Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

A Fine Grained Access Control Model Based on Diverse Attributes

Dr. Rajender Nath[1] and Gulshan Ahuja[2]

[1] Kurukshetra University, Kurukshetra, Haryana, India.

Received: 16 July 2011 Accepted: 8 August 2011 Published: 22 August 2011

Abstract

As the web has become a place for sharing of information and resources across varied domains, there is a need for providing authorization services in addition to authentication services provided by public key infrastructure (PKI). In distributed systems the use of attribute certificates (AC) has been explored as a solution for implementation of authorization services and their use is gaining popularity. AC issued by attribute authority (AA) facilitates identification of a service requester and can be used to enforce access control for resources. AC of a service requester is used as part of credentials supplied during the service request for accessing any resource. As there exist potentially multiple issuing domains which issue credentials, therefore the target domain must allow access to resources by considering different credentials and must be able to decide about which set of attributes can be considered as valid attributes for making access control decisions. In this paper, we present an authorization based access control model that allows a fine grained access control to resources in an open domain by utilizing attributes issued by diverse attribute authorities.

Index terms— attribute certificates, attribute authority, authorization, access control.

1 INTRODUCTION

ith continually changing business environment privacy and protection of resources is becoming more and more important. The access control to resources is bound up with the authentication and the authorization. There is a strong need felt for receptive authorization infrastructure that can cater for rapidly changing dynamic environments and should be able to validate the identity of service requesters.

The commonly used credentials for access are identity credentials, attribute credentials and authorization credentials. Identity based access control systems require identity certificates which are issued and certified by certification authorities (CA). When a CA issues an identity certificate, it binds a particular public key to the name of the service requester (SR) identified by the certificate. In addition to a public key, a certificate always includes information such as the validity period, the name of the CA, the digital signature of the issuing CA etc. Identity based credentials are more suitable where service requesters are already known to the service provider (SP) through the process of registration. This approach works well in a tightly coupled environment. Identity based access control puts a constraint of prior registration of every service requester which limits the scalability of overall system. Another access control approach is based on the authorization certificates which are based on the principle of delegation of rights and responsibilities. The authorization certificates are issued by the authorization authorities who have rights to access the specific resource and thus can delegate full or subset of rights to other users. The authorization certificates usually contain the identity of the resource, identity of the service requester, access rights to access the resource, etc. The advantage of authorization certificates are that service requesters are authenticated in their own domain and another service requester to whom the rights have been delegated can realize the access control based on delegated rights. A different area of research developments is access control based on attributes. In attributes based access control systems the access policy is based on the

various attributes which are assigned to the service requesters. The attribute certificates are issued by Attribute Authority (AA) and these contain the name value pairs of the various attributes. Attributes based authorization offers more flexibility and scalability for an open and distributed environment. The use of AC based on privilege management infrastructure (PMI), allows including and revoking attributes and can contain information about the privileges or roles of a user. AC conveys a short-lived attribute about a given subject and can be used to authenticate the identity of the attribute certificate holder. A real time problem arises when the request made by a service requester requires attributes which have been issued by diverse attribute authorities and are located at different locations. The authorization efforts become more difficult when two or more AAs save attributes for a service requester with different identities. The rest of this paper is structured as follows. Section II highlights the related work. Section III highlights the requirements to develop a new model based on diverse attributes. Section IV describes the implementation architecture and explains the working of proposed model. Finally Section V concludes and briefly describes scope for the future work.

