Digital Identity Management

Roohul Halim Syed Atif Shaharyar
Email: {rooha433, syesh740}@student.liu.se
Supervisor: Anna Vapen, {annva@ida.liu.se}
Project Report for Information Security Course
Linköpings university, Sweden

Abstract

Recent trends in implementation of Identity Management Systems (IDMS) show the emergence of a predominant, hybrid approach which implements the functionalities of both Federated Single Sign-On (FSSO) and User-Centric Identity Management (UCIM). This allows users to control authentication process while still retaining the convenient features of federated single sign on. This paper presents the conceptual differences and similarities in UCIM and FSSO for better understanding of the design approaches to user centric, federated and hybrid IDMS.

1. Introduction

The term digital identity refers to attributes and values that uniquely identify the real world entities (individual, organization, system or machine) that may act/participate in the digital world to gain access to certain resources. The crisis of managing digital identity grows with the proportional growth in usage of digital systems in businesses and government organizations, resulting a single entity forms many identity relations with different digital administrative authorities that knows particular entity in a certain ways.

Over the years many mechanisms have been developed for entities presenting credentials for authentication to gain access to the resources. The differences in approaches are based on system requirements, administrative policies, technologies and security risks however usability of the identification mechanisms remains pivotal to all these factors. Conceptually there are different levels of identity management based on design, implementation and functionalities they provide, that distinguishes roles federated and user centric systems [9].

Moreover the mechanisms of these IDMS differ on the basis of credential management procedures. These procedures depend on whether multi domain identity sharing is required and the degree required for users controlling the process. [1, 9]

1.1 Aim

The aim of this report is to present an overview of different mechanisms of identity management solutions generally used and the recent trends that leads to the forming of new mechanisms. The report also covers different identity management solutions and their taxonomy on the bases of goal, architecture, security and usability. Moreover we intend to answer the following questions:

- What are the factors on which classification of identity management system depends?
- What are the recent trends in IDMS development?
- What are the security and usability aspects of various IDMSs?

On the basis of such a study, differences and similarities between each mechanism of IDMS are presented.

1.2 Method

For data gathering and research we have used the methodology that, first we have selected some scientific and research articles published or presented in reputed conferences related to federated and user-centric identity management from different databases and then we have analyzed them. We have compared federated and user-centric identity management after analyzing it from the papers by means of differences and similarities between them. On the basis of such analysis the results are presented.

1.3 Background

Digital Identity management is the process of representing and identifying individuals in computer networks. During our research and study, we identify three identity mechanisms; federated, user-centric and hybrid. Under each category, there are various identity management systems available in the market, some of

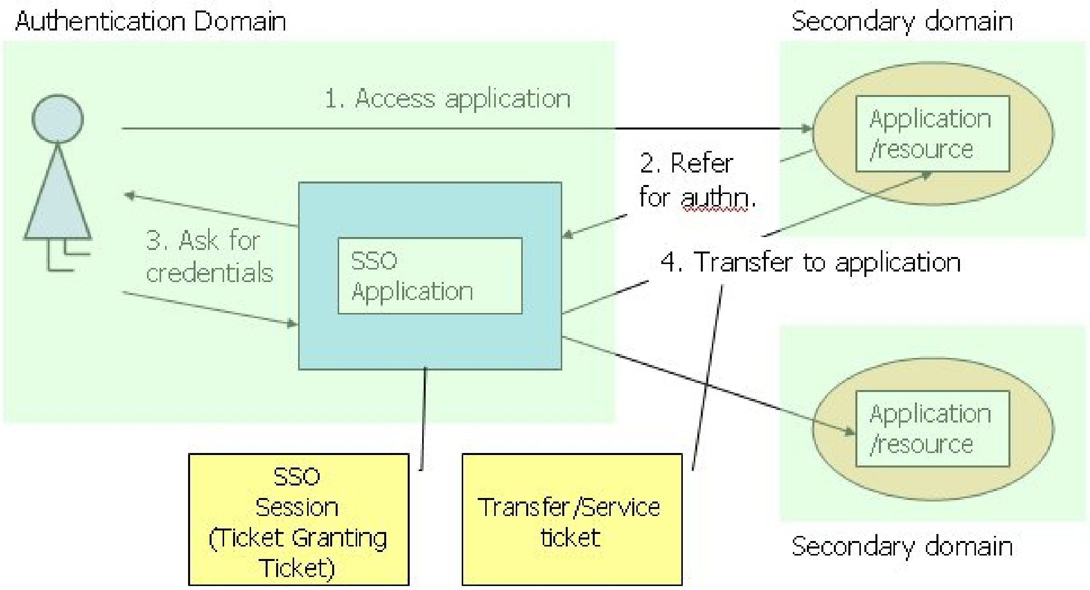

Fig 1. Simple SSO operation

them are open source and some are license based. Various established and big IT companies provide identity management systems and services to their clients.

