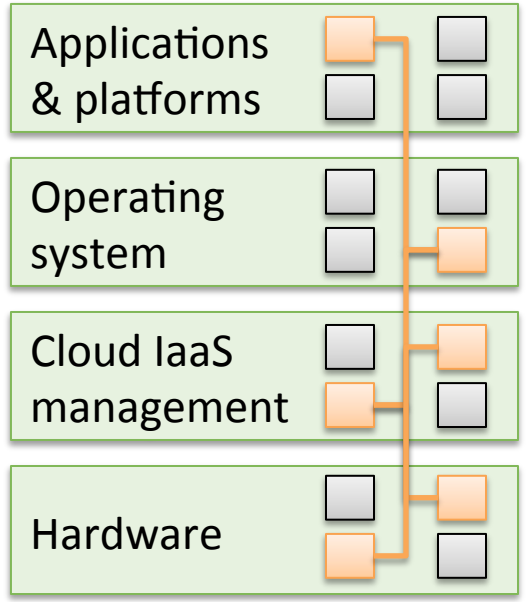
- **Provide modular security**
  - Partition a system into modules, each of which is analyzed by the right expert
  - Specify + analyze security properties with Universal Composability (UC)
  - Compose modules in an optimal fashion while preserving security

Composition throughout the Computing Stack

- **New security and trust models**
  Put trust in the forefront: Who do you trust and for what?

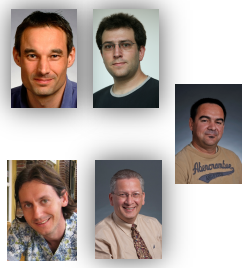
- **Modular & personalized security analysis**
  - Build systems with multi-layered security guarantees
  - Partition the system into modules
  - Assert the security of components individually
  - Analyze security properties of each module with UC
  - Allow the user to pick components based on her needs
  - Derive the overall system's security via composition





Modular Analyses in Progress



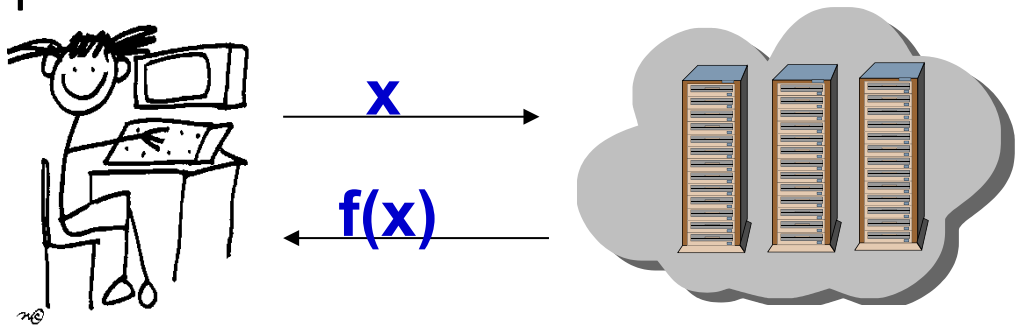



- New, simplified, improved variants of the UC framework
- UC security analysis of
  - Database delegation
  - Blockchain/Bitcoin based fair computation
  - Cloud management system
  - Secure hardware designs
  - Operating system components
  - Network time
- Other composable analyses: Differential privacy
  - Network protocols
  - Databases
  - Bounding information leakage

Motivating Example: Oblivious Computation

C has a (complex) task *f* and input *x*

S has computing power.



C wants S to compute *f(x)* for her – without S learning x.

Examples: Real-time fetus MRI, Genome diagnostics, real-time financial analytics.

How do we do that?

Four solution strategies

- **Secure hardware:** Encrypt to processor-on-chip, use ORAM

➔Trust only that chip, but no software.

- **Homomorphic encryption + Oblivious computation:**

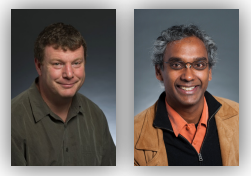
Compute directly on encrypted data, use “obfuscated ORAM”.

➔Trust only client’s local software.

- **Distributed secure computation:**

`secret-share’ *x* and *f* among multiple cloud providers.

➔Trust that servers do not collude.



