Secure Information and Resource Sharing in Cloud Infrastructure as a Service

Cyber Incident Response

Models for Information and Resource Sharing

Amy(Yun) Zhang, Ravi Sandhu
Institute for Cyber Security
University of Texas at San Antonio
San Antonio, TX 78249
Mar 25, 2016

Presented by: Amy(Yun) Zhang

UTSA

I·C·S
The Institute for Cyber Security

Information and Resource Sharing

- Information sharing
  - exchanges of data between a sender and receiver
  - one-to-one, one-to-many, many-to-one, many-to-many
- Resource sharing
  - a computer resource made available from one host to other hosts on a computer network
  - computer programs, data, storage devices, and printers.
    - shared file access
    - shared printer access

Ref: https://en.wikipedia.org/wiki/

Cloud Computing

- Concept
  - a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand.
- Service models
  - Infrastructure as a service (IaaS)
    - computers(physical or virtual machines) and other resources.
    - AWS, Microsoft Azure, OpenStack.
  - Platform as a service (PaaS)
    - a development environment to application developers.
    - Salesforce, Microsoft Azure.
  - Software as a service (SaaS)
    - users gain access to application software and databases.
    - Google, Dropbox.

Ref: https://en.wikipedia.org/wiki/Cloud_computing

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.

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

- Focus on technical challenges
- 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
  - Often ad hoc
- What are the effective ways to facilitate sharing in such circumstances?
  - Information sharing models
  - Infrastructure, technologies, platforms

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.

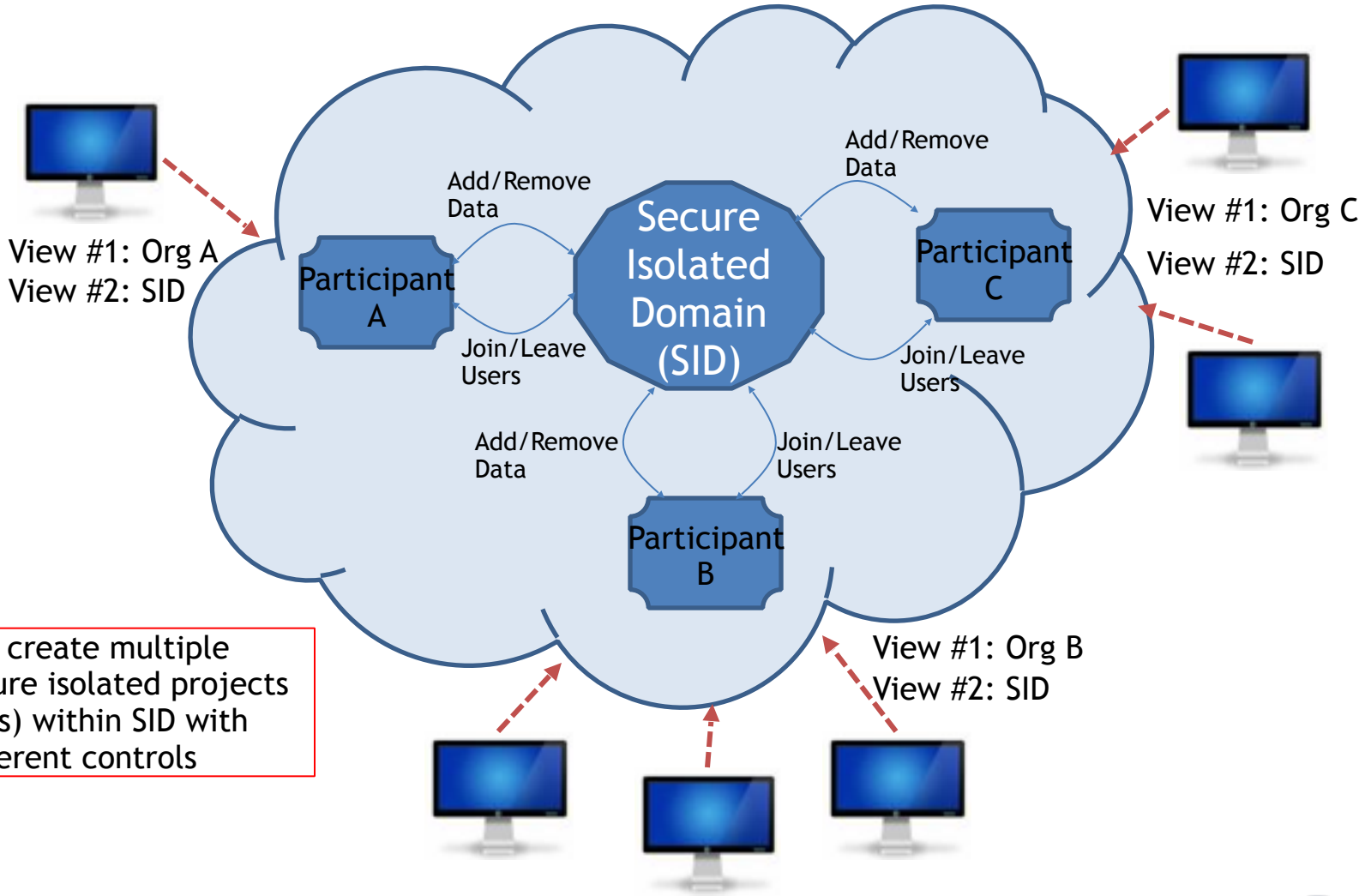
Cloud IaaS Advantages for Cyber Incident Sharing

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

Cloud IaaS Challenges for Cyber Incident Sharing

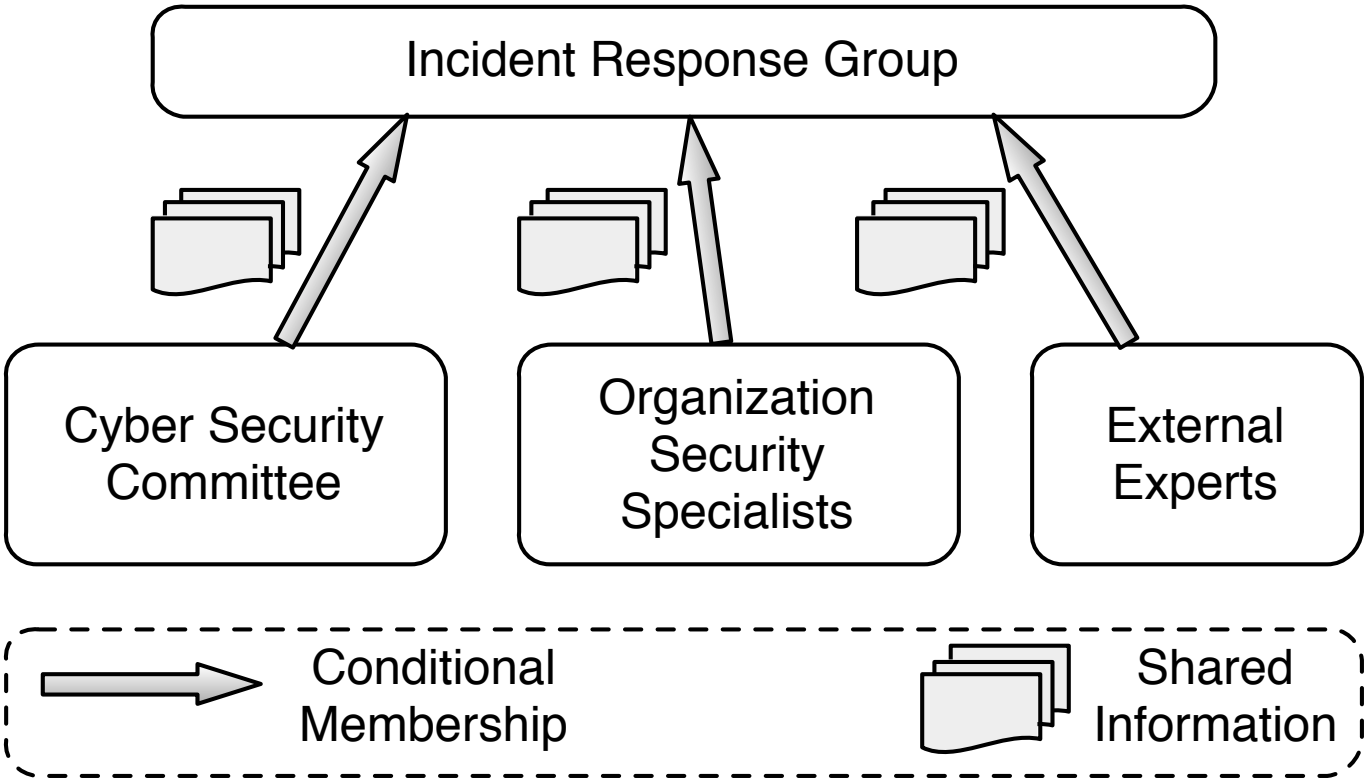
- IaaS clouds lack secure sharing models
  - Storage
  - Compute
  - Networks
- Need ability to snapshot tenant infrastructure, share, and control who can access
  - Share by copy

