

A Group-Centric Model for Collaboration with Expedient Insiders in Multilevel Systems

Khalid Zaman Bijon, Ravi Sandhu, Ram Krishnan
Institute for Cyber Security
University of Texas at San Antonio

May 22, 2012

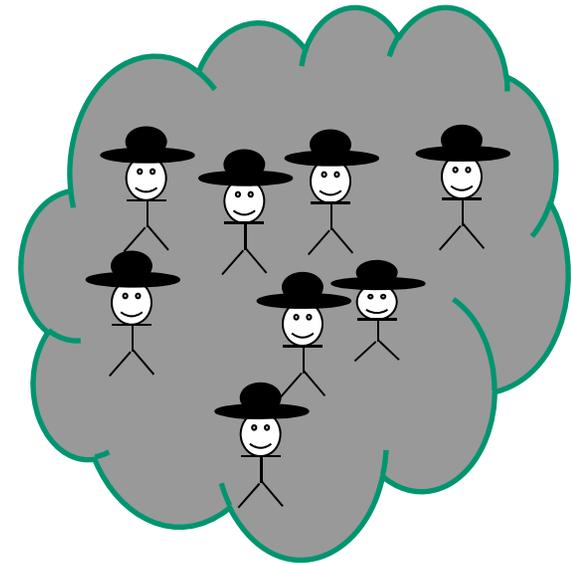
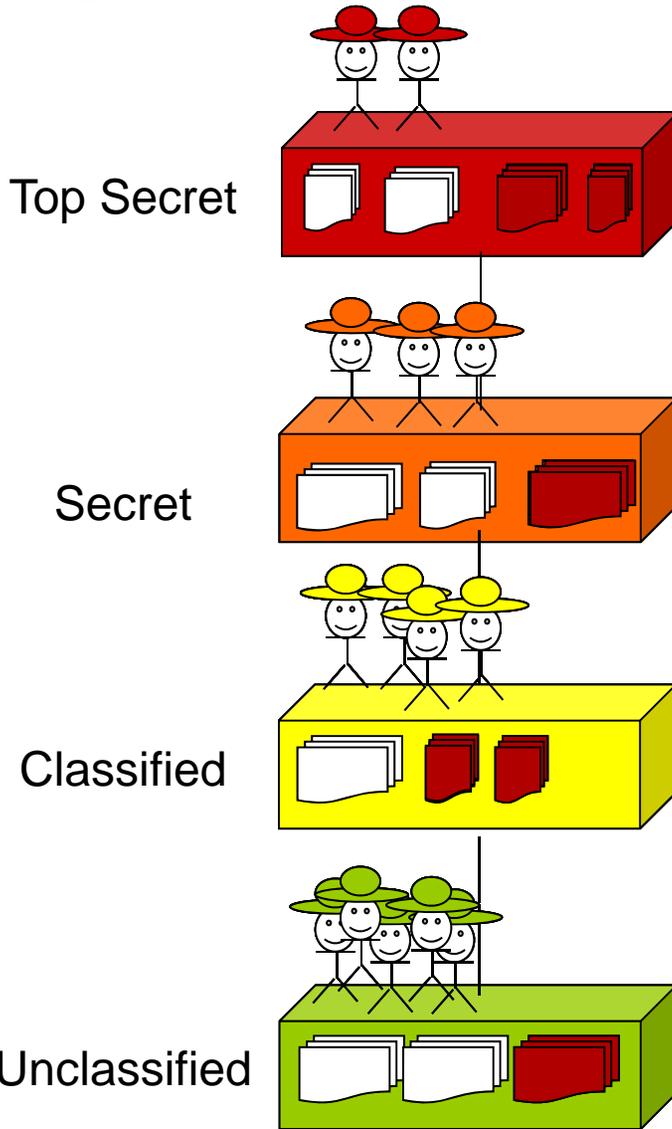
International Symposium on Security in Collaboration Technologies and Systems

- Who are expedient insiders?
 - Any outside Collaborators, i.e. Domain specialists, cyber-security experts, etc.
- Difference with respect to true insiders
 - Transient rather than persistent
 - Information sharing is based on need-to-consult basis
 - Less commitment than long time employees

What are the Challenges?

