Secure Information and Resource Sharing in Cloud Infrastructure as a Service

Cyber Incident Response

Models for Information and Resource Sharing

Amy(Yun) Zhang, Ram Krishnan, Ravi Sandhu
Institute for Cyber Security
University of Texas at San Antonio
San Antonio, TX 78249
Nov 03, 2014

Presented by: Amy(Yun) Zhang

UTSA

I·C·S
The Institute for Cyber Security

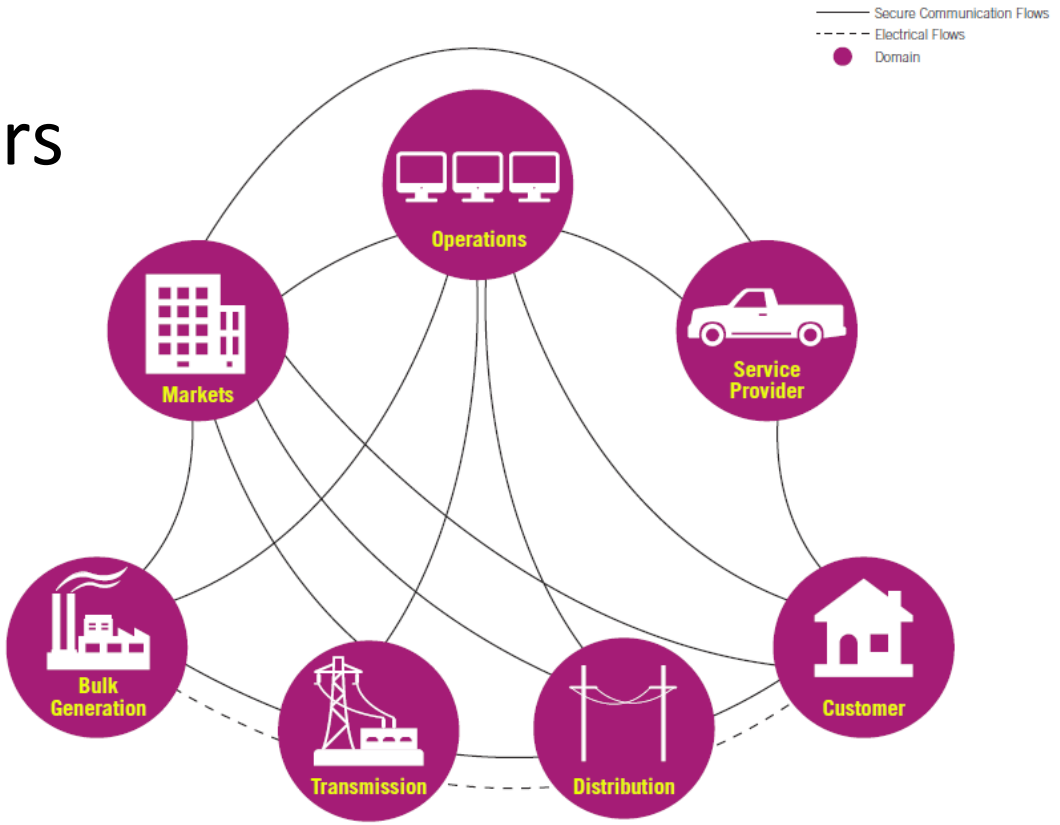
Information Sharing and Coordination Initiatives

- collaboration and coordination to enhance situational awareness
  - Share malicious activities on federal systems
  - Technologies, tools, procedures, analytics

Ref: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

Electric Grid Scenario

- Cyber incidents in electricity providers
  - Local utilities, regional, state, national operators
- Need a standing platform that facilitates sharing
  - Controlled access



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

Cyber Infrastructure for Sharing

- Traditional platforms
  - Shared storage
    - SharePoint, Dropbox, Google Drive, etc.
  - Shared infrastructure
    - Grid computing
- Modern platform
  - Cloud

