Secure Cyber Incident Information Sharing

UTSA Team Leads

Dr. Ram Krishnan, Assistant Professor, ECE

Dr. Ravi Sandhu, Professor (CS) and Executive Director (ICS)

April 09, 2014

UTSA Engineering

I·C·S
The Institute for Cyber Security

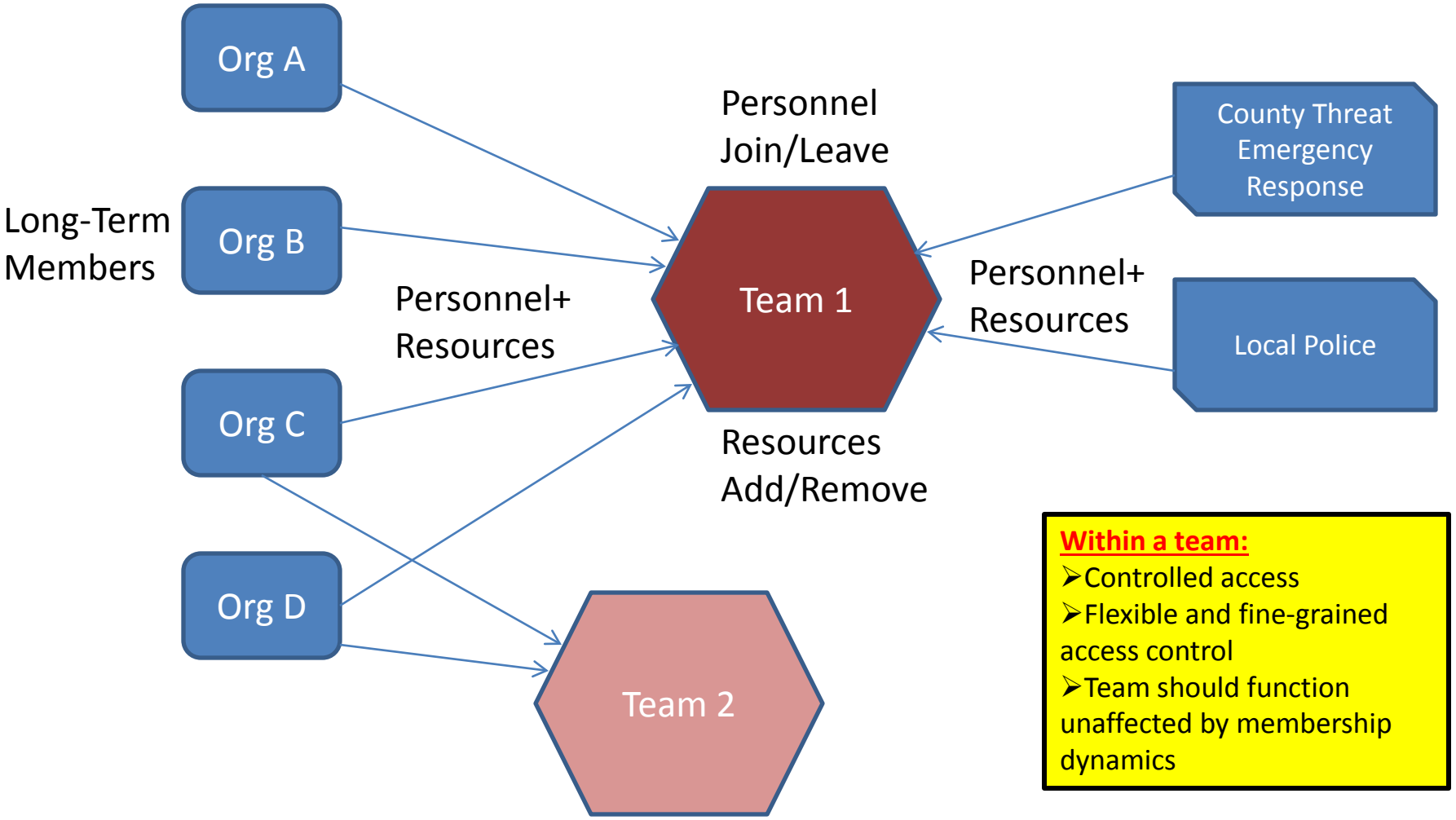
LMI Research Institute (LRI): Academic Partnership Program