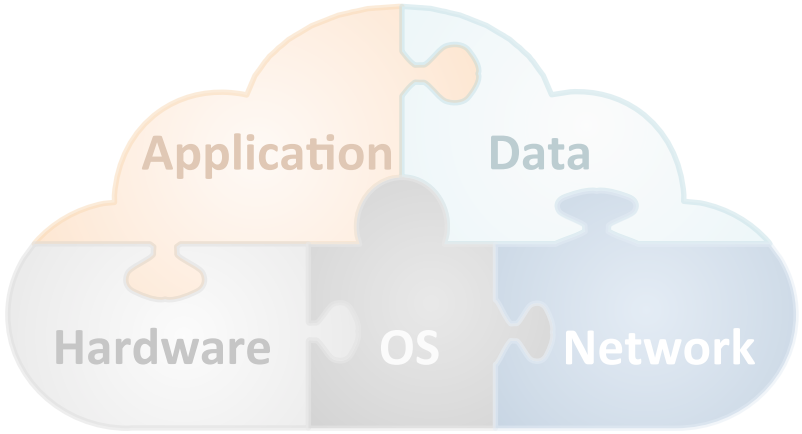
- **Hardware isolation layer:** Segment machines in the datacenter

➔Trust that hardware was configured correctly

BOSTON UNIVERSITY MIT Northeastern University of Connecticut

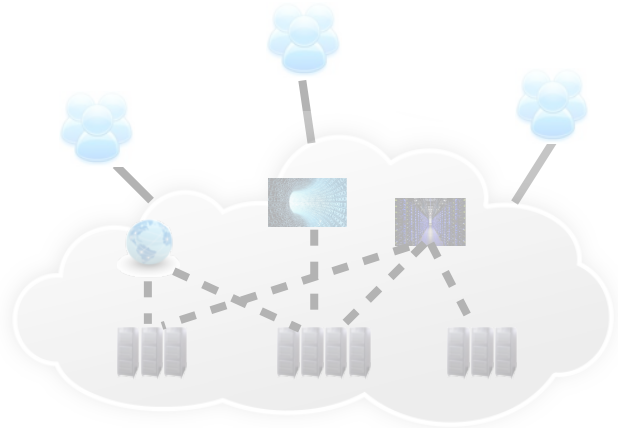
Talk Outline

1. Value of composable security



2. Collaboration with a production cloud

3. Potential of a multi-provider cloud



Massachusetts Open Cloud (MOC)

BOSTON UNIVERSITY · Northeastern · University of Connecticut

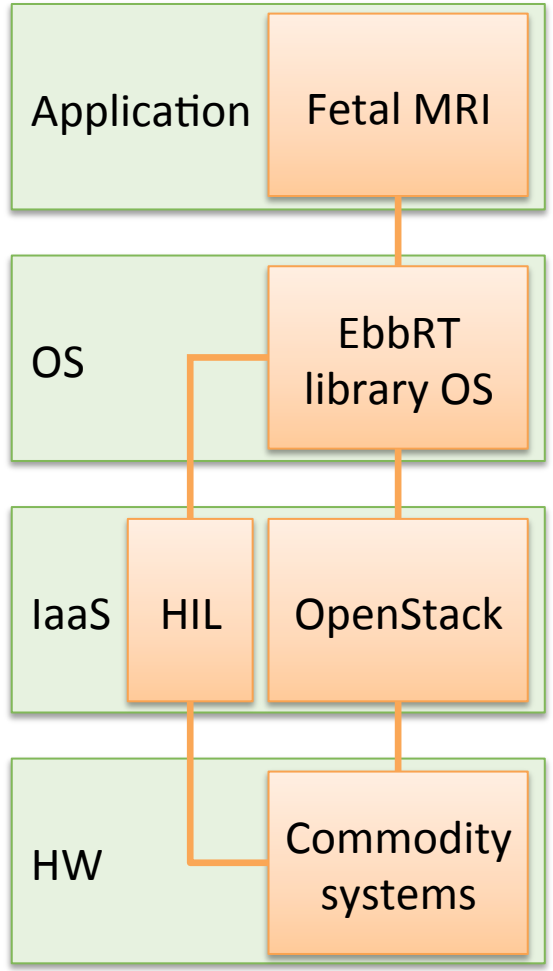
Synergy between MACS and MOC

Types of connections

- *Tech transition*: deploy MACS tech in MOC marketplace
- *Problem creation*: MOC's problems feed MACS research
- *People*: researchers can contribute toward both projects
- *Funding*: joint progress on cloud research has multiplier effect