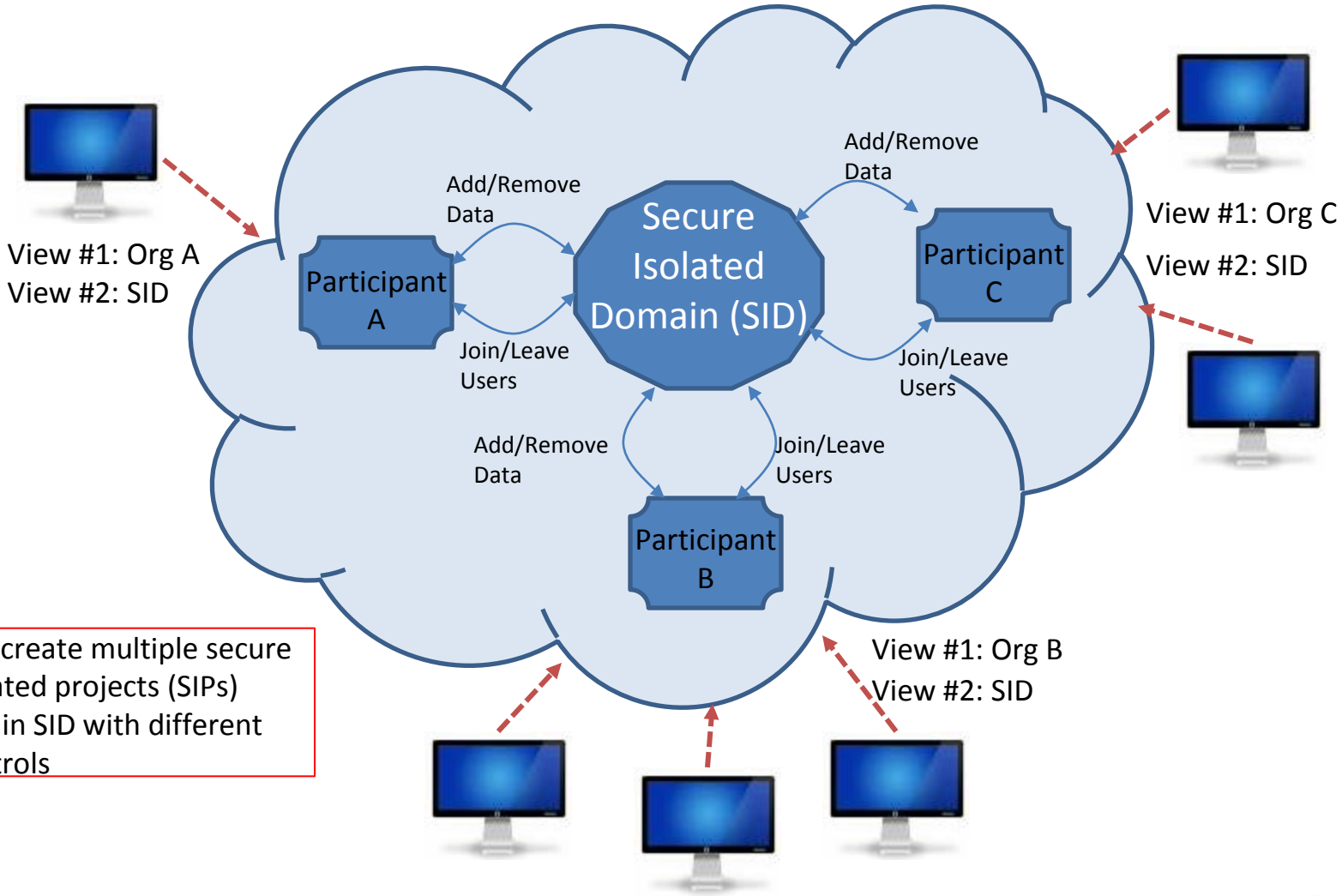
Cloud IaaS Advantages for Cyber Incident Sharing

