Multiple Interactive Authority Model

M.N.Doja[†] and Dharmender Saini[††],

Jamia Millia Islamia(CSE Department), New Delhi, India

Summary
Electronic Document authorization is a process of making an electronic document legally bind to the rules and regulation of an authorizing enterprise. The electronic document can be authorized with a single entity –a single person authorizing an electronic document and a group - more than one person is responsible for authorizing an electronic document. An authorizer in the enterprise can have single authority lets say ,power of purchase and can have multiple authority for example power of purchase ,power of sell etc. Whereas multiple interactive authorities means when in an electronic deal both sender and receiver uses multiple authorities instead of single authority. The interaction means the authorities from both sides are used in a single deal. This paper presents a multiple interactive authority model and multiple authority representation in XML and output in XSL.

Key words:
Multiple Authority Model, Electronic Document, Policy,Iinteractive authority.

1. Introduction

The problem of authorization was raised in 1990 by Fischer [1] for the confirmation of the originality of source. Russell [2] in 1994 described the problem in detail and suggested various options available to the receiver. He suggested some basic principles of authorization at source like auditing by receiver, trusted third party originator, and self audit. He further categorized authorization in two parts i.e. person based authorization and rule based authorization. Person based authorization uses digital signatures and certificates, where as a rule based authorization is based on rules provided to the receiver for verification of authorization. Thomas woo [3] in 1998 suggested the design of distributed authorization service which parallels existing authentication services for distributed systems. In 2000 Michiharu and Santoshi [4] presented xml document security based on provisional authorization. They suggested an xml access control language (XACL) that integrates security features such as authorization, non-repudiation, confidentiality, and an audit trail for xml documents. During the period of 1996 to 2005 various types of authorization and its application like [5, 6, 7] were suggested. In 2005 [8] Burrows presented a method for XSL/XML based authorization rules policy implementation through filing a patent in united state patent office. he implemented XSL/XML based authorization rules policy on a given set of data and used an authorization rules engine which uses authorization rules defined in XSL to operate on access decision information (ADI) provided by the user. Inside the authorization rules engine, a boolean authorization rules mechanism is implemented to constrain the XSL processor to arrive at a boolean authorization decision. Now we, in this paper, are presenting a new multiple interactive authority model and the corresponding policy implementation in XML/XSL.

This paper is organized in four parts. Part 1 presents introduction to the problem addressed , Part 2 explain the multiple authority model, Part 3 presents the method of writing XML policy for such model and Part 4 present the solution to the multiple authority interaction problem.

2. Multiple Authority Model

Multiple authority model involves sender and receiver who have multiple powers to exercise. For example an employee in an financial department have powers of purchase (Signing authority of $100,000) and power of selling some products produced by the company – (for example power of selling products of $500,000) we propose a new multiple authority model which handle interaction between seller and buyers authorities and we call them interactive authorities

2.1 Assumptions and Description

Refer Table 1, suppose at sender and receiver side an authority database comprising of XML authorities is maintained. The authorities unique ID's are generated according the following rule.

(i). Let Zp* be a group of size p where p is a large prime numbers. So Zp= {0.1, 2, 3…….p-1}.

(ii). Let a person at sender has to authorize an electronic document M to be sent to the receiver with his/her multiple authority A [m].

Let A[m] = A [2] = [A1, A2] be a multiple authority (having more than one authority) having two authorities A1 and A2. So A[m] = [A1, A2, A3……..Am] having m authorities.

(iii). Let α be the generator of the group Zp

$X = (A1 \times A2)^{\alpha} \bmod p$

$N1 = A1^{1/\alpha} \bmod p$

Manuscript received March 5, 2008
Manuscript revised March 20, 2008

$N2 = A2^{1/\alpha} \bmod p$

Then a person at the sender end sends to the receiver

[Ex [M], H (M), X, N1, N2]

Where (x,y) is public key pair for the receiver i.e the communication is taking place using public key infrastructure.

Ex[M] = the document M encrypted with public key x of the receiver.

H(M)=hash of document m for message authentication at receiver end.

Let us assume receiver receives N1' for N1, N2' for N2 and X' for X, H' (M) for H (M), and M' for M.

