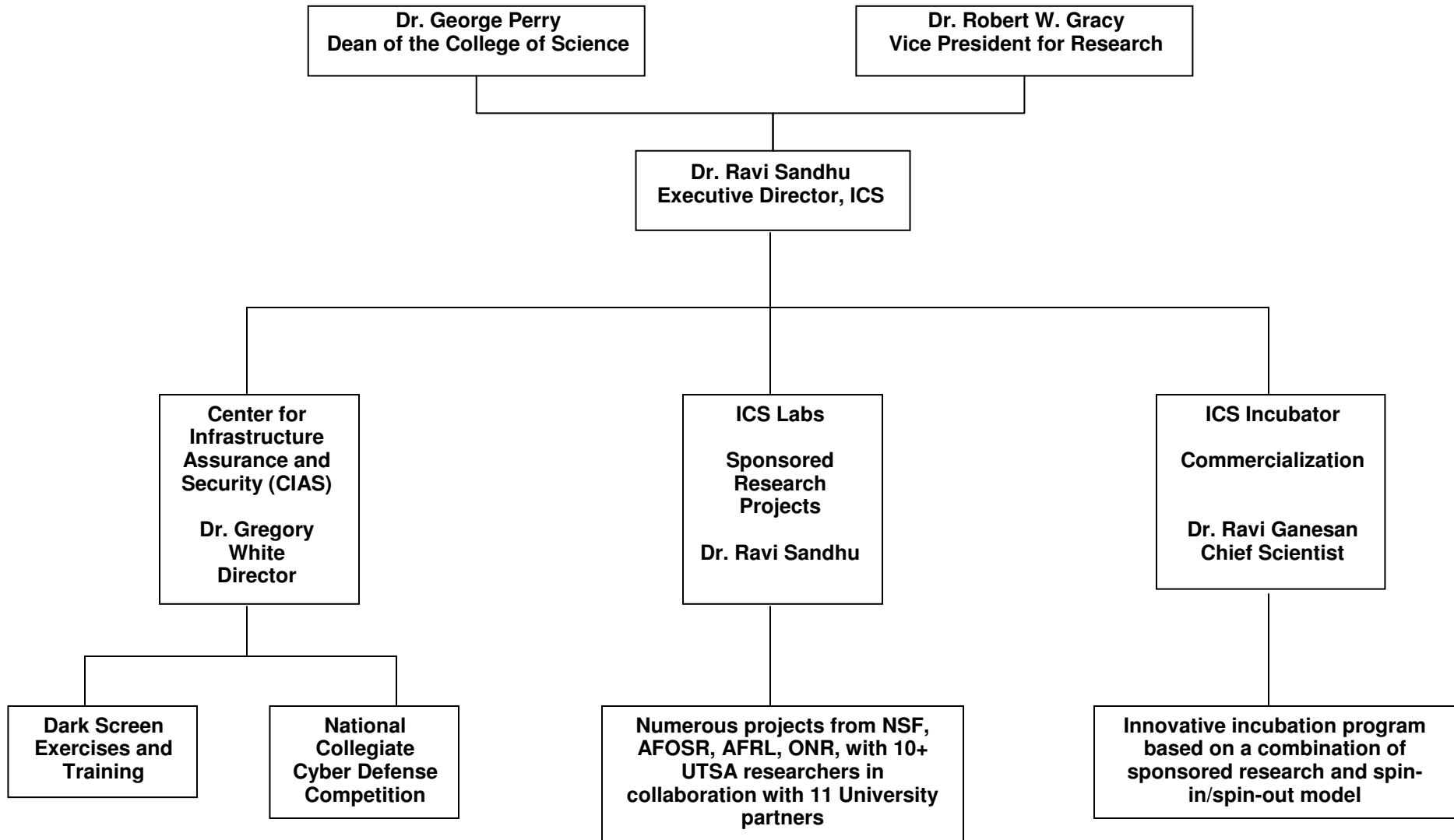


Application-Centric Security Models

Prof. Ravi Sandhu
Executive Director and Endowed Chair
Institute for Cyber Security
University of Texas at San Antonio
June 2009

