# ICS Research Projects

Ravi Sandhu
Institute for Cyber Security
University of Texas at San Antonio

August 30, 2012
IIIT Delhi

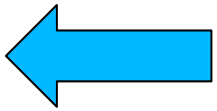
# ICS Philosophy

- Foundations
- Applications
- Technologies

# ICS Projects

- Secure information sharing
- Social network security
- Secure data provenance
- Attribute based access control
- Botnet and malware analysis
- Smart grid security
- Hardware security
- Future internet

# ICS Projects

- Secure information sharing 
- Social network security
- Secure data provenance
- Attribute based access control
- Botnet and malware analysis
- Smart grid security
- Hardware security
- Future internet

# 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

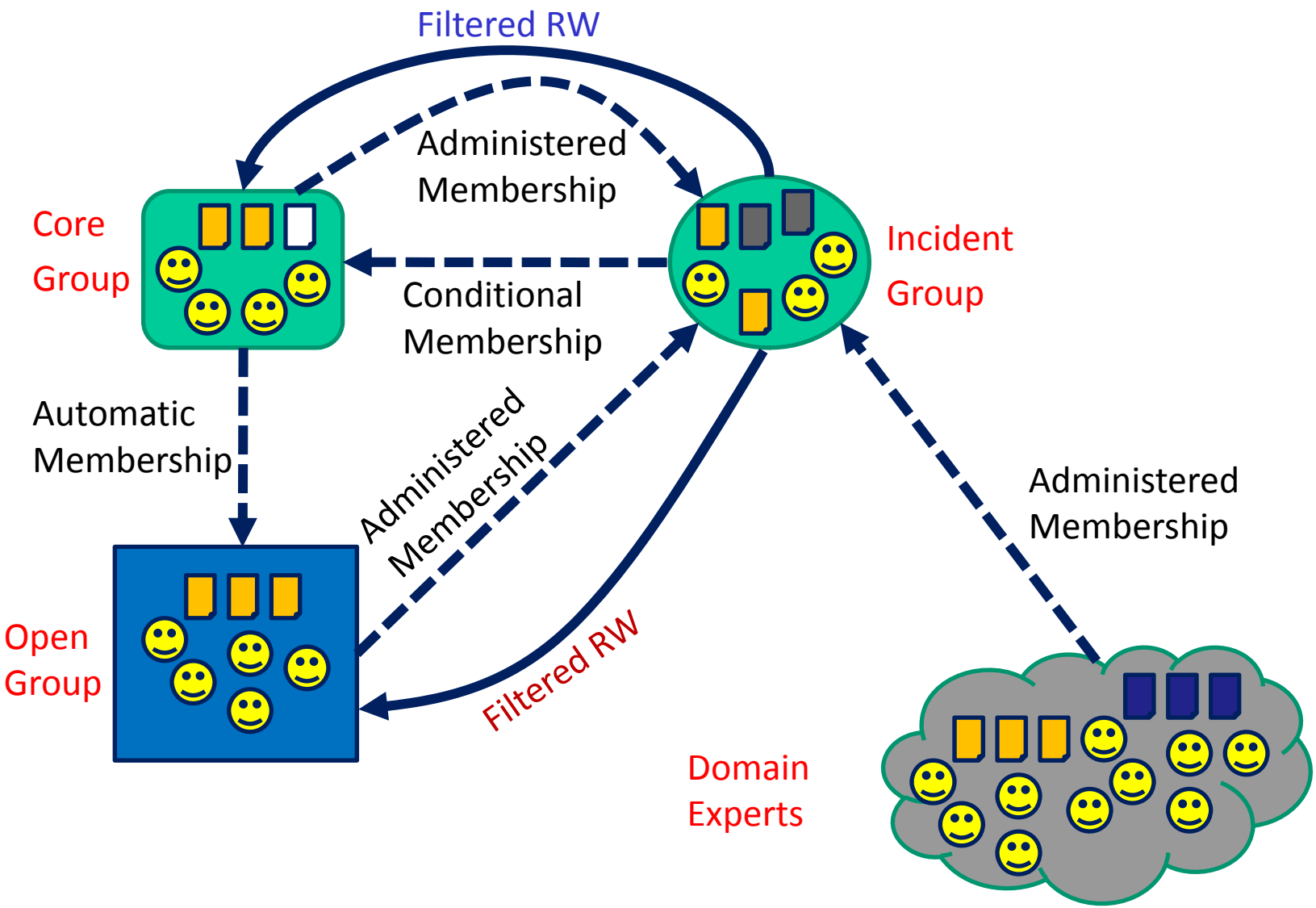
# SIS Policy Construction



- 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