1. *Information selection for collaboration*
2. *Restrict unnecessary access*
3. *Import results*

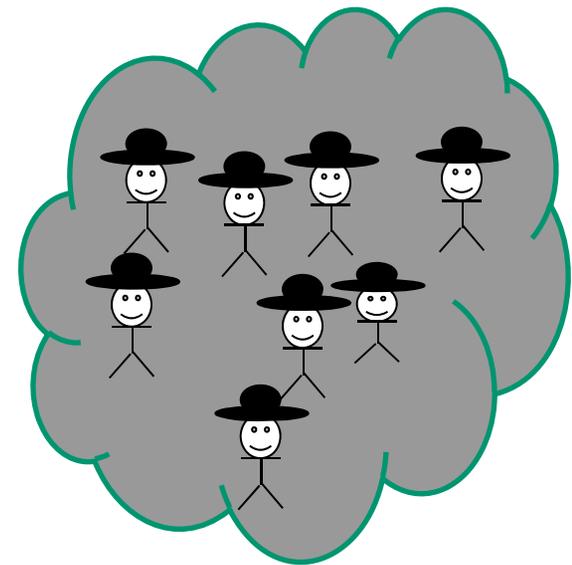
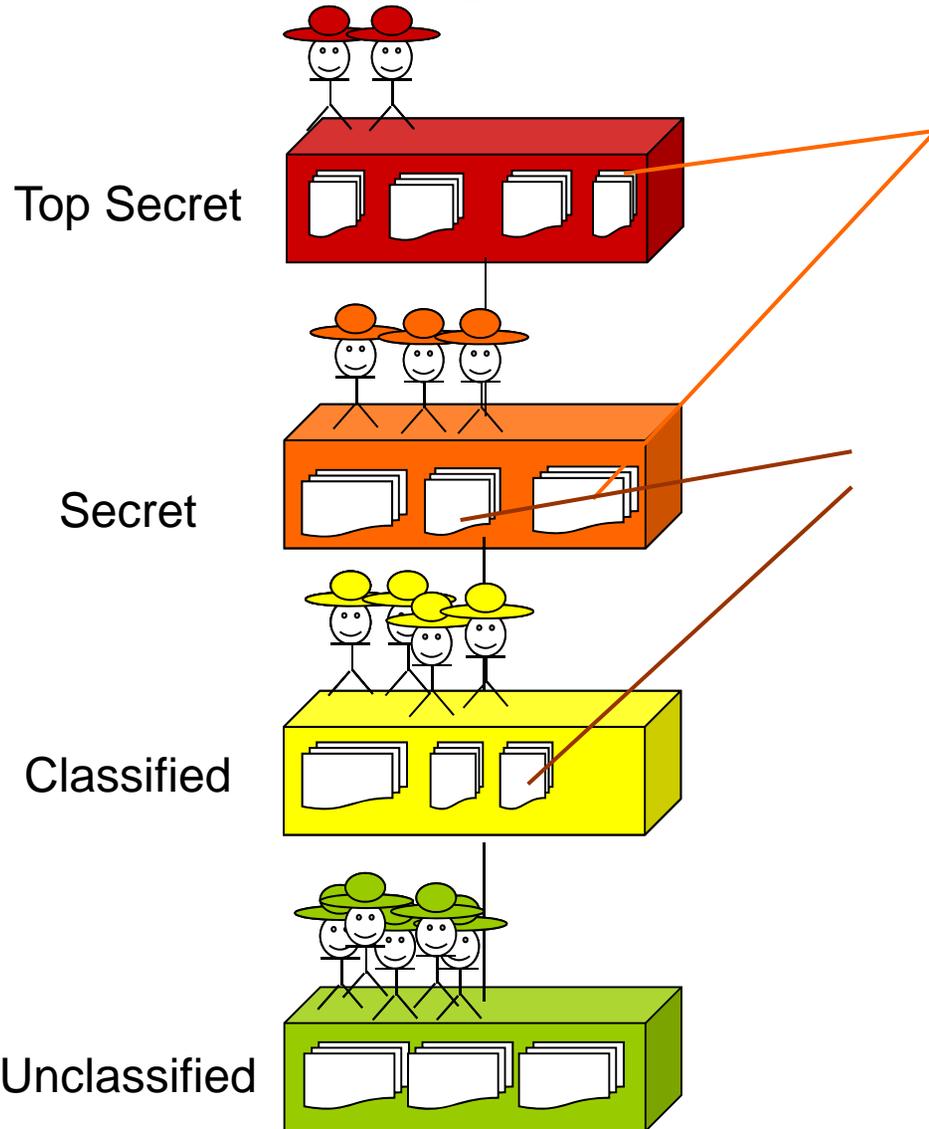
- Assign to a place in existing organizational structure