- 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

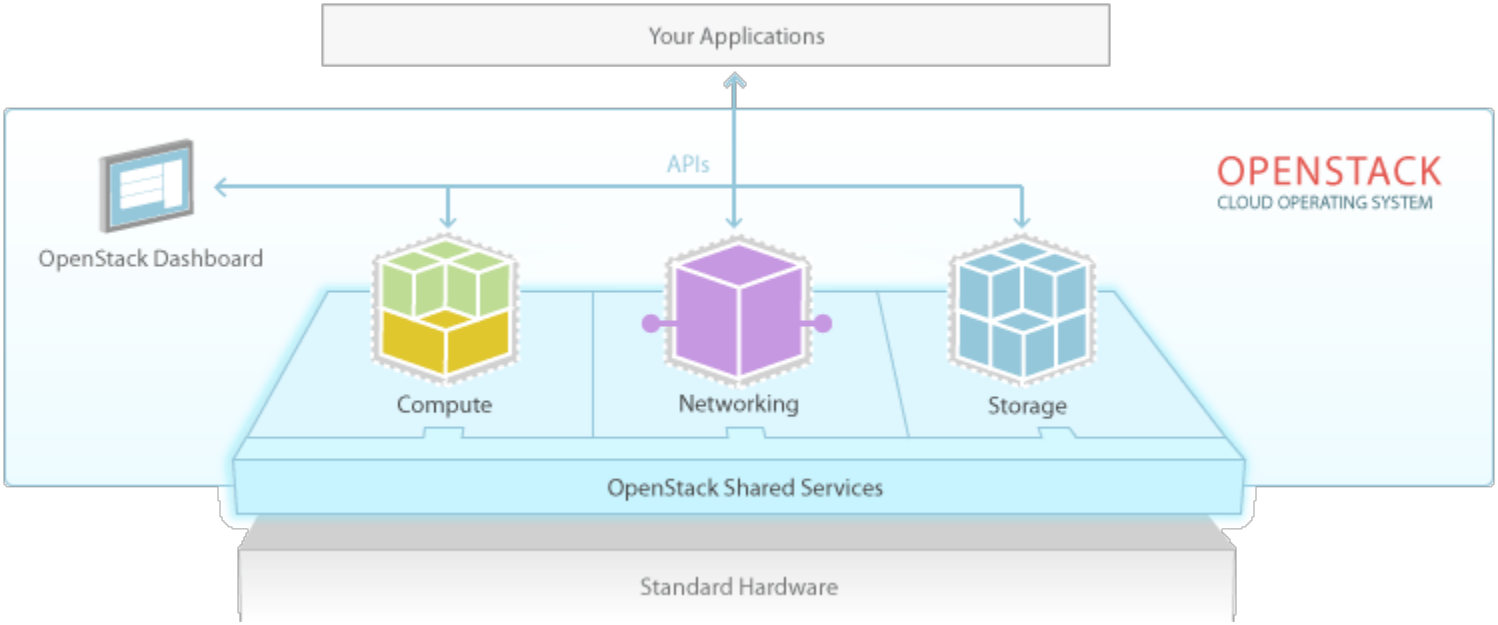


Can create multiple secure isolated projects (SIPs) within SID with different controls

