A Web-Based Multilayer Access Control Model for Multimedia Applications in MPEG-7

Leon Pan and Chang N. Zhang
(Corresponding author: Leon Pan)

Department of Computer Science University of Regina, TRLabs
Regina, SK Canada S4S 0A2. (Email: {panli111,zhang}@cs.uregina.ca)

(Received Oct. 16, 2005; revised and accepted Nov. 25, 2005)

Abstract

This paper presents a Criterion-Based Role-Based Access Control model in which secure permissions (SP), secure operations (SOp), secure objects (SOb), and secure users (SU) are introduced. The security criterion expressions (SCE) embedded in SOb work as locks and the common elements of the security criterion subsets (SCSS) in SOp and SU work as keys. To support web-based applications, the remote secure user-role assignment is done based on user's digital credential(s), and Compact-Secure-Role-SCSS cookies are adopted to simplify the subsequent transactions. The multilayer access control is achieved by actuating locks with the relevant keys. The proposed model, an extension of traditional RBAC, efficiently supports both multilayer access control and non-multilayer access control on the web.

Keywords: CB-RBAC, compact secure cookie, digital credential, MPEG-7, multilayer access control

1 Introduction

Nowadays, the multimedia data cover more and more application domains, ranging from Digital libraries, E-Commerce, Home entertainment, News programs, Remote sensing, to Multimedia editing. The comprehensive set of audiovisual Description Tools provided by the MPEG-7 [14, 15, 17, 20] standard is to create the descriptions (which are in the form of hierarchy) of the multimedia contents in order to facilitate the needed effective and efficient access to multimedia contents. Since the security requirements of multimedia data are left open in the present MPEG-7, researchers and developers need to explore their own methods to protect the sensitive contents (elements) in the multimedia data.

The properties of the multimedia data and web-based applications cause several special security requirements. Multimedia data usually contain huge amount of elements many of which may have different security levels (e.g. a medical education video should prevent the unauthorized users from identifying the patients' identities), as a result, the security system must support multilayer access control. In addition, the multimedia data are frequently played in real time. Thus, the method of protecting the relatively small number of elements (such as patient's face) among the huge amount of elements should be very efficient in order to meet the real time requirement. Besides, more and more multimedia applications are in the distributed environment, it is desirable to assign the access privilege (permission) to the hundreds of thousands remote users automatically. And last, the ideal security system should take into account and make full use of the properties of the descriptions (called metadata) provided by the MPEG-7.

Several research works can be found in the literature relating to multimedia access control [1, 2, 3, 5, 19]. Some of these works [2, 3] lacks the ability of protecting areas in the frames and some are specific to certain form of multimedia data such as video [1, 3, 5] or image [10]. Another common shortcoming of these works is that they are basically the mandatory access control (MAC) the administrative cost of which is relatively higher. Also, the filtering rules of these systems have to be applied to every sub object to determine which sub object(s) is (are) accessible, which is time-consuming. Moreover, they did not take the full advantages of the MPEG-7.

Compared with Mandatory Access Control (MAC) and Discretionary Access Control (DAC), Role-Based Access Control (RBAC) has several superior properties. It simplifies the security management and administration, and provides more access control functions [12]. However, current RBAC model is not suitable for the fine-grained multilayer access control. In order to satisfy multilayer access control requirements in the current RBAC model, much more roles have to be introduced and different versions of a same object (each of which corresponds to a specific security requirement) have to be generated and stored, which not only significantly increase the administrative costs but also cause the datum integrity problem (e.g. when the content of the different versions of the same object are found to be inconsistent, it is difficult to decide which one contains the correct content).

Based on the above observations, a Criterion-Based RBAC (CB-RBAC) model is proposed to support the web-based multilayer access control in MPEG-7. In the proposed model, we introduce a number of new components which are the secure permissions (SP), secure objects (SOb), secure operations (SOp) and secure users (SU). A secure permission is made up of a secure object and a secure operation. A secure object is composed of a number of secure sub objects each of which is a sub object embedded with a security criterion expression (working as a lock) (in the proposed CB-RBAC model, secure objects and secure sub objects are semantic descriptions rather than multimedia data themselves). A secure operation is an operation associated with a security criterion subset (its elements work as the relevant keys of the corresponding secure object). A secure user is composed of a user and a security criterion subset (SCSS) the elements of which can be thought as user's available keys. To assign the remote users to the roles, the digital credentials [6, 7, 8] are adopted to establish the trust. In the user-role assignment process, the multilayer security related attributes in the digital credentials are translated into a security criterion subset (whose elements specify the user's security features) which is combined with a user to form a secure user. Under our Criterion-Based RBAC (CB-RBAC) multilayer access control model, a secure user who is the member of a role possesses all the secure permission(s) assigned to the role. When a secure object is within a user's granted secure permission, he/she can efficiently access (in the mode specified by the secure operation within the same secure permission) only those secure sub objects whose embedded locks are actuated open with the common elements in secure user's SCSS and the corresponding secure operation's SCSS.

The rest of the paper is organized as follows. We first briefly introduce the MPEG-7 standard in Section 2. Then in Section 3, the CB-RBAC model is presented. Section 4 focuses on secure object and secure operation generations. The secure user-role assignment process and Compact-Secure-Role-SCSS cookies are discussed in Section 5. Section 6 explains how the multilayer access control and non-multilayer access control are achieved. And finally, Section 7 concludes the paper.

2 Introduction of MPEG-7 Standard

The MPEG-7 standard provides tools for effectively and efficiently describing the audiovisual contents. Descriptors (Ds), Description Schemes (DSs), and Description Definition Language (DDL) are three main components of the standard. Descriptors are representations of distinctive characteristics of the data, which signify something (the features) to somebody. They define the syntax and the semantics of the feature representation. Description Schemes specify the structure and semantics of the relationships between their components, which may be both Descriptors (Ds) and Description Schemes (DSs). Description Definition Language (DDL) is used to define the syntax of the MPEG-7 Description Tools (Ds and DSs) to allow the creation of new Description Schemes and Descriptors and the extension and modification of existing Description Schemes. DDL is a superset of XML Schema in which array and matrix datatypes (both fixed size and parameterized size) and built-in primitive time datatypes (basicTimePoint and basicDuration) are added. Depending on the different applications, MPEG-7 descriptions may be stored in a database or transmitted along with the data described.

