A Review on Various Identity Management Systems

Gaurav Sharma, Shefali Pruthi

Abstract– In this era there is a significant growth in identity management solution because of their potential importance as what and how properly they handle the sensitive data. The paper present the review on digital identities which is to be handled by various Identity Management System (IDMs). The paper first provide the definition of Digital Identities and their management. Then these digital identities are embedded in a particular model which is called conceptual model of identity management. Then there is a brief review on various Identity Management system and their advantages and disadvantages as proposed by different authors but our focus is on emerging technology i.e. Microsoft Cardspace and the solution for improving its security vulnerabilities.

Keywords--Digital Identities, Identity Management System, Microsoft Cardspace, Sensitive Data.

I. INTRODUCTION

Digital identities play a vital role as many people use these identities to log on to various Web Sites for on line shopping, internet banking, searching. To log on to websites, users have to provide its personal information and remember username/password for every site. So author propose various identity management systems where user's personal information is secured and he does not have to remember username/ password as the whole system works on claims and tokens. The basic model called conceptual model is developed for IDMs which consist of relying party, Identity provider and users and they have their own rules of authentication and their goal is to protect user's personal information. And also there is a concept of single sign on by which in a single session we can log on to multiple sites, but some IDMs followed this concept and some did not. Various IDMs are deployed one of which is open ID which is very much prone to phishing attach as the whole system is using URL routing. After that PRIME came for which deployment of that system was a main concern. After that Microsoft developed Microsoft Cardspace which does not support single sign on but it is not prone to phishing attack. Further is has its limitations which are discussed with their solution in section 6 and 7

II. DIGITAL IDENTITIES AND IDENTITY MANAGEMENT

An identity is a representation of an entity where are an entity has its unique existence and can be uniquely identified in this world. Alternatively an identity is the set of attributes which makes an entity unique and different from all others entities. A representation of identity in a digital system is called a digital identity. An identity management includes management of Identity lifecycle, its authentication and identity information so that users can properly authorize to the system he wants. Identity management is essential part of many security services since it provides assurance of user's legitimacy. As a result identity management is an integral part of any access management system. But with identities great deal of privacy is required as it requires storing, processing and transformation.

III. CONCEPTUAL MODEL OF IDENTITY MANAGEMENT SYSTEM

As of growing use of web application there should be usage of web based IDMs. Web based IDMs aims to address the growing range of security threats and hence simplify the task of identity management for the user and service provider. There are three parties involved namely- A. Service Provider- It is the resource provider, user requests the resource from this and user has to fulfill the relying party's accessing criteria by providing claims. It is also called relying party (RP). B. Identity Provider (IDP)- It helps in validating the credentials, which the user provide to it before accessing RP . If the user is genuine then IDP provides a token to user which helps in accessing the resource from resource provider. C. User- The user accesses the resources from resource provider by first requesting from RP. Identity management framework can be classified into three main classes which depends on the relationship of IDP/IDP and IDP/SP [1].

1. Isolated Framework: In this the service provider trusts only itself and also become an IDP and hence there is no cooperation between parties to support user's authentication.
2. Centralized Framework: In this framework only one IDP is present and that provides identity services to all others SPs within a closed system.
3. Distributed Framework: In this framework there are many IDPs and SPs which trust each other within that group.

IV. SINGLE SIGN ON

With this feature user log in once and gains access to all other interconnected systems without being promoted to log in again at each of them. In case of current framework the user can log on to multiple SPs during a single session after getting authority from single IDP. With the concept of Single Sign On (SSO) the concept arises of single sign off where a user is automatically signed off from the RPs at which he was logged in. The main feature and benefit of SSO is transparency to the users since the main reason for deploying SSO system is users convenience but there is one security concern that is many SSO system, if an attackers breaks the authentication process with the authentication authority (example by cracking the user's password) then he/she can readily access all the participating SPs [2].

Manuscript received on July, 2012.
Asstt. Prof. Gaurav Sharma, CSE, JMIT, Radaur, India,
Scholar Shefali Pruthi, CSE, JMIT, Radaur, India.

