CORBA Security: the Internet, Firewalls, and Beyond

E. John Sebes

Trusted Information Systems, Inc.

Outline of This Talk

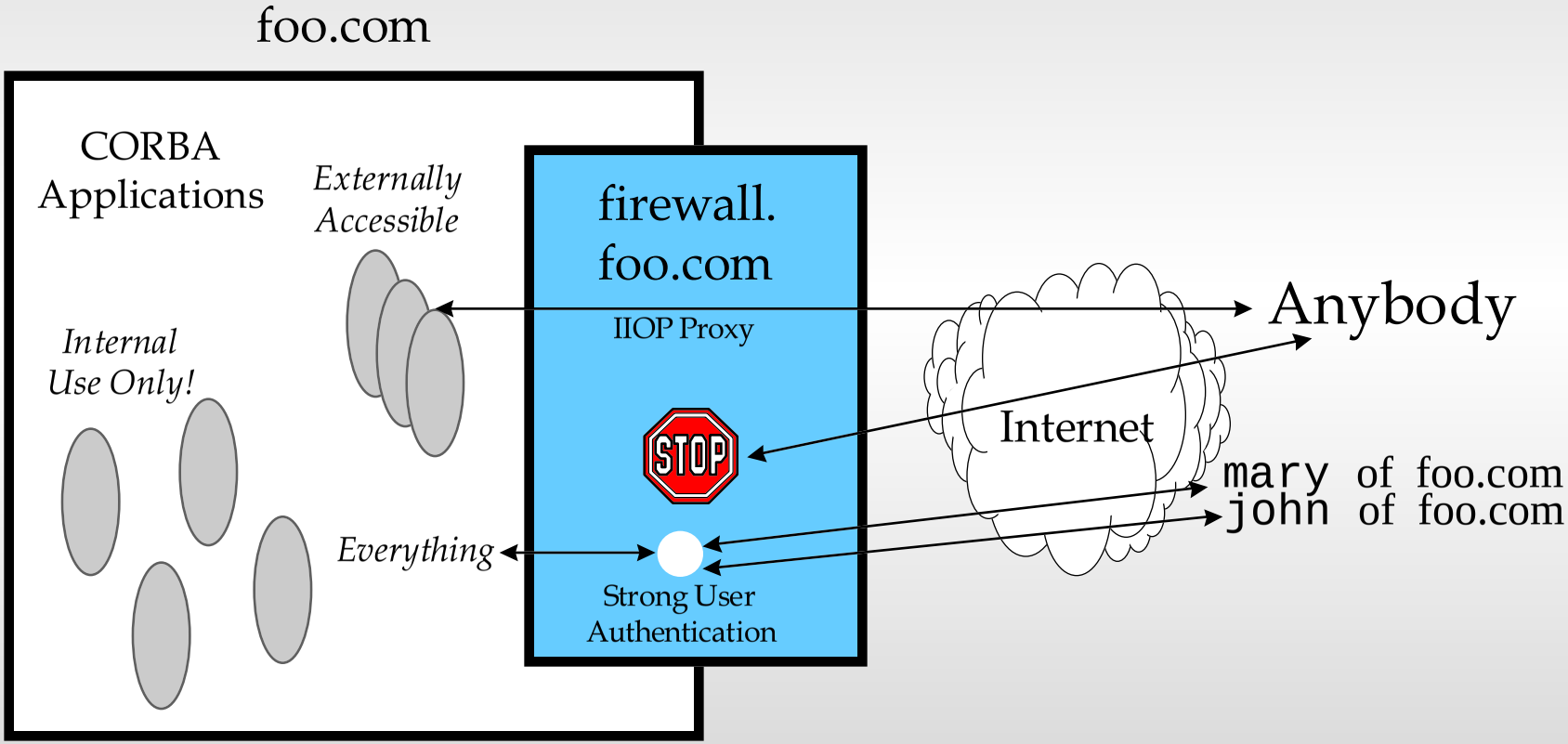
- Security requirements and issues
  - Current situation: where we are today
  - Current technology: what we can use today
  - Evolving situation: where we may be before long
  - New technology: what we may need before long
- Current research: TIS work on CORBA security

  Sigma: research project at TIS (DARPA/Rome Labs funded)
- Onward: open issues, research opportunies

