CERIAS Tech Report 2000-09

A Petri-net based multilevel security specification model for multimedia documents

J. Joshi, A.Ghafoor
Center for Education and Research in
Information Assurance and Security
&
School of Electrical and Computer Engineering,
Purdue UniversityWest Lafayette, IN 47907

A Petri-net based multilevel security specification model for multimedia documents*

J. Joshi, A. Ghafoor

Center for Education and Research in Information Assurance and Security &

School of Electrical and Computer Engineering,

Purdue University, West Lafayette, IN

{joshij, ghafoor}@ecn.purdue.edu

Abstract

With the growing need for multimedia data management, security requirements are becoming very crucial. Composing multimedia documents involves bringing together media objects that exist in various formats. These objects may reside in a distributed environment and belong to different security domains. We propose a time augmented colored-Petri Net model for multimedia document composition that allows the specification of multilevel security. The model also allows handling multiple security policies and hierarchical and path-based protection schemes.

1.0 Introduction

Recent advances in high-performance computing and networking technologies have allowed the emergence of many distributed multimedia applications in medicine, education, digital libraries, e-commerce, etc. These applications are mainly expected to use pre-composed multimedia documents. A multimedia document consist of various media types such as text, audio, image and video. These may be stored in a central archive or distributed over various servers that are interconnected by a broadband network. These objects may belong to different security domains. Each security domain represents the scope of a security policy under different security administration [1]. Composing a multimedia document from these media objects poses the challenge of enforcing multiple security policies. Need for security and access control to individual components can be easily seen in various multimedia applications. For example, a WWW site for distance learning needs to protect access to various components of a multimedia document based on the user category. A course coordinator and a registered student have access to different components of the composite course document. Another example can be drawn from a medical application. Medical records for patients will have various information, X-rays and video scans that need to be protected from unauthorized personnel. At the same time fast and efficient access to specific patient information by a physician may be very critical.

Petri Net model has been found very useful in modeling concurrent computation and complex processes[2]. It has been extended in Generalized Object-Composition Petri Net (GOCPN) to model multimedia synchronization[3][4][5][6].

Several security models have been proposed and applied for developing secure computing systems[7]. Access control mechanism is broadly categorized as discretionary access control(DAC) and mandatory access control (MAC). DAC allows access restrictions that are subject to user discretion, while MAC does not.

In this paper, we present a colored Petri Net based information model that extends the capability of GOCPN by allowing security specification to control access to multimedia documents at the time of presentation. We assume a simplistic model of a trusted user[8] or group of users preparing a multimedia presentation that allows viewing documents from the various security levels where users are not meant to modify the presentation unless they are at the same trusted security level group. We use the multilevel security model to classify different multimedia objects. The paper is organized as follows. In Section 2, we introduce the concept of GOCPN. In section 3, we introduce the concept of multiview model of multilevel security. In section 4, we present the proposed colored-GOCPN. In section 5 we conclude with a discussion on future research.

2.0 Petri Net models of Multimedia

Petri nets have been widely used for modeling and analysis of systems that are characterized as being concurrent, asynchronous, distributed, parallel and nondeterministic[2][9]. Various factors contributing to their success include their graphical nature, the simplicity of the model and the firm mathematical foundation. It also provides modularity in design. Time intervals can be used to describe the presentation of multimedia documents. There are all together 13 possible temporal relationships between two time intervals. Little and Ghafoor[6] used the 13 temporal relationships between two time intervals to specify the synchronization among the media objects.

2.1 GOCPN Model

Basic OCPN[4][6] and XOCPN have been augmented in [3] to GOCPN. GOCPN can be used to model the spatio-temporal synchronization constraints, user interaction, lip-sync operations and TAC operations.

Definition: A GOCPN is a 10-tuple $G = \{P, T, A, AW, PO, PD, PS, POp, TF, SL\}$.

