International Journal of Multidisciplinary Research and Development

Volume: 2, Issue: 4, 191-194
April 2015
www.allsubjectjournal.com
e-ISSN: 2349-4182
p-ISSN: 2349-5979
Impact Factor: 3.762

Pratik Junghare
Department of Information Technology, ISB&M School of Technology, Pune

Dinesh Nanekar
Department of Information Technology, ISB&M School of Technology, Pune

Akanksha Goel
Department of Information Technology, ISB&M School of Technology, Pune

Correspondence:
Pratik Junghare
Department of Information Technology, ISB&M School of Technology, Pune

Research analysis of single sign-on security mechanism for distributed computer networks

Pratik Junghare, Dinesh Nanekar, Akanksha Goel

Abstract
In this aspect we are allowing users to sign on once and have their proof of identities verified by each application or services which they wanted to use afterwards. Number of applications have architectures used by users for utilizing various set of credentials for example tokens for particular application. The single sign on is new way of authentication that allow to legal user with single credential which authenticated by SP (service providers) in distributed networks. In 2012 Chang and Lee discovered mechanism totally based on RSA Cryptosystem mechanism. But that proposed system has two kind of attacks. One is impersonation attack and another one is session attack. Respectively, the first attack deals with credential privacy in the
scheme as a malicious service provider is ready to recover the credentials of a legal user. However the other attack is an impersonation attack without credentials that is session attack which demonstrates how an outside attacker may freely make use of resources and services offered by service providers. In this newly system, to save credential generation privacy, the Trusted party authority signs a Schnorr signature on user identity; and to protect credential privacy.

Keywords: Credentials, Decryption, Encryption, Session Attack, SSO, RSA.

1. Introduction
Single sign on mechanism (sso) is technique in which user can use single credential for the various services in the distributed computer environment. With the increasing of distributed computer network environment user authentication plays important role for accessing various network services.With the wide spread usages of network services, a user may need to maintain more credential (ID/Password/tokens) for accessing various service providers. Which increases complexity on both user side and service provider side. Single sign-on (SSO) mechanism provides solution to this problem, as it allows a user with a single credential to access multiple service providers on distributed computer network. Basically, there are few basic security requirements for Single sign On schemes, namely completeness, soundness and credential privacy. So, developing well efficient and secure mutual authentication protocols is challenging in distributed computer networks.
To prevent dummy servers, users may authenticate service providers first. After both side authentication, a session key may be responsible for to keep the confidentiality and security of data exchanged between a user and a service provider. These scheme offer varying degrees of efficiency. The purpose of this paper to ensure more security to the existing Chang Lee single sign on (SSO) scheme. It also aims to make this scheme more secure by authentication and data transfer between user and provider. It also proposes to use further research into more efficient enhancements to the current work. The main purpose of this paper is to enhance security for single sign-on scheme and eliminate the need for users to remember different credential for different services.

2. Literature Survey
In 2000, Chang and Lee introduced an SSO scheme with user anonymity. Later, Wu and Hsu show that Lee-Chang SSO scheme suffers from credential recovery attack and malicious user attack. Then, Yang et al showed that Wu-Hsu scheme can not maintain credential privacy. In this case malicious service provider can recover users credential and then proposed an improvement to overcome this limitation. In 2006, Mangipudi and Katti [10] shows that Yang et al.'s scheme is insecure against Deniable of Service (DoS) attack and they introduced a new scheme.

In 2009, Hsu and Chuang [11] performed that both Yang et al. and Mangipudi-Katti schemes have not provided user anonymity. Identity disclosure attacks possible on both scheme. Later, to prevent that attacks, Hsu and Chuang proposed an RSA-based user identification scheme. Recently, Chang and Lee [12] proved that the impersonation attacks are possible on Hsu-Chuang scheme and the it requires additional time-synchronized mechanisms.

Then, chang and lee introduced a user anonymity preserving improvement, which uses random nonce to replace additional time-synchronized mechanism, and it does not required PKI (Public key infrastructure) for users, and suits for mobile device users. However, the security analysis [6] shows that Chang-Lee scheme not provide proper user authentication and to preserve credential privacy.

Chang lee scheme is not suitable for the mobile device user in distributed system and network, so it is necessary to overcome the drawback in Chang-Lee scheme. Moreover, the soundness of credential based authentication should be formalized and the credential privacy should be preserved.

in this paper first we state a simple model for SSO with a its definition to formally specify functionality and credential privacy (Section II). Then, after reviewing Chang-Lee SSO scheme in Section III , we improve Chang-Lee scheme by using RSA with digital signature in Section V due to its simplicity and enforceability [14], [15].

