Object Management Group (OMG)
and
National Security Agency (NSA)
First CORBA Security Workshop
April 1-3, 1997 Baltimore, MD

CORBA Deployment Scenarios

CORBASec1.1 Assessment

Bhash Ganti
Senior Principal Scientist
Boeing Commercial Airplanes Group
bhash@atc.boeing.com

CORBASec1.1 Assessment

Focus

- Security issues in a hybrid system (i.e., CORBA and Non-CORBA)

Problem areas

- Security across subsystem boundaries
  - Authentication and Authorization
  - Unambiguous interpretation and mapping of security attributes & operations

Assessment

- Not so good news
  - Sophisticated delegation models may not help in a hybrid CORBA system
  - lack of common semantic models for security services will be a barrier
- Good news
  - May be solved using hybrid access control mechanisms, if implemented

OUTLINE

- CORBA Deployment Scenarios
- Business Drivers
- Functional Requirements
- Security Requirements
- CORBASec 1.1 Assessment
- Summary
- Recommendations

CORBA Deployment Scenarios

CORBA is generally deployed as ...

- A platform for new OO distributed applications

or

- An application integration middleware

or

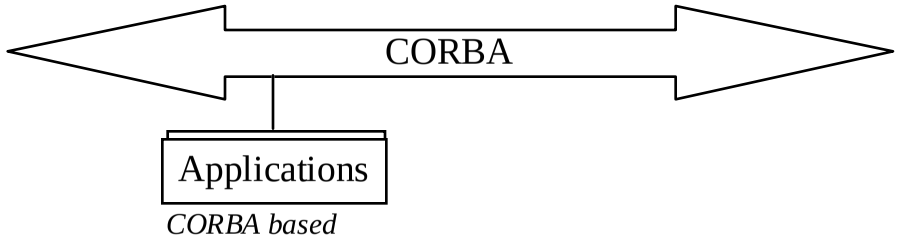
- An enabler for revitalizing legacy systems

Or some combination of these that require interworking with non-CORBA environment

CORBA Deployment Scenario-1
A platform for new OO distributed applications

Predominately CORBA environment with emphasis on new object oriented system development

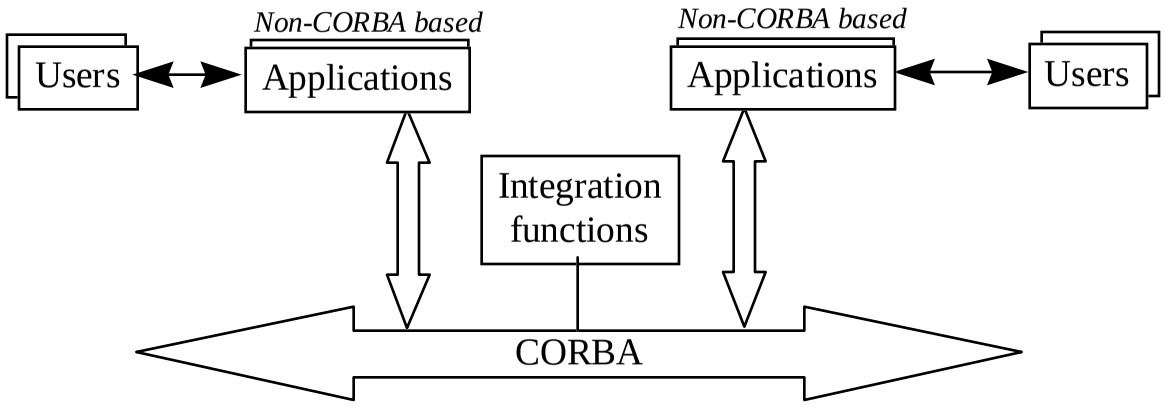
- Green field situation
- Limited interfaces to the existing systems



CORBA Deployment Scenario-2
As an application integration middleware

CORBA infrastructure is primarily used as an application integration layer to loosely couple several independently developed applications

