Secure Information Sharing for Cyber Response Teams

Cyber Incident Response

Models and Platforms for Information and Resource Sharing

UTSA Team

Ram Krishnan, Assistant Professor (ECE)

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

Amy Zhang, PhD Candidate, UTSA

October 06, 2014

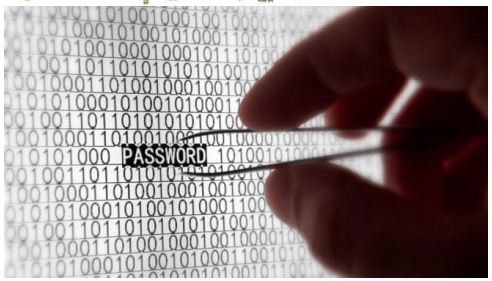
UTSA Engineering

I·C·S The Institute for Cyber Security

THANKS!

Cyber Incidents

- Recent incidents
  - JPMorgan Chase and 9 other financial institutions
    - >76M households compromised
  - Target, Home Depot, Michaels, Nieman Marcus



Cyber Incident Response

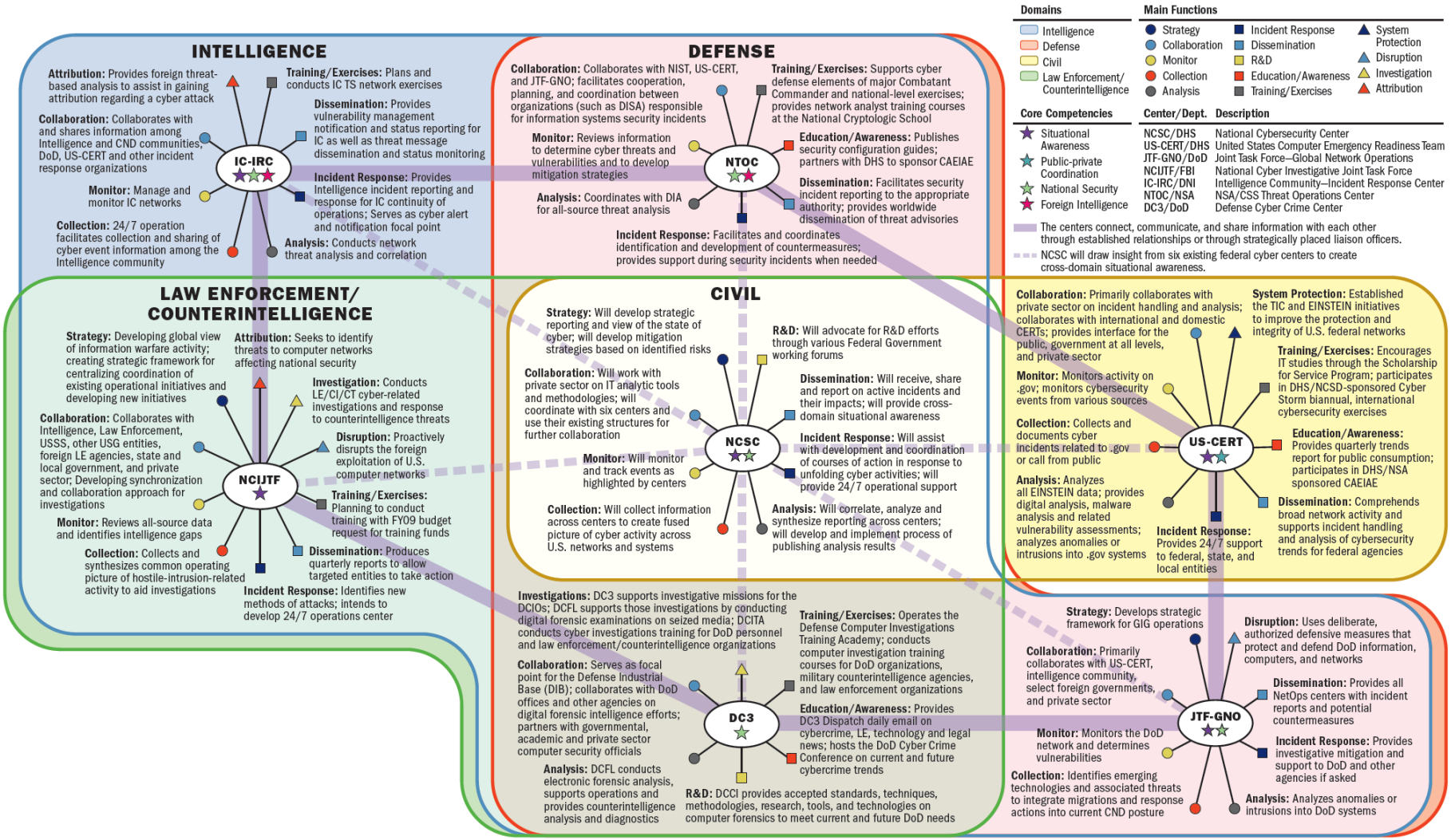
- Information sharing
- Two major challenges
  - Policy
  - Technology