3. Review of Chang-Lee Scheme

In that scheme, RSA are used to initialize a SCPC (smart card producing center) also called trusted authority, and service providers, denoted as Pj 's. The Diffie-Hellman key exchange technique is used to establish session keys. In this scheme, SCPC provides the credential for each user Ui. and RAS is used to make a hashed signature of it. then, Ui uses a knowledge proof to show that it have a valid credential without telling it identity to the evasdropper. Actually in their scheme, this is the idea of user authentication. And the reason why they fails to achieve secure authentication. On the other side, RSA key pair is maintained by each Pj for server authentication. Chang-Lee's SSO scheme consists of three phases: system initialization, registration, and user identification. The details are as follows.

A. System Initialization Phase

The SCPC first selects two large primes p and q, and then calculate N = pq. then, SCPC determines its RSA key pair (e , d) such that ed = 1 mod ∅(N), where ∅(N) = (p − 1)(q − 1). Now SCPC chooses a generator G ∈ Z_n^* here n is also a large prime number. Finally, SCPC distributes (e, g, n, N), keeping d as a secret, and erases (p; q).

B. Registration Phase

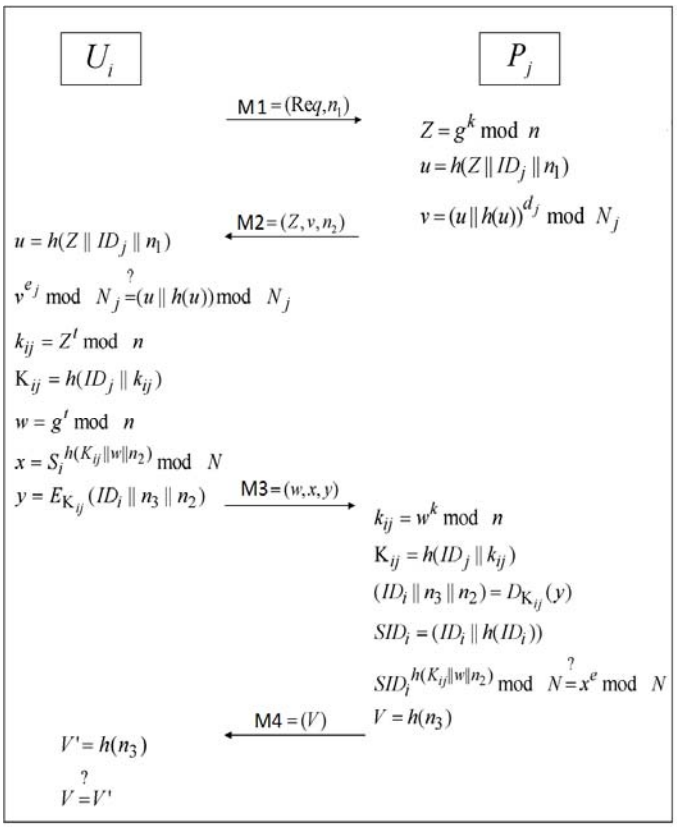
Here, each user Ui sends its unique identity IDi to trusted authority. Then, SCPC returns Ui the credential Si = (IDi II h(IDi))d mod N, here II state a concatenation of two binary strings and h(·) is a cryptographic one-way hash function.now Here, both IDi and Si transferred via a secure channel.

Each service provider Pj and its identity IDj should maintain its own RSA public parameters (ej ;Nj) and private key dj same as doen by SCPC.

C. User Identification Phase

To accessing the services of a service provider Pj , a user Ui needs to prove its identity specified in fig 1. Here, Np and Nu are integers which randomly chosen by Pj and Ui respectively ; n1, n2 and n3 are three random nonce's , and E(·) denotes a symmetric key encryption scheme which is used to protect the confidentiality of user Ui' s identity IDi.

- User Ui sends the service request message M1 to the service provider Pj , Pj generates and returns the user message M2 which includes its RSA signature on (Z, IDj , n1).Now this signature is verified, here user Ui has authenticated service provider Pj successfully. Here, Pj create Diffie-Hellman key exchange variable Z = g^k mod n.
- Then, user Ui generates his Diffie-Hellman key exchange variable Z = g^t mod n and issues a proof $X = S_i^{h(k_{ij}||w||n_2)}$,where K_{ij}=h(IDi || k_{ij}) is the derived session key and k_{ij}= Z^tmod n = w^k mod n = g^{kt} mod n is the key obtained by using the Diffie-Hellman key exchange protocol.
- Proof x = $S_i^{h(k_{ij}||w||n_2)}$ tells Pj that Ui have a valid credential Si without revealing the value of Si. After receiving message M3, x's validity is confirmed by service provider Pj by checking if x = $SID_i^{h(k_{ij}||w||n_2)}$ mod N = X^e mod N, where SIDi = (IDi || h(IDi)).Now user Ui has been authenticated by service provider Pj.
- Finally, message M4 (i.e.h(n3)) show that message M3 has reached to Pj correctly, which show that successfully mutual authentication and session key establishment happened between Pj and Ui.