Value that MOC provides to MACS

- *Access*: data, meta-data, scale, problems, and users
- *Unique trust relationships*: federated datacenter



Interplay: Research → Practice





EbbRT

UC Analysis

Secure Hardware

Hardware Isolation Layer

Bare Metal Imaging

Secure Cloud

U.S. AIR FORCE

Secure Dataverse

Legend:

- **Yellow** = MACS
- **Blue** = MOC
- **Green** = Joint

Interplay: Practice → Research

MOC Monitoring Infrastructure

- Private Monitoring Data

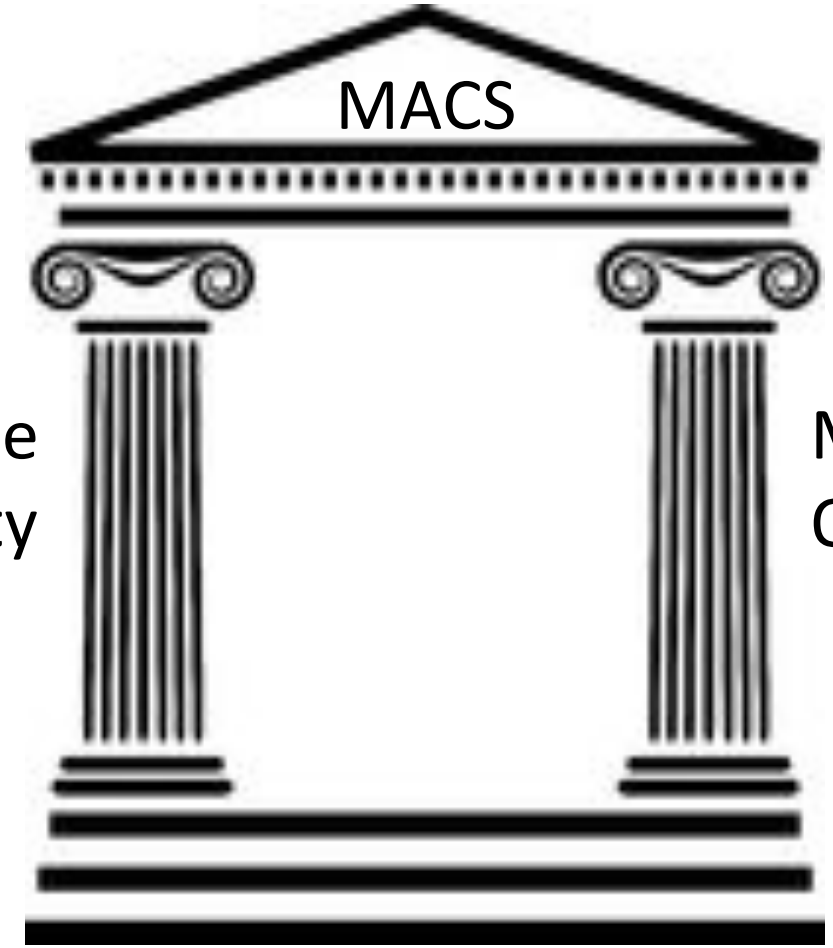

- Federated Monitoring


- Performance and Energy Aware Computing
- Secure Analytics for Public Clouds

Legend:

- **Blue** = MOC
- **Green** = Joint

The Two Pillars of MACS

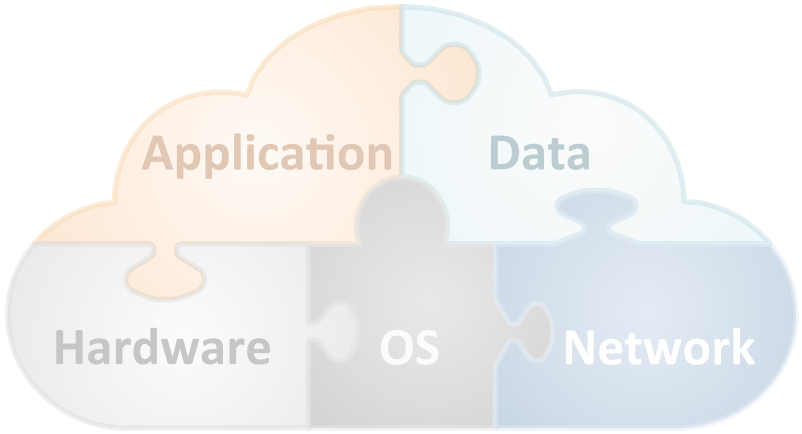


Composable Security

Massachusetts Open Cloud

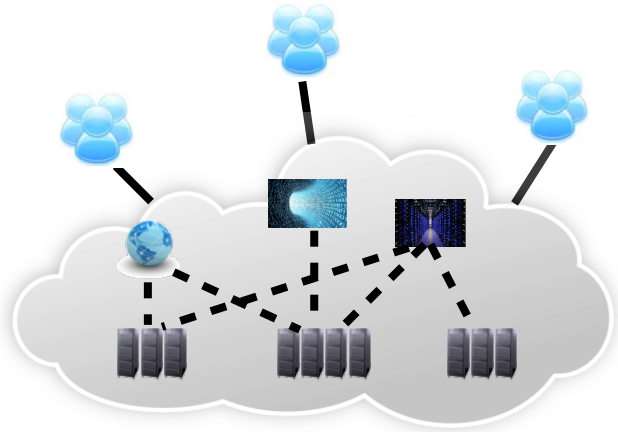
Talk Outline

1. Value of composable security

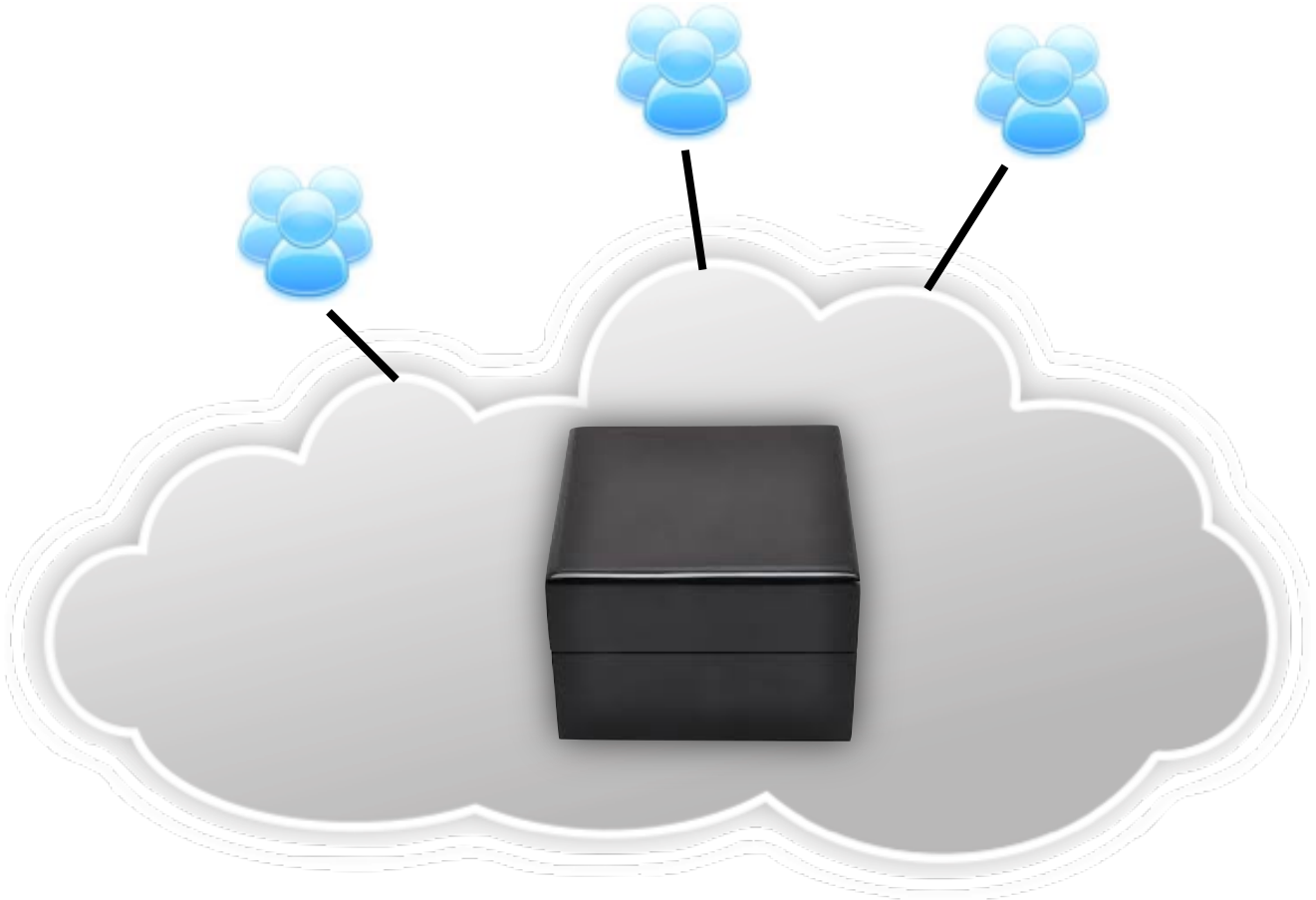


2. Collaboration with a production cloud

3. Potential of a multi-provider cloud



Issue: Today's Clouds are Owned, Operated, and Controlled by a Single Provider

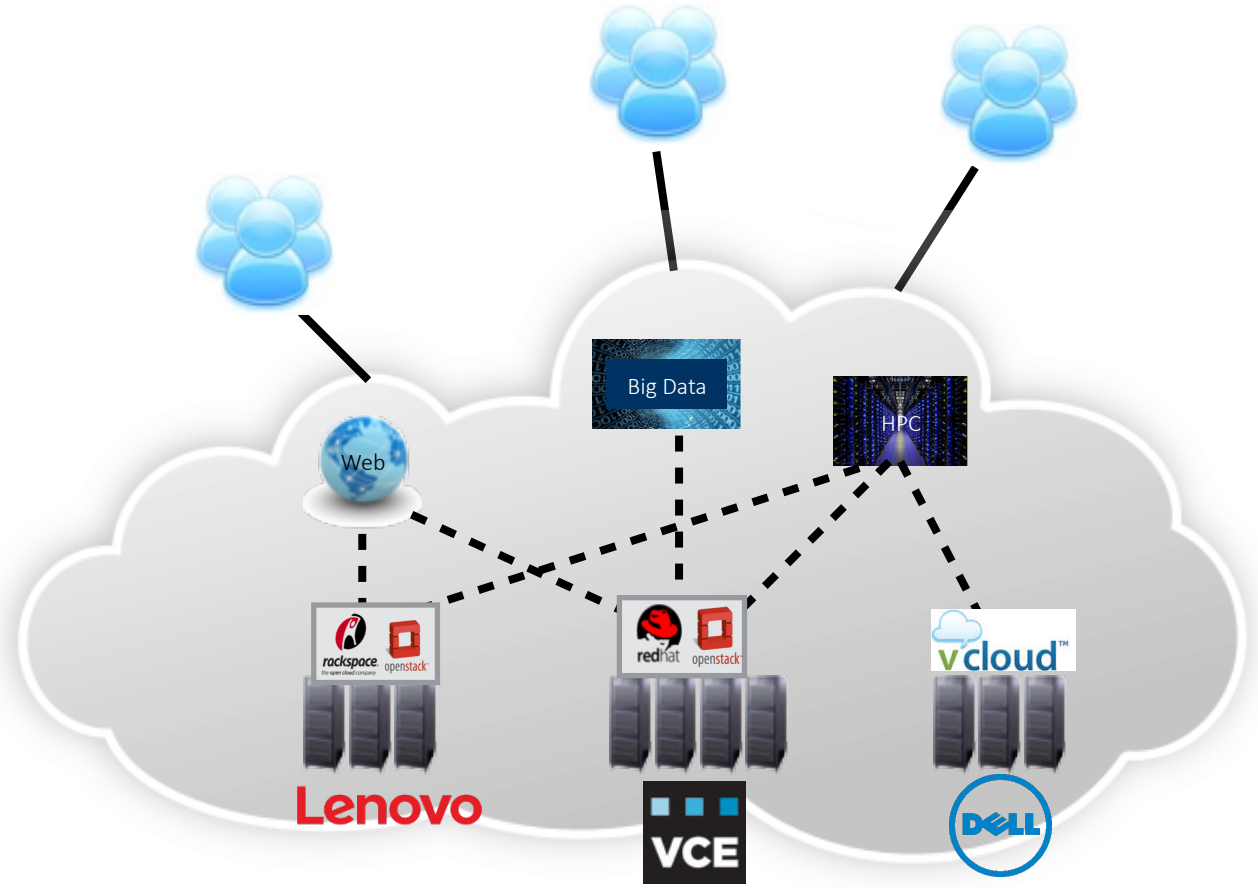


- Limits research & innovation
- Poses security challenges
- Vendor lock-in

We are in the equivalent of the pre-Internet world, where AOL and CompuServe dominated on-line access

