

Temporal Authorizations Scheme for XML Document

Jing Wu, Jennifer Seberry, Yi Mu

Center for Computer Security,School of Information Technology and Computer Science,
 University of Wollongong
 CCSR, SITACS
 Northfields Avenue
 NSW 2522,Australia

Abstract: In a large networking system,to manage authorizations in a complicated XML documents system is very difficult. Recently, Access Policy Sheet (APS) [6] was introduced to provide a solution to access control for XML systems. In this paper, we proposed a temporal access control scheme in APS where the propagation of authorization rights is assumed.The authorization policies can be automatically revoked when the associated time expires. We also provide conflict resolutions for our temporal authorization system.

Key-Words: temporal authorization, partial order, XML, Access control

1 Introduction

XML has been widely applied to manage Internet information. An XML document system could be very large and complicated and its security protection could be also very difficult. Protecting such an XML system requires a sound access control mechanism, which provides formalisms for specifying, analyzing and evaluating security policies that determine how an access right is granted and delegated among particular users.

Recently, researchers [2, 3, 4] have become increasingly interested in developing authorization models which are flexible and expressive enough so as to handle the specification and enforcement of multiple policies. [1, 5, 9] have expressed some interest in developing XML authorization models which are flexible and expressive enough for handling the specification and enforcement of multiple policies. However, those models are very complicated and difficult to realize. In our previous work, Access Policy Sheet (APS) [6], has been introduced. This model provides a simple and dynamic scheme for XML authorization management. However, temporal authorization [8] and authorization propagation have still not been investigated in XML based access control systems including APS. In this paper, we propose some new functions including temporal authorization ,conflict resolutions and the time dependency

which can handle temporal access control policies and policy propagation. In our model, the authorization can be automatically revoked when the associated time expires. By the hierarchical relationships along with the partial orders defined in APS, we also provide a mechanism for the conflict resolutions.

2 Predicates

In this section, we give the definitions of the predicates of **grant**, **delegate** and **cangrant**we used in our model for describing the delgatable authorizations.

Definition 1 (*grant*) *grant is a 5 -tuple predicate $|S| \times |O| \times |T| \times |A| \times |S|$.*

grant(s,o,t,a,g) : grantee s is granted by grantor g the access right a on object o with authorization type t . We can use XML to define the structure of rule Grant In the delegation process, the entity that has been given the access right to delegate by another entity, who has the access right, can perform valid delegations. The following is the definition of our delegable rules. Predicate grant in XML is an authorization rule, where the element grant with attributes grantee; object,authorization_type; access_rights; grantor and status. Here,

$\text{grantor} \in S$,
 $\text{grantee} \in S$,
 $\text{target+path} \in O$,
 $\text{authorization_type} \in \{+|-|*\}$,
where $+, -, *$ denote allow, deny, and delegable, respectively.
 $\text{access_right} \in \{\text{r}, \text{w}, \dots\}$,
 $\text{status} \in \{\text{true}, \text{false}\}$

Definition 2 (cangrant) $\text{cangrant}(s, o, a)$: subject s has the right to grant access a on object o to other subjects.

cangrant is a 3-tuple predicate $|S| \times |O| \times |A|$, where S is a set of subjects which is a grantor or a grantee; $O = \text{target} + \text{path}(V, E)$, target is an XML or URL, path is an XPath expression that eventually selects specific portions (object) of the XML document in XML tree where V is a set of nodes and E is a set of edges; A is the set of access rights. Here,

$\text{subject} \in S$,
 $\text{target+path} \in O$,
 $\text{access_right} \in \{\text{read}, \text{write}, \text{a1}, \text{a2}, \dots\}$,
 $\text{status} \in \{\text{true}, \text{false}\}$

Definition 3 (delegate)

Delegate is a 4-tuple predicate $|S| \times |S| \times |O| \times |A|$ rule, where S is a set of subjects which is a grantor or a grantee; $O = \text{target} + \text{path}(V, E)$, target is an XML or DTD, path is an XPath expression that eventually selects specific portions (object) of the XML document in XML tree where V is a set of nodes and E is a set of edges; A is the set of access rights. Here,

$\text{grantor} \in S$,
 $\text{grantee} \in S$,
 $\text{target+path} \in O$,
 $\text{access_right} \in \{\text{read}, \text{write}, \text{a1}, \text{a2}, \dots\}$,
 $\text{status} \in \{\text{true}, \text{false}\}$

$\text{delegate}(g, s, o, a)$: subject g has directly or indirectly granted subject s access a on object o with delegable type.