Then the receiver verifies

Some authority A[i]? = $(N1')^{\alpha} \bmod p$ and generate the corresponding XML and XSL authority file.

Try for second authority A[i]? = $(N2')^{\alpha} \bmod p$ and generate the corresponding XML and XSL authority file.

Then he verifies

$(X')^{1/\alpha} = (N1' \times N2')^{\alpha} \bmod p$

and H(M')=H'(M) for message authentication.

If everything matches, then receiver got assured that the document M is properly authorized and well within the limit of multiple authority of the sender.

After getting assured of this the receiver check the generated authority in XML and XSL he gets out put as discussed below in part 3

Table 1 An Authority database

Zp	**XML policies**	**Associated XSL file for OUTPUT**
0		
1		
2		
.		
.p-1		

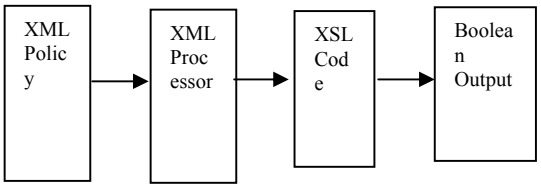

Fig. 1 XML Policy Processing.

3. XML Policy Representation, Evaluation and Output

The Fig 1 demonstrates the submission of xml policy to the xml processor (for example internet explorer or any other browser) then the link given in the xml for xsl file is referenced for xml policy condition. Then the xsl file is evaluated and the resulted output is produced. Below given is the XML policy which is about a user detail and its corresponding style sheet file (xsl file) and the output.

XML Policy:

```
<?xml version="1.0" ?>
<?xml-stylesheet type="text/xsl" href="C:\Documents and Settings\Administrator\Desktop\xml\xyz.xsl" ?>
<XMLADI>
<user>
<name>smith</name>
<ssn>1234</ssn>
</user>
</XMLADI>
```

XSL Styelsheet for converting XML to XHTML

```
<?xml version = "1.0"?>
<xsl:stylesheet version ="1.0" xmlns:xsl="www.w3.org/1999/XSLT/Transform">
<xsl:output method='html'/>
<xsl:template match="/">
<html>
<body>
<xsl: select = "//" />
<xsl:if test= "user/name='smith'">
<table border="1">
<tr bgcolor = "#1acd31"><td>
!Access allowed
</td></tr></table>
</xsl:if>
</body>
```

```
</html>
</xsl:template>
</xsl:stylesheet>
```

OUTPUT:
! Access Allowed

Multiple Authority Representation in XML:

The XML policy writing methods are given at [10]. The simple example of multiple authorities for a group of people is encoded as

```
<?xml version="1.0" encoding="UTF-8"?>
<document>
<nauauthz>
  <user>
        <name>allow_users</name>
<value>user4<id>ID4</id</value>
         <mulauthority>
<purchase>
<limit>30</limit>
        </purchase>
<itemorder>
<itemlimit>20</itemlimit>
        </itemorder>

</mulauthority>
</user>
            </nauauthz>
                  </document>
```

The policy statement says user4 having id as ID4 have multiple authority of purchasing up to 30 lakh and authority of ordering item up to 20Lakh.

4. Multiple interactive authorities

Let party P1 is at the sender end X and P2 be at the receiver end Y. They have multiple authorities [A1, A2] at sender end and [K1, K2] be the multiple authorities at receiver end. The multiple authority for both interactive end is represented by X=A1 S + A2 B and Y=K1 S + K2 B. where S represent that the K1 and A1 is to sell something and K2 and A2 is to buy something. Let the parties P1 and P2 make deal between them make interaction of these multiple authorities in this deal. The deal D in terms of authorities interaction can be represented by D = [A1 op1 A2] op2 [K1 op3 K2], Where op1, op2, and op3 represent some binary operations.

4.1 Possible operations [9]

For arithmetic modulo n, let Zn denote the set
Zn = {0, 1, 2, 3… n – 1}

Zn is obviously the set of remainders with arithmetic modulo n. It is called the set of residues.
The following equalities hold:
$[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$ (i)
$[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$ (ii)
$[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$ (iii)
with the ordinary arithmetic meaning to be ascribed to the +
and × operators. a, b belongs to Zn.
The above mentioned equalities (i),(ii), and (iii) can be used to introduce interaction among authorities.