V. IDENTITY MANAGEMENT SYSTEMS

IDMs has the particular framework and these system helps authorized sources to perform identity management task. There are various identity management systems which are discussed below:

A. OpenID

In this one users name and password is required to log in to many web sites. OpenID is a user centric shared identity service [3]. It allows users to log on to different web sites using a SSO concept. In openID user login to openID server to get the openID and uses that token to authenticate many web applications. The openID framework is a decentralized system as no central authority manages/ authenticate different identity provider and service providers. So the users can choose any of the IDP and get the token. For security and non trackable records the users can also switch between various IDPs. The advantage of openID system is that it is convenient to use and information of user is not provided to service provider in any way. But the disadvantage is that the whole framework hinges on the URL routing to correct open ID provider, if open ID provider is attacked by attacker, and when users authenticate to open ID server and provide credentials then all the credentials can be used by evils scooper and can harmed the users. Thus this framework is acceptable to phishing attacks.

B. PRIME

The PRIME (Privacy and Identity Management for Europe) goals are managing identity, privacy and trust management helping users to protect the data effectively. It embeds Europeans privacy laws and regulate into technology. Its designing evolved to have maximum privacy by providing anonymous and secure communication and there is no transaction linking by default. PRIME had explicit set of rules and these rules are assigned to the roles properly. Finally in this user need the set of tools to support IDM, and this require installation and configuration on the console. The user manages her personal data using the console, discloses personal data and checks the proper handling of her data by the various services she requires [4]. The client application mirrors the server application used by the service provider [5]. The major disadvantage of PRIME technology is that the product is not standardized and it is only possible unless it is interoperable with existing systems. Also it has its middleware which should be implemented on senders and receivers side console, which is an extra overhead.

C. Windows Cardspace

It is a product of Microsoft and is a name given to Microsoft WinFX set of software components. It is a metasystem because it is not replacing previous identity management systems but it is additional layer added to the authentication system. This identity metasystem design to comply with the 7 laws of identity, designed by Kim Cameron of Microsoft [6]. Also cardspace is built upon WS-Federation protocols which consist of WS-Security , WS- Trust, WS-Security Policy. In cardspace every digital identity transmitted on the network contains some kind of security token. The security token can contain a sensitive information or non sensitive information which forms a set of claims. It can be user's first name, last name, address, password, e-mail, or sensitive information like SSN, credit card number. User typically has many infocards saved according to the need of environment a user can select an appropriate infocard, so that it will be fair use of digital identities. Similarly in the Cardspace Framework there are three parties involved i.e. Relying Party , Identity Provider and user as discussed in conceptual model of Identity Management Systems. In cardspace framework relying party send his token policy after user request the resource. Then user login to IDP to authenticate the claims he provided which were demanded by RP. After the claims are verified by IDP the IDP sends the token to user. When user gets the token he sends the token to RP and if RP validates the tokens then user is provided access to the resources he wants.

VI. DISADVANTAGES AND SECURITY VULNERABILITY OF CARDSPACE

1. User's judgement of RP trustworthiness i.e. judging the honesty of the RP is a tedious task. Since in cardspace framework the user has to send its sensitive data in forms of tokens which are actually the claims the RP demanded. If the RP is not trustworthy then he can forge the information and can use it in a unauthorized manner. Microsoft recommends that user should only rely on high assurance certificate like X.509.
2. Reliance on single layer of authentication i.e. in the cardspace framework where there are multiple RP and single IDP then security of that system rely on single layer of authentication. In the majority of cases a simple username and password is used, if the password is cracked the security of entire system is compromised [4].
3. Cardspace can only work with Microsoft windows operating system.[7]
4. In a single working session the user can select only one infocard to present to the RP, sometimes RP demands claims which are totally different from each other and all the claims are not provided by single IDP so it is unable to cover by one infocard.
5. The whole framework lies on DNS server, if the DNS server is hacked then there is potential loss to user.

VII. IMPROVING THE SECURITY OF CARDSPACE

A. Based on SIT Attributes

As proposed by [8] the solution is based on the concept of Secured from Identity Theft (SIT) attributes [9] which is based on Schnorr's Zero Knowledge Protocol [10]-[11]. The concept says that without disclosing the actual values only values deduced from claims or we can say that the broader set of values should be presented and by which actual values are not displayed.

