Community-Based Secure Information and Resource Sharing in Azure Cloud IaaS

Cyber Incident Response

Models for Information and Resource Sharing

Yun Zhang, Farhan Patwa, Ravi Sandhu
Institute for Cyber Security
University of Texas at San Antonio
San Antonio, TX 78249
May 30, 2016

Presented by: Amy(Yun) Zhang

UTSA

I·C·S
The Institute for Cyber Security

Overview

- Motivations
- Scope
- Background
- Secure Isolated Domain (SID) Concept
- Azure Access Control Model
- Azure SID Model
- Enforcement
- Conclusion

Motivations

- Cyber Collaboration Initiatives
  - Cyber attacks are becoming increasingly sophisticated.
    - Hard to defend by a single organization on its own.
  - Collaborate to enhance situational awareness
    - Share cyber information
      - Malicious activities
      - Technologies, tools, procedures, analytics.
- Dominant IaaS cloud platforms are lacking models for group sharing

Ref: www.huffingtonpost.co.uk/2013/04/23/uk-government-faces-1000-cyber-attacks-a-day_n_3138164.html

UTSA

I·C·S
The Institute for Cyber Security

Scope

- Sharing models — sharing amongst a set of organizations
  - Information, infrastructure, tools, analytics, etc.
  - May want to share malicious or infected code/ systems (e.g. virus, worms, etc.)
  - Sensitive
- Cloud service models — focus on Infrastructure as a Service (IaaS) — Microsoft Azure
- Scenario — Cyber Incident Response