Sharing Model in Cloud IaaS



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

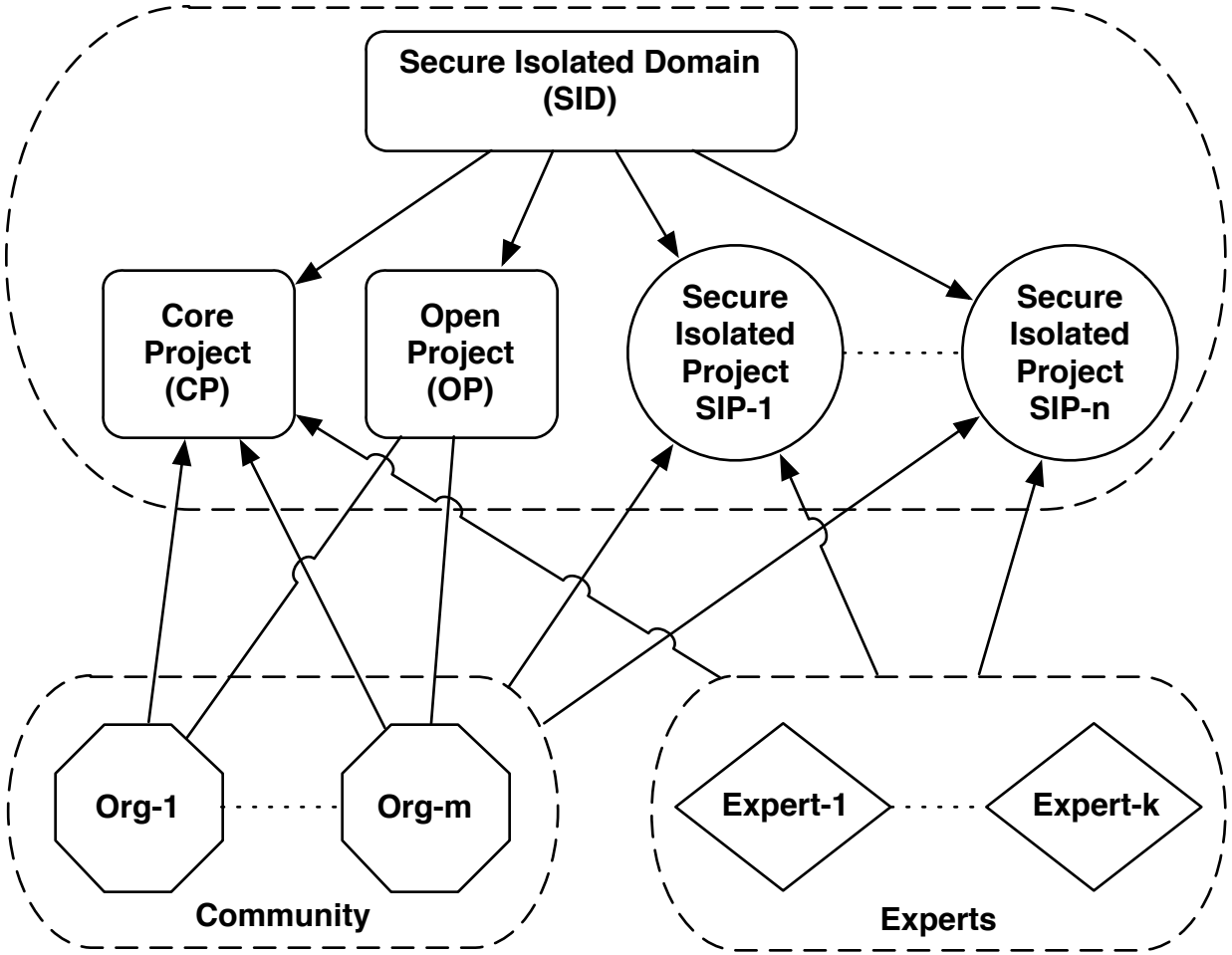
Community Cyber Incident Response Governance



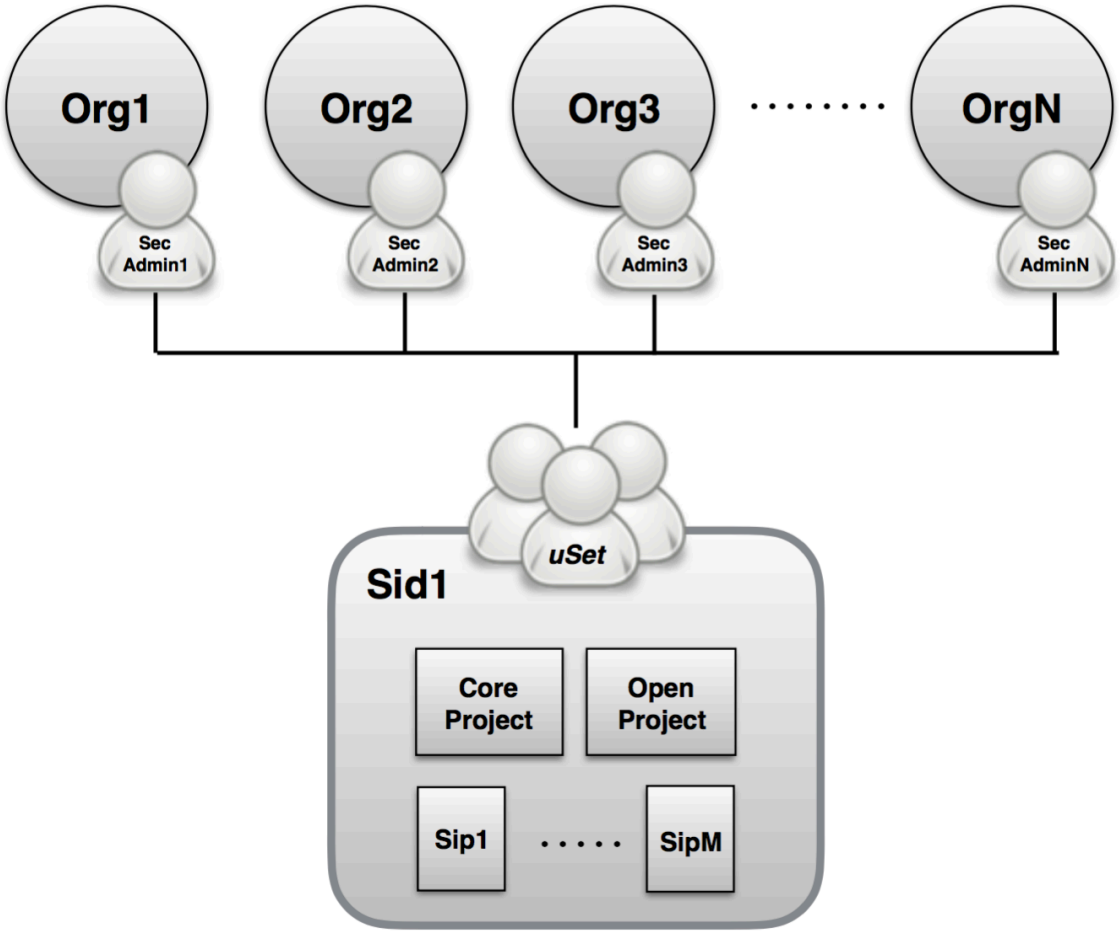
Cyber Collaboration in Cloud

- Cloud platform (community)
  - Cyber Security Committee.
  - Organizations routinely collect cyber information.
  - Cross organization cyber collaborations.

