# Providing Fine Grained Access Control
# in
# CORBA Distributed Object System

Atul Kumar
Department of Computer Science & Engineering
Indian Institute of Technology Kanpur, INDIA

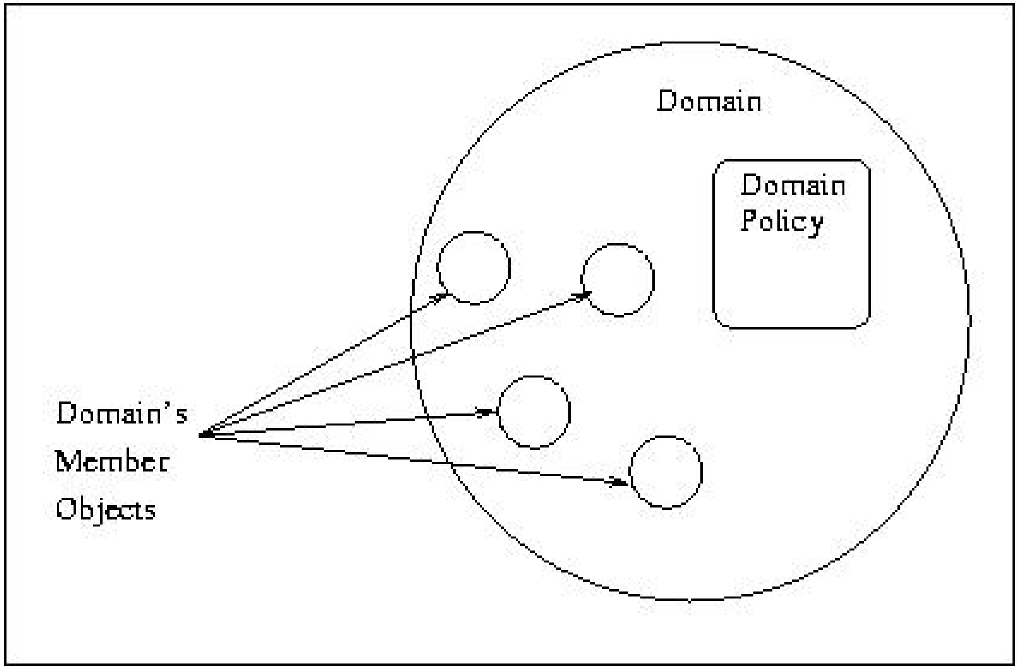
# Object Security

- Security
    - Confidentiality integrity, availability
    - Identification, authentication, access control
        - protected resources, policy
    - Audit, assurance
- Object Security Requirements
    - naming, scale, encapsulation