The interaction of authorities can be better understood with the help of an example.
Example: By using $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$ equation. The Left hand side of equation is used at sender side and right hand side is used at receiver side select us assume A1=2, A2=3, K1=4, K2=5. Then,the sender perform the following calculations:

$D= [[2 \bmod 11 + 3 \bmod 11] \bmod 11 + [4 \bmod 11 + 5 \bmod 11] \bmod 11] \bmod 11$

$D= [[2+3] \bmod 11 + [4+5] \bmod 11] \bmod 11=5$

$D= [5+9] \bmod 11$

D=3

The sender sent the Hash of D i.e H (D) to receiver

At receiver end

Receiver receives the H' (D)

and performs

$(2+3) \bmod 11= 5$
$(4+5) \bmod 11 =9$
$(5+9) \bmod 11=14 \bmod 11=3=D'$
Calculate the Hash of D' i,e. H(D') with similar algorithm as at the receiver end and check if H(D') = received H(D) If all the above condition matches then it assures about the authorized deal having interaction of authorities of both side.

Conclusion

We have presented the multiple authority model with interactive authority and the associated policy representation in Xml/XSL. We have further shown the interaction of authorities with help of an example. We further suggested the multiple authority interaction with usage example

Applicability and Future Scope

The invention is applicable in ecommerce transactions where two parties apply multiple interactive authorities on electronic documents during ecommerce transactions. For example in exchanging goods, services etc. The scheme can be extended to observe hierarchy among group people interacting party.

Acknowledgments

We thank Dr I. J. Kumar, Dean and Head (Bharati Vidyapeeth's college of Engineering, New Delhi) for his encouragement and support in carrying out the work

References

[1] A.M. Fischer,"Electronic document Authorization", Proc. IFIPWG 6.5, Int Symposium, Zurich, 1990.

[2] Selwyn Russell," Audit-by-receiver paradigms for verification of authorization at source of electronic documents", Computers and security; pages 59-67, 1994.

[3] Thomas Y.C. Woo, Simon S. Lam,"Authentication for distributed systems" IEEE Comput., Jan 1998, Pages 39-52

[4] Michiharu and Satoshi,"XML document security based on provisional authorization", 2000 ACM, Pages 87-95.

[5] Patroklos G. Argyroudis and Donal O'Mahony,"Towards flexible authorization management", Proc. ISSC 2005, IEEE Computer Society.

[6] Torsten Braum, Hahnsand Kim," Efficient authentication and authorization of mobile users based on peer - to - peer network mechanism", International Conference on system sciences, IEEE 2005

[7] E. Bertino, F. Buccafurri, D. Ferrari, and P. Rullo, "An Authorization Model and Its Formal Semantics," Proc. 5th European Symposium on Research in Computer Security", 127-142 (September 1998).

[8] Burrows," Method and apparatus for XSL/XML based authorization rules policy implementation", United States Patent Application 2005-0102530A1

[9] Avi Kak, "Finite Fields (PART 2)", Lecture Notes on \Introduction to Computer Security" January 31, 2007

[10] CAS and NAUauthZ - XML Authorization Rules http://www4.nau.edu/its/sia/CAS_NAUauthZ/nau_authz_xml.asp

[11]. M.N.Doja, Dharmendra Saini," Binding Group Authorization Rules With XML Documents With Output In XSL", ICDM 2008, IMT,India ,

M.N.Doja is a professor in Computer Science and engineering Department, Jamia Millia Islamia, New Delhi, India. he has been the Head of Department and Chairperson for research and development board for the same department, for several year.

Dharmender Saini received his B.Tech. from T.I.T&S in Computer Science in 1999 and M.Tech.in 2006 in Computer science and engineering from Guru jhambheswar university, hissar. During 2000-2007, he stayed in Bharati Vidyapeeth College of Engineering as Lecturer and Assistant Professor, Presently persuing PhD from Jamia Millia Islamia University,New Delhi,India