Outside Collaborators

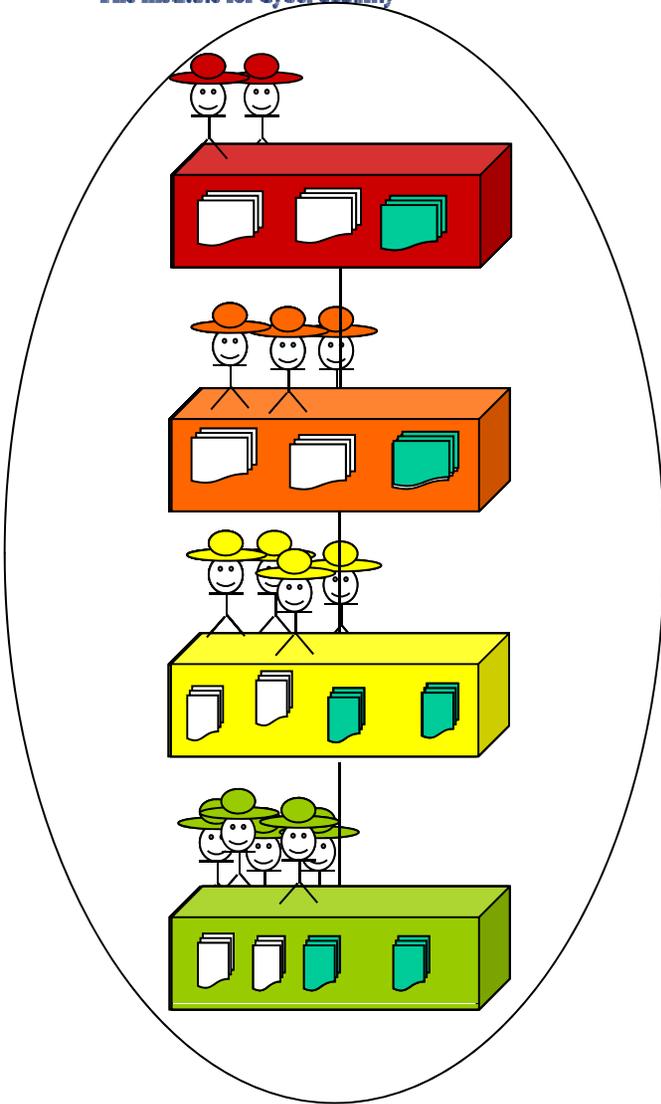
Sharing more information than necessary
Open to more true-insiders than necessary