National Information Sharing and Coordination Initiatives

- Inter-agency 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

National Cybersecurity Center



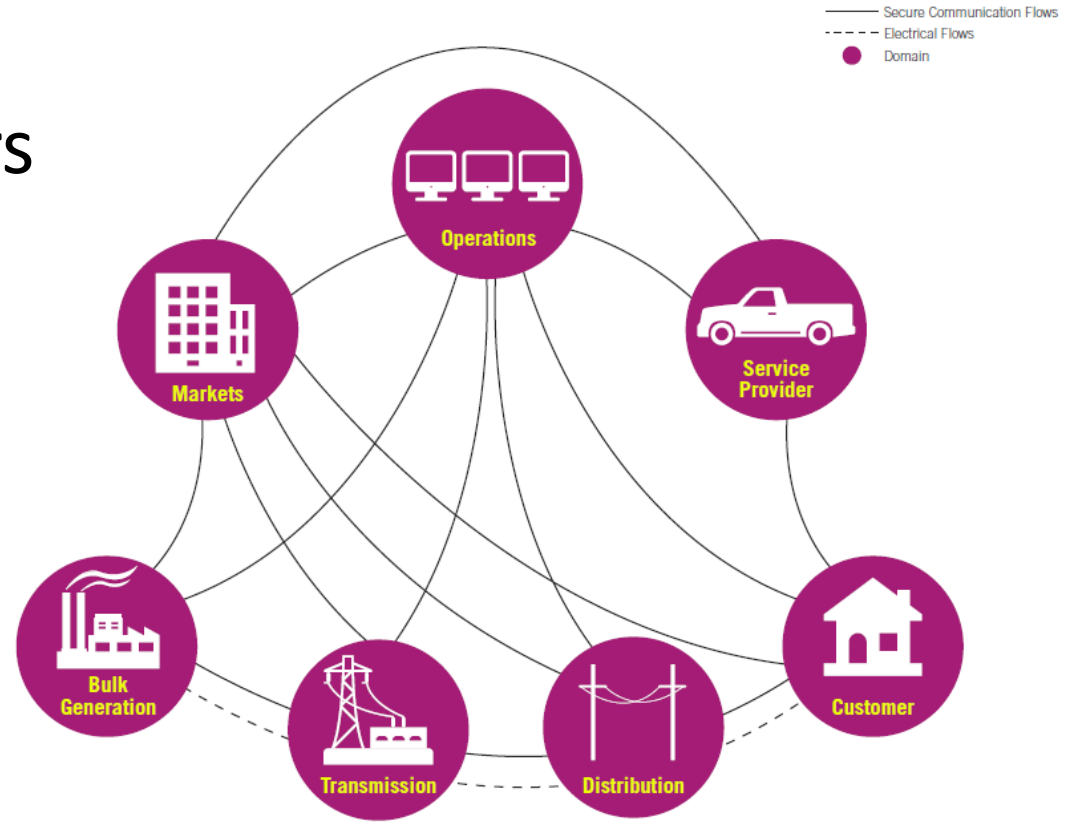
Ref: http://www.whitehouse.gov/files/documents/cyber/CybersecurityCentersGraphic.pdf

Project 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

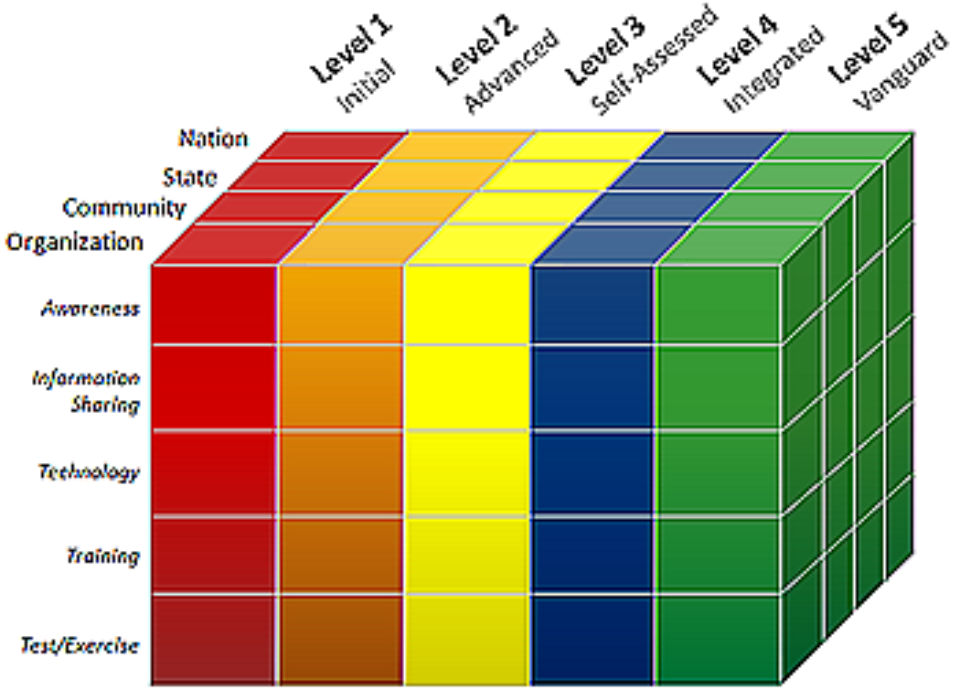
Electric Grid Scenario

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



Community Scenario

- Cyber incidents across critical infrastructure providers in a community
  - Emergency response, healthcare, banks, utility
- Need a community information sharing platform
  - Controlled access



Community Cyber Security Maturity Model
"Yardstick" to determine current cyber security posture

UTSA Engineering

I·C·S The Institute for Cyber Security

Data Exfiltration Scenario

- Unusual file transfers from IP addresses within an org to an external IP address
- Similar activities observed in partner orgs
- Need to find if these events are connected
  - Any correlation between those files?
- Share resources for analysis+collaboration

Key Requirements for Information Sharing

- Cyber infrastructure
- Light-weight and agile
- Rapid deployment and configuration
- Secure isolated environment

Cyber Infrastructure for Sharing

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

Cloud Service Models

Software as a Service (SaaS)

Network accessible software

Platform as a Service (PaaS)

