Security, Privacy and Interoperability in Heterogeneous Systems

Jian Zhong, Peter Bertok, Zahir Tari
Scool of Computer Science and Information Technology, RMIT University
Melbourne, Australia

Presentation Outline

- Objectives
- Limitations of role-based access control
- Proposed model
  - Components
  - Basic mechanisms
- Conclusion

Objectives

- User (subject) access to objects in local and remote domains
- Control secondary data usage
  - Passing on legally obtained data to others
- Manageable system complexity

Role-Based Access Control (RBAC)

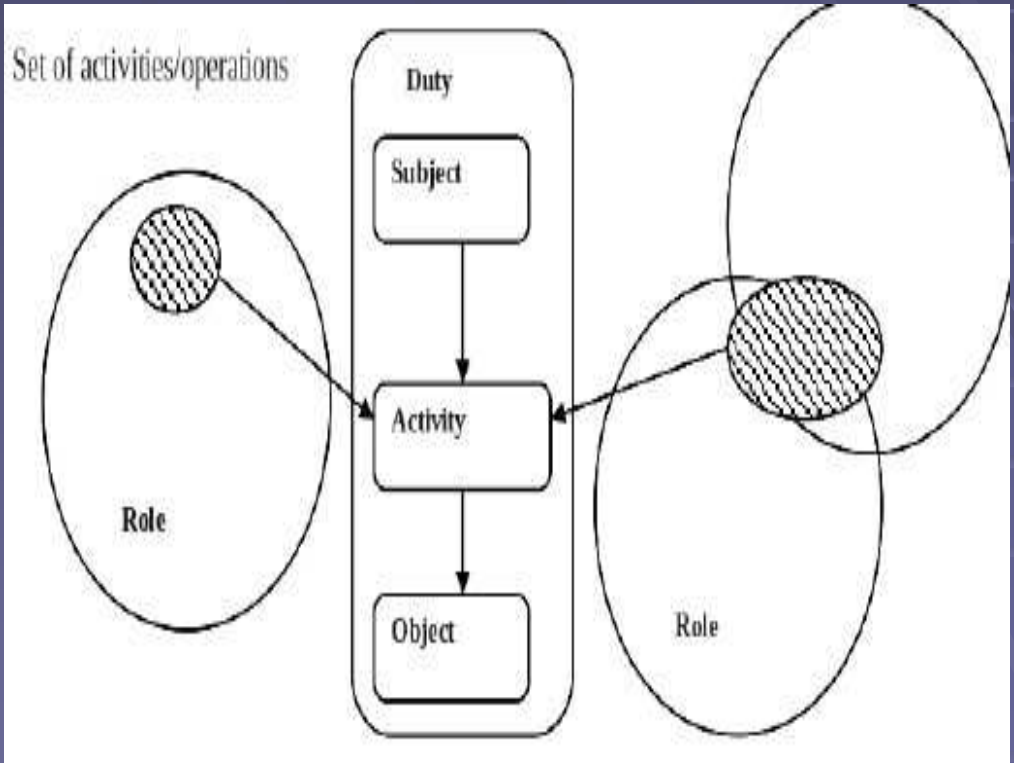
- Suitable for
  - Large systems with many similar users
- Issues
  - Many unique users with diverse privileges require many roles
  - Cross-domain mapping of roles
- Solution
  - Privileges assigned on a per-request basis

Proposed Approach Process Steps

- User privileges are calculated for an access request
  - A subject (user) may have several possible roles, an actual operation may require only some of the privileges of those roles
- Document's access control list (ACL) is evaluated
  - Data may have different ACLs for different components (granular data)
- Authorisation
  - Matching user privileges and ACLs