- Individual Sharing Collaboration

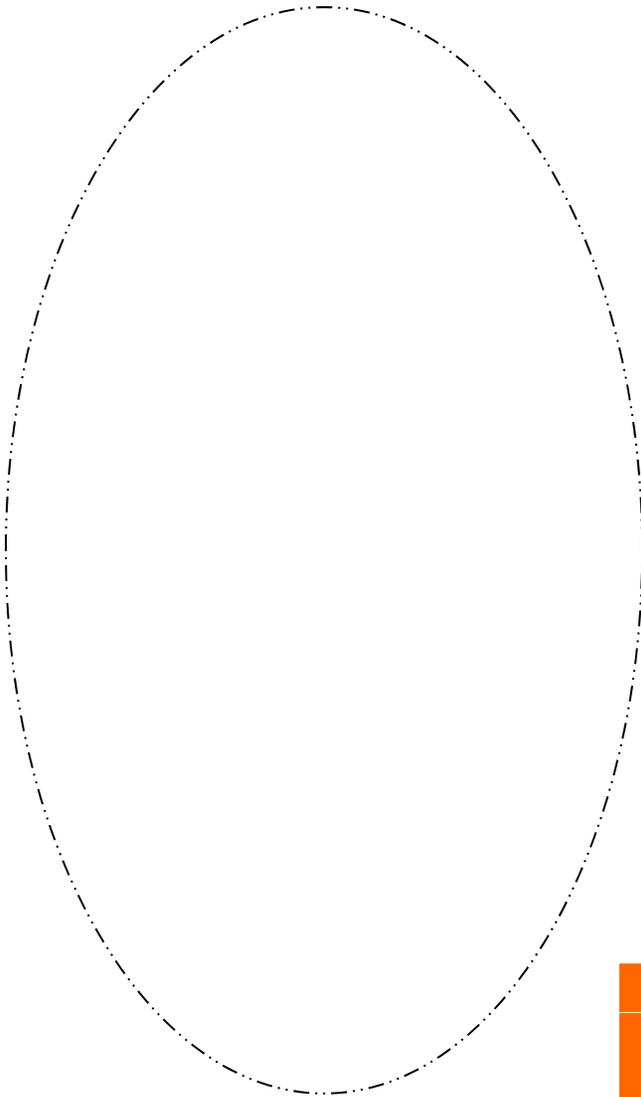


Outside Collaborators

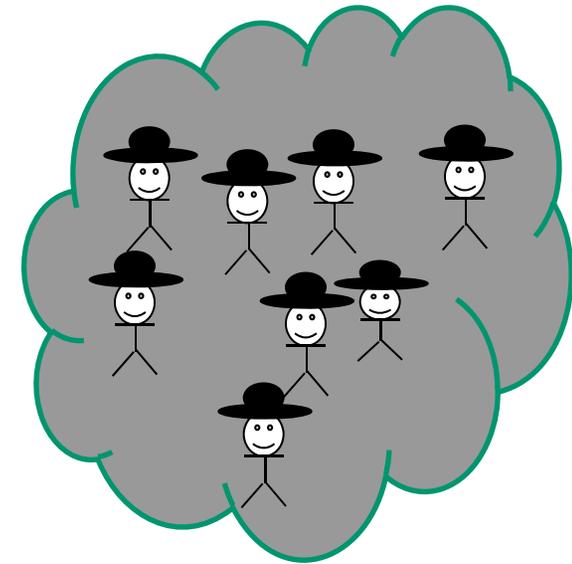
Scalability is the main Issue!