Two MPEG-7 properties lay the foundation of the CB-RBAC model. First, the CB-RBAC model benefits from the fact that the segment description (semantic description) in MPEG-7 can be decomposed and organized into a tree structure. As a description allows to be decomposed into a number of different parts each of which corresponds to a multimedia entity through a multimedia content locator, it is possible for us to separate further-protection-needed entities from non-further-protection-needed entities (These definitions will be given in Section 4).

Another property that makes the CB-RBAC model possible is the extensibility of the Description Schema in MPEG-7. The allowed extension can be the creation of new Description Schema or the modification of the existing ones. This property facilitates the CB-RBAC in two aspects. On one hand, with the proper extension of the Description Schema, more kinds of multimedia entities can be described and thus fine-grained security level can be achieved. On the other hand, the extensibility allows the graceful embedding of the security information.

3 The Criterion-Based RBAC (CB-RBAC) Model

The proposed CB-RBAC model is an extension of RBAC96 [21]. The components of objects, operations, permissions, and users in RBAC96 are enhanced to be secure objects (SOb), secure operations (SOp), secure permissions (SP), and secure users (SU) respectively in the CB-RBAC. A secure object is composed of a number of secure sub objects each of which is a sub object embedded with a security criterion expression (working as a lock). A secure operation is an operation associated with a security criterion subset (whose elements are the relevant keys with respect to the locks embedded in the secure sub objects of the corresponding secure object). A secure object and the relevant secure operation constitute a secure permission. A secure user is a user with a security criterion subset (SCSS) the elements of which specify the user's security features and can be regarded as the user's available keys. To achieve the multilayer access control, the embedded security information (security criterion expressions and security criterion subsets) and the normal Boolean operations are used.

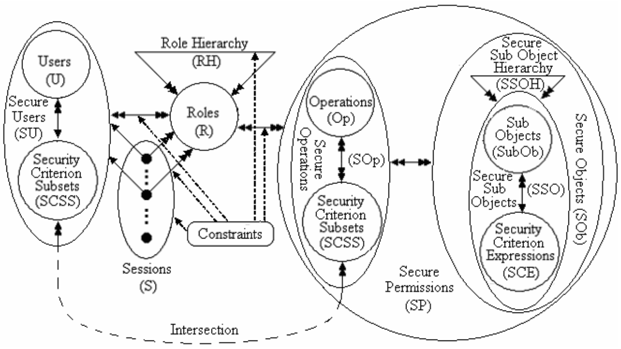


Figure 1: CB-RBAC model

Figure 1 is the logical details of the proposed CB-RBAC model.

The components in the model include:

In the proposed CB-RBAC, S (a set of sessions), U (a set of users), R (a set of roles), Op (a set of operations), Ob (a set of objects), RH (role hierarchy), and the constraints are the same as those in RBAC96 model.

A set of predefined security criteria plays an important role in the CB-RBAC model. A security criterion is a criterion used to specify the secure user's security features and the object's (and the sub object's) security attribute(s). Each security criterion is represented by a Boolean variable denoted by s_i (The Boolean operations "$\wedge$" (logic and), "$\vee$" (logic or), and "$^-$" (negation) are applied to security criteria in this paper).

For example, a security criterion s_3 can be defined to indicate the secure users of professional nurses. When s_3 or $\overline{s_3}$ is included in the description of a secure object (secure sub object) to specify its security attributes, the fact of whether a secure user is a professional nurse (e.g. whether s_3 is used to specify the secure user's security features) is considered to determine whether the secure user is allowed to access that secure object (secure sub object).

A set of security criteria $s_1, s_2, \ldots, s_n$ in an application domain is predefined according to the system security policy and the security requirements. The goal is that the security features of all kinds of secure users and the security attributes of all the possible objects and sub objects can be properly expressed with these security criteria. The total security criteria and their complements in an application domain form a security criterion set (SCS).

Usually, plurality security criteria may be involved in specifying the security features of a user. These security criteria form a set (a subset of SCS, called security criterion subset (SCSS)) which is combined with the user to form a secure user. Another SCSS, which is associated with an operation, is made up of all the relevant keys with respect to the locks embedded in the secure sub objects of the corresponding secure object.

The security criterion expression (SCE) (work as a lock) embedded in a secure sub object is used to specify the security attributes of the secure sub object. A security criterion expression (SCE) is a Boolean expression in terms of security criteria, $s_1, s_2, \ldots, s_n$.

A secure sub object (SSO) is the combination of a sub object (a description of a multimedia element) and the embedded SCE which specifies the security attributes of that sub object.

The existing partial order relations between the secure sub objects are called secure sub object hierarchy (SSOH): SSOH $\subseteq$ SSO $\times$ SSO.

A secure object (SOb) is composed of a number of secure sub objects which are organized in a tree structure (secure sub object hierarchy).

The operations operate on secure objects are secure operations (SOp) each of which is an ordinary operation associated with a SCSS (called SOp's SCSS) whose elements are made up of all the relevant keys (security criteria) with respect to the locks (SCE) embedded in the corresponding secure object: SOp $\subseteq$ Op $\times$ SCSS.

A secure permission (SP) is an allowed access mode of a secure operation (SOp) on a secure object (SOb): SP $\subseteq$ SOp $\times$ SOb.

A secure user (SU) is a user combining with a SCSS (called SU's SCSS) whose elements specify the user's security features: SU $\subseteq$ U $\times$ SCSS.

The new components SOb, SOp, SP, and SU are the enhanced versions of their corresponding counterparts in the RBAC96. The enhancement is transparent to the other components such as roles and sessions. As a result, the common administrative functions in the CB-RBAC system are identical (or very similar) to those in RBAC96.

Note: The abbreviations SCE, SCSS, SOb, and SOp are used to present both singular and plural forms in this paper.