3 Authorization Rules in APS

Directly using XML to describe access control often shows little advantage when the access control system is complicated (e.g., when authorization delegation and propagation are required). In our

model, authorization specifications or rules are provided in an Authorization Policy Sheet (APS) associated with the document/DTD. In APS, the representation of authorizations is described in terms of orders of the objects and subjects and explicit authorization rules.

The APS is separate from the document and DTD and offers great convenience in the administration of access control for system administrators due to its simplicity. The system administrator can manage the system access control by the concise rules given in an APS. The resultant XML sheet can be generated from the corresponding DTD and APS. APS also shows the great advantage due to its convenience in the specification of explicit rights and the implicit rights for XML documents.

The partial orders of the access control components, including subjects, object, types, and rights, are one of the key components in an APS. We will see that they can be used to simplify our access control system by implicit rules in authorization propagations.

The following figure of the XML DOM tree expresses the hierarchy relation of the objects.

Figure 1: DOM tree, where each node represents an object.

Now let's see how to determine the orders of the objects. According to the structure of the DOM tree. In our model, the root node has the greatest order in any order chain. We can describe the hierarchy relation as following: o1 is the root of the tree, o2 and o3 are the descendant nodes of o1 , o4 and o5 are the children nodes of o2 and the grandchildren nodes of o1 , o6 is the child node of o3 and the grandchild nodes of o1 ,

So, we have $\text{o1} > \text{o2} > \text{o4}$, $\text{o1} > \text{o3} > \text{o6}$, and $\text{o1} > \text{o2} > \text{o5}$.

To provide fine grained specification in XML, we utilize the XPath expression to identify the

structure of the tree. An Xpath expressions on an XML document tree is a sequence of element name or predefined functions separated by the character: for the one branch of the tree: o1-o2-o4, node o4 can be expressed as /o1/o2/o4/ and we have the partial order: /o1/ >/o1/o2/ >/o1/o2/o4/.

In general, we have the object partial order chain: /root/ > /root/ child of root/ > ... > /root/child of root/grandchild of root/....

For example:

```
//hospital/ > //hospital/room-info/ >
//hospital/room-info/patient/.
```

Thus, the order of the ancestor nodes in a DOM tree are always greater than the order of the descendant nodes.

An APS sheet consists of a finite set of rules and orders. A rule consists of a set of predicates and conditions associated with the predicates. $r = (P, C)$, where $P = \{p_1, p_2, \dots, p_n\}$ denotes a set of predicates and C denotes a set of conditions. We describe a rule in APS as,

```
<p, attribute> <- <condition>
```

where p is a predicate of arity n in P .

condition denotes the condition with respect to the rule of a predicate.

The structure of rule in DTD is defined as following:

```
<!DOCTYPE rule[
  <!ELEMENT rule (predicate+,condition*)
  <!ELEMENT predicate (grant, cangrant )
    #IMPLIED>
  <!ELEMENT condition (grant, cangrant)*>
]>
```

4 Syntax of Temporal Authorizations

Access Policy Sheet (APS) allows an administrator to manage the rules separated from XML documents and DTD.

Temporal authorizations enforce a rule to have tenable validity. Formally, we add a time interval Δ_i to a rule, e.g., $r_i = (P, C)(\Delta_i)$, where r_i is the temporal rule which has a temporal argument Δ_i defined as $\Delta_i = (s_i, e_i)$. s_i is the start time and e_i is the end time.