OpenStack

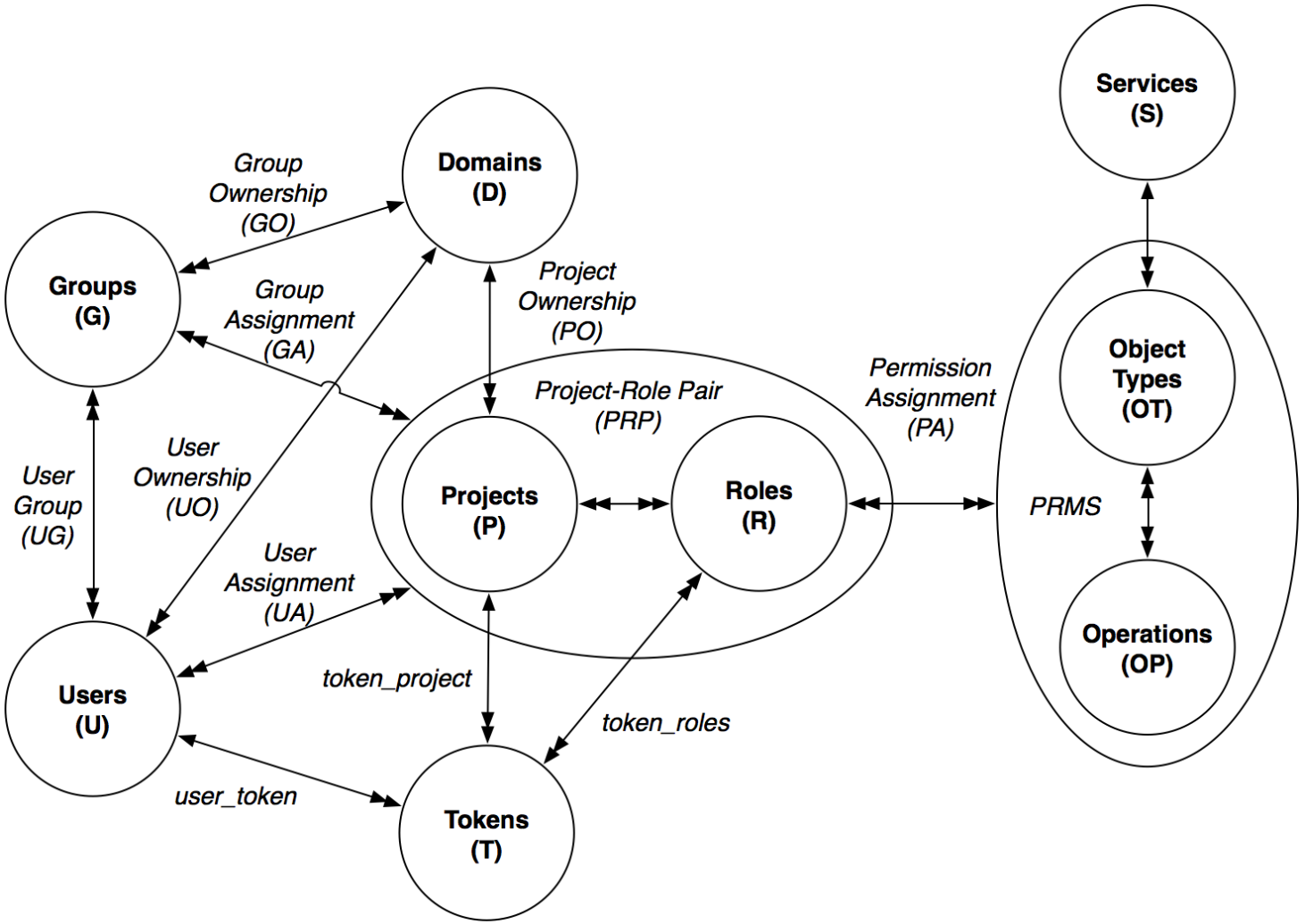
- OpenStack
  - Dominant open-source cloud IaaS software