Organization



Collaboration Group
with Expedient Insider



Outside Collaborators

Just Right Sharing
Scalable

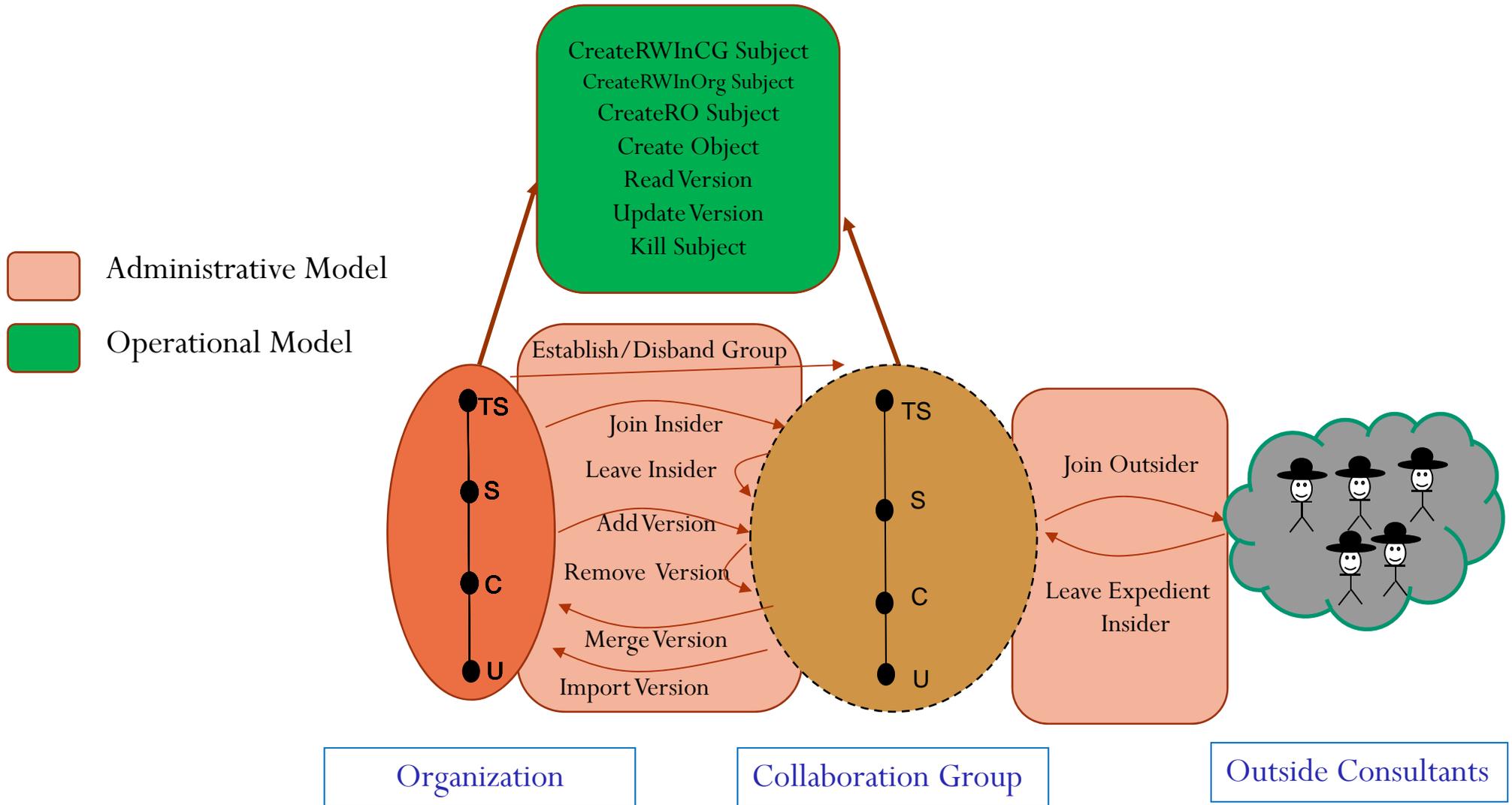
Operational aspect

- User-Subject Model
 - User: human in the system
 - Subject: Programs/processes on behalf of user
- Object-Version Model
 - write creates a new version
 - Security classification of versions (same?)
- Subject Model
 - Read-Only Subject (can not write object but read from multiple groups)
 - Read-Write Subject (can write but limited read capability)