Secure Isolated Domain (SID) Model



SID Service



UTSA

I·C·S
The Institute for Cyber Security

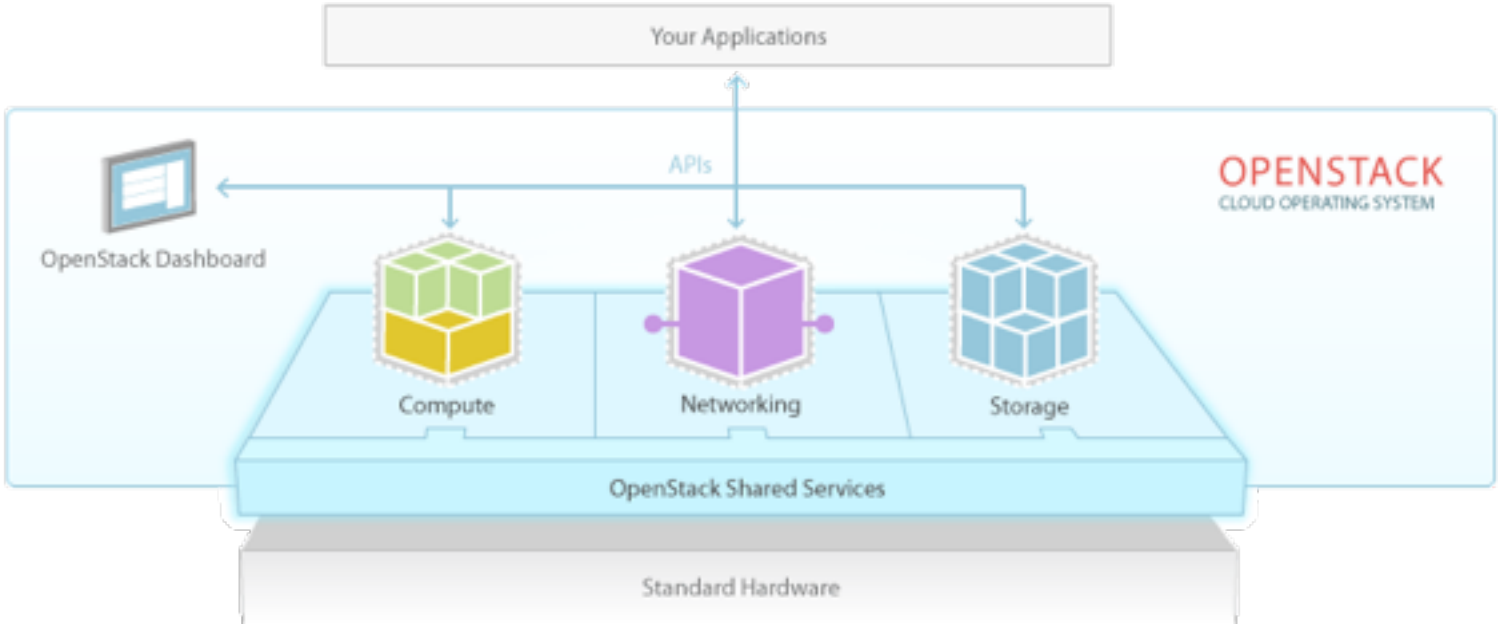
Overview

- Part I: OpenStack
- Part II: AWS
- Part III: Azure

OpenStack

- OpenStack
  - Dominant open-source cloud IaaS software

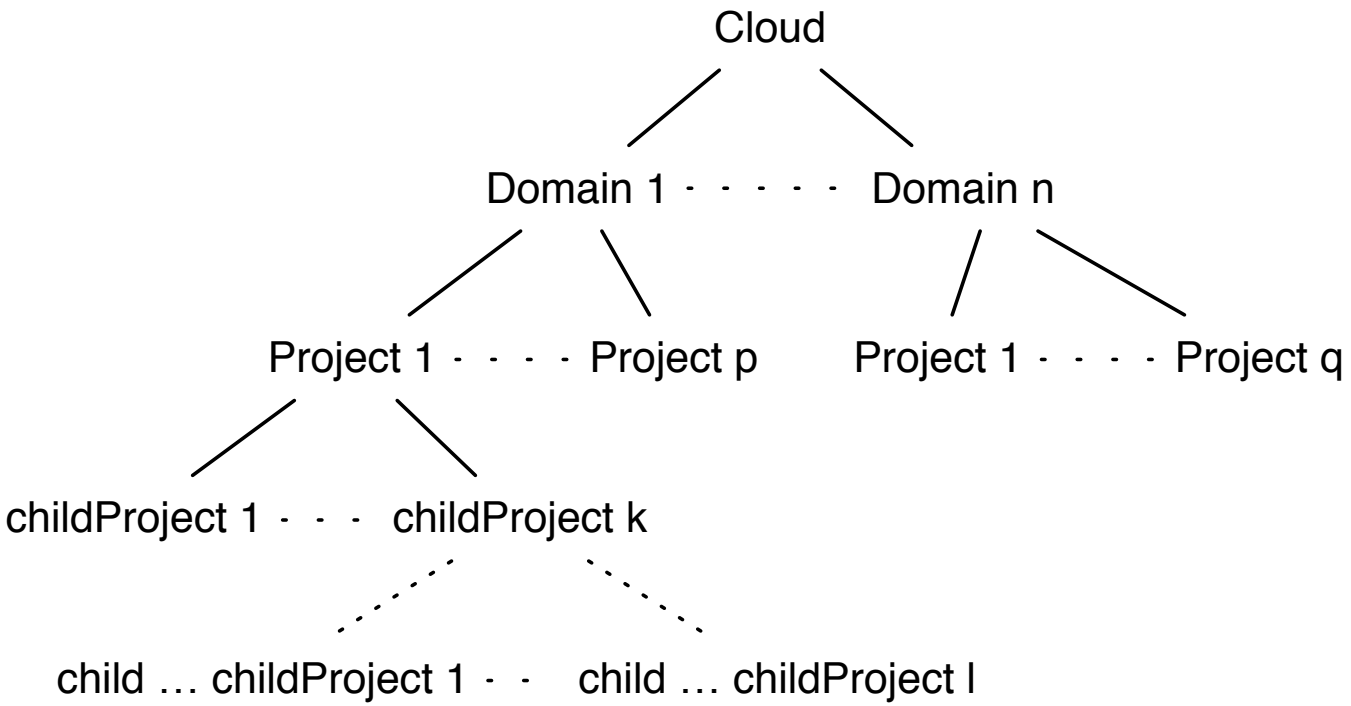
➢ > 200 companies
➢ ~14000 developers
➢ >130 countries