> 200 companies
~14000 developers
>130 countries

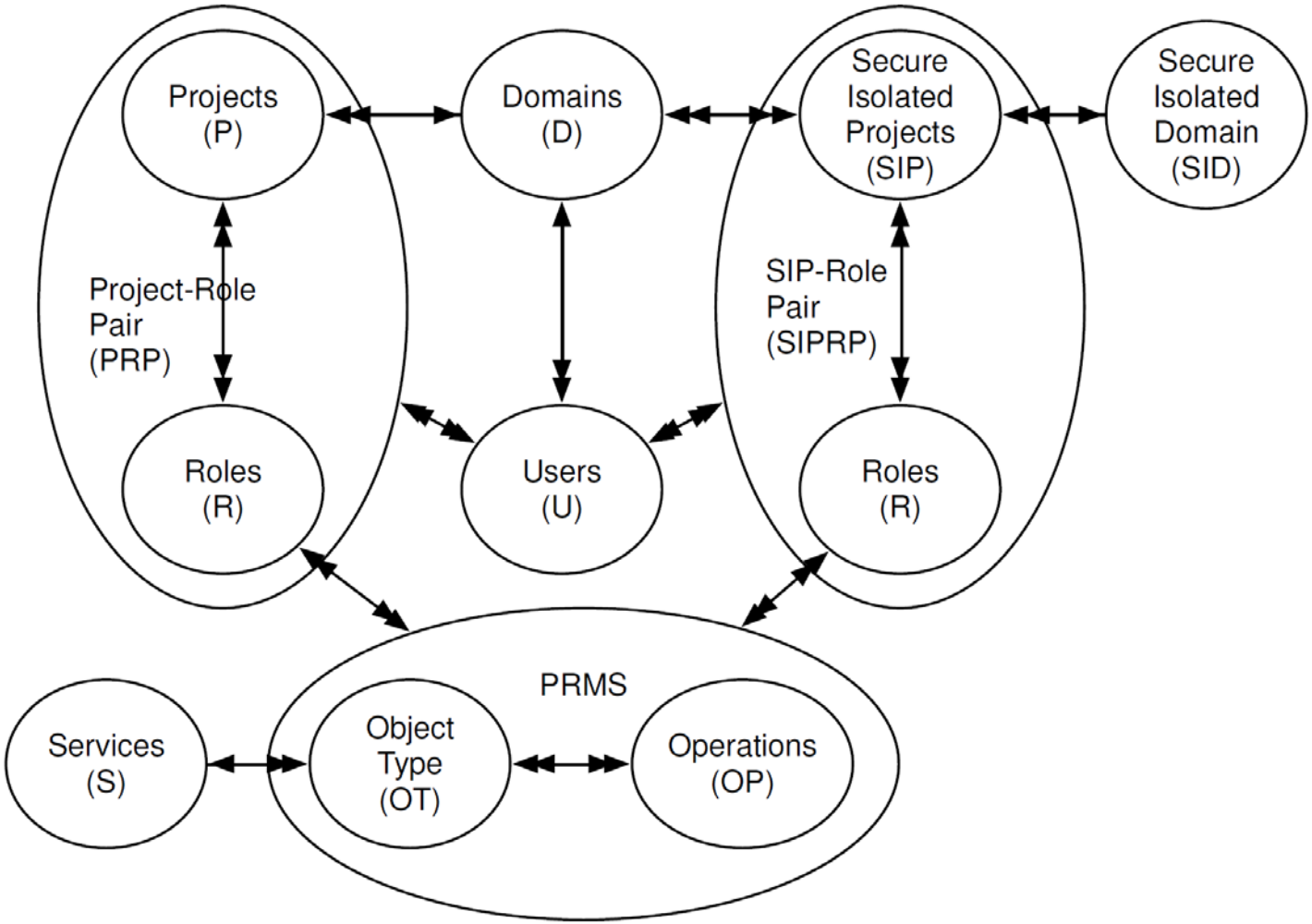


Ref: http://www.openstack.org

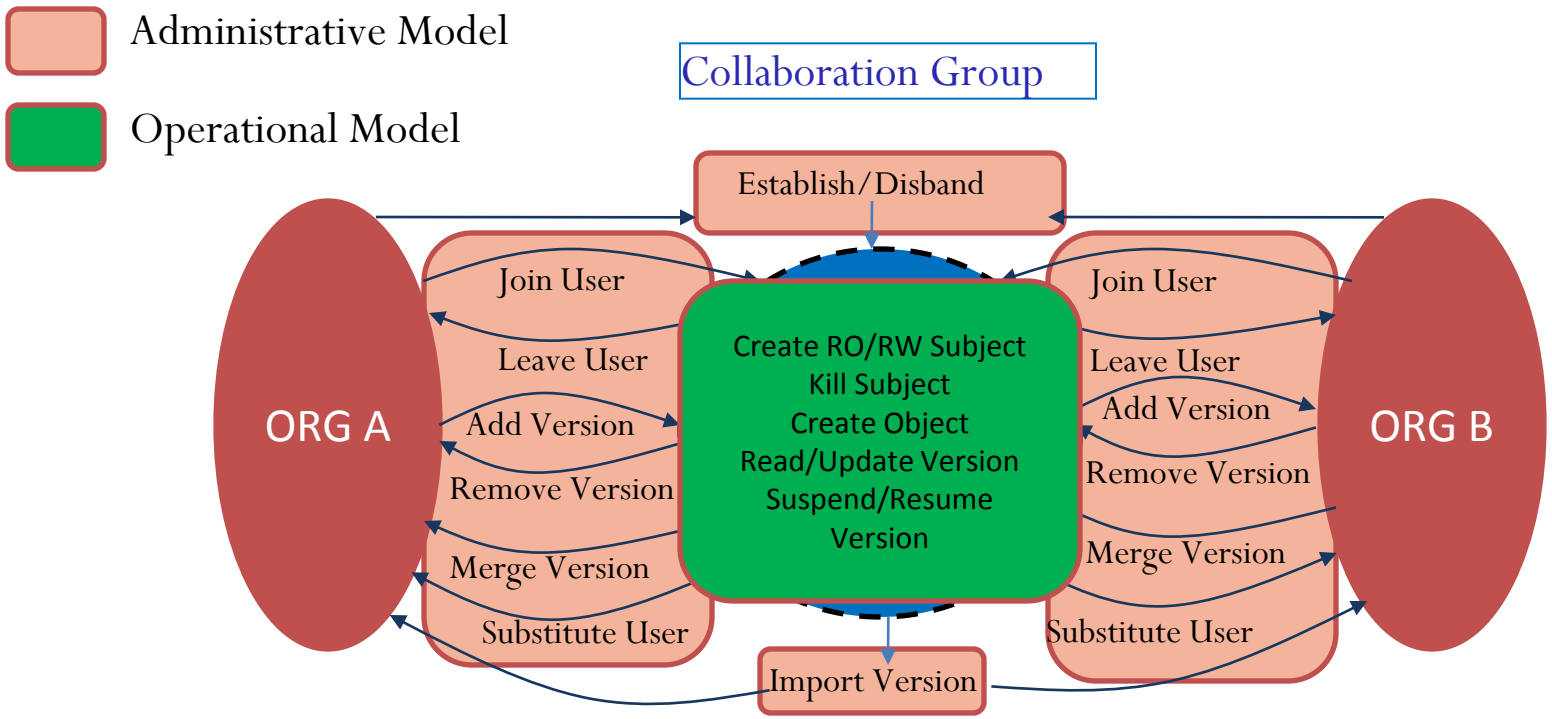
OpenStack Access Control (OSAC)



