CORBA Security Semantics

Javier Thayer

The MITRE Corporation

Bedford, MA

1 March 1997

Work supported by NSA and by NIMA, through the MITRE Open Systems Center.

MITRE

CORBA as Architecture

- View of information system as units interconnected by Abstract Interfaces.
- The design of the units is facilitated by Inheritance and Polymorphism.
- Units usually have an implicit semantics or informal semantics.
- Semantics often left to implementors.

IDL Specification

- Interfaces are declared using Interface Definition Language.
- IDL formal specs are essentially signature declarations.
  - Only types of arguments, return values and exceptions are specified.
- Expedient: No need for costly and usually uninformative formal analyses.
- Convenient: Diverse vendors are more likely to agree on a specification.

MITRE

IDL Underspecification

- **Particular Methods or Services have intended behavioral requirements associated to them**
  - `CircleBank.ReduceBalance(314159265, 49.95).`
  - `BajaVistaData.Subscribers(BostonGlobe, 01803)`
  - `FlightController.SafeDistance(CurrentSpeed())`
  - `ORB.HasAccess?(GetCurrent(),Request)`
- **Unexpressive: IDL cannot formulate intended behavioral requirements for object methods.**
- **Interoperability "Meltdown": Clear issue for safety or security critical object services.**

MITRE

Semantic Specification

- **Interpretation of specification in some model.**
- **Provide useful information about system to implementors, designers and customers.**
  - `Bank.ReduceBalance(Acct, Bal).` **Reduces amount in acct by Bal.**
  - `DBase.Subscribers(Paper, AreaCode)` **Returns list of subcribers.**
  - `Controller.SafeDistance(S)` **?.**
  - `ORB.HasAccess?(Current, Request)` **?**

MITRE

Four types of Reference Models

- Model for information system.
- Model for safety hazards or security threats.
- Model for protection or countermeasures.
- Model for designing protection facilities.

MITRE

Security Threat Models and Analogues

- Model for security threats:
  - Inappropriate access or information flow.
  - Inappropriate modification or use of data.
  - Undesirable loss or unavailability of resources.
- Model for safety hazards:
  - Physical hazards.
  - Component failure.

MITRE

Countermeasure Models and Analogues

- Security Threat Countermeasures
  - Encryption.
  - Signature.
  - Access Control
- For Safety hazards:
  - Linear motion with random autonomous displacements.
  - Fault Tolerance.

MITRE

Reference Modeling Concepts

- Any computational paradigm suitable (OMT, CSP, State Machines.)
- Partial or "lightweight" formal methods for various reference models.
  - Partiality in composition: For instance, avoid concurrrency issues.
- Design Reference Model for implementors
- Reference Models useful for creating specification simulators.

MITRE

Examples

- Bell-LaPadula and Non-Interference models provided three of the "reference models" mentioned above: Information system model, threat model, protection models.
- Original model state-machine based, many subsequent refinements based on other methodologies, including CSP.
- Much original research into Computer Security resulted in an attempt at building more accurate threat models.
- Very difficult to build real world systems in rigorous conformance to design specification.

MITRE

CORBA Security Issues

- Access Control.
- User Authentication.
- Security of communication
- Auditing.
- Non repudiation.
- Security Domains.

MITRE

Access Control

- Extends and Refines File Access Control Concepts.
  - Control on Method types.
  - Control on Method Arguments.
  - Control on Transaction Principal.
  - Delegation Policies can modify Principal access rights during a transaction.
- Access control model
  - Model various access policy types.
  - Model associations between clients and objects.

MITRE

Needed Work

- Determine behavioral specification methodology for CORBA Object Services.
- Translate informal semantics of various access control policies and design models into a behavioral specification.
- Use behavioral specification to develop useful criteria for product conformance.

MITRE