Hierarchical Secure Information and Resource Sharing in OpenStack Community Cloud

Cyber Incident Response

An Model for Information and Resource Sharing

Amy(Yun) Zhang, Farhan Patwa, Ravi Sandhu, Bo Tang
Institute for Cyber Security
University of Texas at San Antonio
Aug 15, 2015

Presented by: Amy(Yun) Zhang

UTSA

I·C·S
The Institute for Cyber Security

Community Cloud

- Community cloud provides services for exclusive use by a specific community, which contains organizations with shared concern, such as mission, security requirements, business models, etc.
    - A community of financial organizations
    - OpenStack

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 in community
    - 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

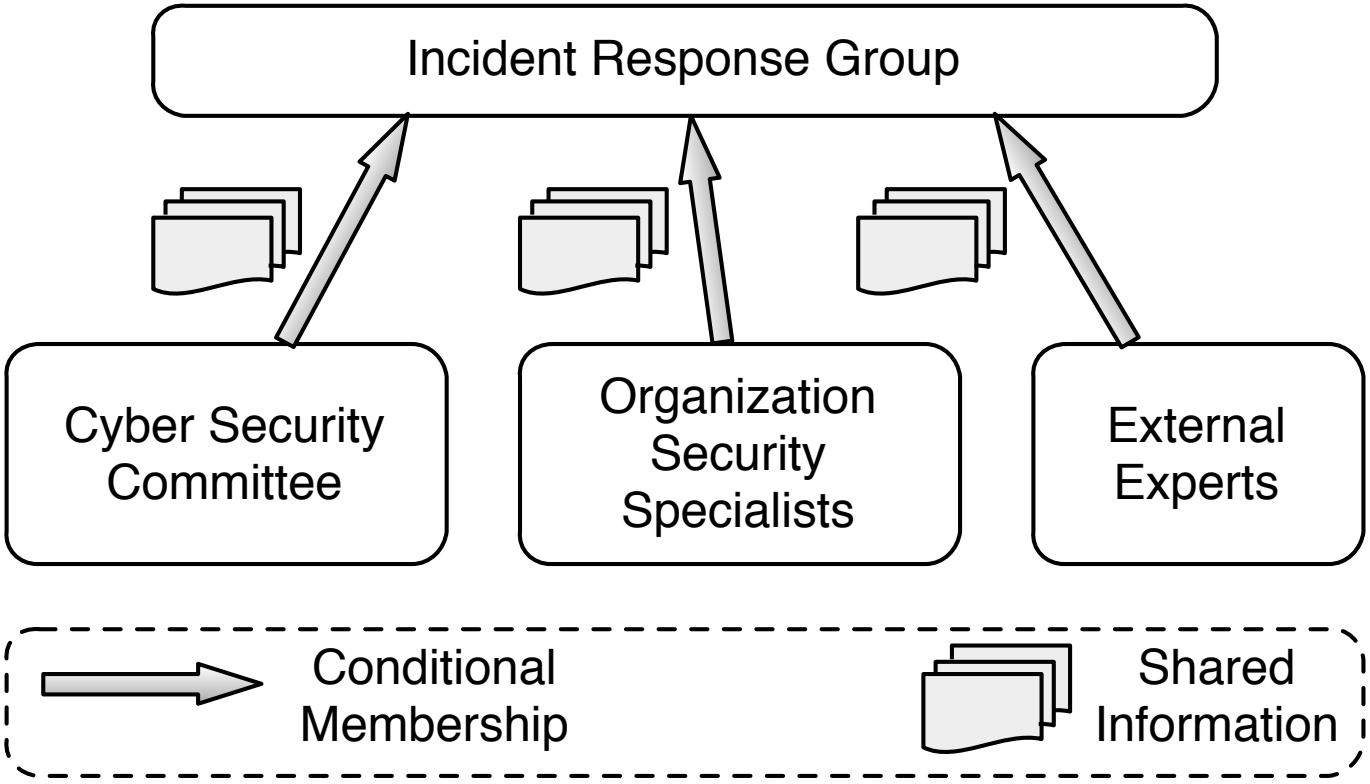
Traditional Cyber Collaboration

- 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.