OSAC-SID


Projects
(P)
Domains
(D)
Secure
Isolated
Projects
(SIP)
Secure
Isolated
Domain
(SID)
Project-Role
Pair
(PRP)
SIP-Role
Pair
(SIPRP)
Roles
(R)
Users
(U)
Roles
(R)
PRMS
Services
(S)
Object
Type
(OT)
Operations
(OP)

Conceptual Model



OSAC-SID Administrative Model

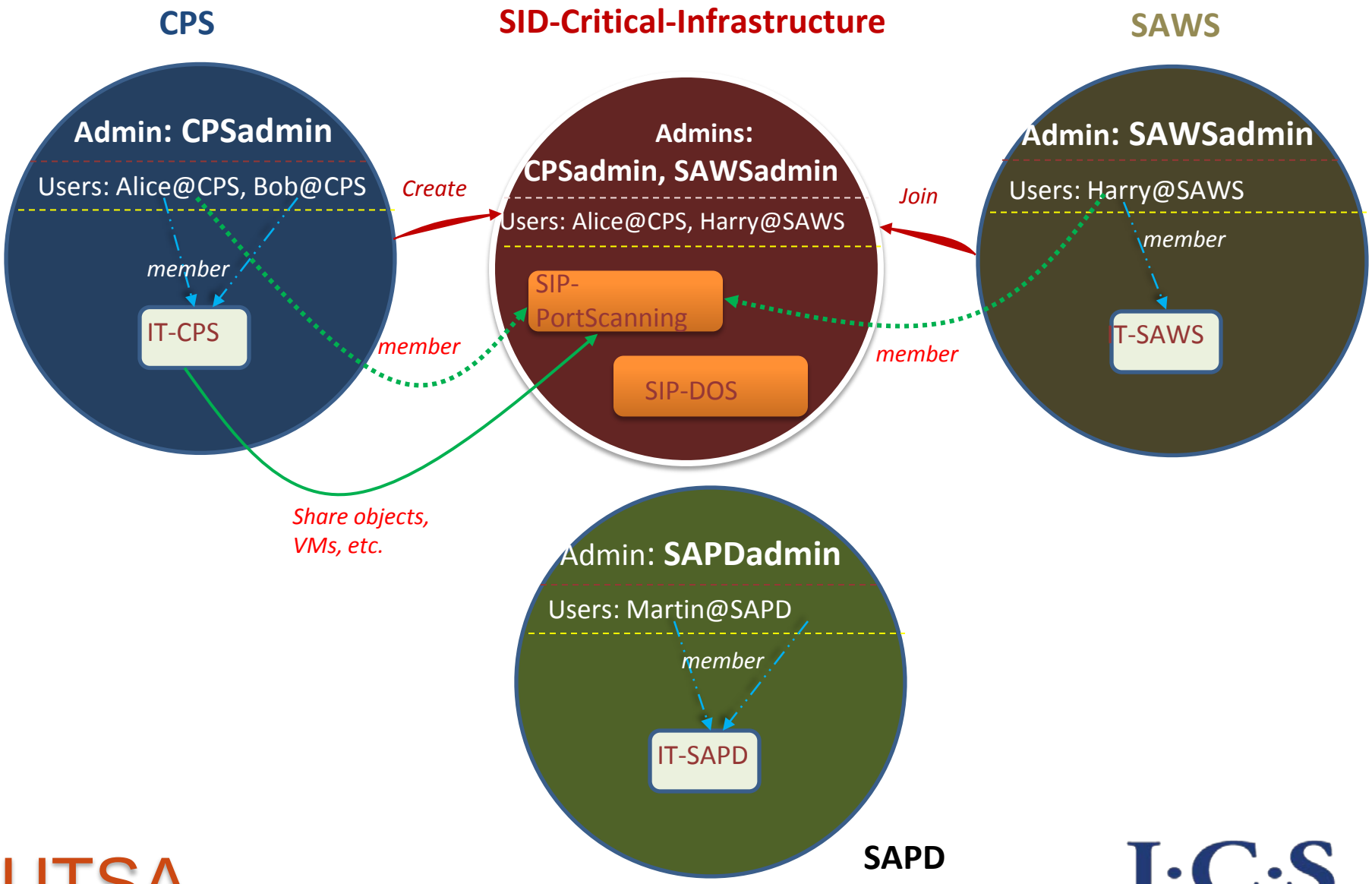
Operation	Authorization Requirement	Update
SipCreate(uSet, sip) */* a set of domain admin users together create a sip */*	$\forall$ u1, u2 $\in$ uSet.((DA(u1)=True $\wedge$ DA(u2)=True $\wedge$ u1 $\neq$ u2 $\wedge$ UO(u1) $\neq$ UO(u2))) sip $\in$ (UNIV_SIP - SIP)	SIPO(sip) = $\bigcup_{\forall u \in uSet}$ UO(u) SIPU(sip) = uSet $\forall$ u $\in$ uSet.SIPA(u) = SIPA(u) $\cup$ {sip} SIP' = SIP $\cup$ {sip}
SipDelete(uSet, sip) */* delete the sip*/*	$\forall$ u $\in$ uSet.((DA(u)=True $\wedge$ sip $\in$ SIPA(u))) $\wedge$ SIPO(sip) = $\bigcup_{\forall u \in uSet}$ UO(u) sip $\in$ SIP	SIPO(sip) = NULL SIPU(sip) = NULL $\forall$ u $\in$ uSet.SIPA(u) = SIPA(u) - {sip} SIP' = SIP - {sip}
SidCreate(uSet, sid) */* a set of domain admin users together create a sid */*	$\forall$ u1, u2 $\in$ uSet.((DA(u1)=True $\wedge$ DA(u2)=True $\wedge$ u1 $\neq$ u2 $\wedge$ UO(u1) $\neq$ UO(u2))) sid $\in$ (UNIV_SID - SID)	SIDO(sid) = $\bigcup_{\forall u \in uSet}$ UO(u) SID' = SID $\cup$ {sid}
