Online Identity Management And SAML

[1]V.G. Anisha Gnana Vincy, [2]J. Sunil
[1]Assistant Professor, [2]Assistant Professor
Department of Computer Science and Engineering,
V V College of Engineering, Tisaiyanvilai.

Abstract - Identity and access management systems provide lots of tools and technologies for managing user access rights to critical information inside an organization. Identity management defines the roles and access rights for online users for accessing network resources. The main objective of Identity Management systems is to provide single identity for individual user. Once the online digital identity has been created, it must be preserved, modified and supervised throughout the access life cycle. In the digital Information world, an identity management system becomes a base to build up a secure network, because managing online user identity is a necessary criteria in the Digital world. Consequently, well-managed user identities provide better control of user access, which reduces internal and external security risks. Authorization messages between sender and receiver are often sent using Security Assertion Mark-up Language (SAML), which is the open standard , an XML framework that provides authentication and authorization services. This chapter covers an overview of the Identity Management Systems and the implementation of SAML open standard for communicating authentication and authorization details across different service providers.

Keywords - digital identity, identity management, SAML, Identity Provider, Service Provider.

1. INTRODUCTION

In a ubiquitous computing world, it is more important to authenticate the remote user to escape from different online threats and attacks. Identity of an online user has become a major concern on the Internet [1]. When it is stolen by the attackers, it makes a big fraud in Internet-based services which create a lack of security in online business providers and disappointment for users. Online Identity Management becomes an essential solution [2] to the security of any online business. Identity management is the process of identifying, authenticating and authorizing a single user or groups of user by defining access rights and restrictions to those users in accessing different applications, systems or network resources with valid identities. A digital identity is a representation of an entity in a specific circumstance which describes the entity attributes: Name, Citizenship, Birthday; Area of interest, Hobbies, Food, Clothes, etc., A digital identity was realized as a detailed identity card. A digital identity is defined as "the identifying property "of a single-person. An identity consists of traits, attributes, and preferences of an individual upon which the personalized online or mobile-based services are obtained. The virtual world along with ubiquitous computing has changed the physical devices to entirely new set of requirements as the associated security issues such phishing, spam, and identity theft has emerged. In the Internet world, it is difficult to determine the identity of third-party. Digital identity management is a key factor that will guarantee not only the online service and utility outlooks but also security and privacy of services.

2.BASICS OF ONLINE IDENTITY MANAGEMENT

Identity management is the activity by which online user identities are characterized and managed in an enterprise environment. Generally, the roles of identity management includes the following:

- Identities for online users are provisioned and organized.
- Automate application provisioning.
- Manages User roles, access rights, and certification details are managed.
- Administrators distribute online applications easily in a secure manner.
- Providing single sign-on access to Users.

The users of an identity management system can include personnels outside of the organization such as clients, trading partners, or Internet-based services, as well as users within an organization. In addition to this , an identity management system has the capbility to manage network elements such as devices, processes, and applications.

Advantages of identity management system:

- Reduces management costs through with centralized account management and task automation.
- Speed up the application deployment process by allowing new applications to make use of the existing structure .
- Reduces the time to grant new user access to the online applications
- Improves security and serviceability through centralized control of user passwords and security credentials.

3. IDENTITY MANAGEMENT ARCHITECTURE

The basic elements of Identity Management System[3] includes the following:

- User who access the online service.
- Identity Provider (IdP) is the trusted provider who provides the user with some identities like single sign-on (SSO) to access other services from different websites .A well-known example for Identity provider is Google which

provides SSO to the users by which users can then access other services directly from Google.In addition to this,IdP provides identity details to a service provider for accessing cloud, mobile and VPN systems services.

- Service Provider (SP) is a website that hosts applications/services for users and also, performs identity verification.
- Identity (Id) of user.
- Personal Authentication Device (PDA) which holds different identifiers and credentials of the user to prove his/her identity..