ravi.sandhu@utsa.edu
www.profsandhu.com



- World leading security modeling and analysis research
 - Role-Based Access Control (RBAC) Model (1996)
 - Catalyzes dominance of RBAC in commercial systems
 - Develops into a NIST/ANSI Standard (2004)
 - Usage Control (UCON) Model (2004)
 - Attribute-Based Access Control on Steroids
 - Unifies numerous extensions/enhancements
 - PEI Framework (2000, 2006)
 - Policy, Enforcement, Implementation Models
 - From what to how
 - Group-Centric Information Sharing (2007)
 - Sharing metaphor of meeting room
 - Equivalently: mission centric
- Bring in partners from leading research universities as appropriate
- Ready to commercialize when appropriate

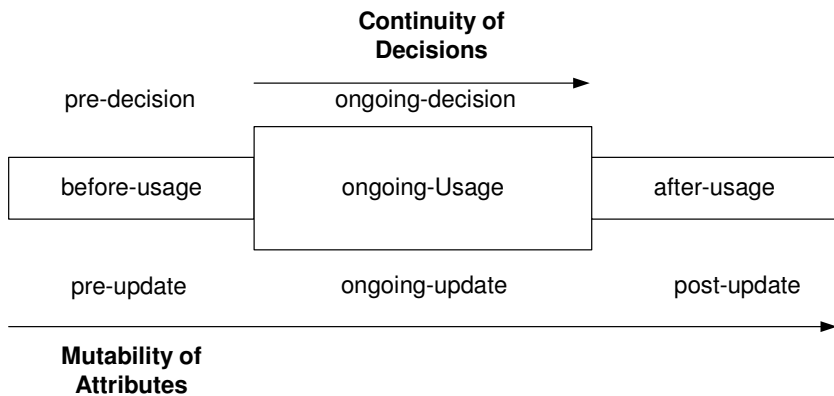
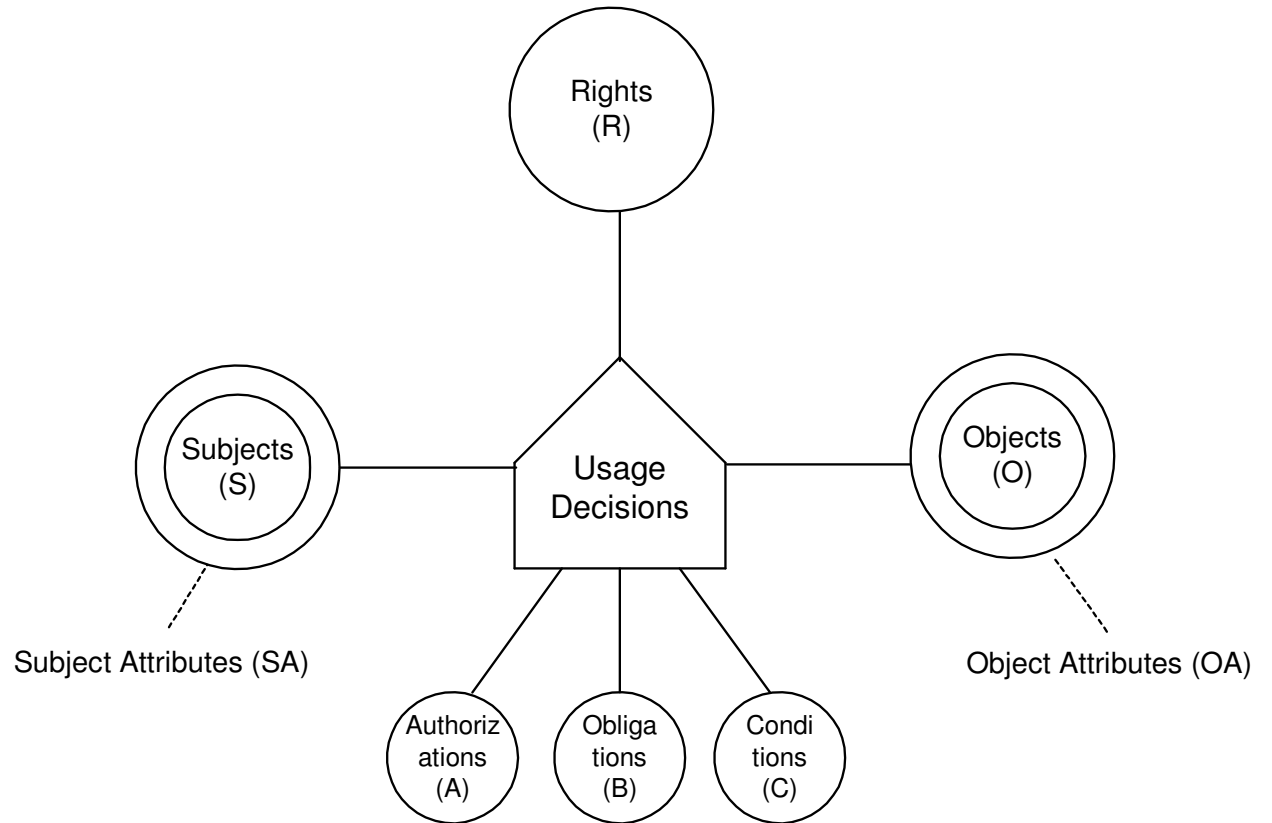
- Our Basic Premise
 - There can be no security without application context
 - Courtney’s Law (1970s, 1980s ??):
 - You cannot say anything interesting (i.e. significant) about the security of a system except in the context of a particular application and environment
- Corollary
 - There can be no security model without application context
- Reality
 - Existing security models are application neutral
 - Assumption is they can be readily “configured” or “policy-fied” to suit application context

