International Journal of Multidisciplinary Research and Development

Volume:2, Issue:4, 153-156
April 2015
www.allsubjectjournal.com
e-ISSN: 2349-4182
p-ISSN: 2349-5979
Impact Factor: 3.762

Harish Pote
Department of Information Technology, ISB&M School of Technology, Pune

Neha Patil
Department of Information Technology, ISB&M School of Technology, Pune

Deepali Gosavi
Department of Information Technology, ISB&M School of Technology, Pune

Correspondence:
Harish Pote
Department of Information Technology, ISB&M School of Technology, Pune

Single sign-on mechanism security enhancement for distributed computer networks

Harish Pote, Neha Patil, Deepali Gosavi

Abstract
Distributed System Single Sign On is an authentication mechanism which allows a user with single credential authenticated by one or more than one Service Providers in Distributed System. Recently, Mr Chang and Mr Lee enhance their previous scheme and they claimed that proposed scheme is more secure than last one SSO mechanism.
In this paper, System implement disadvantages of their scheme, their Single Sign On mechanism having two types of attacks, first one is a malicious service is communicate with the user successfully, then recover the credential and access service providing by another service. Second one is, illegal user without credential access the services by impersonating existent or non-existent user.
Their scheme is based on RSA Encryption; we implement their disadvantages by using efficient Digital Signature with RSA for enhance more security.

Keywords: Distributed System, Single Sign On, Signature, Encryption, Authentication

1. Introduction
The Distributed Computer Network several users and several service providers. It allows all users to access multiple services provided by service providers [1],[2]. User authentication is also play important role in the Distributed System for identifying legal user and provides service to them. To avoid non-existent user or malicious servers we need authenticate the service providers. After authentication, session key play important role to keep data confidentiality when data transaction in between user and service provider [3], [4].
In that process legal user anonymity is impotent to protected [3], [5]. Usually, it is not practical a user maintain different identity and password for multiple services that is increasing `workload of users and service providers. To overcome this problem, the single sign-on mechanism [7] has been proposed so that, after receiving a credential from a trusted authority.
In this paper, System implementing the Chang–Lee scheme [8] are insecure by proposing two types attacks, first one is credential recovering and second one is malicious user without credentials. In first one, a malicious service provider who communicates with the user twice can recover the credential of that user and user this credential to access services and resources behalf of user. The second one is non-existent user impersonate legal user and act as user, since without having valid credential access the services and resources. These attacks that mean the Chang–Lee Single Sign On scheme failure to provide credential privacy and soundness, which are important requirements of SSO scheme. To implement these disadvantage of SSO, we propose enhance scheme for user authentication. We employ RSA with the encryption of signatures [9] to verifiably encrypt credential. Signature with the RSA enhances the security.

1. Related Works
In 2000, Lee and Chang [12] proposed a user identification and key distribution scheme to maintain user anonymity in distributed computer networks.
Later, Wu and Hsu [13] pointed out that Lee-Chang scheme is insecure against both impersonation attack and identity discovery attack. Meanwhile, Yang et al. [14] identified a weakness in Wu-Hsu scheme and proposed an improvement.
In 2006, however, Mangipudi and Katti [15] 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 [16] showed that both Yang et al. and Mangipudi-Katti proposed

schemes were insecure under identity discovery attack, and proposed scheme an RSA-based user identification scheme to overcome the drawbacks. Contrariwise, it is usually not practical by asking one user to maintain different pairs of identity and passwords for different service providers, meanwhile 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 [17] has been introduced so that after obtaining a credential from a SCPC, each legal user can use this single credential to authenticate itself and then access multiple service providers. Instinctively, an SSO scheme should meet at least two basic security requirements, soundness and credential privacy. Soundness is an unregistered user without a credential should not be able to access the services offered by service providers. Credential privacy guarantees that malicious 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 Single Sign-On schemes were given in [18]. Chang and Lee made a careful study of Single Sign-On mechanism. Firstly, they claimed that Hsu-Chuang user identification scheme, essentially an Single Sign-On 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 proposed stimulating RSA based Single Sign-On scheme, which is highly efficient in computation and communication, and does not rely on clock synchronization by using nonce instead of timestamp. Finally, they proposed efficient security analysis to show that their SSO scheme supports secure mutual authentication, session key covenant, and user privacy.