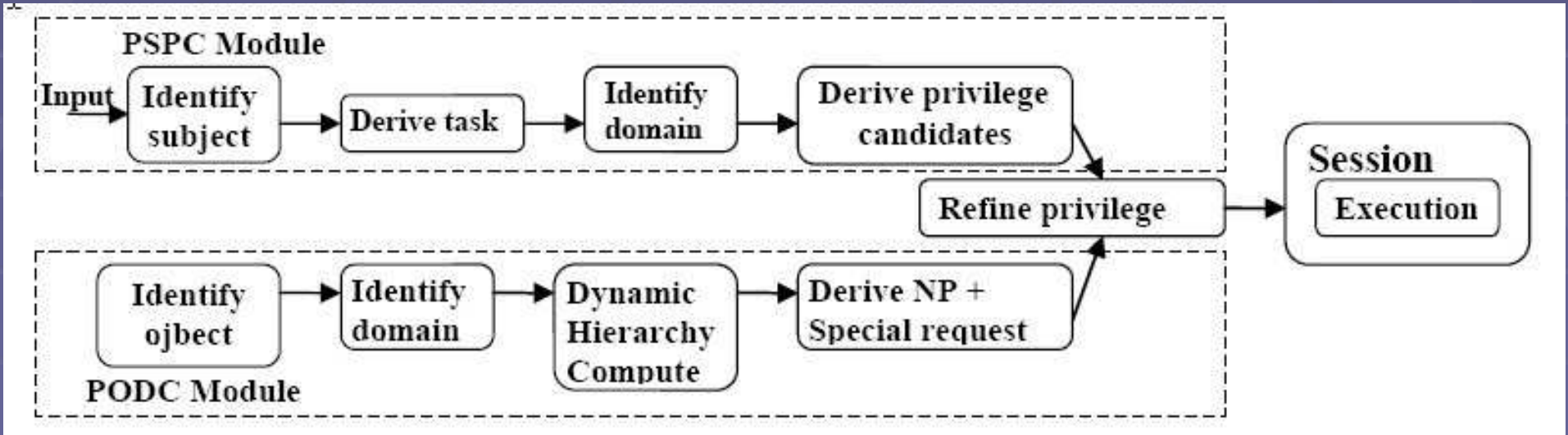
Components
Duties and Labels

- Duty
  - A collection of a subject's activities on an object
  - Can include parts of different roles
- Label
  - Describes the actual privileges of a subject
  - Only positive privileges are considered



Proposed Model

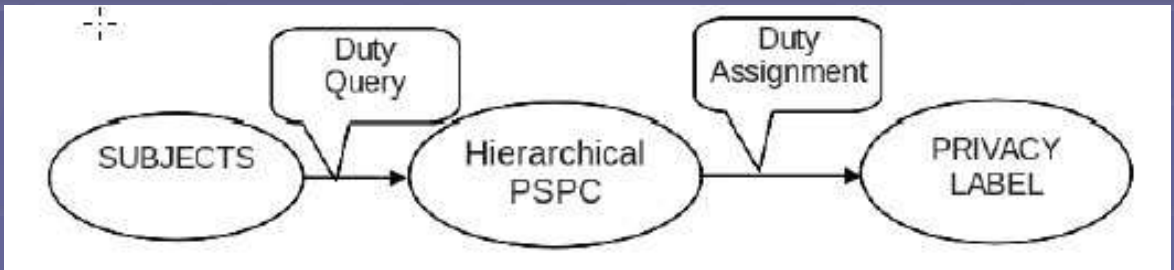
- Components
  - Granular subject privilege control (PSPC)
  - Label-based access control (PODC)
  - Collaboration module



Subject Privilege Control (PSPC)

- Subject lodges an activity request
- System checks if activity is allowed

  (Subject may or may not be allowed to perform certain tasks)
- A generated label describes the privileges associated with this duty