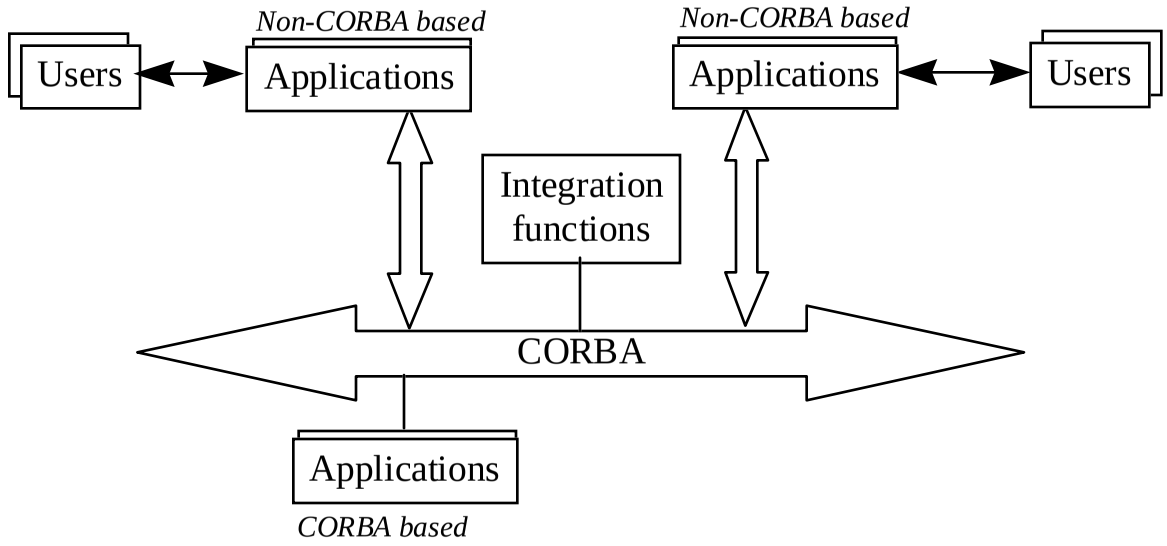
- Infrastructure means, it is there in the background
  i.e., minimal end user functionality - CORBA is invisible
- Application integration layer functions as a messaging bus
- Loose coupling allows independent existence of applications



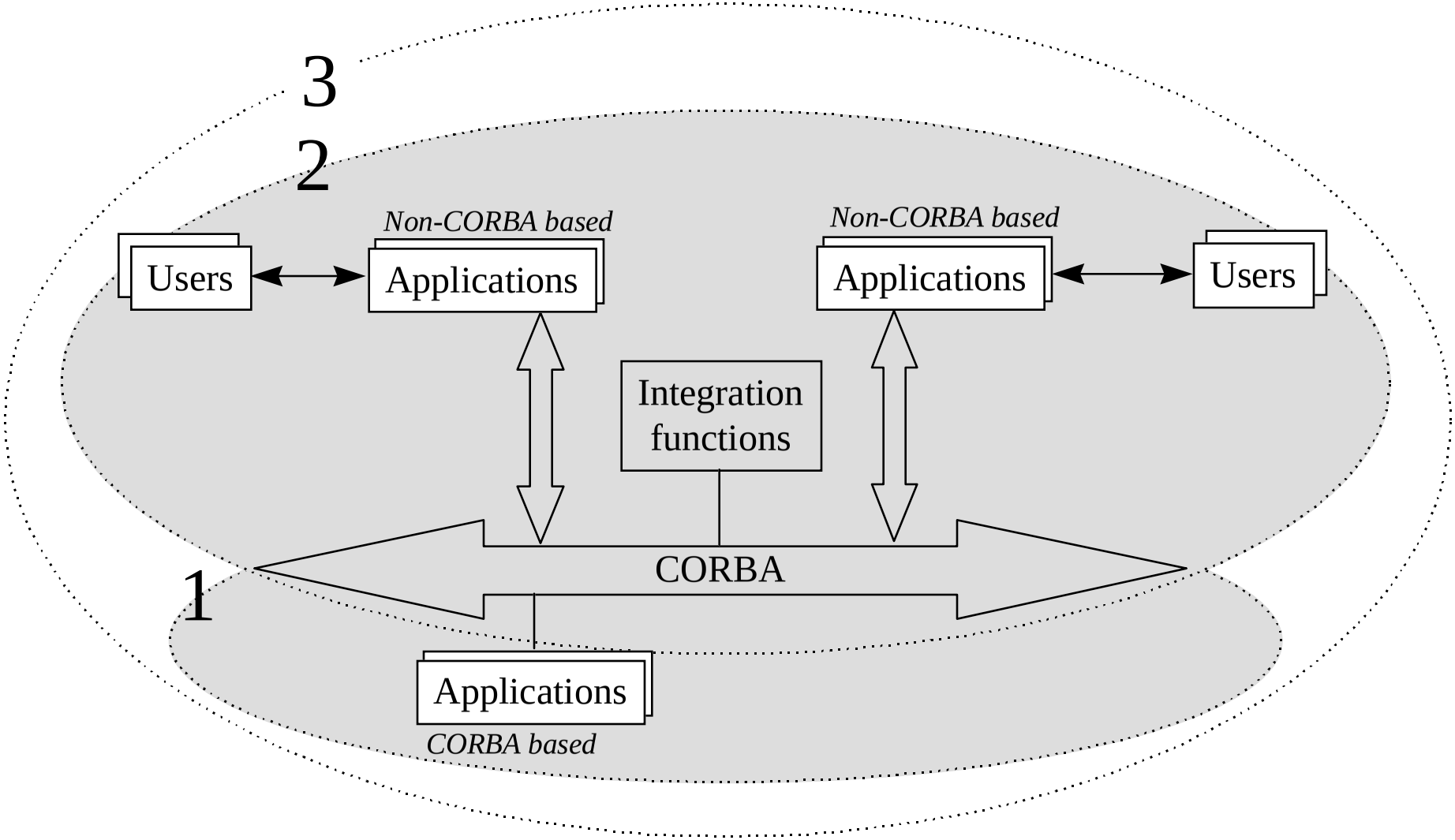
CORBA Deployment Scenario-3
As an enabler for revitalizing legacy systems

