SPECIFICATION AND DEVELOPMENT OF AN AUTOMATIC AND SECURE MULTIMEDIA DOCUMENT SYSTEM

Professor:Arif Ghafoor
Student: James Joshi

CERIAS
&
Distributed Multimedia Systems Lab
School of Electrical and Computer Engineering
Purdue University, West Lafayette, IN

Motivation

- Rapid growth of *Multimedia Applications*
- Trends towards *Large Open Distributed Systems*
- Need for efficient *storage*, *access* and *management* techniques for large archives of Distributed Multimedia Documents
- Complex Security Issues - *multiple domains*, *multiple security policies, multiple data types*
- A need for an *Integrated Framework* for Multimedia Document Specification

Research Objectives

- Security Issues for Multimedia Information Systems
  (*Authorization*/*Access Control* issues)
- Security Specification Mechanisms
- Automatic analysis techniques
  (*safety, consistency, completeness* etc.)
- Efficient query techniques
- Clustering techniques based on Security attributes
  (for *efficient access* and *storage*)

Some Key Issues in Multimedia Systems

- Synchronization of multimedia objects
- Quality of Service Requirements (QoS)
- Security (*Access control*)

An integrated framework for the specification and analysis of these requirements are highly desirable

Our Solution : Petri Net Based Model

Because of

Graphical nature, Ease of concurrency modeling,
Well-established mathematical base

Generalized Object-Composition Petri-Net Model (GOCPN)

- Multimedia Document Composition Model for
  - *Spatial/Temporal Synchronization (including Lip-Sync)*
  - *QoS, QoP specification and Resource allocation*
  - *User Interactivity*
  - *TAC operations*
  - *Hierarchical modeling*
  - *Multimedia Storage*

- Some other related Petri-net models
  - *Interoperable Petri-Net (IPN) in MediaWare - addresses Interoperability of Distributed Objects (uses Synchronization Agents)*
  - *Transitional - OCPN (TOCPN) - interactive temporal structure*
  - *Distributed - OCPN (DOCPN) - Use of priority to model Distributed Teleorchestration*

Security Models and a possible Classification and Combination

[*Fernandez et. al*]

Classification based on

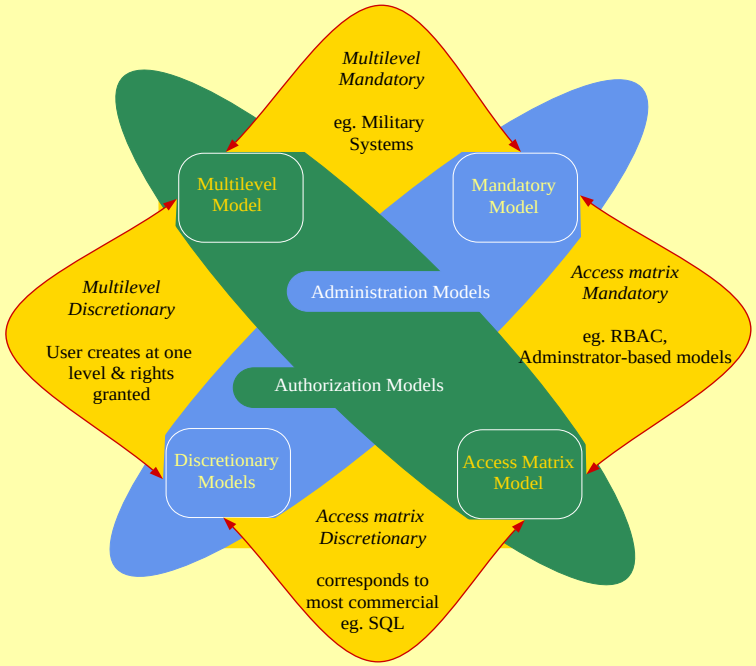
- *Approach to Authorization*

  Multilevel Models
  Access-matrix Models

- *Origin of Access rights*

  Mandatory Models
  Discretionary Models

- *Orthogonal and can be combined to produce four possible policies*



Our Current Focus

Formalizing Specification, Analysis and Verification of secure multimedia documents using GOCPN

- Access Control Operators
  - *Logical operations, Other Common access control structures*
- Access Control based on Inter-Object Dependencies
  - *Control Flow Dependencies, Temporal Dependencies*
- Multilevel Security Specification
  - *Multiple Domains (multipolicy paradigm)*
  - *Incremental composition*

We have proposed a Multilevel Security Specification Mechanism for multimedia documents

Access Control Based on Inter-Object Dependencies

Table 1: Inter-Object Dependencies

Dependency Type	Explanation/Sample Statement
Exclusive access	Accessing n out of N objects (n <= N)
Precedence	Given access to O1 and O2, O1 must precede O2
Strong Causal	O2 is allowed to be accessed only if O1 is allowed to be accessed
Weak Causal	O2 must be accessed if O1 is accessed
Temporal	-Relative (O2 is given access t time units after O1 is given access) -Absolute (O1 is given access at time 10 am on Mon, Fri)

Formalism needed to address complex dependency scenarios arising from these!