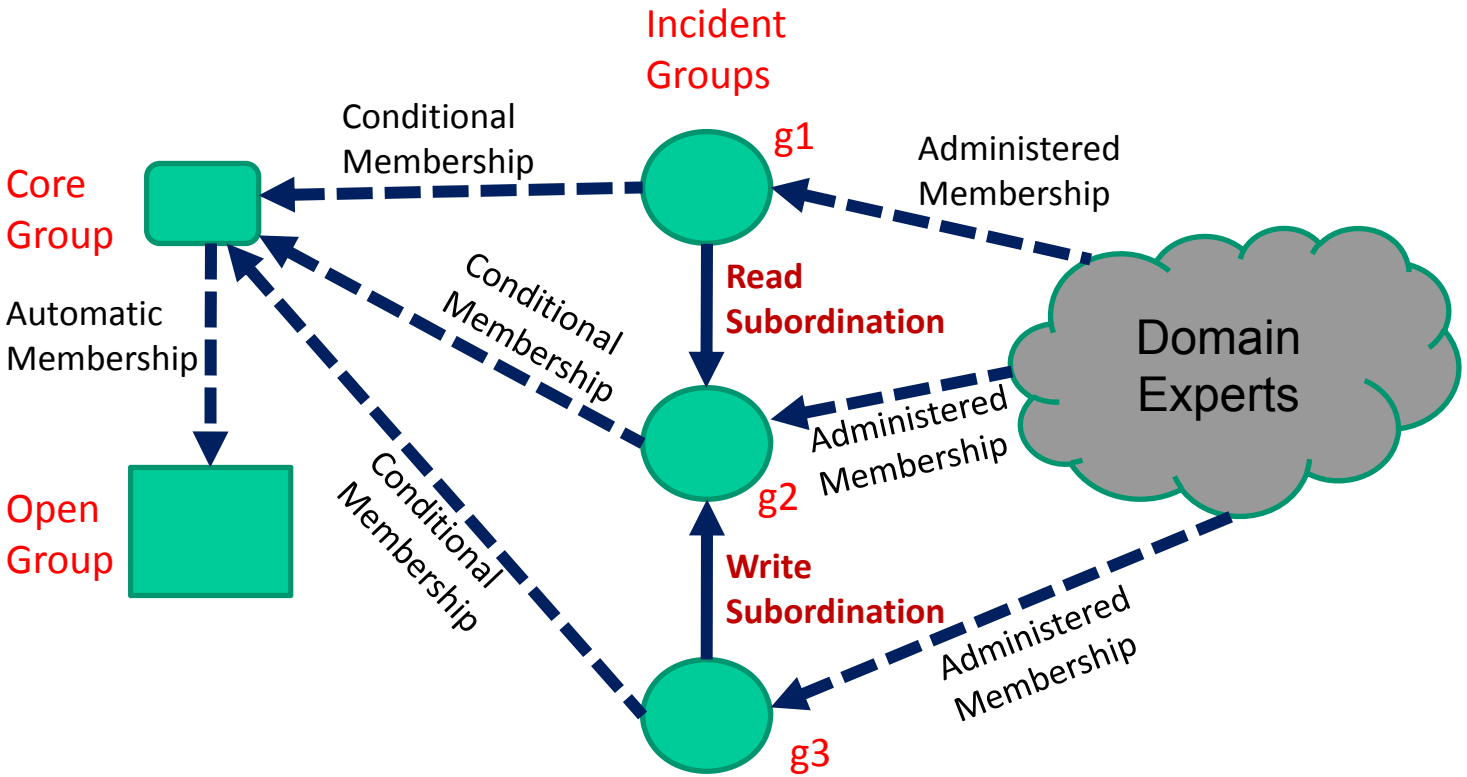
# Community Cyber Security



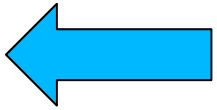


# Community Cyber Security





# ICS Projects

- Secure information sharing
- Social network security 
- Secure data provenance
- Attribute based access control
- Botnet and malware analysis
- Smart grid security
- Hardware security
- Future internet

# Relationship-based Access Control



- Users in Online Social Networks (OSNs) are connected with social relationships
- Owner of the resource can control its release based on such relationships between the access requester and the owner

# Solution Approach



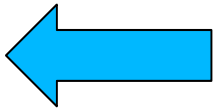
- Using regular expression-based path pattern for arbitrary combination of relationship types
- Given relationship path pattern and hopcount limit, graph traversal algorithm checks the social graph to determine access

# Related Works

| | Fong [7] | Fong [8, 9] | Carminati [6] | Carminati [2, 3] | UURAC |
|---|---|---|---|---|---|
| **Relationship Category** | | | | | |
| Multiple Relationship Types | | ✓ | ✓ | ✓ | ✓ |
| Directional Relationship | | ✓ | ✓ | | ✓ |
| U2U Relationship | ✓ | ✓ | ✓ | ✓ | ✓ |
| U2R Relationship | | | | ✓ | |
| **Model Characteristics** | | | | | |
| Policy Individualization | ✓ | ✓ | ✓ | ✓ | ✓ |
| User & Resource as a Target | | | | (partial) | ✓ |
| Outgoing/Incoming Action Policy | | | | (partial) | ✓ |
| **Relationship Composition** | | | | | |
| Relationship Depth | 0 to 2 | 0 to n | 1 to n | 1 to n | 0 to n |
| Relationship Composition | f, f of f | exact type sequence | path of same type | exact type sequence | path pattern of different types |