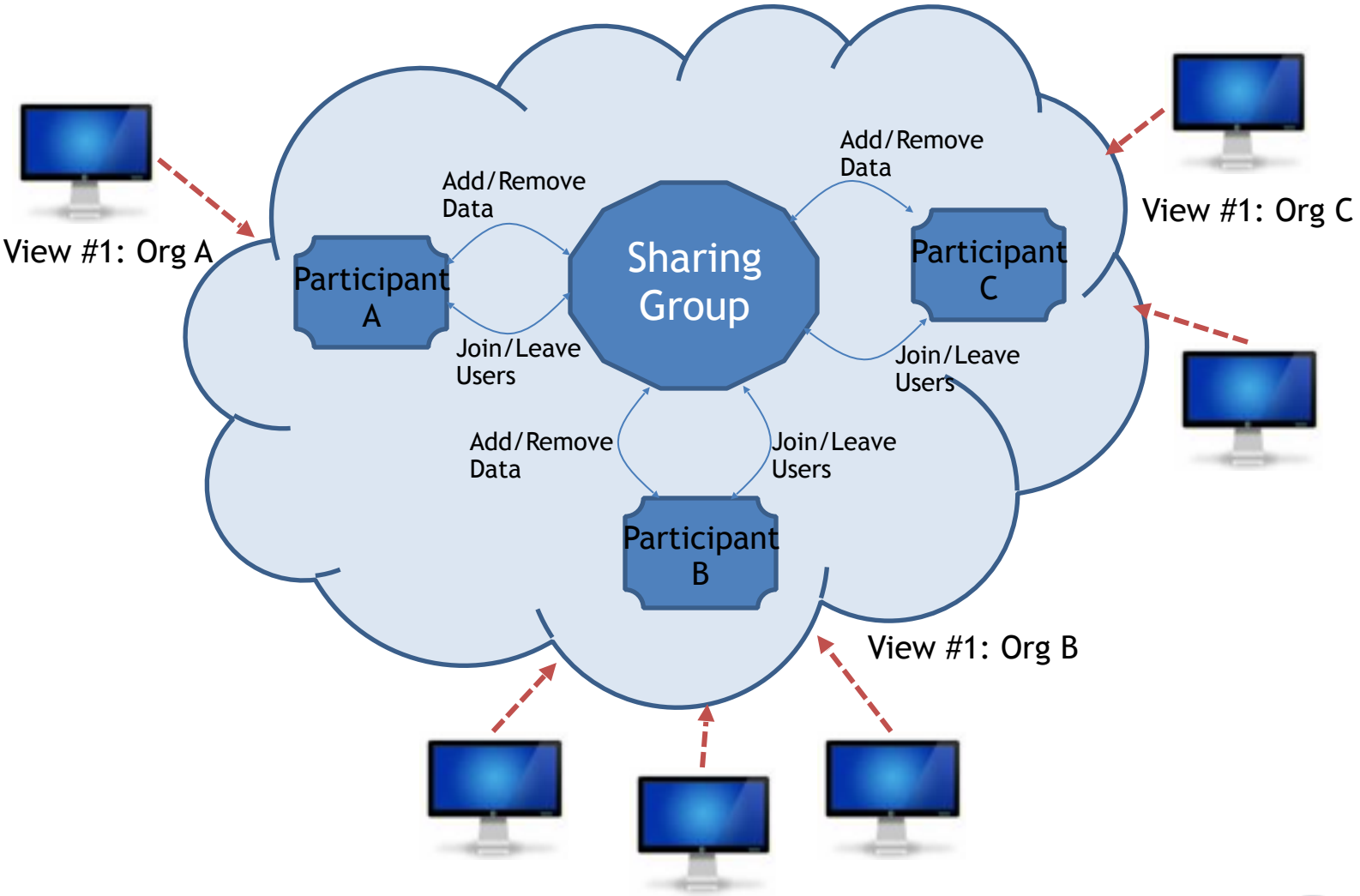
Traditional Cyber Collaboration

- Traditional collaboration
  - Subscription services
  - Limitations
    - Organizations Sharing information through subscription.
    - Organizations are not actively participating in analyzing and processing the cyber information they submit.
    - Organizations don't directly interact with each other on sharing activities.

Cloud IaaS Advantages for Cyber Incident Sharing

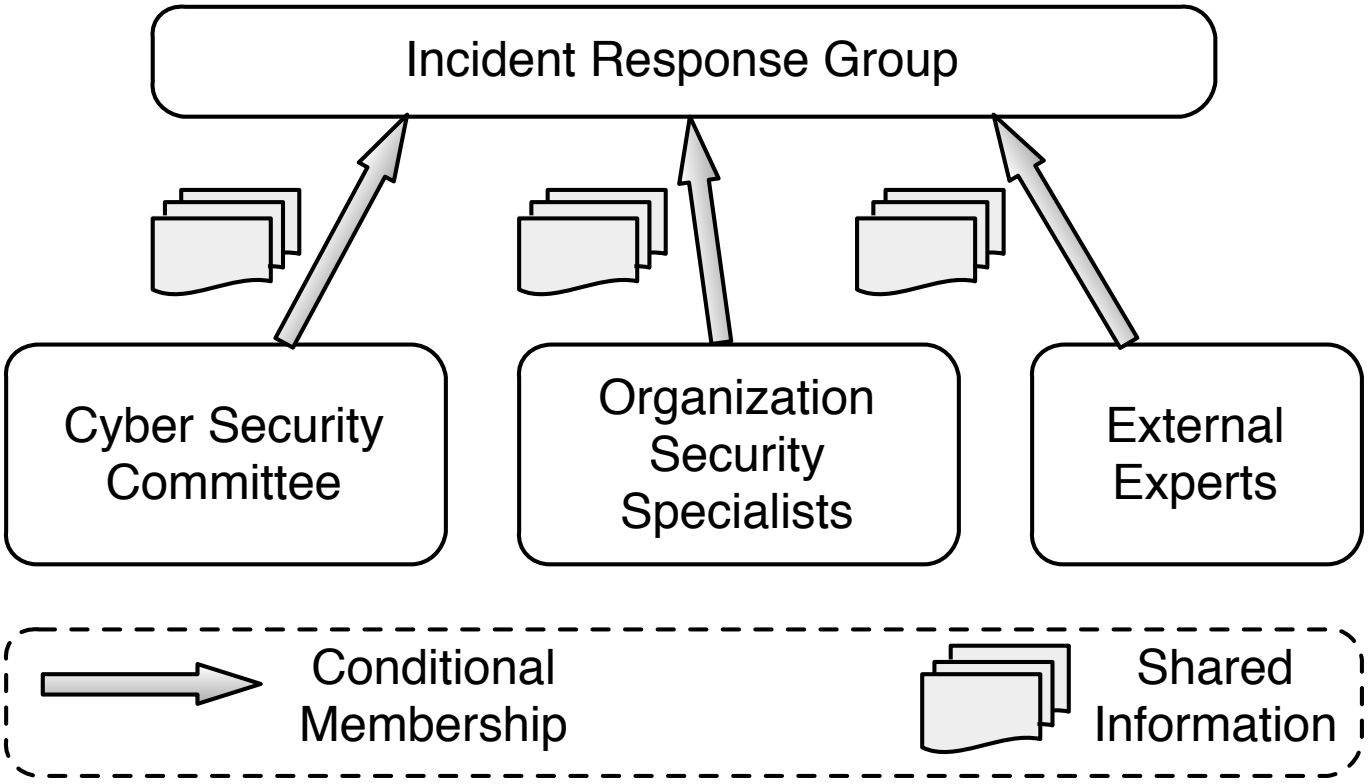
- Virtualized resources
  - Theoretically, one can take a snapshot and mobilize
- Operational efficiency
  - Light-weight and agile
  - Rapid deployment and configuration
  - Dynamic scaling
  - Self-service

Sharing Model in Cloud IaaS



refer paper: Towards a framework for group-centric secure collaboration.