$P = \{p_1, p_2, .., p_m\}$ is a finite set of places with $m \geq 0$. $T = \{t_1, t_2, .., t_n\}$ is a finite set of transitions with $n \geq 0$ and $P \cap T = \Phi$. $A =$ $\{P \times T\} \cup \{P \times T\}$ is a mapping representing arcs between places and transitions. AW: $A \rightarrow B$, $B = \{0, 1\}$ is a weight function of arcs; It is used to determine the token flow and firing condition of the net. PO: $P \rightarrow \{C \times Q\}$ is a mapping of places to the content set C and QoP (Quality of Presentation) set Q. PD: $P \rightarrow D$ represents playout duration of the media object with D as the integer set. PS: $P \rightarrow S$ represents the spatial information of the media object. POp:

*Portions of this work were supported by sponsors of the Center for Education and Research in Information Assurance and Security (CERIAS)

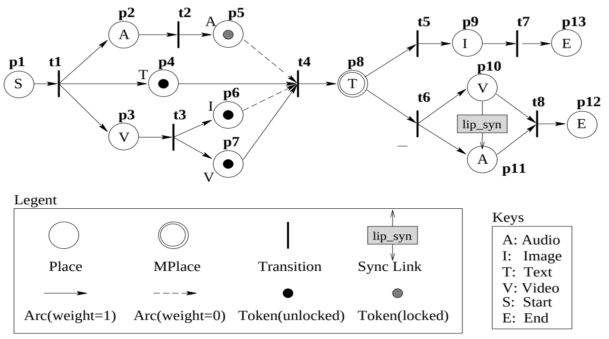


Fig 1. An Example of GOCPN

$P \rightarrow Op$ defines media operations. *SL*: $\{P \times P\} \rightarrow I$ represents lip-sync link between two places. *I* is an integer set that represents maximum skew allowed between two media objects measured by discrete time units. *TF*: $T \rightarrow \{AType, EType\}$ differentiates transition types by its firing rules. For *Atype* transition, its firing mode is automatic(A). For *Etype* transition, its firing mode is event-driven(E). *SL*: $\{P \times P\} \rightarrow I$ represents lip-sync link between two places. I is an integer set representing maximum skew allowed between two media objects measured by discrete time.

An example of GOCPN structure is depicted in *Figure 1*.

Arcs drawn as solid lines are *active* arcs and have *AW* = 1. Those drawn as dashed lines are *inactive* and have *AW* = 0. The firing rule for GOCPN is as follows:

- A transition *t* fires if each of its *active* input place *p* has atleast *AW(p,t)* unlocked tokens.
- A transition fires immediately if it is *AType*; if the transition is *EType* it fires only when triggered by the input place.
- Firing transition results in removal of a token from each input place and depositing a token to each output place
- A place starts the presentation of associated object after locking a token. The token is unlocked if the duration *PD(p)* expires or the end of the media stream is reached.
- The *lip-sync* link indicates enforcing strict synchronization between linked objects within allowable skew specified by *SL*.

In *Figure 1*, the transition t4 is enabled because each of its *active* input places p4 and p7 has an unlocked token indicated by black inner oval. t4 fires immediately and terminates the media presentation in places p5 and p6 by removing a token from them.

3.0 Security Mechanism for Multimedia

Multimedia objects such as video clips, audio files or images and documents, can be isolated objects stored within a single computer or distributed in a large number of interconnected systems. These objects may belong to different security domains. Bringing together such objects for the composition of a synchronized presentation poses considerable technical challenge in terms of enforcing multiple security constraints.

3.1 Multilevel security

Multilevel security has been proved to be a practical model for many military and commercial applications where some form of natural hierarchy or compartmentalization exists. Distribution of information in such organizations is controlled by some measure of *sensitivity* or on *need-to-know* basis. The *sensitivity* of information is determined by its content, context, aggregation or time[10]. It is required to effectively ensure that users can access only the information for which they have the required clearance. The multilevel access control is enforced by defining a binary relation $'\geq'$ or '*dominates'* between the *clearance level* of an *active* entity(*subject*) and the *classification level* of a *passive* entity(*object*). For security levels l_1 and l_2, $l_1 \geq l_2$ means that l_1 *dominates* l_2.