SidDelete(uSet, sid) */* delete the sid*/*	$\forall$ u $\in$ uSet.((DA(u)=True $\wedge$ sid $\in$ SIDA(u))) $\wedge$ SIDO(sid) = $\bigcup_{\forall u \in uSet}$ UO(u) sid $\in$ SID	SIDO(sid) = NULL SID' = SID - {sid}
UserAdd(admin, r, u, sip) */* sip admin add a normal user to a sip*/*	sip $\in$ SIPA(admin) $\wedge$ DA(admin)=True $\wedge$ UO(admin) $\in$ SIDO(sid) $\wedge$ sip $\in$ sid $\wedge$ UO(u) = UO(admin) $\wedge$ r $\in$ R $\wedge$ sip $\in$ SIP $\wedge$ u $\in$ U	(u, (sip, r)) $\in$ SIPUA $\wedge$ SIPU'(sip) = SIPU(u) $\cup$ {u}
UserRemove(admin, r, u, sip) */* sip admin remove a normal user from a sip*/*	sip $\in$ SIPA(admin) $\wedge$ DA(admin)=True $\wedge$ UO(admin) $\in$ SIDO(sid) $\wedge$ sip $\in$ sid $\wedge$ UO(u) = UO(admin) $\wedge$ r $\in$ R $\wedge$ sip $\in$ SIP $\wedge$ u $\in$ U $\wedge$ (u, (sip, r)) $\in$ SIPUA	(u, (sip, r)) = NULL $\wedge$ SIPU'(sip) = SIPU(u) - {u}
CopyObject(u, so1, c1, p, d, so2, c2, sip, sid)	so1 $\in$ SO $\wedge$ c1 $\in$ C $\wedge$ p $\in$ P $\cup$ SIP $\wedge$ d $\in$ D $\cup$ SID $\wedge$ so2 $\in$ (UNIV_SO - SO) $\wedge$ c2 $\in$ C $\wedge$ sip $\in$ P $\cup$ SIP $\wedge$ sid $\in$ D $\cup$ SID $\wedge$ (so1, c1) $\in$ SOO $\wedge$ (c1, p) $\in$ CO $\wedge$ (p, d) $\in$ PO $\cup$ SIPO $\wedge$ (c2, sip) $\in$ CO $\wedge$ (sip, sid) $\in$ PO $\cup$ SIPO $\wedge$ u $\in$ U $\wedge$ (u, (p, r)) $\in$ UA $\wedge$ (u, (sip, r)) $\in$ SIPUA)	SO' = SO $\cup$ {so2} SOO' = SOO $\cup$ {(so2, c2)}