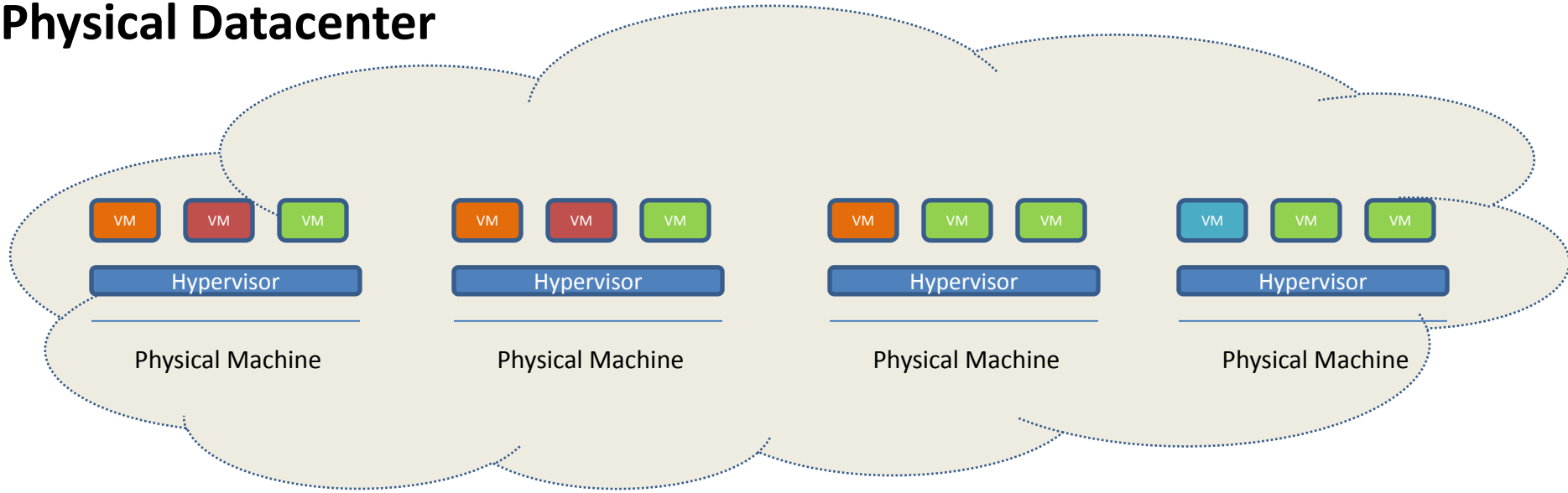
App dev environment with cloud characteristics

Infrastructure as a Service (IaaS)

Virtualized hardware infrastructure

IaaS Cloud

Physical Datacenter



Tenant 1: Need 3 VMs

Tenant 2: Need 3 VMs

Tenant 3: Need 2 VMs

Tenant 2: Need 3 VMs

Tenant 4: Need 1 VM

Each tenant sees a virtual private datacenter

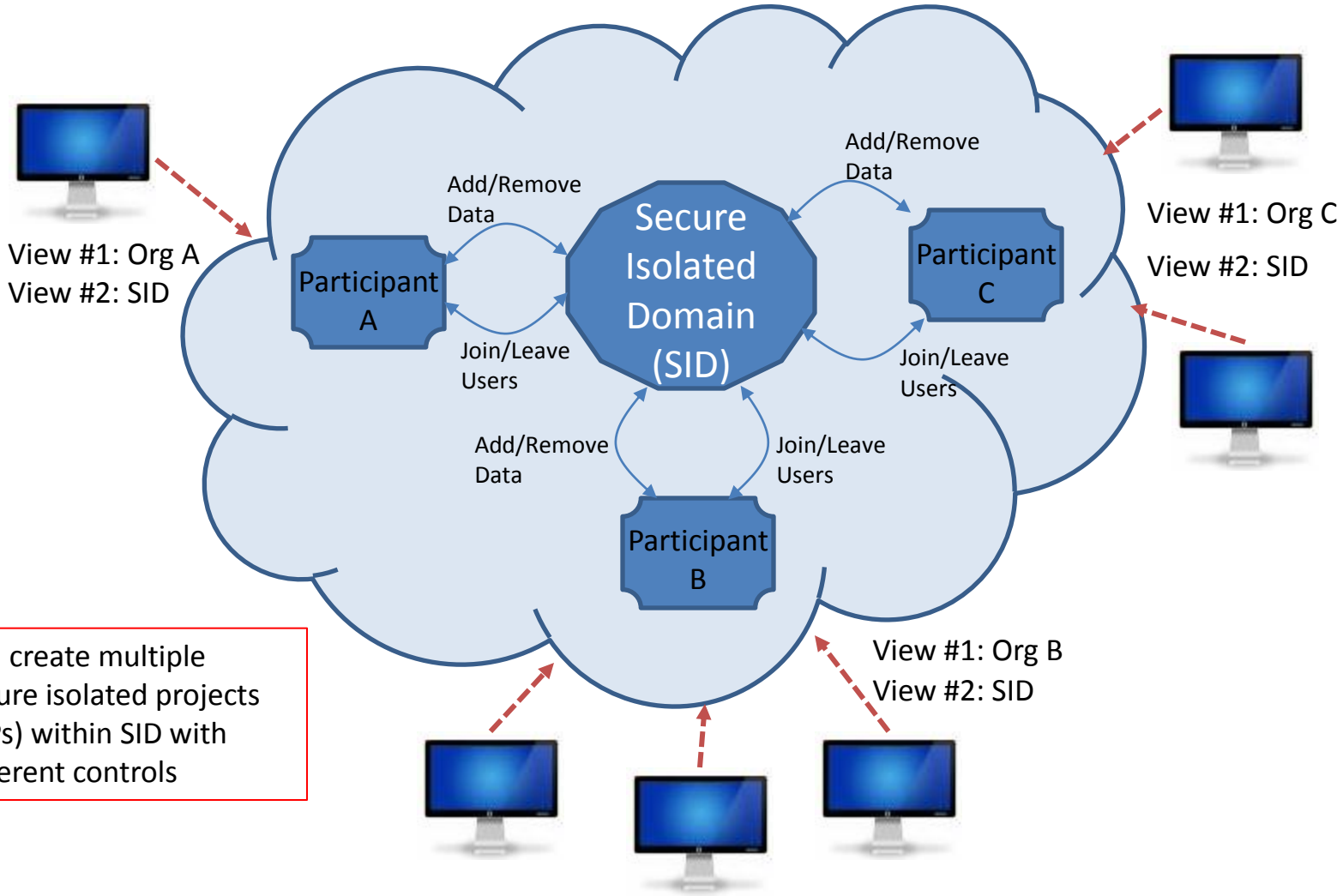
Cloud IaaS Advantages for Cyber Incident Sharing

