Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 12, December 2013, pg.40 – 44

SURVEY ARTICLE

A Survey on Single Sign-On Mechanism for Multiple Service Authentications

Arul Princy.A[1], Vairachilai.S[2]

PG Student[1], Assistant Professor[2], Department of CSE

NPR college of Engineering and Technology, TamilNadu, India

Email: sheelaprincy4@gmail.com [1]; vairachilai2676@gmail.com [2]

Abstract-Single sign-on(SSO) is a mechanism that uses a single action of authentication to permit an authorized user to access all related, but independent software systems or applications without being prompted to log in again at each of them during a particular session. Recently, some user identification schemes have been proposed for distributed computer networks. Unfortunately, most existing schemes cannot preserve user anonymity when possible attacks occur and those schemes are insecure. Based on the various cryptography techniques and methods there are few practical and secure single sign-on models are proposed. This survey paper provides an overview of a single sign-on scheme by presenting their features, functionality and benefits to analyze the security level. The objective is to make observations about how the security of this SSO scheme can be improved.

Keywords—Single Sign-On (SSO)

I. INTRODUCTION

Single sign-on (SSO) is a method of access control that enables a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again. Single sign-off is the reverse process whereby a single action of signing out terminates access to multiple software systems. As different applications and resources support different authentication mechanisms, single sign-on has to internally translate to and store different credentials compared to what is used for initial authentication.

With the widespread use of distributed computer networks, it has become common to allow users to access various network services offered by distributed service providers. Consequently, user authentication (also called user identification) plays a crucial role in distributed computer networks to verify if a user is legal and can therefore be granted access to the services requested. To avoid bogus servers, users usually need to authenticate service providers. After mutual authentication, a session key may be negotiated to keep the confidentiality of the data exchanged between a user and a service provider.

In many scenarios, the anonymity of legal users must be protected as well. However, practice has shown that it is a big challenge to design efficient and secure authentication protocols with these security properties in complex computer network environments. There are few practical and secure single sign-on models, even though it is of great importance to current distributed application environments.

Most of the current application architectures require the user to memorize and utilize a different set of credentials (eg, username/password or tokens) for each application he/she wants to access. However, this approach is inefficient and insecure with

the exponential growth in the number of applications and services a user has to access both inside corporative environments and at the Internet. Single sign-on (SSO) is a new authentication mechanism that enables a legal user with a single credential to be authenticated by multiple service providers in distributed computer networks.

Historically a distributed system has been assembled from components that act as independent security domains. These components comprise individual platforms with associated operating system and applications. These components act as independent domains in the sense that an end-user has to identify and authenticate himself independently to each of the domains with which he wishes to interact. This scenario is illustrated above. The end user interacts initially with a Primary Domain to establish a session with that primary domain. This is termed the Primary Domain Sign-On and requires the end user to supply a set of user credentials applicable to the primary domain, for example a username and password.

The primary domain session is typically represented by an operating system session shell executed on the end user's workstation within an environment representative of the end user (e.g., process atrributes, environment variables and home directory). From this primary domain session shell the user is able to invoke the services of the other domains, such as platforms or applications. To invoke the services of a secondary domain an end user is required to perform a Secondary Domain Sign-on. This requires the end user to supply a further set of user credentials applicable to that secondary domain.

An end user has to conduct a separate sign-on dialogue with each secondary domain that the end user requires to use. The secondary domain session is typically represented by an operating system shell or an application shell, again within an environment representative of the end user. From the management perspective the legacy approach requires independent management of each domain and the use of multiple user account management interfaces.

Considerations of both usability and security give rise to a need to co-ordinate and where possible integrate user sign-on functions and user account management functions for the multitude of different domains now found within an enterprise.

II. SOME OF THE FRAMEWORKS

OpenSSO

The Open Web SSO project (OpenSSO) provides core identity services to simplify the implementation of transparent single sign-on (SSO) as a security component in a network infrastructure. OpenSSO provides the foundation for integrating diverse web applications that might typically operate against a disparate set of identity repositories and are hosted on a variety of platforms such as web and application servers. This project is based on the code base of Sun Java™ System Access Manager, a core identity infrastructure product offered by Sun Microsystems.

JOSSO – Java Open Single Sign-On Project Home

JOSSO, or Java Open Single Sign-On, is an open source J2EE-based SSO infrastructure aimed to provide a solution for centralized, platform neutral, user authentication and authorization. The framework allows multiple web server/applications such as the Apache HTTP Server, Apache Tomcat, JBOSS, ASP, PHP etc to authenticate users with credential store. JOSSO communicates with credential stores over the Lightweight Directory Access Protocol (LDAP) or a JDBC connection. JOSSO exposes Single Sign On services using SOAP over HTTP protocol allowing it to easily integrate with non-Java applications. JOSSO implements JAAS (Java Authentication and Authorization Service) to authenticate and enforce access controls upon users.