CORBA and Firewalls

- Firewalls must process CORBA network traffic in three related cases
- Internet: world access to "public" CORBA-based application services
- Extranet: selective access to services shared with collaborating organizations
- Intranet: controlled access to services shared within an organization
- Three trust models: none (Internet), organizational (Extranet), individual/role (Intranet)

Internet Firewall and CORBA



Internet Firewall and CORBA

- Current situation: possible to proxy CORBA protocols
  - Inter-operability protocols: IIOP, DCE-CIOP, …
  - Proxies and stateful inspectors are OK
  - But packet filters are very risky for CORBA protocols
  - No current products, only proof of concept prototypes
- Current technology: existing firewall technology
- Evolving situation: beyond existing firewalls
  - Finer granularity of control, object-oriented permissions
- New technology: integration with & development of:
  - Distrbuted authentication, scaleable OO access management

ORB Gateways

- ORB Gateway is single point of external access to object services of an enclave
  - Mediates outside object requests based on nature of request and attributes of requester
  - Interprets security attributes from other enclaves
  - Enforces enclave policy for external object access
- Might be part of a firewall, especially for initial try with modest scope and little sophistication
- "ORB Gateway" connotes control of traffic between *ORB*s of multiple enclaves, rather than gateway or proxy control of traffic with outside world

ORB Gatewaying Today

- Simple approach can provide basic controls on ORB interoperation
- Proxy IIOP as first-class inter-network protocol
  - No tunneling of IIOP via HTTP
- Policies based on per-method and per-object controls
  - ACLs, capabilities, or access classes for each
- This is the approach of current Sigma prototypes, and of Orbix's "Wonderwall" product
- Not rocket science!

