

Service Oriented Federated Identity System Framework

Min Wu, Xiaoqiang Liu, Yongsheng Ding, Jiaxun Chen

College of Information Sciences and Technology

Donghua University, Shanghai 201620, P. R. China

* Email: wm@dhu.edu.cn, liuxq@dhu.edu.cn, ysding@dhu.edu.cn, jxchen@dhu.edu.cn

Abstract:

The rapid evolution of network and distributed computing, such as Service Oriented Architecture (SOA), is increasing the challenge of securely controlling access to enterprise IT resources. As gaining access to distributed resources becomes increasingly vital, the ability to make sure that the right people have secure access to the right information at the right time becomes a critical requirement. Leading enterprises have deployed identity federation to be closer to partners, accelerate execution of business partnerships, cut cost and complexity of integrating outsourced services. This paper discusses the requirements of federated identity system. A Services Oriented Federated Identity System Framework is proposed, which emphasizes flexible identity management and dynamic discovery. Furthermore, How to use ontology to describe the semantics of identity information is discussed.

Keywords: Web Services, Federated Identity, SOA, Ontology

1. Introduction

The rapid evolution of network and distributed computing, such as Service Oriented Architecture (SOA), is increasing the challenge of securely controlling access to enterprise IT resource. Leading enterprises have deployed identity federation system to get closer with partners, accelerate execution of business partnerships, cut cost and complexity of integrating outsourced services.

Until now, most SOA deployments have relied on application or system-level authentication for establishing trusted user identity[1]. This has been achieved via mutual authentication mechanisms available in transport protocols such as HTTPS and TLS. But it limits the ability to add application or system resources in a 'computing-on-demand' environment dynamically.

The rapidly growing number of users, the constant addition of new platforms, systems, databases, and applications, and the continual change in the legal environment, have made traditional manual processes

for managing identities obsolete, and have elevated the importance of identity management in major organizations in both the public and private sectors around the world. Some standards, such as like Web Services Security (WSS)[2], Security Assertion Markup Language (SAML)[3] and Web Services Trust Language (WS-Trust)[4] enable sharing identity information across boundaries so that they provide both individuals and enterprises with new methods for dealing with decentralization, integration, and cross-domain access control and policy enforcement.

To overcome the limitations of Web Services systems causing by their distributed architecture, we explore the techniques of building federated identity management system. Federated identity solutions provide a standardized means for allowing businesses to directly provide services for trusted third-party users or users they don't directly manage. It refers to the ability to associate with one or many in a federation domain, so that the users from one enterprise domain are granted access to the services of another enterprise based on federated identities and attributes. In this paper we firstly discuss the related work of federated identity system, then propose a Services Oriented Federated Identity System Framework, which emphasizes flexible identity management and dynamic discovery.

Since the basic metadata elements defined in the federated domain are different, it is very difficult to discover identification information in another domain. To overcome this problem we propose to use ontologies to describe the semantics of identity information. Ontology is machine processable since it conforms to a formal, well-defined syntax. In this way, even when different domains use different metadata, it is possible to formally translate the concepts.

The remainder of this paper is organized as follows. The related work and research motivation are given in Section 2. The technical details of Services oriented federated identity system framework are described in Section 3. Metadata ontology of Framework is given in Section 4. Conclusions are mentioned in Section 5.

2. Related Work and Research Motivation

Federated identity is an emerging technology which has attracted attention from both industry and academia. There are a number of companies and universities participating in studying standards and providing federation solutions. Some fundamental work has been done on the digital identification. [5] examines digital pseudonyms and credentials and the concepts of identity management are described in the context of multilateral security. The proposed identity management scheme is based on the concept of the partial and full identities of a user. [6] gives a logical model on a 3 layered semantic model theory derived from RDF. But they don't go deep in research of federated identity.

In a white paper[7] published to the Microsoft Web site in May 2005, Microsoft describes the identity metasytem this way: "This metasytem, or system of systems, would leverage the strengths of its constituent identity systems, provide interoperability between them, and enable creation of a consistent and straightforward user interface to them all. The resulting improvements in cyberspace would benefit everyone, making the Internet a safer place with the potential to boost e-commerce, combat phishing, and solve other digital identity challenges." The identity metasytem will build on top of two of the WS-* protocols: the WS-Trust and WS-Metadata Exchange ones. The Liberty Alliance[8] is a consortium of approximately 170 companies that develops federated identity management specifications which include: Identity Federation Framework (ID-FF), Identity Web Services Framework (ID-WSF), Identity Services Interface Specifications (ID-SIS). The liberty standards are fairly comprehensive and ever evolving.

PRIME[9] is an European RTD Integrated Project which addresses research issues of digital identity management and privacy in the information society. The objective is to develop solutions to empower individuals to control their private sphere and manage their identities and trigger persuasive deployment of privacy-enhancing identity management solutions. White paper[10] gives public integration framework, public architecture & specifications and application-driven prototypes. Shibboleth[11] is a project of Internet2/MACE. The objective is to provide an open sharing of web resources through a secure and privacy-preserving way of exchange user property information. It

emphasizes on access control techniques and federated administration issues.