IBM Tivoli Access Manager is a federated Single sign on solution single sign-n and sign-off across the enterprise and the capability to configure security policies to prevent unauthorized access to private corporate applications [10]. Sun OpenSSO Enterprise provides complete solution of Single Sign-On (SSO) for internal and external applications [11]. Oracle Enterprise Single Sign-On is designed to use any LDAP directory or any database server as its user record storage. It can work with biometrics or token solutions [12]. The very famous SSO open source system, which is originally developed by Yale University and it, became Jasig project in December 2004 [7], is known as CAS (Central Authentication Service). This system is very popular among the educational institutes and it provides more or less all the functionality, which any other FSSO systems provide. We can also take an example of Google, Microsoft and yahoo; it provides single sign-on to its users when accessing emails, groups, docs etc.

2. Federated Identity Management

A federation is a group of institutions and organizations that sign up to an agreed set of policies for exchanging information about users and resources to enable access and use of resources and services. The federation, combined with identity management software within institutions and organizations, can be referred to as federated access management. Federated identity systems bring together two or more separately managed identity systems to perform mutual authentication and authorization tasks and to share identity attributes and offer users cross-domain single sign-on [6].

In Federated Identity management, one party collects all information and manages it and facilitates all information between them.. A Federated Single Sign-on (FSSO) system is an IDMS that allows the use of the same user's Personal Identification Information (PII) across multiple organizations within a federation [3].

Normally users have to sign-on to multiple systems with multiple sign-on pages, each of which may involve different usernames and passwords. The goal of FIM is to permit users to access different resources such as (websites and/or applications) from one sign-on. User has to sign in only once to access all the resources and services of different partners across the enterprise. There will be only one partner for allocating and managing the identities.

Federated Identity management involves three parties; the client web browser, application which is requesting for authentication and the third is SSO server [6]. Figure 1 shows the details operation of the Federated Single Sign-on mechanism.

The hassles of administration regarding managing user accounts become simple by implementing single sign-on. The SSO server performs authentication and only the authentication server stores the password – this increases the overall security since the passwords are not passed across the network to other applications. The credentials never leave the authentication domain, it just passes a ticket to the application and the application never knows about the credentials. Secondly the affiliated or secondary domains must have to trust on the authentication domain that credentials must be asserted properly and protect it from unauthorized use.

Although implementing SSO decreases some security aspects but it increases in some other ways. For example, if a user leaves his machine without logging off, a malicious user can access the application. Though it is a general security problem but it is even worst with SSO because the malicious user can have access to all resources and application. Another security problem is that a single central authentication service is used for all the applications; it can be very attractive for the attackers who plan for a denial of service attack. With a single central authentication, if the access information has been hacked then it means that the attacker can access all the resources with one access information [6].

Federated SSO have some dependencies i.e. it relies on other infrastructure like authentication system, requires interface to the web server and identity management/registration. Most SSO systems are HTTP based and rely on cookies which is widely accepted and supported by the browsers but users who disable cookies or change browser security settings may lose SSO capability, HTTP redirection and placement of token in a query string are other dependencies of the SSO systems. HTTP is a stateless protocol, every time SSO software must check every request by the user's end, that he/she is authenticated user and have access to the resources. The session or authentication polices should be maintained on the SSO server. This means that every time the user clicks on a link or URL, there is traffic between the user browser, web application and SSO server. This traffic can become large; therefore most modern single sign on systems use LDAP (lightweight Directory Access Protocol) directories to store the authentication and authorization policies [7].

SSO Needs protocol between authentication domain and target application like Token/ticket-based and SAML POST/artefact profiles. Applications often need more than just authentication information like attributes of the user etc. X.509 certificates provide an alternative approach for the cookies but it has some draw backs – it requires installation on the user's machine and it can be confusing for users [7].