- 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

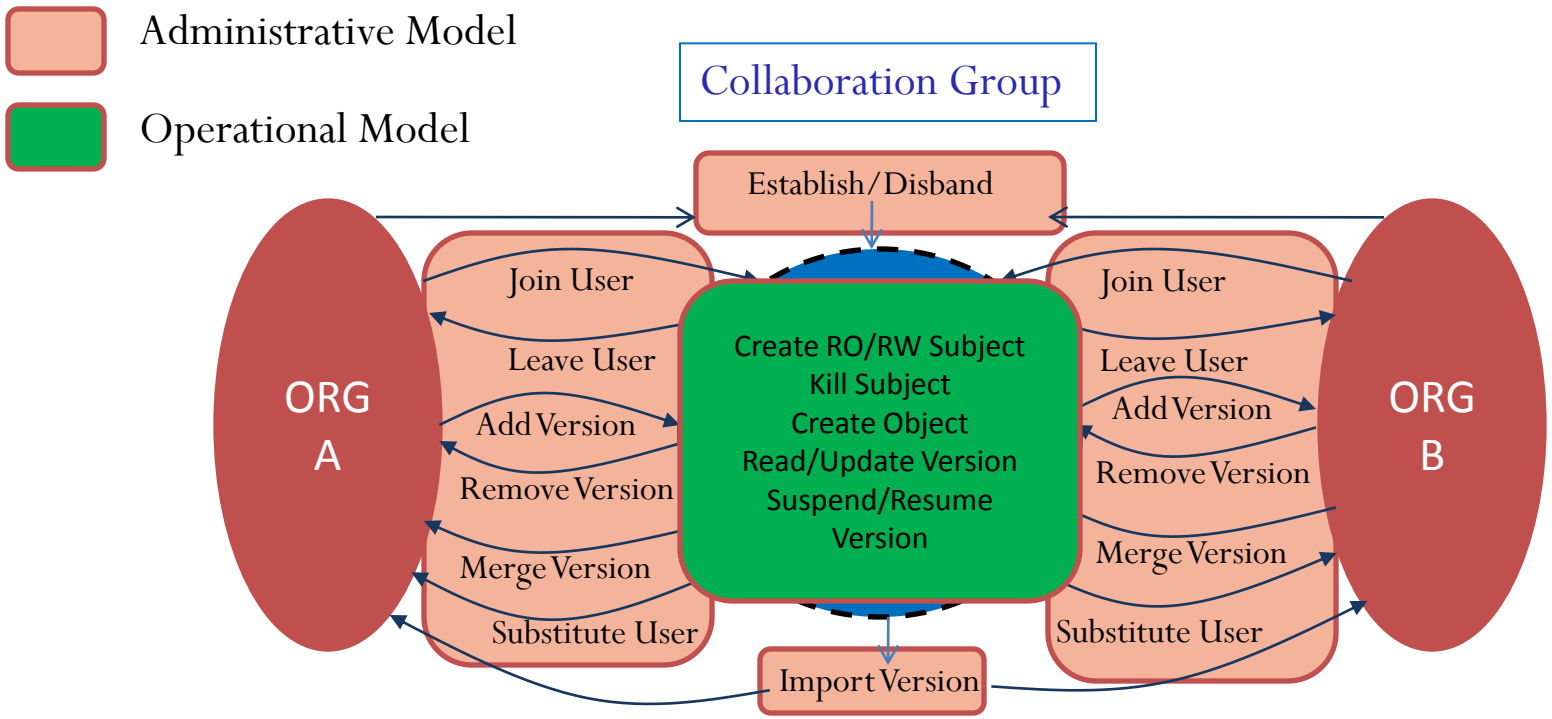
- Tenants are strongly isolated
- IaaS clouds lack secure sharing models
  - Storage
  - Compute
  - Networks
- Need ability to snapshot tenant infrastructure, share, and control who can access
  - Share by copy

Sharing Model in Cloud IaaS

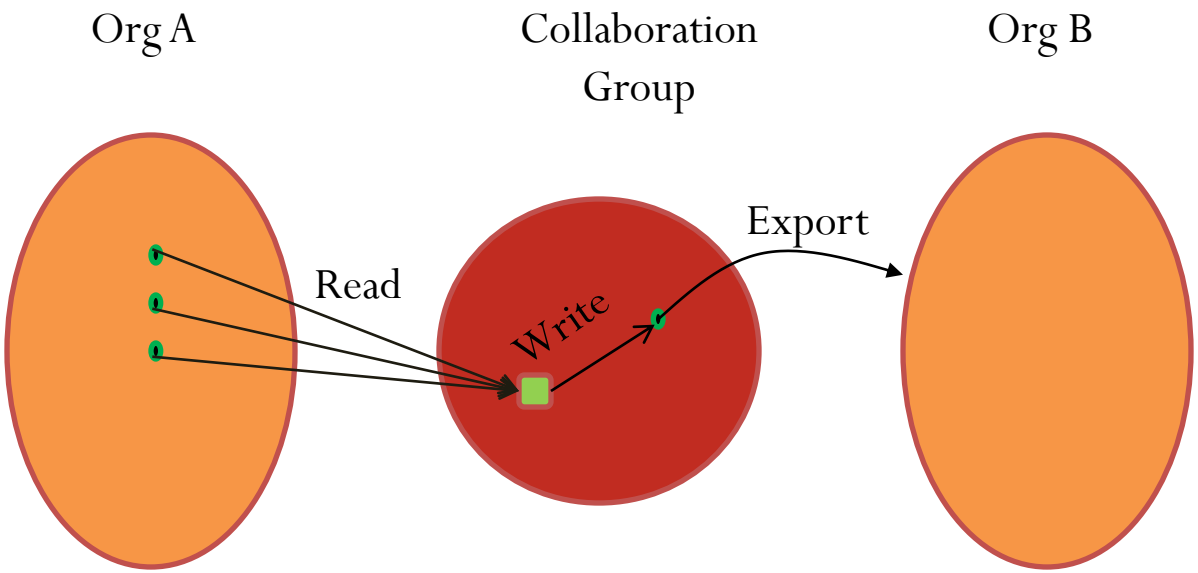


Can create multiple secure isolated projects (SIPs) within SID with different controls

