Access Control in Multidomain Environments

Arif Ghafoor
School of Electrical and Computer Engineering

4/27/2001

Basics

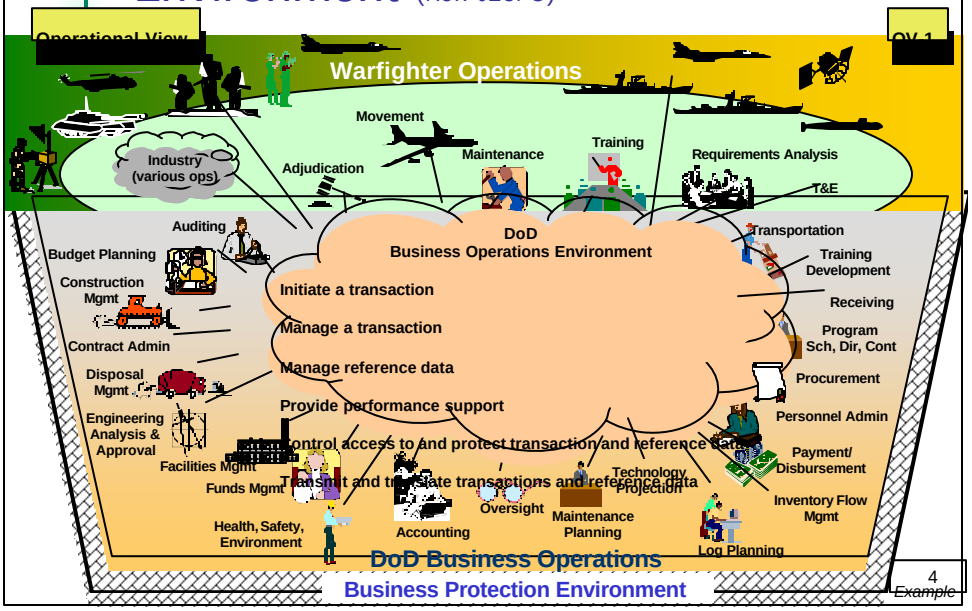
- Access control
  - Restrict access to system entities to authorized personnel
- Security Domain
  - A bounded group of subjects and objects under a single security policy
- Multidomain Secure Environment
  - Ensuring a secure interaction among participating domains

Current Systems

- Single domain systems
- Multidomain systems
  - Open Interconnected Heterogeneous Systems
    - Web applications, E-Government, Global enterprises

3

DoD Business Operations Environment (Ref: JECPO)



4

Example

Discretionary Access Control (DAC)

- Subjects have ownership over objects
  - A subject can pass access rights to other subjects at his discretion
- Highly flexible and currently most widely used
- Not appropriate for
  - high assurance systems, e.g., a military system
  - Many complex commercial security requirements
- "Trojan horse" problem

5

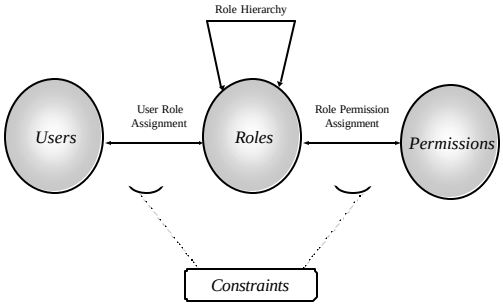
Mandatory Access Control (MAC)

- Subjects/objects have security levels forming a lattice
- Flow of information is restricted.
  - Example: (*no-readup*), (*no-writedown*)
- Well-know MAC model is the Bell-LaPadula model

6

Role Based Access Control (RBAC)

- Access control in organizations is based on roles that individual users take on as part of the organization.
  - A role is "is a collection of permissions"



7

Advantages of RBAC

- Allows Efficient Security Management
  - Administrative roles to manage other roles
  - Role hierarchy allows inheritance of permissions
- Principle of least privilege
  - Minimizes damage
- Separation of Duties constraints
  - Prevents fraud
- Grouping Objects
  - Permissions can be grouped according to a class of objects
- Policy-neutrality
  - Provides generality

8

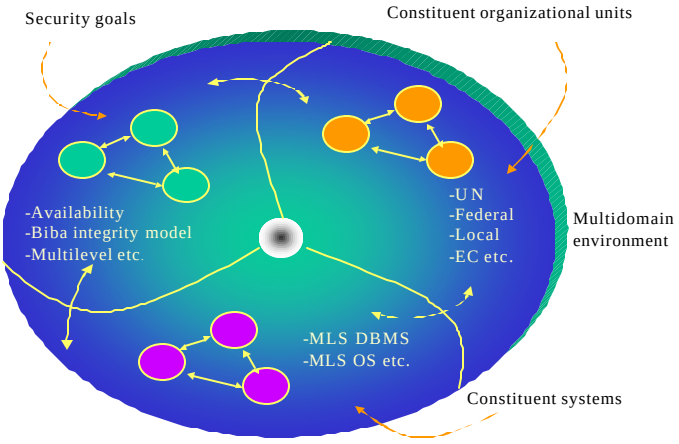
Advantages of RBAC

- Encompasses DAC and MAC policies
- Potential for use in multidomain environment
  - Open interconnected systems
    - Similarity of role concepts
    - Provides a generic representation of security policies

9

Multidomain Environments

- Dimensions of heterogeneity



10

Key Access Control Challenges in a Multi-Domain Environment

- Semantic heterogeneity
- Secure interoperation
- Assurance and risk propagation
- Security Management

11

Semantic heterogeneity

- Different systems may use different security policies
  - e.g., DAC, MAC, Chinese wall, Integrity policies etc.
- Variations of the same policies
  - e.g., BLP model and its several variations
- Naming conflict on security attributes
  - Similar roles with different names
  - Similar permission sets with different role names
- Structural conflict
  - different multilevel lattices / role hierarchies

12

Secure Interoperability

- Principles of secure interoperation

  Principle of autonomy

  - If an access is permitted within an individual system, it must also be permitted under secure interoperation in a multi-domain environment.