SAML Single Sign-On (SSO) Service for Google Apps

Security Assertion Markup Language (SAML) is an XML standard that allows secure web domains to exchange user authentication and authorization data. Using SAML, an online service provider can contact a separate online identity provider to authenticate users who are trying to access secure content.

Google Apps offers a SAML-based Single Sign-On (SSO) service that provides partner companies with full control over the authorization and authentication of hosted user accounts that can access web-based applications like Gmail or Google Calendar. Using the SAML model, Google acts as the service provider and provides services such as Gmail and Partner Start Pages (PSP). Google partners act as identity providers and control usernames, passwords and other information used to identify, authenticate and authorize users for web applications that Google hosts.

III. LITERATURE SURVEY

3.1 Optimistic Fair Exchange of Digital Signatures

As more business is conducted over the Internet, the *fair exchange problem* assumes increasing importance. For example, suppose player A is willing to give an electronic check to player B in exchange for an electronic airline ticket. The problem is this: how can A and B exchange these items so that either each player gets the other's item, or neither player does.

Both electronic checks and electronic airline tickets are implemented as digital signatures. One could use an on-line trusted third party in every transaction to act as a mediator: each player sends his item to the third party, who upon verifying the correctness of both items, forwards the item to the other player.

In this paper, a new protocol is presented for fair exchange that takes a different approach. This protocol uses a trusted third party, but only in a very limited fashion: the third party is only needed in cases where one player attempts to cheat or simply crashes; therefore, in the vast majority of transactions, the third
party will not need to be involved at all. The protocol can also be adapted to exchange encrypted data. It relies on a trusted third party, but is "optimistic," in that the third party is only needed in cases where one player crashes or attempts to cheat.

Compared to a protocol using an on-line third party, the optimistic approach greatly reduces the load on the third party, which in turn reduces the cost and insecurity involved in replicating the service in order to maintain availability. It also makes it more feasible to implement the trusted third party service as a distributed, fault-tolerant system, eliminating the single point of failure.

A key feature of this protocol is that a player can always force a timely and fair termination, without the cooperation of the other player, even in a completely asynchronous network. A specialization of this protocol can be used for contract signing; this specialization is not only more efficient, but also has the important property that the third party can be held *accountable* for its actions: if it ever cheats, this can be detected and proven.

This new protocol can be used to exchange commonly used digital signatures, including RSA, DSS , Schnorr, Fiat–Shamir, GQ , and Ong–Schnorr signatures, as well as the payment transcripts used in Brands off-line, anonymous cash scheme. Moreover, the protocol can also be adapted to exchange digital content, such as music or stock quotes, and to the related problem of certified e-mail.

3.2 Secure Communication Using Generalized Digital Certificate

A digital certificate is the combination of a statement and a signature of the statement, signed by a trusted certification authority. This work proposes using generalized digital certificate (GDC), for user authentication and key agreement for efficient secure communication. A GDC contains user's public information, such as the information of user's digital driver's license, digital birth certificate, etc., and a digital signature of public information signed by a trusted certificate authority(CA). The trusted third party who issues the Digital Certificate is called as the Certification Authority (CA). This digital signature will never be revealed to the verifier directly. Therefore, the digital signature of a GDC becomes a security factor which can be used for user authentication.

Digital certificate is actually the combination of a statement and a digital signature of the statement. X.509 public-key digital certificate has been widely used to provide authentication on the user's public key contained in the certificate. In X.509 public key digital certificate, the statement normally contains the public key along with some general information's , which is signed by trusted certification authority.

The user is authenticated if he is able to prove that he has the knowledge of the private key corresponding to the public key contained in the X.509 public-key digital certificate. However, the public key digital certificate itself cannot be used to authenticate a user since a public-key digital certificate contains only public information and can be easily recorded and played back once it has been revealed to verifier.

A new form of digital certificate is introduced in this paper. The approach mentioned in the above paper enables a user to be authenticated and a shared secret session key to be established with his communication partner using any general form of digital certificates. In GDC, the public information does not contain any user's public key. Since user does not have any private and public key pair, this type of digital certificate is easier to manage than the X.509 public-key digital certificates.

