Integrating External User Profiles in Collaboration Applications

George Mathew
Department of Computer and Information Sciences
Temple University
Philadelphia, PA, USA
George.Mathew@temple.edu

***Abstract*—Due to the increase in federated nature of collaboration applications, users from multiple institutions have the potential to participate in activities centered around common regions of interest. However, existing technologies address external users at a coarse grained level. Consequently, mechanisms to integrate external user profiles into collaboration applications are practically non-existent. This prevents an end user from having locus of control in managing permissions to resources for users that are external to their parent institution. In this paper, the need for a fine grained access control mechanism for end users, that allows them to transparently manage permissions to external users in collaboration applications, is addressed. Mechanisms that need to be in place to provide a framework for realizing this capability are outlined. Some of the components that exist now are reviewed in this context. The end users will benefit from a holistic framework by having empowerment over resource management for external collaborators in a natural way.**

Keywords-Collaboration Application; External User Profile; Collaborative System Architecture

I. INTRODUCTION

Thanks to grid computing [1], federated technologies [2] and web services [3], the collaborative nature of applications are on the rise. These collaboration applications have to deal with users from multiple institutions and/or corporations. End users will find it necessary to identify a user in another institution or corporation to participate in an activity related to a common region of interest. In a collaborative document management system, this could be granting permission to an external collaborator to edit a document. In a collaboratively shared calendar system, granting access to one's calendar to an outside user is another scenario. The common thread in these use cases is the need for an end user to locate (or identify) a user from an external source and grant certain permissions to a resource. Granting permission to a resource is well understood. However, the problem of locating a user from an external source and incorporating his/her credentials into local environment is not well addressed. This becomes more interesting if the lookup and resource permissions management has to be as seamless as possible to the end user.

II. COLLABORATION APPLICATIONS

Collaboration applications tend to be distributed, networked and make use of local as well as non-local resources. Earlier middleware technologies DCE [4] and CORBA [5] eventually yielded to Web Services to realize Service Oriented Architecture. Web services has the added advantage of being platform neutral and programming language independent. Collaboration applications similar to shared calendars, document management systems and data grid systems are all tapping into this great potential. With web services acting as the conduit, applications can cross institutional and corporate boundaries. The growing business needs for inter-institutional activities can take advantage of this facility in collaborative applications. Jstor [6], caBIG [7] and DGI Integration project [8] are examples. The existing federated inter-institutional collaboration applications rely on the trust between institutions to gain access to resources. The users from an external institution are authenticated through an identity provider and the user profiles stay with the parent institution. Access to a trusted system or a limited set of exposed applications are managed by site administrators and the end user plays no part in it. This is a very restrictive state of affairs. The Grouper [9] project from Internet2 provides a mechanism to create groups from inter-institutional population. However, this mechanism does not allow end user transparency for controlling access to resources in collaboration applications.

III. USER PROFILES

A 'user profile' is a set of attributes that helps in identifying a user uniquely in a collaboration environment. The two complementary components of user profile controls, in collaboration applications contexts, are vested in two user populations: internal and external. The internal vs. external role of a user is dependent upon which component the subject of discussion is and which component the user belongs to.

A. Internal User Profiles

The first component in user profiles management encompasses mechanisms that facilitate the control of internal users over their profiles being exposed. One aspect of this facility is a mechanism that can provide users with limit control over exposure of their profiles to external services. This entails

Digital Object Identifier: 10.4108/ICST.COLLABORATECOM2009.8329
http://dx.doi.org/10.4108/ICST.COLLABORATECOM2009.8329

having a mechanism for internal users to interact with a profiles registry and setting their preferences. The second aspect is an external facing service that enforces the user preferences and serves requests from outside. This service implementation has to be based on standard protocols.