In APS, we define a temporal rule as

```
{\tt <p, attributes> <- <conditions><time\_interval>}
```

For example,

```
<garnt, Alice, patient_info.xml,
//Star_Hospital/operation_info,
+, read&write, Bob> <-
<cangrant, Bob,
*+//Star_Hospital/operation_info, read>
<09/10/05,11/10/05>
```

This rule is applied to predicate **grant**, condition **cangrant** and the validity period of the authorization which contains the start time and the end time. Grantee Alice has the access right **read** and **write** on the Xpath specified object **hospital_info.xml**, with the Xpath **//Star_Hospital/operation_info**. Grantor Bob has the authorization to grant **read** on the all files of the same directory to others. The validity period of the rule is 09/10/05-11/10/05.

According to the structure defined in the associated DTD (omitted), the authorization will be able to be converted to the standard XML as follows.

```
<rule>
  <grant>
    <subject>
      <grantee>
        <name> Alice</name>
      </grantee>
    </subject>
    <object>
      <target>hospital_info.xml</target>
      <path>//nurse/operation_info</path>
    </object>
    <authorization_type> + </authorization_type>
    <access_right> read </access_right>
    <access_right> write</access_right>
    <subject>
      <grantor>
        <name> Bob</name>
      </grantor>
    </subject>
  </grant>
  <condition>
    <cangrant>
      <subject>
        <grantee>
          <name> Alice </name>
        </grantee>
      </subject>
      <object>
        <target>hospital_info.xml </target>
        <path>//nurse/operation_info</path>
      </object>
      <access_right> read </access_right>
    </cangrant>
    <validity>
      <start> 09-10-05 </start>
      <end> 11-10-05 </end>
    </validity>
  </condition>
</rule>
```

5 Conflict Resolution

Since both positive and negative authorizations can co-exist in our system, conflict resolution among rules must be considered. Also, since we allow implicit authorization (authorization via authorization propagation), implicit conflicts make the problem more complicated. The policy of “the most specific subject(or object) takes precedence” which is proposed by E. Bertino [1] cannot be adapted to our model. In fact, according to the inheritance hierarchy relation in the partial order chain, we can get the policy of the “the least specific takes precedence”. The basic idea of solving conflicts is outlined as follows.

5.1 General Rules

Using delegation relation. According to the delegation relation, if subject s delegates subject s' directly or indirectly an authorization on object o and access right a , then, when a conflict w.r.t o and a occurs, the authorization from s (i.e. s is the grantor) will always override the one from s' .

From authorization type inheritance. For two conflicting authorizations w.r.t. a subject, an object, and an access right, according to the inheritance hierarchy of authorization type $- > + > *$, the authorization with a lower partial order will override the one with a higher type order.

From subject inheritance. For two conflicting authorizations w.r.t. an object, a right, and an authorization type, according to the inheritance hierarchy of subjects, if $s > s'$, then the authorization w.r.t. s will override the inherited one with s' .

From object inheritance. For two conflicting authorizations w.r.t. a right, a grantor, and a grantee, we consider the object inheritance relation. According to the inheritance hierarchy of objects, if $o > o'$, then the authorization on o will override the inherited one on o' .

From access right inheritance. For two conflicting authorizations w.r.t. a grantor, a grantee, and an object, according to the inheritance hierarchy of access rights, if $a > a'$, then the authorization on a will override the inherited one on a' .

5.2 Solving conflicts for Temporal Authorizations

According to the definition of temporal authorization in the preceding section, we denote by $r_i(\Delta_i)$ the temporal authorization, where $\Delta_i = (s_i, e_i)$ is the validity period of rule r_i , s_i is the start time, and e_i is the end time. Our conflict resolution is twofold: resolution without the time factor (given in the preceding section) and resolution with the consideration of the time factor. For example, for two conflict authorizations $r_i(\Delta_i)$ and $r_j(\Delta_j)$, we consider the conflict resolution of the r_i and r_j omitting the time factor first, using the methods we discussed in the preceding section. Then, we consider the time factors Δ_i and Δ_j . We denote by ϕ the time overlap of two temporal authorizations, i.e., $\phi = \Delta_i \cap \Delta_j$, by \Rightarrow an override operator, and by \Leftrightarrow a conflict operator.

Suppose we have two rules $r_i(\Delta_i) \Leftrightarrow r_j(\Delta_j)$, where $\Delta_i = (s_i, e_i)$, $\Delta_j = (s_j, e_j)$. If $\phi \neq 0$, we have the following cases.

