Modular Approach to Cloud Security

Lead PI: Ran Canetti, Project Director: Mayank Varia

Website: bu.edu/macs

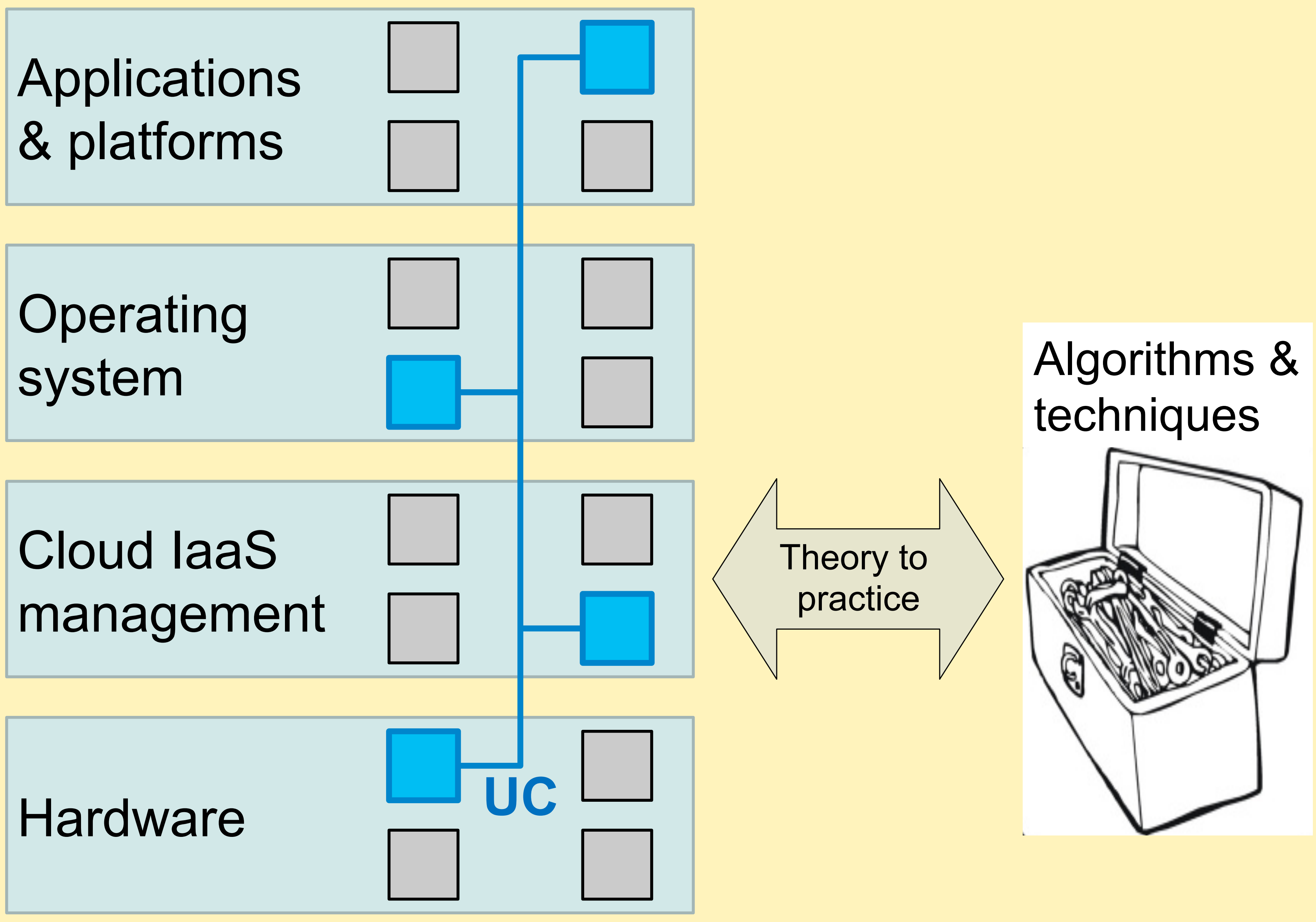
Objective: Design a cloud architecture with meaningful, multi-layered security guarantees. Rather than reasoning about security "in one blow," analyze each component individually, and then derive the security of the whole system using a compositional approach.