In [18], Han et al. proposed a generic SSO construction which relies on broadcast encryption plus zero knowledge (ZK) proof showing that the prover knows the corresponding private key of a given public key. So, obliquely each user is implicit to have been issued a public key in a public key infrastructure (PKI). In the setting of RSA cryptosystem, such a ZK proof is very ineffective due to the complexity of interactive communications between the prover (a user) and the verifier. So, compared with Han et al's generic system, Chang-Lee scheme has several attracting features: less underlying primitives without using broadcast encryption, high efficiency without recourse to ZK proof, and no requirement of PKI for users.

Table 1: Notations used in the algorithm

Notations	Descriptions
SCPC	A trusted authority
U_i, P_j	The user and service provider respectively
ID_X	The identity of the entity X
S_X	The secret token of entity X
e_X	The public key of entity X
d_X	The private key of entity X
$E_k(M)$	The symmetric encryption of plaintext M using key K
$D_k(C)$	The symmetric encryption of cipher text C using key K
h(·)	The one way hash function
‖	The concatenation operator

2. Proposed Scheme

1. Initialization

I. Select two large prime p and q and calculate N=p*q

II. Determine key pair (e,d), ed= 1 mod Φ(N)
   a. Where , Φ(N)=(p-1)*(q-1)

III. Select generator g over fields Z*n
   a. Where, n is large odd prime number

IV. Protect d, and publish (e,g,n,N).

2. Registration

I. After request of user U_i SCPC gives ID_i to user and $S_i = h(ID_i)^{2d} \ mod \ N$.

II. As user Service provider is also register to SCPC and each Service Provider $P_j$with the identity ID_j maintain key pairs of signing and verifying keys.
   a. $\sigma_j(SK_j, msg)$ signing key,
   b. $Ver(PK_j, msg, \sigma_j)$ Verifying key. $output\ is\ 0\ or\ 1, signature\ is\ invalid\ or\ valid\ respectively.$

3. Authentication

1. User U_i send request to Service Provider P_j. $msg1(req, n1)$.
2. P_j calculate its session key $Z = g^k \ mod \ n$
3. Set $u = Z||ID_j|| \ n1$ and issue $v = \sigma_j(SK_j, u)$.
4. P_j send msg to U_i. $msg2(Z, v, n2)$
5. User sets $u = (Z||ID_j||n1)$and verify $Ver(PK_j, u, v) = 0$ if output is 0 signature is invalid user terminate conversation or accept signature of P_j.
6. User select random number t and calculate w, k_{ij}, K_{ij}. Where, $w = g^t mod\ n., k_{ij} = Z^t mod\ n., K_{ij} = h(ID_j||k_{ij})$
7. For authentication user encrypt signature S_i. $P_1 = S_i \cdot y^r mod\ N\ and\ P_2 = g^r mod\ N$. Where r is random integer with fixed length.
8. Then user calculate two commitment
   a. $a = (y^e)^{r1} mod\ N$
   b. $b = g^{r1} mod\ N.$
9. For NIZK proof calculates.
   a. $d_x = h(K_{ij}||w||n2||y^{er}||P_2||y^e||g||a||b)$
   b. $s = r1 - d_x \cdot r$
   Then $x = (P_1, P_2, a, b, d_x, s)$
10. User encrypt his ID_i , new nonce $n3$, $P_j's$ nonce using session key K_{ij}.
   a. Cipher text $C = E_{K_{ij}}(ID_i||n2||n3)$.
11. U_i send msg to P_j. $msg3(w, x, C)$.
12. P_j decrypt cipher text received by user and recover $(ID_i||n2||n3)$

13. And compute

$$y^{er} = \frac{{P_1}^e}{h(ID_i)^2 mod} N$$

a. $a = (y^e)^s \cdot (y^{er})^c mod\ N$
b. $b = g^s \cdot {P_2}^c mod\ N$

14. P_j verify $(c, s) \in \{0,1\}^k \times \pm\{0,1\}^{\in(l_G+k)+1}$. if output is negative terminate conversation otherwise accept msg to user with nonce $V = h(n3)$.
15. $msg4(v)\ to\ user.$
16. User check $V = h(n3).true\ or\ not$. if true then proceed otherwise terminate conversation.

Encryption and Decryption-:

ElGamal Public key encryption algorithm is used for the encryption and decryption between user and the provider. The ElGamal Algorithm provides an alternative to the RSA for public key encryption.