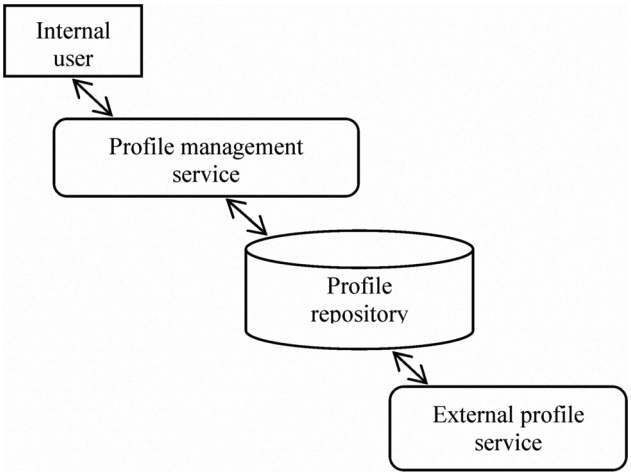

Fig 1. User Profile Management

Profile schema, part of World Wide Web Consortium's P3P specification is a standard for coding user profiles. InetorgPerson is another standard schema (used in LDAP). These schemas are widely used in inter-institutional collaboration applications. The issue of end user empowerment in controlling their profiles was addressed in the IDRepository project (Koch and Möslein [10]). The IDRepository concept addresses the user controls over their profiles outside of any collaboration application context. The underlying premise is that one should be able to control the degree of exposure of one's personal profile to another party [11]. Fink and Kobsa have done work on profile servers [12]. SAML and WS-Security are published standards used as the basis for federation services. Shibboleth [13], a widely used federation service that makes use of SAML assertions, allows the controlled delivery of user profiles to trusted sites. In general, the representations and delivery services that facilitate control of internal user profiles to external agencies have been studied. Components that make use of these mechanisms have been implemented. Toolkits (eg : Globus [14]) that take advantage of these are already in use.

B. External User Profiles

The second component of user profile controls is related to external users. This is the complementary aspect of allowing a collaboration application user to manage access controls for external users to shared resources within the context of the application. Signet [15] addresses the privilege management of access to resources and services at a higher level. It is a policy enforcer that guards the gate to grant or deny access to an application and does not deal with fine grained access control within the application.

Before proceeding further, a definition for 'region of interest' is in order. A 'region of interest' is the specific target (or resource) in a collaboration application that two or more collaborators are interested in. For example, an MRI may be the region of interest for a patient and doctor, in an electronic medical records system. A 'system of record' is the authoritative bookkeeper for the metadata associated with a given region of interest. Logical copies could be simultaneously in use within collaboration application contexts. In a shared calendar system, two or more users could be viewing the same events for a particular day. If an editing occurs on the region of interest (the calendar for the particular day), the metadata is updated on the system of record. The application may or may not have facilities to relay this updates to individual views of the other collaborators.

In order to facilitate controlling the permissions associated with the region of interest, two concepts need to be realized: 1) search capability to find the external user from a repository; and 2) associate permissions to an external user with the region of interest. In case the user knows the handle to the external user profile, it is not necessary to do a search.

IV. LOCATING EXTERNAL USER PROFILES

The external user profile repository could be a publicly exposed directory similar to LDAP or IDRepository. In a collaboration application context, the end user should be able to locate external users just as transparently as local users. This is a natural extension to traditional local application interaction. As an example, if Mike wants to give permission to Don (in the same institution, but in a different department Z) access to his shared calendar, Mike needs to know the user handle associated with Don. However, if Mike does not know Don's handle in the profile registry, he could use the fact that Don is in department Z to search for Don's user handle in the local user repository. A parallel can be drawn when searching for external users. The additional dimensionality of institution contributes to an extra attribute to the inter-institutional search. However, the search record can be kept consistent by tagging the value for institution attribute as 'local' when searching for users in parent institution. The list of institutions the user can choose from, can be restricted to the list of member institutions in a federation. Or, the institution attribute could be left open for the user to input. Once the attributes for the search are collected, the external user lookup service is engaged; provided the institution attribute is not 'local'. The alternative is to use a globally unique handle to associate user profiles. Proposals from OpenGroup have suggested globally unique user handles based on a combination of userid and a derivative of DNS domain name space [15]. If asd432 is the userid for a user in the organization with domain name dns.dom, the globally unique user handle could be asd432.dns.dom or some URI made up of the related components. To implement this, SRV record facility in DNS is made use of. Another option is to have an external central authority to hand out unique user handles. This mechanism will need the use of digital certificates. Commercial vendors are already doing identity vetting and user id provisioning (eg: crederity [16]). The user profiles need institutional affiliations as part of the user credentials to effectively work in a collaborative environment.