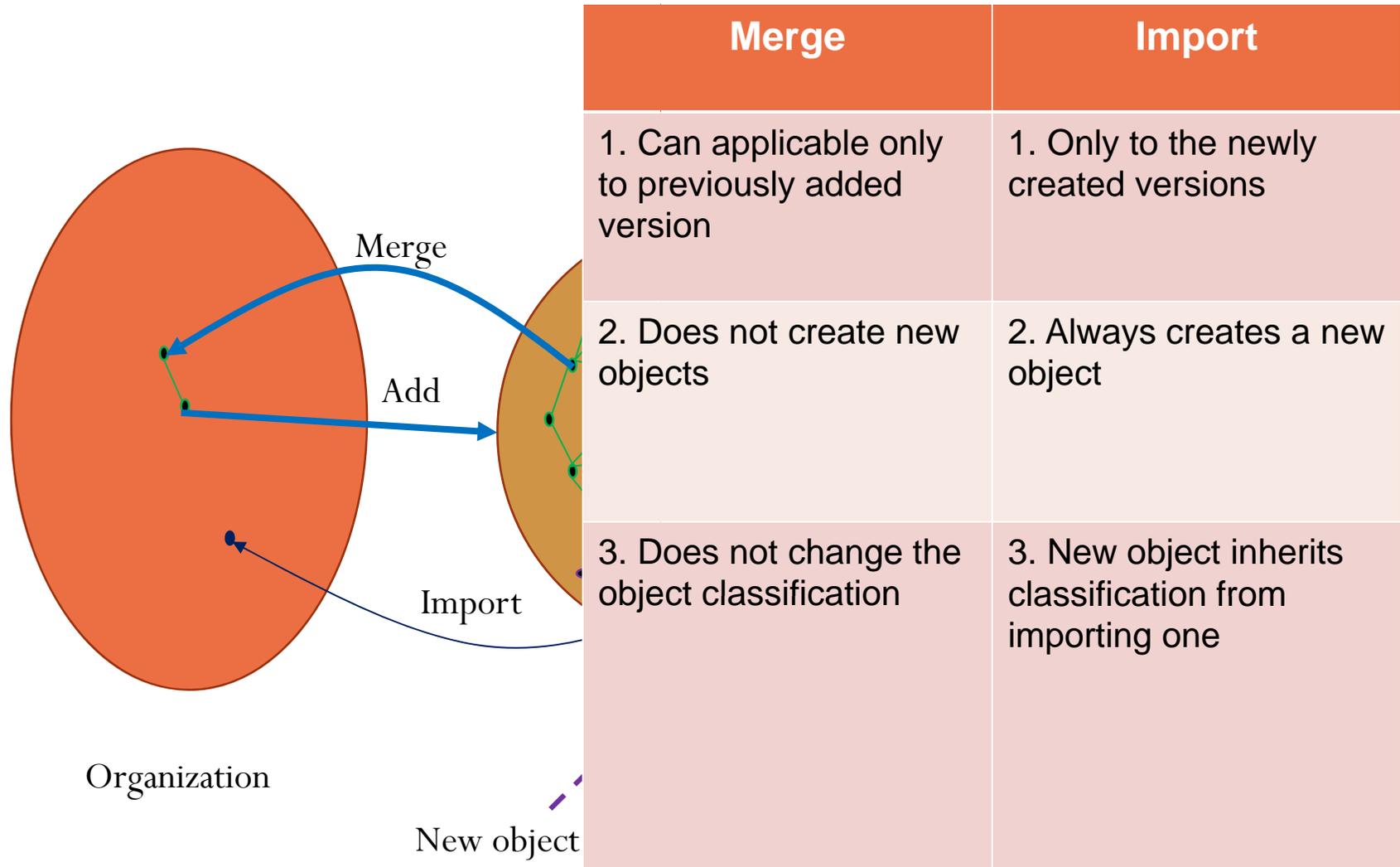
Administrative aspect

- Membership Management
 - True Insider: Regular employee
 - Expedient Insider: Collaborators, Consultants
- Group Lifecycle
- Objects Management
- Lattice Structure
- G-SIS specification

True Insiders	Expedient Insiders
1. Simultaneously hold membership in multiple groups and organization	1. Can get membership to multiple groups but not in organization
2. Retain the same organization clearance when joining a new group	2. Assigned a single clearance for every group they join
3. Can access all objects that <ul style="list-style-type: none">- Satisfy dominance relation- in organization or joined groups	3. Can access all objects that <ul style="list-style-type: none">- Satisfy dominance relation- in joined groups only



Read Only	Read Write
1. Can not write, read is restricted by BLP simple security property	1. Can read and write, however, write is restricted by BLP strict * property
2. User determines the security clearance (\leq user's clearance)	
3. Can read objects across groups	3. restricted within the same group it was created
4. Can not create new object	4. Can create new object and object inherits its clearance
5. Read operation does not create new object versions	5. Only a write operation always create a new version of the respective object, however, does not change the classification of the version



Global Sets and Symbols:

SL: Finite lattice of security levels with dominance ordering \succeq
 CG: Finite set of existing groups
 U: Finite set of existing users
 O: Finite set of existing objects
 S: Finite set of existing subjects
 UNIV_V: The universal set of versions (an infinite set)
 Org: The organization (a constant symbol)

User Attributes: $\text{Att}(U)=\{\text{clearance, ucg, orgadmin, cgadmin, utype}\}$

clearance: $U \rightarrow \text{SL}$
 ucg: $U \rightarrow 2^{\text{CG}}$
 orgadmin: $U \rightarrow \{\text{True, False}\}$
 cgadmin: $U \rightarrow 2^{\text{CG}}$
 utype: $U \rightarrow \{\text{Insider, Expedient_Insider, null}\}$

Objects Attributes: $\text{Att}(O)=\{\text{classification, origin, versions}\}$

classification: $O \rightarrow \text{SL}$
 origin: $O \rightarrow \text{CG} \cup \{\text{Org}\}$
 versions : $O \rightarrow 2^{\text{UNIV_V}}$

Subject Attributes: $\text{Att}(S)=\{\text{clearance, owner, belongsTo, type}\}$

clearance : $S \rightarrow \text{SL}$
 owner: $S \rightarrow U$
 belongsTo: $S \rightarrow \text{CG} \cup \{\text{Org}\}$
 type: $S \rightarrow \{\text{RW,RO}\}$

Object Version Attribute: $\text{Att}(O, V)=\{\text{vMember, classification}\}$

vMember : $O \times \text{UNIV_V} \rightarrow 2^{\text{CG} \cup \{\text{Org}\}}$
 classification: $O \times \text{UNIV_V} \rightarrow \text{SL}$
 /* These are partial function defined only for the versions that exist for each object*/

- Join Insider operation could modify clearance
 - A manager of the organization could be a group director, etc.
- Add object operation could modify classification
 - A secret object might get top secret classification in collaboration group
- Add object could sanitize information
 - Organization might not want to share actual object

**A novel method to manage expedient-insider
collaboration in multi level systems**

Advantage of Group Centric Collaboration Model

- Selective information sharing
- Controlled flow back of results
- Does not interfere with the main lattice structure
- Easier to manage collaborations

Future Work

- Collaboration group with multiple organizations, expedient insiders, etc.
 - Merging different organization's structures

Thank You 😊