4 Secure Object and Secure Operation Generations

4.1 Secure Object Generation

In the CB-RBAC model, an "object" can be either a common object (A passive entity that contains or receives information) or a metadata element (a description of a multimedia entity). In MPEG-7, each description of a multimedia entity contains a multimedia content locator pointing to the corresponding multimedia entity and the accessing information (e.g. TimePoint, Duration, and Quality etc.) to specify the accessing mode to the multimedia entity. Besides, the metadata (descriptions) and the corresponding multimedia entities have a one-to-one relation and they can always be assigned the same security attribute (level). Therefore, if a description is accessible (inaccessible), its corresponding multimedia entity is also accessible (inaccessible). In other words, a multimedia entity can be effectively protected by protecting its corresponding description. In the following discussions, all the objects and the sub objects refer to the descrip-

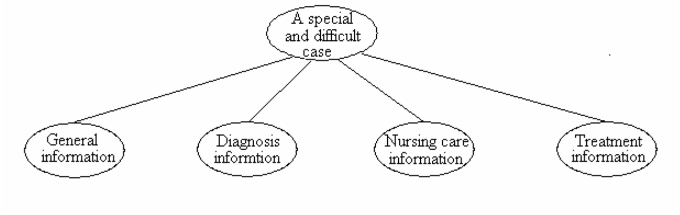


Figure 2: The original description tree of a multimedia archive

tions (metadata) of the multimedia data unless they are indicated explicitly otherwise.

Basically, objects (the same are the sub objects) can be classified into no-further-protection-needed objects to which all authorized users can access and further-protection-needed objects all or part(s) of which is (are) accessible only for those authorized users who have certain security features. In the original description tree of a multimedia file (object), if a leaf description node includes the description of multiple further-protection-needed sub objects or a further-protection-needed sub object and a non-further-protection-needed sub object, the description node must be decomposed further. The purpose of the decomposition is to guarantee that every further-protection-needed sub object can be protected independently. As we discussed in section 2, MPEG-7 supports this kind of decomposition.

After the decomposition, a proper SCE is selected and embedded into each sub object of the description tree in the depth-first, post-order. A predefined table called the Content-SCE table is used to simply the SCE assignment to the leaf nodes. If the content of a leaf node belongs to a Group of further-protection-needed content in the Content-SCE table, the corresponding SCE of the Group of further-protection-needed content is adopted as that leaf node's SCE. If the content of the leaf node does not belong to any Group of further-protection-needed content, the constant false, F, is adopted as the SCE for that leaf node (which implies that the leaf node is a non-further-protection-needed sub object). The SCE of each non-leaf node (interior and root) is formed by logic 'OR' of all of its direct children's SCE (the results are simplified into the form of Sum of Products (SoP) with the products sorted according to the number of the products' terms.

Each record in the Content-SCE table contains two fields: Group of further-protection-needed content and Security criteria expression (SCE) which is created in advance for a specific application domain by the following steps:

1) Find out all the further-protection-needed sub objects in that application domain, which are the collection of all the possible further-protection-needed leaf nodes in all the objects.

2) According to the system security policy and the content of the sub object, define the protection criterion combination for each further-protection-needed sub object in the form of SCE.

3) Aggregate the further-protection-needed sub objects according to their corresponding SCE. That is, the further-protection-needed contents with the same SCE are aggregated into the same group of further-protection-need contents.

Note that all the SCE in Content-SCE table are of the form of Sum of Products (SoP) with the products sorted according to the number of the products' terms.

Example 1 *Suppose that a federated digital library contains multimedia archives about special and complicated medical cases which are referenced by doctors, nurses and researchers (special doctors). Every multimedia archive, properly described by the tools provided in MPEG-7, includes general, nursing care, diagnosis, and treatment information in the heterogeneous form (text, image, audio, and video). The descriptions of the multimedia archives provide the means for accessing the whole multimedia archive or its element(s) (The descriptions are used to represent the corresponding multimedia archives or their elements in the following discussion, which does not lose the generality). The original description tree of a multimedia archive is shown in Figure 2 (each node in the description tree corresponds to a piece of multimedia datum).*

There are leaf nodes that describe multiple further-protection-needed sub objects or a further-protection-needed sub object and a non-further-protection-needed sub object. These leaf nodes should be decomposed. To find out all the further-protection-needed contents (sub objects), we need to establish the system security policy.

The security policy is derived from existing laws, ethics, regulations, and generally accepted practices. The multilayer access control related security policy is that different users (e.g. doctors, nurses and researchers) should be able to access only the useful and necessary information according to their positions and responsibilities. The system security policy of the Example 1 can be as follows.

1) All of the secure objects (the multimedia archives and the corresponding descriptions) are accessible only to those secure users who are the member of the roles to which the secure permissions (which include those secure objects) have been assigned.

2) Some contents of these secure objects are restricted to certain kinds of secure users. The contents and the corresponding restrictions in this example include:

   a. The patient's sensitive personal information (such as health card number) is only accessible to those nurses who are responsible for patient record administration.

   b. Nurses are not allowed to access the contents of diagnosis and treatment.

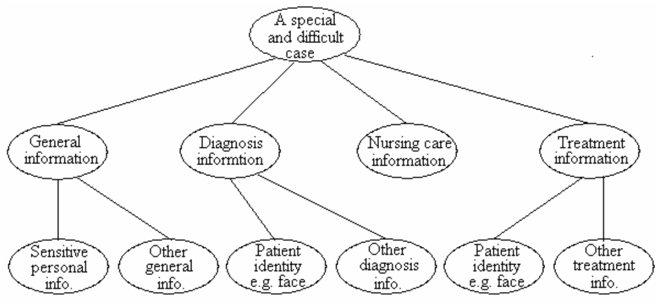


Figure 3: The decomposition of a multimedia archive description tree

c. Researchers are not able to access to the patient's identity.

Based on the above security policy, the possible further-protection-need contents (sub objects) can be generated. They are patient's personal information, patient's identity, diagnosis information (except identity), and treatment information (except identity).

From the above security policy, we can also determine the relevant security criteria in this example:

1) s_1, indicating nurses who are responsible for patient record administration.

2) s_2, indicating researchers (special doctors).

3) s_3, indicating nurses.

4) s_4, indicating clinic doctors.

Thus, the security criterion set (SCS) of this example is $\{s_1, s_2, s_3, s_4, \overline{s_1}, \overline{s_2}, \overline{s_3}, \overline{s_4}\}$.

The Content-SCE table, which includes all the further-protection-needed contents and their related security criterion expressions (SCE), is produced (see Table 1) according to the system security policy. Note that the further-protection-needed contents are integrated according to their SCE in the Content-SCE table.