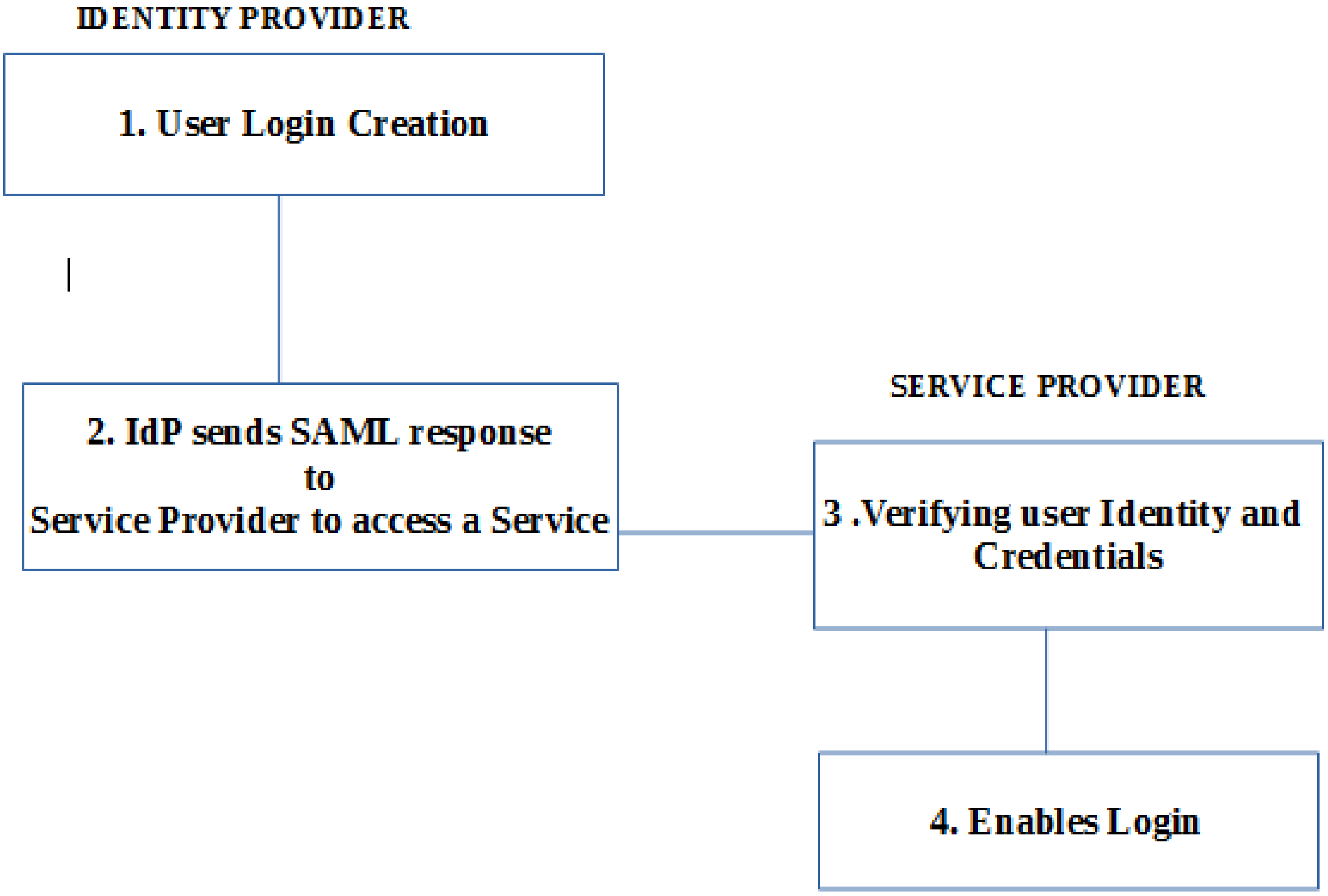
IDENTITY PROVIDER
1. User Login Creation
2. IdP sends SAML response to Service Provider to access a Service
SERVICE PROVIDER
3 .Verifying user Identity and Credentials
4. Enables Login

Figure 1: General Scenario When An Identity Provider Logs In To A Service Provider.

Identity management is closely related to authenticating entities as digital identities in the field of computer networks[4]. Authentication is defined as the process of verifying credentials about specific identities. Authentication failure will affect the validity of the whole system. Strong authenctication is enforced using password, PIN,one-time-password, voice, face, fingerprint(Biometrics).Digital identity is build around three connected factors namely usefullness, cost and risk[5].

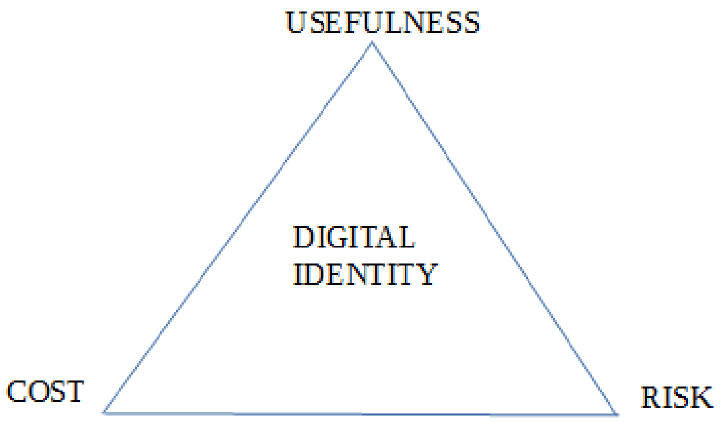

Figure 2 :Factors that affect Digital Identity

4. SAML PROTOCOL

SAML stands for Security Assertion Markup , is a open standard , XML-based framework[7]. SAML helps to transfer user authentication for and authorization details between two parties in the network. Most probably, SAML is used between an Identity Provider which represents some online enterprises and a Service Provider. SAML act as a standard which is used by different enterprises, government agencies and different service for collaborating identities through the internet. SSO(Single-Sign On) is the well-known use case of SAML.