The digital signature of the GDC is used as the secret token of each user. The owner of this kind of digital certificate never reveals signature of GDC to a verifier in plaintext. Instead, the owner computes a response to the verifier's challenge to prove that he has the knowledge of the digital signature of GDC. Thus, owning a GDC can provide user authentication in a digital world. Therefore the key management in using GDC is much simpler than public key digital certificate and the session key established using this approach can be used for secure communication between the entities.

3.3 Efficient user identification scheme with key distribution preserving anonymity

In 2000, Lee and Chang presented a user identification scheme that also can simultaneously achieve key exchange requirement while preserving the user anonymity. Their idea is valuable especially when it is applied to some applications in which the identity of the user should be protected from the public in the distributed computer networks. Unfortunately, this paper shows that their scheme is insecure under two attacks and a more efficient identification scheme is proposed for preserving the same merits.

With the rapid growth of computer networks, people rely more on digital communications. The computer networks connect hosts and user terminals into a distributed computing environment which provides the advantages of increasing reliability, sharing information and computing power, etc. However, there might exist some potential problems that should be taken into consideration, e.g., who can have access to the information and up to what privilege he owns, etc. It is important to develop some effective mechanisms to protect the systems from malicious attackers.

Among all the mechanisms, user authentication is the first armor to prevent the unauthorized adversary form obtaining the system resources or information. In the distributed computing environments, it might be required to maintain the user anonymity. That is, only the service provider can identify the user, while all other entities cannot determine any information of the user's identity.

In 2000, Lee and Chang proposed a user identification scheme based on the security of the factoring problem and the one-way hash function. Their scheme has the following advantages: (1) users can request services without revealing their identities to the public; (2) each user needs to maintain only one secret; (3) it is not required for service providers to record the password files for the users; (4) no master key updating is needed if a new service provider is added into the system.

Based on the same cryptographic assumptions made in their scheme, a new identification scheme is proposed to eliminate the security leaks. The proposed scheme achieves the same requirements of the Lee-Chang scheme and outperforms their scheme in both aspects of computational complexities and communication costs.

3.4 Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards

User authentication and key agreement is an important security primitive for creating a securely distributed information system. Additionally, user authentication and key agreement is very useful for providing identity privacy to users. This paper presented a robust and efficient user authentication and key agreement scheme using smart cards.

In various network environments, if a user needs to use or control a remote server, the user first needs to pass the authentication scheme of the server. To provide a secure authentication system, password-based methods are often used
in many remote log-in servers. A new scheme based on elliptic curve cryptosystems are proposed for providing all the functionalities and enhancing the efficiency of Fan *et al.*'s scheme.

The proposed scheme consists of five phases: 1) the parameter generation phase; 2) the registration phase; 3) the precomputation phase; 4) the log-in phase; and 5) the password-changing phase. In the registration phase, the server identifies a user and then issues a smart card to the identified user. Then, the user and the server do the log-in phase to authenticate each other and generate an agreed-upon session key. If the user wants to change his password, he needs to do the password-changing phase.

This scheme can prevent the insider attack and it is very useful in limited computation and communication resource environments to access remote information systems. The main merits include the following: 1) the computation and communication cost is very low; 2) there is no need for any password or verification table in the server; 3) a user can freely choose and change his own password; 4) it is a nonce-based scheme that does not have a serious time-synchronization problem; 5) servers and users can authenticate each other; 6) the server can revoke a lost card and issue a new card for a user without changing his identity; 7) the privacy of users can be protected; 8) it generates a session key agreed upon by the user and the server; and 9) it can prevent the offline dictionary attack even if the secret information stored in a smart card is compromised.

3.5 Provably Secure Single Sign-on Scheme in Distributed Systems and Networks

Distributed systems and networks have been adopted by telecommunications, remote educations, businesses, armies and governments. A widely applied technique for distributed systems and networks is the single sign-on (SSO) which enables a user to use a unitary secure credential (or token) to access multiple computers and systems where he/she has access permissions.

With the wide spreading of distributed computer networks, various network services have gained importance and popularity in recent few years. Consequently, user authentication has been widely used in distributed computer networks to identify a legal user who requires accessing network services. To prevent bogus servers, mutual authentication should be considered, and also, a session key establishment is normally required.

However, designing efficient and secure mutual authentication protocols is challenging in computer networks. Moreover, with the increasing usage of network services, a user may need to maintain more and more ID/password pairs for accessing different distributed service providers, which impose a burden on users and service providers as well as the communication overhead of computer networks. Single sign-on (SSO) mechanism provides a good remedy to this problem, as it allows a user with a single credential to access multiple service providers.