Cyber Collaboration in Community Cloud

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

Community Cyber Incident Response Governance

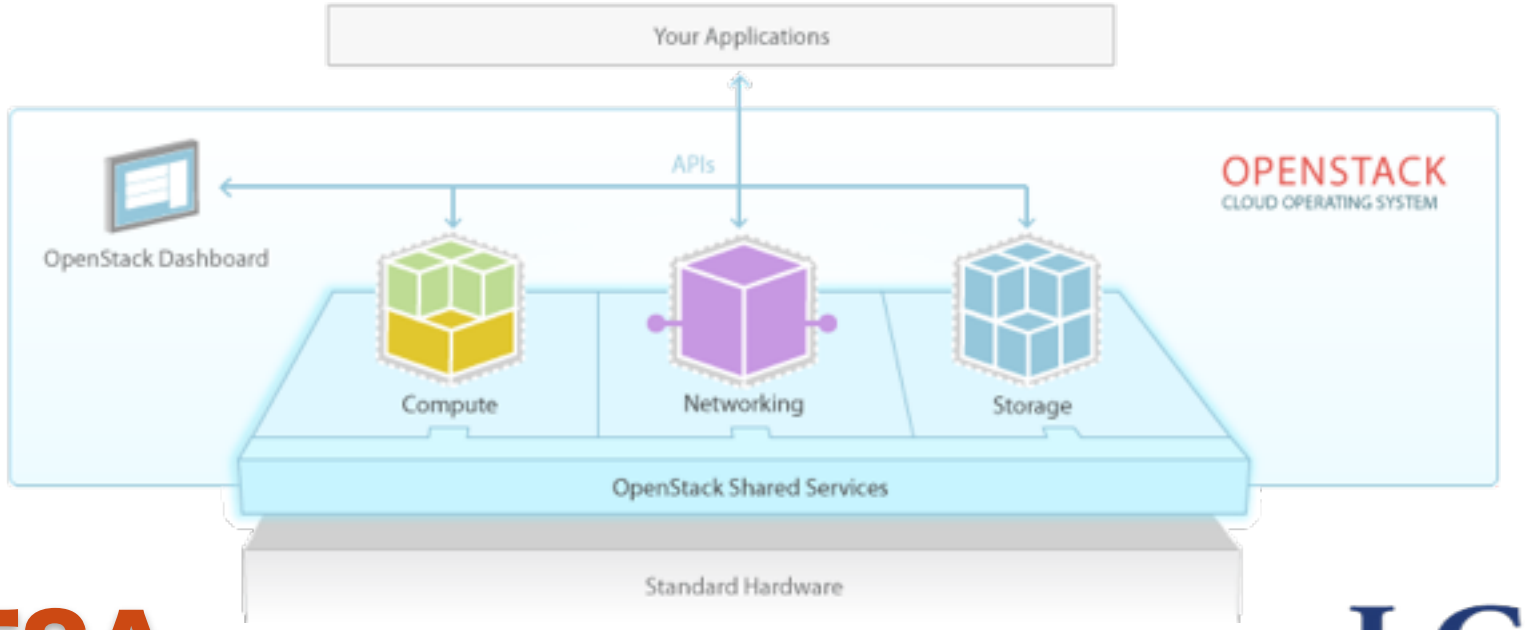


Assumptions and Scope

- In a community cloud platform
- OpenStack
- Sharing amongst a set of organizations
  - Sensitive cyber information, infrastructure, tools, analytics, etc.
  - May share malicious or infected code/systems (e.g. virus, worms, etc.)
- Focus on access control model