- Discretionary Access Control (DAC)
 - Characteristic: Owner-based discretion
 - Drawbacks:
 - Classic formulation fails to distinguish copy from read
 - Application context drives ownership and its delegation
- Lattice-Based Access Control (LBAC)
 - Characteristic: One directional information flow in a lattice of security labels
 - Also known as: Bell-LaPadula, Multi-Level Security, Mandatory Access Control (ignoring subtle differences)
 - Drawbacks:
 - Many applications violate one directional information flow
 - Many applications do not fit within preexisting security labels

- **Role-Based Access Control (RBAC)**
 - Characteristic: Role is central, administration is simple
 - Drawbacks:
 - Need to define the roles for each application/environment
 - Lack of standardized roles results in lack of interoperability
 - Too open: can be configured to do DAC or LBAC
- **Attribute-Based Access Control (ABAC)**
 - Characteristic: subsume security labels, roles and more as attributes and enforce attribute-based policies
 - Drawbacks:
 - All the RBAC drawbacks on steroids
 - Administrative complexity

Usage Control Model (UCON)

- unified model integrating
 - authorization
 - obligation
 - conditions
- and incorporating
 - continuity of decisions
 - mutability of attributes

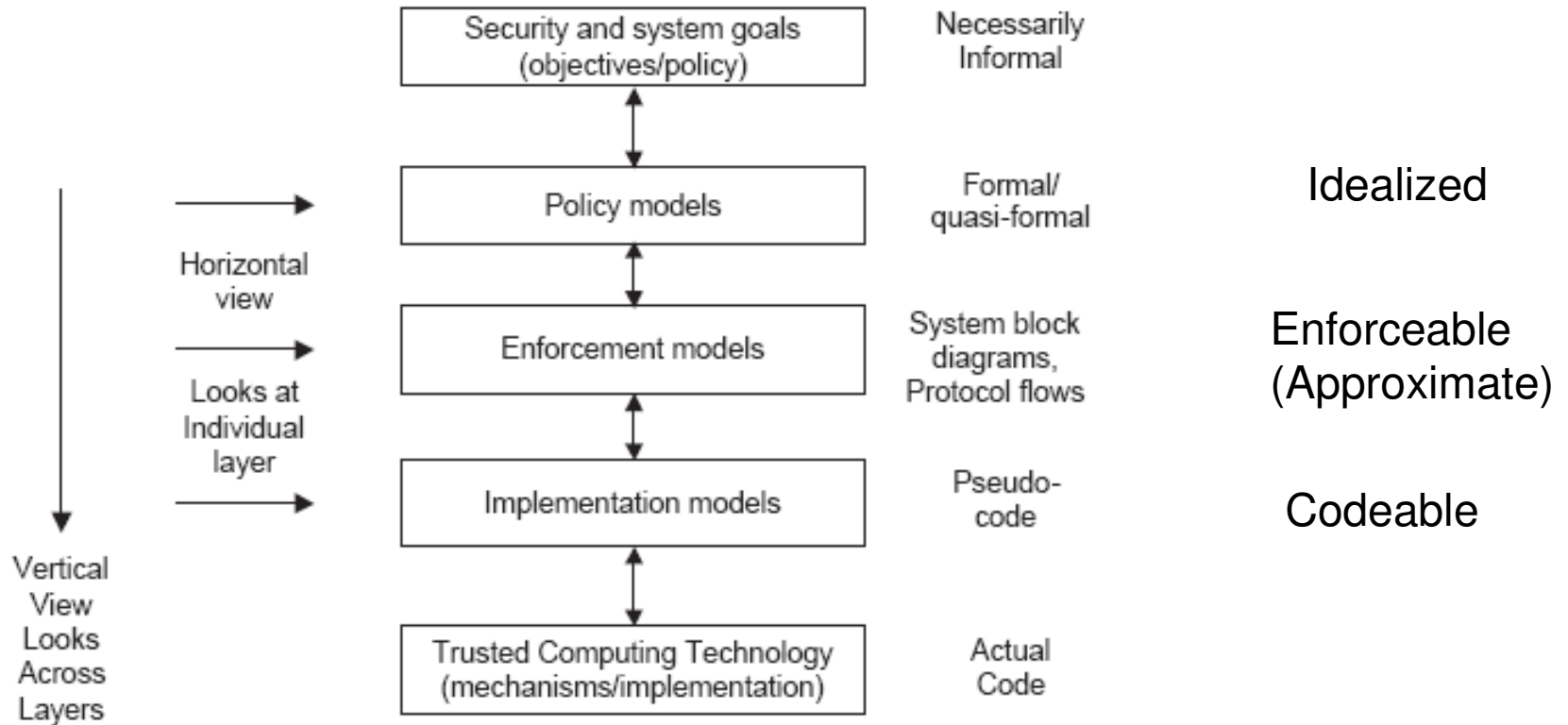


UCON is Attribute-Based Access Control on Steroids

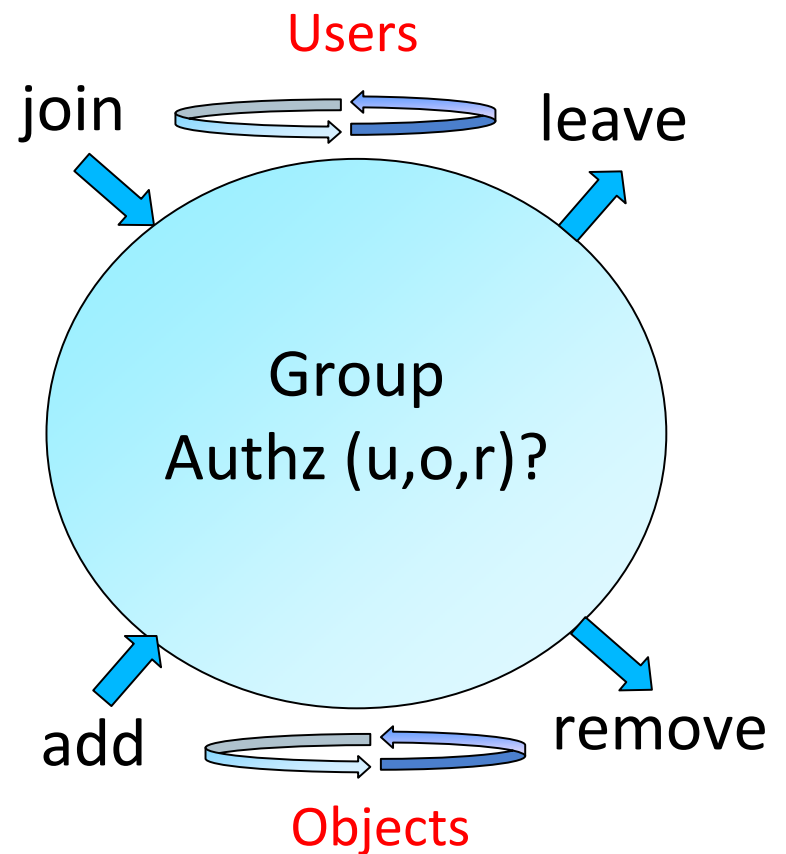
- DAC
- LBAC
- RBAC
- ABAC
- ... and many, many others
- UCON
 - ABAC on steroids
 - Simple, familiar, usable and effective use cases demonstrate the need for UCON
 - Automatic Teller Machines
 - CAPTCHAs at Public web sites
 - End User Licence Agreements
 - Terms of Usage for WiFi in Hotels, Airports
 - Rate limits on call center workers