The profile service (or lookup service) in the external institution can return a real handle or camouflaged handle to the user. If a camouflaged handle is returned, a translator

Digital Object Identifier: 10.4108/ICST.COLLABORATECOM2009.8329
http://dx.doi.org/10.4108/ICST.COLLABORATECOM2009.8329

service has to mediate the association with the real user profile. Also, if multiple matches are returned, the end user has to pick the right external user. These two conditions are not difficult to deal with. Hence, for simplicity, assume a real user handle is returned. The end user who initiated the lookup can now assign permissions in the region of interest to the external user. If this user was never associated with any regions of interest (nor had a user profile created statically – see section V), this will trigger a registration for the external user in a local repository. This local registration could be accomplished by recording the information in two stores. One is a repository of external users. The other is a repository of permissions associated with external users. Keeping a single repository of external users makes the store shareable between multiple applications. Note that this repository can be different from the local repository for internal user profiles. For the purpose of clarity, let this repository be referred to as LREU (Local Repository for External Users).

V. STATIC AND DYNAMIC USER PROFILE CREATION FOR EXTERNAL USERS.

Creating profiles in LREU could be done statically or dynamically. Static profile creation would necessitate a system administrator to gather information about the external user and set up the profile in the LREU. This activity is outside the context of any collaboration application. Dynamic profile creation is initiated by a collaboration application and would create a profile for the external user in the LREU. The attributes necessary for the profile creation would be at the disposal of the application as a side effect of the search. Once LREU comes into existence, the search for external users should consult the LREU before contacting the external profile server (see fig 2). In fig 2, the branch labeled 1 is first traversed for checking external user profiles in LREU.

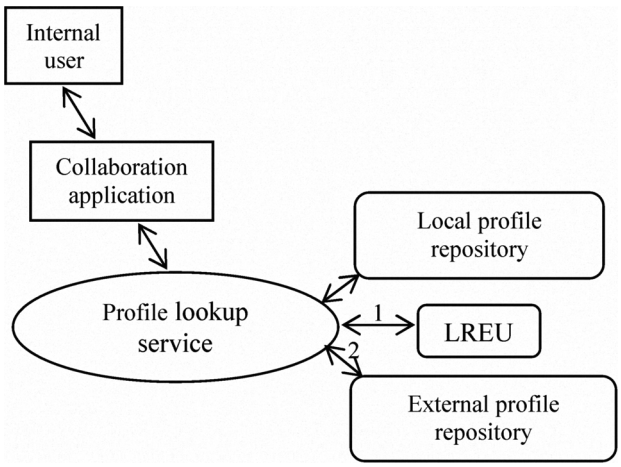

Fig 2. Profile locator service (with LREU)

Storing the permissions is usually done in containers built into the applications. The application can store a user handle and the permissions. However, it is possible to externalize the repository of ACL's (Access Control Lists). PIP (Policy Information Point) in XACML [15] can be used to store the access control for the user within the application. A hybrid model where ACL's of local users are within the application and those of external users are in XACML containers is another approach.

In case an institution does not have an externally open user profile repository, a collaborator should be able to initiate an invite. The invite could go out through any channel of collaboration.