Community Cyber Incident Response Governance

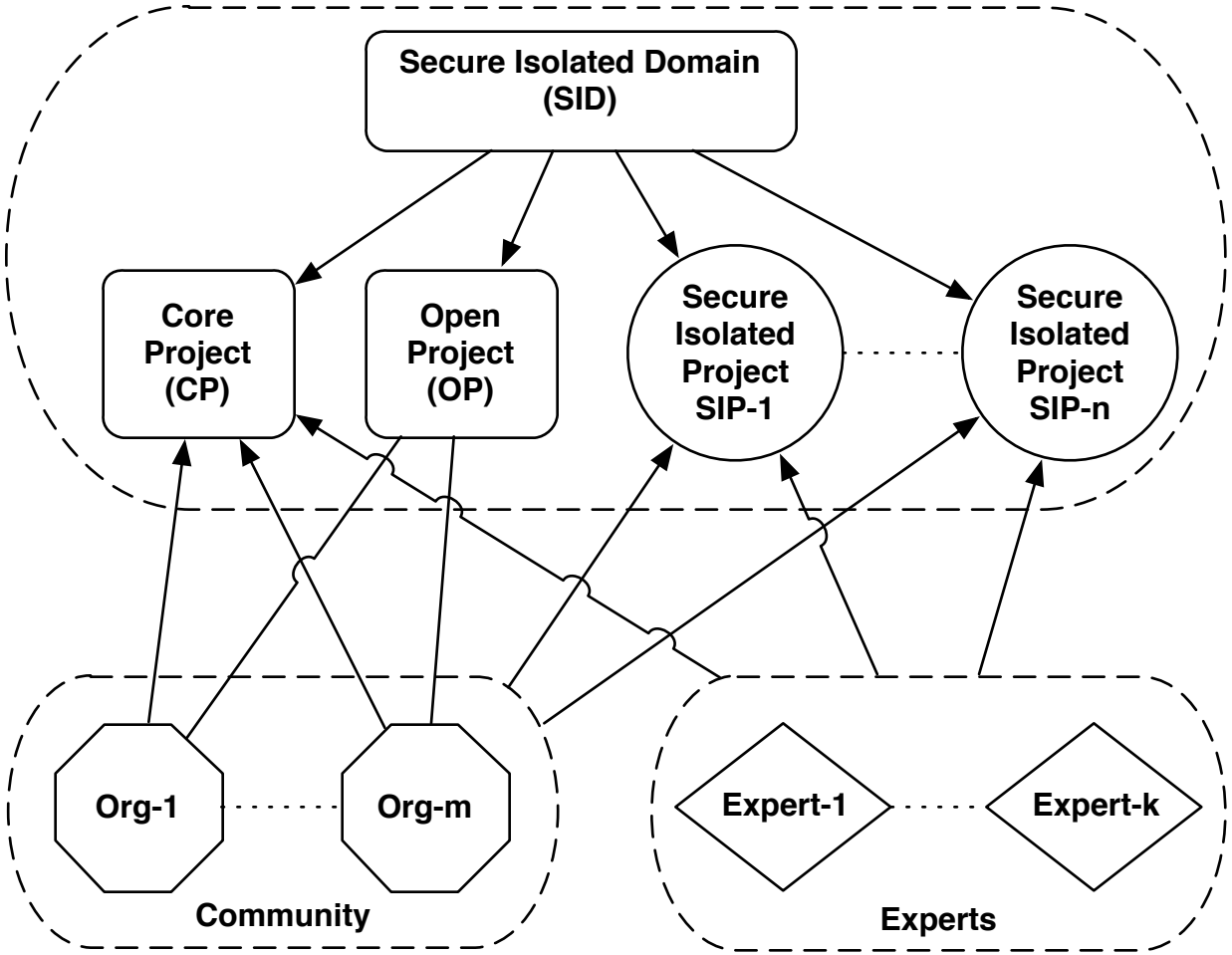


refer paper: RT-based administrative models for community cyber security information sharing.

