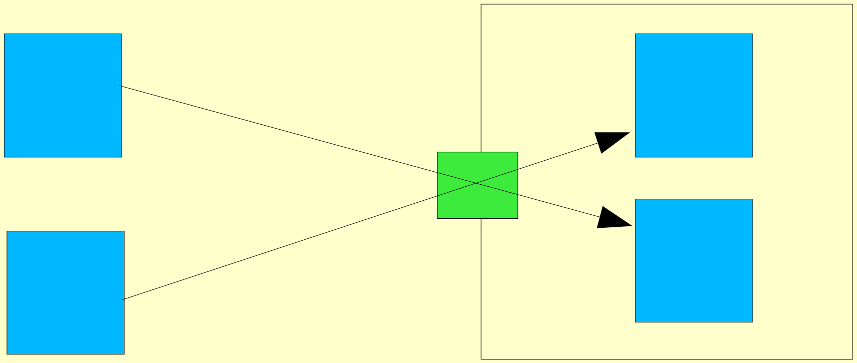
Technique For Managing Access To Secure CORBA Services

Phillip L. Mesnier

Object Computing, Inc.



Why Security Matters

- It is becoming more common to Deploy a DRE system with Internet access
  - This opens the system up to possible misuse and resource mismanagement
- Platforms frequently permit many users to start processes
  - Internal security is as important as external security

OBJECT COMPUTING, INC.

Current Access Security Options

- An implementation of CORBA Firewall specification
- Non-CORBA solutions, such as a port forwarding third-party firewalls

Limitation Of CORBA Firewall

- Runtime burden may be imposed by intermediate gateways

- Requires potentially complicated configuration to describe route

Limitation Of Non-CORBA Firewalls

- Port-limiting firewalls require specific administration to add new services
- Services require well-known ports

A Need To Restrict Server-Side Access

- Many developers may have access to a production host
- Inadvertent activation of services may impact the production system
- No current firewall product restricts *who* may start a service

OBJECT COMPUTING, INC.

Our Middle Ground Solution: PBXIOP

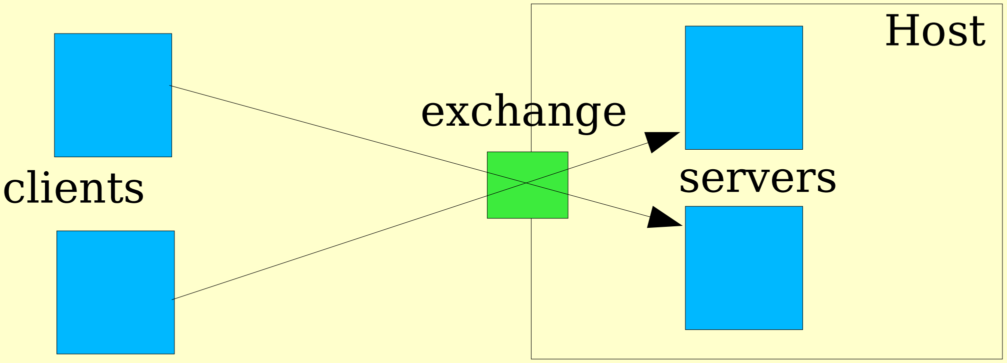
- Does not impose a post-connection runtime burden
- Allows an arbitrary number of services to share an endpoint
- Prevents unauthorized users from attaching to that endpoint

What Is PBXIOP?

- A specialization of IIOP providing an alternative means of connection establishment
- A private branch exchange system is an apt analogy, hence the prefix “PBX”

Participants In PBXIOP

- A single, persistent "exchange" with single access point
  - mediates connection establishment
- Clients, Servers connect through the exchange



Low Runtime Overhead

- Once a connection is established the connection delegate is no longer involved
  - Clients and servers may negotiate additional security, such as exchanging X.509 certificates

Low Configuration Burden

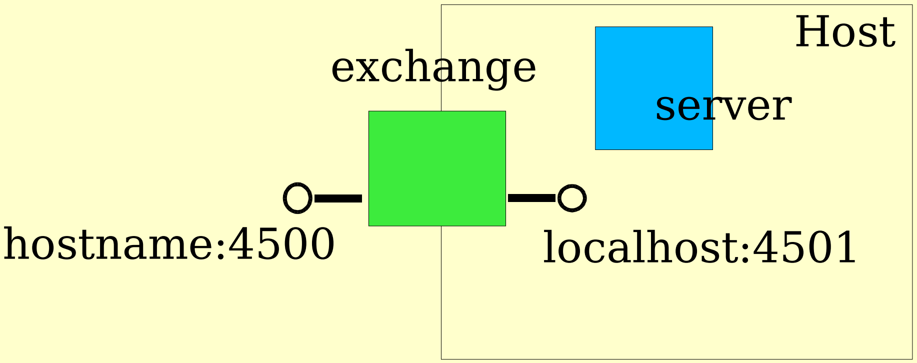
- Requires no specialized policies
- Loaded via ORB specified ESIOP mechanism
- Server may use a well-known or ephemeral endpoint
- Clients may use corbaloc style object references