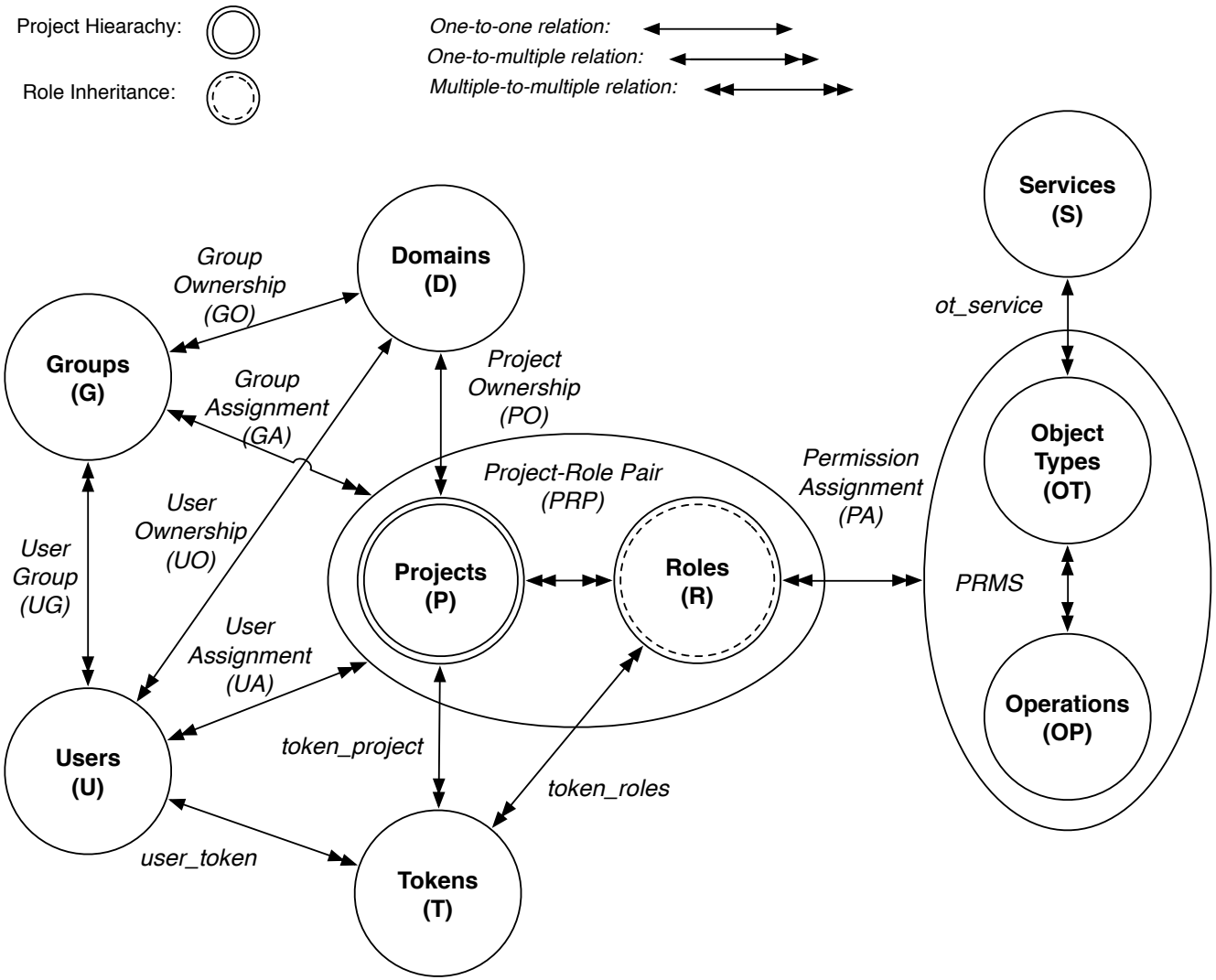
Ref: http://www.openstack.org

OpenStack HMT

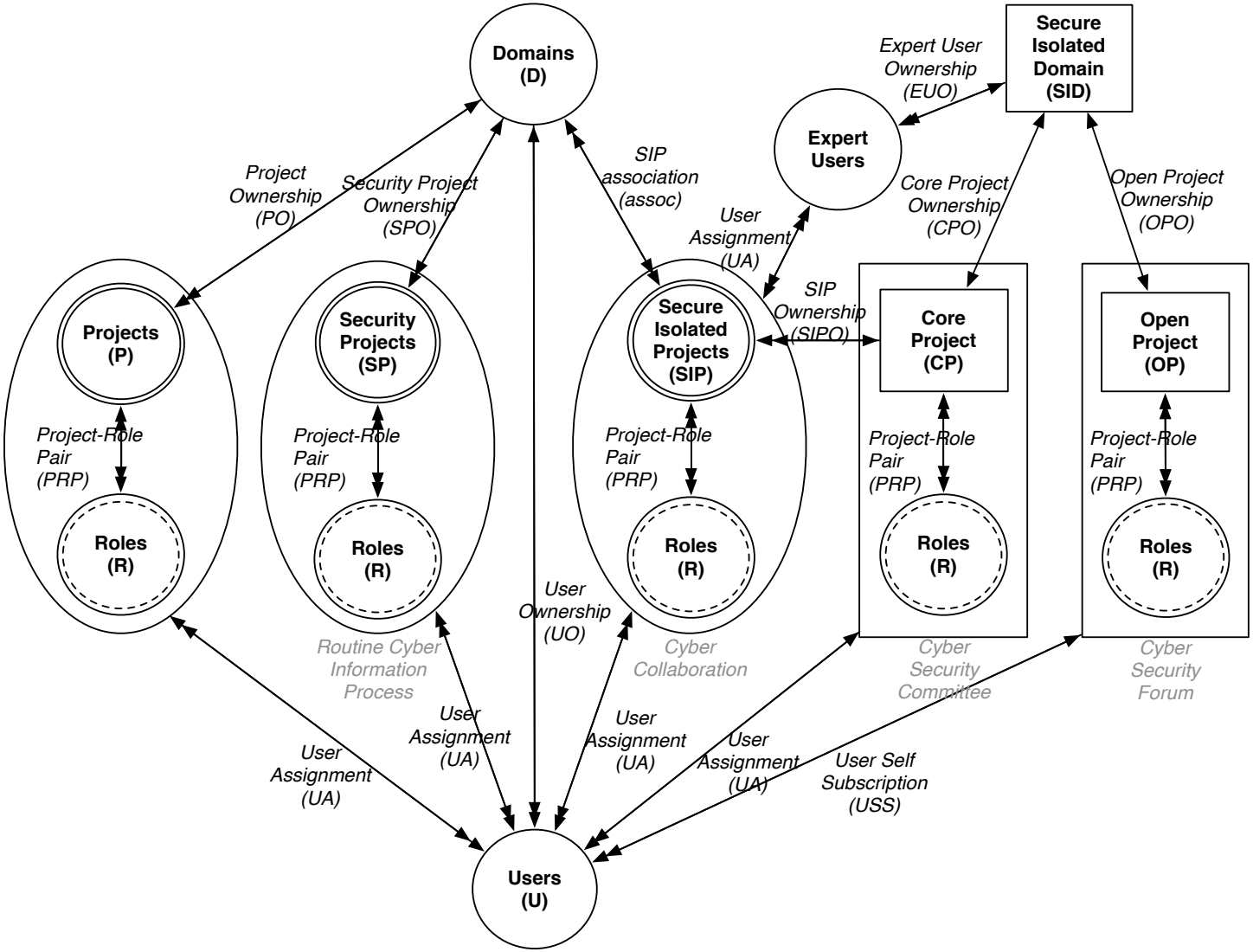
- HMT : Hierarchical Multitenancy



OSAC Model with HMT



OSAC-HMT-SID Model

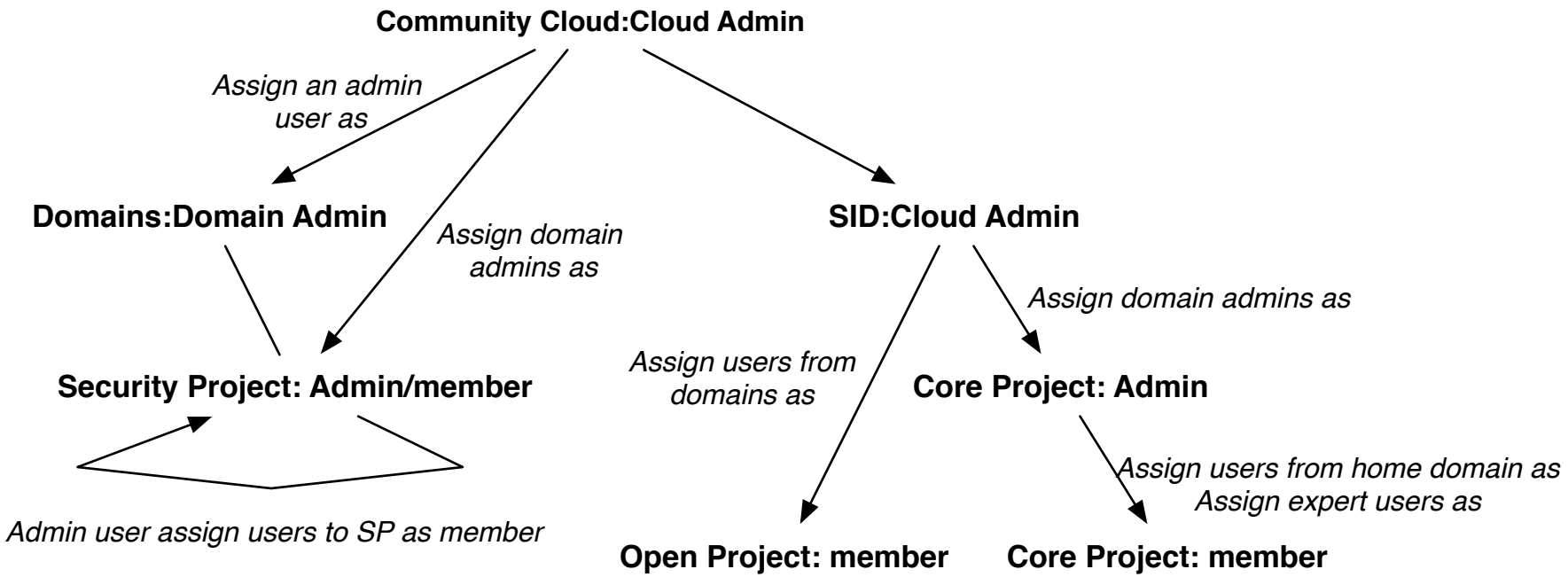


OSAC-SID Administrative Model

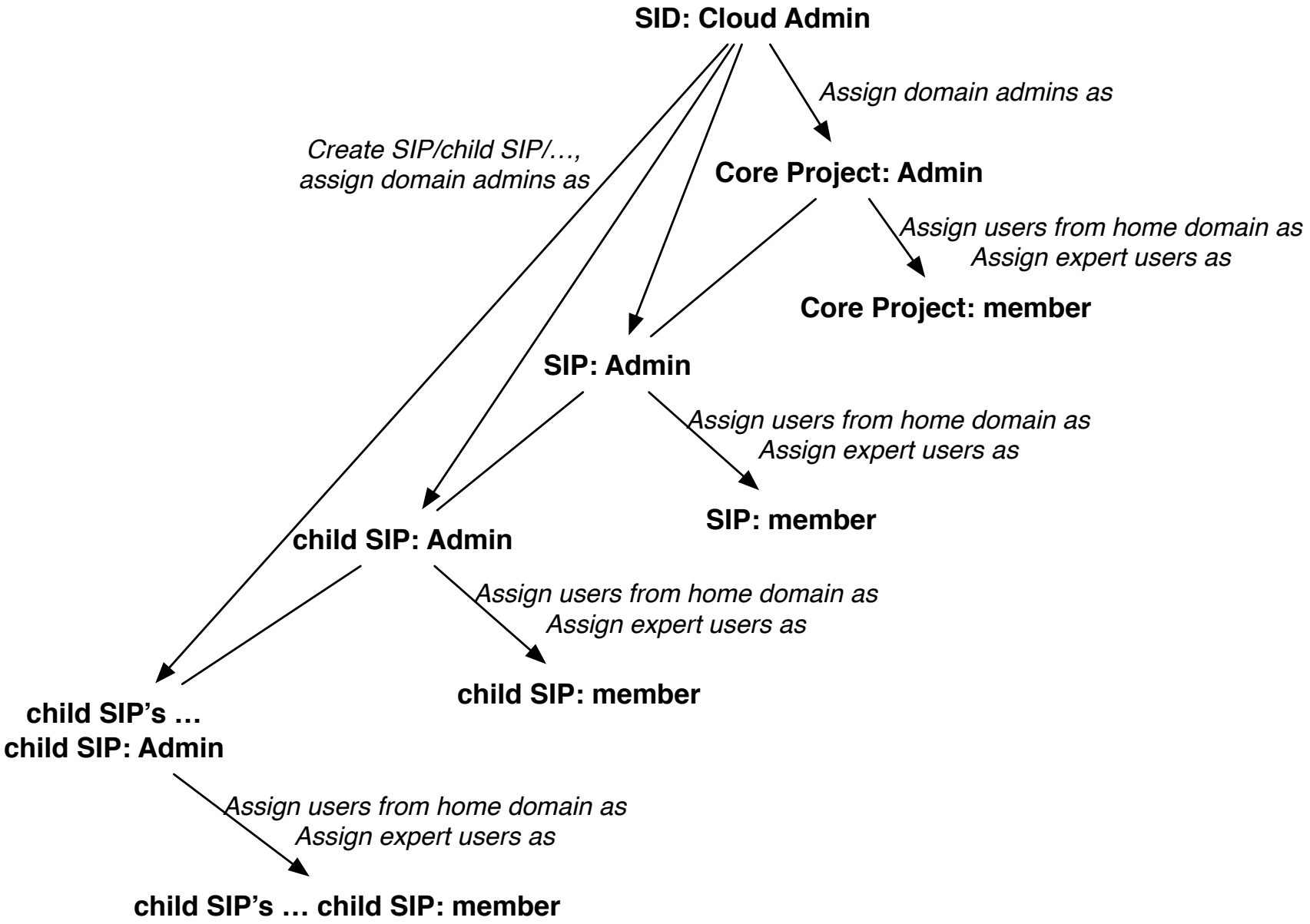
- **SipCreate(uSet, sip)**
  /* A subset of Core Project/domain admin users together create a sip */
- **SipDelete(uSet, sip)**
  /* The same subset of Core Project/domain admin users together delete a sip*/
- **UserAdd(adminuser, r, u, sp, p)**
  /* CP/Sip admin can add a user from his home domain Security Project to CP/sip*/
- **UserRemove(adminuser, r, u, sp, p)**
  /* CP/Sip admin can remove a user from the Core Project/sip */
- **OpenUserSubscribe(u, member, OP)**
  /* Users subscribe to Open Project */
- **OpenUserUnsubscribe(u, member, OP)**
  /* Users unsubcsribe from Open Project */
- **CopyObject(u, so1, sp, so2, p)**
  /* Copy object from Security Project to Core Project/SIP */
- **ExportObject(adminuser, so1, p, so2, sp)**
  /* Export object from Core Project/SIP to Security Project */
- **ExpertUserCreate(coreadmin, eu)**
  /* Core Project admin users can create an expert user */
- **ExpertUserDelete(coreadmin, eu)**
  /* Core Project admin users can delete an expert user */
- **ExpertUserList(adminuser)**
  /* Admin users of Core Project and SIPs can list expert users */
- **ExpertUserAdd(adminuser, r, eu, proj)**
  /* Core Project/sip admin can add an expert user to Core Project/sip*/
- **ExpertUserRemove(adminuser, r, eu, proj)**
  /* Core Project/sip admin can remove an expert user from Core Project/sip */

