Ensuring Information Assurance in Federated Identity Management

Dongwan Shin, Gail-Joon Ahn, and Prasad Shenoy
Laboratory of Information Integration, Security, and Privacy (LIISP)
Department of Software and Information Systems
University of North Carolina at Charlotte
Charlotte, NC 28223, USA
{doshin, gahn, pnshenoy}@uncc.edu

Abstract

Surveys and polling data confirm that the Internet is now a prime vehicle for business, community, and personal interactions. The notion of identity is the important component of this vehicle. When users interact with services on the Internet, they often tailor the services in some way for their personal use. For example, a user may establish an account with a username and password and/or set some preferences for what information the user wants displayed and how the user wants it displayed. The network identity of each user is the overall global set of these attributes constituting the various accounts. In this paper, we investigate two well-known federated identity management (FIM) solutions, Microsoft Passport and Liberty Alliance, attempting to identify information assurance (IA) requirements in FIM. In particular, we focus on principal IA requirements for Web Services (WS) which plays an integral role in enriching identity management through federation.

Keywords
Identity management, federation, web services, information assurance

1 Introduction

Identity management (IM) has been recently considered to be a viable solution for simplifying user management across enterprise applications. As enterprises have changed their business operation paradigm from brick-and-mortar to click-and-mortar, they have embraced a variety of enterprise applications for streamlining business operations: emailing systems, customer relationship management (CRM) systems, enterprise resource planning (ERP) systems, supply chain management (SCM) systems, and the like. However, a non-trivial problem has been compounded by this reinforcing line of enterprise applications, *the problem of managing user profiles*. Every new addition of those applications has proved to be subject to bringing in a new database for storing user profiles, and it was quite costly and complex for enterprises to manage all those profiles, which were often redundant. Considering business-to-business (B2B) environments, where a set of users consists of not only their employees or customers but also those of their partners', this problem became even worse. As a set of underlying technologies and processes overarching the creation, maintenance, and termination of user identities, IM has been proposed to address this issue.

Furthermore, the prevalence of business alliances or coalitions necessitates the further evolution of IM, so called federated identity management (FIM). The main motivation of FIM is to enhance user convenience and privacy as well as to decentralize user management tasks through the federation of identities among business partners. As a consequence, a cost-effective and interoperable technology is strongly required in the process of federation, and Web Services (WS) has proved to be a good candidate for such a technology as it has served to provide the standard way to enable the communication and composition of various enterprise applications over distributed and heterogeneous networks.

Since identity federation is likely to go along with the exchange of sensitive user information in a highly insecure online environment, security and privacy issues with such exchange of information are key concerns in FIM. In this paper, we describe a comparative study of FIM to investigate how to ensure information assurance (IA) for identity federation. We first discuss key benefits of FIM and how WS can play an integral role in enriching IM through federation. Then, we investigate two well-known FIM solutions, *Liberty Alliance* [13] and *Microsoft Passport* [5], attempting to identify IA requirements in FIM.

0-7803-8396-6/04/$20.00 © 2004 IEEE

The rest of this paper is organized as follows. Section 2 discusses three approaches to IM, along with the prior research related to our work. We also discuss WS components briefly. Section 3 describes FIM, particularly, Liberty and Passport in detail. Section 4 discusses the role of WS in federating identities in the two model. Section 5 describe IA requirements for FIM. Section 6 concludes this paper.

2 Background and Related Works

In this section, we start with the discussion of three approaches to IM: *isolated IM*, *centralized FIM*, and *distributed FIM*, including previous works related to IM. Thereafter, we discuss the core components of WS architectures.

2.1 Identity Management and Related Works

The isolated IM model is the most conservative of the three approaches. Each business forms its own identity management domain (IMD) and has its own way of maintaining the identities of users including employees, customers, and partners. Hence, this model is simple to implement and has a tight control over user profiles. However, it is hard to achieve user convenience with this model since different IMDs are likely to have different authentication processes or mechanisms for their users and corresponding authentication policies may vary between players.

The centralized FIM model has a single identity provider (IDP) that brokers trust to other participating members or service providers (SP) in a Circle of Trust (CoT). IDP being a sole authenticator has a centralized control over the identity management task, providing easy access to all SPs domains with simplicity of management and control. The drawback of this approach is a single point of failure within a CoT infrastructure in case that IDP fails to provide authentication service. User convenience can be also achieved partially in that the single sign-on (SSO) for users are only effective within SPs which belongs to the same CoT.