With the information of all the possible further-protection-needed contents (sub objects), the original description tree is decomposed further so that every further-protection-needed content is described independently (see Figure 3).

From Table 1 and Figure 3, the secure object can be produced by embedding a SCE into each node according to the discussion above (see Figure 4). The number beside each node indicates the order in which the SCE are embedded.

4.2 Secure Operation Generation

To generate a secure operation, the corresponding security criterion subset must be generated first. The security criteria within a SOp's SCSS are the collection of the security criteria appeared in the SCE of the corresponding secure object. Hence the security criterion subset in a secure operation is made up of all the security criteria appeared in the SCE of the corresponding secure object. These security criteria are the relevant keys to determine the state of the SCE (locks) within the secure object.

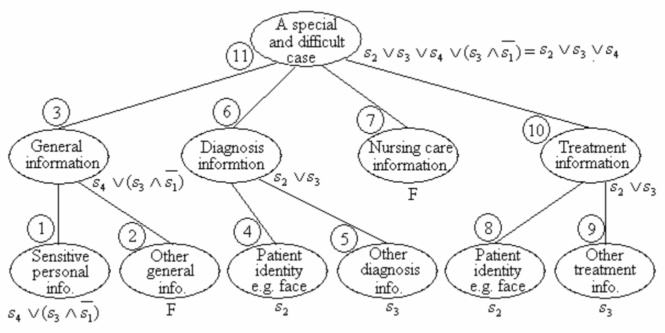

A special and difficult case
11
$s_2 \vee s_3 \vee s_4 \vee (s_3 \wedge \overline{s_1}) = s_2 \vee s_3 \vee s_4$
3
General information
$s_4 \vee (s_3 \wedge \overline{s_1})$
6
Diagnosis informtion
$s_2 \vee s_3$
7
Nursing care information
F
10
Treatment information
$s_2 \vee s_3$
1
Sensitive personal info.
$s_4 \vee (s_3 \wedge \overline{s_1})$
2
Other general info.
F
4
Patient identity e.g. face
s_2
5
Other diagnosis info.
s_3
8
Patient identity e.g. face
s_2
9
Other treatment info.
s_3

Figure 4: The secure object of a medical multimedia archive

Each SOp's SCSS corresponds to a specific secure object. The SOp's SCSS of the secure object in Figure 4 is $\{\overline{s_1}, s_2, s_3, s_4\}$.

5 Secure User-role Assignment on the Web

It is the security administrator's responsibility to assign secure users to roles and to generate the proper SCSS (which are embedded in the secure users to specify their security features) according to the system security policy and the users' relevant characteristics. However, manually assigning users to roles and generating the proper SCSS is a formidable task for the hundreds of thousands of the remote users in the web applications. A mechanism that can automatically generate the proper SCSS and assign the remote users to roles is of great importance. The mechanism requires a proper means to establish the trust between the remote secure users and the server(s). In CB-RBAC, we use digital credentials for the needed trust establishment.

Digital Credentials [9] are the digital equivalent of paper documents and other tangible objects traditionally used for establishing a person's privileges, characteristics, identity, and so on. Users can establish trust in such a way that only the needed attributes of the digital credentials are provided. When digital credentials are used for the purpose of the secure user-role assignment in the proposed CB-RBAC model, a set of security policies (authorization rules) provides the guide for the assignment and a Credential-criterion table specifies the mapping relations between the attributes of the credential and the security criteria (The relevant attributes of a user's available digital credentials determine the elements (security criteria) of the security criterion subset associated with

Table 1: The Content-SCE table of the Example 1

Group of further-protection-needed content	Security criterion expression (SCE)
Patient's personal data	$s_4 \vee (s_3 \wedge \overline{s_1})$
Diagnosis information (except identity); treatment information (except identity)	s_3
Patient's identity	s_2

the user).

5.1 Digital Credential Based Security Policy for Secure User-role Assignment

For each role in the system, the security policy must specify which digital credential(s) is (are) needed if a remote secure user is assigned to this role. The role hierarchy in CB-RBAC has exactly the same properties as that in RBAC96: senior role inheriting junior role's permissions; junior role inheriting senior role's users [22]. Because of the second property, authorization rules that are valid to assign a user to a senior role must also be valid to assign him/her to its junior roles. To simplify the set of the authorization rules, the rules specified for the senior roles need not be repeated for the junior roles; and the security policy (authorization rules) can be established for every role (to which secure users need to be assigned) from most senior roles to most junior roles.

According to the authorization rules, a secure user is assigned to one or more roles based on his/her available credential(s) and request. Usually, the secure user is assigned to those role(s) which include(s) as much as possible permission according to the security policy and his/her available credential(s) to facilitate the subsequent transactions the user might perform. This strategy does not violate the least privilege principle, because the determination is made in each session to activate only the role(s) necessary for the user's work.

To simplify the discussion, we do not consider the possible existing constraints (which will not lose generality) about secure user-role assignment and define the assignable role(s) formally.

Definition 1 *(Assignable role): According to the secure user's available digital credentials and the system security policy, all the roles to which the secure user can be assigned are called assignable roles with respect to that secure user.*

Suppose that a role hierarchy contains five roles for a digital library (see Figure 5). The credential group beside each role reflects the security policies for the secure user-role assignment. The secure permissions (SP) within each role are the secure permissions assigned to the role. If a remote secure user applies for a secure permission, SP4, the system checks the digital credentials provided by the user and assigns him/her to the proper role(s) in the following steps:

1) Find out the role(s) $r_i (i = 1, 2, \ldots)$ that contains (contain) the applied secure permission. In this example, we get role2.

2) If $r_i (i = 1, 2, \ldots)$ or any of its (their) ancestor role(s) is (are) assignable role(s), go to 3; otherwise go to 4. For this example, if C4∧C5 or C4∧C6 is provided, role2 is assignable; if C11∧C12 is provided, role5, the role2's parent, as well as role 2 is assignable

3) If there is an assignable role r which is the ancestor of all the other assignable roles, the secure user is assigned to this role r. For example, if the user provides C4 (medical member credential), C6 (master card credential), C11 (VIP member credential), and C12 (specialist credential), he/she is assigned to role5 (The relevant assignable roles are role2 and role5. Role5 is the parent of role2).