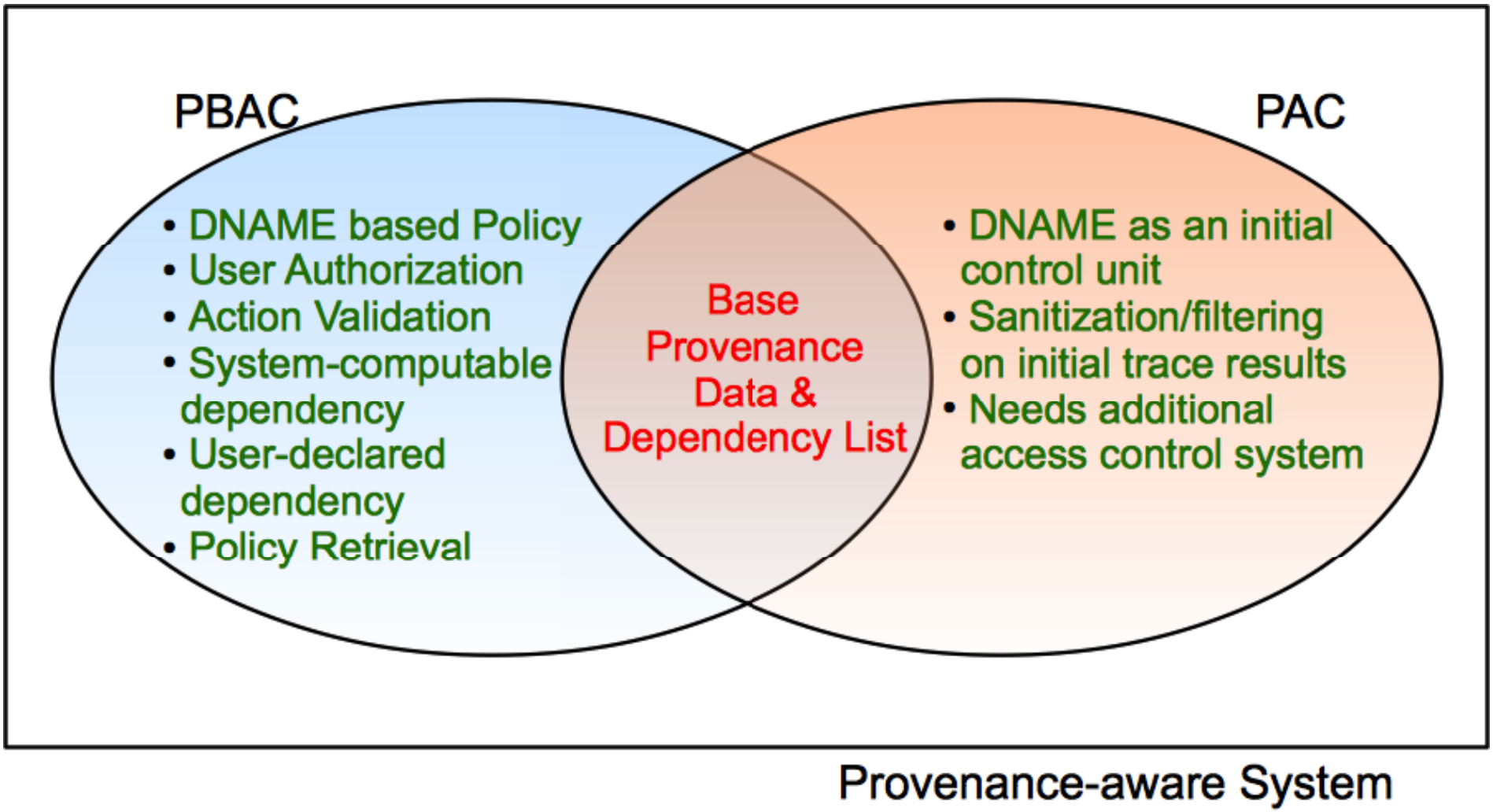
- The advantages of this approach:
  - Passive form of action allows outgoing and incoming action policy
  - Path pattern of different relationship types make policy specification more expressive

# ICS Projects

- Secure information sharing
- Social network security
- Secure data provenance 
- Attribute based access control
- Botnet and malware analysis
- Smart grid security
- Hardware security
- Future internet