3.2 Multiview model of multilevel security

Multilevel database security is an active area of research and related work can be found in[10][11]. Here we briefly explain the multiview model proposed in [11], which we use to provide secure access to multimedia objects by using the augmented GOCPN.

In this model the assignment of classification levels are done at the object level (instances). We use an example to illustrate this. Assume 2 levels of classification applied to an object - *Classified*(C) and *Unclassified*(U) as in *Fig 2*. User A with a clearance for unclassified level creates an object O_1 and assigns to attribute **Name** the classification U and to attributes **Age** and **Country** the classification C. O_1 is given the sensitivity level U. As **Age** is classified at C, he may put a '*cover story*'. In the Classified database, pointers to the same object state in Unclassified database are created. For any attribute classified as C, the actual value is copied. Thus as shown in *Fig 3,* for a user with clearance U, the attribute **Age** is hidden and attributes **Name** and **Country** are visible. However, he is unaware of the fact that value for **Country** is a '*cover story*' and thinks **Country** is an unclassified attribute. If later, A updates the classified information, he only updates the object state which is stored in the classified database. For example, A can use his clearance C to change the value of **Name** to 'John' in the classified database. The value 'Ralph' in the unclassified database now becomes a '*cover story*'.

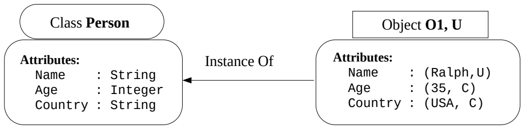


Fig 2. Multiview model: Creation of an object

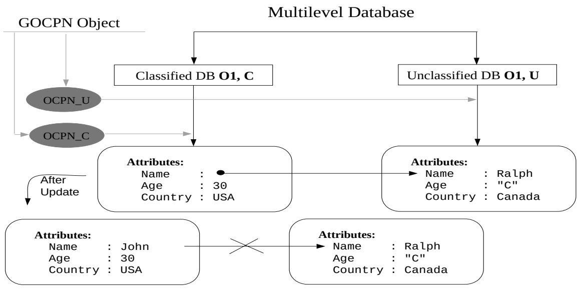


Fig 3. Multiview model of security

4.0 Augmented GOCPN

To incorporate selection based on the clearance level of the users, we introduce addition of the colored tokens. transition guards and arc expressions into GOCPN model. We augment the GOCPN as follows.

Definition: A *colored-GOPCN* is a *14-tuple* $G_c = \{G, \Sigma, C_p, G_t, E_a\}$ Where: G refers to the 10-tuple of GOCPN defined earlier. We make *PT*: $P \rightarrow \{regular, decision, SPlace, EPlace\}$. $\Sigma : \{S_d, S_{s_1}, S_{s_2}, \ldots, S_{s_n}, S_{AM}\}$ is a finite set of non-empty types called colors which will be discussed in section 4.3. C_p: $P \rightarrow \Sigma$ is a color function. G_t: $T \rightarrow B_E$ is a guard function defined from T into boolean expressions B_E such that $\forall t \in T : [Type(G_t(t)) = Boolean \wedge Type(Var(G_t(t))) \subseteq \Sigma]$.
E_a: is an arc expression from A to expressions such that $\forall a \in A : [Type(E_a(a)) = C_p(p(a)) \wedge Type(Var(E_a(a))) \subseteq \Sigma]$.

Each token represents a color (type). A color carries the information about the identity of the subject and/or the security clearance on each objects. To make the modeling systematic and modular we introduce special places *SPlace* and *EPlace*, and a special type of transition called a *Gate-transition*. We also introduce *Authorization Module* (AM) for generating authorizations for access to places.