B. Selective Disclosure, Anonymous Credentials and Zero Knowledge Proof

In selective Disclosure certified and minimized data is revealed and this is done by using predicates (=, <=,>=,<>) on the attributes. An anonymous credential scheme allows a user to derive from a single master secret multiple cryptographic pseudonyms [4]. A zero knowledge proof is a protocol where one party i.e. the prover, proves that he knows the solution of problem to the other party i.e. the verifier without revealing the actual details of a solution. A zero knowledge proof must satisfy 3 properties namely completeness, soundness and zero knowledge.

VIII. CONCLUSION AND FUTURE WORK

In this paper we reviewed digital identities, its model and various identity management systems. Various IDMS like openID and PRIME are not widely used because of their various disadvantages. So currently emphasis is given on Microsoft cardspace to deploy it globally. It has two major security limitations and for which various measures to rectify are provided like ZKP, selective disclosure. When ZKP will be integrated within SAML token then user's privacy is protected in case of hijacked passwords or vicious SP [4].

REFERENCES

1. Gail-Joon Ahn, Moonam Ko, and Mohamed Shehab. Portable user-centric identity management. In Proceedings of the IFIP TC-11 23rd International Information Security Conference, IFIP 20th World Computer Congress, IFIP SEC 2008, Milano, Italy, pages 573{587. Springer-Verlag, 2008.]
2. Dieter Gollmann. Computer Security. John Wiley and Sons, 2004
3. Identity Management Forum , The Open Group, "White Paper: Identity Management, "Mar2004, http://www.opengroup.org/idm/
4. Bharat Bhargava1, Noopur Singh2, Asher Sinclair3 " Privacy in Cloud Computing Through Identity Management" proceeded at International Conference on Advances in Computing and Communication (ICACC April 2011)
5. (2010) PRIME Framework V3, https://www.primeproject.eu
6. K. Cameron, M.B. Jones. Design Rationale behind the Identity Metasystem Architecture, http://research.microsoft.com
7. Privacy And Practicality of Identity Management Systems ,Waleed A. Alrodhan, Technical Report 17 Mar 2010, pges-96
8. Addressing privacy issues in CardSpace Waleed A. Alrodhan and Chris J. Mitchell Royal Holloway, University of London, Third International Symposium on Information Assurance and Security. Pages 285-291.
9. A. Bhargav-Spantzel, A. C. Squicciarini, and E. Bertino. Establishing and protecting digital identity in federation systems. In Proceedings of the 2005 ACM Workshop on Digital Identity Management, Fairfax, Virginia, USA, pages 11–19. ACM, November 2005.
10. U. Fiege, A . Fiat and A. Shamir . Zero Knowledge Proofs of identity. In STOC: Proceedings of the nineteenth annual ACM conference on Theory of Computing , New York, NY, USA, pages 210-217.ACM, 1987
11. C. P. Schnorr. Efficient identification and signatures for smart cards. In G. Brassard, editor, Advances in Cryptology– CRYPTO 89: Proceedings of the ninth Annual International Cryptology Conference, Santa Barbara, California, USA, volume 435 of Lecture Notes in Computer Science, pages 239–252. Springer, 1990

AUTHORS PROFILE

Asstt. Prof. Gaurav Sharma, received his B. Sc.and M. Sc.degrees in computer science from Kurukshetra University, Kurukshetra in 1999 and 2001, respectively. Also, he holds the degree of M.Tech in Computer Science from Guru Jambeshwar University, Hisar. He is currently a Ph. D.candidate in Department of Computer Science, Punjabi University, Patiala. Also, he is working as Assistant Professor in Engineering college, JMIT Radaur. His research interests include grid computing, Software engineering, and artificial intelligence and published more than 15 research papers in various journals and international conferences.

Scholar Shefali Pruthi, received her B. Tech in computer science from Kurukshetra University, Kurukshetra in 2010. Currently she is pursuing her M. Tech from Kurukshetra University, Kurukshetra. Her research interests include cloud computing and identity management. She is novice in this field and this is her first paper.