VI. ACCESSING REGION OF INTEREST BY EXTERNAL COLLABORATORS

In a federated environment, if the external user later accesses the application by authenticating through an IDP (Identity Provider), the federation service can pass the same user handle (real or camouflaged) through a channel, and the collaboration application can honor the permissions set for this user on the region of interest. In this case, the external user should be able to use the application and work in a transparent way.

Another model is where the application running on the external user's local system allows the external user to interact with the region of interest with the permissions granted, as if it is a local activity within the application context. This is a natural way for users to work. However, this model requires a listener service that can relay the information and register the details related to permissions on the region of interest in a local repository. In this case, synchronous activities require a locking service.

VII. SUMMARY

In order for inter-institutional collaboration applications to present a transparent user experience that transcends collaborators from multiple institutions, various facilities are needed to be in place. Functionalities of the required components were elaborated. Some of the facilities that exist were outlined. However, more work needs to be done in making this a seamless experience for the collaborators. Mechanisms for a transparent user experience need to address 2 issues; 1) a locator service that allows end user to search and find a target user in an outside institution, and 2) underlying framework to hold the metadata associated with the region of interest. Users should be able to control the exposure of their profiles to external entities. Collaboration applications can benefit from a complete framework that provides seamless end user experience with fine grained control over regions of interest.

REFERENCES

[1] I. Foster and C. Kesselman, "The Grid 2 : Blueprint for a New Computing Infrastructure", (2nd ed), Morgan Kaufman, San Francisco, CA, USA, 2004.

[2] Aberdeen Group. "Federated identity systems: An executive white paper", Technical Report, Aberdeen Group, Boston, MA, USA, June 2002.

[3] E. Newcomer, "Understanding Web Services: XML, WSDL, SOAP and UDDI", Addison-Wesley, Boston, MA, USA, 2002.

[4] W. Rosenberry, D. Kenney and G. Fischer, "Understanding DCE", O'Reilly and Associates, Sebastopol, CA, USA, 1993.

Digital Object Identifier: 10.4108/ICST.COLLABORATECOM2009.8329
http://dx.doi.org/10.4108/ICST.COLLABORATECOM2009.8329

[5] "CORBA FAQ", http://www.omg.org/gettingstarted/corbafaq.htm

[6] "Jstor – Trusted archives for scholarship", http://jstor.org

[7] "caBIG – Cancer Biomedical Informatics Grid", http://cabig.nci.nih.gov

[8] "D-Grid Integration project", http://dgi.d-grid.de

[9] "Grouper – Open source toolkit to manage groups", http://grouper.internet2.edu

[10] M. Koch and K.M. Möslein, "Identities Management for E-Commerce and Collaboration Applications", International Journal of Electronic Commerce, 9(3), M.E.Sharpe, Inc., Armonk, NY, USA, 2005. pp. 11-29

[11] R. Clark, "Internet privacy concern confirm the case for an intervention", Communications of the ACM, 42(2), February 1999, pp. 60-67

[12] J. Fink and A. Kobsa, "A review and analysis of commercial user modeling servers for personalization on the World Wide Web", User Modeling and User-Adaptation Interaction, 10(2-3), Springer Netherlands, June 2000, pp. 209-249

[13] "Shibboleth – Federated Single Sign-On Software", http://shibboleth.internet2.edu

[14] B. Sotomayor and L. Childers, "Globus Toolkit 4 : Programming Java Services", Morgan Kaufman, San Francisco, CA, USA, 2005

[15] "Signet Privilege Management System", http://middleware.internet2.edu/signet

[16] "The Open Group – Identity Management", Available: http://www.opengroup.org/dif/dirday25/cc25disc.htm

[17] "Crederity – identity and credentials service provider", http://crederity.com

Digital Object Identifier: 10.4108/ICST.COLLABORATECOM2009.8329
http://dx.doi.org/10.4108/ICST.COLLABORATECOM2009.8329