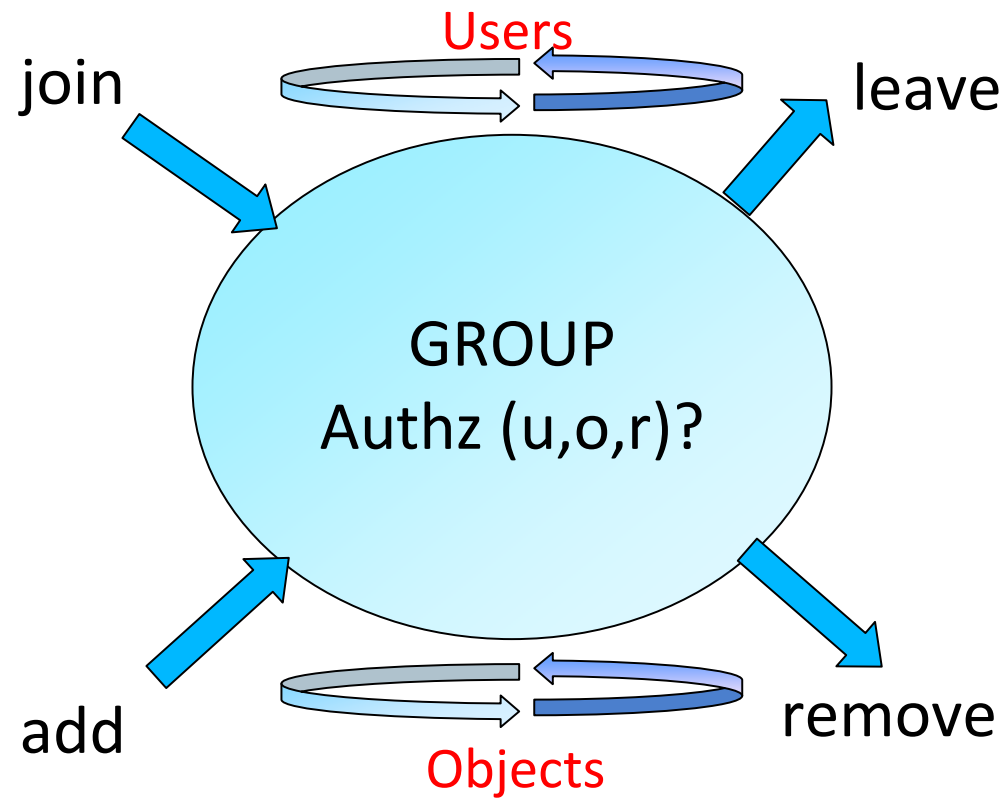
- Our Basic Premise
 - There can be no security model without application context
- So how does one customize an application-centric security model?
 - Meaningfully combine the essential insights of
 - DAC, LBAC, RBAC, ABAC, UCON, etcetera
 - Directly address the application-specific trade-offs
 - Within the security objectives of confidentiality, integrity and availability
 - Across security, performance, cost and usability objectives
 - Separate the real-world concerns of
 - practical distributed systems and ensuing staleness and approximations (enforcement layer) from
 - policy concerns in a idealized environment (policy layer)