The objective of this paper is to develop security architecture of federated identity system whose goals include simplifying administration and increasing security. The benefits of our framework include following:

- Allowing each domain to maintain their own user's identity and related attributes information, eliminating proliferation of new accounts, reducing number of accounts to maintain as well as number of passwords to reset for individual users
- Leveraging investments in existent authentication by propagating identity to external domains
- Reducing identity theft threat by reducing number of accounts and passwords transmission between domains, minimizing user information exposure through credentials exchanging
- providing mechanism to handle the constraints and dependencies among the federated identity management through ontologies

3. Services Oriented Federated Identity System Framework

Federated identity provides a simple and smart mechanism to identify and validates the users from friendship or ally organization who would seamless access to Web Services in trusted union without repeat authentication. It also assures that the different identities of the same user can safely link between the participators. Members of federated domain validate their user's identity independently in their domain and exchange identity information each other. Federated identity solutions must manage the complete user lifecycle, which include user and account creation, account linking, authentication, access control, and account termination. we propose Services Oriented Federated Identity System Framework, shown in Fig. 1.

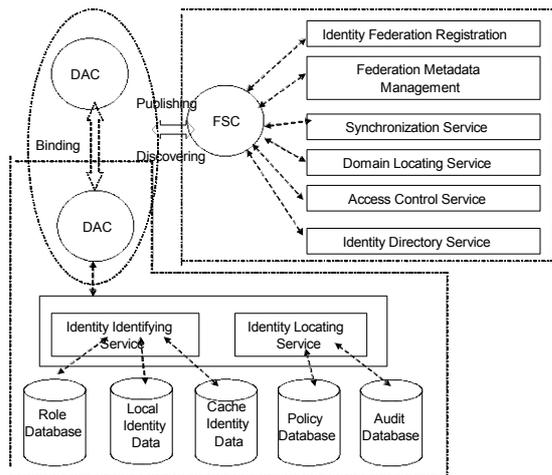


Fig.1. Service Oriented Federated Identity Management Framework

SOA is an emerging architectural style for crafting next-generation enterprise applications. While the SOA approach strongly reinforces well-established, general software architecture principles such as information hiding, modularization, and separation of concerns, it also adds additional themes such as service choreography, service repositories, and the service bus middleware pattern. Thus the Services Oriented paradigm attempts to promote flexibility and agility through loose coupling[12].

The Framework is composed of Federation Service Center (FSC) and several Domain Authentication Center (DAC). Recur to the Services Oriented theoretic, FSC 's function includes register, discovery of federation services and validation of identity and data encryption. DAC 's function includes identity management services for their own domain, such as maintaining the local user's identity data and certifications. It also includes applying federation request to FSC.

FSC involves following function modules:

- 1) Identity Federation Registration: DAC applying for joining in a federated domain and registering at the FSC, then getting a global identity symbol defined by XNS[13].
- 2) Federation Metadata Management: due to enforcing disparate identity management system, different organization having inconsistent definition of identity, utilizing ontological technology for identity data semantics transferring between FSC and DAC.
- 3) Synchronization Service: providing cache of identity data among the federation users, improving efficiency of system and reliability of services. Once some federated domain's user data changing, DAC submitting data updating event to FSC, then giving a notice to other entities to modify correlative data.
- 4) Domain Locating Service: locating and binding

DAC dynamically according to other DAC's identity request .

- 5) Access Control Service: base on Public Key Certificate(PKC, fulfilling identity authentication, data encryption and digital signature to ensuring the validity, confidentiality, integrity and non-repudiation to Web Services, establishing Attribute Certification (AC) to define role permission;

- 6) Identity Directory Service: implementing identity directory management of federation system.

Service oriented federated identity management system works as following:

- 1) DAC of domain A applies for federation registration to FSC. Then FSC publishes the Web Service information of domain A. If other domains want to obtain access to the service, it should register to FSC and get corresponding public key digital certification and attribute certification.
- 2) If a user from domain B wants to access to some Web Service of domain A, he should provide his global identity symbol and individual identity certification. The Identity Identifying Service of domain A judges whether the request user is belong to domain A or whether exists cache identity record. If the answer is negative, domain A forwards request to Identity Locating Service and asks it to resolve the owner of request user's identity.
- 3) Identity Locating Service sends request to Domain Locating Service of FSC. After Domain Locating Service discovers that request user is belong to domain B, it signs the digital signature to request of client and sends to Identity Identifying Service of domain B which gain identity information of request. Then it judges the deploying authority according to access control rule. If it permits, it returns public key digital certification and attribute certification.
- 4) Access control service of FSC estimates privilege of requester. If it permits, it sends credence defined by SAML to Identity Locating Service of Domain A and gives notice to Domain A to update user information.
- 5) Domain A sends assertion to requester of Domain B and responses to its request. After it establishes a local session, requester can deploy Web Services announced by the assertion.
- 6) Once user information of Identity Management System of Domain B Varied, Domain B submits Data Update Event to FSC. Synchronization Service of FSC gives notice to Domain A to modify the caching user information.