Some Problems to address: Conflicts and Dependency constraint satisfaction

We are currently formalizing analysis techniques using
Siphon detection and Reachability analysis

Multilevel Security Specification for Multimedia Documents

Colored GOCPN - Our proposed extension to GOCPN for allowing multilevel security specification of preorchestrated documents

Multiple Security Domains

- each *security domain* represents the scope of a *security policy*
- introduces *inter-domain* constraints (currently being studied - *Metapolicies*)
- domains may contain subdomains

Colored-GOCPN

- *Colored tokens* repesent authorized tokens carrying clearance level of a subject
- *SPlace*, *Gate-transtions* and *EPlace* provide the mechanism for access control
- *Authorization module* (*AM*) checks/generates authorized tokens
- Each pair of *SPlace*, *EPlace* is associated with a domain
- An *AM* is associated with a *security domain*
- A *set of places* represent a multilevel object corresponding to each level
- *MultiView* model of Object Oriented database provide the most direct support.

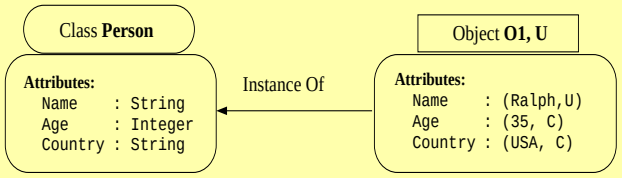
Multilevel Security Specification for Multimedia Documents

Basic Bell-LaPadula

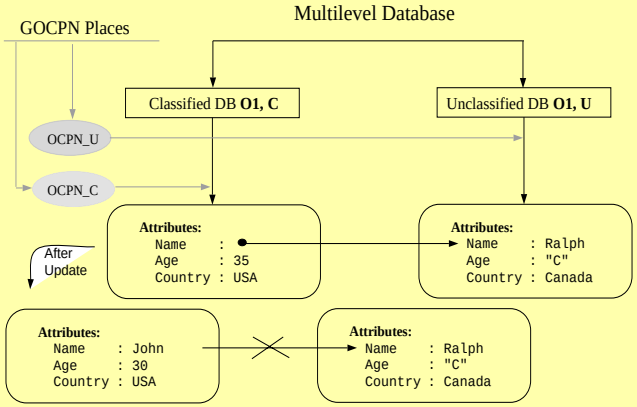
- *Simple property(no read-up)*
- **property(no write-down)*

MultiView Model of OO databases[*Cuppens et. al*]

- *decomposes n-level OO database into n-views*
- *each view is for a given classification level and contains lower or equally classified data*



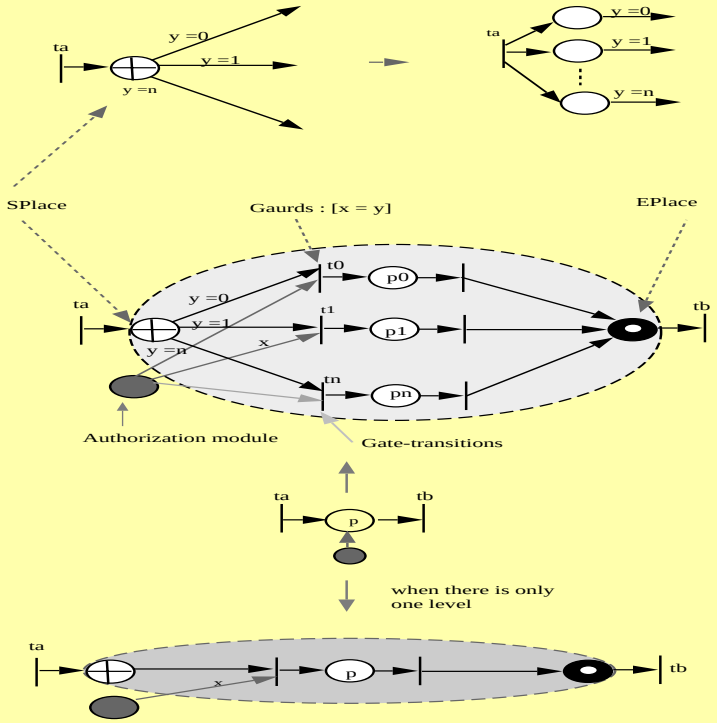
MultiView Model - Object Creation



MultiView Model - View for each level

Multilevel Security Specification for Multimedia Documents

- *p0 - default place, accessed when Subjects are not cleared*
- *SPlace, EPlace act as security Boundary*
- *SPlace generates (n+1) colored tokens*
- *AM generates one auhtorized token*
- *A transition gate fires if guard condition is met (token from SPlace and AM match)*