CORBA acts as a service layer to repackage legacy information

- Business process changes usually cut across several systems
- Service layer provides the users the ability to interact in terms of business entities not systems
- Repackaging information means transformation of UI - Web frontend



CORBA Deployment Scenario



Business Drivers
CORBA Deployment

Business Process Reengineering

- Integration of commercially available business applications
- A common facility to link information flow across multiple legacy applications in preference to point solutions - n vs n(n-1)/2 scenario
- Migrate towards a service based approach
- Add value to users by providing process centric rather than system centric view of information
- Do all this in a cost effective fashion in a heterogeneous environment

If CORBA can deliver a secured heterogeneous distributed system that can meet information protection needs, we have a winner

Functional Requirements
CORBA Deployment

Integration Functions

- Asynchronous messaging backbone
  - store-forward capability
  - smart routing
  - guaranteed delivery once
- Audit facility
  - application event logging for trouble shooting
  - Checkpointing for system recovery
- System management facility
  - alerts and diagnostic tools for improved uptime

New Functions

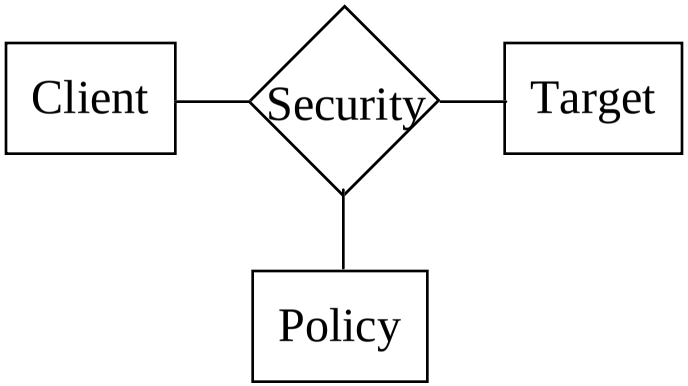
- Encapsulation of legacy system as business objects
- Composition of new business objects

Security Requirements
CORBA Deployment

The key requirements in a hybrid CORBA system are:

- Scaleable cross-domain authentication
- Scaleable authorization service
- Invisible security policy mediation - mainly authorization
- Secure infrastructure elements for the hybrid system
  - should be secure and can not be bypassed
  - should not pose undue security administration burden
  - administration should be invisible to most users

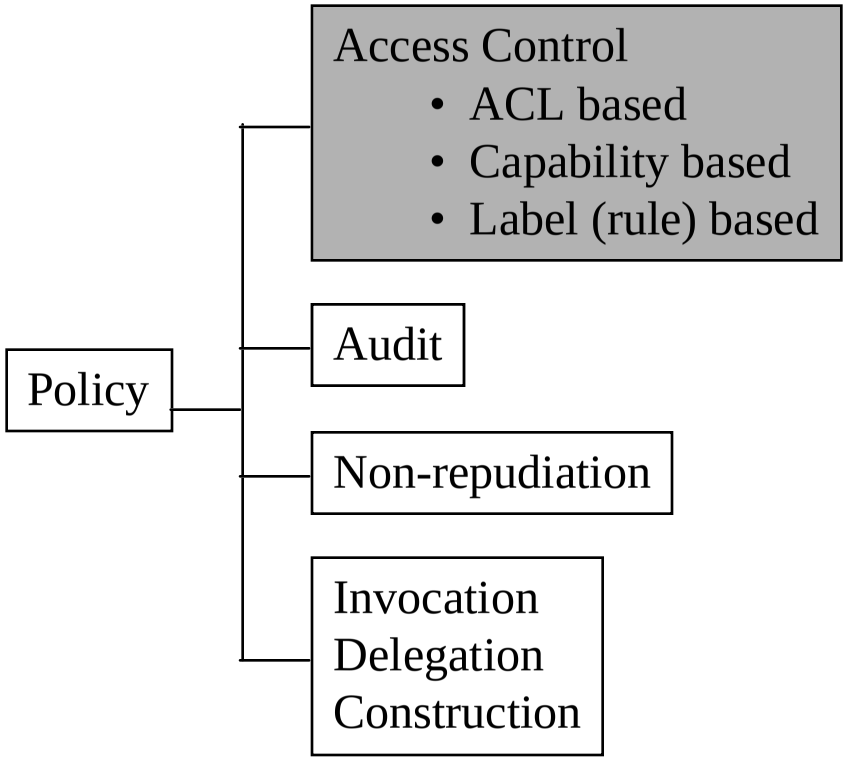
CORBASec1.1 Assessment
Security Concepts



Security is a
three way
many-to-many relationship
among client, policy and target

- Security is a three legged stool
- Policy governs behavior
  - can be invisible or visible
  - allows multiple policy mechanisms
- Security specification
  - Defines the syntax, usage and some implementation objects to ensure secure “security services”
  - Does not define semantics
  - Security services can be part of the ORBOS or implemented outside the ORBOS