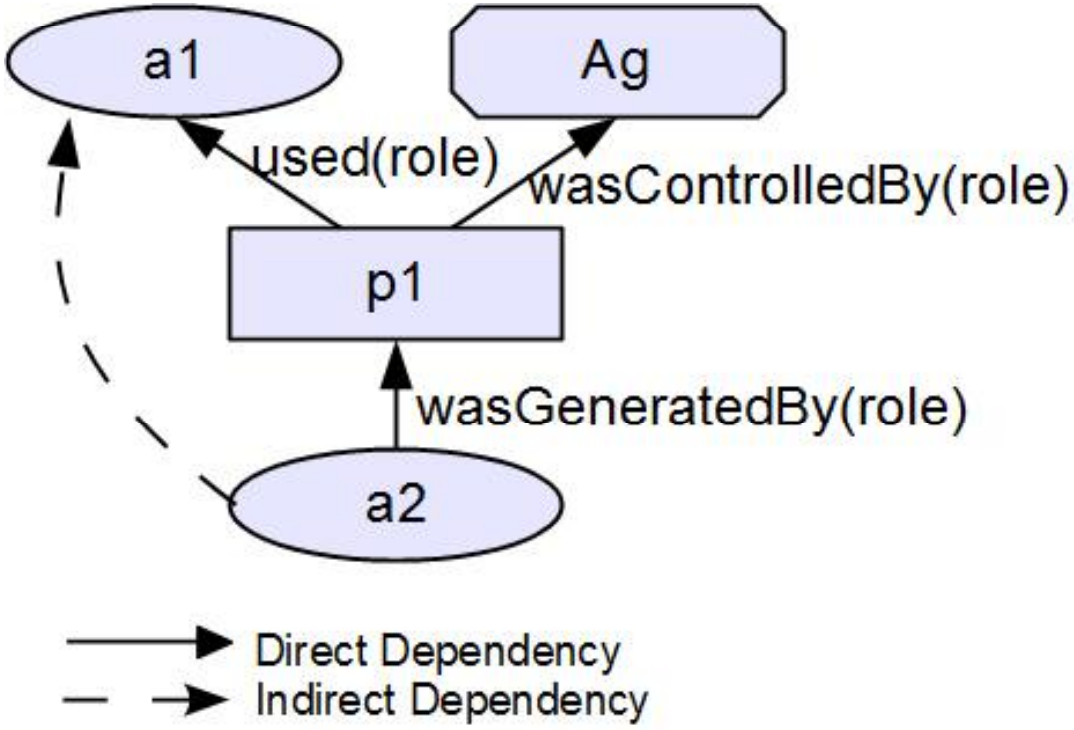
# Provenance Based Access Control (PBAC) vs Provenance