3. User Centric Identity

User centric identity is management in which user are in context rather than the organizations. A user -centric IDMS needs to support user control and consider user-centric architectural and usability aspects. [1] It enables people to choose which of their identities to use at which sites, analogously to how they choose which card to pull out of their wallet in different circumstances. In user centricity the user is involved in every identity transaction. It provides user to choose identity form different identity providers on whom they trust. It enables users to protect their privacy and easiness to adopt and use. No need to remember passwords and username for different applications, the user can use same username and password everywhere.

OpenID is an access user mechanism for user centric identity and it is also a decentralized mechanism for single sign on. Users have the option to select the provider on whom they trust and only maintain relationships with identity providers on whom they trust and rely and in this context the user has control over his attributes and he is involved in every identity provisioning transaction [1]. It solves the problem of scattering online profile across the dozens of sites.

3.1 OpenID Framework

OpenID 1.0 was originally developed in 2005 by Brad Fitzpatrick, Chief Architect of Six Apart, Ltd.. It is now deployed by a wide range of websites, particularly those heavy in user-generated content [1].

OpenID 1.0 provides HTTP-based URL authentication protocol. However with the new upgraded protocol, OpenID authentication 2.0 is becoming the community driven platform, such that it provides better flexibility and encourage innovation. OpenID 2.0 introduced new technology called XRI (Extensible Resource Identifiers) instead of URL based authentication technique. XRI has better security and support for both public and private identifiers. OpenID 2.0 still provides support for both URL and XRIs as user identifiers. With continuing growth and development the OpenID framework is considered as feasible solution for UCIM. [4]

3.2 OpenID mechanism

OpenID shares the authentication session from one web site in essence. The mechanism works as the user **A** log into to OpenID provider (e.g. www.OpenIDpro.com) after registration, receives the OpenID URL to create session. Now if user **A** wants to get registered on some other web site (e.g. www.abc.com) on the internet which provide support for OpenID then instead of supplying user name and password, user only give its OpenID URL and (www.abc.com communicate with www.OpenIDpro.com to check if user **A** has the authentication session or not). If yes then login and create new session for itself and if not then redirect to www.OpenIDpro.com.

3.2.1 YADIS, URL, XRL and OpenID

Yadis is a service discovery system, which allows relying parties authenticate the user only by providing the identity URL. It supports services such as Single sign-on across web sites, which is used in the implementation of OpenID_A Yadis ID can either be a traditional URL or a newer XRI (Extensible Resource Identifiers) i-name, where the i-name must resolve to a URL. A Yadis ID can either be a URL or XRI i-name, where the iname must resolve to a URL. The Yadis URL either equals to the Yadis ID (if this is a URL) or it can be a resolved URL of the XRI i-name [5]. It is important to understand the need of XRI, beside the well mature URL based technology. Generally there are two important reasons for using XRI. First the domain-name based URL can be expired or changed and the credentials for representing the entity can no more resolvable at the site it belongs. Secondly XRI uses HTTPS as default configuration therefore while using XRI it is not required to further configure the HTTPS protocol for securing the procedures of OpenID [5].

4. Differences and Similarities

Although the concept of federated and user centric identity management have different from each other, in terms of controlling the identities. But they have some similarities and differences from which they can be identified. We would like to compare the two systems because if the implementation approaches are the same than we can identify their relatives advantages and disadvantages.

4.1 Similarities

FID and UCIM both allow a user to authenticate with a single identity across different sites, although in UCIM users have full empowerment to choose his/her identity provider. Web-based distributed authentication and authorization services, such as controlled access to protected content resources are supported by both FSSO and UCIM. There are some issues which are related to FID an UCIM i.e. redirection from destination site to service provider and after authentication from the identity provider, redirect back to the destination site. Sessions are maintained on both destination and identity provider, but on every operation the destination site confirmed it from the service provider that the user is logged in or not, and it lead to large traffic between the destination site, browser and service provider [5, 6].

4.2 Differences

Federated Identity management has only one service provider for authentication but in UCIM there can be anonymous and randomized service providers, i.e. the user has full right to choose his/her identity provider. Moreover, FIM have a centralized database for user credentials. UCIM uses a decentralized approach because it uses more than one identity provider. Federated identity allows a user to authenticate at a single site and there is no need to provide additional information to other sites, while at the other hand in UCID, additional information is required on the first logon. By definition Federated identity management involves three main entities, namely user, identity provider (IdP) and service provider. The IdP manages and potentially issues user credentials, and the service providers (also known as relying parties) are entities that provide services to users based on their attributes whereas a user centric IDMS needs to support user control and consider user-centric architectural and usability aspects [1].