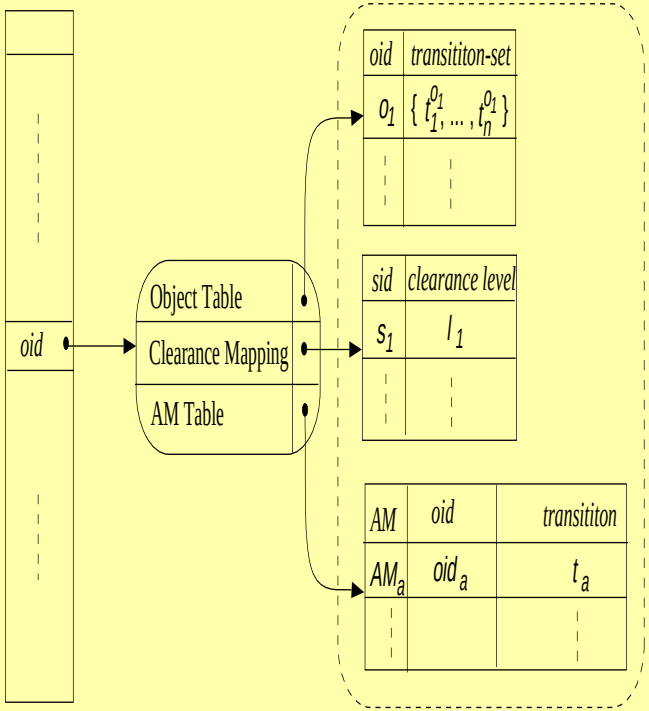


Multilevel Security Specification for Multimedia Documents

Each AM maintains information about

- Objects - *atomic, composite and those recognized* - in its domain
- *Constituent objects* and associated *AMs* incase the constituent objects are under other domains
- *Clearance* Mapping for subjects

One way of organizing the information is as shown in this figure. *oid* is the object (document id) recognized by an AM. *Object Table* lists the constituent objects from the current domain, *AM Table* lists the constituent objects in other domains and their associated AMs



Colored-Tokens

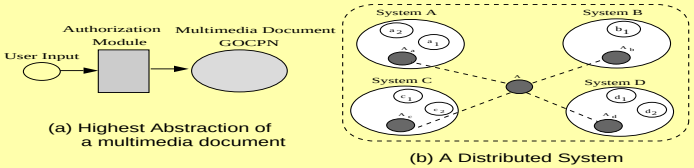
Colored Tokens

- Let S_{sid} be the set of *sid* and let S_{oid} be the set of *oid*s

Tokens and color sets as follows:

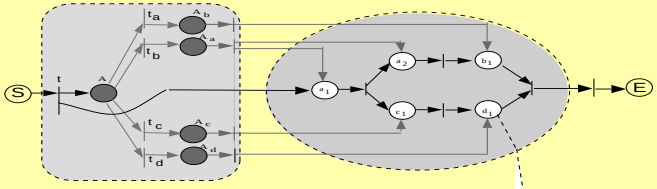
- $token_d \in S_d = \{(sid,oidset) | sid \in S_{sid}, oidset \subseteq S_{oid}\}$
  is the *default token* OR *authorization-request* token
- $token \in S_i = \{(sid,oid, l) | sid \in S_{sid}, oid \in S_{oid}, l \in s_i\} \cup S_d$
  is the set of all tokens an *AM* or a *SPlace* can generate, it depends on the security domain that the *AM* and *SPlace* represent. The set $S_i - S_d$ is the set of the *authorization tokens*.

A Simple Example

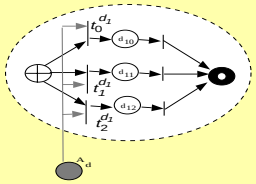


(a) Highest Abstraction of a multimedia document

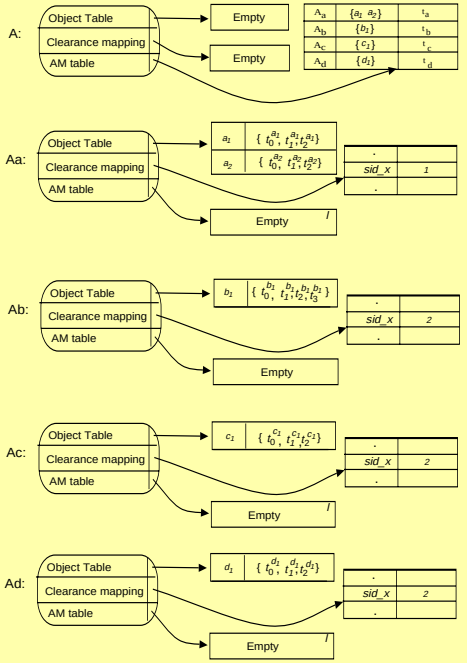
(b) A Distributed System



(c) colored-GOCPN document



(d) MLP-net of d1



Summary and Future Work

Current Status

- We have proposed a Multilevel Security Specification Mechanism for multimedia documents using colored-GOCPN
- We are currently looking at information flow control issues

Future work

- Generalization of the extended specification model to handle
  * inter-domain constraints
  * multiple policies (DAC, MAC, RBAC etc)

- Multimedia database security issues to enhance support for application level specification and security enforcement
- Implementation