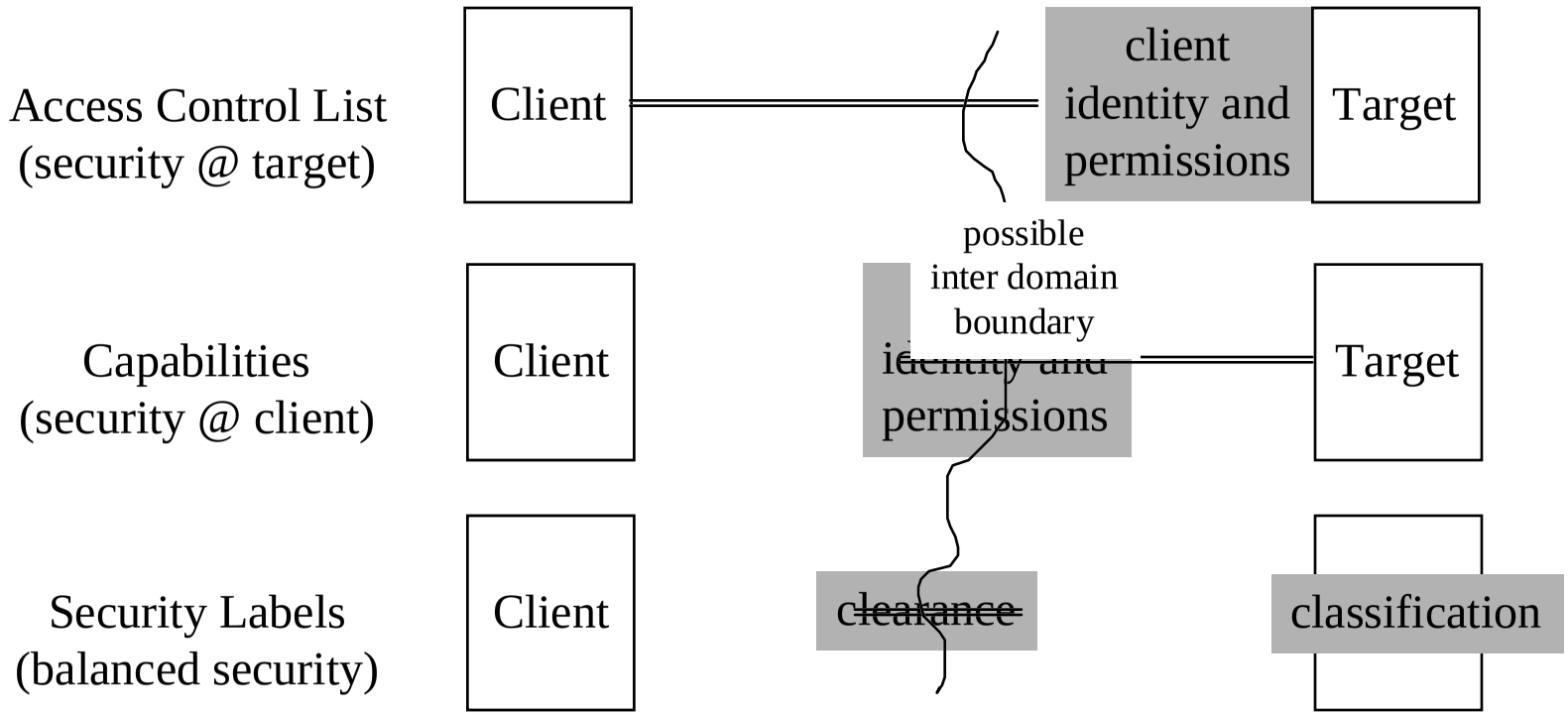
CORBASec1.1 Assessment
Security Policies



Policy describes and enforces security contract between clients and targets

- I&A policies left for implementers
- Key challenges
  - delegation in a hybrid system
  - semantics of the policies
  - coordination of the policies
  - commercially available security mechanisms may not be rich enough for canonical implementation of security service across hybrid domains
  - distributed authorization