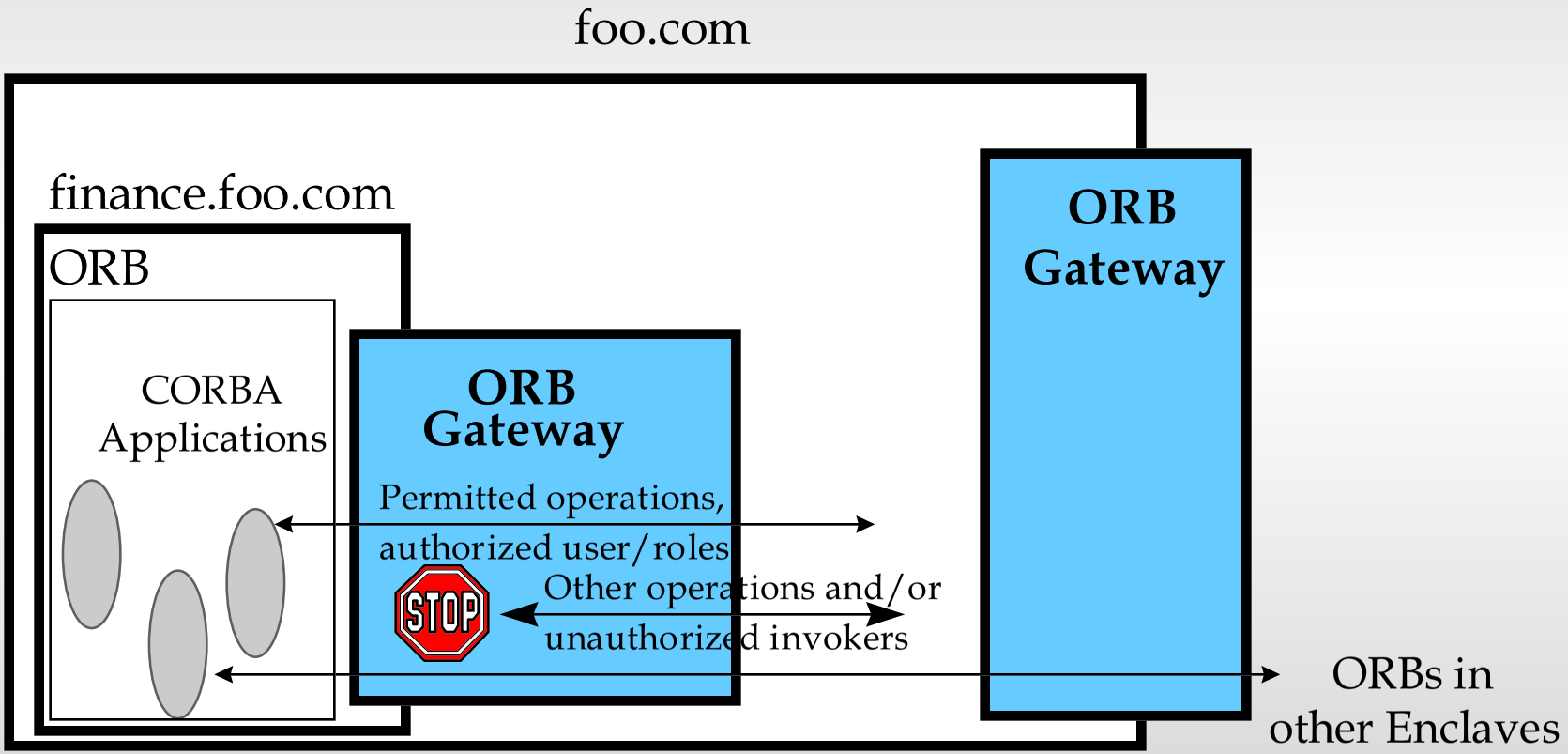
ORB Security and Assurance

- Fact of life: current commodity OSs *do not support* strong, unbypassable, tamperproof security mechanisms in ORBs
- Best current approach to unbypassable distributed security mechanisms: control of network topology
- Same approach as for security and control of inter-ORB and/or Internet-based CORBA computing
- Use and extend basic approach from firewalls
  - Extend to handle more sophisticated needs of distributed object system-of-systems

Concept of Operation

- Protect enterprise networks, interoperate with world
  - Gateway security for CORBA IOPs over Internet
- Divide network into separate enclaves
  - Each enclave composed of users, resources with some degree of trust
  - ORB security mechanisms sufficient to threats within enclave
  - Dedicated insiders may be able to subvert security mechanisms
- Protect interoperating enclaves from each other
  - Gateway security for CORBA IOPs over intranets