A Single Exchange Supports Many Servers

- Many servers on a host may register with a single exchange
- Connections are delivered to servers via socket passing mechanism
  - Unix domain socket
  - Named Pipe

Servers Register With Exchange

- The server uses a supplied address as a hint to find the exchange
  - The exchange listens for server connections on a localhost endpoint
  - Supplies desired extension, if any



Servers Authorized By User

- Server declares user identity
- Exchange challenges
- Server answers challenge

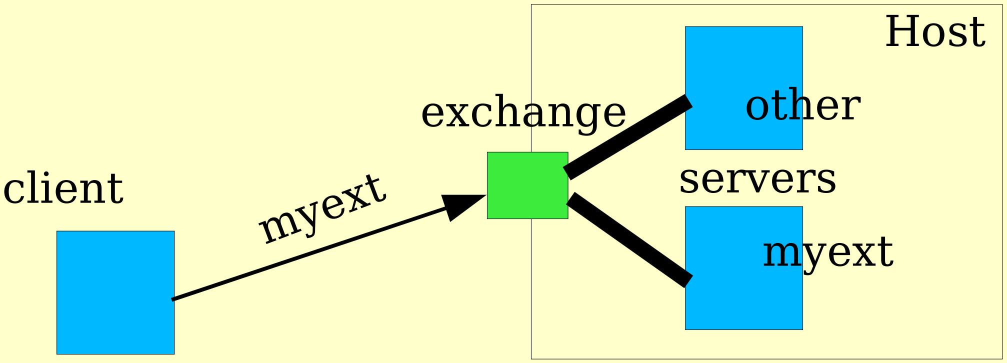
Exchange Supplies Address

- The address combines exchange's external host/port with the servers' extension
  - For instance: myhost:1234:myext
- Server is responsible for advertising endpoint

OBJECT COMPUTING, INC.

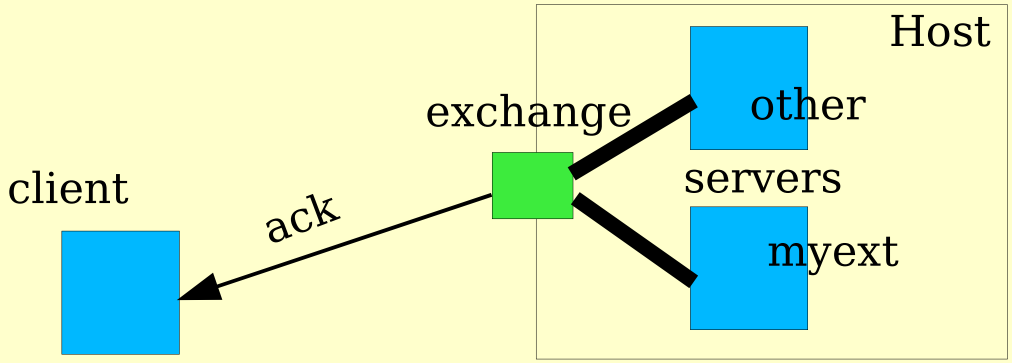
Clients Connect To Exchange

- Using the host/port portion of the address advertised by the server
- Sends desired extension



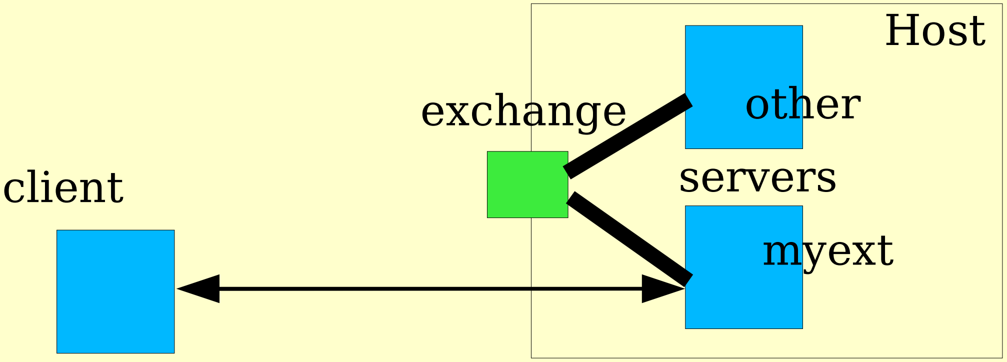
Exchange Validates Request

- Sends a single octet as an ACK
  - Connector waits for acknowledgment before returning
- Exchange closes connection if requested server is not available



Exchange Passes Connection To Server

- Exchange is no longer associated with the connection
- Server completes connection establishment



Integration

- PBXIOP implementations exist for TAO 1.3a and JacORB 2.2
- TAO integration achieved via TAO specific pluggable protocol framework
- JacORB integration presented an opportunity to exercise the ETF

OBJECT COMPUTING, INC.

Future Enhancements

- Client – Exchange protocol could be secured
- Could be used with non-CORBA services
- Exchange could work with port-masking firewalls and NAT

OBJECT COMPUTING, INC.

Availability

- PBXIOP is not yet freely available
- Permission to share is on a case by case basis

Concluding Remarks

This technique for managing secure access shows that it is possible to provide a moderate level of access security without unduly burdening services

THANK YOU!