PEI Models: 3 Layers/5 Layers

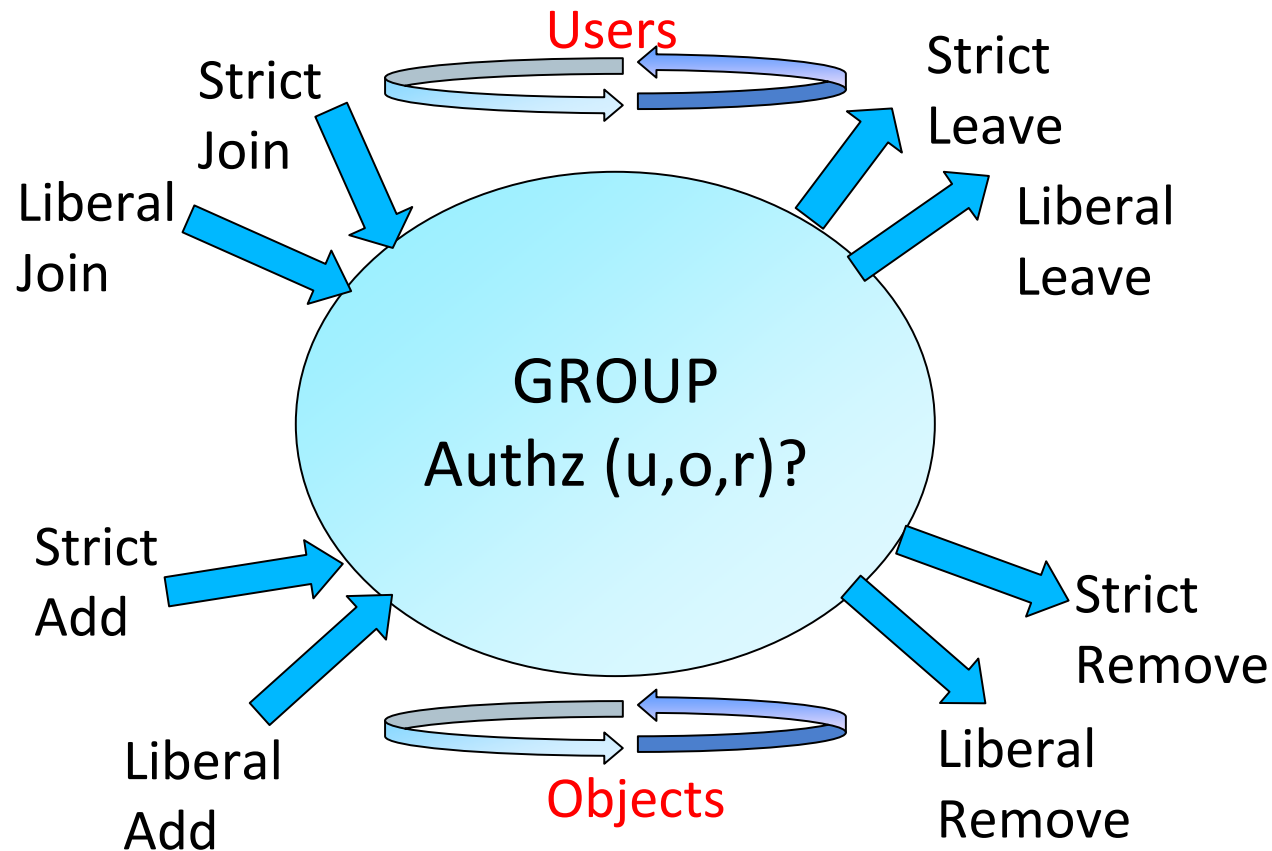


- Brings users & objects together in a group
 - Focuses on manageability using groups
 - Co-exists with dissemination-centric
 - Two metaphors
 - Secure Meeting Room (E.g. Program committee)
 - Subscription Model (E.g. Secure multicast)
- Operational aspects
 - Group characteristics
 - E.g. Are there any core properties?
 - Group operation semantics
 - E.g. What is authorized by join, add, etc.?
 - Read-only Vs Read-Write
- Administrative aspects
 - E.g. Who authorizes join, add, etc.?
 - May be application dependant
- Multiple groups
 - Inter-group relationship