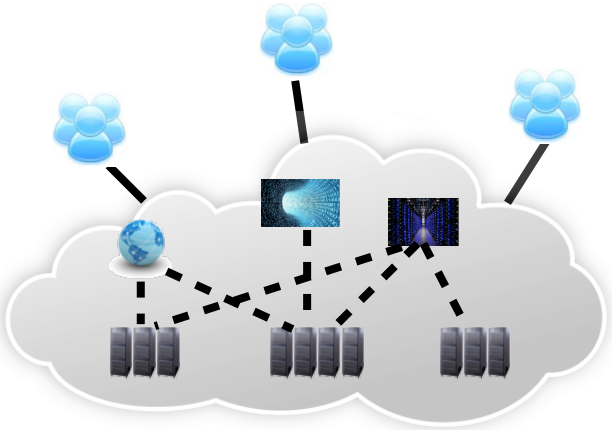
New Model: “Open Cloud Exchange”

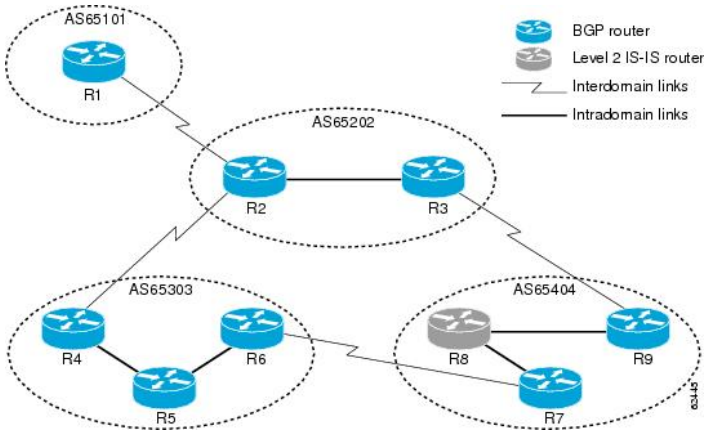
- Multiple providers in a level playing field
- Users/applications control what services they use



Revamping Large-Scale Internet Protocols

Single provider : Multi-provider cloud :: Autonomous system : Internet





New environment ⇒ New rules ⇒ New chance to bake-in security

BOSTON UNIVERSITY MIT Northeastern University of Connecticut

MPC as a Service & Application to Pay Equity

GOAL 3

Evaluating Success

Employers agree to participate in a biennial review to discuss successes and challenges, as well as contribute data to a report compiled by a third-party on the Compact's success to date. Employer-level data would not be identified in the report. The specific data to be reported will build on data already required by federal and state authorities and should not create an additional reporting burden.

The Boston Globe

The congresswoman, who had signed onto a bill addressing income disparity between men and women, was impressed by the relevance he outlined. ***"It's linking it back for the members of Congress,"*** Clark said. ***"Nobody would think, oh, the Paycheck Fairness Act, how is that tied into NSF funding?"***

Thanks!