OpenStack

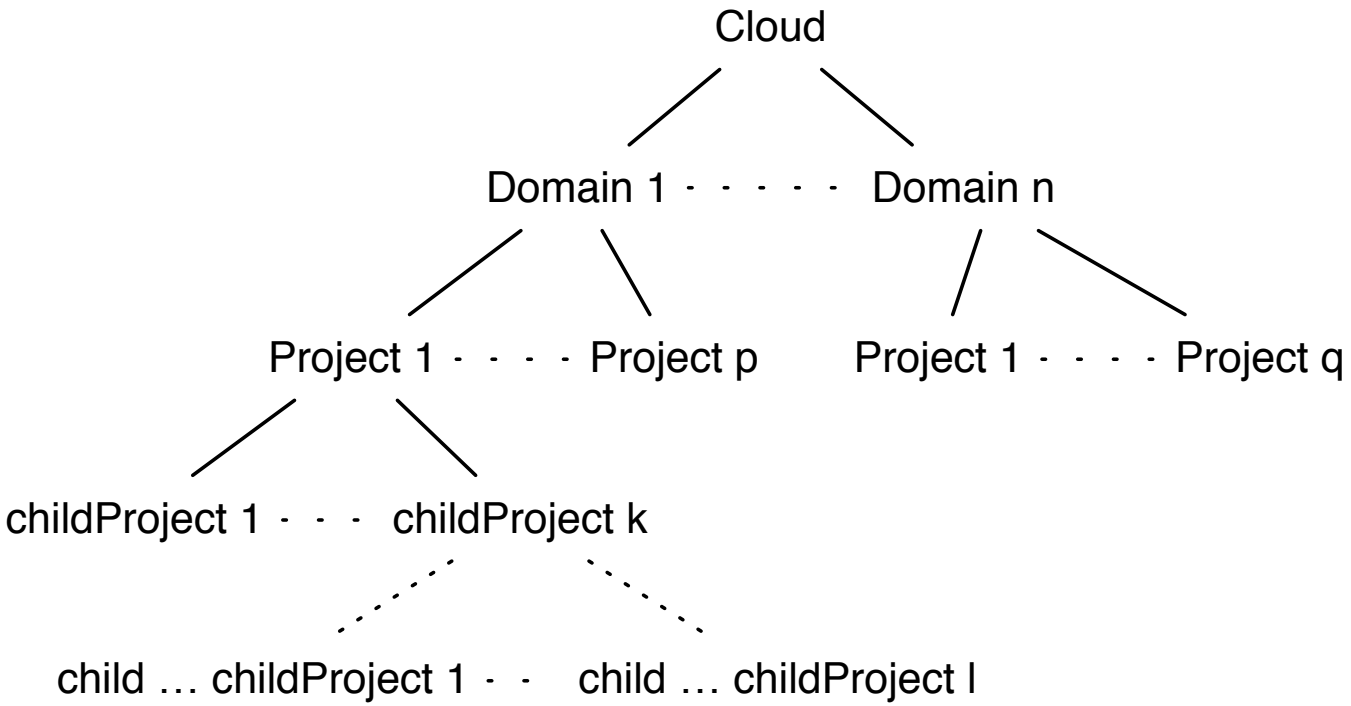
- Dominant open-source cloud IaaS software
  - OpenStack software controls large pools of compute, storage, and networking resources throughout a datacenter, managed through a dashboard or via the OpenStack API.