The distributed FIM model provides a frictionless IM solution by forming a federation and making authentication a distributed task. Every member agrees to trust user identities *vouched for* by other members of the federation. This helps users maintain their segregated identities, making them portable across autonomous policy domains. It also facilitates SSO and trust, thereby allowing businesses to share the identity management cost with its partners. As we will discuss later, Microsoft Passport is based on the centralized FIM model, while Liberty Alliance aims to be the distributed FIM model.

Earlier works related to user identity management were mostly focused on a user-centric approach [9], where users have control over IM functions. A simple idea of managing user identities is described in [6], where the author proposed the use of personal card computers to handle all payments of a user, thereby ensuring the privacy and security of the user's identity on the Web. Hagel and Singer [12] discussed the concept of *infomediaries* where users have to trust and rely on a third party to aggregate their information and perform IM tasks on their behalf while protecting the privacy of their information. The Novell digitalme technology [8] is such an infomediary that allows users to create various identity cards that can be shared on the Internet according to users' preferences. Users can control both what information is stored in each card and conditions under which it may be shared. Although none of the related works directly address identity federation, the ideas and discussions from these research lay the foundation for FIM.

2.2 Web Services Components

As self-contained and modular applications that have open, standard-based interfaces, WS facilitates the communication and composition of various enterprise applications by leveraging XML-based messages over Internet protocols. This loosely coupled architecture of WS provides enterprise with an ability to create low-cost solutions for proper business operations as well as interaction networks with their employees, customers, and partners.

WS architecture has four key components: consumer, SOAP [1], WSDL [2] and UDDI [4]. The consumer represents a user of WS. Universal Description Discovery and Integration (UDDI) defines operations of a service registry and is a data structure for registering and storing business information and technical specifications. The user queries UDDI to find a specific WS that he intends to use. The result of the query is a formal description of the service called Web Services Description Language (WSDL). WSDL is an interoperable and machine-understandable description of WS. It provides the functional description of services along with protocol and deployment details. WSDL also enables a dynamic, delayed binding of service components and contains information that can be consumed by the user to communicate with WS; for example, information like service endpoints for sending messages, the format of request or response messages, and message signatures. Simple Object Access Protocol (SOAP) is an XML/HTTP-based message transfer protocol for WS. SOAP is used for accessing services, objects, and servers in a platform-independent manner. SOAP can potentially be used in combination with a variety of other protocols like SMTP.

3 Federated Identity Management

In this section, we discuss FIM in general, Liberty Alliance and Microsoft Passport in particular. Federated identity gives the ability to securely recognize and leverage user identities owned by trusted organizations within or across CoTs, and identity federation allows organizations to securely share confidential user identities with trusted ones, without requiring users to re-enter their name and password when they access their network resources. Additionally, identity federation provides the ability to optionally and securely share user information such as their profiles or other data between various trusted applications, subject to user consent and organizational requirements.

Two well-known FIM solutions, Liberty Alliance and Microsoft Passport have fundamentally the same goal of managing web-based identification and authentication. Both enable organizations to build IM systems that can be federated across many disparate sources, whereby each user can have a single network identity that provides SSO to the web sites that have implemented either or both of the systems.

3.1 Liberty Alliance

Liberty Alliance is a consortium of more than 150 companies working together towards developing an open, interoperable standard for FIM. It is aimed towards realizing the notion of a cohesive, tangible network identity, which can facilitate SSO and frictionless business operations. It is a distributed FIM model, relying on the notion of IDP and SP, as we discussed earlier. IDP is responsible for carrying out identity federation. Authentication messages or authentication requests are passed between IDP and SP. IDP and SP in Liberty Alliance Model actually are WS, deployed on respective locations and open for incoming messages from other IDP and SP. We will discuss in a later section how WS works in Liberty.

3.2 Microsoft Passport

Microsoft Passport provides authentication services for Passport-enabled sites called participating sites. It was initially released as a service and not an open specification and precedes Liberty Alliance by at least a year. It is the underlying authentication system of Microsoft Hotmail and Microsoft Network, and it is integrated for use in Windows XP. A centralized Passport server is the only IDP in Passport model and contains users' authentication credentials and the associated unique global identifier called Passport Unique Identifier (PUID). Passport is an example of a centralized FIM model. Unlike Liberty Alliance, cookies play a major role in Passport architecture where Passport server stores and reads identity information in the form of session and browser cookies stored securely at a client side.