Conceptual Model



Read-only Vs Read-Write Subjects

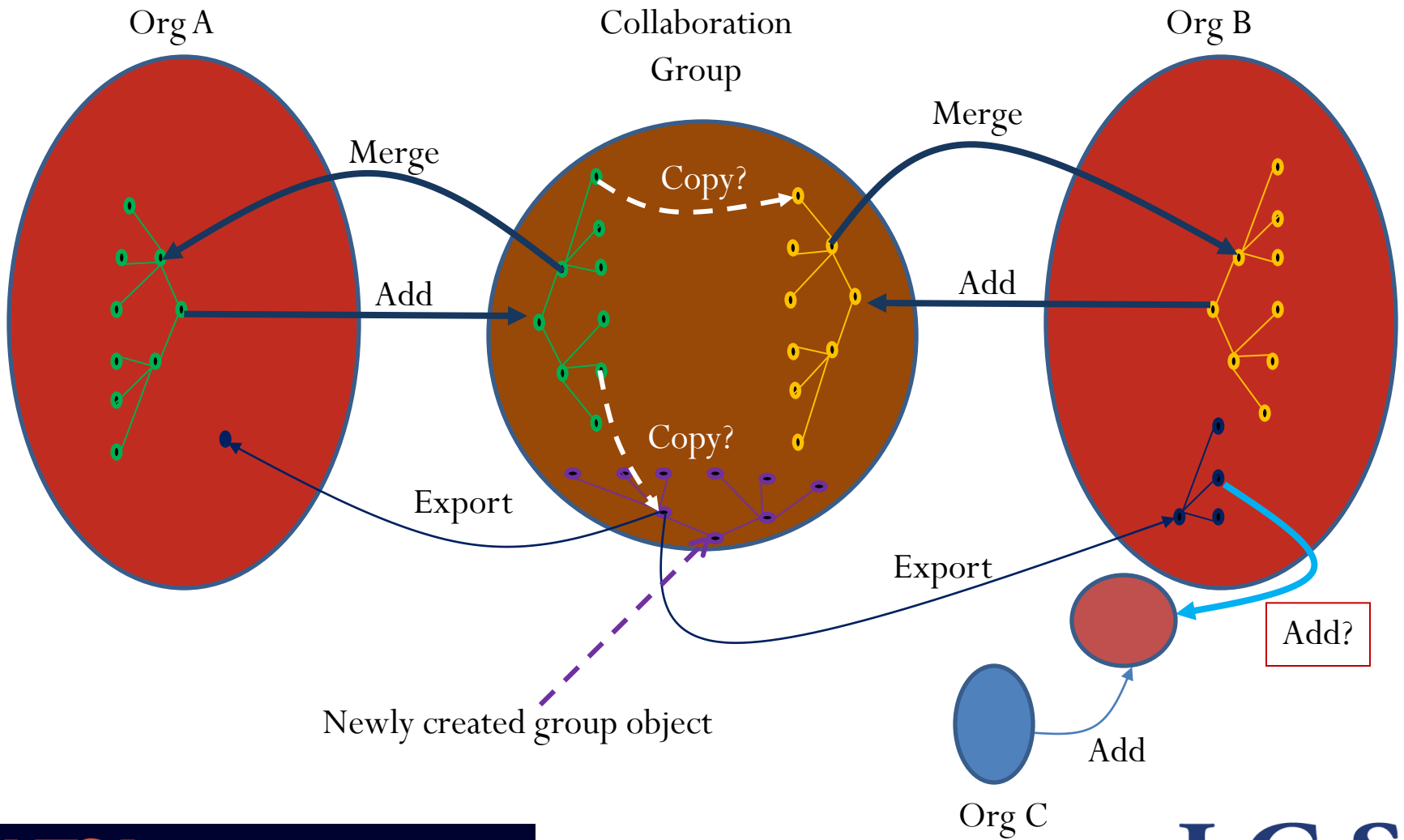


- Read Only subjects can read from multiple groups/entities
- Read-Write subjects restricted to one group