CORBASec1.1 Assessment
Range of Access Control Mechanisms

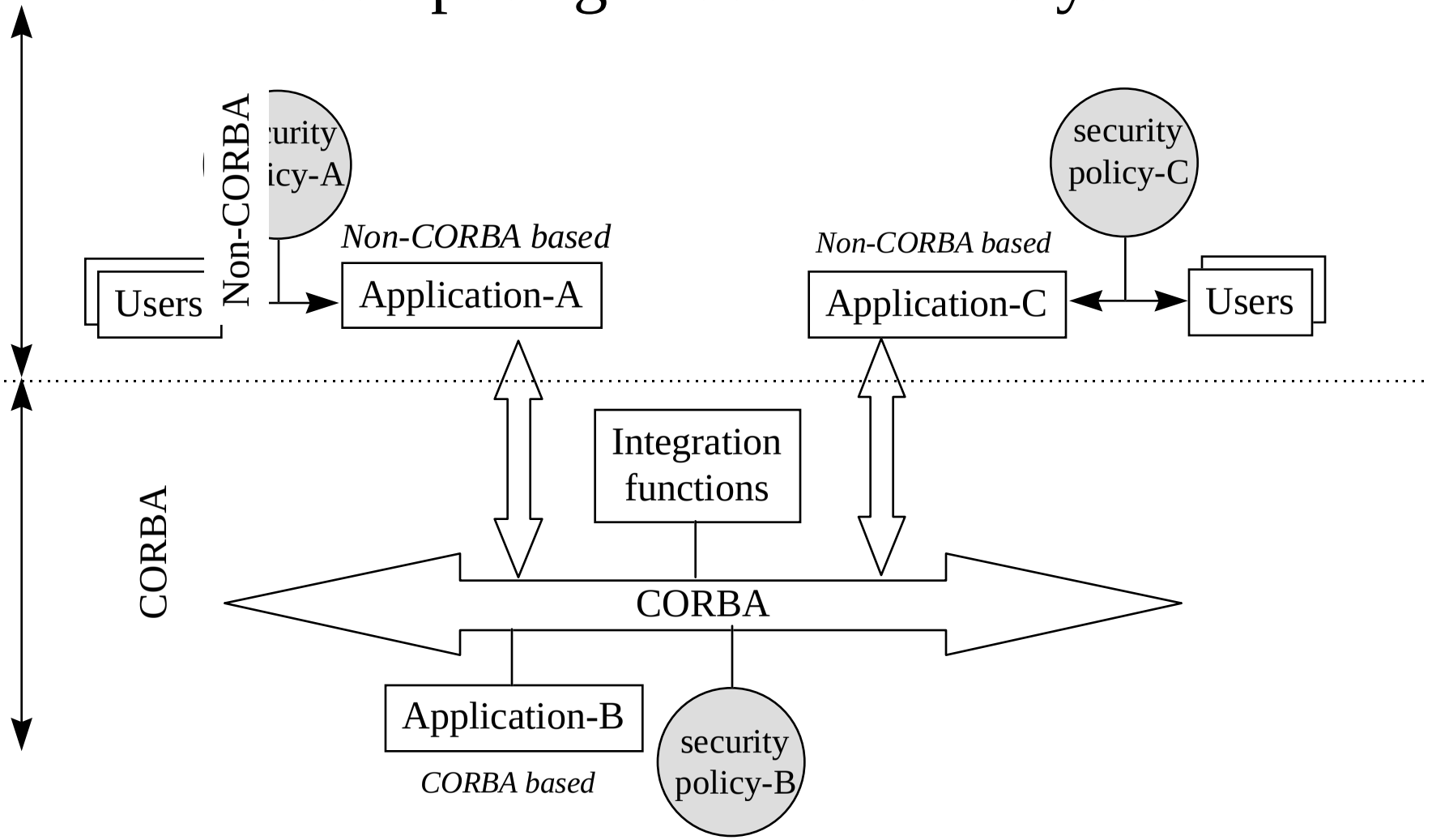


There may be a need for all three mechanisms in a CORBA deployment environment

CORBASec1.1 Assessment
Comparison of Access Control Mechanisms

Feature	ACL	Capabilities	Security Labels
Access control decision	made near target	made near client	rule based
Security policy domain	target's domain	client's domain	system imposed
Suitability	stable user base	small # of targets	mandatory controls
Granularity	high	high	low
Scaleability	average	average	high
Grant/revoke privileges	controlled by target	not easy to control	rule based
Implementation	table driven	table driven	rule based

CORBASec1.1 Assessment
Computing Model for Analysis



CORBASec1.1 Assessment
Access Control Strategy

Motivation

- The access control policy for CORBA objects that serve non-CORBA domains should be invisible
- System security administration overhead should be minimal

