Group-Centric Models for Secure Information Sharing

Prof. Ravi Sandhu
Executive Director and Endowed Chair

March 30, 2012

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

Joint work with ICS colleagues:
Ram Krishnan, Jianwei Niu and Will Winsborough

Goal: 4th Element

- 3 succesful access control models in 40+ years
  - Discretionary Access Control (DAC)
  - Mandatory Access Control (MAC)
  - Role-base Access Control (RBAC)
- Crucial ingredients for success
  - Strong mathematical foundations
  - Strong intuitive foundations
  - Significant real-world deployment

What is the 4th Element?

- DAC – owner control
- MAC – information flow in a lattice
- RBAC – organizational/social alignment
- Dynamics/agility
  - DAC: too loose, too fine-grained
  - MAC: too rigid, static lattice
  - RBAC: too enterprise centric
  - Group-centric conceived to fill this gap

Historical Aside on Dynamics/Agility

- Harrison, Russo and Ullman 1976: HRU
  - dynamics leads to undecidable safety
- Jones, Lipton, Snyder 1978: Take-Grant
  - simple models can be efficiently decidable
- Sandhu, 1988, 1992: SPM, TAM
  - sophisticated models can be efficiently decidable

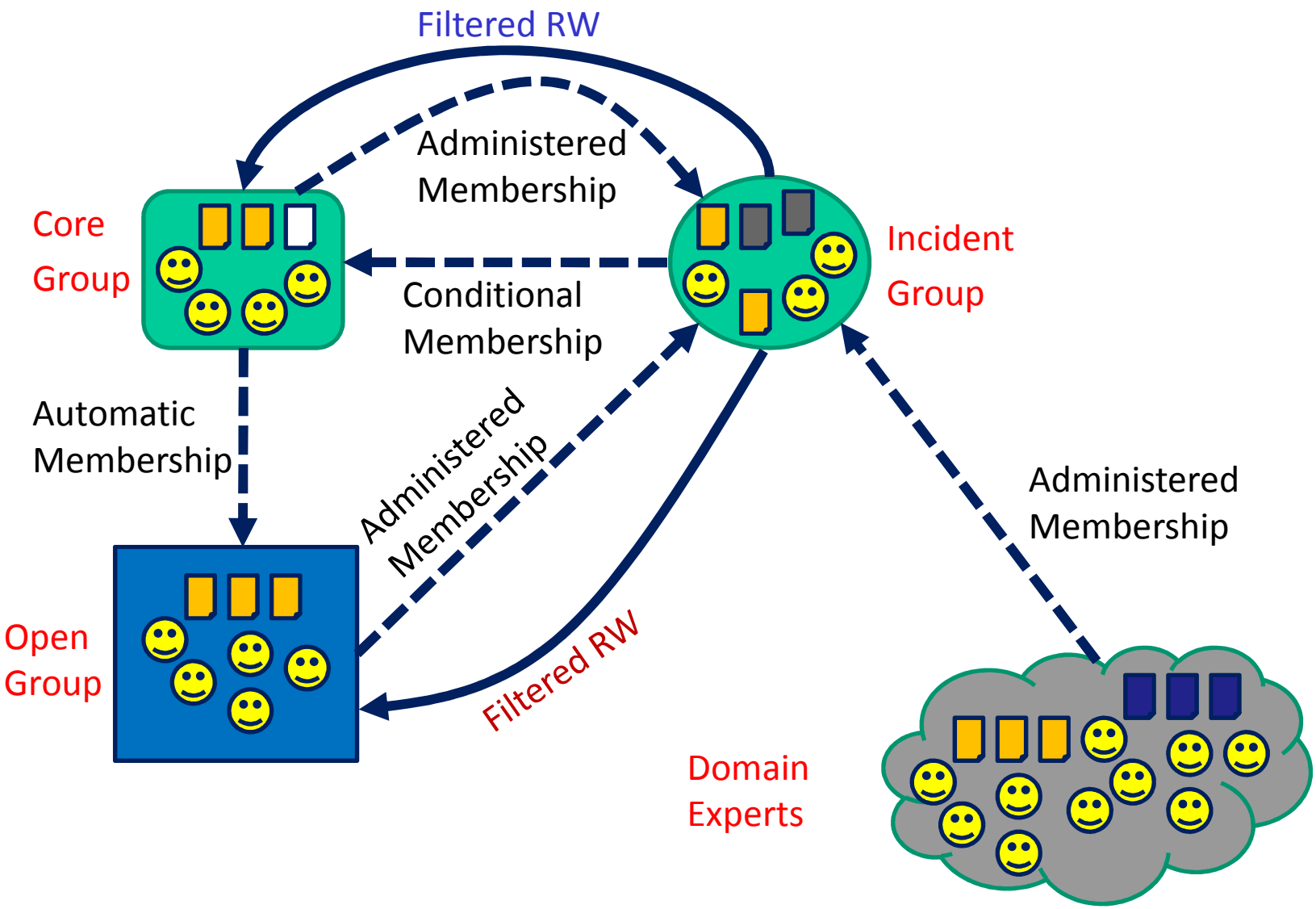
Goal: Share but protect

- Containment challenge
  - Client containment
    - Ultimate assurance infeasible (e.g., the analog hole)
    - Appropriate assurance achievable
  - Server containment
    - Will typically have higher assurance than client containment
- Policy challenge
  - How to construct meaningful, usable, agile SIS policy
  - How to develop an intertwined information and security model