   Otherwise, the user is assigned to those assignable roles or any of its (their) ancestor role(s)) which have no parent assignable roles. For example, if a secure user provides C1, C4∧C5, and C7 to apply the secure permission SP3, he/she will be assigned to role2 and role3 (The assignable roles are role1, role2 and role3. Role2 and role3 have no parent assignable roles).

4) Refuse the user's application.

In the above process of the secure user-role assignment, those digital credential attributes which refer to multilayer access control need to be translated into a SCSS to specify the secure user's security features. To record these attributes, the system stores a table (Credential-criterion table) which maps the multilayer security related attributes of every digital credential to the corresponding security criteria. Table 2 is an example of the digital credential C4 which has three multilayer security related attributes: "Profession", "Administration on patient's record", and "Research".

When a remote secure user submits C4 and C6 to apply for the secure permission SP4 (whose secure object is shown in Figure 4), if the "Profession" attribute of C4 is "Doctor", the "Administration on patient's record" attribute is "No", and the "Research" attribute is "No', the secure user will be assigned to role 2 and his/her SU's SCSS is $\{\overline{s_1}, \overline{s_2}, s_4\}$.

Table 2: An example Credential-criterion table of the medical member credential

Digital credential			**Security criterion**
Credential name	**Attribute name**	**Attribute value**	
Medical-Member-Digital-Credential (C4)	Profession	Doctor	s_4
		Nurse	s_3
	Administration on patient's record	Yes	s_1
		No	$\overline{s_1}$
	Research	Yes	s_2
		No	$\overline{s_2}$

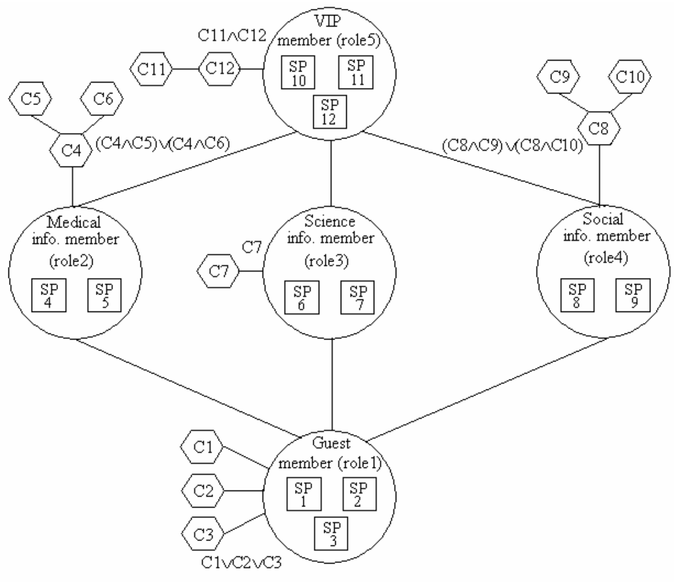


Figure 5: The digital credentials for remote secure user-role assignment in Example 1

5.2 Compact Secure Role-SCSS Cookie

A cookie [13, 16, 18] is a piece of state information sent by a server when a client visits the server through Hypertext Transfer Protocol (HTTP). The state information is included in any future HTTP request made by the client to the server.

The Role-SCSS cookie mechanism (see Figure 6 (a)) can be used to remember the multilayer security related SCSS and the role(s) to which a secure user is assigned. Instead of asking the same credentials again, the Role-SCSS cookie can be used in the subsequent communications between the web server and the browser. The Role-SCSS cookie defined for the CB-RBAC model contains following 6 parameters:

1) Domain: the parameter specifies the domain in which the cookie is valid.

2) Secure: the parameter indicates to the browser whether the cookie should only be sent by using a secure protocol (e.g. SSL).

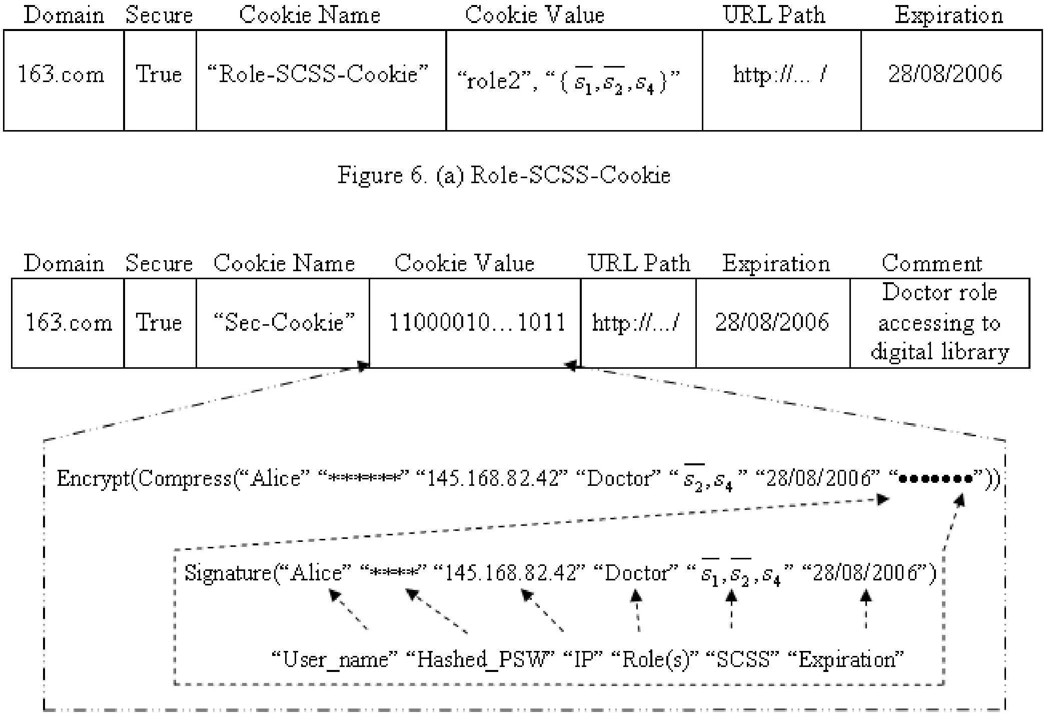
3) Cookie Name: the parameter specifies the name (type) of the cookies; the default value is "Role-SCSS-Cookies".