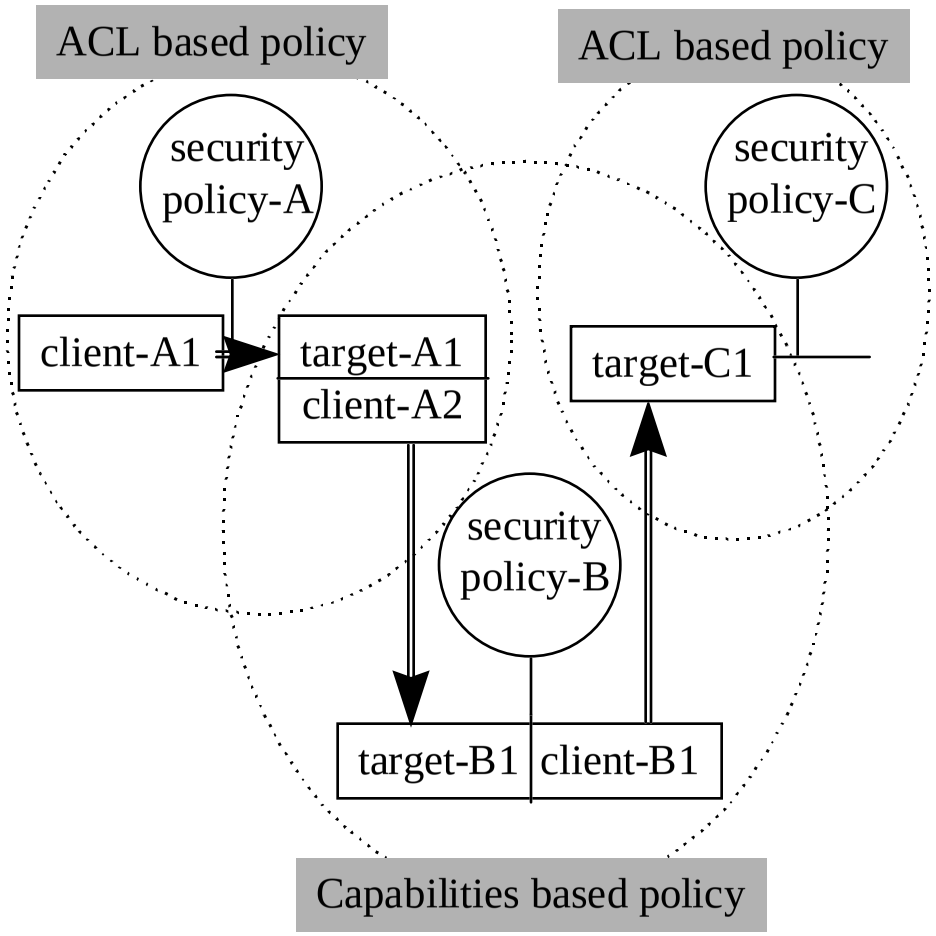
Security Strategy

- A scaleable, trustworthy and self-administering CORBA authorization service not directly based on user's identity

Implication

- ACL based access control mechanism may not be suitable - not scaleable
- Capabilities based access control mechanism may have a distinct advantage
- Label based access control mechanism may provide an elegant solution as the rules for governing the interactions can be imposed by the system

CORBASec1.1 Assessment
Key Security Characteristics



- Inter domain policy mediation is no longer a problem
- Inter domain delegation is addressed indirectly
- Use of capabilities based access control policy for the CORBA domain ‘B’ shifts the responsibility of security administration to the non-CORBA domain ‘A’.
- For cross domain functional integration the number of clients/targets in the CORBA domain ‘B’ is small and stable and therefore, will not impose undue burden on the non-CORBA domains ‘A’ and ‘B’

Summary

- CORBA deployment may be classified into three different categories. They share many of the same security issues characteristics of a hybrid system.
- The main problem area is cross domain security in a hybrid system
- Deployment of authorization service may well be by far the most complex of all the security services in a hybrid system
- A case for multiple access control policies within a single integrated system has been presented. Analysis supports the claim that judicious use of multiple policies will simplify the security administration complexities
- The CORBASec1.1 delegation model may not be useful in a hybrid system
- CORBA security specification accommodates multiple access control policies. It remains to be seen how CORBA vendors may deliver all three access control mechanisms that can interoperate

Recommendations

- Need more focus on problems of cross domain security
  (*The lessons learned from DCE - all or nothing proposition is not attractive to the customers*)
- Need semantic models for security policies
  - Security specification primarily addresses (by choice)
    - Syntactical definition of the service interfaces
    - Security mechanism transparency
  - A semantic meta model for security policies may identify the deficiencies of currently available security mechanisms
  - Absence of a standard semantic model(s) will greatly hinder deployment of secure CORBA in a non-CORBA environment.
    In a single vendor pure CORBA environment this may not be problem
- Recommend a working group to define the requirements - potential for an RFP?