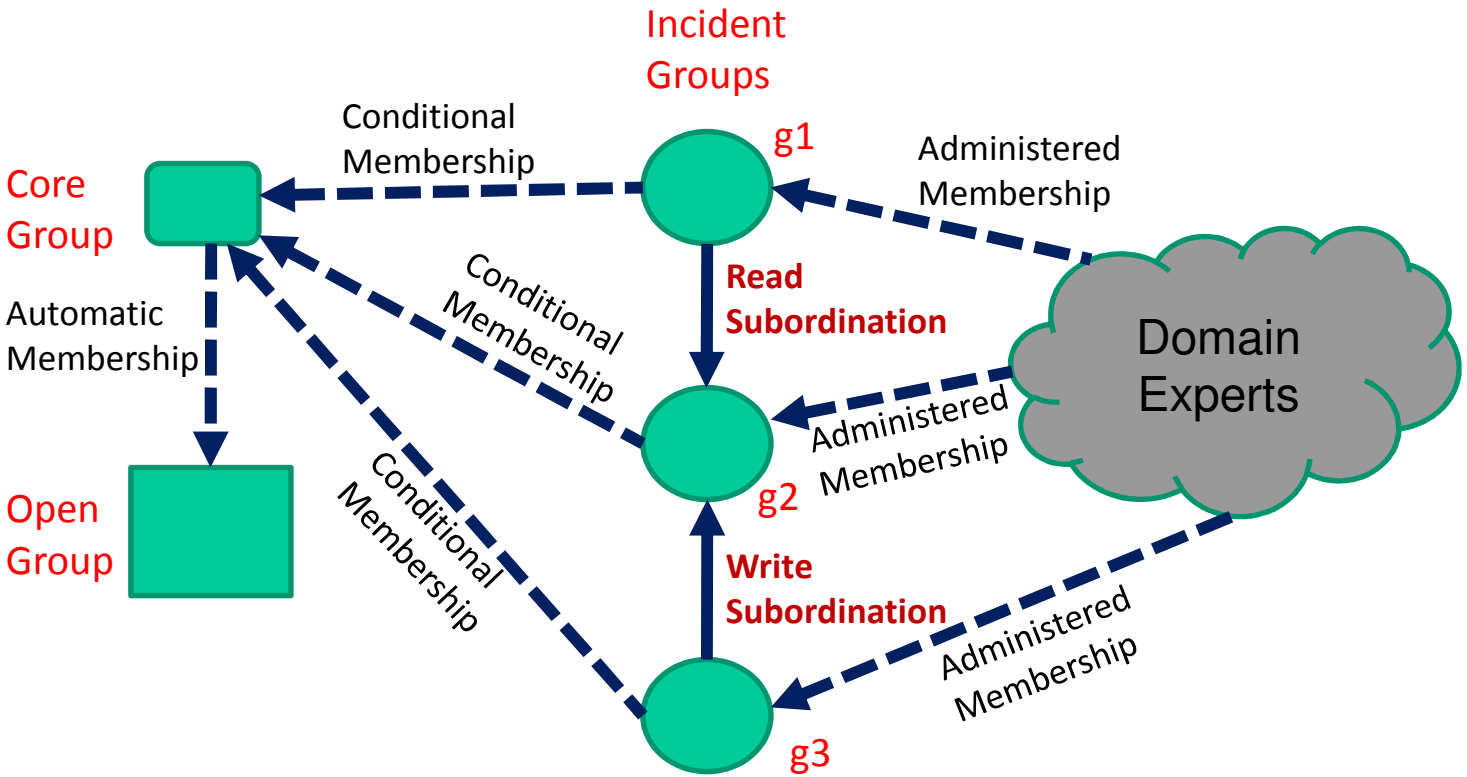
SIS Policy Construction

- Dissemination Centric (d-SIS)
  - Sticky policies that follow an object along a dissemination chain (possibly modified at each step)
- Group Centric (g-SIS)
  - Bring users and information together to share existing information and create new information
  - Metaphors: Secure meeting room, Subscription service
  - Benefits: analogous to RBAC over DAC