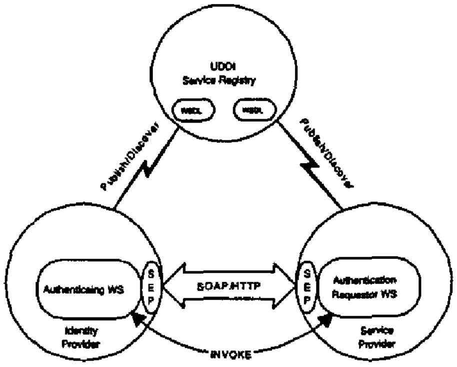

Figure 1: Role of WS in FIM

4 Role of Web Services in FIM

In this section, we start with the discussion of the role of WS in identity federation. Identity federation usually involves three actors: IDP, SP, and users. IDP in a CoT performs the task of authentication and SP relies on IDP for authentication information of a user before granting the user access to its services. Identity federation occurs with the user's consent to federate his local identity at SP with his identity at IDP which further facilitates SSO. In this process of federation, as shown in Figure 1, WS provides SOAP/HTTP-based standard communication vehicles among the providers. SP can discover IDP either statically or by querying a UDDI registry. Afterwards, SP communicates with IDP by reading its WSDL from UDDI, whereby SP can exchange authentication request/response through service endpoints (SEP) specified in WSDL.

4.1 Web Services in Liberty Alliance

In Liberty Alliance, each CoT has one or more providers using SOAP/HTTP based communication channels for exchanging authentication-related information between WS endpoints. Both SP and IDP follow agreed-upon schema for federation and SSO.

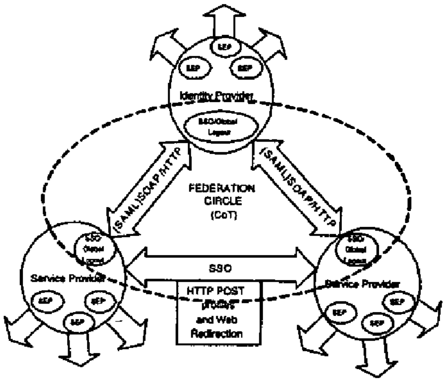

Figure 2: Liberty Alliance model

Security Assertion Markup Language (SAML) [11] is an essential component in this process for the purpose of asserting authentication status of users between the providers. A federated sign-in done at IDP would provide user with a valid session that is respected by all the SPs in its CoT. Figure 2 shows the WS-enabled FIM architecture for Liberty Alliance which hosts two WS components, SSO Login and Global Logout.

SSO Login WS endpoints facilitate federated login for SSO. Federation requires a user to opt-in by providing consent for mapping his identities at IDP and SP. As a result, both IDP and SP store a *pseudonym* as a name identifier for the user. Pseudonyms are used by IDP later when the user requests an SSO. IDP vouches for SAML-based user authentication request from SP by providing SAML-based authentication response.

Global Logout WS endpoints, also called Single Logout endpoints, receive and process logout events from SP and IDP. Typically, when a user logs out from one provider, the user's SSO session which is active at the rest of providers is invalidated by sending a message to these WS endpoints. The user agent accesses Global Logout WS at IDP and indicates that all SPs, which the IDP has provided authentication for during the current session, must be notified of the session termination. Then, the user agent receives an HTTP response from IDP that confirms the completion of a global logout.

4.2 Web Services in Microsoft Passport

Figure 3 shows the Passport architecture with WS endpoints. There are WS components that make up Passport authentication service and involve the implementation of the authentication service [5]. The primary WS component that makes up Passport authentication model is Login Service.

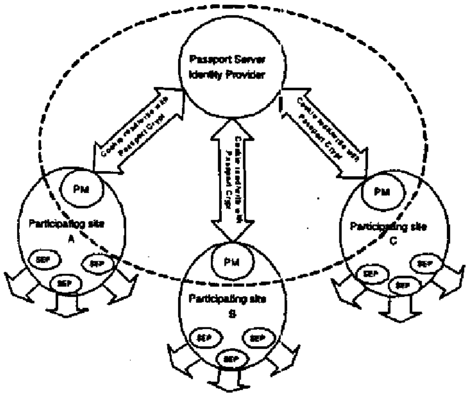

Figure 3: Passport Architecture

As implied by its name, Login WS is mainly in charge of the user authentication service. For instance, a user logging in to any Passport-enabled site is automatically authenticated by all other Passport-enabled sites, thereby enabling SSO. Subsequent sites receive the authentication status of the user from Login WS through a Component Configuration Document (CCD). CCD is an XML document used by Passport to facilitate the synchronization of the user's authentication status in participating sites.