4. Attacks on Chang-Lee Sheme

As we seen Chang-Lee scheme achieves mutual authentication. By the above discussion, here we conclude that chang-lee scheme is not secure from the two attack respectively "credential recovery attack ", which is related

to the credential privacy in the chang-lee scheme. And another is "impersonation attack without credential" in which outsider attacker can freely access the services which is offered by the service provider. This two attack can affect both user and the service provider in the real life.

Now we first describe this two attack and then analyze them.

A. Credential recovering attack

Chang-Lee SSO scheme guaranty the credential privacy upon receiving the credential proof x = $S_i^{h_2}$mod N, where h2 denotes h(k_{ij} || w || n_2), h2 not allow Pj to recover user Ui's credential Si, it comput Si = $x^{h_2^{-1}}$ mod N, where h_2^{-1} refers to h_2^{-1} mod (N). Its difficult to calculate h_2^{-1} that's why RSA cryptosystem is secure, i.e, attacker can not derive the RSA private key from the public key and a given ciphertext. Here we could treat (h2; h_2^{-1}) as another RSA public/private key pair the same RSA modulus N. Therefore, assume that a malicious service provider Pj run the Chang-Lee SSO scheme with the same user Ui twice Pj will be able to recover Ui's credential Si by using extended Euclidean algorithm. That is to say, Pj can crack Si from equations x = $S_i^{h_2}$ mod N and x $'$ = $S_i^{h_2'}$ mod N.

Above attack mount by two or multiple malicious service providers. Finally, the attack will lead to a serious effect. after recovering a valid credential of a legal user Ui, a malicious Pj freely enjoy the services offered by other service providers. On the one hand, in Chang-Lee SSO scheme its specifies that SCPC is the trusted party [14]. So, it state that service providers are not trusted parties then they may be malicious. And also Wu-Hsu's scheme not protect the user's credential against a malicious service provider [9].

In addition, if all service providers are implicit to be trusted, to identify him Ui can simply encrypt his token Si by RSA public key of a Pi. Then, Pi can inconsequentially decrypt this ciphertext to get Ui's credential and confirm its validity by checking it's signature is issued by SCPC or not.

B. Impersonation Attack Without Credentials

The Impersonation attack may permit an outside attacker who didn't have any valid credential to act as a a legal user or even a non register user enjoy services generously.The attack is explained in detail as follows.

1) To pretend to be a legal user Ui with his identity IDi to access services from service provider Pj , an attacker E first sends service provider Pj request message m1.

2) after getting message m2 from Pj , E checks Pj 's signature and choose t as a random integer to calculate (ki j ,Ki j ,w).then , attacker E checks that $h(k_{ij}$ || w || $n_2)$ is divisible by e or not. If not, then E chooses another t.

3) $if\ h(k_{ij}$ || w || $n_2))$ is divisible by e, let $h(k_{ij}$ || w || $n_2)$= e·b for some integer b ∈ Z. then attacker E computes x by calculating x = SID_i^b , here SID_i = ID_i || h(ID_i).

4) now E can act like user Ui to complete the verification by sending m3 = (w, x, y) to service provider Pj , Pj notice that = $SID_i^{h(k_{ij}||w||n_2)}$ mod N = X^emod N. because we have: $SID_i^{h(k_{ij}||w||n_2)}$mod N =$SID_i^{e\cdot b}$ mod N = X^e mod N.

Here, attack can succeed for one random number t at rate about 1=e in a new session. accordingly, if e = 3 the above attack can succeed Even if e is as large as 65537(= 216+1), its not a issue of attacker that trying 65537 times to achieve a successful impersonation. Furthermore, in Chang-Lee scheme even timeout was introduced then also its not problem for attacker E as it can start new sessions by using the different identities.

Secondly, here we suppose that e is a small integer and attacker E knows the identity $ID_i$of one legal user's. This is explained below. in the system initialization phase Chang-Lee scheme (Section IV-A)

state that the trusted party SCPC set its RSA key pair (e; d),here RSA does not give any limitation on the length of public exponent e.

Furthermore, this happen because of the following two reasons:

(a) To make faster RSA signature verification, few security standards (e.g. PKCS #1 [18]), popular web sites ((e.g. Wikipedia [20])) and academic papers (e.g. [19]) suggest that value of e can be set as 3 or 65537;

(b) as Chang-Lee scheme is not efficient even for mobile devices in distributed networks, these devise have few resources for storage and computing so using small e can provide auxiliary computational advantage to them.