4. Exploring Metadata Ontology in the Framework

In the above framework, a fundamental assumption is that the involved domains share a common

expressing of identity information. But in fact each domain uses an unique mechanism for their own user identification. If the metadata is given by coding lists in one domain, it is very difficult to locate a user's identification in another federated domain by using this metadata. To alleviate this problem, we propose to use metadata ontologies rather than coding lists. Ontology is defined through a formal ontology language like DAML/OIL[14], RDFS[15] and OWL[16] so that it can be machine processable. Even if each federated domains use different ontologies, a formal translation of concepts can be facilitated through ontology mapping. It becomes possible to use rules to further enhance the semantics. Hence, Registering, locating and synchronizing identity information across federated domains are greatly facilitated.

In Fig.2, we present a part of an example ontology to define attribute hierarchy, attribute names of federated identity. In the example ontology, the range of "TypeCode" property is defined to be the "IdentityType" class. The "IdentityType" class has subclasses such as 'Demographic', 'Social' and 'Employment', etc. Demographic attributes include basic information like 'name', 'gender' and 'birthday'. Employment attributes include employment information like 'department', 'title', 'staff number', etc. Credential attributes are depended on the user's role or context of transaction. These subclasses can be further specialized by relating them to specific federated domains or local domain identity maintenance facilities. Users can show different credentials and personal information to different service providers due to varied trust. We use OWL to define these ontologies. In OWL, relationships between classes are formally defined through "objectProperties". For example, we can define a "FederationType" object property to associate "FederationDomain" class with the "IdentityType" class. Through this object property, the "Employment" IdentityType can be related with the "Access Control Service" class. When such relationships are formally defined through ontology languages, further constraints and dependencies can be enforced through rules.

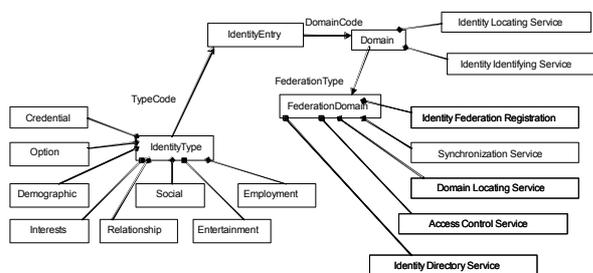


Fig.2. An example of Identity Metadata Ontology

Our objective is not to propose integrated identity ontology but rather to show how it can be specified by standard method. Furthermore, domain ontology

and task ontology are defined so that it can fulfill reasoning about the identity equivalence and trust propagation. When metadata is defined through ontologies, there is possibility to handle the constraints and dependencies among the identity management. The dependencies among them can be handled in an automated way by defining the related rules. Additionally, it also can be done to fulfill identity discovery across federated domains.

5. Conclusion and Future Work

Services Oriented Federated Identity System Framework shares common services and user interfaces, to increase efficiency, reduce implementation complexity and simplify using. It provides a simple and smart mechanism to identity and validates the users from friendship or ally organization who would seamless access to Web Services in trusted union without repeat authentication. It also assures that the different identities of the same user can safely link between the participators. Members of federated domain validate their users' identity independently in their domain and exchange identity information each other. Ontology modeling for identity assertions is vital for sharing a common concept of digital identity throughout a federated domain. It is also important for establishing relationships between identity and other related concepts like trust.

In the future we would do some work to establish trust authority infrastructure to fulfill automatic trust negotiation and to provide better user privacy protection by evaluating domain policies dynamically.

Acknowledgements

This work was supported in part by the National Nature Science Foundation of China (No. 60474037 and 60004006), and Program for New Century Excellent Talents in University (NCET-04-415).

Reference

[1] http://wp.bitpipe.com/resource/org_1138132830

877/9180_IdentityWebServ_edp.pdf?site_cd=bp

[2] <http://www.oasis-open.org/committees/wss/>

[3] <http://www.oasis-open.org/committees/security/>

[4] <http://www.ibm.com/developerworks/library/ws-trust/>

[5] S. Clauß, M. Kohntopp, "Identity management and its support of multilateral security", Computer Networks: The International Journal of Computer and Telecommunications Networking, Vol(37), pp.205-219, 2001

[6] G. Hogben, M. Wilikens, I. Vakalis, "On the ontology of Digital Identification", Proc. Of International Federated Conferences(OTM '03),Italy, 2003

[7] <http://msdn.microsoft.com/webservices/webservices/understanding/advancedwebservices/default.aspx?pull=/library/en-us/dnwebsrv/html/identitymetasystem.asp>

[8] <http://www.projectliberty.org/>

[9] <http://www.prime-project.eu.org/>

[10] http://www.prime-project.eu.org/prime/public/press_room/whitepaper/PRIME-Whitepaper-V1.pdf

[11] <http://shibboleth.internet2.edu/>

[12] <http://www-128.ibm.com/developerworks/library/ws-soad1/>

[13] <http://xml.coverpages.org/xns.html>

[14] <http://www.daml.org/>

[15] <http://www.w3.org/TR/2003/WD-rdf-schema-20030123/>

[16] <http://www.w3.org/TR/owl-semantic/>