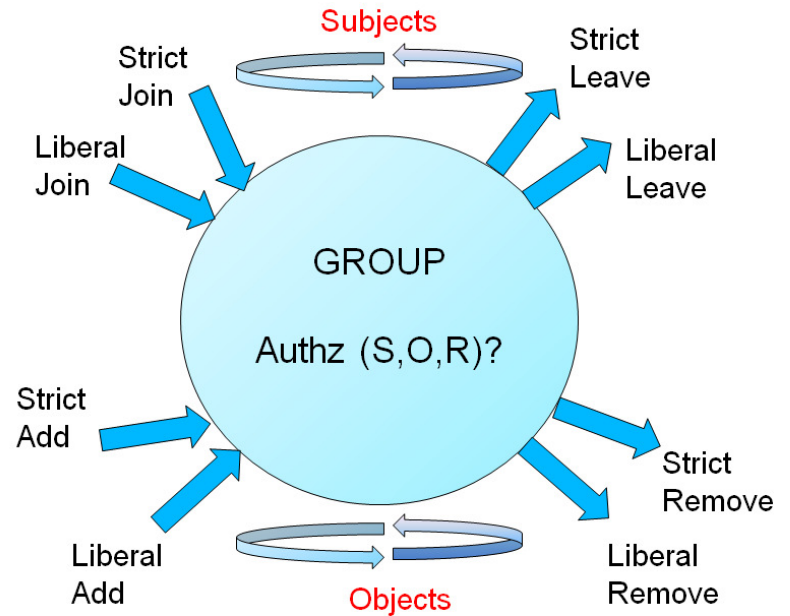
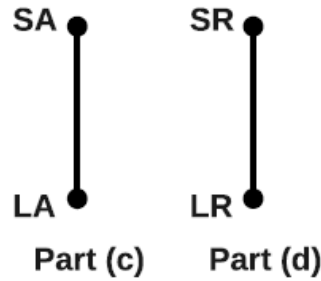
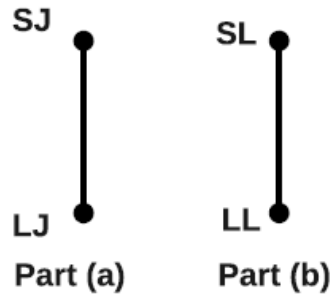