Enforcement

- Set up the cloud



Enforcement



Overview

- Part I: OpenStack
- Part II: AWS
- Part III: Azure

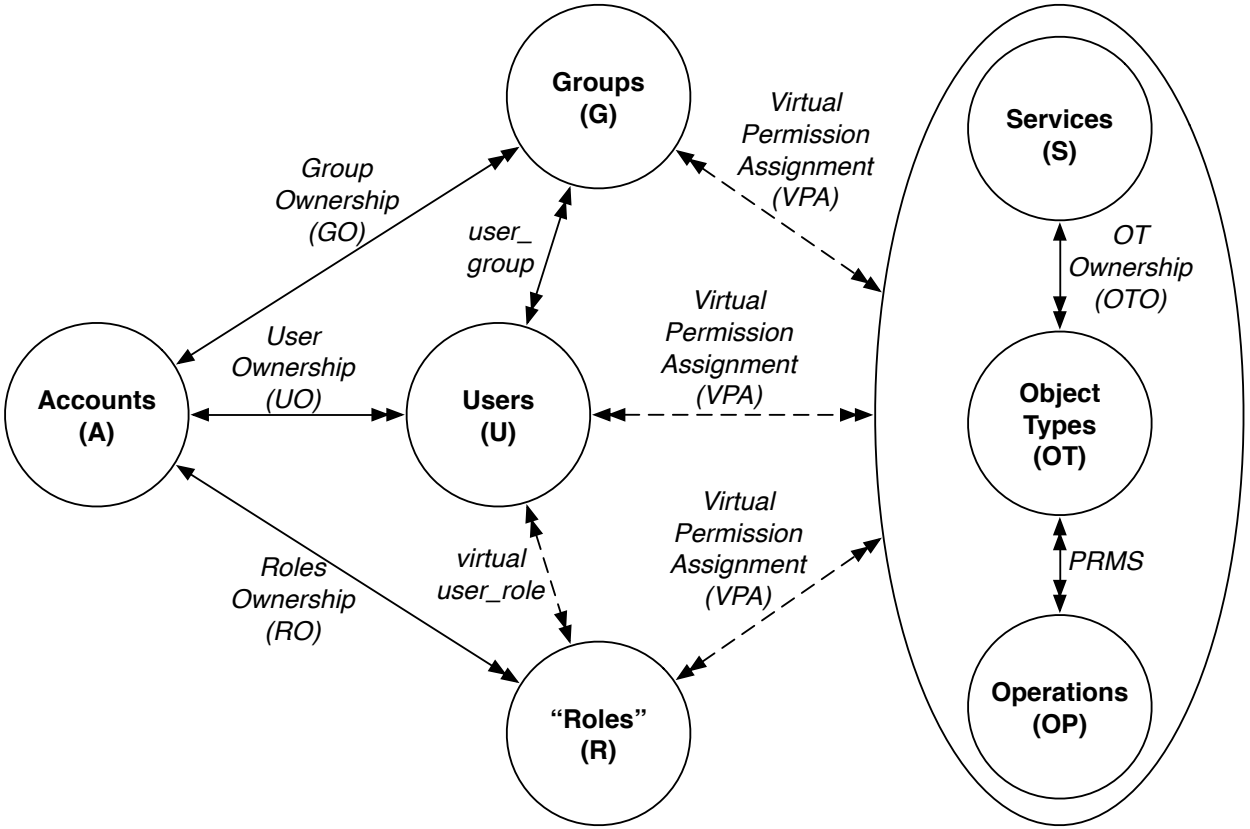
Amazon Web Service (AWS)

- Dominant public cloud software
  - **Amazon Web Services** (**AWS**), a collection of remote computing services, also called web services, make up a cloud-computing platform offered by Amazon.com.