Access Control (PAC)





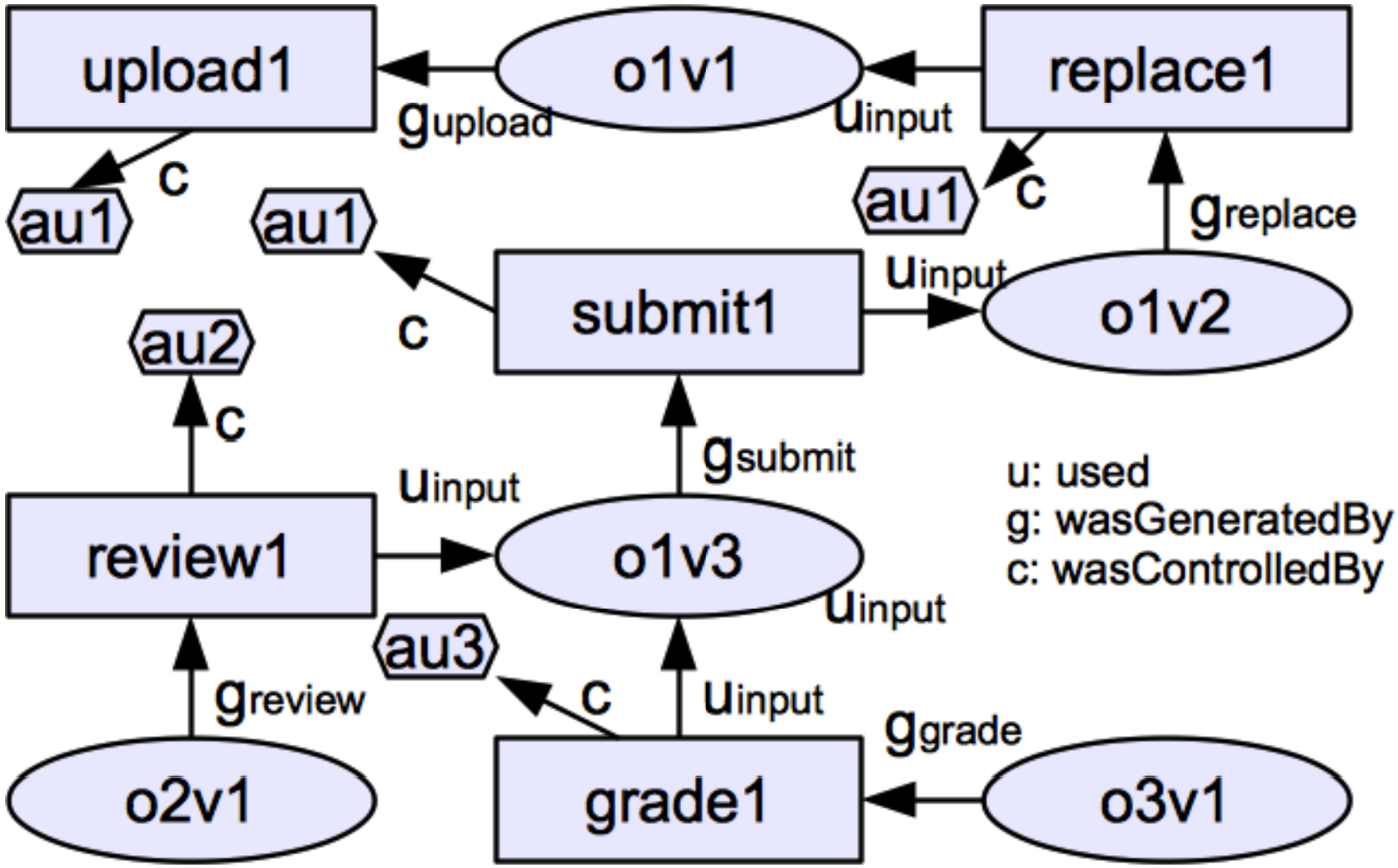
# OPEN PROVENANCE MODEL (OPM)