1. Security of the RSA depends on the difficulty of factoring large integers.
2. Security of the ElGamal algorithm based on the difficulty of computing discrete logs in a large prime modulus

Data which is send from each provider to user is encrypted and send to user, then user decrypts it and the original data is regained. All these encryption and decryption are done using Elgamal Public key encryption algorithm. This implemented in Java using socket programming and it uses server programs and client programs. We can run the providers parallel by using multithreading features of Java.

Elgamal has the advantage that the same plaintext gives a different Cipher text each time it is encrypted. The ElGamal Algorithm provides an alternative to the RSA for public key encryption. Security of the ElGamal algorithm depends on the difficulty of computing discrete logs in a large prime modulus.

ElGamal has the disadvantage that the cipher text is twice as long as the plaintext. Elgamal is quite slow.

ElGamal-:

To overcome the drawback in the Chang-Lee scheme [8], we propose an improvement by implementing ElGamal Public key encryption algorithm.

Elgamal comprises two users. In Elgamal,

- Each user has a private key x
- Each user has three public keys: prime modulus p, generator g and public Y = gx mod p
- Secure key size > 1024 bits (today even 2048 bits)
- Elgamal is quite slow; it is used mainly for key authentication protocols

Say Alice and Bob is two user, Prime p and generator g are public keys of Bob, Alice chooses the random key k, Bob chooses random x, then bob calculate Y as Y = g x mod p and send it to Alice, Alice then calculate K as K = Y k mod p, From the k and K Alice calculate the two cipher c1 and c2, C1= g k mod p and C2=M K mod p

Then this c1, c2 send to the Bob, Bob can calculate K by K= ${C_1}^X$ mod p and recovers message M = K^{-1}C2 mod p , Here K^{-1}= the inverse of K mod p

4. Conclusion

In this paper, we validated two effective impersonation attacks on Chang and Lee's SSO scheme [8]. The first attack shows that their proposed scheme cannot preserve the privacy of a user's credential; therefore, a malicious service provider can imitate a legal user in order to enjoy the resources and services from other service providers. The second attack interrupts the soundness of authentication by giving an outside attacker without credential the chance to impersonate even a unreal user and then easily access resources and services provided by service providers. We also debated why their well-organized security arguments are not strong enough to assurance the security of their SSO scheme.

In addition, we clarified why Hsu and Chuang's scheme [6] is also vulnerable to these attacks. Also, by employing an efficient verifiable encryption of RSA signatures introduced by Ateniese [9], we proposed an upgraded Chang–Lee scheme to achieve soundness and credential privacy. As future work, it is stimulating to formally define authentication soundness and construct efficient and provably secure single sign-on schemes. Based on the draft of this work [10], a initial formal model addressing the soundness of SSO has been proposed in [11]. Further research is essential to inspect the maturity of this model and study how the security of the improved SSO scheme proposed in this paper can be formally proven.

5. References

1. A. C. Weaver and M. W. Condtry, "*Distributing internet services to the network's edge*," *IEEE Trans. Ind. Electron.*, vol. 50, no. 3, pp.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.*, vol. 58, no. 6, pp. 2163–2172, Oct. 2010.
3. W. B. Lee and C. C. Chang, "*User identification and key distribution maintaining anonymity for distributed computer networks*," *Comput. Syst. Sci. Eng.*, vol. 15, no. 4, pp. 113–116, 2000.
4. 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.
5. 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.*, vol. 57, no. 2, pp. 793–800, Feb. 2010.
6. 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.
7. "Security Forumon Single Sign-On," TheOpenGroup [Online].Available: *http://www.opengroup.org/security/l2-sso.htm*
8. 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.
9. G. Ateniese, "*Verifiable encryption of digital signatures and applications*," *ACM Trans. Inf. Syst. Secure.*, vol. 7, no. 1, pp. 1–20, 2004.
10. G. Wang, J. Yu, and Q. Xie, "*Security analysis of a single sign-on mechanism for distributed computer networks*," Cryptology ePrint Archive, Rep. 102, Feb. 2012 [Online]. Available: http://eprint.iacr.org/2012/107
11. 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.
12. Chin-Chen Chang, "*A secure single mechanism for distributed computer networks*," *IEEE Trans. On Industrial Electronics, vol. 59, no. 1*, Jan 2012.

13. 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.
14. 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.
15. 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.
16. 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.
17. Data Encryption Standard, NIST Std. FIPS PUB 46-2, 1988.
18. Elgamal Encryption Standard, NIST Std. FIPS PUB 197, 2001.