Finally, we would like to underscore that impersonation attacks without valid credentials seriously abuse the security of SSO schemes. Because it allows outsider attacker to be authenticated successfully without having valid token which is given by the trusted authority after registration

5. Discussions

In chang and lee given security system, they shown that how their SSO system is stronger in terms of security mechanism where those impersonation attack offered in earlier pattern mean that sso design was not so powerful.Hence ,why all of their results not sufficient to ensure the security of that system? What is security mistake in that design? And what we can find out from these attack to secure same kind of situation occurring once more in next propose sso system? So all that issues we talk in this segment.

In [14], the plan of chang lee sso system has been studied in three various ways:

1. The BAN logic [21] was used to show their accuracy of chang lee system.

2. Informal security point were given to express that their system defend some attacks, counting impersonation attacks.

3. A formal defense proof was set to prove that their system is a protected authenticated key exchange (AKE) protocol [22]

However, these security mechanism analysis and evidence are still not sufficient to assure the full protection of chang lee scheme, as discussed above. Firstly, in 1990s it has been identified that though BAN logic has been revealed useful to recognized some attacks, it may grant protocols that are really unsafe in practice because of some practical flaw in the logic [23]. Additionally, in [14] the authors did not offer details to illustrate how BAN logic can used to confirm that their system assure common authentication.

In fact, at last of section V-A [14], we can show that U_i and P_i can verify each other by using protocol.

An attacker re-uses a preceding nonce n_2 to fake message m_3 or choose a random credential s_i to calculate SID_i by $SID_i = S_i^e$ mod N. One more necessity of a secure AKE protocol is that protocol must secure common verification.

From above planning, the use of credential proof $x = S_i^{h_2}$mod N leading to two attacks in opposed to chang lee

sso system. More importantly, $x = S_i^{h_2} \bmod N$ is a proof that user U_i known credential S_i.

but , this is not a secure proof for service provider P can recover S_i and an outer attacker may be able to get legitimate without a credential. Based on this examination, a natural enhancement on Chang-Lee system is to swap non-interactive verification x by a accurate but interactive zero knowledge (ZK) proof [15] that shows the proves information of secret $S_i = SID_i^d \bmod N$ lacking illuminating any additional information about credential i. In detail, using verifiably encrypted signature showing in [25] a user Ui can encrypt other user credential Si with public key of trusted party and convinces a service provider Pj that ciphertext does contain Si with respect to Ui's identity IDi.

Finally, we comment that our study above shows that Chang-Lee SSO design fails to gain secure authentication, without disturbing its security for achieving user session key privacy.

6. Attacks on Hsu-Chuang Scheme

Here , we discuss the difference between Hsu-Chuang scheme [11] Chang-Lee scheme [14] and discuss why our impersonation attacks also pertain to Hsu-Chuang scheme. In a summary, it different from Chang-Lee scheme in the below three aspects.

Firstly, in Hsu-Chuang scheme a user Ui 's credential Si is a raw RSA signature signed by the SCPC, i.e., Si = $ID_i^d \bmod N$, here IDi is Ui's identity.

Secondly, service provider Pj authenticate itself by sending a signature $u = g_j^{h(Z||T_1||\, id_j)\cdot d_j} \bmod N_j$, where Z is the Diffi-Hellaman (DH) key material generated by Pj , current timestamp T1, and IDj is Pj 's identity.

Finally, user Ui issues and sends a proof $X = S_i^{h(k_{ij}\,||\,Z\,||\,w\,||\,T_2)} mod\ N$ to Pj ,x is validated by checking if $ID_i^{h(k_{ij}\,||\,Z\,||\,w\,||\,T_2)} = X^e \bmod N$ [14].

According to the above discussions , Hsu-Chuang scheme is still not secure even with such a improvement. The reason is that this two attacks against Chang-Lee scheme apply to Hsu-Chuang scheme directly. This gives the conclusion that Hsu-Chuang scheme also not able to satisfy both of

Privacy of credential and soundness of authentication

7. Conclusion

In this paper, we demonstrated two attacks on Chang and Lee's single sign-on (SSO) scheme [14].The first attack in which credential are recover by the malicious service provider and act as the legal user and access the services and resources from the service provider , hence their scheme can not protect the privacy of a user's credential.

The second attack in which the nonexistent user can act like the legal user and there is chance that this nonexistent user can freely access the services and resources provided by the service provider.

We also discussed why their well-organized security mechanism are not secure enough to

guarantee the security of their SSO scheme. And also see that , this attack is also possible on

Hsu and Chuang's scheme [11].

8. 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," CryptologyePrint 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. [18]. Elgamal Encryption Standard, NIST Std. FIPS PUB 197, 2001.