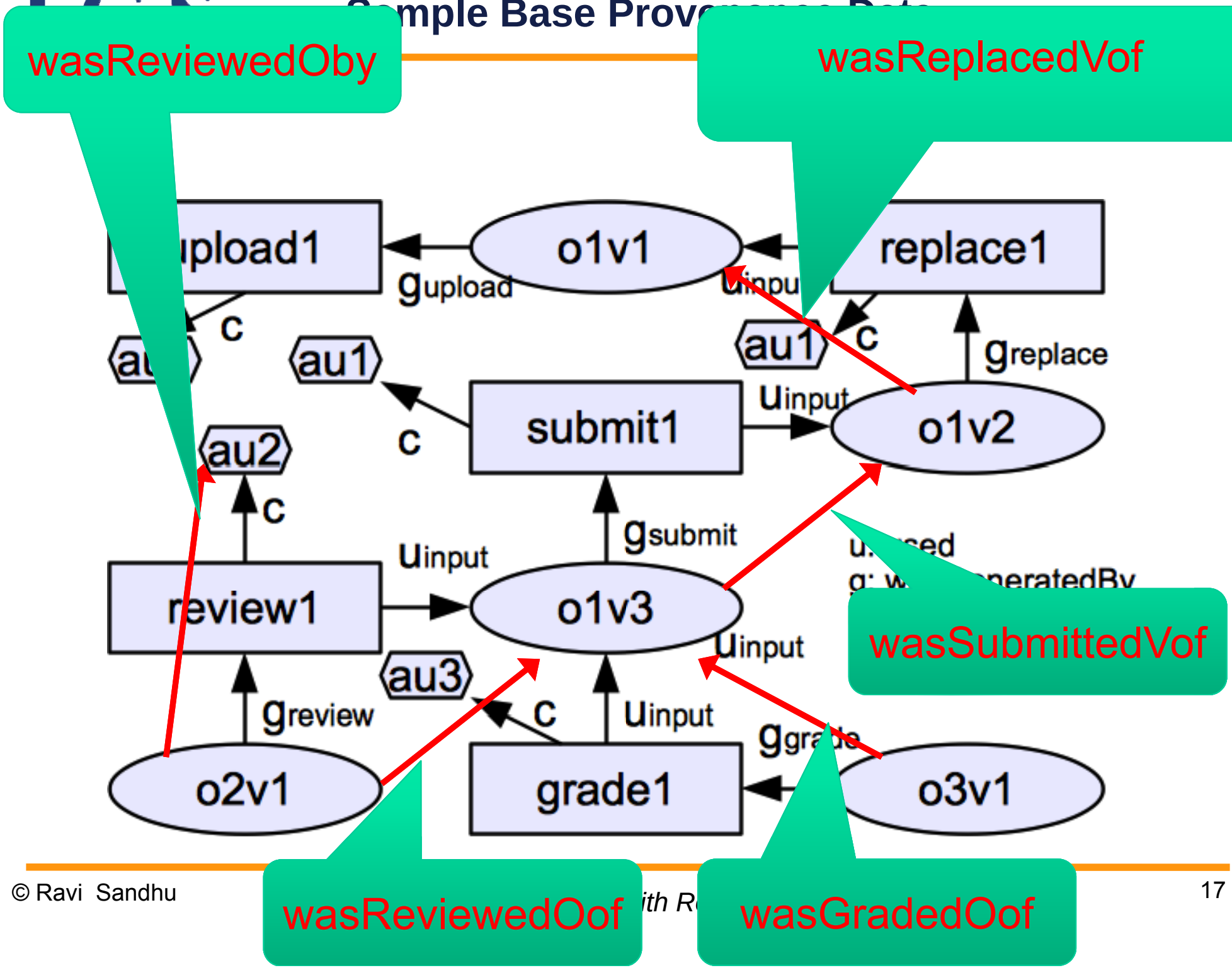


# Sample Base Provenance Data

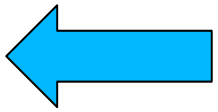




## Sample Base Prov



# ICS Projects

- Secure information sharing
- Social network security
- Secure data provenance
- Attribute based access control 
- Botnet and malware analysis
- Smart grid security
- Hardware security
- Future internet

# Access Control Models

- Discretionary Access Control (DAC), 1970
  - Owner controls access
  - But only to the original, not to copies
  - Grounded in pre-computer policies of researchers
- Mandatory Access Control (MAC), 1970
  - Synonymous to Lattice-Based Access Control (LBAC)
  - Access based on security labels
  - Labels propagate to copies
  - Grounded in pre-computer military and national security policies
- Role-Based Access Control (RBAC), 1995
  - Access based on roles
  - Can be configured to do DAC or MAC
  - Grounded in pre-computer enterprise policies