Malicious Group Subject

Object

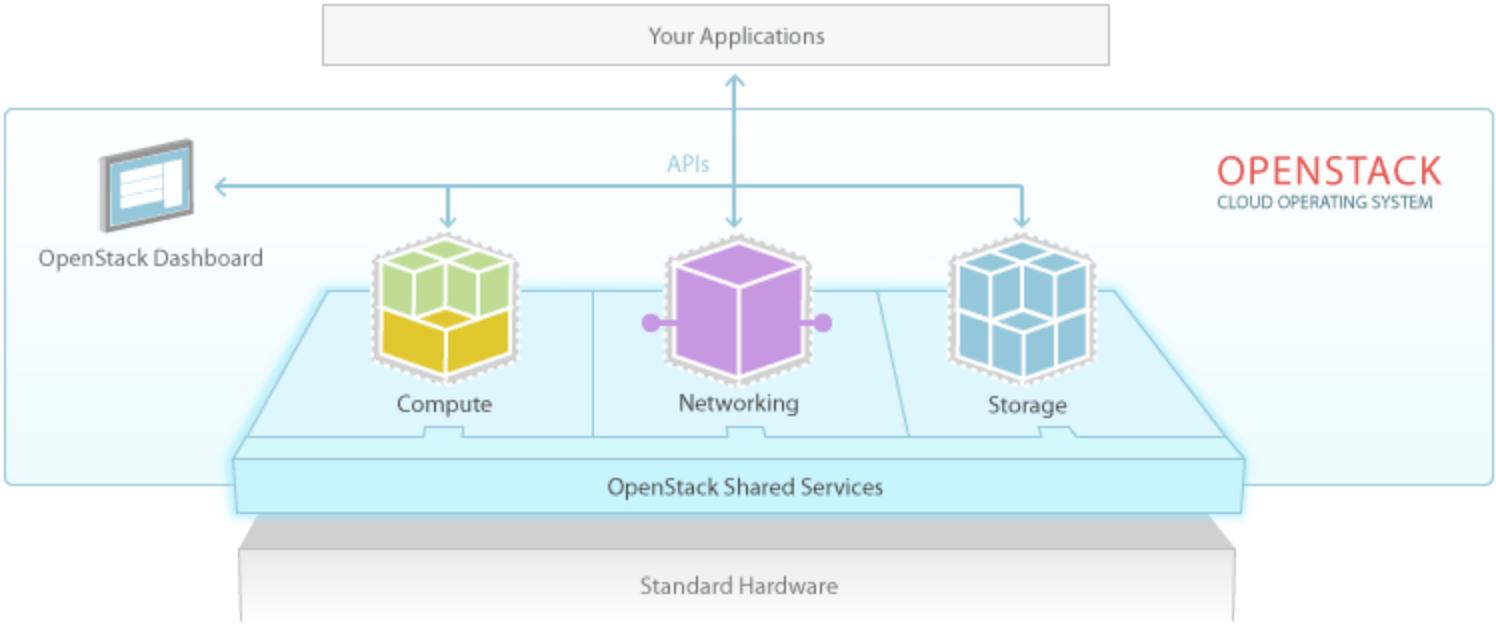
Merge Vs Export of Objects



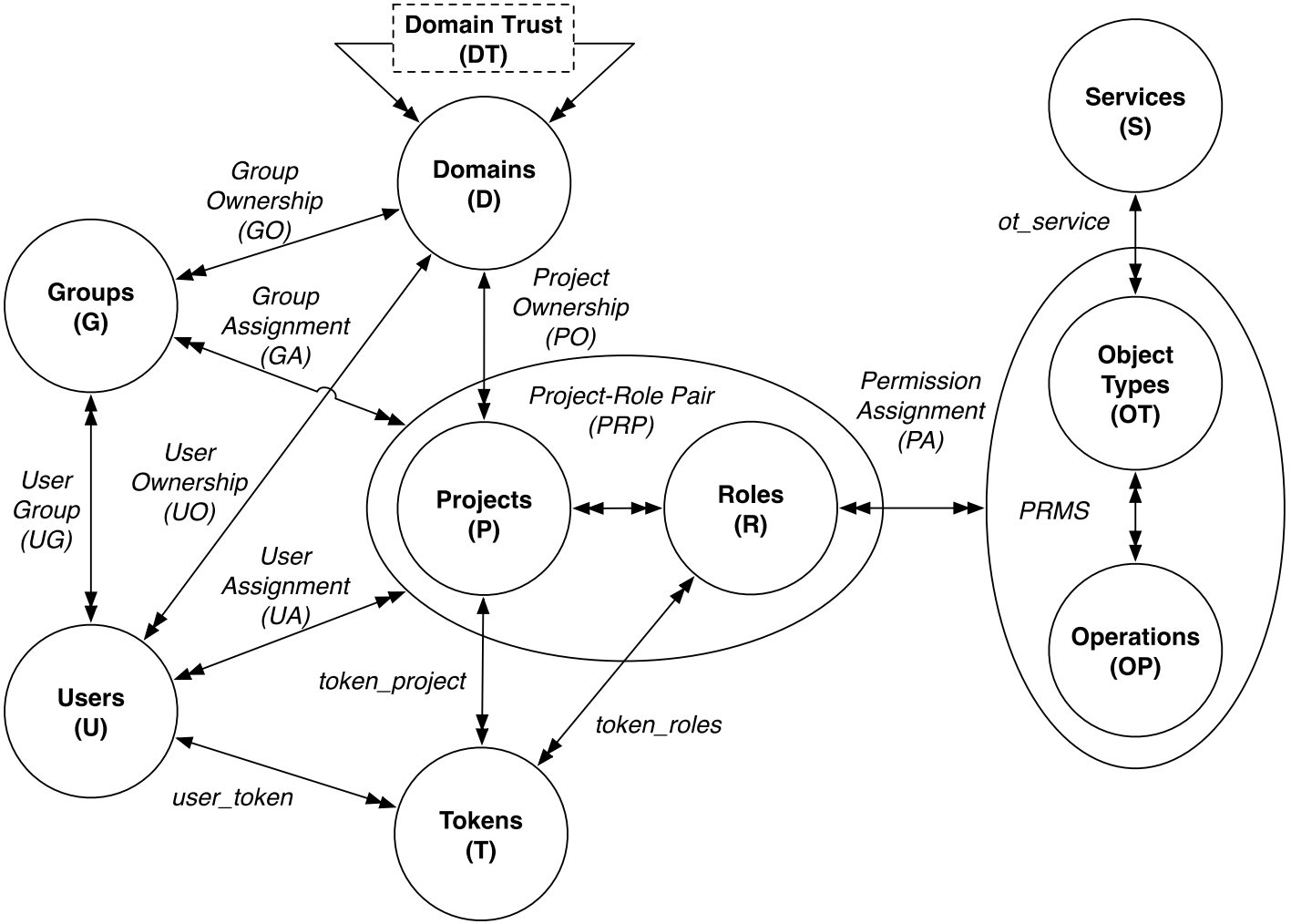
OpenStack

- OpenStack
  - Dominant open-source cloud IaaS software

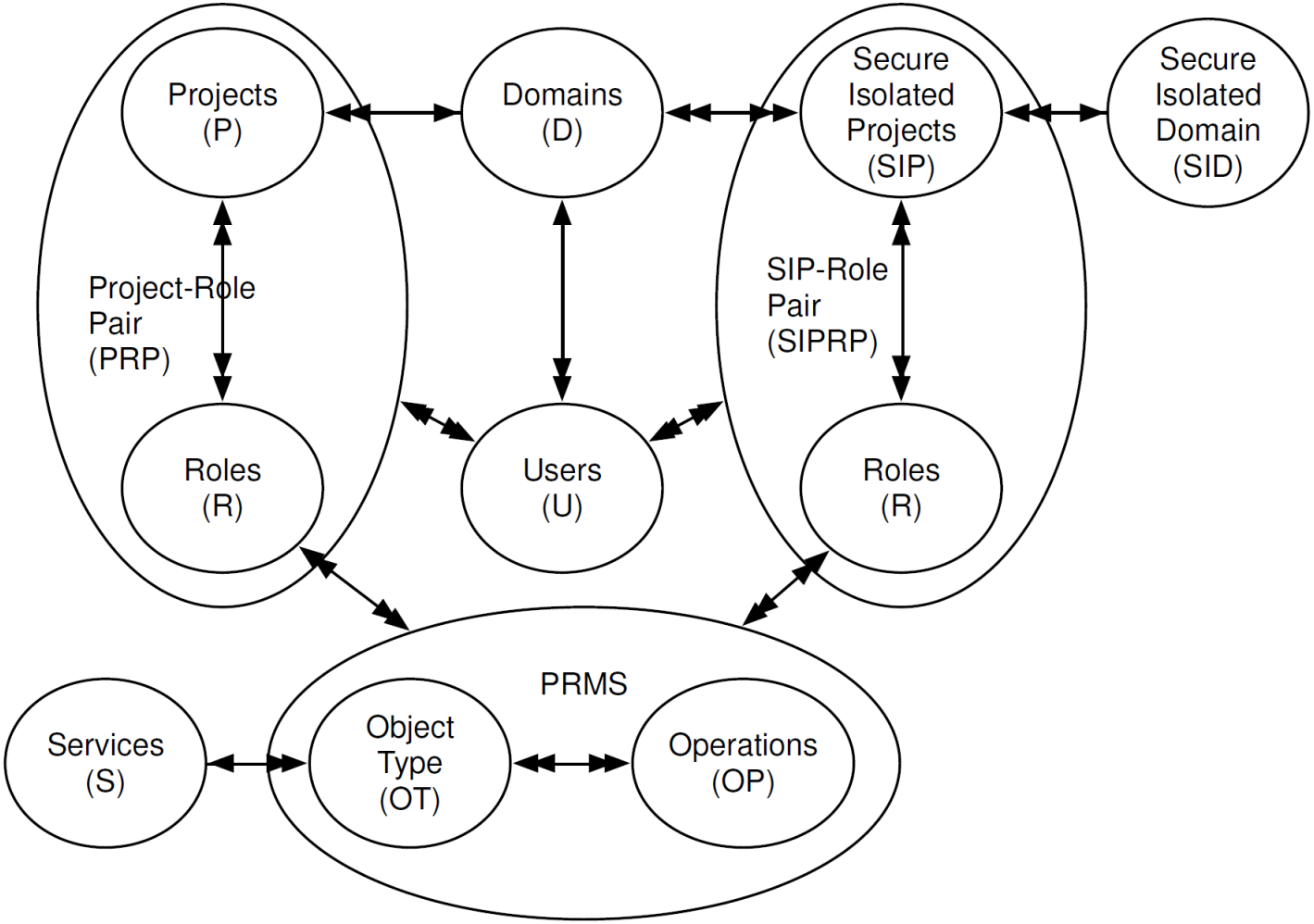
- > 200 companies
- ~14000 developers
- >130 countries



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)

OSAC-SID Administrative Model