4) Cookie Value: the parameter contains the role(s) to which the secure user has been assigned and the SCSS whose elements reflect the secure user's security features.

5) URL: the parameter indicates the cookie's valid path.

6) Expiration: the parameter contains the cookie's expiration date.

The Role-SCSS cookies work well if every user is honest: none tries to acquire permissions illegally. However, the threats come from several aspects. Because the Role-SCSS cookies are stored and transmitted in plain text, they can be easily modified, copied by the end users and intercepted by other users on the web. The network threats can be prevented by adopting the widely used Secure Sockets Layer protocol (SSL) [11]. To prevent the Role-SCSS cookies from unauthorized modification and copy, the cookie has to be enhanced to be Compact-Secure-Role-SCSS cookie, which includes seven parameters (see Figure 6 (b)). The values of Domain, Secure, URL Path, and Expiration parameters are not changed in the Compact-Secure-Role-SCSS cookies. However, the value of the Cookie Name is replaced by the value of "Sec-Cookie" to indicate the different type of the cookie. The most significant difference is the values of the Cookie Value parameter. It is now made up of "name" "PSW" "IP" "Role(s)" "SCSS" "Expiration" and "Signature" (where, the "Signature" is the digital signature of the "name" "PSW" "IP" "Role(s)" "SCSS" and "Expiration" by the server). These parts are arranged in the fixed format (each part is enclosed in a pair of quotation marks separated by a blank) and order to form a complete value. Then it is compressed to reduce its size. Finally, it is encrypted. When a server receives a Compact-Secure-Role-SCSS cookie (Cookie Name and Cookie Value), it processes the Cookie Value in the following order: decrypt it, decompress it, and separate it to get "name" "PSW" "IP" "Role(s)" "SCSS" "Expiration" and "Signature". The "name" and "PSW" (which correspond to user's name and password) are used to authenticate the



Domain	Secure	Cookie Name	Cookie Value	URL Path	Expiration
163.com	True	“Role-SCSS-Cookie”	“role2”, “{ $\overline{s_1}$, $\overline{s_2}$, s_4 }”	http://... /	28/08/2006

Figure 6. (a) Role-SCSS-Cookie

Domain	Secure	Cookie Name	Cookie Value	URL Path	Expiration	Comment
163.com	True	“Sec-Cookie”	11000010…1011	http://.../	28/08/2006	Doctor role accessing to digital library

Encrypt(Compress(“Alice” “*******” “145.168.82.42” “Doctor” “$\overline{s_2}$, s_4 ” “28/08/2006” “•••••••”))
Signature(“Alice” “*****” “145.168.82.42” “Doctor” “$\overline{s_1}$, $\overline{s_2}$, s_4” “28/08/2006”)
“User_name” “Hashed_PSW” “IP” “Role(s)” “SCSS” “Expiration”

Figure 6. (b) Compact-Secure-Role-SCSS-Cookie

Figure 6: The Role-SCSS-cookie and the corresponding Compact-Secure -Role-SCSS-cookie

owner of the cookie. The “IP” (which stores the IP address of the user’s computer) is used to discover the unauthorized entities illegally using the cookie on other computers. The “Signature” is used to check whether there exist any unauthorized modifications. As the Compact-Secure-Role-SCSS cookies are no longer in plain text, we add a new parameter, Comment, to describe the usage information of the cookie so that users will not be puzzled when they possess many Compact-Secure-Role-SCSS cookies at the same time. When a Compact-Secure-Role-SCSS cookie is used, it is easy to authenticate the owner of the cookie, to verify the integrity of the cookie, and to guarantee the confidentiality of the cookie.

6 Multilayer and Non-multilayer Access Controls in CB-RBAC

6.1 Multilayer Access Control

In CB-RBAC, a secure user is granted secure permissions in the same way as a user is granted permissions in RBAC96. The secure user possesses all the secure permissions assigned to the roles of which he/she is a member. When he/she accesses to a secure object (which is in one of his/her granted secure permissions) in the mode defined in the corresponding secure operation, he/she can only access those secure sub objects whose embedded SCE (locks) are actuated open by the common security criteria in his/her SCSS (available keys) and the corresponding SOp’s SCSS (relevant keys).

The procedure of determining whether a secure sub object (SSO) should be protected is performed by evaluating its embedded SCE according to the common elements in the corresponding SOp’s and SU’s SCSS. The evaluation of a security criterion expression (SCE) can be done by the following two steps. First, substitute all the security criteria in the SCE with true, T, or false, F, according to the following rules: all the security criteria in SCE that are not the common elements in SOp’s SCSS and SU’s SCSS have the value of false, F; and all the security criteria appear in SCE and the intersection of SOp’s SCSS and SU’s SCSS have the value true, T. Second, the SCE is evaluated according to the normal evaluation procedure in Boolean algebra. For example, if the common elements of SOp’s SCSS and SU’s SCSS are $s_1, \overline{s_2}$ and s_3, the evaluation values of the expressions $s_1 \vee s_4$, $s_1 \wedge s_2$, $\overline{s_2} \wedge s_3$, $s_2 \vee s_4$, and $s_3 \wedge \overline{s_4}$ are T ∨ F=T, T ∧ F = F, T ∧ T = T, F ∨ F = F, and T ∧ F = F respectively. The true, T, evaluation value of a SCE implies that the protective criteria of the corresponding secure sub object (SSO) are satisfied and the secure sub object is not accessible. On the contrary, when the evaluation value of the SCE is false, F, the criteria of protecting the related secure sub object are not contented and the secure sub object is accessible.

The multilayer access control is achieved by traverse the SOb in the depth-first preorder. Each SCE is evaluated by the common elements in the related SOp’s and

SU's SCSS. Note that whenever the evaluation value of a node (secure sub object) is false, F, the children of that node need not be evaluated (which are called early termination) and the node as well as its child nodes are accessible. Especially, if the root is evaluated false, F, (which means there are no further-protection-needed sub objects in that SOb), all the rest nodes in the SOb need not be evaluated. In addition, the evaluation of each SCE is performed in such a way that all its products are evaluated one by one from shorter-term-product to longer-term-product and the short-circuit evaluation is adopted, which raises the efficiency in two aspects. On one hand, since the security criteria not in the intersection of SOp's SCSS and SU's SCSS always have the value of false, F, in a SCE when the SCE is evaluated and all the SCE are in the form of SoP and their products had been sorted according to the number of the terms (criteria) in these products, the products whose number of terms (criteria) is larger than the number of the common elements in SOp's SCSS and SU's SCSS will always be evaluated as false, F. Therefore, these products whose number of terms is bigger than the number of the common elements of SOp's SCSS and SU's SCSS need not be evaluated. On the other hand, the evaluation process can stop whenever one product (whose term number is smaller or equal to the number of the common elements of SOp's SCSS and SU's SCSS) in a SCE is evaluated true, T, (which results in the evaluation value of the whole SCE true, T). The above properties usually can reduce the computational expense significantly.