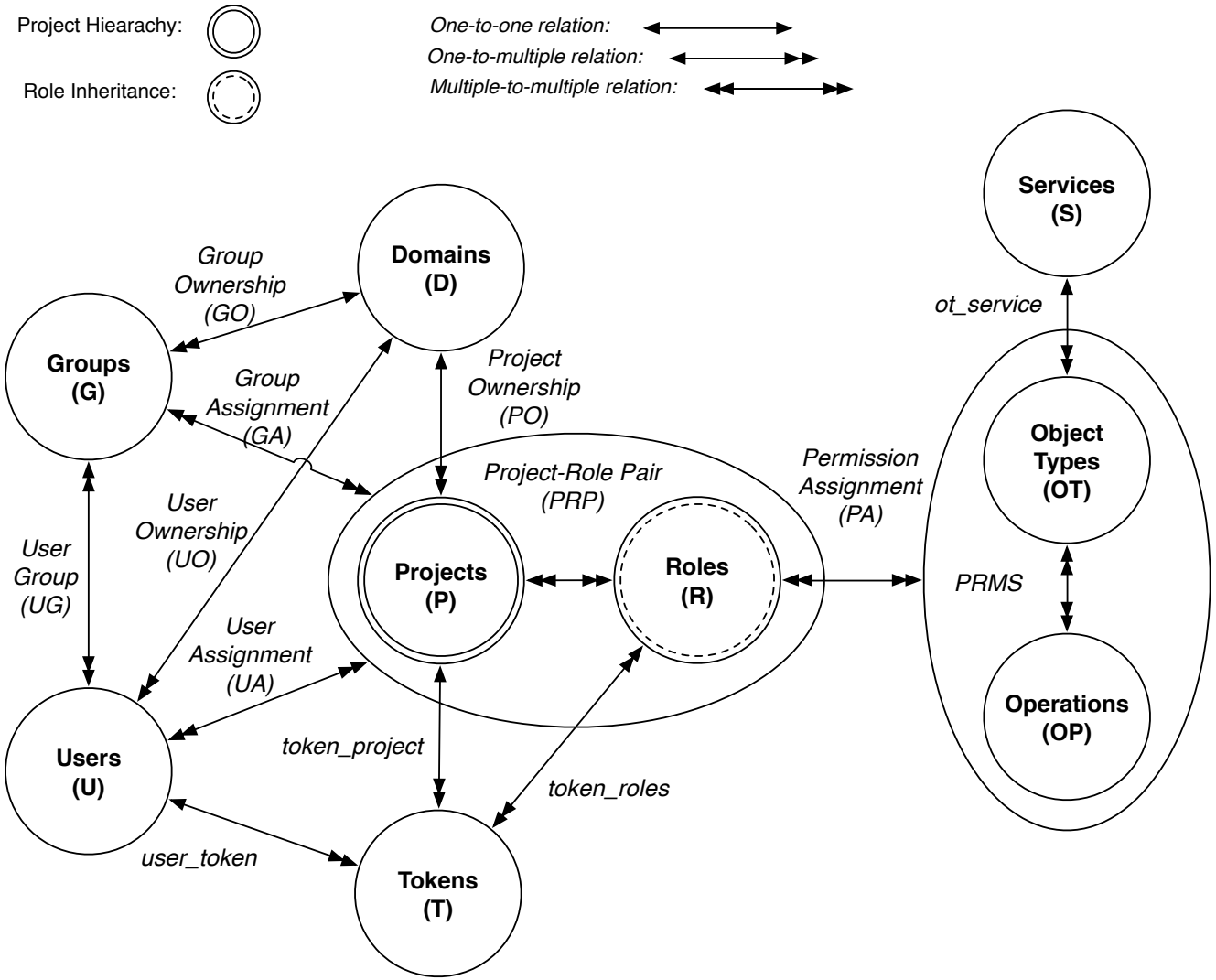
Ref: http://www.openstack.org

OpenStack HMT

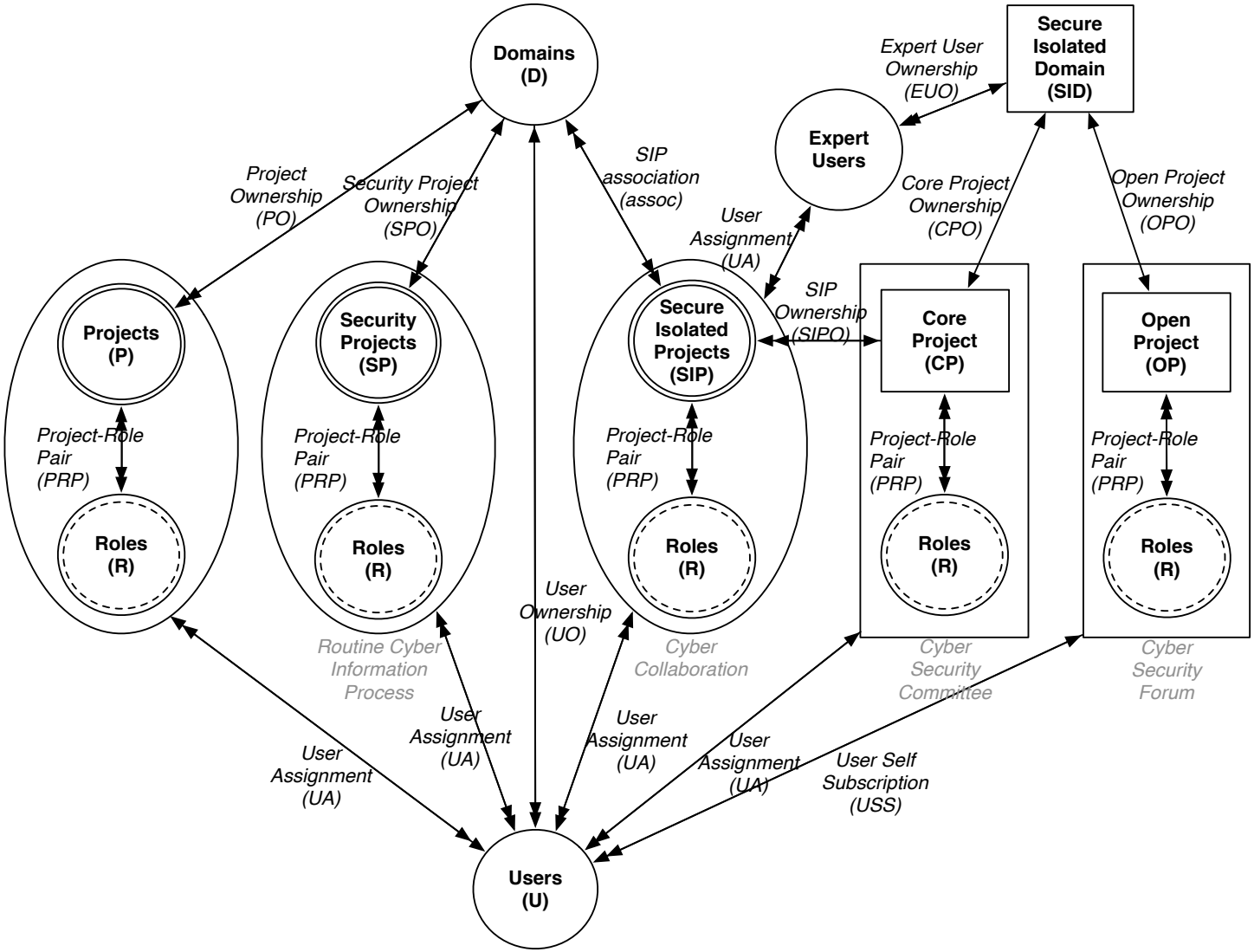
- HMT : Hierarchical Multitenancy



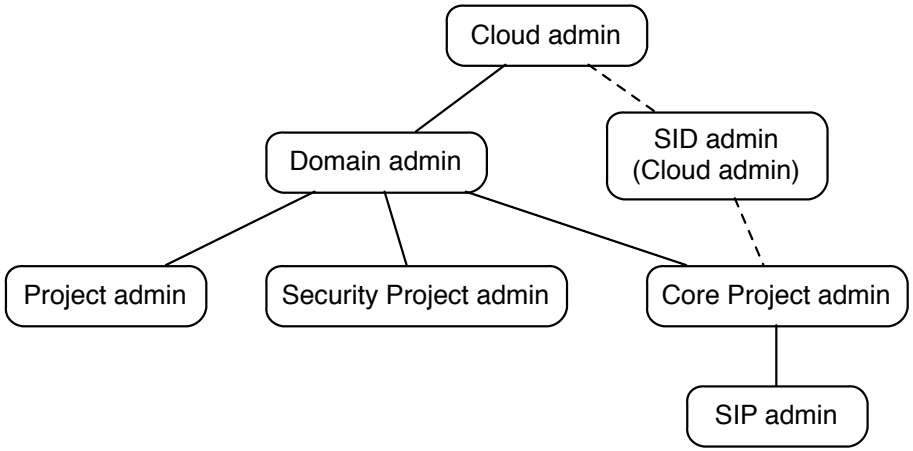
OSAC Model with HMT

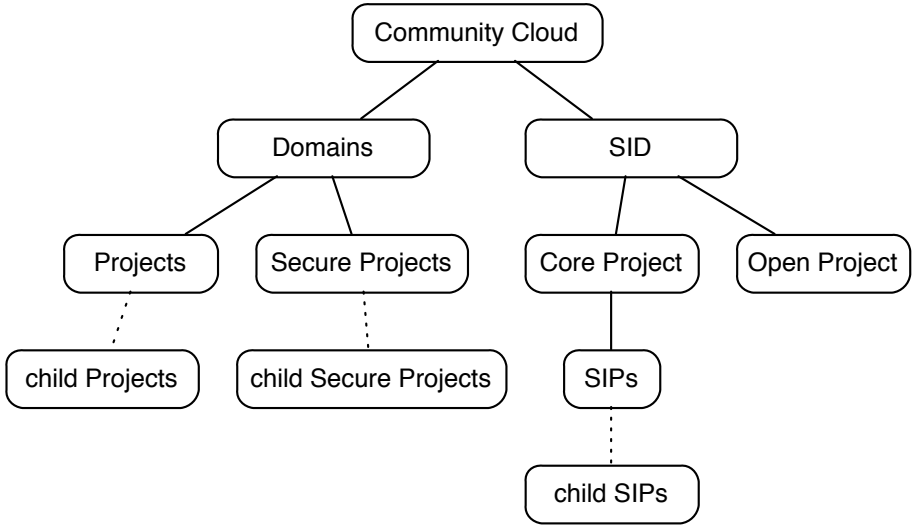


OSAC-HMT-SID Model