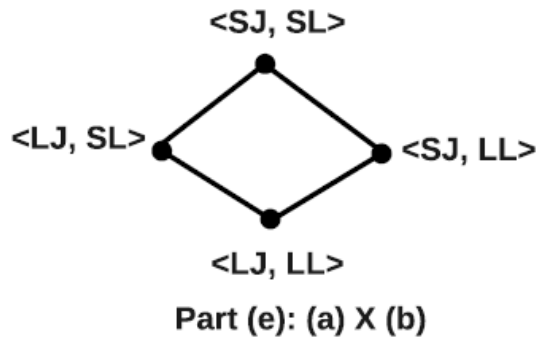
g-SIS Operation Semantics



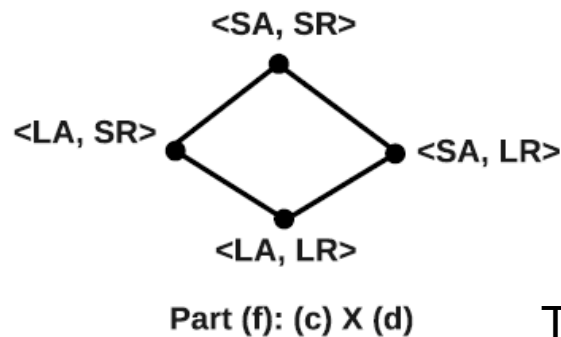
Family of g-SIS Policy Models



Subject Model



Object Model



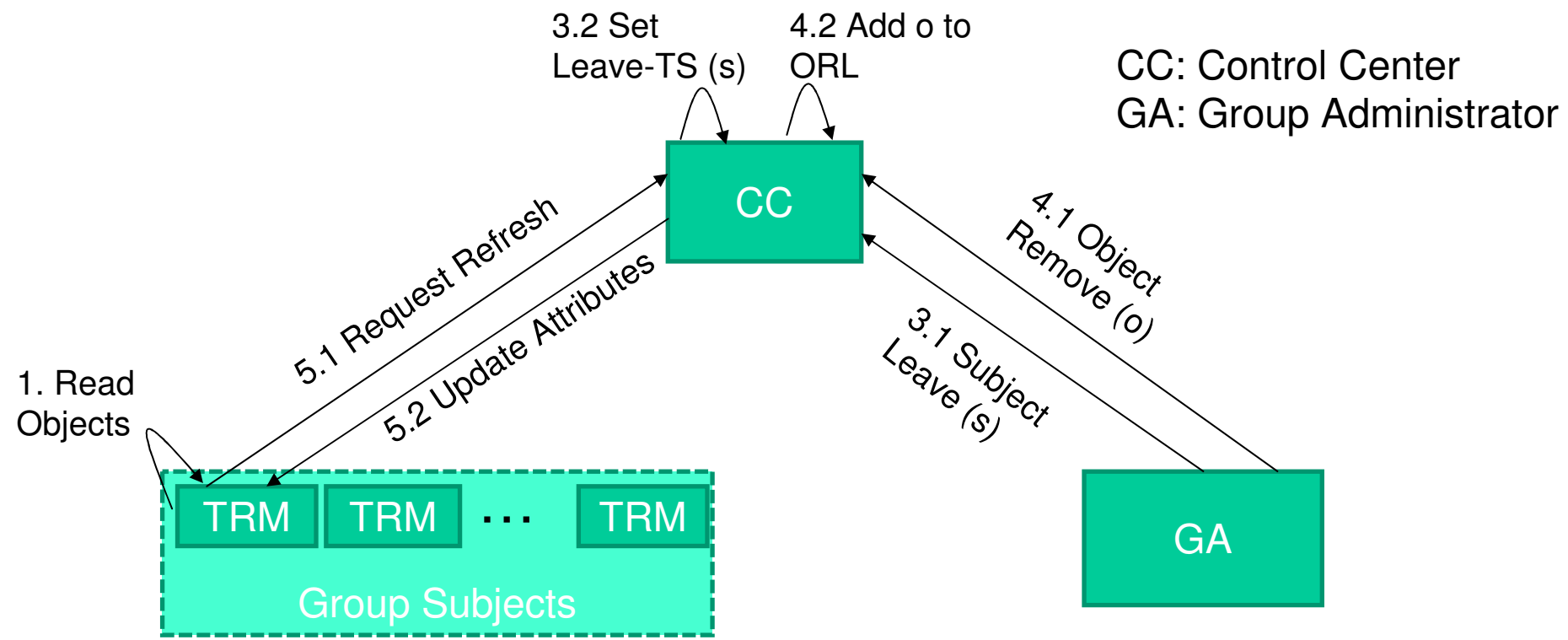
g-SIS models: (e) X (f)

Traditional Groups: <LJ, SL, LA, SR>
Secure Multicast: <SJ, LL, LA, *>

Most Restrictive
g-SIS Specification:

$$\square(\text{Authz} \leftrightarrow (\neg \text{SR} \wedge \neg \text{SL}) \mathcal{S} (\text{SA} \wedge (\neg \text{SL} \mathcal{S} \text{SJ})))$$

g-SIS Enforcement Model



CC: Control Center
GA: Group Administrator

Subject Attributes: {id, Join-TS, Leave-TS, ORL, gKey}
 ORL: *Object Revocation List*
 gKey: *Group Key*

Object Attributes: {id, Add-TS}

Refresh Time (RT): TRM contacts CC to update attributes

- Additional Trusted/Semi-Trusted Servers
- Approximate Enforcement

- Finally, the Implementation layer models spell out protocol details and details of TRM algorithms

- Application-Centric Security Models require
 - State-of-the-art approaches such as UCON, PEI
 - Mix-and-match essential ideas of DAC, LBAC, RBAC, UCON
- Relevance to cyber range
 - Cyber range is itself a new application and technology
 - Group based information sharing is a good fit for information sharing within the cyber range
 - Cyber range capabilities will need to support next generation security models
 - Cyber range capabilities will need to support application-centric security models
 -
 -