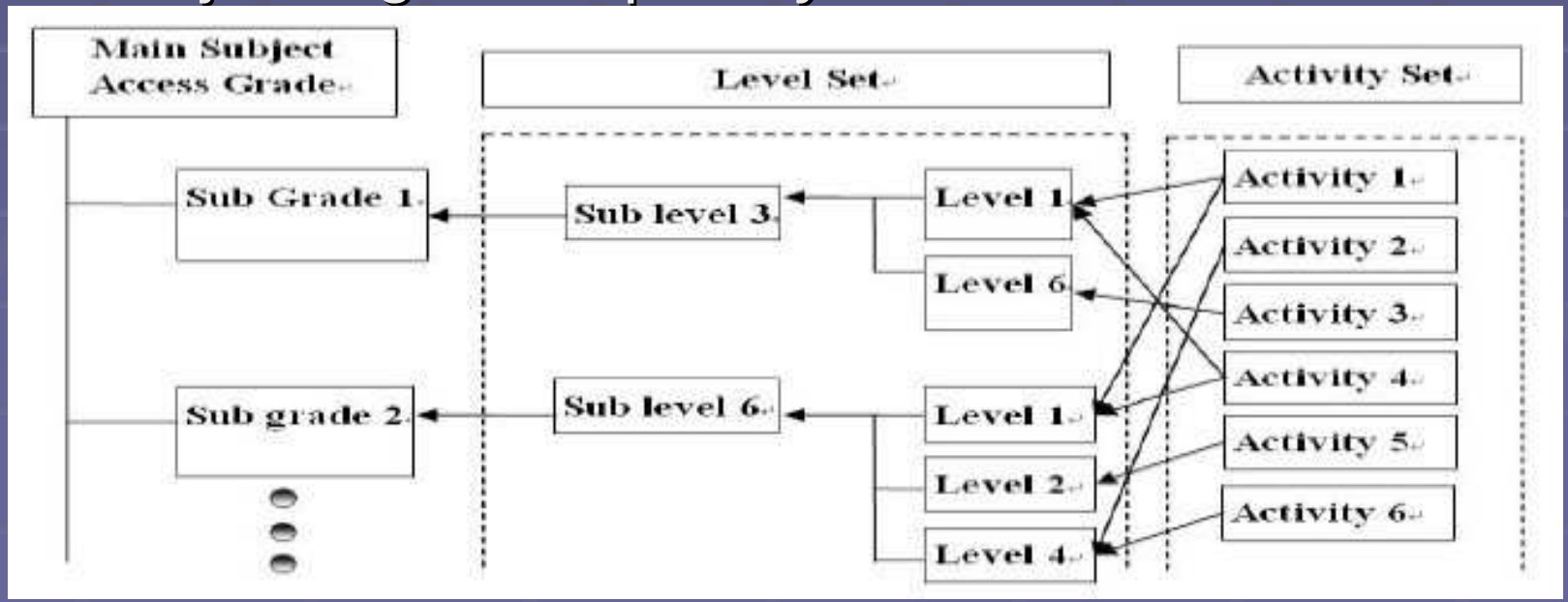


Activities and Privileges

- Hierarchy of activities
  - Subject activity level

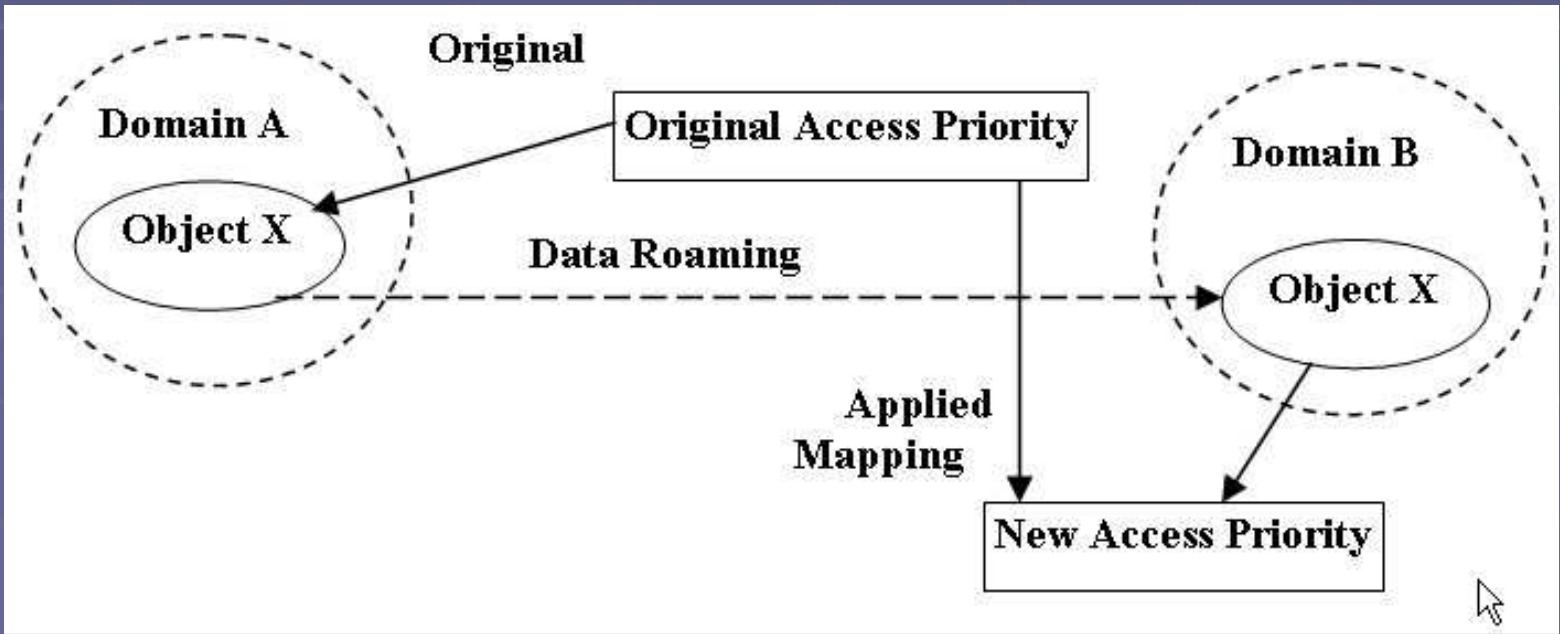
    Related to one activity only
  - Subject grade