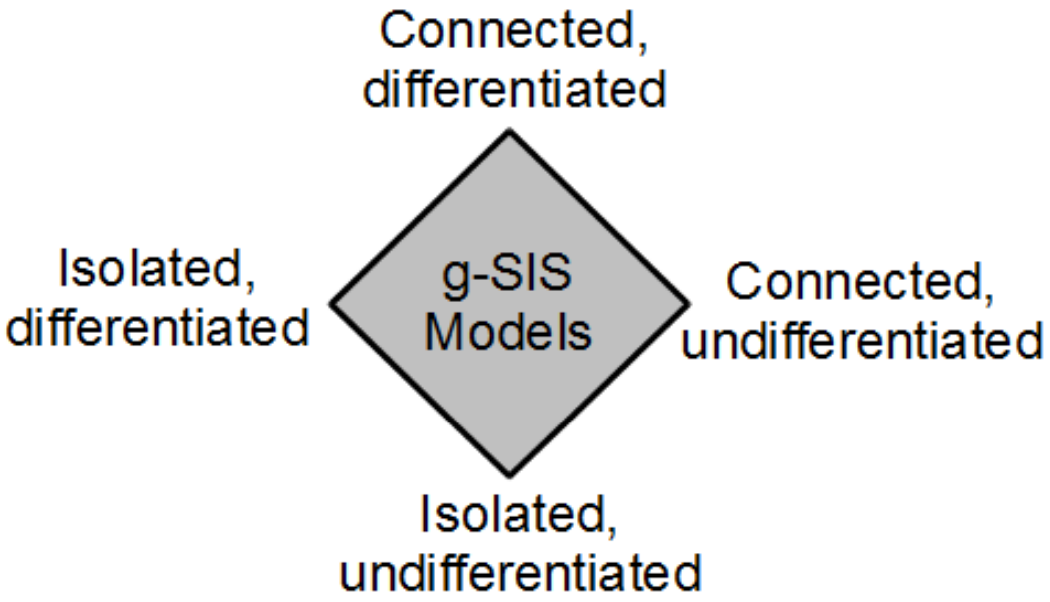
Community Cyber Security



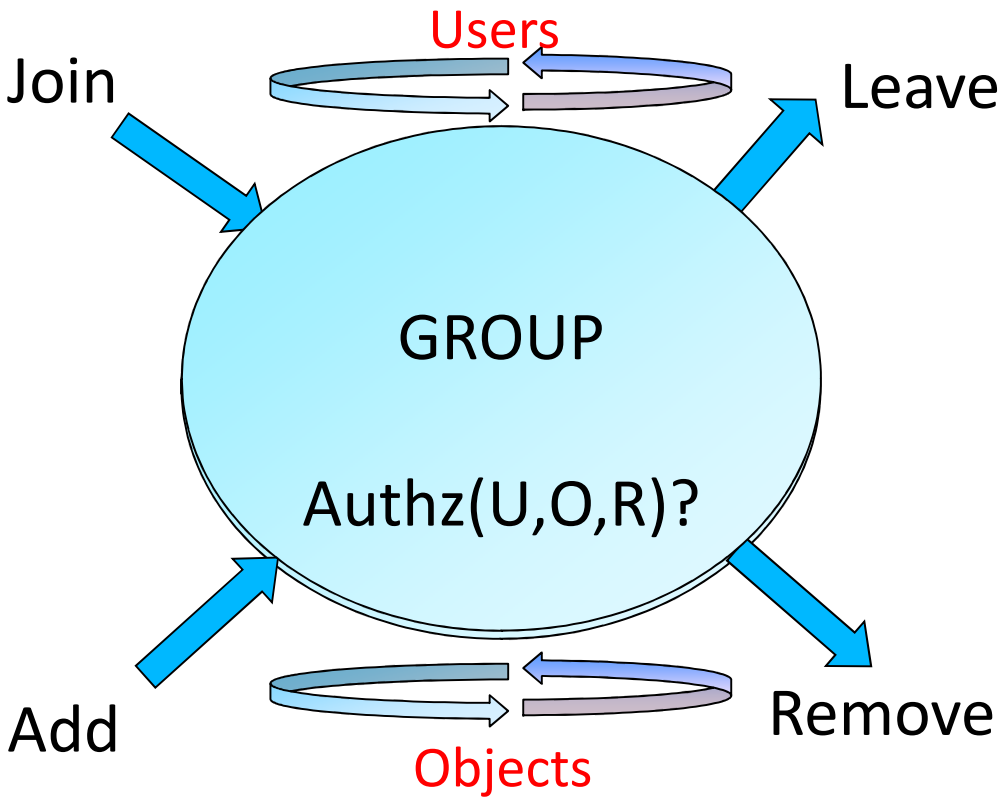
Community Cyber Security



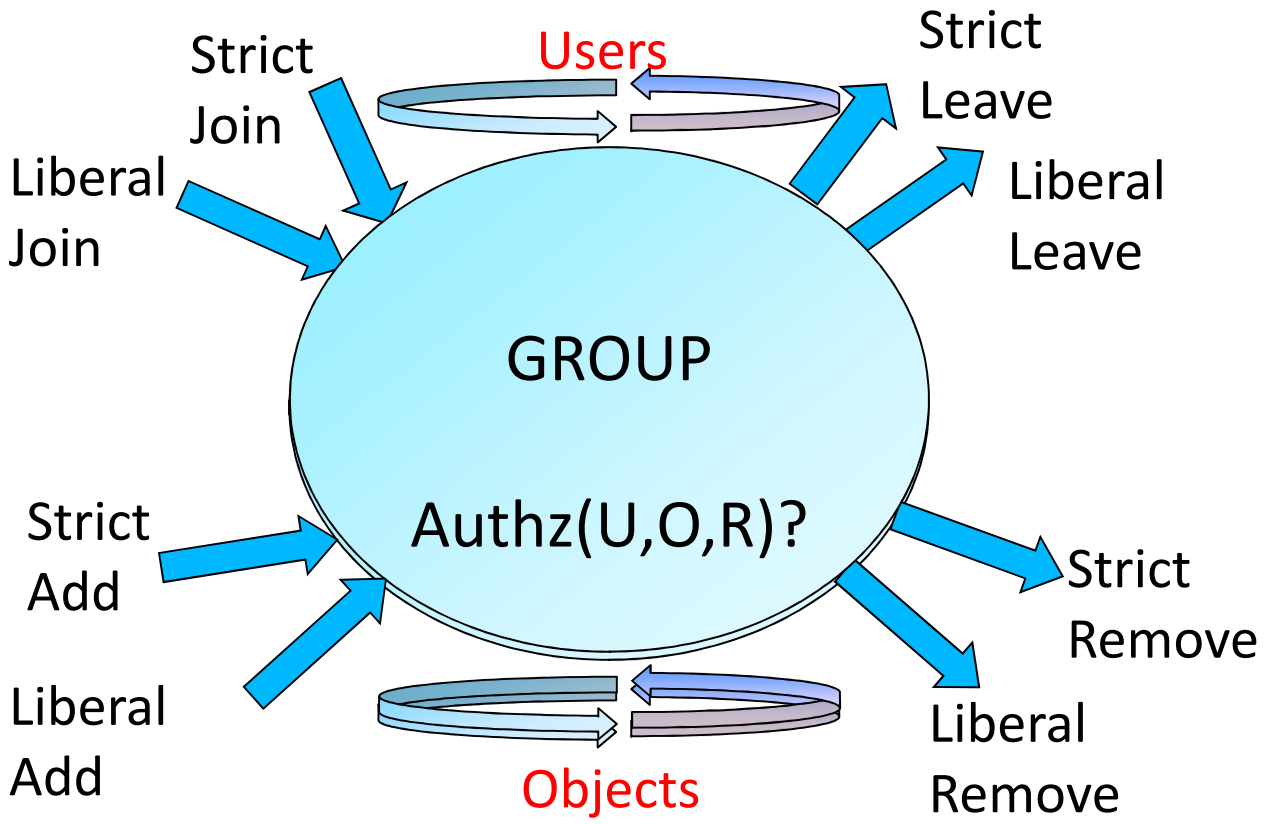
A Family of g-SIS Models



Isolated, Undifferentiated g-SIS Models

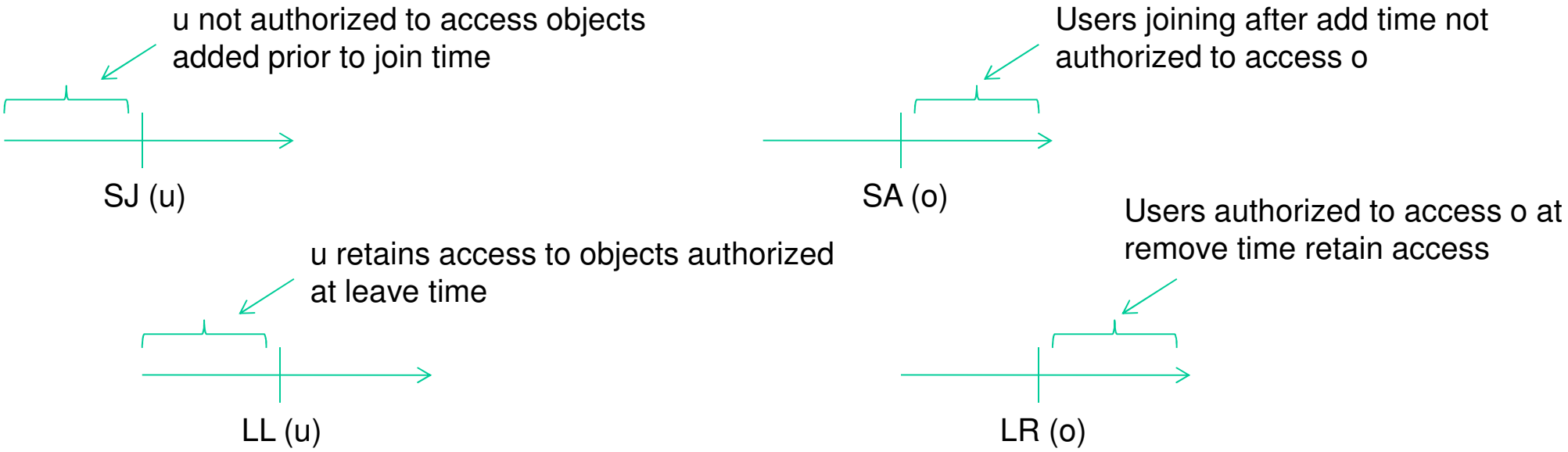


Isolated, Undifferentiated g-SIS Models



Group Operation Semantics