Ref: https://en.wikipedia.org/wiki/Amazon_Web_Services

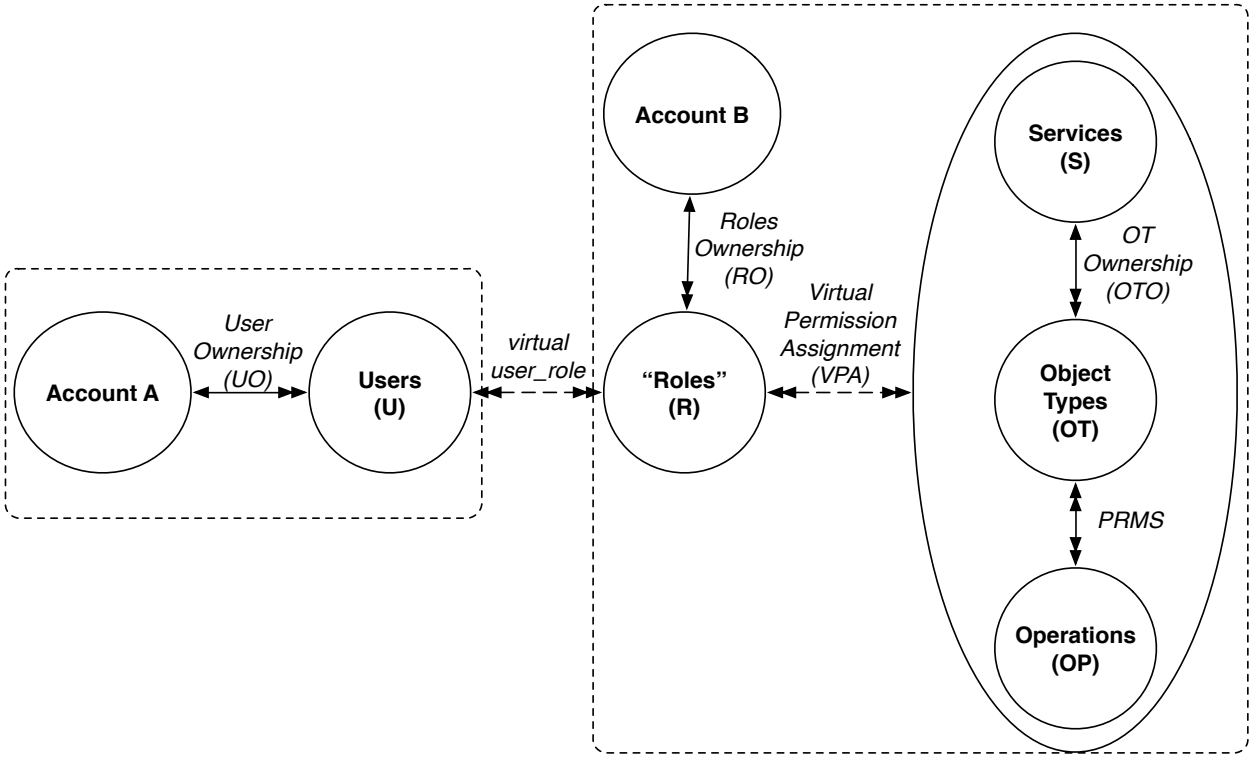
AWS Access Control Model

- AWS Access Control within a Single Account

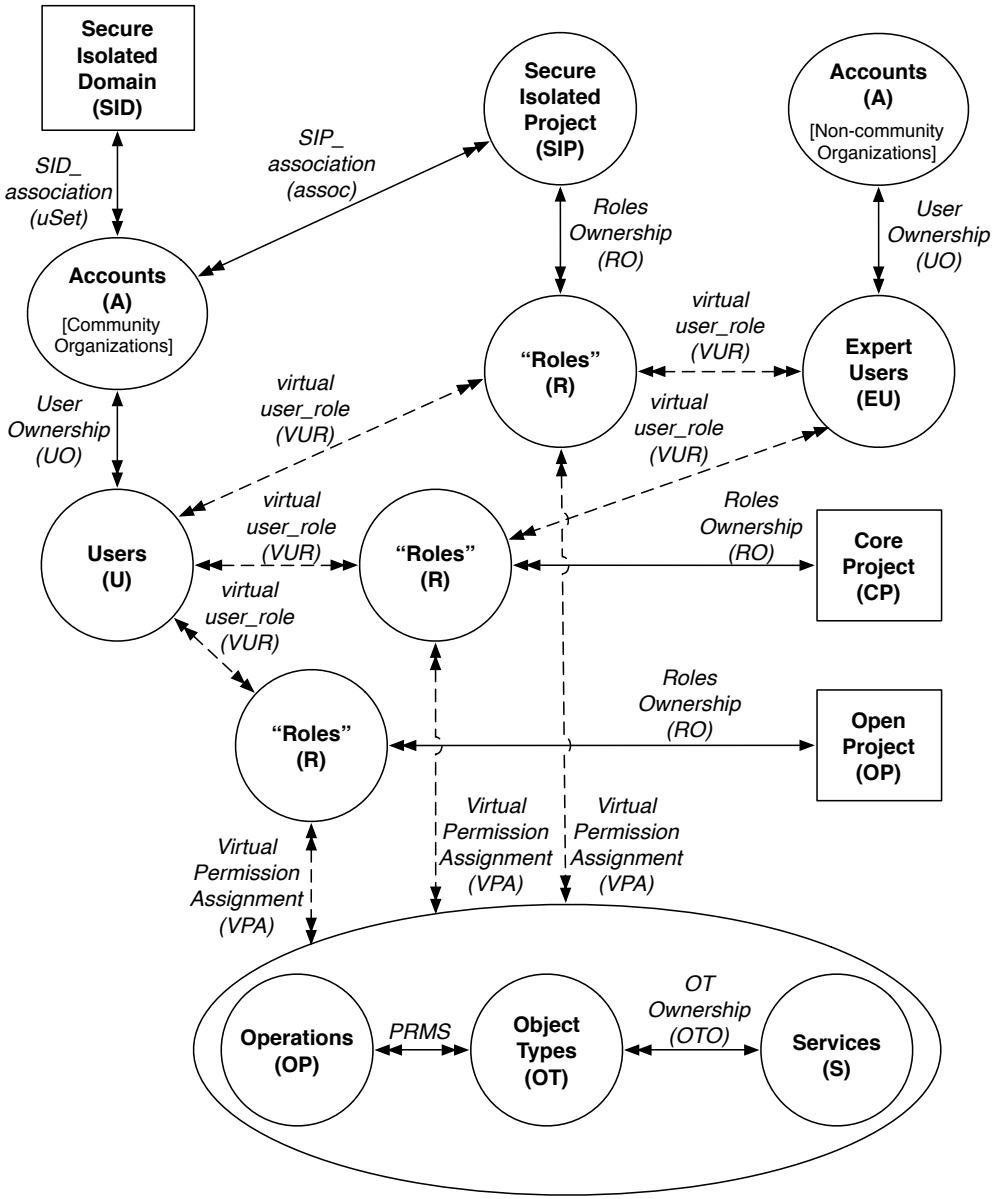


AWS Access Control Model

- AWS Access Control Across Accounts [Users in account A access services and resources in account B]



AWS Access Control Model with SID Extension



UTSA

I·C·S
The Institute for Cyber Security

AWSAC-SID Administrative Model

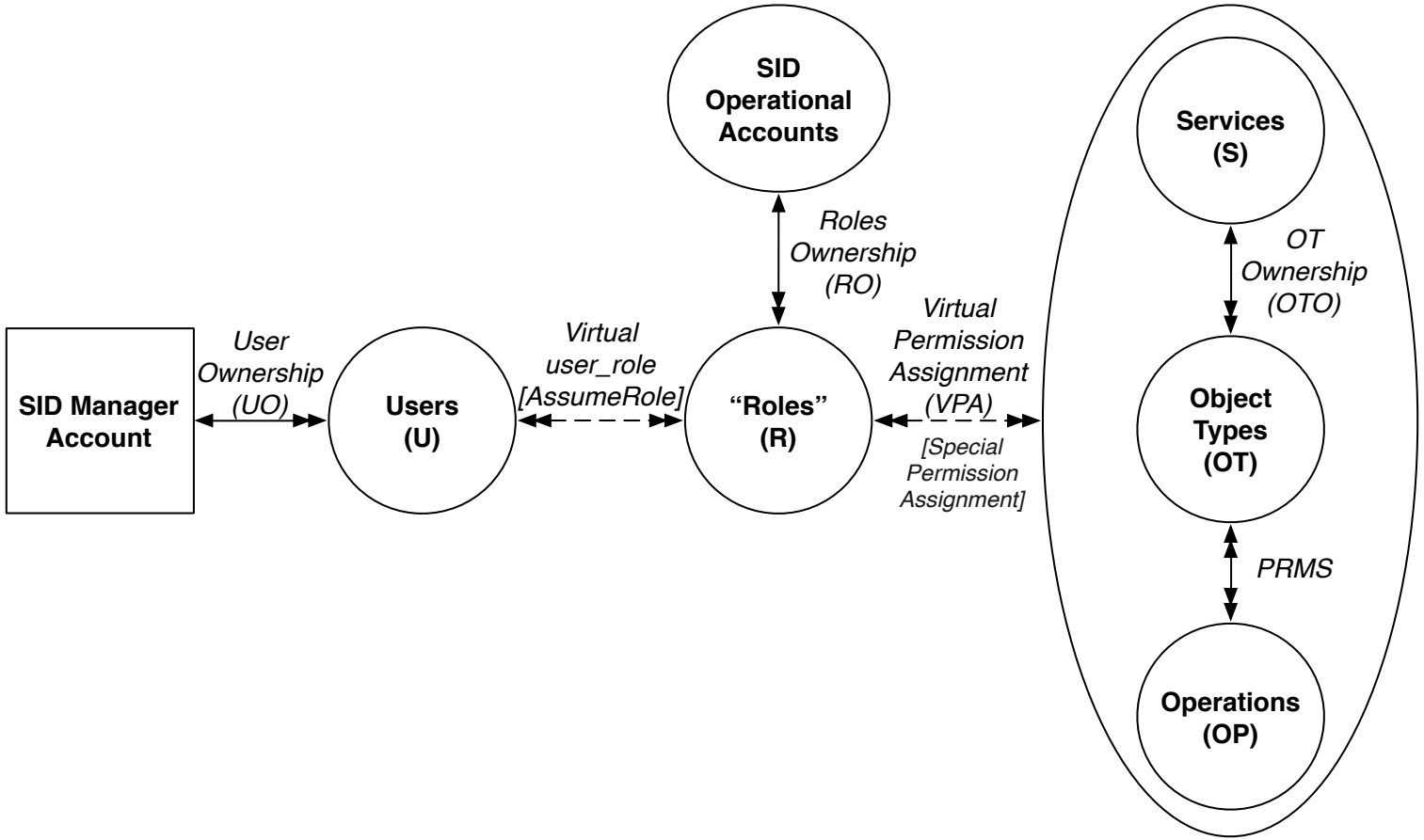
- **SipCreate(subuSet, sip)**
  /* A subset of organization security admin users together create a sip */
- **SipDelete(subuSet, sip)**
  /* The same subset of security admin users together delete a sip */
- **CpUserAdd(adminu, u)**
  /* CP admin add a user from his home account to CP */
- **CpUserRemove(adminu, u)**
  /* CP admin remove a user from CP */
- **SIPUserAdd(adminu, u, r, sip)**
  /* Sip admin add a user from his home account to SIP */
- **SIPUserRemove(adminu, u, r, sip)**
  /* Sip admin remove a user from SIP */
- **OpenUserAdd(u)**
  /* Users add themselves to OP */
- **OpenUserRemove(u)**
  /* Users remove themselves from OP */

AWSAC-SID Administrative Model

- **CpEUserAdd(adminu, eu)**
  /* CP admin add an expert user to CP */
- **CpEUserRemove(adminu, eu)**
  /* CP admin remove an expert user from CP */
- **SipEUserAdd(adminu, eu, r, sip)**
  /* SIP admin add an expert user to SIP */
- **SipEUserRemove(adminu, eu, r, sip)**
  /* SIP admin remove an expert user from SIP */
- **CpCopyObject(u, o1, o2)**
  /* Users copy object from organization accounts to CP */
- **CpExportObject(adminu, o1, o2)**
  /* Admin users export object from CP to organizations accounts */
- **SipCopyObject(u, r, o1, o2, sip)**
  /* Users copy object from organization accounts to a SIP */
- **SipExportObject(adminu, o1, o2, sip)**
  /* Admin users export object from SIP to organization accounts */