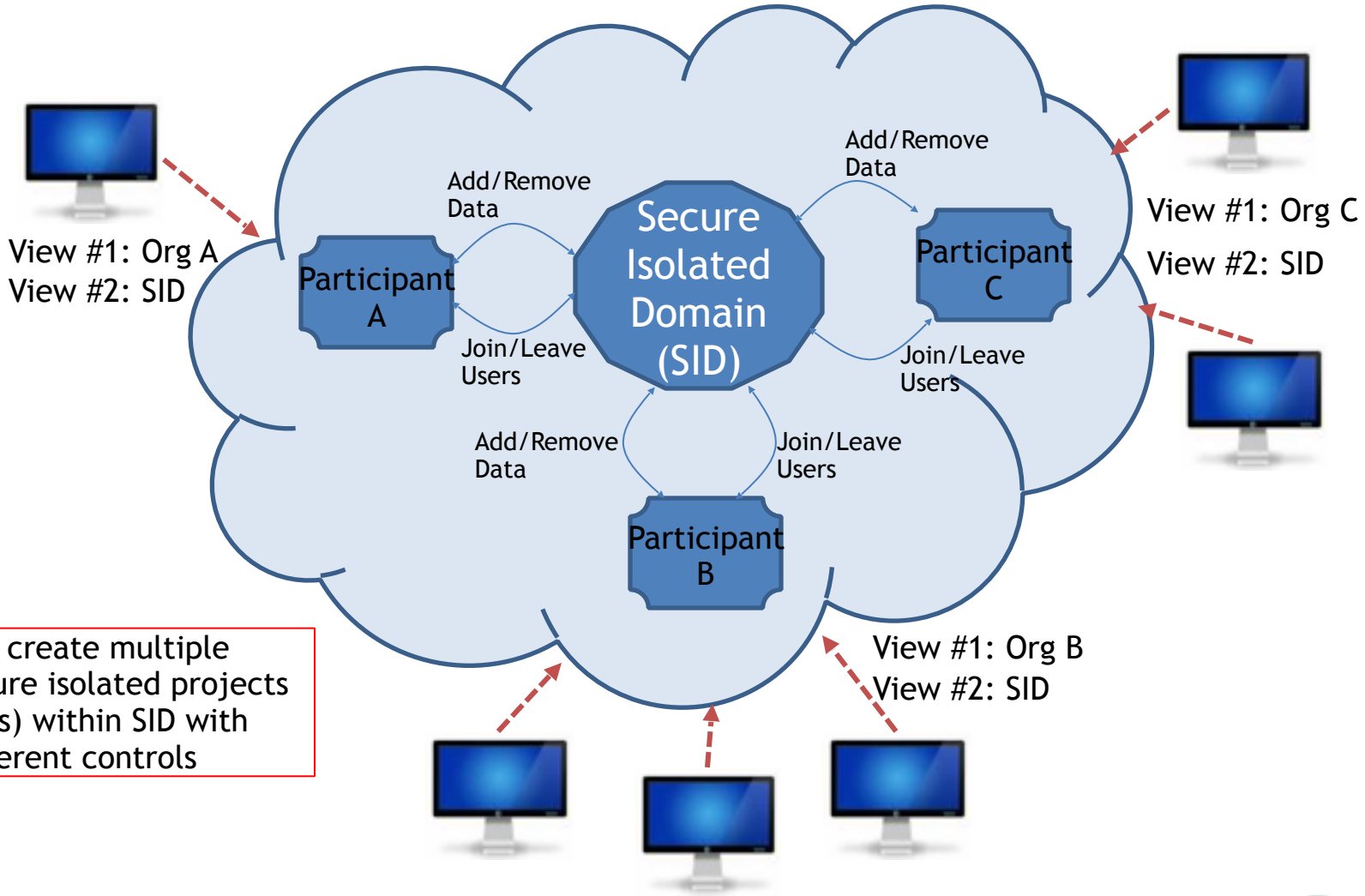
Cyber Collaboration in Cloud

- Cloud platform — IaaS
  - Community in Cloud
  - Cyber Security Committee.
  - Organizations routinely collect cyber information.
  - Cross organization cyber collaborations.