4.1 Security Boundary and Access Control

A *SPlace* indicates the start of a *security domain* and is associated with a color set. A *Gate transition* is a transition that is between a *SPlace* and an object with a given classification. A *Gate-transition* has a guard expression [x=y] where x is the token from AM and y is the token from its input *SPlace*; if the tokens match, the transition fires allowing access to its associated object. As shown in *Fig 4*, the token between *SPlace* and p_i carries a colored token that has level information i. The places $p_1, p_2, .., p_n$ in *Fig 4* represent the same object classified at n different classification levels each protected by a *Gate-transition*. For example p_1 can be OCPN_U in *Fig 2*. An *EPlace* represents the end of the security domain. Thus, *SPlace* and *EPlace* define the security boundaries of a *security domain*, while a *Gate-transition* acts as security check points for access to objects. As shown in *Fig 4*, we refer to the multi-level view of a place with its *SPlace, EPlaces, Gate-transitions* and with views of objects at different classification levels as *MLP-net*. In *Fig 4*, the grayed GOCPN is the *MLP-net* of the place p shown in the left. We define a *default token* as the element of S_d . All the arcs other than those between *SPlaces* and associated *Gate-transitions*, and that occur in AM are assumed to carry a *default color*. The guard expressions of transitions other than *gate-transition* is assumed to be TRUE. Thus when all *MLP-nets* are abstracted by their places, only the *default token* flows through the GOCPN describing the document.

4.2 Authorization Module

As shown in *Fig 5*, a multimedia document may be composed of distributed objects residing in different systems and security domains. For example, objects a_1, a_2 belong to system *A*, b_1 belongs to system *B*, c_1 belongs to system *C* and d_1 belongs to system *D*. These objects can be put together to form a multimedia document as shown in *Fig 5(c)*. The *Fig 5(a)* shows the top level view where AM is shown as a substitution transition. The expanded view of the Authorization module *Fig 5.c(i-iv)* shows that it is composed of a number of sub AMs that handle authorizations within individual security domains. Module A handles the top level authorization and sends authorization requests to A_a, A_b, A_c and A_d. This includes sending the *userid* and *objectid*. Each sub-module does authorization checks and sends appropriate tokens (or authorization requests) to the associated *Gate-transitions* (or to its sub-AMs). For example A_d generates tokens for the three level *MLP-net* of place d_1. System *D* itself can be a distributed system and place d_1 can itself be a an abstraction of another GOCPN in which case AM_d may need to issue authorization requests to its sub-AMs. We assume that an AM generates appropriate tokens if a user is to be authorized to access an object at some sensitivity level.

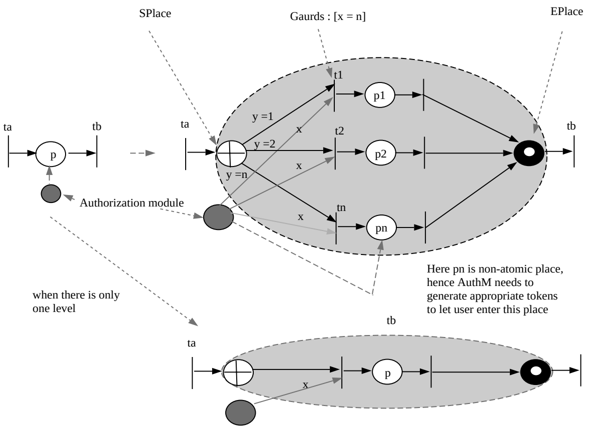
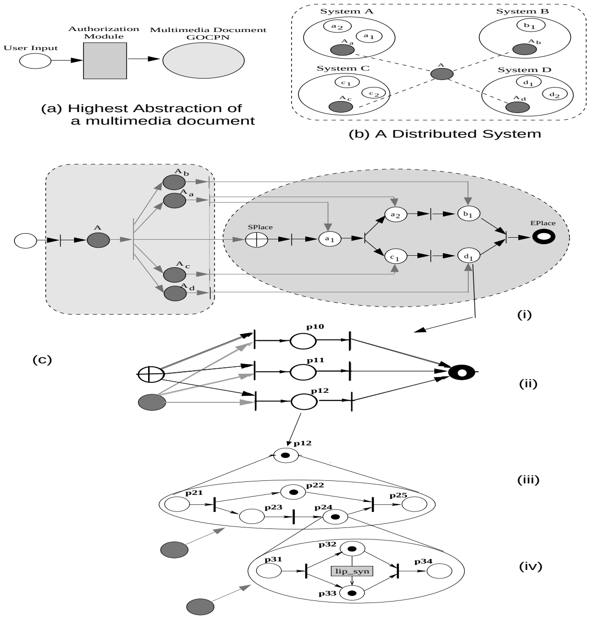