Three step process:

1.Design many systems with different security and privacy guarantees at each layer of the computing stack

2.Draw from the algorithmic toolbox of yesterday in order to design these systems, while also contributing toward the toolbox of tomorrow.

3.Combine the solutions necessary to achieve a user's desired security, reasoning via Universal Composability (UC).



Selected Scientific Merits

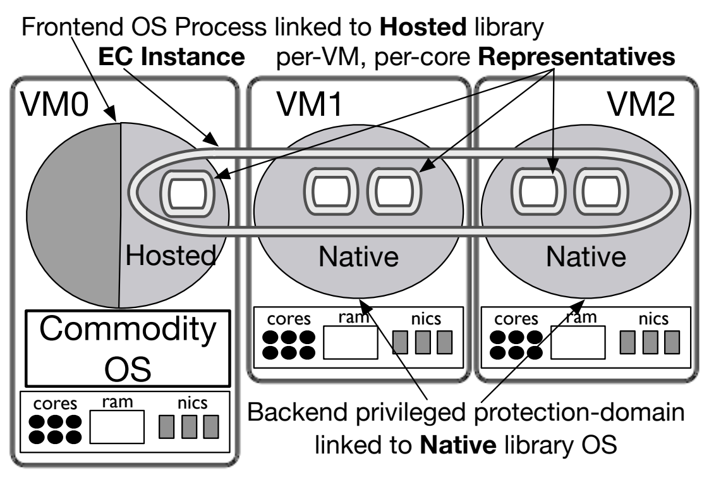
Universal composability

- Updated & streamlined the UC toolbox
- Explored the connection between UC and differential privacy, elucidating the value of the latter toward security
- Conducted UC analyses of secure DB delegation, fair computing via Bitcoin, signature-based authentication via a global PKI, and all IaaS mechanisms
- Held 2-day workshop with 40 attendees

Operating systems

•Designed an open-source modular operating system for the cloud

•Demonstrated performance of a lightweight event-driven library OS


Frontend OS Process linked to Hosted library
EC Instance
per-VM, per-core Representatives
VM0
VM1
VM2
Hosted
Native
Native
Commodity OS
cores
ram
nics
Backend privileged protection-domain linked to Native library OS

Algorithms & techniques

- Rigorously explored multi-key FHE and the stronger notion of spooky encryption
- Studied adaptive security of MPC constructions and verifiable outsourced computing in the (realistic) RAM model
- Explored constructions, limitations, and uses of indistinguishability obfuscation
- Advanced the art in access-pattern hiding mechanisms such as ORAM

Cloud management (Iaas)

- Performed a modular security analysis of the OpenStack IaaS framework
- Designed and analyzed a moving target defense mechanism for long-term safe execution of a critical cloud service
- Discovered and disclosed flaws in the network time protocol, and analyzed the security of the resulting procedure

Applications & platforms

- Deployed distributed secure computing systems for legacy MapReduce code, to calculate pay equity, and to search public data like maps and Yelp reviews
- Built a metadata-protecting anonymous messaging app using differential privacy
- Deployed ABE to build crypto-enforced access control of outsourced files
- Attacked and secured outsourced DBs

Hardware

•Designed two custom processors for secure computation, with isolation enforced via crypto (Ascend) or systems design (Sanctum).

•Analyzed the security benefits and weaknesses of Intel's SGX.

•Provided bare-metal isolation of physical services on the cloud.

Selected Impacts

Scientific Impact

- Showcase composable design and analysis as a viable basis for secure system design
- Bring beautiful and novel algorithmic techniques for privacy-preserving computation to the cloud

Broader Impact

- Deployment on the Massachusetts Open Cloud to impact cloud computing practice
- Increase uptake of cloud computing
- Outreach programs to expose Boston area middle- and high-school students along with their teachers to cybersecurity principles and techniques

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

BOSTON UNIVERSITY
Northeastern
University of Connecticut