When $s_i = s_j$ and $e_i = e_j$, then we have

$$\begin{cases} r_i \Rightarrow r_j : r_i(s_i, e_i) \\ r_j \Rightarrow r_i : r_j(s_j, e_j) \end{cases}$$

which means two conflict authorizations completely overlap. If $r_i \Rightarrow r_j$, then we have $r_i(s_i, e_i)$. If $r_j \Rightarrow r_i$, then we have $r_j(s_j, e_j)$. The following cases are self-explanatory; therefore, we omit the explanation.

In the case of $s_i \neq s_j, e_i = e_j$, we have

$$\begin{cases} r_i \Rightarrow r_j : r_i(s_i, e_i), r_j(s_j, s_i) \\ r_j \Rightarrow r_i : r_j(s_j, e_j) \end{cases}$$

In the case of $s_i = s_j, e_i \neq e_j$, we have

$$\begin{cases} r_i \Rightarrow r_j : r_i(s_i, e_i) \\ r_j \Rightarrow r_i : r_j(s_j, e_j), r_i(e_j, e_i) \end{cases}$$

In the case of $s_i \neq s_j, e_i \neq e_j$, we have

$$\begin{cases} r_i \Rightarrow r_j : r_i(s_i, e_i) \\ r_j \Rightarrow r_i : r_j(s_j, e_j), r_i(s_i, s_j), r_i(e_j, e_i) \end{cases}$$

When $s_i > s_j, e_i > e_j$, we have

$$\begin{cases} r_i \Rightarrow r_j : r_i(s_i, e_i), r_j(e_i, e_j) \\ r_j \Rightarrow r_i : r_i(s_i, s_j), r_i(s_j, e_j) \end{cases}$$

If there is no time overlap between two conflict authorizations, then each rule is taken separately without any influence from the other.

$$\left\{ \begin{array}{l} r_i \Leftrightarrow r_j \\ \Delta_i \cap \Delta_j = 0 \end{array} \right. : r_i(\Delta_i), r_j(\Delta_j)$$

6 Conflict Resolution with Authorization Propagation

Authorization propagation is implemented in terms of the partial order of subjects, objects and access rights. As defined in [4], we allow the implicit rules derived from the explicit rules in terms of partial ordering.

Figure 2: Rule propagation in a DOM tree.

Figure 2 shows an XML DOM tree, where object \circ_1 is the root of the tree, \circ_4 and \circ_2 are the nodes on one branch of the tree. \circ_4 is the descent node of \circ_2 . According to the partial order rule of the propagation on the objects we introduced before, there exists a partial order relation $\circ_2 > \circ_4$.

Suppose that in APS there are two authorization rules r_4 and r_2 actively applied to \circ_4 and \circ_2 , respectively. With authorization propagation, r'_4 is derived from r_4 . The authorization rule w.r.t. \circ_2 is then affected by r'_4 . If r_4 is in conflict with r_2 , then r'_4 is also in conflict with r_2 . The conflict resolution discussed in Section 6.1 is still applicable.

We now discuss it further by considering the time factor. Suppose that the above authorizations are temporal rules, $r_4(\Delta_4)$ and $r_2(\Delta_2)$. For \circ_2 , $r'_4(\Delta_4)$ derived from $r_4(\Delta_4)$ is also applied. Consequently, we have

$$\left\{ \begin{array}{l} r_4(\Delta_4) \Leftrightarrow r_2(\Delta_2) \\ \Delta_4 \cap \Delta_2 = 0 \end{array} \right. : r'_4(\Delta_4) \not\Leftarrow r_2(\Delta_2)$$

and

$$\left\{ \begin{array}{l} r_4(\Delta_4) \Leftrightarrow r_2(\Delta_2) \\ \Delta_4 \cap \Delta_2 \neq 0 \end{array} \right. : \left\{ \begin{array}{l} r'_4(\Delta_4) \not\Leftarrow r_2(\Delta_2); \\ r'_4(\Delta_4) \Leftrightarrow r_2(\Delta_2); \end{array} \right.$$