2 RELATED WORK

Traditional access control approaches base their authorization decisions on subject's identity. A number of research papers based on attributes based authorization have been proposed by researchers. Ioannis Mavridis et al. [1] proposed a mechanism for access control based on attribute certificates for medical Internet applications. David Chadwick [2] proposed X.509 privilege management infrastructure. Later David Chadwick et al. [3] proposed Role-Based Access Control with X.509 Attribute Certificates. The proposed approach in paper adopted the standard X.509 PMI to build an efficient role-based trust management system in which role assignments can be widely distributed among organizations, and an XMLbased local policy determines which roles to trust and which privileges to grant. Jordi Forne et al. [4] presented an implementation of an authorization system for web based applications based on the ITU-T X509 recommendations which specifies use of privilege management infrastructure for realizing access control. Access control mechanism based on authorization, using attributes issued by a remote attribute authority, has been proposed by S. Cantor. [5]. Wei Zhou et al. [6] proposed a role based access control with attribute certificates. Alfieri R. et al. presents a VOMS model [7] for managing authorization in a Grid Environment and allows coalition of multiple attributes. Eric Yuan [8] proposed an attribute based access control (ABAC) model as a new approach, which is based on subject, object, and environment attributes and supports both mandatory and discretionary access control needs. M Liu et al. [9] proposed an attribute and role based access control model ARBAC for web services. However, the role remains static and when assigned it becomes out of date. Alan H. Karp [10] proposed an implementation based on authorization based access control (ABAC) for services oriented architecture. David W Chadwick [11] presented a model and protocol elements for linking AAs, service providers and user attributes together, under the sole control of the user and allowed merging the attributes from multiple AAs in order to grant the user access to its resources. Frikken K et al. [12] proposed an approach for attribute based access control with hidden policies and hidden credentials. Shen Hai Bo et al. [13] proposed an attribute based access control model for web services. Nirmal Dagdee et al. [14] proposed an access control methodology for sharing of open and Domain confined data using Standard Credentials. The methodology requires that various types of standard credentials and related attributes are identified and published by some apex authority so that the resource providers can define their access policies in terms of these standard credentials. In real terms, identification of standard credentials is a very difficult task and is not suitable for largely distributed systems having millions of service requesters. Regina N. Hebig et al. [15] describe a prototype implementation with an architecture based on the standards XACML, SAML, WSPolicy, WS-SecurityPolicy and WS-Trust which puts the focus on sharing identity and attribute information across independent domains for the purpose of access control.

3 III.

4 PROBLEM FORMULATION

The service requester's credentials may be stored or issued in a variety of places, for example, each AA may store the attributes or the credentials it issues in its own repository. When a service requester makes a request to service provider for accessing a resource and presents its credentials. At service provider's end, the presented set of attributes may not be sufficient enough to grant access to a resource. This necessitates that service requester must collect together the credentials required for making access to a resource. David W Chadwick [11] presented a model and protocol elements for linking attributes from multiple AAs. His approach requires input from the user who wish to link attributes from multiple AAs. However, the main issue with his approach is that user has to initiate multiple browser instances and execute steps for cross linkages between multiple attribute authorities. If the number of attributes required for grant of access belongs to multiple attribute authorities, the same process is to be carried multiple times for providing linkages between multiple attribute authorities. This makes the task of service requester more complex and time consuming. We propose a new model where the service requester's task of creating linkages is eliminated and the process of linkage is initiated by service provider only. The proposed work also takes care of the privacy concern of the service requester to ensure that service provider will be able to link attributes from multiple attribute authorities only when service requester desires to create linkages with multiple attribute authorities.

IV.

5 PROPOSED MODEL

This section describes the details of proposed model. The approach requires that all organizations who are willing to exchange and share information among them must form agreements for a number of conditions i.e. security mechanisms to be used, attribute definitions etc. and must pre establish a certain level of trust. Such sort of arrangement is termed as federation and is same as Shibboleth federations **??**16]. The mechanism assumes that linking between AAs is based on secured shared information and there also has to be secured shared information between a service requester and all attribute authorities where service requester is registered for attribute sharing.

An authorization model based on diverse attributes from different attribute authorities is shown in Figure 1. The diagram reflects following components involved in the access mechanism.

6 a) Overview

A service requester can acquire multiple identities by registering with a number of attribute authorities. The decision to register with the attribute authority can be based on its reputation, quality of service etc. The mechanism requires that every service requester and all AAs to whom requester wishes to link must exchange and agree upon conversation framework for transfer of information between them.

7 PDP PEP

The service provider should not be able to obtain attributes from any AA without knowledge and permission from the service requester. The AAs who are willing to exchange information must make groups with predefined policies and rules. There has to be one or more than one primary attribute authority. The primary attribute authorities act as the root for all other AAs which are members of the group. Before making a request for accessing any resource, the service requester must acquire credentials from one of the primary certified authority. The attributes returned by the primary AA contain a basic set of the attributes along with information about all AAs for which service requester has already registered and has agreed to use additional attributes. Each service provider in the federation is free to decide about the number and types of attributes for granting access requests. The service providers may grant access on basic set of attributes or may decide to impose more security check by imposing requirement for additional attributes from one or more AAs.

8 b) SAML based conversation framework

We use SAML assertions for describing conversation tokens. Figure 2 depicts conversation framework between service requester and provider. Figure 3 describes the format of SAML based conversation tokens.

Let ATS b be the basic set of attributes and ? is an alphabet, a non-empty finite set. Let service requester SR is registered with three attribute authorities. As identity SR 1 with attribute authority AA1, as identity SR 2 with AA2, as identity SR 3 with AA3. The conversation token from the primary attribute authority to service requester will be of the form as defined below.