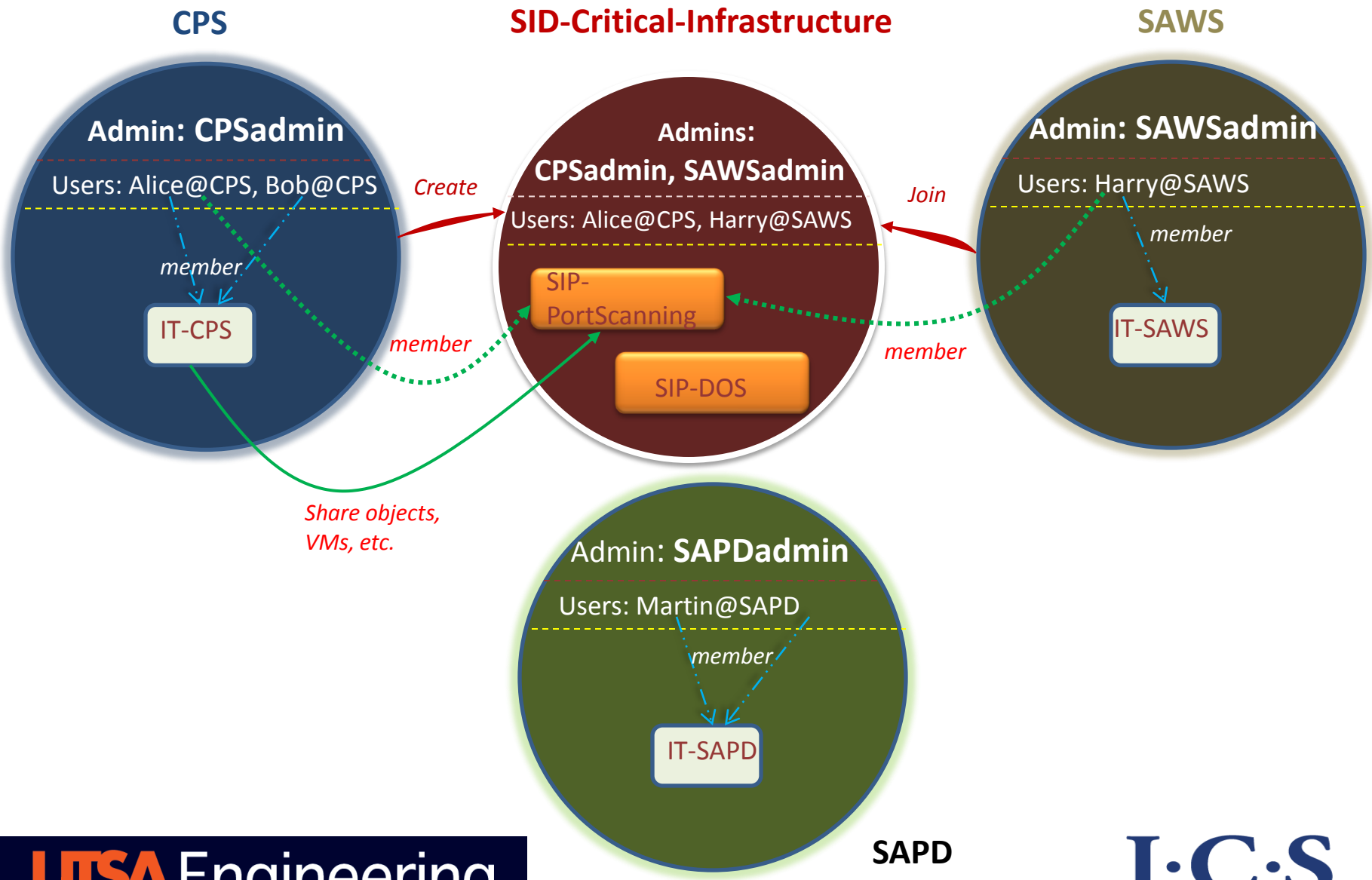
Operation	Authorization Requirement	Update
SipCreate(uSet, sip) */* a set of domain admin users together create a sip */*	∀ u1, u2 ∈ uSet.((DA(u1)=True ∧ DA(u2)=True ∧ u1 ≠ u2 ∧ UO(u1) ≠ UO(u2))) sip ∈ (UNIV_SIP - SIP)	SIPO(sip) = $\bigcup_{\forall u \in uSet}$ UO(u) SIPU(sip) = uSet ∀ u ∈ uSet.SIPA(u)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