OSAC-HMT-SID Administration Relation and Resources Ownership



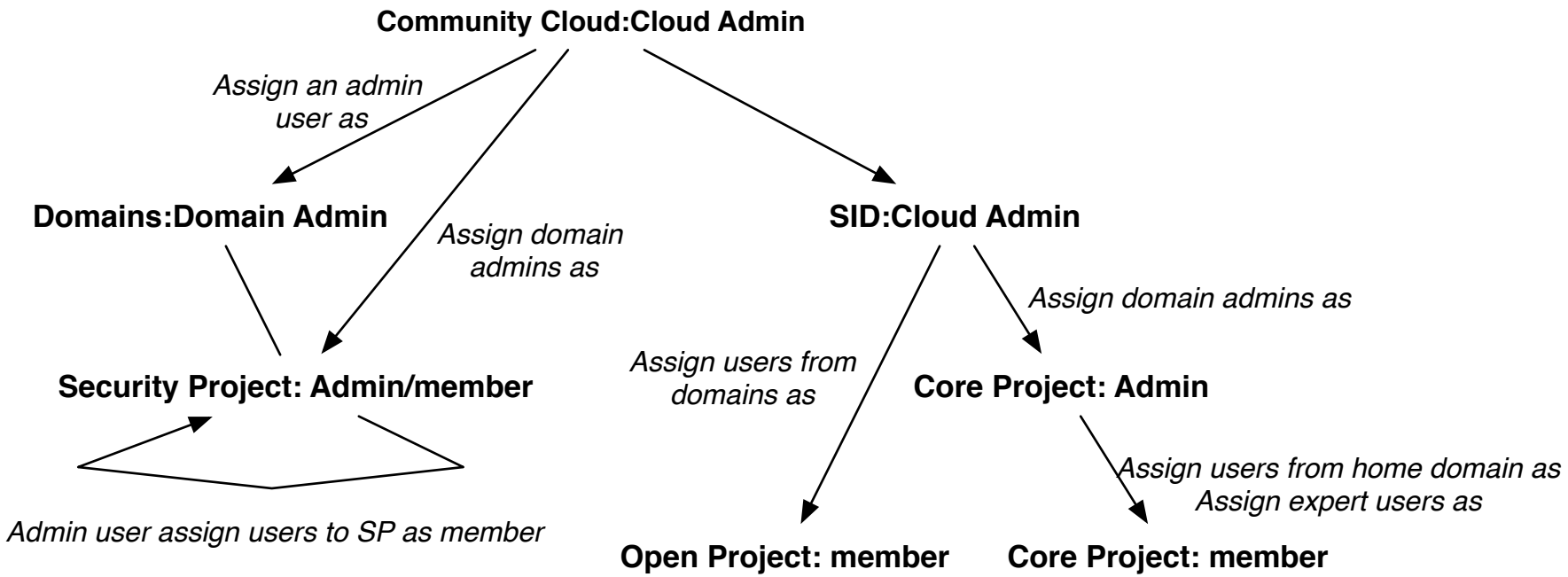


OSAC-SID Administrative Model

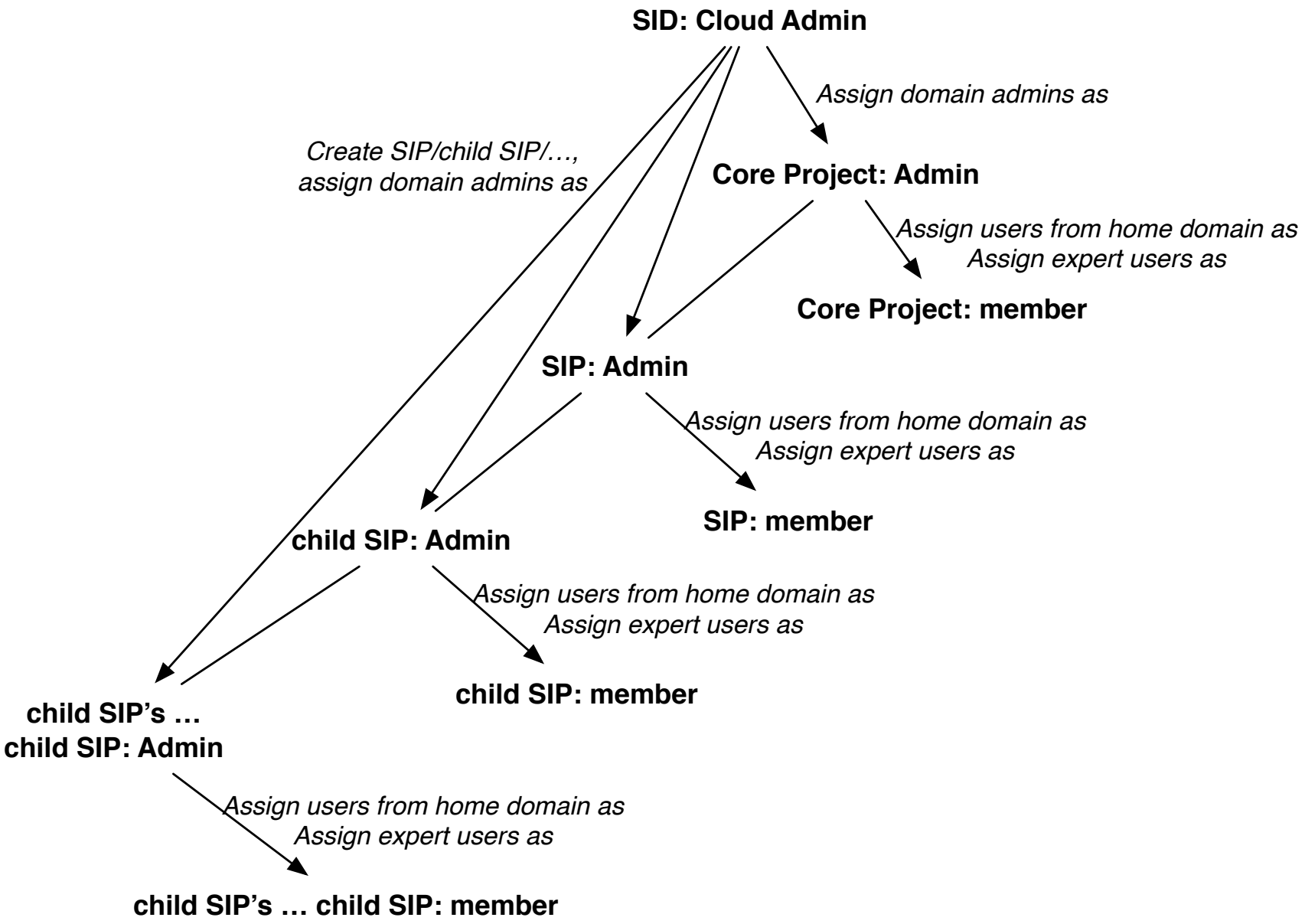
- **SipCreate(uSet, sip)**
  /* A subset of Core Project/domain admin users together create a sip */
- **SipDelete(uSet, sip)**
  /* The same subset of Core Project/domain admin users together delete a sip*/
- **UserAdd(adminuser, r, u, sp, p)**
  /* CP/Sip admin can add a user from his home domain Security 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



Conclusion and future work

- Suggested OSAC-HMT-SID model to OpenStack
  - Cyber collaboration across organizations
    - cyber incident response
    - Self-service
    - Cyber Security Committee.
    - Share data, tools, vms, etc.
  - Potential blueprint for official OpenStack adoption
- Future work
  - Explore other model options.
  - Explore local roles in the model.
  - Explore models in other dominant cloud platforms.

Thanks!