† uSet: a set of domain admin users.

OSAC-SID Operational Model

Operation	Authorization Requirement	Update
Nova:		
CreateVM(vm, sip, u)	vm ∈ (UNIV_VM - VM) ∧ sip ∈ SIP ∧ u ∈ U ∧ ∃ (perms, r) ∈ PA.(perms = (vm, create) ∧ (u, (sip, r)) ∈ SIPUA)	VM' = VM ∪ {vm} VMO' = VMO ∪ {(vm, p)}
DeleteVM(vm, sip, u)	vm ∈ VM ∧ sip ∈ SIP ∧ u ∈ U ∧ ∃ (perms, r) ∈ PA.(perms = (vm, delete) ∧ (u, (sip, r)) ∈ SIPUA)	VM' = VM - {vm} VMO' = VMO - {(vm, p)} vm = NULL
Swift:		
CreateContainer(c, sip, u)	c ∈ (UNIV_C - C) ∧ sip ∈ SIP ∧ u ∈ U ∧ (u, (sip, r)) ∈ SIPUA)	C' = C ∪ {c} CO' = CO ∪ {(c, p)}
DeleteContainer(c, sip, u)	c ∈ C ∧ sip ∈ SIP ∧ u ∈ U ∧ (u, (sip, r)) ∈ SIPUA)	C' = C - {c} CO' = CO - {(c, p)} c = NULL
UploadObject(so, c, sip, u)	so ∈ UNIV_SO ∧ c ∈ C ∧ sip ∈ SIP ∧ u ∈ U ∧ (u, (sip, r)) ∈ SIPUA) if ∃ so' ∈ SO. (so = so'), then so' = so	SO' = SO ∪ {so} SOO' = SOO ∪ {(so, c)}
DownloadObject(so, c, u, p)	so ∈ SO ∧ c ∈ C ∧ sip ∈ SIP ∧ u ∈ U ∧ (u, (sip, r)) ∈ SIPUA)	
DeleteObject(so, c, sip, u)	so ∈ SO ∧ c ∈ C ∧ sip ∈ SIP ∧ u ∈ U ∧ (u, (sip, r)) ∈ SIPUA)	SO' = SO - {so} SOO' = SOO - {(so, c)} so = NULL

SID and SIP in OpenStack



Conclusion and future work

- Developed sharing models
  - Formal specification
- Enhanced OpenStack 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
  - Potential blueprint for official OpenStack adoption
- Future work
  - more fine grained access control within a SIP
  - harden the implementation to prevent overt information flow

Thanks

- Q&A