Here, we give an example. Suppose that in XML document `medical.xml`, there are two nodes in the DOM tree, `//hospital/room-info/` and its child node `//hospital/room-info/patient/`. According to the hierarchy relation of the objects, we have a partial order relation:

```
{\tt //hospital/room-info/ >
hospital/room/patient/}.
```

Assume that $r_1(\Delta_1)$ and $r_2(\Delta_2)$ are two temporal rules w.r.t. the above objects respectively.

```
r1(\Delta_1):
<grant, Alice,medical.xml,
//hospital/room-info/,+,read,Bob>(01/04/05,01/07/05)
r2(\Delta_2):
<grant, Alice,medical.xml,
//hospital/room-info/patient/,-,read,Bob>(01/06/05,01/12/05)
Through the propagation,  $r'_2(\Delta_2)$  is derived from  $r_2(\Delta_2)$ . That is,
r'_2(\Delta_2):
<grant, Alice, medical.xml
//hospital/room-info/,-,read,Bob>(01/06/05,01/12/05)
Obviously, for the same object medical.xml//hospital/room-info/,  $r'_2(\Delta_2)$  is in conflict with  $r_1(\Delta_1)$ .  $\Delta_1 = (s_1, e_1) = (01/04/05, 01/07/05)$  and  $\Delta_2 = (s_2, e_2) = (01/06/05, 01/12/05)$  follow the case,  $s_2 > s_1$  and  $e_2 > e_1$ . According to the conflict resolution we analyzed in section 6.2,  $r_1$  will override  $r'_2$  in the period of 01/04/05 to 31/05/05 and  $r'_2$  will override  $r_1$  in the period of 01/06/05 to 01/12/05.
```

7 Conclusion

Access control in XML documents is very complicated and difficult to manage. Access Policy Sheet (APS) provide us with a concise methodology to resolve the problem. In this paper, we proposed a temporal APS which can handle time related authorizations including conflict resolution, authorization delegation, authorization propagation. Based on our previous work, our new model can be used to satisfy the temporal requirement for XML authorizations.

This paper presents a compositional formal framework for the specification of our temporal access control policies. With a temporal intervals of validity, the authorization would automatically

revoked when the associated temporal interval expires. By the hierarchical relationships along with the partial orders defined in APS, we had given the conflict resolutions in several conditions.

- [9] Francois Siewe, Antonio Cau, Hussein Zedan, A Compositional Framework for Access Control Policies Enforcement, *FMSE'03, October 30, 2003, Washington, DC, USA*, pp 161-172.

References

- [1] E.Bertino, P.A. Bonatti and E. Ferrari , A temporal role-based access control model, *ACM Transactions on Information and System Security*, 2001, 4(3):pp191-233.
- [2] Li Qin, Vijayalakshmi Atluri, Concept-Level Access Control for the Semantic Web, *ACM workshop on XML Security*, October ,2003.
- [3] Designing a Distributed Access Control Processor for Network Services on the web. *ACM workshop*, Nov,22, 2002.
- [4] D. Samarati, E.Bertino and S. Jajodia, An Authorization Model for a Distributed Hypertext System, *IEEE Trans On Knowledge and Data Engineering*, 8(4), pp 555-562 ,1996.
- [5] Chun Ruan, Vijay Varadharajan and Yan Zhang, A Logic Model for Temporal Authorization Delegation with Negation, *Springer-Verlag, ISC 2003, LNCS 2851*, pp 310-324
- [6] Jing Wu, Yi Mu, Jennifer Seberry, and Chun Ruan, Access Policy Sheet for Access Control in Fine-Grained XML, *The First IFIP Workshop on Trusted and Autonomic Ubiquitous and Embedded Systems (TAUES 2005)*, Lecture Notes in Computer Science, Springer Verlag, 2005, pp. 149-161.
- [7] Chun Ruan and Vijay Varadharajan and Y. Zhang, Logic-based reasoning on delegatable authorizations, *In proc. of the 13th international Symposium on Security and Privacy, IEEE Computer Society Press*, 1997, pp 31-42.
- [8] E.Bertino, C.Bettini,E. Ferrari and P. Samarati, An access control model supporting periodicity constraints and temporal reasoning, *ACM Transactions on Database Systems*, 1998, 23(3): pp231-285.