Overview of CORBA Security

Konstantin Beznosov
March 7, 2000
CEN6502
Outline

- Introduction into computer security
- Security in OO systems
- CORBA security model overview
- Application access control in CORBA
- Resource Access Decision Facility
- Further Information
What is Security?

• security -- “safety, or freedom from worry”
  – computers too heavy to steal
  – insurance
  – redundancy (disaster recovery services)
Conventional Approach to Security

Protection

- Authorization
- Accountability
- Availability

Assurance

- Design Assurance
- Development Assurance
- Operational Assurance

- Access Control
- Data Protection
- Audit
- Non-Repudiation
- Service Continuity
- Disaster Recovery
Protection

provided by a set of mechanisms (countermeasures) to prevent bad things (threats) from happening
Authorization -- protection against breaking rules

• Rule examples:
  – No one outside the company can read proprietary data
  – Tellers can initiate funds transfers of up to $500;
    Managers -- up to $5,000
    Transfers over $5,000 must be initiated by a VP
  – Attending physician can read patient HIV status
Authorization Mechanisms: Access Control

enforces the rules, when rule check is possible
Authorization Mechanisms: Data Protection

- No way to check the rules
  - e.g. telephone wire
- No trust to enforce the rules
  - e.g. MS-DOS
Accountability

- You can tell who did what when
- Audit -- actions are recorded in audit log
- Non-Repudiation -- evidence of actions is generated and stored
Availability

• Service continuity -- you can always get to your resources

• Disaster recovery -- you can always get back to your work after the interruption
Assurance

Set of things the system builder and the operator of the system do to convince you that it is really safe to use.

- The system can enforce the policy you are interested in, and
- the system works
Basic Object Interaction Model

• Objects do work by sending messages to one another
• ORBs handle the complexity of delivering messages to objects
Object Security Issues & Requirements: Naming

• Issues
  – no names,
  – no unique names,
  – aliases
difficult to state security policies

• Requirement
  – ability to define object security policy without having to know its name.
Object Security Issues & Requirements: Scale

• Issues
  – too many objects
  – name-based grouping is not good for security grouping

• Requirements
  – Policies -> policy groups, objects -> policy groups
  – Operation-level control, operations -> policy groups, no knowledge of operation semantics
Object Security Issues: Encapsulation

- No knowledge of the internals, difficult to know what policy is needed to protect the system
Overview of CORBA Security Model

Key Concepts

- Policy-based Protection
- Policy domains
- Execution context
- Credential
- Interfaces
Enforcement of Policies

Security Enforcement Subsystem

Execution Context
- Credential
  - Identity
  - Privileges

Message
- Policy Enforcement Code

Target Object

Domain
- Domain Policy

Client Application

ORB
Protection Policies

Subject action object

- Access control policy
  - `subject` may do `invoke method` to `object`
- Message protection policy
  - `ORB` must do `apply specified QoP` to `message`
  - QoP: authentication, integrity, confidentiality
- Audit Policy
  - if `action matches pattern` then `system` must do `generate` to `new audit event`
Protection Policies (2)

Subject action object

- Non-Repudiation Policy
  - if action matches pattern then subject initiating action must do generate to new non-repudiation evidence
  - if action matches pattern then subject receiving request must do verify to non-repudiation evidence
User Authentication

Client Application

User Sponsor

Principal Authenticator

Credential

Execution Context

Identity

Privileges

Security Enforcement Subsystem

ORB
Security Attributes of Subjects

Subject: Jean Baptiste Bernadotte
- Access id: Marshal Bernadotte
- Role: Empress of the French

Group: Royalty
- Access id: Josephine Bonaparte

Subject: Josephine Beauharnais Bonaparte
Application Access Control

• Granularity of control is coarse
• Many points of control
  (commonality, consistency, administration issues)

module SecurityLevel1 {
  interface Current : CORBA::Current {
    Security::AttributeList get_attributes (
      in Security::AttributeTypeList attributes
    );
  };
};

Framework of Resource Access Decision Facility

1. Application Request
2. Authorization Request
3. Reply to Authorization Request
4. Reply to Application Request
RAD Components

1: access_allowed
2: get_policy_decision_evaluators
3: get_dynamic_attributes
4: combine_decisions
5: * evaluate
RAD Design Benefits

• Decoupling authorization logic from application systems
  – centralized administration of security policies
  – independent development and evolution of application and security services
• Generality of the solution
• Policy-neutral
• Support for request-specific factors
Further Information

- “CORBA Security: An Introduction to Safe Computing with Objects” by Bob Blakley
- “Instant CORBA” by R. Orfali, D. Harkley, and J. Edwards
- CORBASEC FAQ http://cadse.cs.fiu.edu/corba/corbasec/faq/
- corba-security@cs.fiu.edu
- CORBA security specification
- RAD project
  http://cadse.cs.fiu.edu/research_projects/research3/