International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

# Security Enhancement of Single Sign-On Mechanism for Multiple Service Authentications

**Anil. P. Jawalkar[1], R. Radha[2]**

[1]M.Tech Student, Department of CSE, Malla Reddy College of Engineering and Technology, Gundlapochampally village, Medchal Mandal, Rangareddy District, A.P, India

2Associate Professor, Department of CSE, Malla Reddy College of Engineering and Technology, Gundlapochampally village, Medchal Mandal, Rangareddy District, A.P, India

**Abstract:** ***In this paper, permit users to sign on only once and have their identities automatically verified by each application or service they desire to access afterwards. There are lots of practical and secure single sign-on mechanisms even though it is of remarkable significance to current distributed application environments. The majorities of application architectures involve the user to memorized and utilize a different set of credentials (eg, username/password or tokens) for each application he/she wants to open. In this method is uneconomical and insecure with the exponential growth in the number of applications and services a user has to retrieve both inside corporative environments and at the internet. The Single sign-on is a novel authentication method that allows a authorized user with a single credential to be authenticated by multiple service providers in distributed computer networks. In this paper we projected a new single sign-on scheme and state its security by supplying well-organized security arguments. In this paper shows the Chang & Lee scheme and it intend to improve security using RSA encryption and decryption. Recognition of user is an important access control method for client–server networking architectures. The goal of a single sign on policy is to eradicate individual sign on procedures by centralizing user authentication and identity management at a central identity provider. In this paper a SSO the user should flawlessly authenticated to his multiple user accounts once he verify his identity to the identity provider.***

**Keywords:** Single Sign-On (SSO), Single Channel Per Carrier (SCPC)

## 1. Introduction

Identification of user is an important access control mechanism for client–server networking architectures. The goal of a single sign on platform is to eliminate individual sign on procedures by centralizing user authentication and identity management at a central identity provider. In a single sign-on solution, the user should seamlessly authenticated to his multiple user accounts (across different systems) once he proves his identity to the identity provider. Nevertheless, in many current solutions, the user is required to repeat sign on for each service using the same set of credentials, which are validated at the identity provider by each service. User authentication [3], [4] plays a crucial role in distributed computer networks to verify the legacy of a user and then can be granted to access the services requested. To prevent bogus servers, users usually need to authenticate service providers.

After mutual authentication, a session key may be negotiated to keep the confidentiality of data exchanged between a user and a provider [4], [5], [6]. In many scenarios, the anonymity of legal users should be protected as well [4], [7], [6]. These protocols offer varying degrees of efficiency. This paper aims to ensure more security to the existing Chang Lee SSO scheme. It also aims to add additional security during data transfer between user and provider. It also proposes further research into more efficient enhancements to the current work. The main objective of this paper is to enhance security for single sign-on solutions and eliminate the need for users to repeatedly prove their identities to different applications and hold different credentials for each application.

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.

## 2. Related Work

In 2000, Lee and Chang [4] proposed a user identification and key distribution scheme to maintain user anonymity in distributed computer networks. Later, Wu and Hsu [8] pointed out that Lee-Chang scheme is insecure against both impersonation attack and identity disclosure attack. Meanwhile, Yang et al. [9] identified a weakness in Wu-Hsu scheme and proposed an improvement. In 2006, however, Mangipudi and Katti [10] pointed out that Yang et al."s scheme suffers from DoS (Deniable of Service) attack and presented a new scheme. In 2009, Hsu and Chuang [11] showed that both Yang et al. and Mangipudi-Katti schemes were insecure under identity disclosure attack, and proposed an RSA-based user identification scheme to overcome the drawbacks.