4.1. Benefits of SAML

SAML- Security Assertion Markup Language is an XML-based context which is used by the online identity management for authorization and authentication of user credentials and access rights. It delivers many welfares to online enterprises as well as governments. On the other hand, SAML has been commonly accepted for the following three reasons:

1. Consistent

The consistent format of SAML helps to inter operate with any kind of system independent of execution.

2. Security

In the recent computing, security of enterprise applications is most important criteria .In order to enforce security, SAML is used to deliver a single point of authentication at identity provider side which indicates that user credentials not ever leave the firewall limit, and then SAML declares the identity to others. SAML strengthens the security through Public Key Infrastructure (PKI) to protect the declared identities against attempted attacks.

3. User Experience

SAML provides the capability for online users to securely access various applications using a single set of credentials entered once. This provides the foundation for federation as well as single sign-on (SSO). This allows online user to run their business faster and more proficiently.

4.2. SAML provider

In SAML , a provider is an entity which represents a server or any other computer that provides some sort of services for the online users. Therefore, the networked computer which provide or consume SAML services are known as service providers. One of the most essential kind of service provider which provides different services is termed as an identity provider. An identity provider provides user authentication. It also determine the different services the user is approved to access across different entities in the system.

4.3. SAML assertion

A SAML assertion is the XML document which transmit all the information from one system to another system in a network. Once an identity provider authorized the user, it sends a SAML assertion document to the server computer which provides those services to the user. To enforce security, a SAML assertion document can be encrypted.

4.4. Basic SAML Authentication process

Implementation of SAML includes a Service Provider (SP) ,online user and an Identity Provider (IdP). A SAML Authentication process is described as follows:

1. User sends the resource request to the Service Provider.
2. The Service Provider(SP) generates the SAML Authentication request which determines the suitable identity provider .
3. SP redirects the authentication request to that Identity provider ; Here, the single sign-on service is an Identity Provider(IdP).
4. User authenticates itself to the Identity Provider upon Receiving the SAML authentication Request.
5. The IdP (SSO service) parses the request and authenticates the user.
6. IdP generates SAML Response.
7. IdP return the SAML Response to the User.
8.User deliver the SAML Response to the Service Provider.
9.Service Provider grant resource access to user upon receiving the SAML Response.