Secure Isolated Domain (SID) Model



Sharing Model in Cloud IaaS



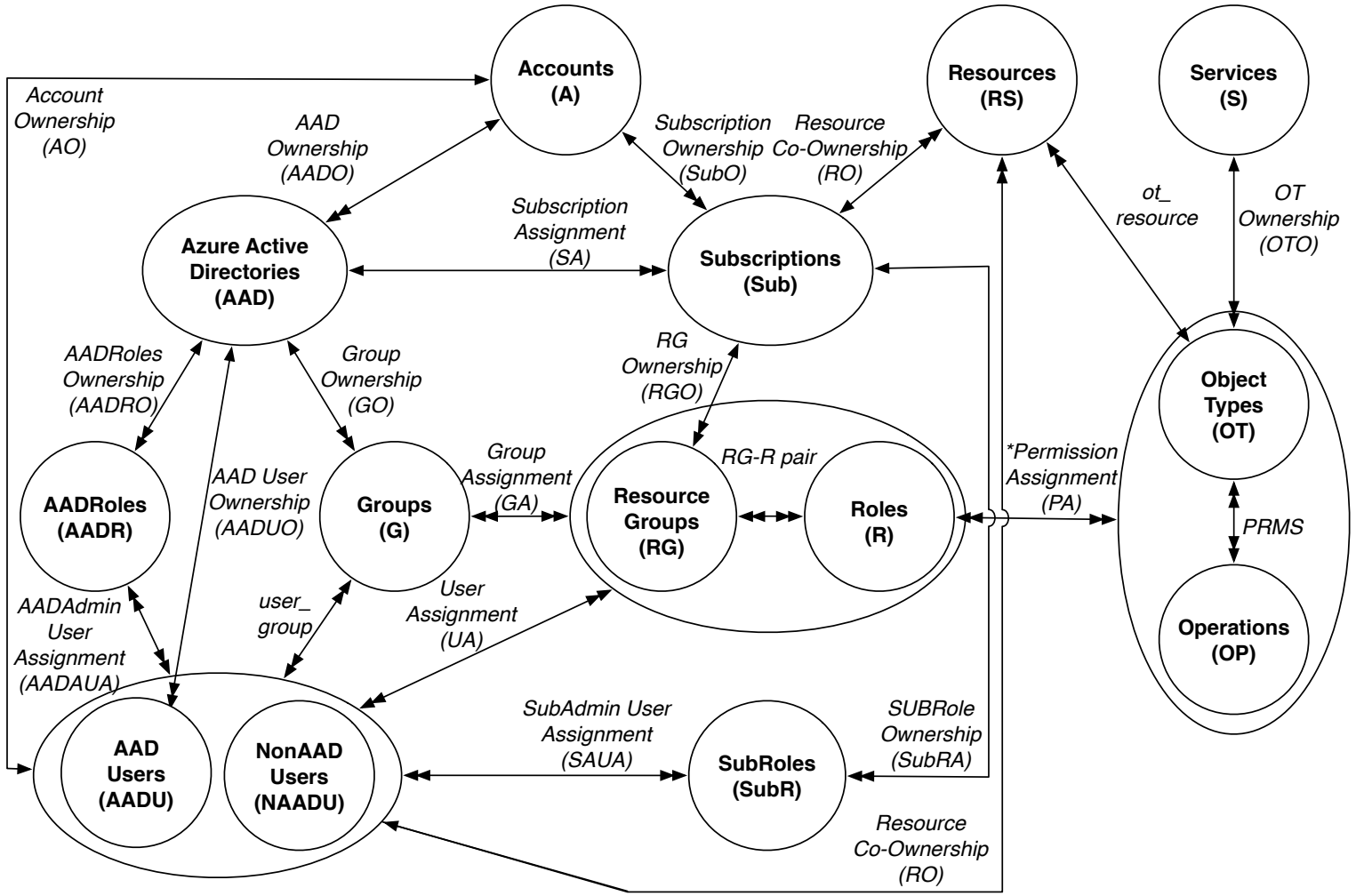
Can create multiple secure isolated projects (SIPs) within SID with different controls