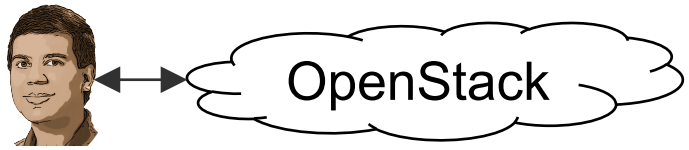
bu.edu/macs

Modular Security at Scale

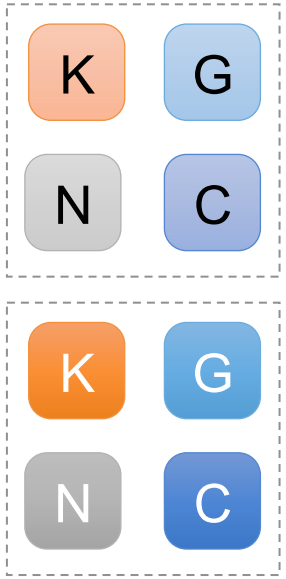
- *Our goal*: Provide modular analysis of a computing environment "from head to toe," have the system be implemented and used
- *To evaluate security*: specify and analyze security guarantees using the Universal Composability (UC) framework
- *To compare performance*: need implementations, plus a working platform in order to examine workloads + gather measurements

Modular OpenStack Analysis

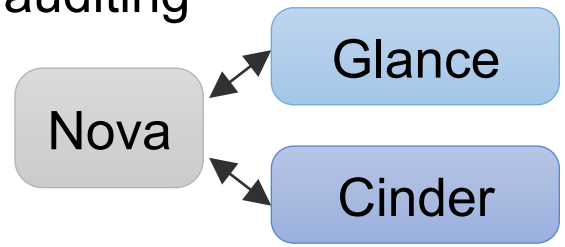
1. User ↔ cloud
   - Bearer tokens
   - Policy engine



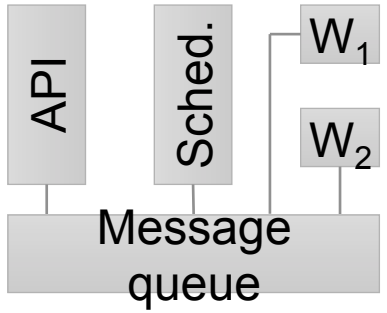
2. Between deployments
   - Federation between Keystones
   - Federation between all services



3. Between services
   - System isolation of services
   - Logging & auditing

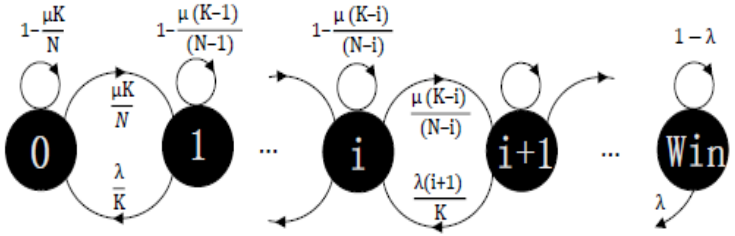


4. Within a service
   - End-to-end encryption
   - Isolation of workers

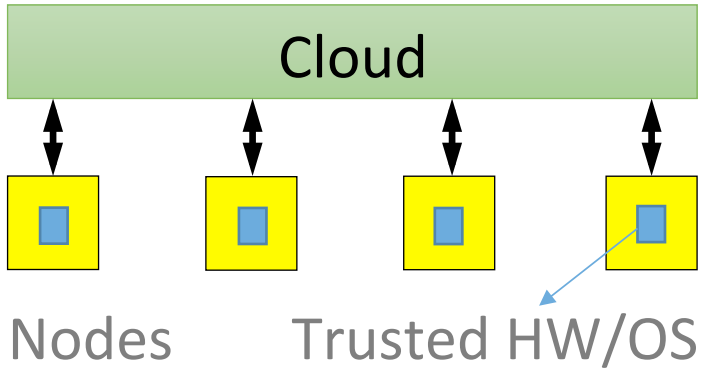


Network-based Moving-Target Defense

- Shared resources in the cloud are a security…
  - Disadvantage: large, homogeneous attack surface
  - Advantage: diversity of workloads provides a place to hide



- Objective: continuous, long-term protection of secrets
- Method: distribute secrets amongst many nodes, periodically migrate & refresh
- Markov-style analysis computes Prob[Identification] based on churn and cost
- If attacker is removable, security can be measured in USD
- How do we justify the cloud's ability to evict an attacker?
  - Traditionally, rely upon a special trusted dispatcher
  - We analyze the judicious use of several crypto primitives on the existing cloud infrastructure to overcome prior limitations



BOSTON UNIVERSITY MIT Northeastern University of Connecticut