ATS {SR, Time_Stamp}P B K SR AA1{ SR 1, Time_Stamp}P B K AA1 AA2{ SR 2, Time_Stamp}P B K AA2 AA3{ SR 3, Time_Stamp}P B K AA3 c) Authentication of conversation tokens As per figure 1 and figure 2, the authorization process is divided in to 2 parts: obtaining of basic set of attributes from the primary attribute authority and use of attributes for making authorization decisions. For the first part, since it is assumed that service requester trusts the primary attribute authority and can decrypt and obtain the basic set of attributes using its private key P V K SR. The primary attribute authority also passes on the encrypted info for every other AA where service requester's attributes are already located. This encryption is carried using public key of the corresponding attribute authority. The second part is an establishment stage where ECT is used by service provider to make access decision. When a service requester makes a request for accessing a resource, the service provider executes following tasks:

Task 1: Service requester obtains credentials from primary attribute authority. The credentials issued by primary attribute authority to the service requester are encrypted using public key of respective authority and are sent in format as in figure 3.

Task 2 : The service requester decrypts the basic attributes, using its private key P V K SR and presents the basic set of attributes along with encrypted info about AAs, acquired from primary AA, to service provider.

Task 3 : On receiving the request, the service provider checks for the basic set of attributes against already specified policies in the policy store to decide whether access can be granted or not.

Task 4 : In case the existing policies do not allow access based on basic set of attributes contained in the service request, the PDP module passes the service request to the AALM module.

Task 5 : AALM module extracts the information from the service request to find out for which all other AAs service requester has already registered. The request message along with the requester's URL was encrypted using public key of concerned AA so it can be decrypted using private key by the concerned AA only. The service provider just knows that at which attribute authority the service requester is registered so this helps to maintain the privacy concern of the requester because service provider can not determine the identity and attributes of the requester located on a particular AA.

Task 6 : AALM sends a request message for the required attributes to the concerned AAs along with the encrypted info about requester's identity and date time stamp.

Task 7 : AA decrypts the information corresponding to its requested attribute set using its private key and extracts the identity of service requester and also verifies the date and time stamp for validity of message. For example SR had already registered with AA1 as SR 1 , therefore upon successful decryption of the message, AA1 can ascertain about SR 1 .

Task 8 : To make sure that SR is willing to allow attributes from AA, it redirects an authentication request to SR.

Task 9 : Once the service requester authenticates with AA, the information regarding attributes required by the service provider is shown and service requester is given a choice to allow passing back the set of attributes to the service provider.

Task 10 : Once the confirmation is made by the service requester, the one or more required attributes are sent back to the service provider.

Tasks from 6 to 9 are repeated for every AA to whom AALM module sends a request for additional attributes. In the event of any AA failing to provide required attributes the request is terminated with an appropriate response to the service requester.

The access control decision based on diverse attributes can be realized in terms of a function f (ATS b) or f (ATS b $\times$ ATS i $\times$ ATS j $\times$ ATS j)

Where ATS b is the basic set of attributes for SR, and ATS i , ATS j , ATS j are the set of attributes for three different attribute authorities identified as AA i , AA j , AA k respectively.

The above mentioned function is implemented and used by PEP component to decide whether the access to resource can be allowed based on basic set of attributes or attribute assignments from multiple AAs can be evaluated. The implementation of function solely depends upon the policies and requirements of the service provider. The evaluation outcome can be considered for granting access to the resource. The access control mechanism discussed in this paper allows in implementing fine grained access control based on multiple attributes. The proposed approach allows every service provider to decide the level of security for granting access request. The service provider can choose to allow access request based on the basic set of attributes or may put more restrictions by imposing requirements for attributes from one or more AAs. The use of basic set of attributes works well [1]

Figure 1:

[1] © 2011 Global Journals Inc. (US) Global Journal of Computer Science and Technology Volume XI Issue XV Version I

? Policy Decision Point (PDP) evaluates the applicable policies against service requests. PDP checks for the available attributes in the service request to
check whether access request can be granted or
not. In case the attributes contained in service
request are not sufficient enough for grant of access
to resource, it hands over the request parameters
along with information about additional attributes
required for grant of access request.
? Attributes authorization and linker module (AALM) is
responsible for contacting concerned attribute
authorities for making request of additional
attributes and sends back the attributes received
from multiple attribute authorities to PDP.
? Policy store contains policies for making access
control decisions. The policies can be stored in XML
format as it allows standard representation of
access control rules. Extensible access control
markup language (XACML) [17] [17] can be used to
allow implementation of access control policies. ? Policy management interface allows handling of policies in the policy store.