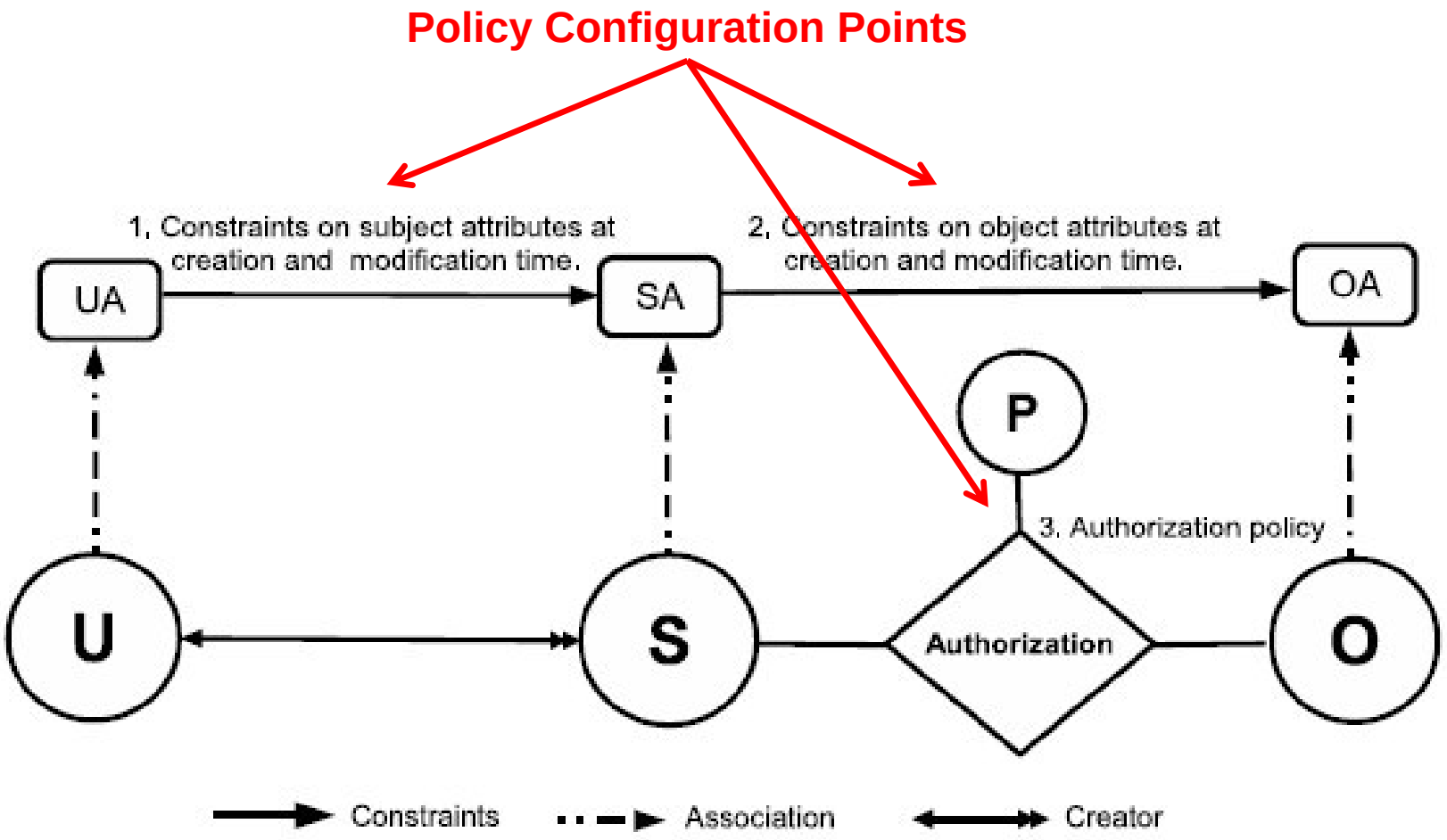
**Numerous other models but only 3 successes: SO FAR**

# RBAC Shortcomings



- Role granularity is not adequate leading to role explosion
  - Researchers have suggested several extensions such as parameterized privileges, role templates, parameterized roles (1997-)
- Role design and engineering is difficult and expensive
  - Substantial research on role engineering top down or bottom up (1996-), and on role mining (2003-)
- Assignment of users/permissions to roles is cumbersome
  - Researchers have investigated decentralized administration (1997-), attribute-based implicit user-role assignment (2002-), role-delegation (2000-), role-based trust management (2003-), attribute-based implicit permission-role assignment (2012-)
- Adjustment based on local/global situational factors is difficult
  - Temporal (2001-) and spatial (2005-) extensions to RBAC proposed
- RBAC does not offer an extension framework
  - Every shortcoming seems to need a custom extension
  - Can ABAC unify these extensions in a common open-ended framework?

# ABACα Model Structure



# ICS Projects

- Secure information sharing
- Social network security
- Secure data provenance
- Attribute based access control
- Botnet and malware analysis
- Smart grid security
- Hardware security
- Future internet