    Subject's general priority



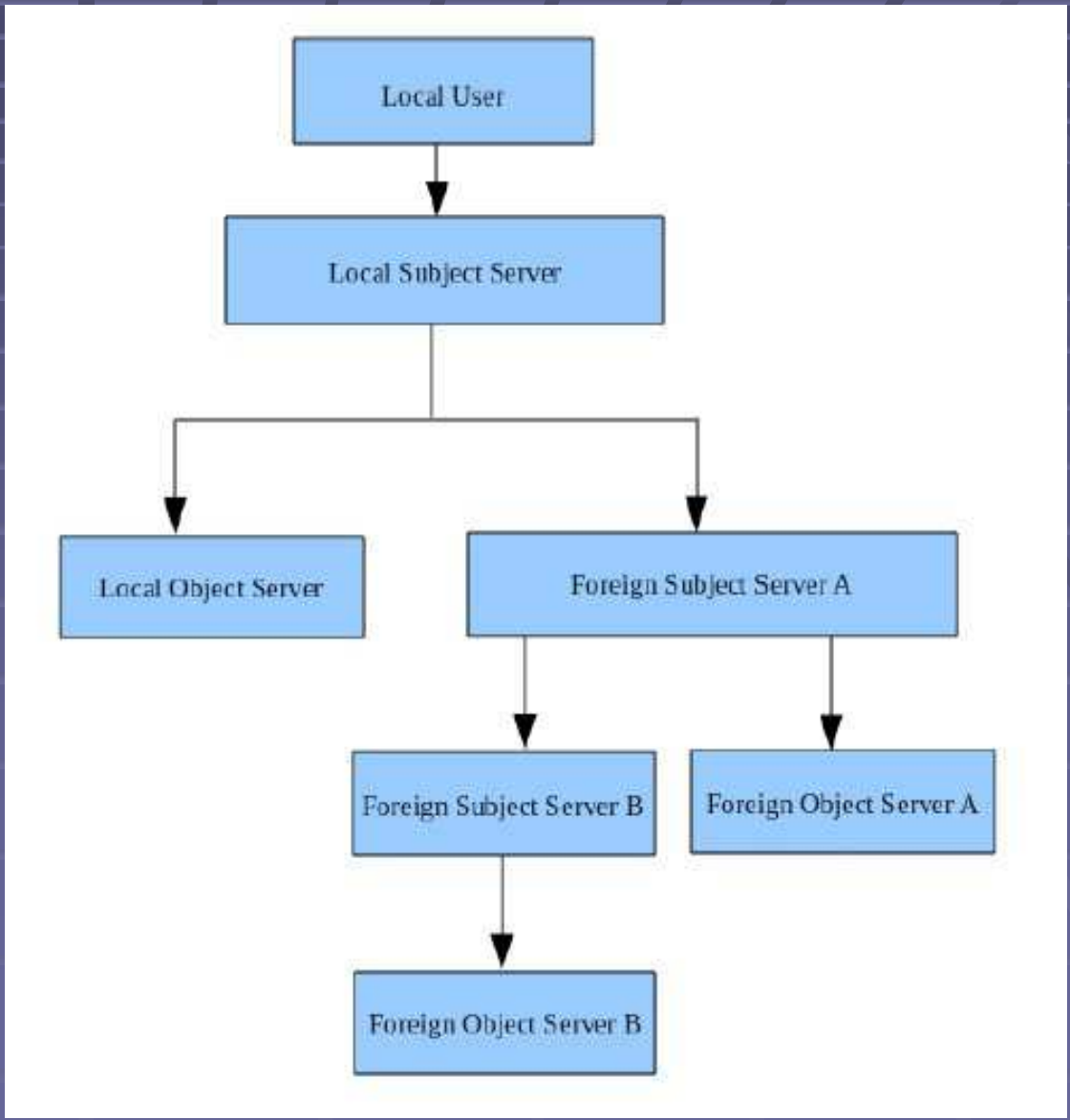
Roaming

- When accessing remote objects, the subject hierarchy at the remote location may be different
- The local access rights hierarchy is mapped into the remote one (via a mapping function)
- A label is produced for the mapped duty