Enforcement

- SID Service Setting-up

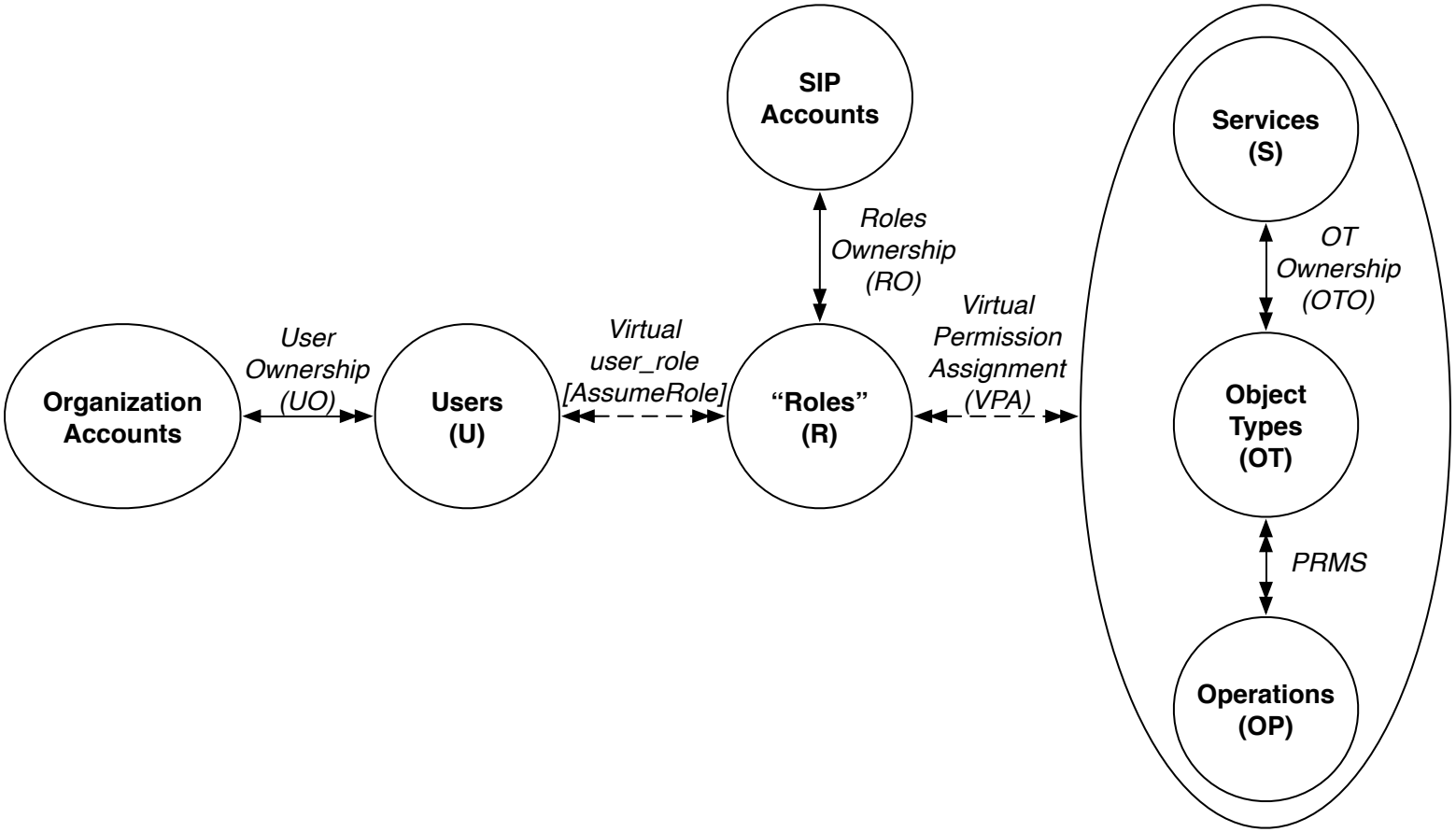


Enforcement

- 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 User Assignment



Enforcement

- SIP request handling
  - Users from *uSet* send a SIP request to SID manager
  - SID manager creates a SIP
  - SID manager associates the group of organizations to the SIP
  - Two roles are created in the SIP account: *SIPadmin* and *SIPmember*
    - *SIPadmin* allows the user have limited administrative power to use the role *SIPmember* and specify policies for users from organizations to join the SIP
  - SID manager returns an SIP account number with the name of the *SIPadmin* role to each user from *uSet*.

Overview

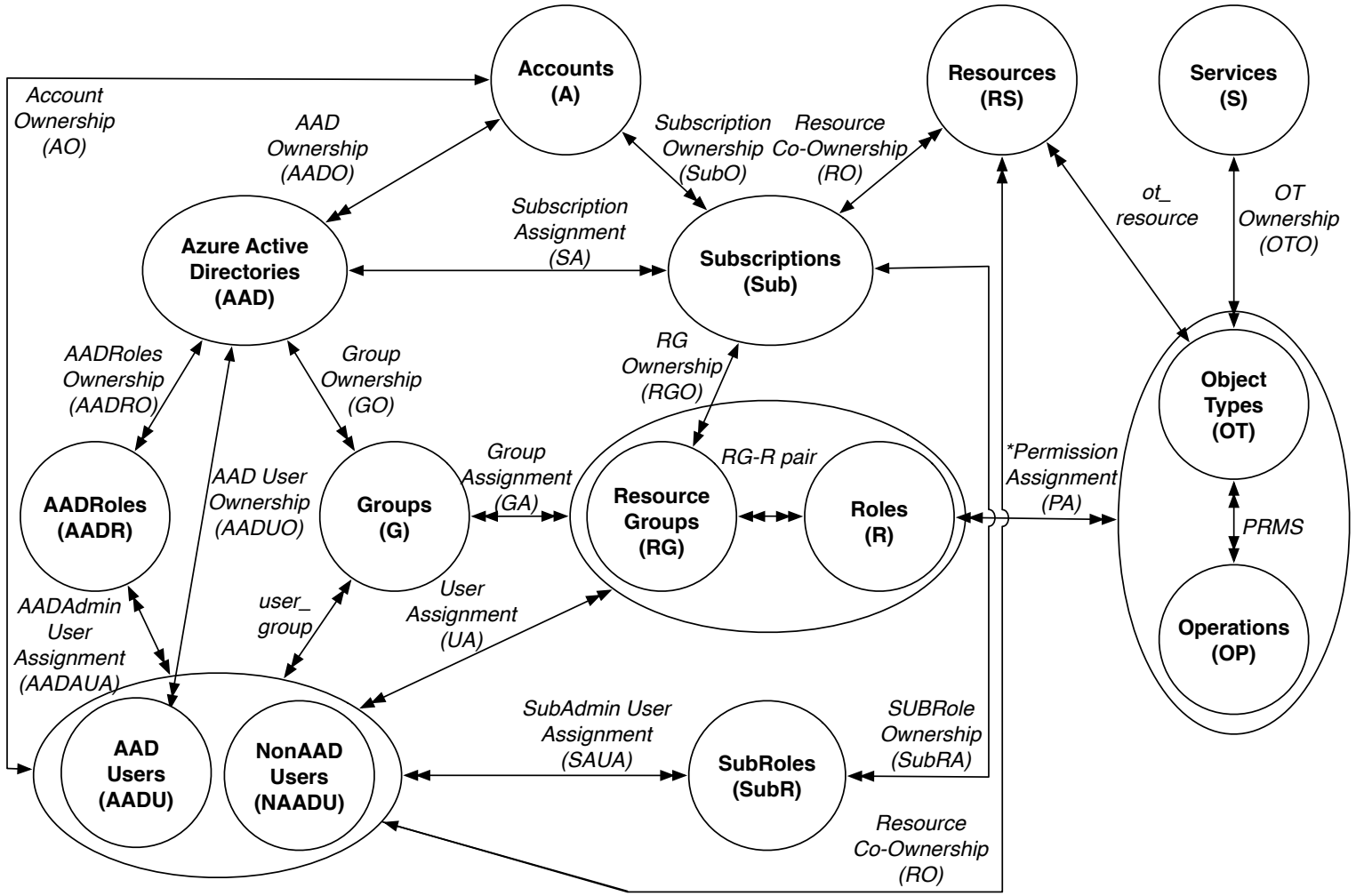
- Part I: OpenStack
- Part II: AWS
- Part III: Azure

Microsoft Azure

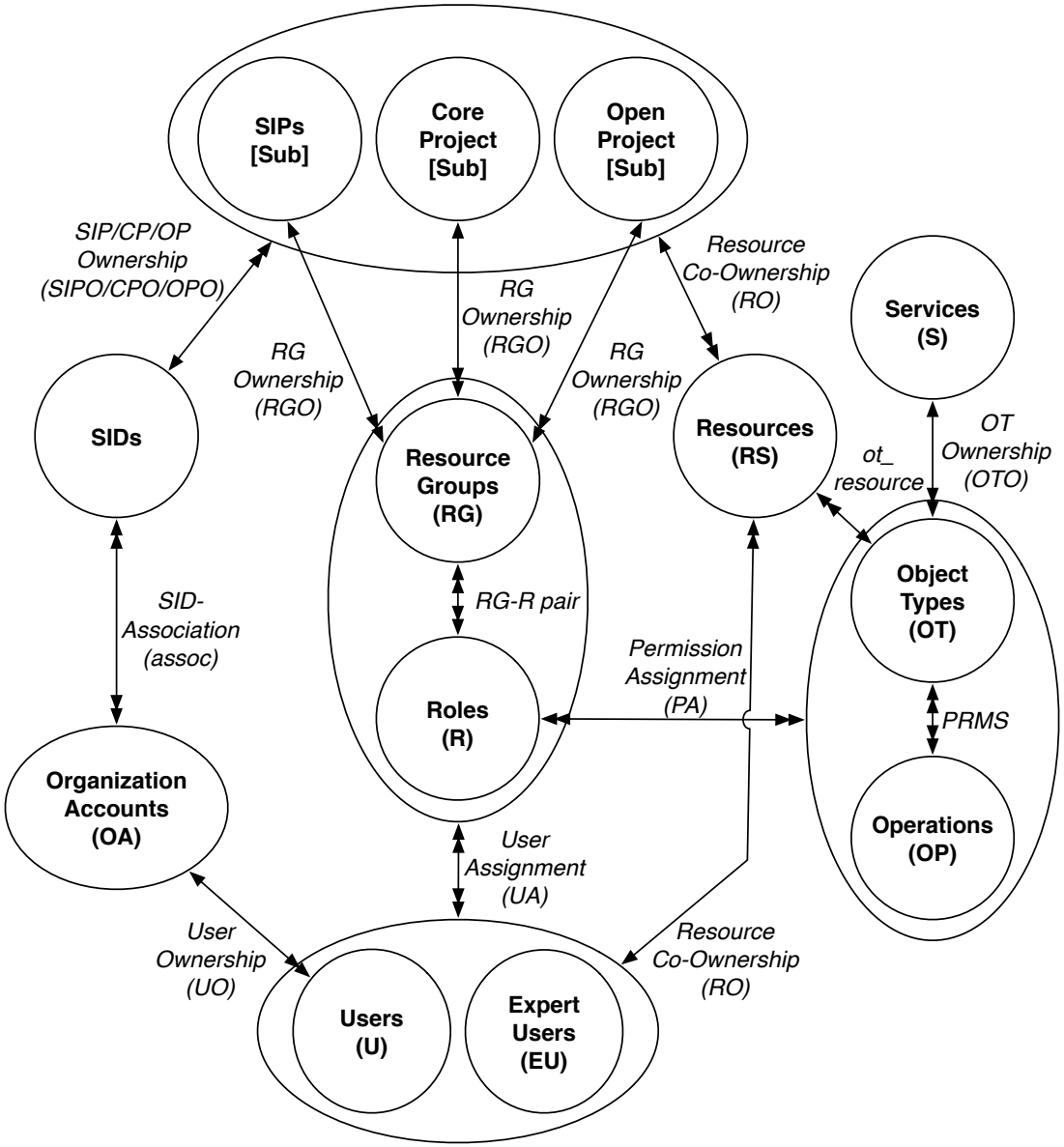
- Popular public cloud software
  - **Microsoft Azure:** is a cloud computing platform and infrastructure created by Microsoft for building, deploying, and managing applications and services through a global network of Microsoft-managed datacenters.