On the other hand, it is usually not practical by asking one user to maintain different pairs of identity and passwords for different service providers, since this could increase the workload of both users and service providers as well as the communication overhead of networks. To tackle this problem, single sign-on (SSO) mechanism [12] has been introduced so that after obtaining a credential from a trusted authority, each legal user can use this single credential to authenticate itself and then access multiple service providers. Intuitively, an SSO scheme should meet at least two basic security requirements, i.e., soundness and credential privacy. Soundness means that an unregistered user without a credential should not be able to access the services offered by service providers. Credential privacy guarantees that colluded dishonest service providers should not be able to fully recover a user"s credential and then impersonate the user to log in other service providers. Formal security definitions of SSO schemes were given in [13]. Chang and Lee made a careful study of SSO mechanism. Firstly, they argued that Hsu-Chuang user identification scheme, actually an SSO scheme, has two weaknesses: (a) An outsider can forge a valid credential by mounting a credential forging attack since Hsu-Chang scheme employed naive RSA signature without any hash function to issue a credential for any random identity selected by a user ; and (b) Hsu-Chuang scheme requires clock synchronization since timestamp is used in their scheme. Then, Chang and Lee presented an interesting RSA based SSO scheme, which is highly efficient in computation and communication (So it is suitable for mobile devices), and does not rely on clock synchronization by using nonce instead of timestamp. Finally, they presented well-organized security

## 3. Problem Statement

It is usually not practical by asking one user to maintain distinct pairs of identity and password for different service providers, since this could increase the workload of both users and service providers as well as the communication overhead of networks. To tackle this problem, the single sign-on (SSO) mechanism [16] has been introduced so that, after obtaining a credential from a trusted authority for a short period (say one day), each legal user's authentication agent can use this single credential to complete authentication on behalf of the user and then access multiple service providers. Intuitively, an SSO scheme should meet at least three basic security requirements, i.e., unforgeability, credential privacy, and soundness.

### 3.1 Scope

We identify the flaws in their security arguments to explain why attacks are possible against their SSO scheme. Our attacks also apply to another SSO scheme proposed by Hsu and Chuang, which inspired the design of the Chang–Lee scheme. Moreover, by employing an efficient verifiable encryption of RSA signatures proposed by Ateniese, we propose an improvement for repairing the Chang–Lee scheme.

### 3.2 Disadvantages

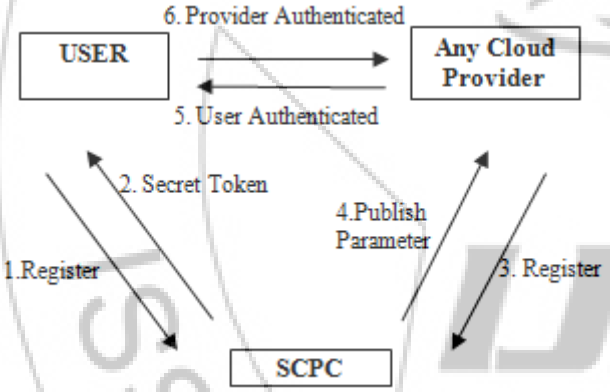
1. Actually an SSO scheme, has two weaknesses an outsider can forge a valid credential by mounting a credential forging attack since the scheme employed naïve RSA signature without using any hash function to issue a credential for any random identity.
2. Their scheme is suitable for mobile devices due to its high efficiency in computation and communication.

## 4. System Implementation

Single Sign-On

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 a distributed computer network. The single sign-on (SSO) mechanism has been introduced so that, after obtaining a credential from a trusted authority for a short period, each legal user's authentication agent can use this single credential to complete authentication on behalf of the user and then access multiple service providers. Intuitively, an SSO scheme should meet at least three basic security requirements, i.e., unforgeability, credential privacy, and soundness. Unforgeability demands that, except the trusted authority, even a collusion of users and service providers are not able to forge a valid credential for a new user. Credential privacy guarantees that colluded dishonest service providers should not be able to fully recover a user's credential and then impersonate the user to log in to other service providers. Soundness means that an unregistered user without a credential should not be able to access the services offered by service providers.

## 5. Provider Authenticated




### 5.1 Credential Recovering Attack

In this attack, a malicious service provider who has communicated with a legal user twice can successfully recover the user's credential. Then, the malicious service provider can impersonate the user to access resources and services provided by other service providers.

### 5.2 Impersonation Attack

In this attack may enable an outside attacker without any valid credential to impersonate a legal user or even a nonexistent user to have free access to the services.

### 5.3 Smart Card Producing Center

In their scheme, RSA cryptosystems are used to initialize a trusted authority, called an SCPC (smart card producing center), and service providers, denoted as 's. The Diffie–Hellman key exchange technique is employed toestablish session keys. In the Chang–Lee scheme, each user applies a credential from the trusted authority SCPC, who signs an RSA signature for the user's hashed identity. After that, uses a kind of knowledge proof to show that he/she is in possession of the valid credential without revealing his/her identity to eavesdroppers. Actually, this is the core idea of user authentication in their scheme and also the reason why their scheme fails to achieve secure authentication as we shall show shortly.