SPlace
Gaurds : [x = n]
EPlace
ta
tb
p
ta
t1
p1
y =1
y =2
y =n
x
t2
p2
x
tn
pn
x
tb
Authorization module
Here pn is non-atomic place, hence AuthM needs to generate appropriate tokens to let user enter this place
when there is only one level
tb
ta
p
x

Fig 4. Colored GOCPN

4.3 Colored Tokens

For the colored-GOCPN to be powerful enough to model both the document structure and AM, we require that *sid*(for subjects), *oid* (for objects) and the *clearance* levels of a *subject* be incorporated in the tokens. We construct the color sets as follows. Let s_1, s_2,.., s_n be such that s_i is the set of security levels of i^{th} security domain, where n is the number of security domains. Let s_0 be a one member set such that its element can represent the lowest level of any of the sets s_1, s_2,.., s_n. Let S_{sid} be the set of *subjectids*. Let S_{oid} be the set of *objectids* (name of places). We enforce the following in the colored-GOCPN: $token \in S_d = \{(sid, oids) | sid \in S_{sid}, oids \subseteq S_{oid} \cup s_0\}$ is the set of *authorization request* and *default tokens (*when *oids* is the



(a) Highest Abstraction of a multimedia document

(b) A Distributed System

Fig 5. GOCPN and Distributed System

element in s_0. For an associated security domain s_i, a *SPlace* generates $|s_i|$ tokens, one for each element of s_i and sends one to each gate-transition. The token generated is of the form $token \in S_{s_i} = \{(sid, oid, l) | sid \in S_{sid}, oid \in S_{oid}, l \in s_i\}$. Let $S = \{(sid, Sub_{oid}) | sid \in S_{sid}, Sub_{oid} \subseteq S_{oid}\}$. An AM generates $token \in S_{AM} = \bigcup_{i=1}^{n} S_{s_i} \cup S$. Mainly two forms of tokens are generated - one form is the same as the tokens generated by *SPlaces*. $|s_i|$ such tokens of same value are generated and sent to the associated *gate-transitions*, where s_i is the security domain associated with the corresponding *SPlace* and the *gate-transitions*. The second form is used when an AM sends an *authorization request* to the sub AMs.

Example: We revisit *Fig 5c(i)*. Here we assume that each object is atomic and has 3 security levels - 1, 2 and 3. The *sid* (*Fig 6*) is used as user input. t_1 receives a default token *(John, 1)* where $s_0 = \{1\}$. t_1 fires and sends the default token to place A. A sends four different tokens to t_2 (same as the collection of tokens sent out from t_2) which are sent to A_a, A_b, A_c and A_d as shown - e.g. token *(John, {a_1, a_2})* sent to A_a. Each of t_a, t_b, t_c and t_d receives tokens from its AM places(same as those on the output arcs) which are sent to *Gate-transitions* of the *MLP-nets* of their respective output places. For example, t_a receives tokens *(John, a_1, 2)* and *(John, a_2, 2)* which are sent to the *Gate-transitions* of *MLP-nets* of places a_1 and a_2. This inherently has the path based access control. For example to reach d_1, a_1 and c_1 must be reachable first.

Now assume that d_1 can be expanded as in *Fig 5c(i)-(v)*. Assume that the *p22* is an abstraction of another GOCPN in another security domain (sub domain for security domain represented by A_d). Thus after authorizing access to place *p12* in *Fig 5c(ii)*, A_d needs to check authorization for place *p22*. Thus to access GOCPN represented by *p22*, three levels of authorizations are needed. Furthermore, path at the top level - a_1 followed by c_1 - needs to be followed before d_1 can be accessed, followed by access to *p12* and then *p22*. Thus we see that a combination of both path based and hierarchical protection schemes can be achieved.