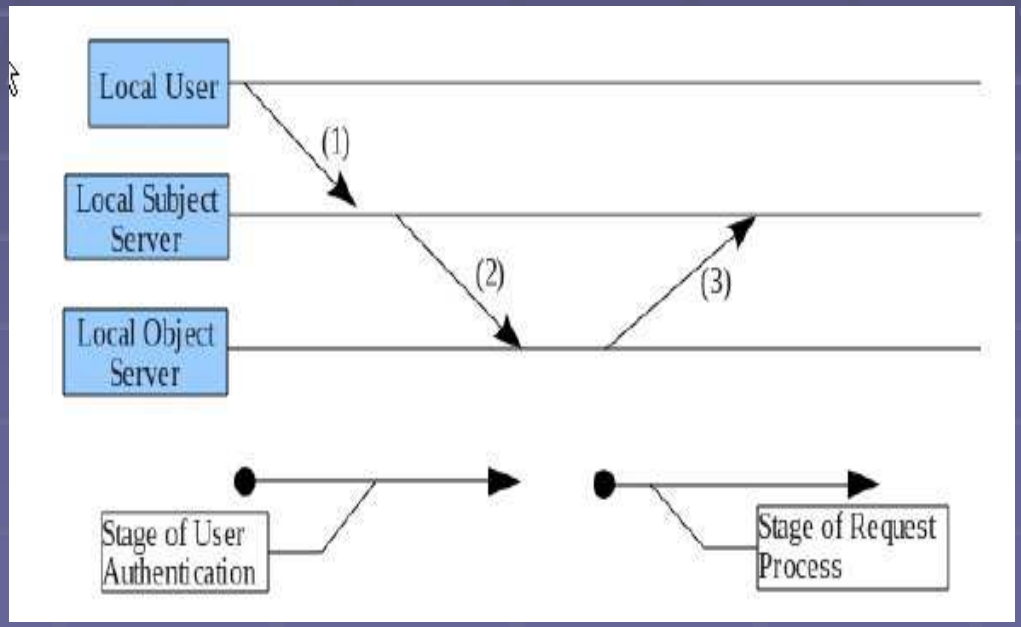
Accessing Local and Remote Objects

- Data is made available by the subject server
- When accessing an object, access rights are evaluated at the object's location
- The mapping function produces a label for a remote subject
- Cascaded mapping is possible