5 Information Assurance in FIM

As an effort to identify principal IA requirements for FIM, we discuss security and privacy concerns relevant to WS in FIM in this section. We also describe how Liberty Alliance and Microsoft Passport deal with these concerns to fulfill such requirements in their architectures.

5.1 Security Concerns in FIM

Security concerns in FIM can be observed from the perspective of the general objectives of information security: availability, integrity, and confidentiality. In addition, authorization is also an important aspect to be considered in that controlled access to federated identity information is strongly required.

Ensuring Availability: The availability of information in FIM models concerns system reliability and timely delivery of information. In FIM models, the availability of information can be ensured by not only having a common protocol or mechanism for communicating authentication and other information between parties but also securing communication channels and messages.

Channel security can be achieved using protocols like TLS1.0/SSL3.0 or other protocols like IPsec with security characteristics that are equivalent to TLS or SSL. However, these protocols can only provide security at the transport level and not at the message level. Liberty specifications strongly recommend TLS/SSL with well-known cipher suites [18] for channel security. More details has been discussed in [17].

Integrity and Confidentiality: Message security is important in FIM for preventing attackers and intermediaries from tampering the messages that are in transit. Improper message security generates concerns like identity theft, false authentication, and unauthorized use of resources. Web Services Security (WSS) [14] tries to address these issues by providing security extensions such as digital signature and encryption to SOAP messages. Signing a SOAP payload using XML Digital Signature [10] ensures the integrity of the message. The sender can sign a SOAP message with his private key. The receiver can then verify the signature with the sender's public key to see if the message has been modified. In WS architecture, public key infrastructure (PKI) can be leveraged to have organizations sign security assertions instead of issuing certificates. Liberty Alliance specifications recommend XML Digital Signature and Encryption [15] for encrypting a complete SOAP message or a part of the SOAP message to maintain the integrity and confidentiality of its contents. Microsoft Passport takes an approach to encrypting cookies for securing data contained within them. Cookies store sensitive information like user profiles that can be securely accessed by authorized parties.

Authorization: FIM requires communicating parties to provide controlled access of information to legitimate users. Authorization deals with what information a user or an application has access to or which operations a user or an application can perform. Proper authorization mechanisms are necessary in WS communication especially when the communication endpoint is across multiple hops. Liberty specifications recommend a permission-based attribute sharing mechanism, which enables users to specify authorization policies on their information that they want to share. Similarly, Microsoft Passport allows users to have their choices regarding the information they want to share with participating sites.

5.2 Privacy Concerns in FIM

Privacy is a growing concern with FIM models due to the voluminous exchange of sensitive information that occur across enterprises. Securing communication channels and encrypting messages may help preserve the privacy of relevant information only up to some extent. The security concerns that we discussed in the previous section are obviously applicable to privacy as well. In WS-enabled FIM where the receiver of a message may not be its ultimate destination, improper security measures may result in unauthorized access of user's personal information which leads to violation of privacy.

Protection of user identities and personal information can be achieved by using the principle of pseudonymity. Obfuscating message payloads can also preserve their privacy by making them accessible only by authorized parties having proper credentials or keys [16]. Privacy enhancing technologies like Platform for Privacy Preference (P3P) [7] provide a solution for point-to-point privacy protection based on user preferences. However, such solutions do not scale for a more open, interoperable WS architecture.

Liberty's SAML implementation uses pseudonyms constructed using pseudo-random values that have no discernable correspondence with users' identifiers at IDP or SP. The pseudonym has a meaning only in the context of the relationship between the two communicating parties. The intent is to create a non-public pseudonym so as to contravene the linkability to users' identities or activities, thereby maintaining the privacy.

Organizations using FIM models is required to follow four key principles of fair information practices which are discussed in [3]:

- *Notice*: Users should receive prior notice of the information practices.
- *Choice*: Users have a choice to specify what information will be used and the purpose for which the information is collected.
- *Access*: Users should be able to access and modify their personal information as and when needed.
- *Security*: Users should be assured that the organizational system is capable of securing their personal information.

Liberty specifications have recently proposed an approach to sharing user attributes on the basis of user's permission. The specifications also provide a set of guidelines that will help businesses adhere to these principles. Microsoft Passport's approach to online privacy is also based on adherence to these aforementioned principles.