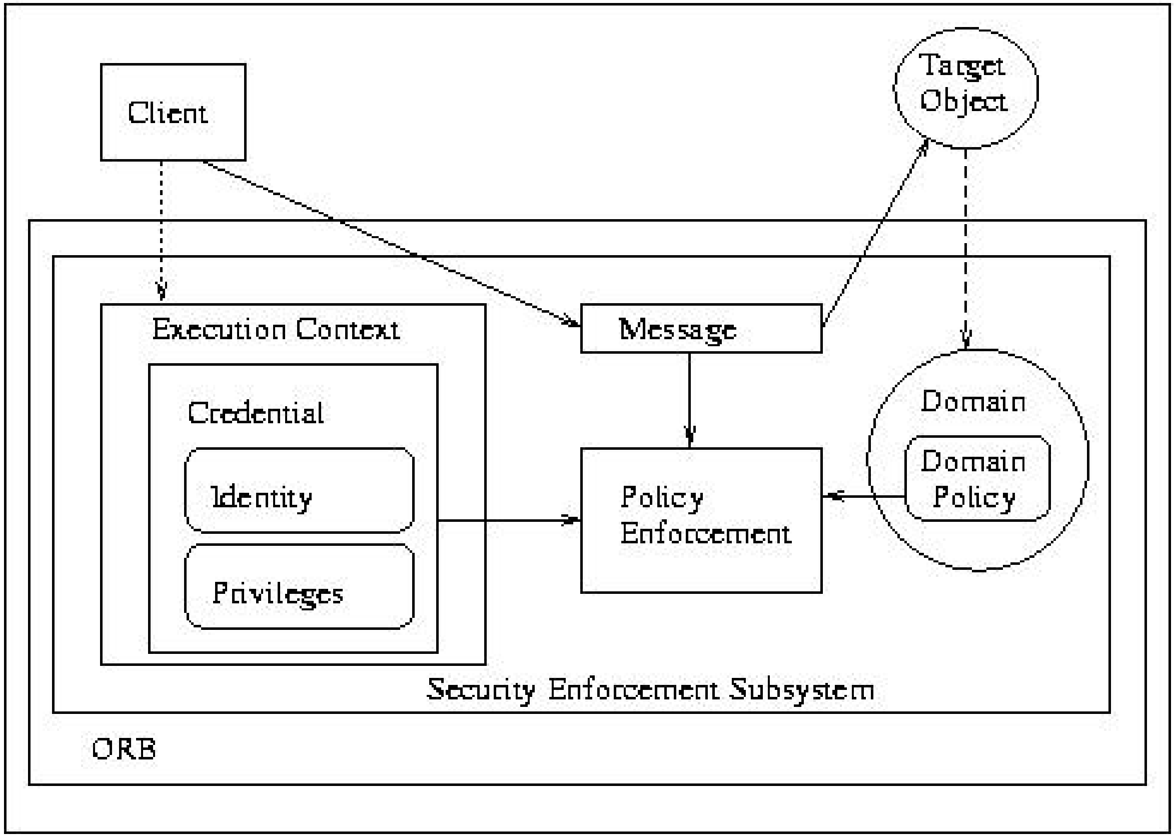
# CORBA Security Model

- Protection
  - Policy
    - access control policy
    - message protection policy
    - audit policy
    - non-repudiation policy
  - domain, subjects, objects, actions
- Execution context
  - ORB, credential, identity, privileges

# CORBA Security Model (contd..)



# CORBA Security Model (contd..)



# Domain and Access Control Policy

- Domain: group of objects
- Privilege Attributes: group of subjects
- Policy: applicable to all objects in a domain
  - subject **A** may perform action **X** (on domain members)
- Required Rights: group of actions
  - **g**et, **s**et, **u**se, **m**anage
- Domain access control policy
- **subject** is granted rights <**right list**>

# CORBA Access Control Policy

- **Examples**
  - **A** is granted rights **g**, **s** and **m**
  - **B** is granted right **g**
- Makes managing of access control policies easy
- Useful when number of objects in a system is large

# Fine Grained Access Control

- Required to control access at service (method) and object level
- Subject:
  - user, group of user or a role
- Object
  - object, group of objects, a method of an object, a group of methods in an object

# Access Control Rules

- *subject* **a** is granted access to *object* **o**
- *subject group* **A** is granted access to *object* **o**
- *subject* **a** is granted access to *method* **m** of *object* **o**
- *subject group* **A** is granted access to *method* **m** of *object* **o**
- *subject* **a** is granted *rights* **s**, **m** on *domain* **D**
- *subject group* **A** is granted *rights* **g**, **s** on *domain* **D**

# Implementation over CORBA Security Service

- Tool to provide a management layer over CORBA Security Service
- Uses CORBA Security Service management Interfaces
- Security Managers can specify access control policy using fine grained model
- Layer above CORBA Security Service translates these rules transparently

# Mapping policy to CORBA Security Service

- If the target of a policy is a single object
  - create a new CORBA Security Service domain with only one object
- If the target of a policy is an individual method
  - Create a new domain for that object
  - Create a new right family with new required rights
  - Method’s required right set contains one right from the new right family

# Implementation

- GUI tool to help administrators create and manage
  - new subjects: users, group of users, role
  - specify fine grained access control policy
- No change in CORBA Security Model
  - Tool uses CORBA Security Service interfaces to map access control policy
- Uses stable storage to save fine grained policy and newly created domains and right families