Key Accomplishments (1)

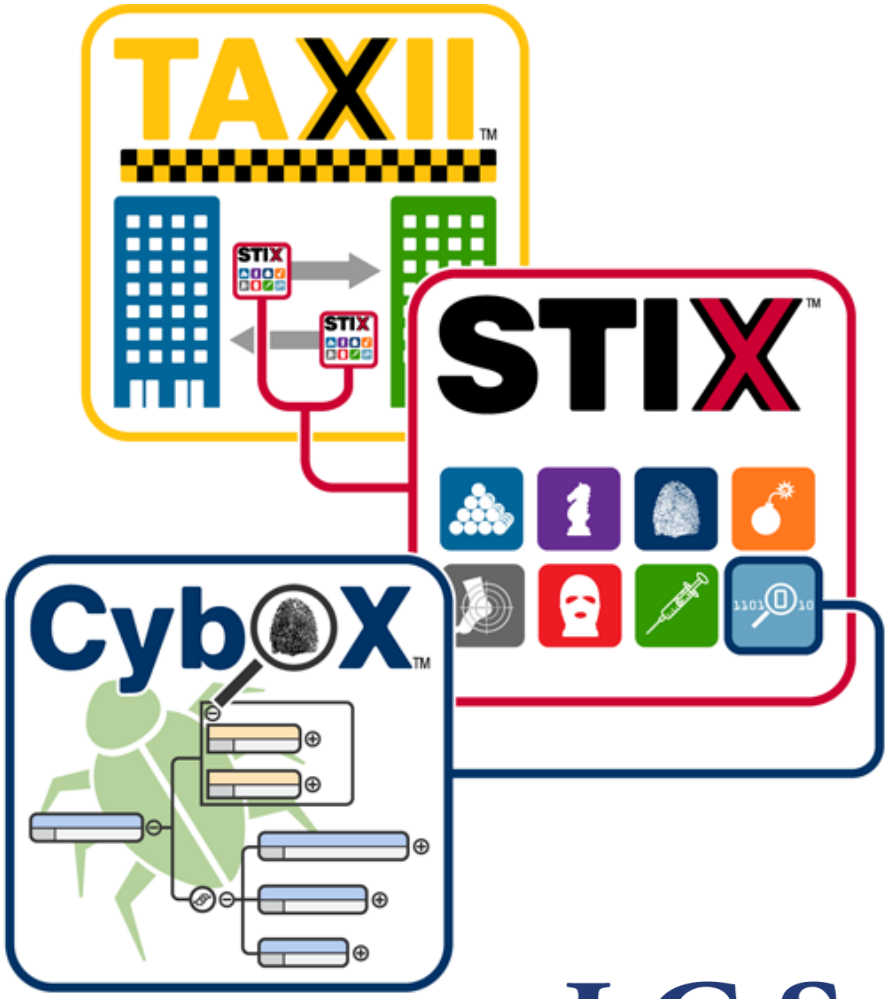
- Developed sharing models
  - Formal specification
  - Cloud-based instantiation
- Enhanced OpenStack with SID/SIP capabilities
  - Cyber incident response capabilities out of the box
    - Self-service
    - SID/SIP specific security
    - Share data, tools, etc. in an isolated environment
    - Ability to execute and analyze malicious code in an isolated environment
  - Practitioners can deploy a “cyber incident response” cloud
  - Potential blueprint for official OpenStack adoption

Key Accomplishments (2)

- Initial work published in Association for Computing Machinery (ACM) Workshop on Information Sharing and Collaborative Security (WISCS '14)
  - To be presented on November 3, 2014 in Scottsdale, AZ
  - Potential dissertation topic for Amy Zhang, PhD Candidate

Next Steps (1)

- Integrate STIX-TAXII in SID
  - Information Sharing Specifications for Cybersecurity
- Trusted Automated eXchange of Indicator Information (TAXII)
- Structured Threat Information eXpression (STIX)
- Cyber Observable eXpression (CybOX)



Next Steps (2)

- Fine-grained and expressive access control
- Hardened SID/SIP
- User-friendly interface for management
- Develop cyber incident response lifecycle management in cloud
  - Prepare, share, detect & analyze, contain/eradicate, post-incident activity, etc.

Thanks

- Comments, Q&A