Microsoft Azure

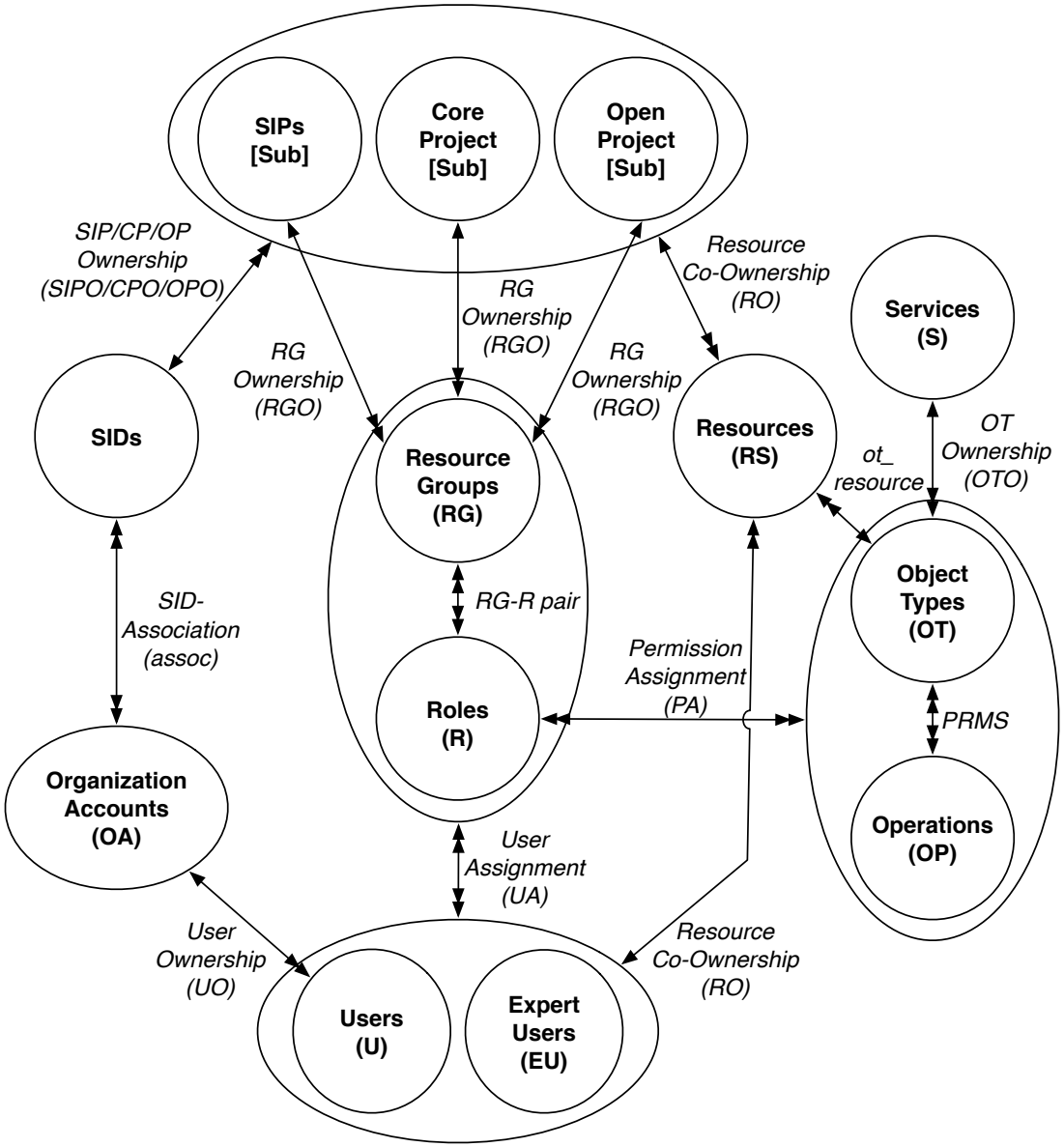
- Popular public cloud software
  - **Microsoft Azure:** is a cloud computing platform and infrastructure created by Microsoft for building, deploying, and managing applications and services through a global network of Microsoft-managed datacenters.

Ref: https://azure.microsoft.com/

Azure Access Control Model



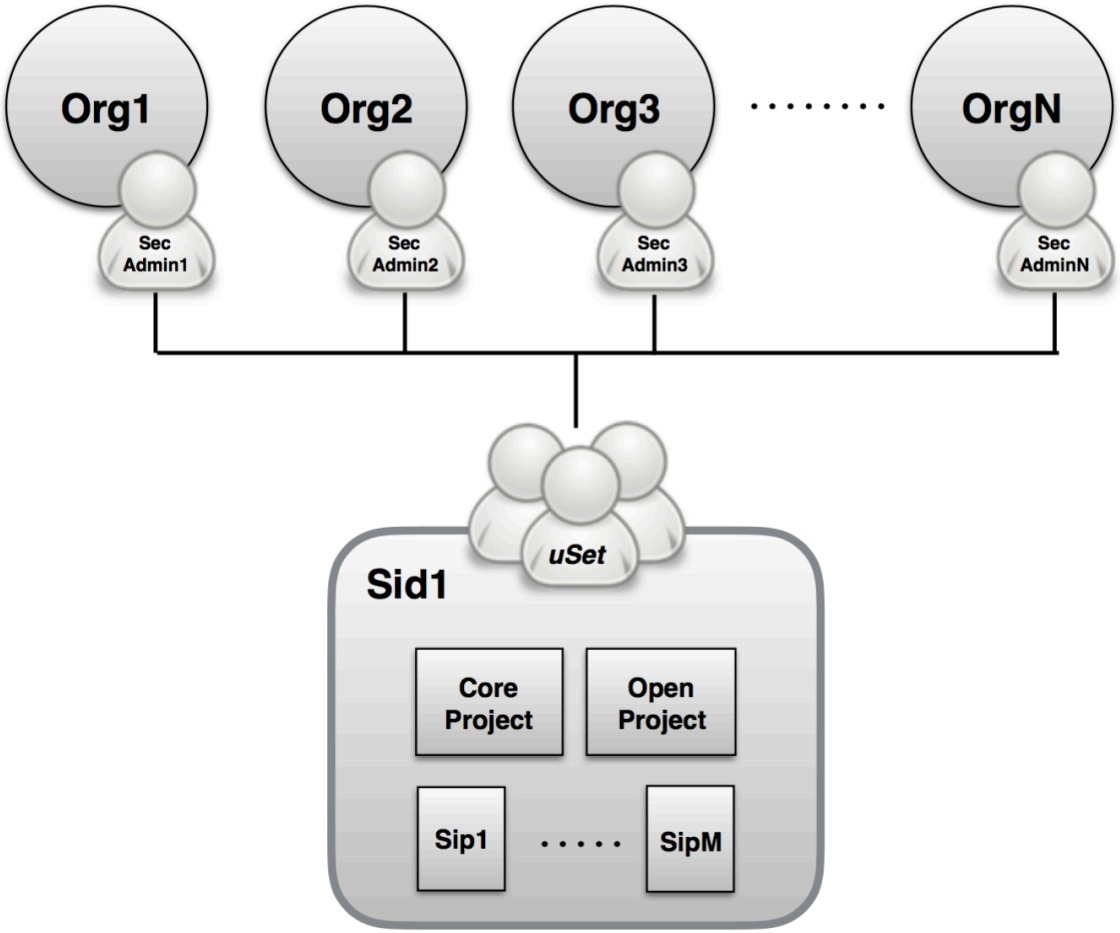
Azure Access Control Model with SID Extension