- Strict Vs Liberal operations
  - User operations (SJ, LJ, SL, LL)
  - Object operations (SA, LA, SR, LR)



The π-System g-SIS Specification

π-system g-SIS Specification:

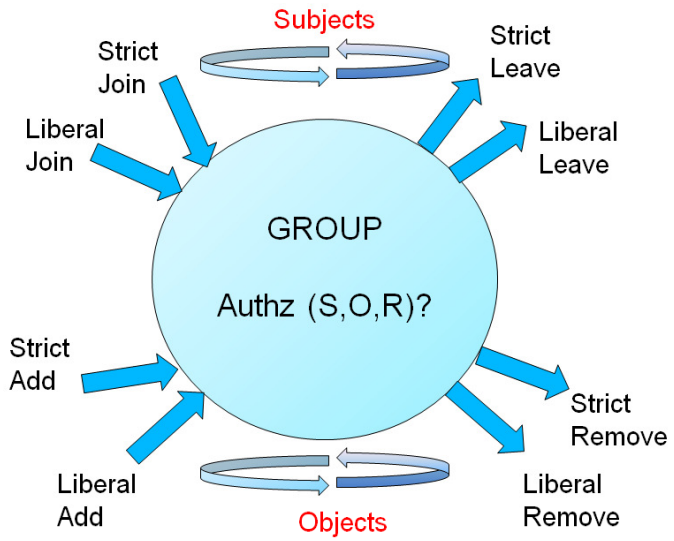
$$\pi = \Box(\text{Authz} \leftrightarrow \lambda_1 \vee \lambda_2) \wedge \bigwedge_{0 \leq j \leq 3} \tau_j$$

$$\lambda_1 = ((\neg \text{SL} \wedge \neg \text{SR})\ \mathcal{S}\ ((\text{SA} \vee \text{LA}) \wedge ((\neg \text{LL} \wedge \neg \text{SL})\ \mathcal{S}\ (\text{SJ} \vee \text{LJ}))))$$

Add after Join

$$\lambda_2 = ((\neg \text{SL} \wedge \neg \text{SR})\ \mathcal{S}\ (\text{LJ} \wedge ((\neg \text{SR} \wedge \neg \text{LR})\ \mathcal{S}\ \text{LA})))$$