### 5.4 Advantages

1. Users need only one password for access to all applications and systems. Users have immediately have access to all necessary password-protected applications.
2. Users don't need to remember multiple passwords. Users don't have to guess passwords, which potentially expose applications to unauthorized users.
3. The authors claimed to be able to: "prove that and are able to authenticate each other using our protocol." but they provided no argument to show why each party could not be impersonated by an attacker. Second, the authors did discuss informally why their scheme could withstand impersonation attacks.
4. The authors did not give details to show how the BAN logic can be used to prove that their scheme guarantees mutual authentication.
5. In other words, it means that in an SSO scheme suffering these attacks there are alternatives which enable passing through authentication without credentials.

## 6. Conclusion

Most existing single sign-on schemes suffer from various security issues and are vulnerable to different attacks. In this paper, we first formalized authenticated key exchange single sign-on scheme. Specially, we formally defined secure authentication for both users and service providers as such a treatment has not been studied yet [6]. Moreover, a Schnorr mechanism based SSO scheme has been proposed to overcome the drawbacks of Chang-Lee scheme [12] but keep the same advantages. In this new scheme, to preserve credential generation privacy, the TCP signs a Schnorr signature [18][13] 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 [18][13] 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.

## References

[1] Weaver and M. W. Condtry, "Distributing Internet services to the network's edge", IEEE Trans. Ind. Electron., 50(3): 404-411, Jun. 2003.
[2] L. Barolli and F. Xhafa, "JXTA-OVERLAY: A P2P platform for distributed, collaborative and ubiquitous computing", IEEE Trans. Ind.Electron., 58(6): 2163-2172, Oct. 2010.
[3] L. Lamport, "Password authentication with insecure communication",Commun. ACM, 24(11): 770-772, Nov. 1981.

[4] Chin-Chen Chang, "A secure single mechanism for distributed computer networks," IEEE Trans. On Industrial Electronics ,vol. 59, no. 1, Jan 2012.
[5] W. B. Lee and C. C. Chang, "User identification and key distribution maintaining anonymity for distributed computer networks," Computer Systems Science and Engineering, 15(4): 113-116, 2000.
[6] W. Juang, S. Chen, and H. Liaw, Robust and efficient password authenticated key agreement using smart cards, IEEE Trans. Ind. Electron.,15(6): 2551-2556, Jun. 2008.
[7] X. Li, W. Qiu, D. Zheng, K. Chen, and J. Li, "Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards," IEEE Trans. Ind. Electron., 57(2): 793-800, Feb. 2010.
[8] T.-S. Wu and C.-L. Hsu, "Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks," Computers and Security, 23(2): 120-125, 2004.
[9] Y. Yang, S. Wang, F. Bao, J. Wang, and R. H. Deng, "New efficient user identification and key distribution scheme providing enhanced security," Computers and Security, 23(8): 697-704, 2004.
[10] K. V. Mangipudi and R. S. Katti, "A secure identification and key agreement protocol with user anonymity (sika)," Computers and Security, 25(6): 420-425, 2006.
[11] C.-L. Hsu and Y.-H. Chuang, "A novel user identification scheme with key distribution preserving user anonymity for distributed computer networks," Inf. Sci., 179(4): 422-429, 2009.
[12] Data Encryption Standard, NIST Std. FIPS PUB 46-2, 1988.
[13] Advanced Encryption Standard, NIST Std. FIPS PUB 197, 2001.
[14] W. Stallings, Cryptography and Network Security, 4th ed. Upper Saddle River, NJ: Pearson, Nov. 2005, pp. 334–340.
[15] Lee WB, Chang CC. User identification and key distribution maintaining anonymity for distributed computer network. Computer Systems Science 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.
[17] M. Bellare and P. Rogaway, "Entity Authentication and Key Distribution", CRYPTO, pp. 232-249, 1993.
[18] C.P. Schnorr, "Efficient Identification and Signatures for Smart Cards", CRYPTO ,pp. 239-252, 1989.
[19] 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.
[20] 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.
[21] 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.
[22] 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.
[23] 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.
[24] 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.
[25] 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.