UTSA

I·C·S
The Institute for Cyber Security

SID Service

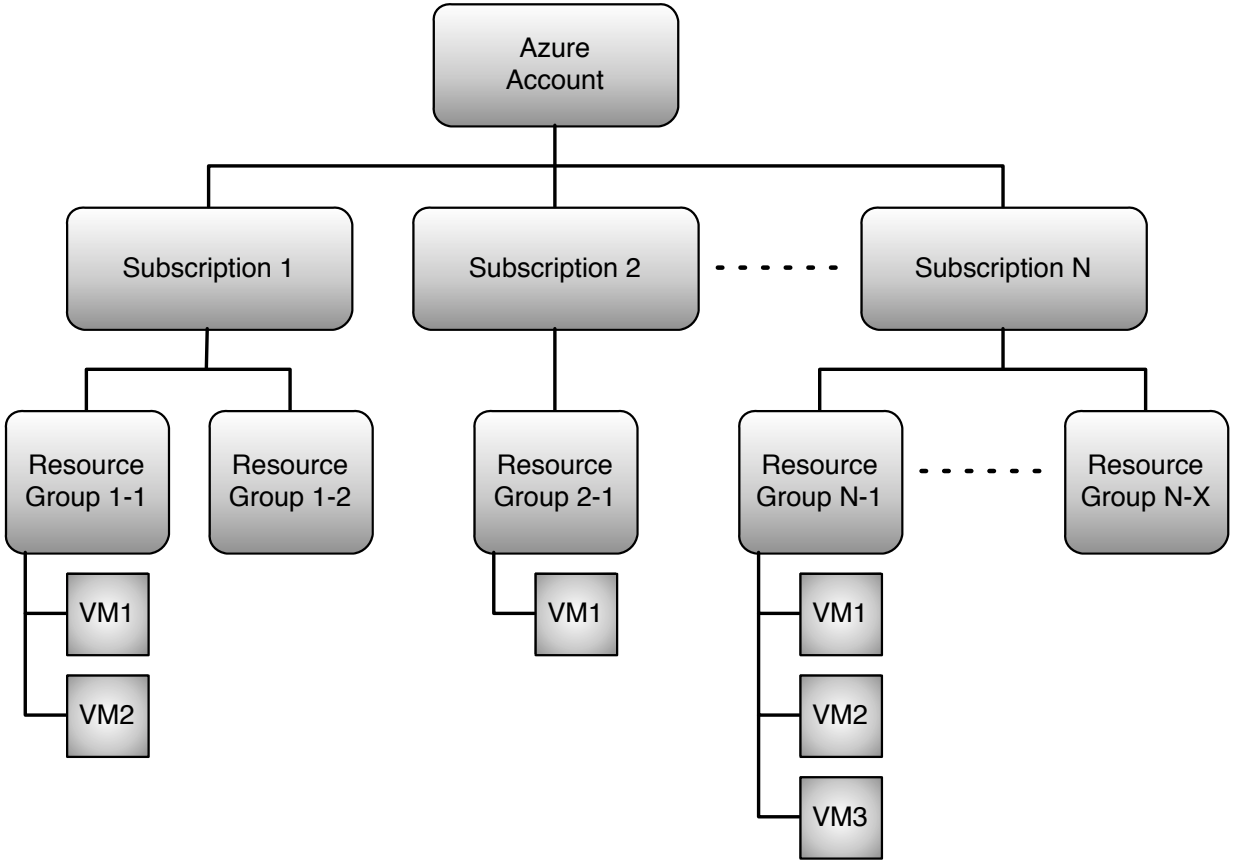


UTSA

I·C·S
The Institute for Cyber Security

Enforcement

- Azure Account Resource Division

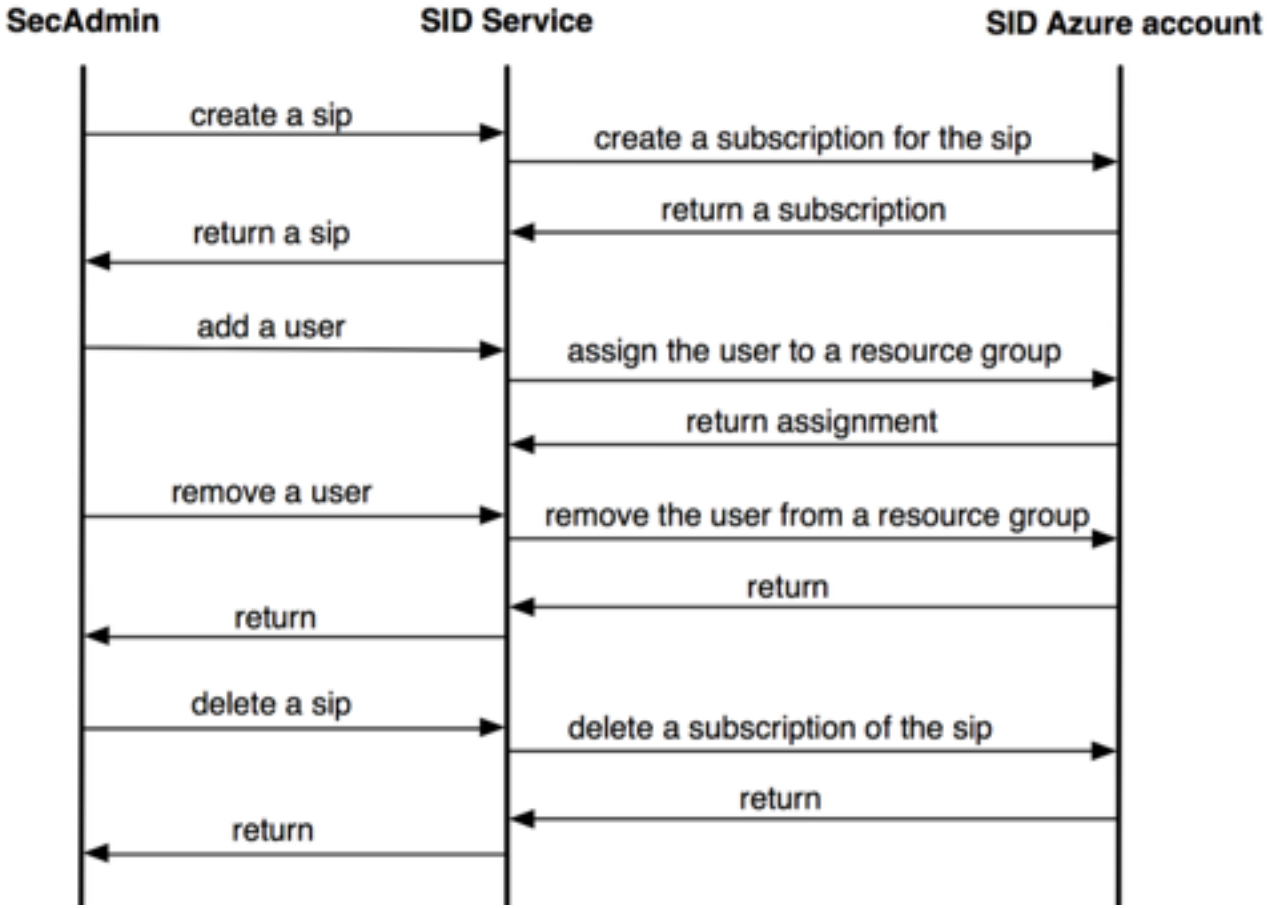


Enforcement

- Setting up SID service
  - Create two roles in the Core Project account: *CPadmin* and *CPmember*
    - *CPadmin* allows the user have limited administrative power to use the role *CPmember* and specify policies for users from his organization.
  - Create one role in the Open Project account: *OPmember*
    - *CPadmin* allows all users from the community to access the Open Project account.
  - SID manager maintains a list of security administrative users (*uSet*) from organizations.

Enforcement

- SIP request



Conclusion and future work

- Developed sharing models
  - Formal specification
- Enhanced Azure Cloud IaaS with SID/SIP capabilities
  - Cyber incident response capabilities
    - Self-service
    - SID/SIP specific security
    - Share data, tools, etc. in an isolated environment
    - Ability to execute and analyze malicious code in an isolated environment
- Future work
  - more fine grained access control within a SIP
  - compare SID/SIP enforcement on dominant IaaS cloud platforms (OpenStack, AWS and Azure)


Thanks!