Add before Join



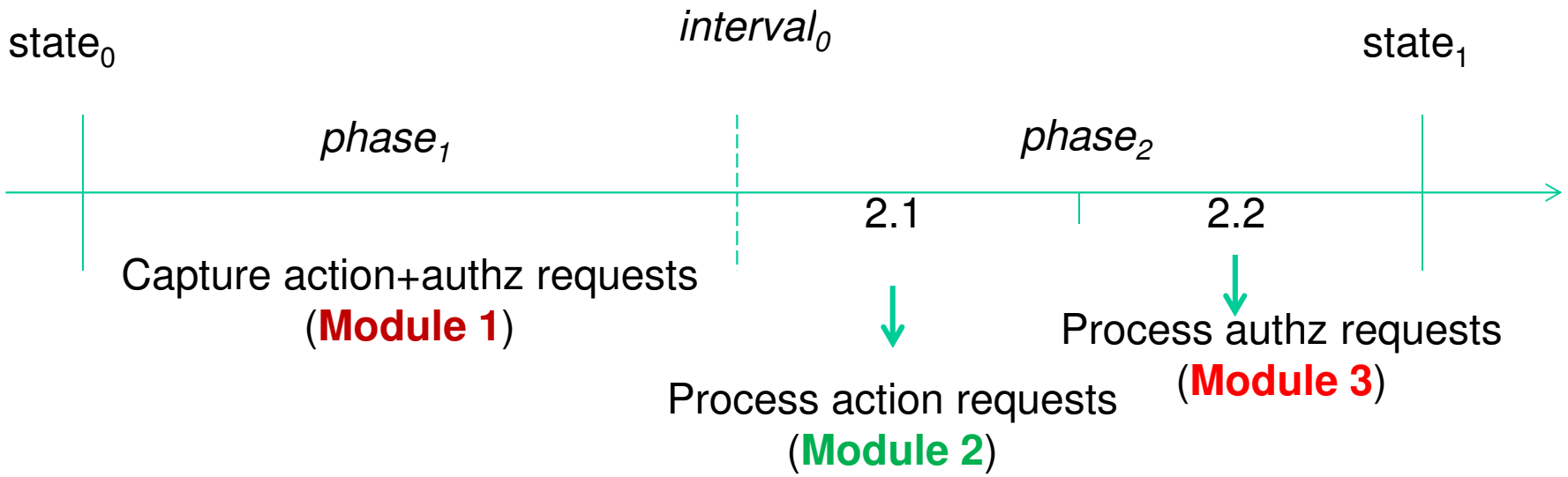
Well-formedness constraints rule out invalid traces

Examples:

1. user joining and leaving in the same state
2. leaving before joining

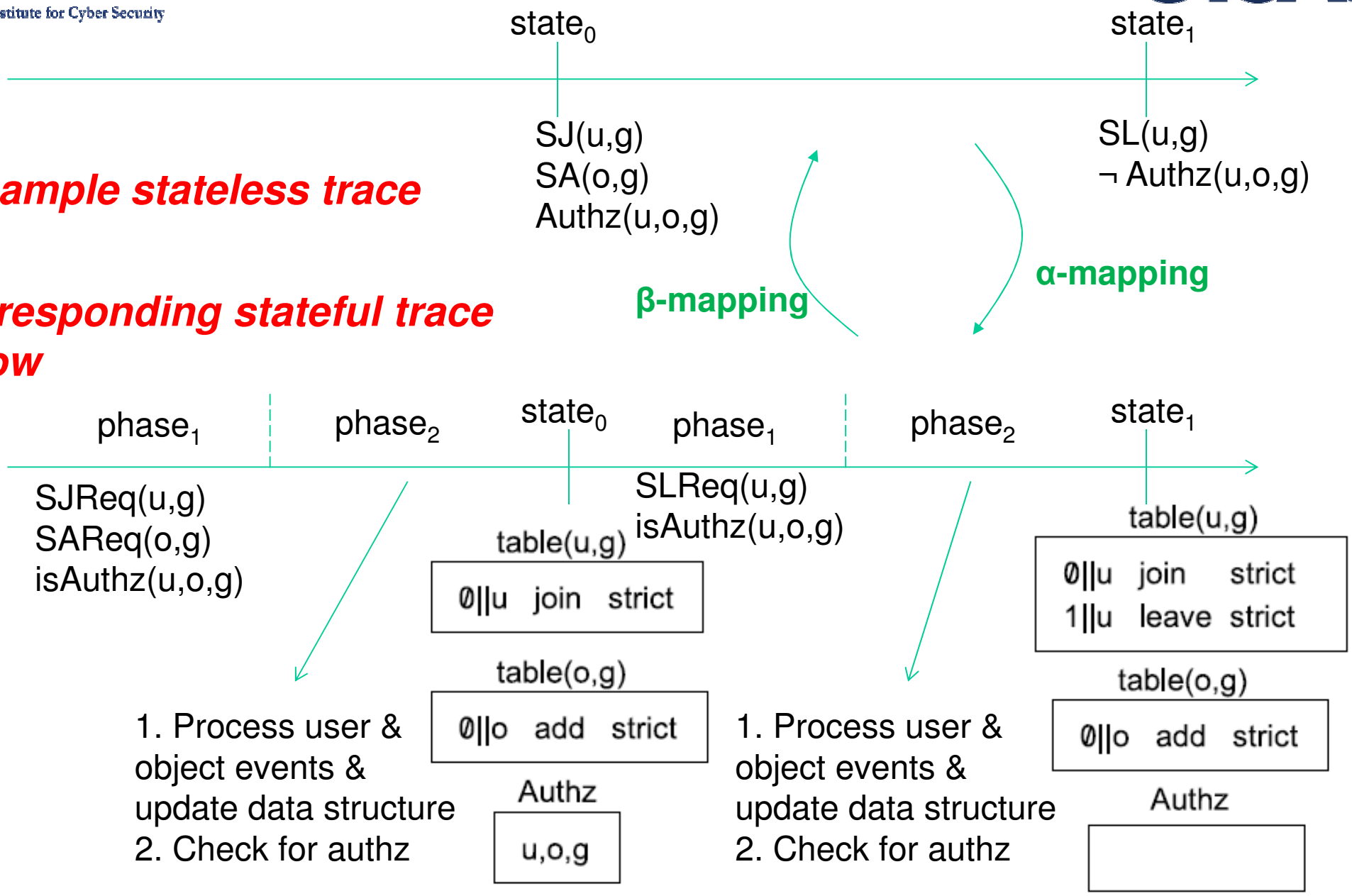
Stateful Specification

- Consists of three modules

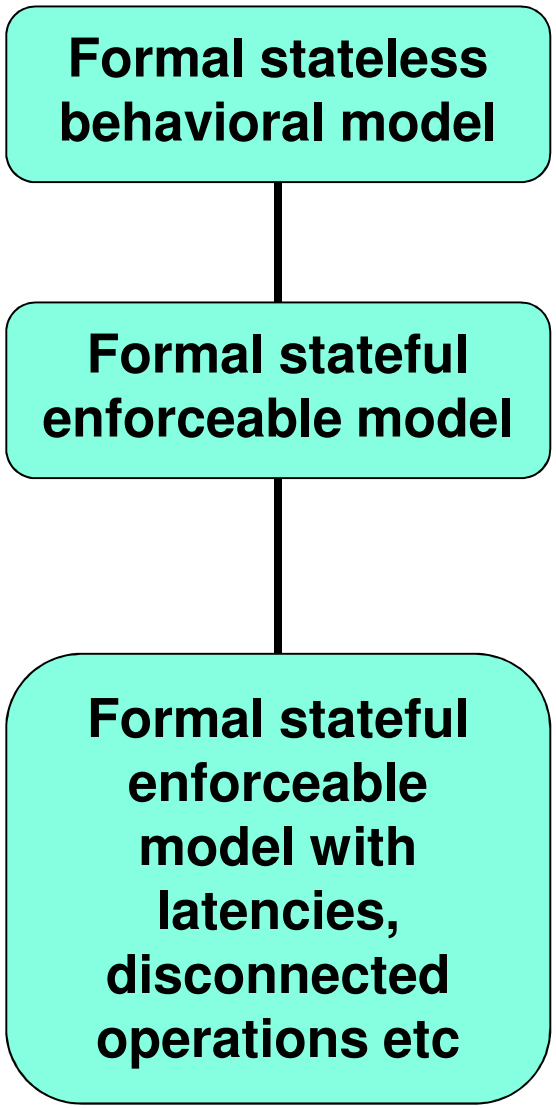


- Module 2 maintains and manages data structures
  - Keeps track of historical joins and leaves and adds and removes for users and objects
- Module 3 consults with that data structure

Stateless and Stateful Equivalence



Formal Models Development



Provable security properties

Proof of equivalence

Proof of safe equivalence

Why not ABAC (Attribute-Based Access Control)?