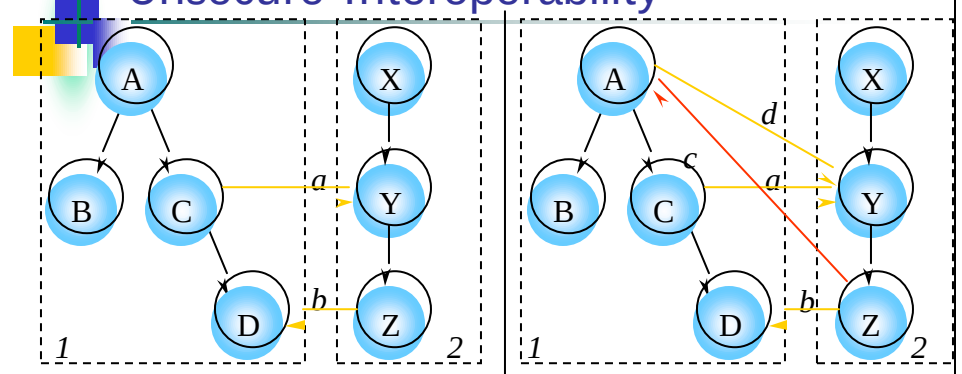
  Principle of security

  - If an access is not permitted within an individual system, it must not be permitted under secure interoperation.

- Interoperation of secure systems can create new security breaches

13

Unsecure Interoperability



F_{12} - permitted access between systems 1 and 2

(1) F_{12} = {a, b, d} Direct access

(2) F_{12} = {c}

14

Challenges in Secure Interoperability

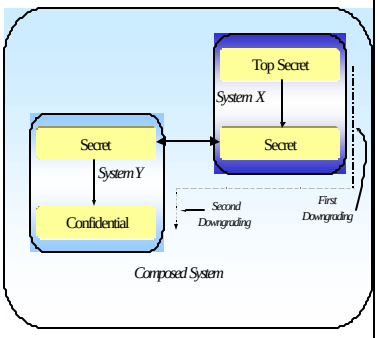
How to ensure autonomy and security principles?

- Determining inconsistencies/incompleteness in security rules.
- Identifying security holes
- Selecting optimality criteria for secure interoperability: maximizing number of domains, direct accesses

15

Assurance and Risk Propagation & Security Management

- Assurance and Risk propagation
  - Breach in one domain can render the whole environment insecure
  - Cascading problem
- Security Management
  - Centralized/Decentralized
  - Managing global metapolicy
  - Managing policy evolution



16

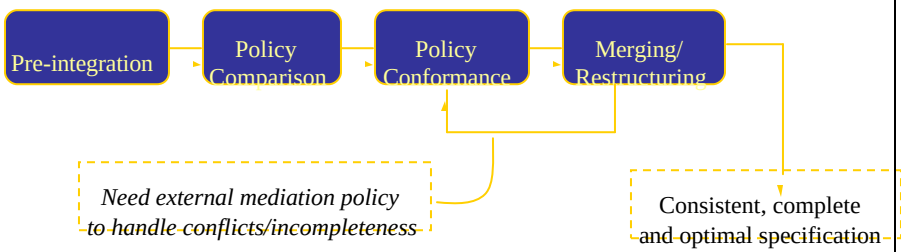
Approaches to Multidomain Problem

- Policy-Metapolicy specification framework
  - Ad-hoc, Formal models: lattice merging, RBAC
- Agent based approach (Policy agents)
- Architectural approaches (CORBA, DCE)

17

A Multi-Domain Access Control Framework

- A Multi-Phase Framework
- Based on Generalized RBAC (GRBAC) model
  - Temporal and Non-temporal constraints



18

Pre-integration Phase

- Requires GRBAC representation of arbitrary policies. A policy mapping technique is needed for non-RBAC systems.
- Uses an information base
  - Semantic information about domains including policies, roles and attributes
  - Integration/merging strategies to generate the overall configuration of the multi-domain environment.

19

Policy Comparison and Conformance

- Tools & techniques for detecting
  - Semantic conflicts
    - Naming conflicts
    - Structural conflicts
  - Rule conflicts
- Mediation policies are needed for resolution
  - Predefined meta-policies
  - Domain cooperation by administrators
- Tradeoffs
  - Determine optimal/heuristic solutions secure interoperability

20

Merging/Restructuring

- Merging/integrating policies
  - Restructure domain policies according to the selected optimal criteria
  - Generate integrated global policy
- Repeat policy conformance step
  - Re-evaluation and restructuring of meta-policy

21

Conclusion

- Emerging distributed and Web applications have significant security challenges due to heterogeneity of underlying domains.
- Novel solutions and techniques are needed to allow secure interoperability and integration of multiple systems

22