It is time to explain why the intersection of a secure operation's and a secure user's SCSS is used to evaluate the corresponding secure object in stead of using the secure user's SCSS only. Note that the elements of a secure user's SCSS are user's available security criteria many of which may have nothing to do with the SCE evaluation of a specific SOb. This means that there may be some redundant elements in the secure user's SCSS with respect to a specific secure object. Because the redundant security criteria increase the computational expense in the process of the SCE evaluation, we eliminate them by using the intersection of a secure operation's and a secure user's SCSS. For example, a secure user's SCSS is $\{s_1, s_2, s_3, s_4, s_6\}$ and the secure operation's SCSS is $\{s_5, s_6, s_7, s_8, s_9\}$. If $\{s_1, s_2, s_3, s_4, s_6\}$ is used to evaluate a SCE, $s_5 \vee (s_6 \wedge s_7) \vee (s_7 \wedge s_8 \wedge s_9)$, every term of the SCE has to be evaluated. If the intersection of the two SCSS $\{s_6\}$ is used to evaluate the same SCE, according to the short-circuit evaluation discussed above, only the first product s_5 needs to be evaluated to get the evaluation value of the whole SCE.

In Example 1, when a remote secure user applies for the secure permission SP4 with digital credentials C6 (which has no multilayer security related attributes) and C4 (whose multilayer security related attributes are shown in Table 2), the user is assigned to the role2 with the SCSS, $\{\overline{s_1}, \overline{s_2}, s_4\}$. The secure operation's SCSS in the SP4 is $\{\overline{s_1}, s_2, s_3, s_4\}$. Thus, $\{\overline{s_1}, s_4\}$ should be used to evaluate the corresponding secure object. Figure 7 shows the result (the shaded nodes are inaccessible (partially or completely) to this secure user).

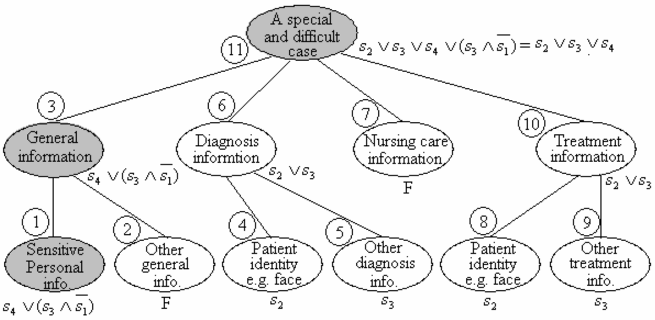

A special and difficult case
11
$s_2 \vee s_3 \vee s_4 \vee (s_3 \wedge \overline{s_1}) = s_2 \vee s_3 \vee s_4$
3
General information
$s_4 \vee (s_3 \wedge \overline{s_1})$
6
Diagnosis informtion
$s_2 \vee s_3$
7
Nursing care information
F
10
Treatment information
$s_2 \vee s_3$
1
Sensitive Personal info.
$s_4 \vee (s_3 \wedge \overline{s_1})$
2
Other general info.
F
4
Patient identity e.g. face
s_2
5
Other diagnosis info.
s_3
8
Patient identity e.g. face
s_2
9
Other treatment info.
s_3

Figure 7: The accessible and inaccessible sub objects of a multimedia archive

Note that the SCE of the nodes 4, 5, 8, and 9 are not evaluated because the early termination in nodes 6 and 10 (their SCE evaluation values are "F").

6.2 The Non-multilayer Access Control

In the proposed CB-RBAC model, every SCE within a SOb is a fixed expression unless the contents of the description or the system security policy changes. The security levels of its secure sub objects are determined by the embedded SCE as well as the common elements in the related SOp's and SU's SCSS. When there is no common elements in the related SOp's and SU's SCSS, none of the secure sub objects in the related SOb needs further protection (because all the SCE in the SOb are evaluated false), which means that all the security criteria specifying a secure user's security features have nothing to do with the evaluation of SCE of that SOb. Especially, when a SU's SCSS is set to NULL, the non-multilayer access control is achieved for that secure user.

The proposed model also supports the non-multilayer access control for multiple secure users. By embedding the constant "F" into the root of those objects which do not include any further-protection-needed sub object, the special secure objects are formed. When these secure objects are accessed, the evaluation value of their roots are false, F, which results in that the whole secure objects are accessible. As a result, the non-multilayer access control is achieved for all the secure users.

7 Conclusion

This paper presents a CB-RBAC model to support web-based multimedia multilayer access control in MPEG-7 by introducing the secure users (SU), secure objects (SOb), secure operations (SOp) and secure permissions (SP). The proposed model takes advantage of the properties of MPEG-7 standard to generate a secure object by embedding a security criterion expression (SCE) into each of its sub object (a multimedia semantic description). A secure operation is created by associating a security criterion subset (its elements are the collection of security criteria appeared in the SCE of the corresponding SOb) with an ordinary operation. Similarly, a secure user is the user combining with a proper SCSS. With the cooperation of a secure user, a secure operation and a secure object, the multilayer access control is achieved through a powerful but simple mechanism. A secure sub object's security level depends not only on the embedded security criterion expression (SCE) but also on the common elements of the relevant SOp's and SU's SCSS, which results in a flexible multilayer access control system. In addition, the method of using digital credentials and Compact-Secure-Role-SCSS cookies is effective and secure for web-based applications.

The proposed CB-RBAC model is an important step on enhancing the existing RBAC model. The required multilayer access control is handled gracefully by this model. To address the requirements of temporal dimension, the CB-RBAC model can adopt the ideas and methods proposed in [4] and apply them to both roles and the related security criterion subsets (SCSS). This issue will be discussed in detail in a separate paper.