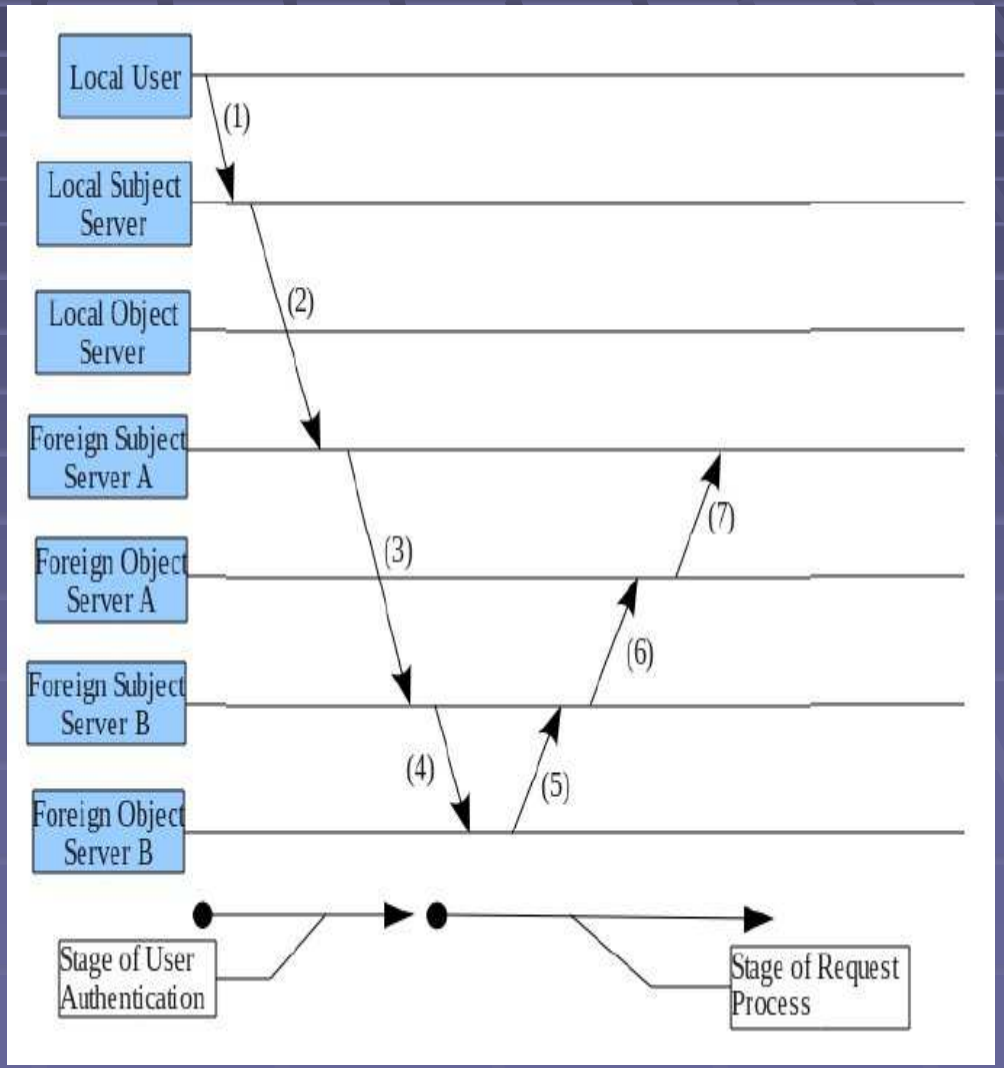
Local Access

- User acquires a privacy label from the subject server
- The object server matches the privacy label against the object's ACL, and grants (or denies) access



Remote Access

- Accessing data in a remote domain
  - Subject is mapped into the object's domain
- A subject accessing data while in a foreign domain (subject roaming)
  - Request is initiated from the home domain
  - Data is delivered to the current location of the subject



Conclusion

System features

- Data access in multiple domains
- Mapping subjects between different domains
- Labels carry access information (rights and privileges)