- Through formal working relationships with universities across the country, LMI bridges the gap between academia and industry to create innovative solutions and explore new research topics
- The partnership program exposes students to real-world challenges faced by the federal government through structured, funded research projects

Cyber Incident Response

- Secure information sharing amongst a set of entities/organizations
  - Often ad hoc
- What are the effective ways to facilitate information sharing in such circumstances?
  - Information sharing models
  - Infrastructure, technologies, platforms

Agile Incident Response



Within a team:

- Controlled access
- Flexible and fine-grained access control
- Team should function unaffected by membership dynamics

Cyber Incident Information Sharing Scenarios

- High-assurance scenarios
  - Closed network
  - Data exfiltration
- Medium-assurance scenarios
  - Community
  - Electric grid

Key Requirements

- Cyber infrastructure sharing to support data and compute
- Light-weight and agile
- Rapid deployment and configuration
- Secure environment

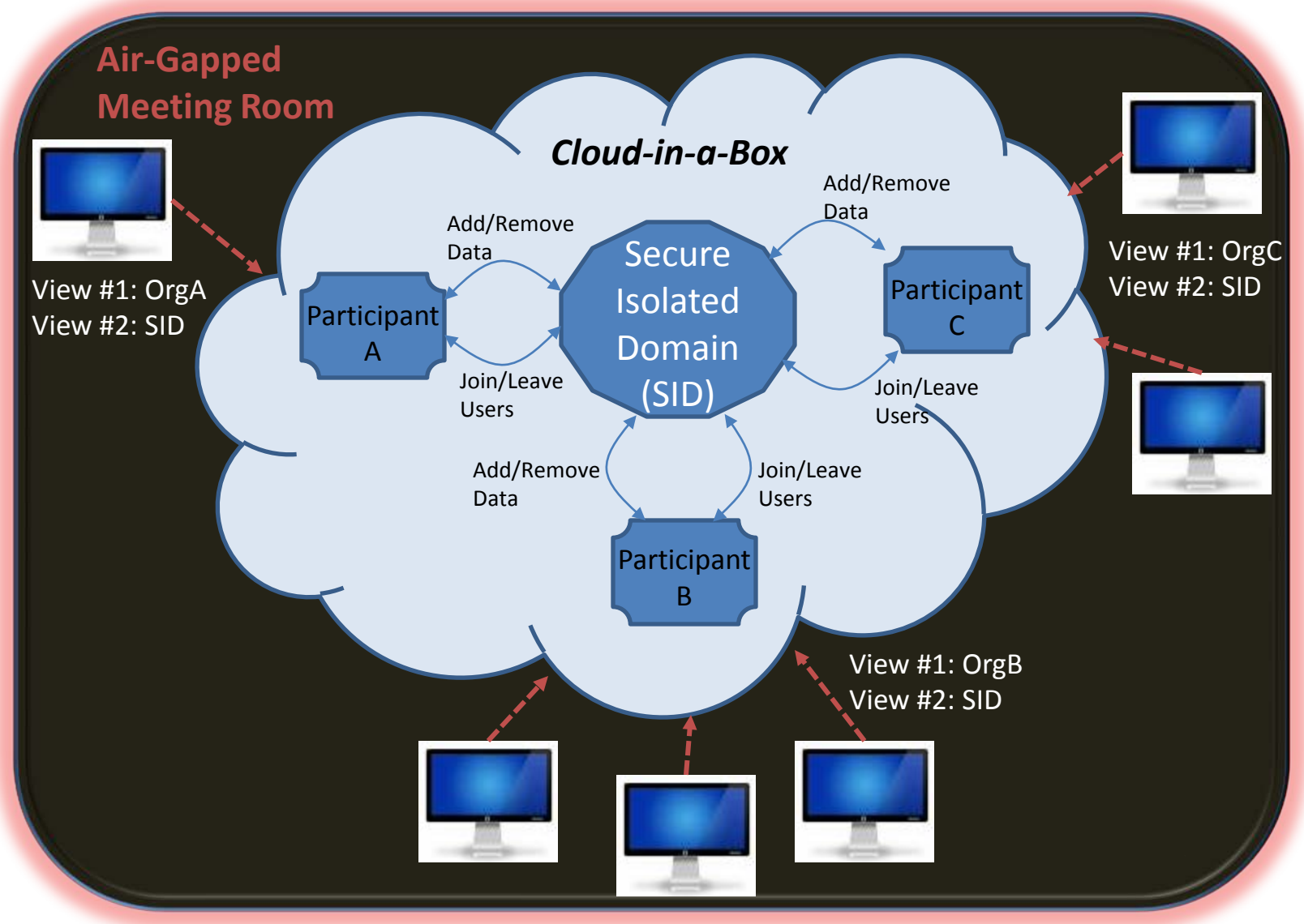
Cloud Infrastructure as a Service

- Virtualized IT infrastructure (servers, storage, networks, OS, etc.)
  - Delivered as a service over a network, on demand, dynamic scaling, etc.
- Prominent examples
  - Amazon AWS
  - OpenStack

Information Sharing in a High-Assurance Scenario

- Physically secure meeting room
- Air-gapped network
- Cloud-in-a-box

Enforcement in Cloud IaaS



Next Steps

- UTSA to incorporate 24 AF input
- Develop prototype in OpenStack
- Share research results with 24 AF
  - August/September

Thanks

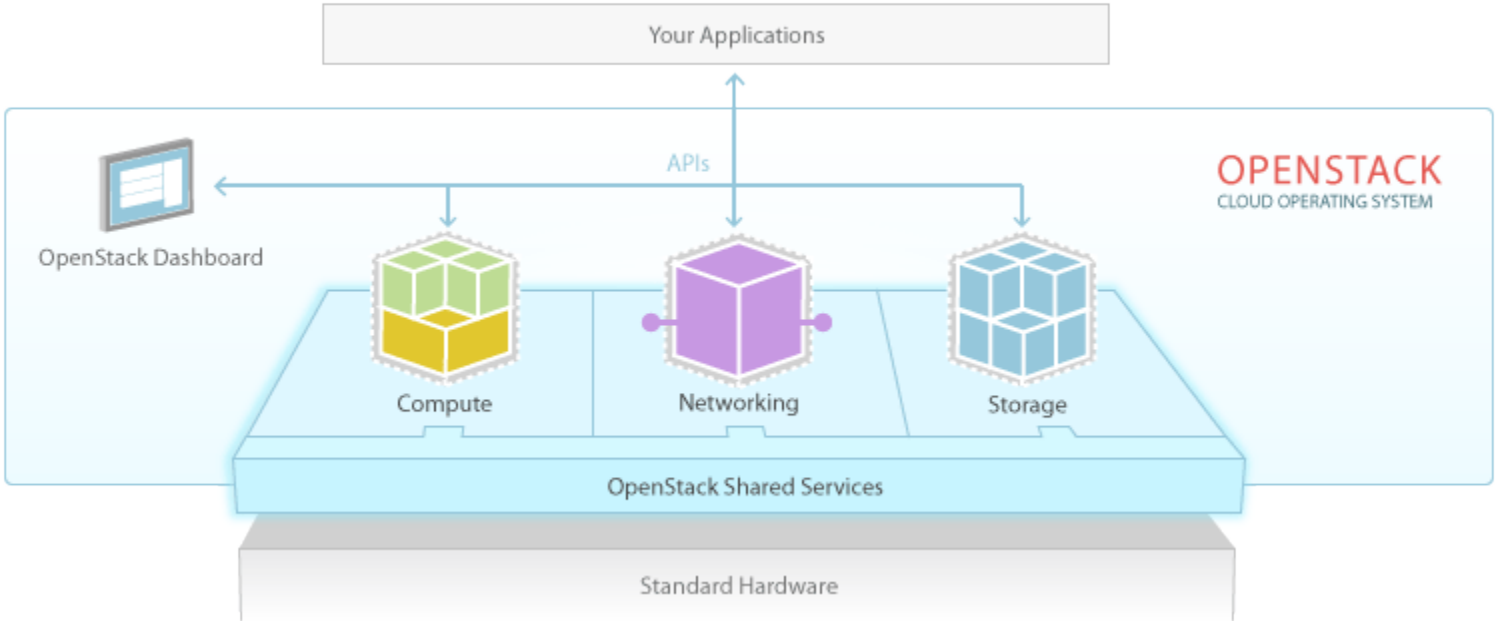
- Comments, Q&A

Backup

OpenStack

- OpenStack
  - Dominant open source cloud IaaS platform

- > 200 companies
- ~14000 developers
- >130 countries



Project Goal