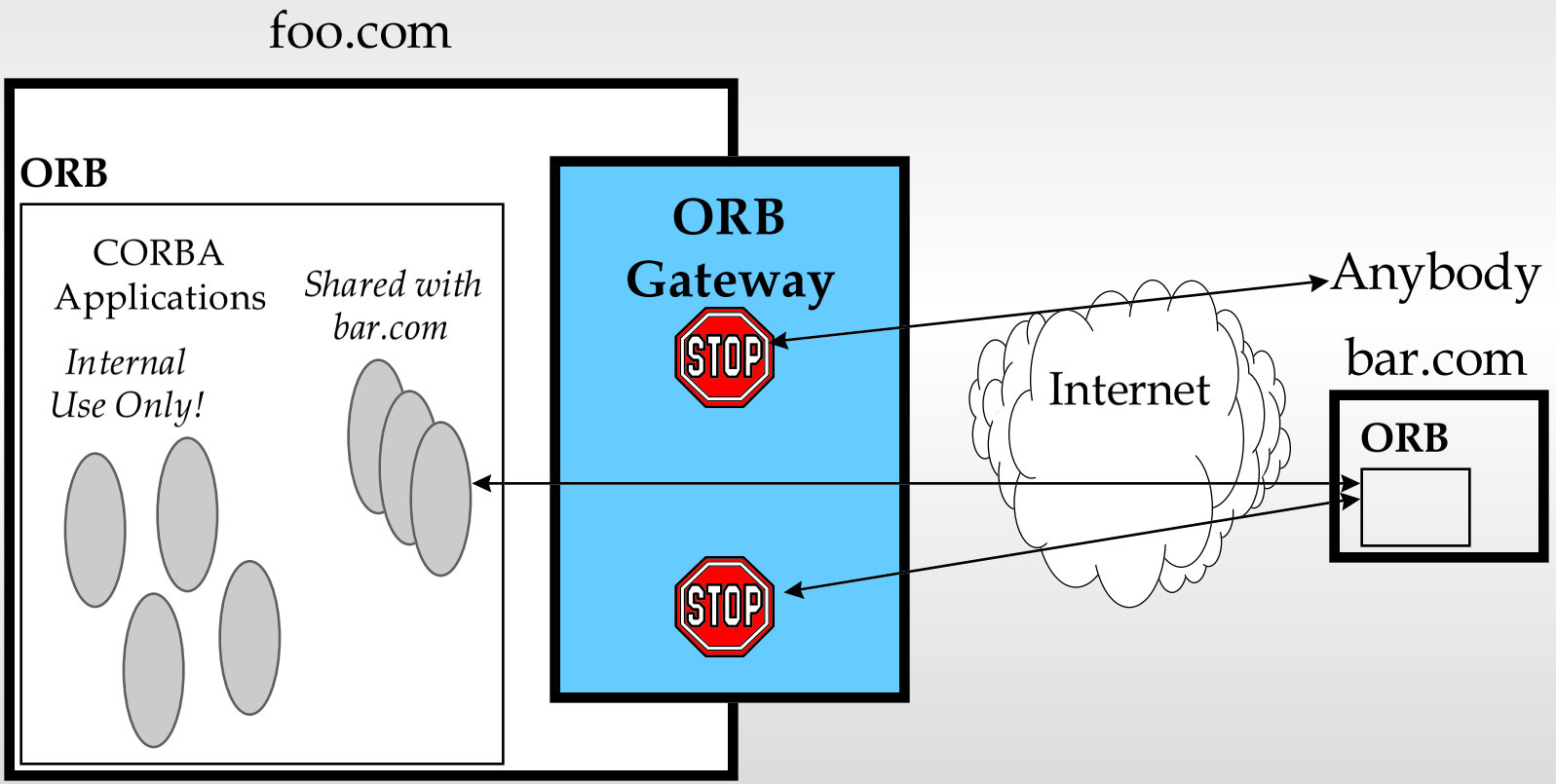
Intranet and ORB Gateway



Intranet and CORBA Gateway

- Current/evolving/new situation, technology:
  - Same as with "Extranet" collaboration via Internet and ORB gateway: IOPs, distributed authentication, SECIOP, SSL, policy management; upcoming ORB features or research
- But different requirements:
  - Not necessarily multiple ORBs
  - Definitely multiple policies
  - Fine grained OO access control and roles

Internet and ORB Gateway



Internet and ORB Gateway

- Current situation: beyond existing firewall technology
  - Inter-operability protocol implementations combined with middleware-based authentication
- Current technology: Kerberos, Sesame, SPKI,…
  - But no SecIOP implementations yet!
  - Maybe: simple capability via SSL (current OMG RFPs)
- Evolving situation: state of flux for ORB features:
  - Distributed authentication, security policy management
- New technology: some features may be in ORBs RSN
  - Other features are research topics

Sigma Project Overview

- 3 year project to address access controls for distributed object-oriented systems based on CORBA
- Developing security mechanisms for
  - Interoperability between enclaves:
    ORB Gateway; Distributed authentication
  - Interoperability within enclaves:
    Domain and Type Enforcement (DTE); MLS ORB
- Early results applicable to current issues in CORBA security, firewalls, IIOP over the Internet, ...