6 Conclusion and Future Works

Information security and privacy issues are the key concerns in FIM because identity federation requires the exchange of sensitive user information in a highly insecure and open network. In this paper, we discussed two well-known FIM solutions, Microsoft Passport and Liberty Alliance and how WS can play an integral role in FIM. Also, we identified and discussed core IA requirements in FIM focusing on WS-relevant issues.

The Liberty Alliance Phase 2 specifications are recently developed to address how to enable users to control the use and disclosure of their personal information and how to enable service provider and attribute provider negotiate acceptable usage directives regarding either the intended use of a requested attribute, or the allowed usage of a requested attribute. Our immediate work will focus on a privacy attribute management framework within Liberty Alliance which can provide users with a high level of confidence in the privacy of their personal data. Developing IA metrics for FIM is another issue that we intend to work on in the near future. It is generally believed that no single perfect set of IA metrics can be applied to all systems. Thus, we will investigate IA metrics specifically designed for FIM systems.

Acknowledgements

This work was partially supported at the Laboratory of Information of Integration, Security and Privacy at the University of North Carolina at Charlotte by the grants from e-Business Technology Institute, National Science Foundation (NSF-IIS-0242393), and Department of Energy Early Career Principal Investigator Award (DE-FG02-03ER25565).

References

[1] W3C Note: Simple object access protocol v 1.1. Technical report, http://www.w3.org/TR/SOAP/, 2000.

[2] W3C note: Web services description language (WSDL) v 1.1. Technical report, http://www.w3.org/TR/wsdl12/, 2001.

[3] Federal Trade Commission. online profiling - a report to congress, part 2. Technical report, http://www.ftc.gov/os/2000/07/onlineprofiling.htm, 2002.

[4] Universal description, discovery and integration (uddi) v 3.0. Technical report, http://uddi.org/pubs/uddi-v3.00-published-20020719.htm, 2002.

[5] Mircrosoft Corporations. microsoft .net passport review guide. Technical report, http://www.microsoft.com/net/services/passport /review_guide.asp, 2003.

[6] D. Chaum. Security without identification: Card computers to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, 1985.

[7] L. Cranor, L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle. The platform for privacy preferences 1.0 (p3p1.0) specification. Technical report, www.w3.org/TR/2002/REC-P3P-20020416/, 2002.

[8] L. F. Cranor. Agents of choice: Tools that facilitate notice and choice about web site data practices.

[9] H. Damker, U. Pordesch, and M. Reichenbach. Personal reach ability and security management - negotiation of multilateral security. In *Proceedings of Multilateral Security in Communications*, Stuttgart, Germany, 1999.

[10] D. Eastlake, J. Reagle, J. Boyer, B. Fox, and E. Simon. XML - signature syntax and processing. Technical report, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/, 2002.

[11] P. Hallam-Baker and E. Maler. Assertions and protocols for OASIS SAML. Technical report, http://www.oasis-open.org/committees/security/docs/cs-sstc-core-01.pdf, 2002.

[12] J. Hegel and M. Singer, editors. *Net Worth: Shaping Market When Customers Make the Rule*. Harvard Business School Press, 1999.

[13] J. Hodges and T. Watson. Liberty architecture overview v 1.2-03. Technical report, http://www.sourceid.org/docs/sso/liberty-architecture-overview-v1.1.pdf, 2003.

[14] IBM. Web services security (WSS) specifications 1.0.05. Technical report, http://www-106.ibm.com/developerworks/webservices/library/ws-secure/, 2002.

[15] T. Imamura, B. Dillaway, and E. Simon. XML encryption syntax and processing. Technical report, http://www.w3.org/TR/2002/CR-xmlenc-core-20020304/, 2002.

[16] M. C. Mont, S. Pearson, and P. Bramhall. Towards accountable management of identity and privacy: Sticky policies and enforceable tracing services. Technical report, http://www.hpl.hp.com/techreports/2003/HPL-2003-49.pdf, 2003.

[17] P. Shenoy, D. Shin, and G.-J. Ahn. Towards ia-aware web services for federated identity management. In *Proceedings of IASTED International Conference on Communication, Network, and Information Security*, pages 10–12, New York, USA, December 2003.

[18] T. Watson. Liberty ID-FF implementation guidlines v 1.2.02. Technical report, Liberty Alliance Project, 2003.