Intuitively, there are three basic security requirements for SSO schemes, namely completeness, soundness and credential privacy. However, to the best of our knowledge soundness has not been formally studied yet and how to preserve both soundness and credential privacy is still a challenge.

However, most existing SSO schemes have not been formally proved to satisfy credential privacy and soundness of credential based authentication. To overcome this drawback, they formalise the security model of single sign-on scheme with authenticated key exchange. Specially, the difference between soundness and credential privacy is pointed out and they define them together in one definition. Also, they propose a provably secure single sign-on authentication scheme, which satisfies soundness, preserves credential privacy, meets user anonymity, and supports session key exchange.

The proposed scheme is very efficient so that it suits for mobile devices in distributed systems and networks. In this new scheme, to preserve credential generation privacy, the *TCP* signs a Schnorr signature on user identity; and to protect credential

privacy and soundness, the user exploits his/her credential as a signing key to sign a Schnorr signature on the hashed session key. In fact, Schnorr signature mechanism is more efficient than RSA mechanism which has been employed by Chang-Lee scheme. Thus, the proposed scheme reduces the computation cost, enhances the confidentiality, and preserves soundness and credential privacy.

IV. CONCLUSION

In this paper we have done literature survey for analyzing the security of the Single sign-on mechanism. This is our first paper in which only the overview of various secure user authentication techniques have been done and after that we will do the experiment for analyzing the attacks against the Single sign-on scheme and we will provide the security against those attacks in order to meet the credential privacy and soundness of authentication. We are going to use JAVA coding for analyzing these improved security levels and performance.

REFERENCES

[1] Guilin Wang,Jiangshan Yu, and Qi,"Security analysis of a single sign-on mechanism for distributed computer networks,"*IEEE Trans. Industrial Informatics.*,vol. 9,no. 1,Feb 2013.

[2] N. Asokan, Member, IEEE, Victor Shoup, Member,IEEE, and Michael Waidner, Member,IEEE, "Optimistic Fair Exchange of Digital Signatures",*IEEE Journal on selected areas in communications*,vol. 18,no.4,April 2000.

[3] Bismin V Sherif, Andrews Jose,"Secure Communication Using Generalized Digital Certificate"*International Journal of Computer Applications Technology and Research*,vol. 2,Issue 4, 396-399, 2013.

[4] T.-S.Wu and C.-L. Hsu, "Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks," *Comput. Security*, vol. 23, no. 2, pp. 120–125, 2004.

[5] W. Juang, S. Chen, and H. Liaw, "Robust and efficient password authenticated key agreement using smart cards," *IEEE Trans. Ind. Electron.*, vol. 15, no. 6, pp. 2551–2556, Jun. 2008.

[6] J. Yu, G.Wang, and Y.Mu, "Provably secure single sign-on scheme in distributed systems and networks," in *Proc. 11th IEEE TrustCom*, Jun.2012, pp. 271–278.

[7] C.-C. Chang and C.-Y. Lee, "A secure single sign-on mechanism for distributed computer networks," *IEEE Trans. Ind. Electron.*, vol. 59, no. 1, pp. 629–637, Jan. 2012.

[8] The Open Group, "Security Forum on Single Sign-on", http://www.opengroup.org/security/l2-sso.html.

[9] C.-L. Hsu and Y.-H. Chuang, "A Novel User Identification Scheme with Key Distribution Preserving User Anonymity for Distributed Computer Networks", *Inf. Sci.*, vol. 179, no. 4, pp. 422-429, 2009.

[10] C.P. Schnorr, "Efficient Signature Generation by Smart Cards", *J. Cryptology*, vol. 4, no. 3, pp. 161-174, 1991.

[11] C. Fan, Y. Chan, and Z. Zhang, "Robust remote authentication scheme with smart cards," *Comput. Secur.*, vol. 24, no. 8, pp. 619–628, Nov. 2005.

[12] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Designs, Codes Cryptogr.*, vol. 19, no. 2/3, pp. 173–193, Mar. 2000.

[13] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, pp. 120–126, 1978.

[14] C. Schnorr, "Efficient signature generation by smart cards," *J. Cryptology*, vol. 4, pp. 161–174, 1991.

[15] Lee WB, Chang CC. User identification and key distribution maintaining anonymity for distributed computer network. Comput Syst Sci Eng 2000;15(4):211e4.

[16] K. Lauter, "The advantages of elliptic curve cryptography for wireless security," *Wireless Commun.*, vol. 11, no. 1, pp. 62–67, Feb. 2004.