Because the proposed model is an extension of the RBAC model and exploits the simple Boolean operations, it has many merits. First, it inherits the advantages of the RBAC model because the extensions of secure users and secure permissions do not change the logical structure of the model. The second merit comes from the model itself. The use of Boolean expression is very natural to support the multilayer access control in MPEG-7. Both further-protection-needed sub objects and non-further-protection-needed sub objects (and the corresponding multimedia elements) are expressed explicitly by one mechanism. Even complex security requirements can be expressed elegantly by the adopted Boolean expressions. And the model has the potential to accommodate to the more complicated requirements. The next merit is its efficiency and effectiveness. By adopting the strategy of the early termination and the short-circuit evaluation of SCE, the computational expense is reduced and the redundant operations are eliminated. And last, the model can adapt to a wide range of applications. Both multilayer access control and non-multilayer access control are supported by the same model. Although it is designed to address the multilayer access control in MPEG-7, it also suits for other applications that require multilayer access control and whose data can be organized in a hierarchical (tree) form. In conclusion, the CB-RBAC model can effectively and efficiently support the web-based multilayer access control in MPEG-7 and has the potential to deal with the multilayer access control in broader variety of applications.

References

[1] W. Aref, M. Hammad, A. C. Catlin, L. Llyas, T. Ghanem, A. Elmagarmid, and M. Marzouk, "Video query processing in the VDBMS testbed for video database research," in *Proceedings of the First ACM International Workshop on Multimedia Databases*, pp. 25-32, New Orleans, LA, USA, 2003.

[2] E. Bertino, E. Ferrari, and A. Perego, *Max: An Access Control System for Digital Libraries and the Web*, http://semioweb.msh-paris.fr/euforbia/download/max.pdf

[3] E. Bertino, M. Hammad, W. Aref, and A. Elmagarmjd, "An access control model for video database systems," in *Proceedings of the Ninth International Conference on Information and Knowledge Management*, pp. 336-343, McLean, Virginia, United States, 2000.

[4] E. Bertino, P. A. Bonatti, and E. Ferrari, "TRBAC: A temporal role-based access control model," *ACM Transactions on Information and System Security (TISSEC)*, vol. 4, issue 3, pp. 191-233, Aug. 2001.

[5] E. Bertino, J. Fan, E. Ferrari, M. S. Hacid, A. Elmagarmjd, and X. Zhu, "A hierarchical access control model for video database system," *ACM Transactions on Information System*, vol. 21, no. 2, pp. 155-191, 2003.

[6] M. Blaze, J. Feignhbaum, and J. Lacy, "Decentralized trust management," *IEEE Symposium on Security and Privacy*, pp. 17-28, Oakland, CA, May 1996.

[7] M. Blaze, J. Feignhbaum, and A. D. Keromytis, "KeyNote: Trust management of public-key infrastructures," in *Security Protocals, 6th International Workshop*, pp. 59-63, Cambridge UK, 1998.

[8] M. Blaze, J. Feignhbaum, J. Ioannidis, and A. D. Keromytis, *The KeyNote Trust Management System*, Version 2, Internet Drafft RFC 2704, Sep. 1999.

[9] S. Brands, *A Technical Overview of Digital Credentials*, http://www.xs4all.nl/#brands/, 1999.

[10] E. Fernandez-Medina, G. Ruiz, and S. De Capitani di Vimerati, "Implementing an access control system for SVG documents," in *Lecture Notes in Computer Science*, pp. 741-753, Catania, Italy, 2003.

[11] A. Freier, P. Karlton, and P. Kocher, *The SSL Protocol Version 3.0*, internet Draft, Mar. 1996.

[12] V. Gligor, "Characteristics of role-based access control, symposium on access control models and technologies," in *Proceedings of the First ACM Workshop on Role-based Access Control*, no. 10, pp. 9-14, Gaithersburg, Maryland, United States, 1996.

[13] *HTTP Cookies*: http://www.netscape.com/newsref /std/cookies_spec.html.

[14] ISO/IEC JTC1/SC29/WG11N5525, *MPEG-Overview (Version 9)*, http://www.chiariglione.org/mpeg/standards/mpeg-7/mpeg-7.htm

[15] H. Kosch, *Distributed Multimedia Database Technologies Supported by MPEG-7 and MPEG-21*, CEC

Press, Boca Taton London, New York Washington, D.C., 2004.

[16] D. M. Kristol, L. Montulli, *HTTP State Management Mechanism*, Draft-ietf-http-state-man-mec.txt, 1999.

[17] B. S. Manjunath, P. Salembier, and T. Sikora, *Introduction to MPEG-7 Multimedia Content Description Interface*, John Wiley & Sons, Ltd., 2002.

[18] K. Moore, and N. Freed, *Use of HTTP State Management*, Draft-ietf-http-state-man-mec-12.txt.

[19] L. Pan and C. N. Zhang, "Using metadata to protect the audiovisual contents in MPEG-7 applications, in *SAM'04*, pp. 287-293, Las Vegas, Nevada, USA, 2004.

[20] P. Salembier and J. R. Smith, "MPEG-7 multimedia description schemes," *IEEE Transactions on Circuits and Systems for Video technology*, vol. 11, no. 6, pp. 748-759, 2001.

[21] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-based access control models," *IEEE Computer*, vol. 29, no. 2, pp. 38-47, 1996.

[22] R. Sandhu, V. Bhamidipati, and Q. Munawer, "The ARBAC97 model for role-based administration of roles," *ACM Transactions on Information and Systems Security (TISSEC)*, vol. 2, no. 1, pp. 105-135, 1999.

Leon Pan is a Ph.D. candidate in the Department of Computer Science, University of Regina. He received his Master degree in Computer Science at Tianjin University in 1989 and his Bachelor degree in Computer Science at Tianjin University in 1986. He has worked as an advanced programmer and a computer engineer for more than eleven years.

Chang N. Zhang has been at the University of Regina since 1990 where he is currently a Professor of the Department of Computer Science, and Adjunct Scientist with Telecommunication Research Labs (TRLabs). He received his B.S. in Applied Math from the Shanghai University, and a Ph.D. in Computer Science and Engineering from Southern Methodist University.