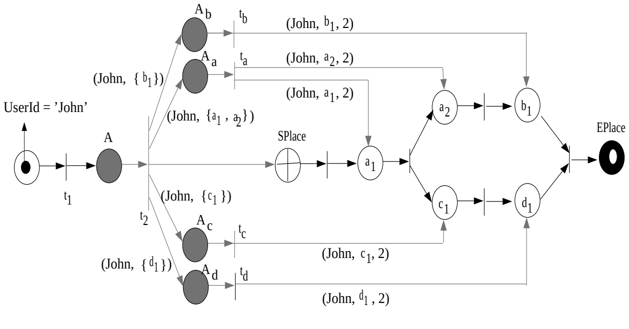


Fig 6. An example

5.0 Conclusion

Multilevel secure multimedia documents have many applications. Media objects composing a multimedia document come from databases, independently existing files and over the network. This diversity necessitates handling multiple protection schemes. We have augmented GOCPN with colored tokens that carries authorization information and allows hierarchical modeling of media objects from multiple security domains. It is assumed that the multimedia objects are pre-orchestrated before they are published for viewing.

Each authorization module encapsulates an important processing requirement which needs to be well defined and modeled. [12] propose authorization rules that can be implemented in AMs of the augmented GOCPN using Petri-net models for normal logic forms[13]. Further research involves structured representation of authorization process, conflict resolution, and presentation schedule and searching issues based on security attributes. With a properly modeled authorization module, augmented GOCPN can provide a powerful integrated hierarchical modeling mechanism for structuring multimedia documents that have numerous constraint parameters related to QoS, QoP, interobject synchronization and security.

References

[1] Ahmed Patel, "Security management for OSI networks", *Computer Communication*, vol 17, Jul. 7, 1994

[2] James L. Peterson, "Petri net theory and the modeling of systems", Prentice-hall, 1981

[3] Zhaohui Kevin Li, "Multimedia modeling, indexing and presentation in distributed networked environments", Ph.D. Thesis, Purdue University, Apr., 1998.

[4] T.D.C. Little and A. Ghafoor, "Synchronization and storage models for multimedia objects," *IEEE Journal on Selected Areas in Communications*, vol. 8, no. 3, pp. 443-427, 1990

[5] E. Bertino, E. Ferrari, "Temporal Synchronization Models for Multimedia Data", *IEEE Transactions on Knowledge and Data Engineering*, vol. 10, no. 4, Jul./Aug. 1998.

[6] T.D.C. Little and A. Ghafoor, "Interval-based Conceptual Models for Time dependent Multimedia Data", *IEEE Transactions on Knowledge and Data Engineering*, vol. 5, no. 4, pp. 551-563, Aug. 1993.

[7] C.E. Landwehr, "Formal models of computer security", *ACM Computing Surveys*, Sept. 1981.

[8] Li Gong, X. Qian, "Enriching the expressive power of Security Labels", *IEEE Transactions on Knowledge and Data Engineering*, vol. 7, no. 5, October 1995.

[9] K. Jensen, "Colored Petri Nets - Basic concepts, analysis methods and practical use volume 1", *Springer*, second edition, 1996.

[10] A. Baraani-Dastjerdi, J. Pieprzyk, R. Safavi-Naini, "A multi-level view model of secure object-oriented databases", *Data and Knowledge engineering* 23 (1997) pp. 97-117.

[11] N. Buulahia-Cuppens, F. Cuppens, A. Gabillon, K. Yazdanian, "Multilevel Security in Object-Oriented Databases", *Workshops in Computing - Security for Object-Oriented Systems* (eds: B. Thuraisingham, R. Sandhu, T.C. Ting), Washington D.C, 1993.

[12] E. Bertino, C. Bettini, E. Ferrari, P Samrati, "A Temporal Access Control Mechanism", IEEE Transactions on Knowledge and Data Engineering, vol. 8, no. 1, Feb 1996.

[13] T. Shimura, J Lobo, T. Murata, "An Extended Petri Net Model for Normal Logic Programs", IEEE Transactions on Knowledge and Data Engineering, vol 7, No. 1 Feb 1995