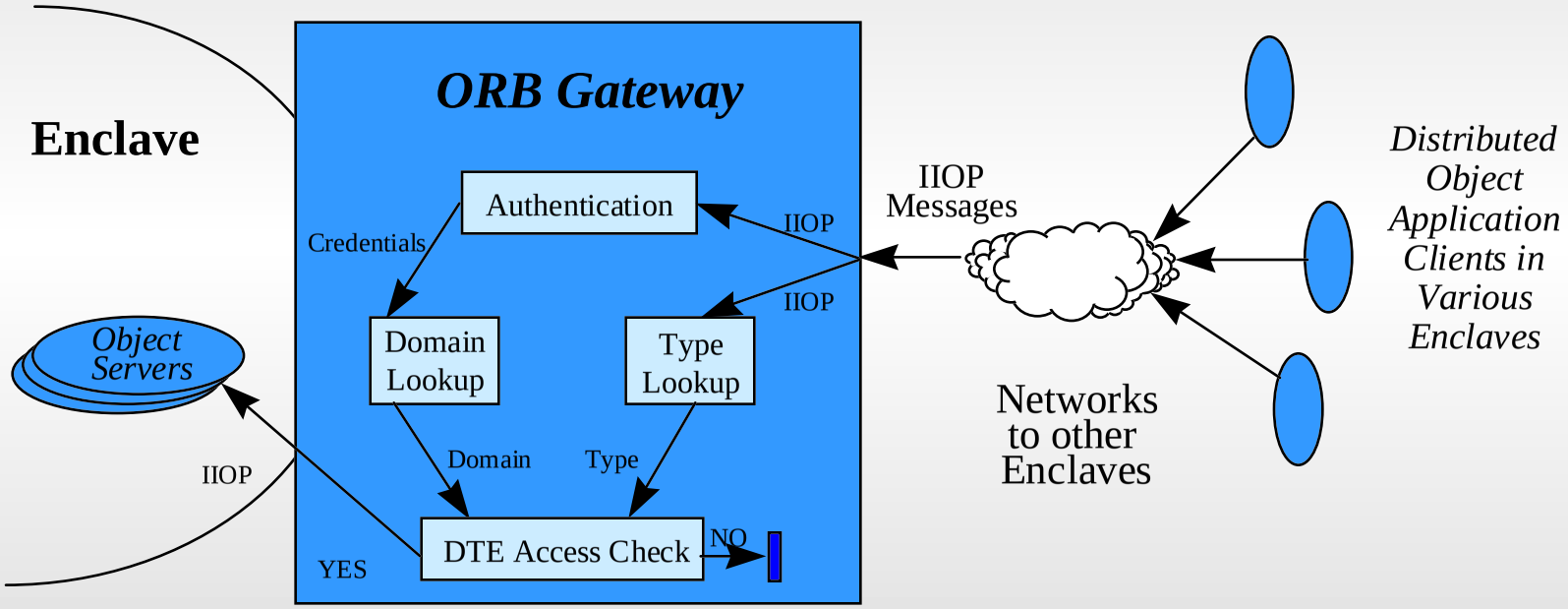
Ongoing Sigma Research

- More advanced ORB Gateway security mechanisms
  - Composable distributed authentication framework and protocols
  - Flexible, scalable authorization via Domain and Type Enforcement (DTE)
- Domain and Type Enforcement (DTE) for intra-ORB security within enclaves
- Multi-level secure (MLS) technology for ORB security in MLS enclaves

ORB Gateway Access Control

- Mediation can be performed on a per-service, per-method, or per-object-instance basis.
- Can also depend on requester's security attributes
  - Obtained from network data and/or request message
  - Obtained via authentication mechanisms which depend on cryptographic mechanisms
- Decisions computed by DTE access checking code
  - Maps other enclave security attributes to DTE data
  - Derived from OO DTE definitions