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

Azure Access Control Model



Azure Access Control Model with SID Extension



UTSA

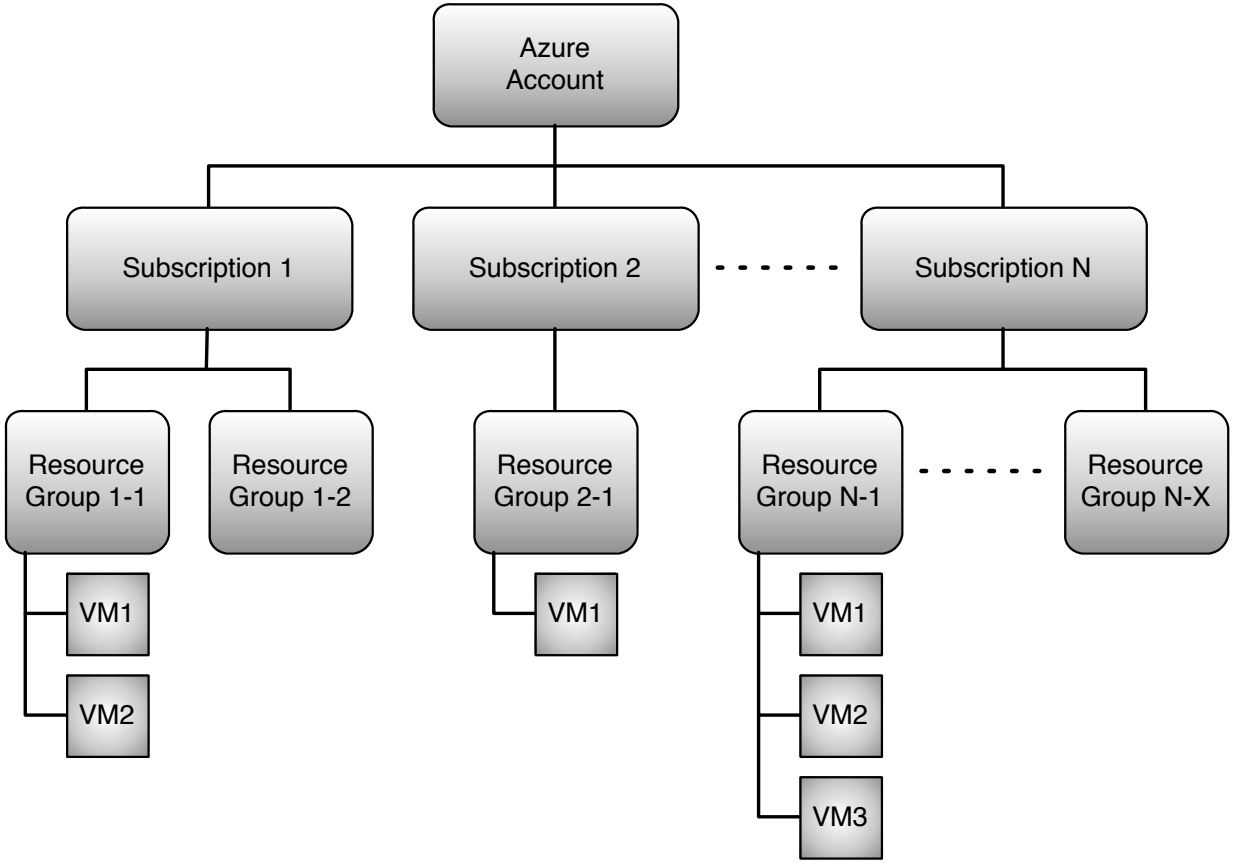
I·C·S
The Institute for Cyber Security

AzureAC-SID Administrative Model

- **SipCreate(uSet, sip, sid)**
  /* A set of organization security admin users together create a sip */
- **SipDelete(subuSet, sip, sid)**
  /* The same set of security admin users together delete a sip */
- **UserAdd(adminu, u, p, sid)**
  /* Admin users add a user from his home account to a Cp/Sip */
- **UserRemove(adminu, u, p, sid)**
  /* Admin users remove a user from a Cp/Sip */
- **OpenUserAdd(u, op, sid)**
  /* Users add themselves to a Op */
- **OpenUserRemove(u, op, sid)**
  /* Users remove themselves from a Op */
- **ExpertUserAdd(adminu, eu, p, sid)**
  /* Admin users add an expert user to a Cp/Sip */
- **ExpertUserRemove(adminu, eu, p, sid)**
  /* Admin users remove an expert user from a Cp/Sip */
- **CopyObject(u, o1, o2, p)**
  /* Users copy object from organization accounts to a Cp/Sip */
- **ExportObject(adminu, o1, o2, p)**
  /* Admin users export object from a Cp/Sip to organizations accounts */

Enforcement

- Azure Account Resource Division

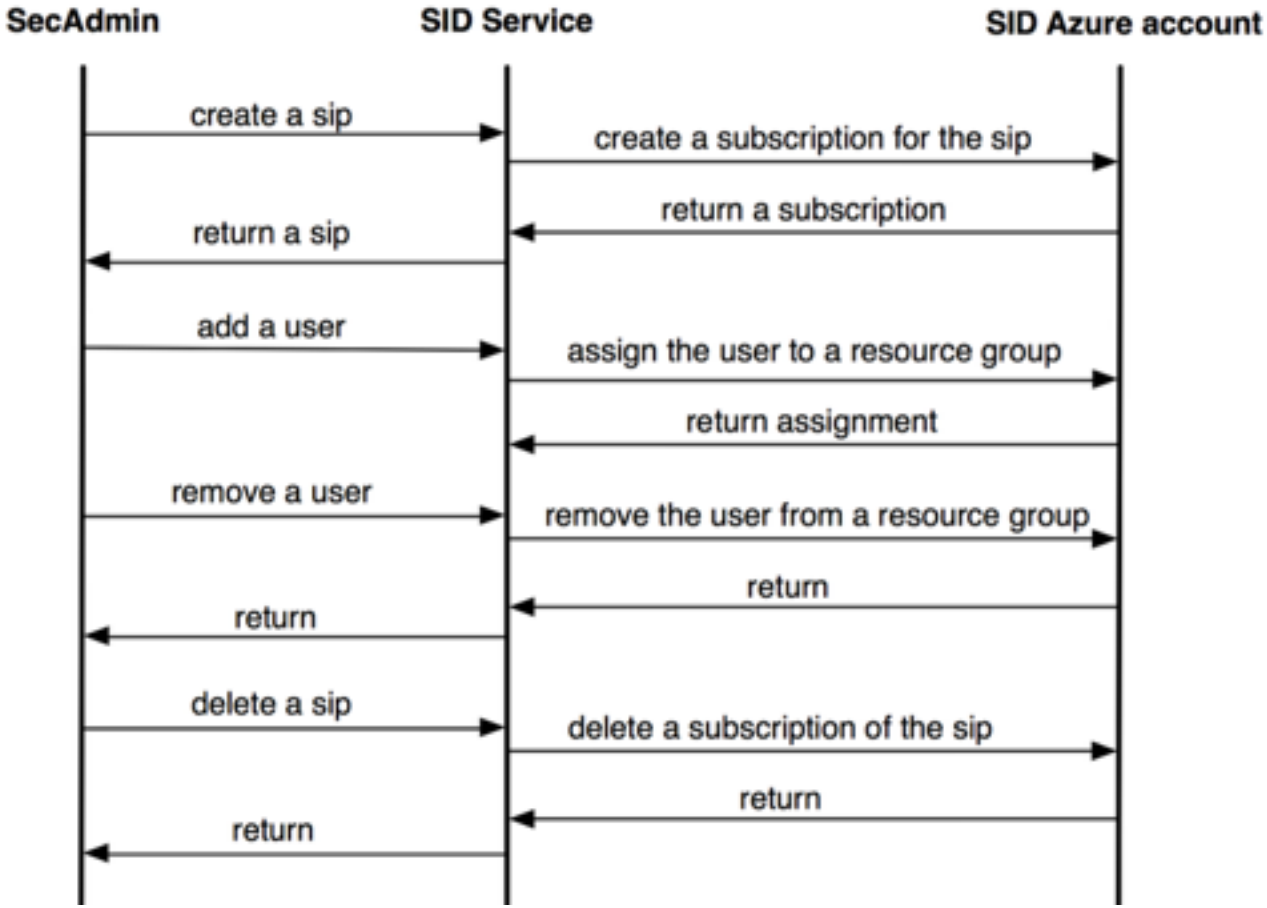


Enforcement

- 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 Dominant 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
  - Practitioners can deploy a “cyber incident response” cloud
- Future work
  - more fine grained access control within a SIP


Thanks!