5. Windows CardSpace

The recent trends are leading towards the design of a new approach to IDMS where users are allowed to control the authentication process while still retaining the convenient features of federated single sign on, Microsoft provides an IDMS called Windows Cardspace. It is based on a new Microsoft .Net component designed to give users a consistent digital-identity experience using a specialized user agent. Microsoft addresses the problems of identifying authentic sites to the users with reliability and is also overcoming the problem related to usernames and passwords.

Users face many problems in identification on the sites they use. Username/password authentication is common and easier but its security laps are well known. Password reuse, insecure passwords, forgotten passwords, and poor password management practices provides greater opportunities for attackers furthermore password theft attacks enabled by counterfeit web sites and man in the middle attacks, requires a new solution [8,9]. Windows CardSpace can be consider as such a solution.

Windows CardSpace is suited to maintain a set of personal digital identifiers and that is performed through "information cards". These cards are much easier to use than the username and passwords, moreover this solution is more secure than passwords. In addition to this, Information cards are managed on client computers by a software component called an identity selector. An identity selector is a user interface (UI) that appears when a user attempts to authenticate to a Web site that requests an information card.

Microsoft’s CardSpace [8, 9] utilizes client side software to achieve user control and an identity credential is provided by online identity providers selected by a user, therefore in this ways user enjoys both the features of UCIM and FSSO.

6. Conclusion

The IDMS provides users the ways to manage their identities through their unique attributes and values, there are differences in approaches to IDMSs. An IDMS can be classified as federated, user centric and as a hybrid system. The FSSO provides a way to bring together more than one separately managed identity system, to perform authentication across multiple domains with a single sign-on. In Federated Identity management, one party becomes identity provider and collects all credentials and manages all the information between other parties. A Federated Single Sign-on (FSSO) system is an identity management system (IMS) that allows the use of the same user's Personal Identification Information (PII) across multiple organizations within a federation

On the other hand user centric identity management systems consider users perspectives in managing identities in which users are allowed to control authentication process, their privacy preferences, choosing their user names and passwords for accessing different resources and decide which service provider to use. OpenId is the example of such kind of system.

The recent trends are leading to words the design of new approach to IDMS where users are allowed to control authentication process while still retaining the convenient features of federated single sign on, Windows CardSpace is the example of such system.

References

[1] Abhilasha Bhargav-Spantzel, Jan Camenisch, Thomas Gross, Dieter Sommer, User centricity: A taxonomy and open issues Source**,** Volume 15, Issue 5 (October 2007), ACM - DIM 2006, Pages 493-527

[2] McKnight, D. and Chervany, N.: *The Meanings of Trust*. Technical Report MISRC 96-04, Management Information Systems Research Center, University of Minnesota, 96.

[3] A User-centric Federated Single Sign-on System Suriadi Suriadi, Ernest Foo, Audun Jøsang : Information Security Institute - Queensland University of Technology, Brisbane, Australia

[4] David Recordon VeriSign Inc, Mountain View CA, Drummond Reed Cordance Corporation, Sammamish WA, OpenID 2.0: a platform for user-centric identity management,proceedings of the second ACM workshop on Digital identity management

[5] The Identity and Accountability Foundation for Web 2.0, http://www.yadis.org/

[6] Maler, E.; Reed, D.; The Venn of Identity: Options and Issues in Federated Identity Management, Volume 6, Issue 2, March-April 2008 - IEEE Pages 16 – 23

[7] Jasig Community, www.ja-sig.org: date viewed : 27 April 2009

[8] Windows CardSpace, www.msdn.microsoft.com/en-us/windows/aa663320.aspx: date viewed : 20 April 2009

[9] Bramhall, P. Hansen, M. Rannenberg, K. Roessler, T. Hewlett- Packard Labs., Palo Alto; User-Centric Identity Management: New Trends in Standardization and Regulation, Volume: 5, Issue: 4, IEEE; page(s): 84-87

[10] IBM - Tivoli Access Manager for Enterprise, www-01.ibm.com/software/tivoli/products/access-mgr-esso/: date viewed : 7th May 2009

[11] Sun OpenSSO Enterprise, www.sun.com/software/products/opensso_enterprise/index.xml: date viewed : 7th May 2009

[12] Oracle Enterprise Single Sign-On, www.oracle.com/technology/products/id_mgmt/esso/index.html: date viewed : 7th May 2009