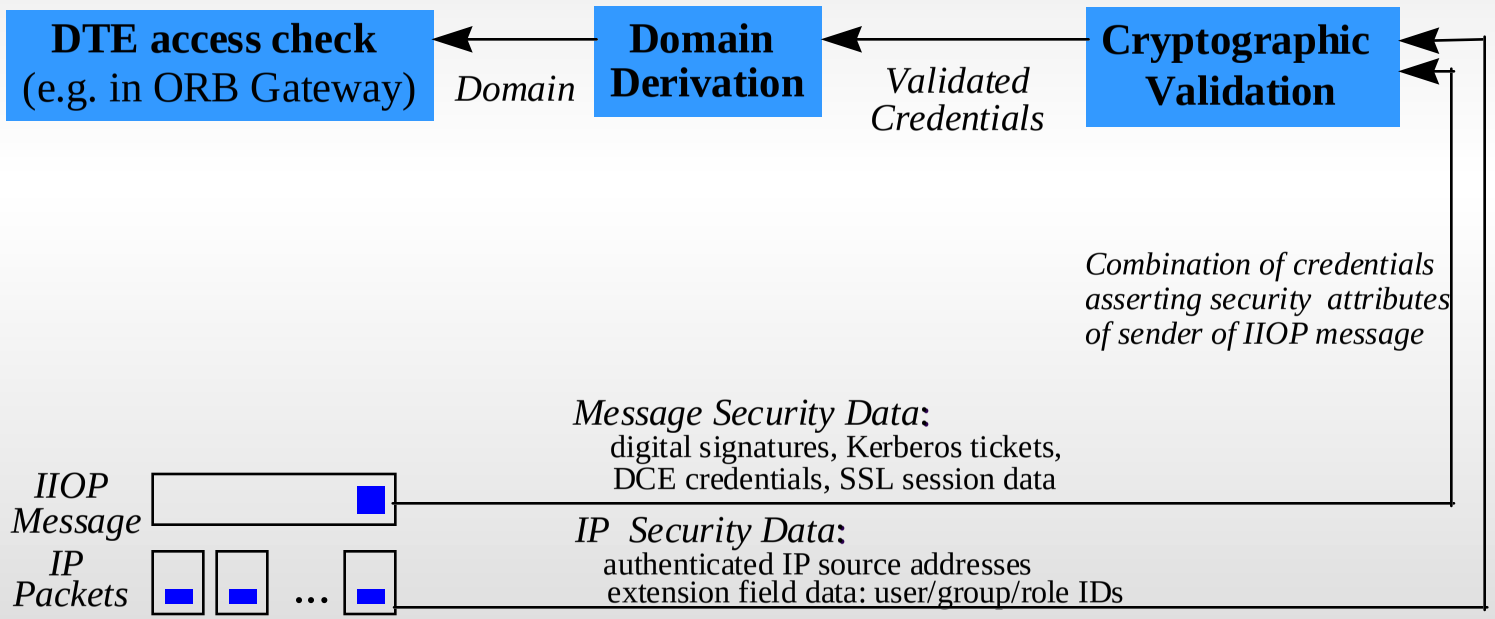
ORB Gateway Prototype



Distributed Authentication

- Goal: develop and demonstrate suite of authentication mechanisms for CORBA security
  - Based on functional specs of CORBA Security standard, IIOP protocol, Sec IIOP, SSL, etc.
- Multi- protocol framework, several authentication techniques (Digital signatures, Kerberos, IP security)
- Scaleable support for multiple degrees of trust/privilege
- Sigma project currently developing proof of concept prototypes, for integration with IIOP in ORB Gateway

Distributed Authentication Techniques



DTE for Object-Oriented Distributed Systems

- Typical approach for access control in distributed systems, server processes enforce server-specific ACLs, e.g., DCE
- Problems
  - ACLs proliferate, are hard to understand, don't scale
  - Fragmentary, discretionary restrictions
  - Does not constrain servers
- Potential Solution: Object-Oriented DTE
  - Equivalence classes for scalability
  - Coordinated enforcement imposed by ORB/middleware

Prototype Demonstrations

- Initial ORB Gateway prototype
  - 3 Party : Client, Gateway, Server
  - Simple DTE policy enforcement
  - IIOP over Internet, interoperates with ILU
- Object-Oriented DTE Demo
  - Simple package pickup/delivery application
  - Interfaces described in CORBA IDL
  - Access to OO services -- per role, controlled by DTE OS and DTE-enhanced ORB
  - Distributed system with DTE and non-DTE hosts

Onward: Research Opportunities

- Dynamic virtual enclaves with CORBA
- CORBA guards, automated releasability
- ORB unbypassability/tamperproofness
- ORB security plug-ins, role-based authorization, DTE
- Security policy management
- ORBs for MLS systems, Multi-level secure ORBs

Onward: Current Issues

- IIOP over the Internet, through firewalls
  - IIOP tunneled via HTTP, for now(?)
- IIOP, Java, World Wide Web, and firewalls
- Research (Sigma), product R&D (Wonderwall)
- Firewall vendor plans for IIOP: still early
- OMG may take the lead with IIOP and firewalls
  - Demonstrate a plan for IIOP/Internet/firewalls
  - Demonstrate ORB market as market for IIOP and firewalls
  - Continue to push envelope with IIOP/WWW/Java

For More Information

- TIS staff here in Baltimore :

  John Sebes, Dan Sterne, Michelle Abram, Gregg Tally
- E-Mail us:
  - Terry Benzel: tcvb@la.tis.com (Sigma project lead)
  - John Sebes: ejs@ba.tis.com (ORB Gateway team lead)
  - Deborah Shands: dshands@tis.com (Authentication team lead)
  - Dan Sterne: sterne@tis.com (DTE team lead)
- TIS Web site for more information about the Sigma project
  http://www.tis.com/research/distributed/sigma.html
- Check OMG Web site for latest revisions and status of draft RFP on CORBA and Firewalls
  http://www.omg.org/members/doclist.html