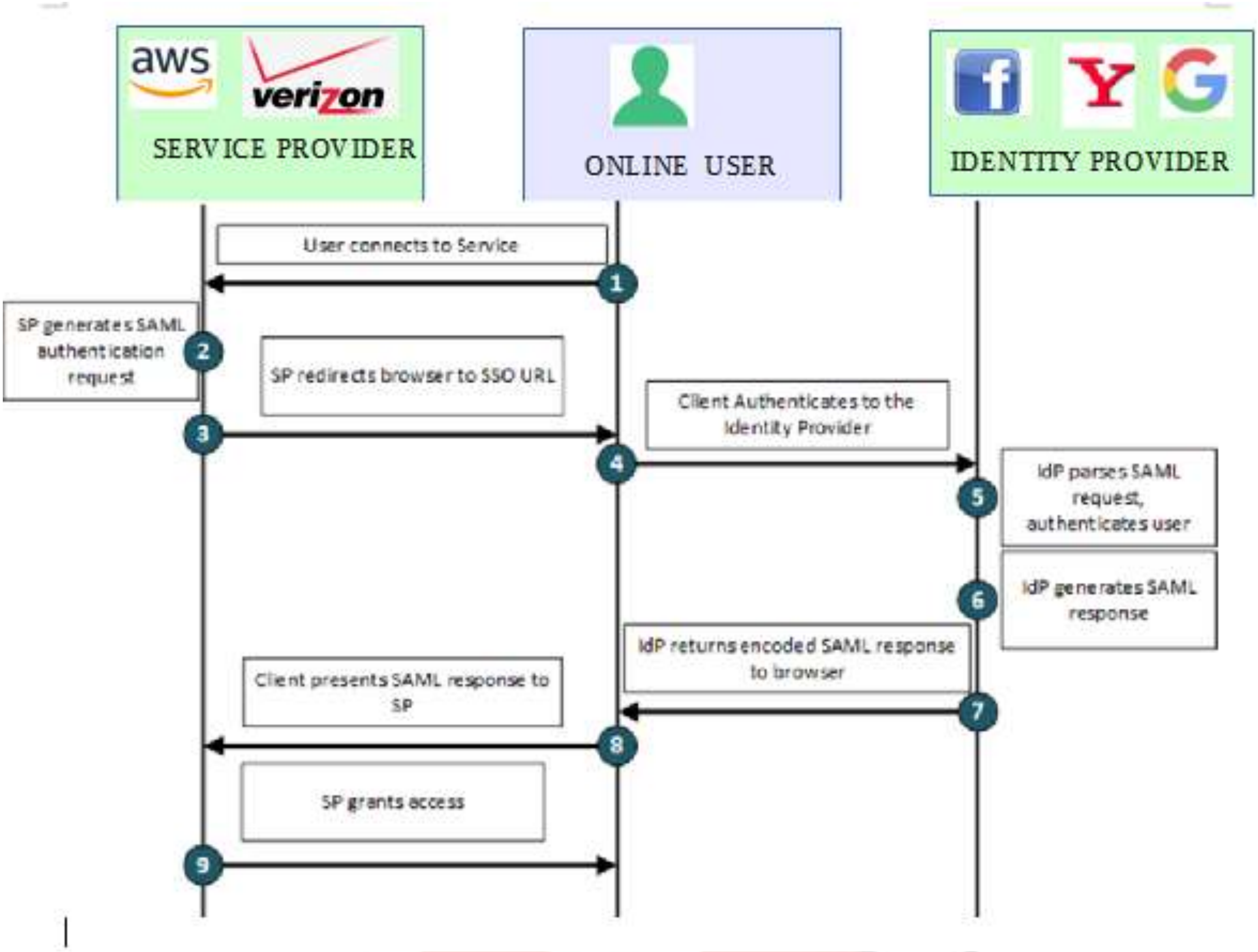
aws
verizon
SERVICE PROVIDER
ONLINE USER
IDENTITY PROVIDER
User connects to Service
1
SP generates SAML authentication request
2
SP redirects browser to SSO URL
3
Client Authenticates to the Identity Provider
4
IdP parses SAML request, authenticates user
5
IdP generates SAML response
6
IdP returns encoded SAML response to browser
7
Client presents SAML response to SP
8
SP grants access
9

Figure 3. A SAML authentication process

5. GUIDELINES TO CLEAN UP THE ONLINE IDENTITY

In order to maintain good standard for any organization ,it needs a virtuous online identity. The digital foot mark will demonstrate individuals everything about the particular enterprise when they perform online search .Online reputation of Individuals are easily predictable from profile information, to the images for comment. Individuals can maintain a good reputation by cleaning up some sort of online Identity. Some guideline for maintaining good reputation are given as follows:

- Search yourself in different search engines and remove the unwanted post or images .
- Delete Social Media Accounts which is no longer in use .
- Individuals personal blog indicates their personality. It is better to remove posts with inappropriate language which can damage your online image.
- Careful posting of messages ,images and any kinds of post is very important in Social Sites. Do not post anything which might cause business client to form a negative opinion.

6. CONCLUSION

Online Identity management is a collection of procedures and applications to manage and guaranteed access to the online digital information and resources of an organisation. This chapter provided a basics of Identity Management along with the important protocol SAML which is used for authentication and authorization process. Both online business enterprises and governments are strengthening online user's identity protection as the identity theft increases. In addition to the modern security technologies, online users and enterprises need to pay ambient care to the most suitable security measures for implementing identity management systems which make use of password-based authentication and Single sign-on (SSO) methodologies.

REFERENCES

[1] Samlinson, E.; Usha, M., "User-centric trust based identity as a service for federated cloud environment," in Computing, Communications and Networking Technologies (ICCCNT),2013 Fourth International Conference on , vol., no., pp.1-5, 4-6 July 2013.

[2] Tim Mather, Subra Kumaraswamy, and Shahed Latif, 2009, Cloud Security and Privacy. An Enterprise Perspective on Risks and Compliance,O'Reilly Media, 336.

[3] CSA SecaaS Implementation guide : Identity and Access Management September 2012.

[4] Yan Yang; Xingyuan Chen; Guangxia Wang; Lifeng Cao, "An Identity and Access Management Architecture in Cloud," in Computational Intelligence and Design (ISCID), 2014 Seventh International Symposium on, vol.2, no., pp.200-203, 13-14 Dec. 2014.
[5] https://en.wikipedia.org/wiki/Identity_management .
[6] https://www.infosecurity-magazine.com/identity-access-management/
[7]http://www.oracle.com/technetwork/middleware/webcenter/portal/learnmore/wcp-saml2- federatedsso-wp-2857359.pdf