Figure 2: ?

V.

.1 CONCLUSION

In this paper, authors have proposed a mechanism for allowing access to a resource based on the multiple attributes from one or more AAs. The merit of the proposed approach is that service provider can link to the attribute authorities and obtain attributes for grant of access only when it is permitted by the service requester. Even if the service provider is able to determine that to which all AAs the service requester has already registered, it can not automatically obtain attributes without service requester's permission. The proposed approach focuses only on authorization of requests based on attributes. The future work may consider other aspects related with attributes based access without involvement of centralized authority and automated trust establishment.

[Hebig ()] 'A Web Service Architecture for Decentralized Identity-and Attribute-based Access Control'. Regina N Hebig . *IEEE International Conference on Web Services*, 2009.

[Mavridis et al. ()] 'Access Control based on Attribute certificates for Medical Internet applications'. Ioannis Mavridis , Christos Georgiadis , George Pangalos , Khair Marie . *Journal of medical Internet Research* 2001. 3.

[Dagdee and Vijaywargiya ()] 'Access control methodology for sharing of open and Domain confined data using Standard Credentials'. Nirmal Dagdee , Ruchi Vijaywargiya . *International Journal on Computer Science and Engineering* 2009. 1 (3) p. .

[Liu and Guo H Q (2005)] 'An Attribute and Role-Based Access Control Model for Web Services'. M Liu , Su J D Guo H Q . *proceedings of The Fourth International Conference on Machine Learning and Cybernetics*, (The Fourth International Conference on Machine Learning and CyberneticsGuangzhou, China) August 2005. p. .

[Shen et al. ()] 'An attribute based access control model for web services'. Hai Shen , Hong Bo , Fan . *Proceeding of the 7th International Conference on Parallel and Distributed Computing, Applications and Technologies*, (eeding of the 7th International Conference on Parallel and Distributed Computing, Applications and Technologies) 2006. IEEE.

[Attribute Certificates IEEE internet computing (2003)] 'Attribute Certificates'. *IEEE internet computing*, march-april 2003. p. .

[Frikken et al. (2006)] 'Attribute-Based Access Control with Hidden Policies and Hidden Credentials'. K Frikken , M Atallah , Jiangtao Li . *IEEE Transactions on Computers* Oct. 2006. 55 (10) p. .

[Yuan ()] 'Attributed Based Access Control (ABAC) for Web Services'. Eric Yuan . *IEEE International Conference on Web Services*, 2005.

[David and Chadwick ()] 'Authorisation using Attributes from Multiple Authorities'. W David , Chadwick . *Proceedings of the 15th IEEE International Workshops on Enabling Technologies Infrastructure for Collaborative Enterprises*, (the 15th IEEE International Workshops on Enabling Technologies Infrastructure for Collaborative Enterprises) 2006.

[Karp ()] 'Authorization-Based Access Control for the Services Oriented Architecture'. Alan H Karp . *Proceedings of the Fourth International Conference on Creating, Connecting and Collaborating through Computing*, (the Fourth International Conference on Creating, Connecting and Collaborating through Computing) 2006.

[Chadwick ()] David Chadwick . `http://sec.cs.kent.ac.uk/download/X509pmiNATO.pdf` *The X.509 Privilege Management Infrastructure*, 2002.

[Alfieri et al. (2005)] 'From gridmap-file to VOMS: managing authorization in a Grid environment'. R Alfieri , R Cecchini , V Ciaschini , L Dell'agnello , A Frohner , K Lorentey , F Spataro . *Future Generation Computer Systems* Apr. 2005. 21 (4) p. .

[Zhou and Meinel ()] 'Implement Role based access control with attribute certificates'. Wei Zhou , Christoph Meinel . *The 6th IEEE International Conference on Advanced Communication Technology*, 2004. p. .

[Chadwick et al.] *Role-Based Access Control*, David W Chadwick , Alexander Otenko , Edward Ball . with X.509.

[Cantor (2004)] *Shibboleth Architecture, Protocols and Profiles*, S Cantor . `http://shibboleth.internet2.edu/` 22 September 2004. (Working Draft 02)

[Hanarejos ()] 'Web-based Authorization based on X.509 Privilege Management Infrastructure'. J , M F Hanarejos . *IEEE Pacific Rim Conference on Communications, Computers and signal Processing*, 2003.