Security Research on the MOC

Mayank Varia
bu.edu/macs
Cloud Computing
Underlying Complexity
Modularity
Modularity
Cloud Security

How can we secure this???
Cloud Security Today

Application
Data
Hardware
OS
Network

Medical data
Financial data
Scientific data

Virtual Infrastructure

User Applications
OS Interface
Scheduler and Resource Manager
File Systems & Network Protocols
Device Drivers
Computer Hardware
In security, the sum of the parts is often a hole.

Dave Safford, circa 2000
Modular Approach to Cloud Security
Our Approach

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

• **Provide modular security**
  – Partition a system into modules
  – Analyze each module separately (by the right experts)
  – Compose modules in an optimal fashion while preserving security
Trust Relationships

Cloud-centric ➔ Service-centric

**Cloud-centric**
- Trusted cloud infrastructure

**Service-centric**
- Guarantee to users
  - Privacy of their data
  - Correctness & timeliness of stored results

Empower user to make meaningful tradeoffs between security, trust, efficiency, and cost
**Composition**

**Question:** How do the pieces fit together?

**Answer:** Universal composability framework

**Def (UC protocol emulation & realization).** A protocol $\pi$ UC-emulates protocol $\phi$ if for any PT adversary $A$, there exists a PT adversary $S$ such that for all PT environments $E$ that output only one bit:

$$\text{UC-Exec}_{\phi,S,E} = \text{UC-Exec}_{\pi,A,E}$$

**Thm (composition).** Let $\pi$ and $\phi$ be subroutine-respecting PT protocols such that $\pi$ UC-emulates $\phi$. Then, $\rho^{\pi/\phi}$ UC-emulates rho for any PT protocol $\rho$. 
Examples in the Poster Session

Searchable encryption

- **Goal:** permit querying over encrypted databases
- **Research:** model of trust required in DB server on range queries
- **Composition:** 1st composable definition of secure DB delegation

OpenStack

- **Goal:** understand, model, and bolster the security of OpenStack, a popular open-source cloud architecture
- **Research:** analyzed the security OpenStack provides to users
- **Composition:** began to decompose OpenStack and analyze the security provided by each component
From Theory to Practice & Back Again

- Bring composable security to practice
- Bring novel algorithmic techniques to practice
- Provide environment to test & compare solutions
- Inform theory of actual needs of cloud systems
MACS Summary: The Road Ahead

1. Research
   Design new algorithmic solutions to cloud security challenges

2. Implement
   Spans network, hardware, OS, application, and data security

3. Deploy
   Integrate building blocks for security into the MOC: an operational, commercial-grade cloud

4. Analyze
   Produce an analytical framework that enables composition and amplification of the security of each component
Thanks!

bu.edu/macs