Improved Security Analysis of A Single Sign on Mechanism for Distributed Computer Networks

Avadhut Lakule[1], Adnan Sayed[2], Chaitali Shinde[3], Priya Indore[4]
SIT
Lonavala, Maharashtra, India
avdhutlakule[1],sab.adnan91[2]chitrashinde291[3],indorepriya93[4]@gmail.com

***Abstract*-Distributed system & network have been adopted by telecommunication remote education, business, armies & goverments.Amostly used technique for distributed system & network is the single sign on which enables authenticated user with a single crenditial to be authenticated by multiple service. Provided in distributed network.However most existing single singn on mechanism have been formally proved to satisfy crendential privacy and soundness of credential based authentication to overcome this drawback. We formalize the security model of single sign on mechanism with authenticated key exchange. We identify all the flaws in the Chang-lee, Hsu-Chang system to explain why attacks are possible against their single sign on scheme where these system are fail to fulfill the crendeital privacy and soundness of authentication moreover by implementing and efficient verifiable encryption of RSA signatures proposed by Athensis. We promote the formal study of soundness of authentication as an open problem**

Index Terms—Security analysis for Single sign-on, Distributed systems and networks, Soundness, Authentication, Information security.

I. INTRODUCTION

With the widespread use of distributed computer network, it has become common to allow users to access multiple network services offered by distributed service provider. Consequently user authentication has been strictly and widely used in distributed network to identify a legal user who requires accessing network services. To avoid unauthenticated access, user usually needs to authenticate service provider to access that server. After mutual authentication, a session key may be negotiated to keep the security and confidentiality of the data exchanged between a user and service provider. Moreover with wide usage of network services a user may need to maintain more and more id/password pairs for accessing multiple distributed service provider, which increase a burden on users and service providers as well as the communication overhead of computer network. Single sig on provide good mechanism or solution to his problem as it permits a user with a single crendital to access multiple service providers. The main 3 important basic requirement for SSO schemes, namely completeness, soundness and crendital privacy, so we introduce the formal study of the soundness of authentication as one open problem. To overcome this problem first we checked and did survey of all the single sign on security mechanism for distributed network and analysis the all the paper of written in SSO scheme.to overcome the drawback of existing network service and improve the proposed system we did research on Chang-Lee system, WU-Hsu system and tried to improving the proposed system.

II. RELATED WORK

In 2012, Chang and Lee proposed an improved efficient remote user identification scheme for mobile device users, the scheme employs single sign-on technique, supports session key establishment, and preserves user anonymity. However, the scheme neither provides credential privacy nor soundness. In this section, We briefly reviews the Chang-Lee scheme and its drawbacks.

A. Review of the Scheme

Chang-Lee's *SSO* scheme consists of three phases: system Initialization , registration, and user identification. The details are as follows.

1) System Initialization Phase: The trusted authority *TCP* determines the RSA key pair (*e*, *d*) and a generator *g*, and publishes public parameters.

2) *Registration Phase:* In this phase, the trusted authority signs an RSA signature $Si = (IDi||h(IDi))d \bmod N$ to user *Ui* as the credential. For each service provider *Pj* , he needs to maintain his own RSA public parameters (*IDj, ej,Nj*) and Private parameter *dj* similar as *TCP*.

3) *User Identification Phase:* In this phase, the session key is $Kij = h(IDi||kij)$, where *kij* is the plain Diffie-Hellman session key. For identifying service providers, an RSA signature scheme has been used; for user authentication, the user need to provide a proof
$z = Sh(Kij\ ||k2||n2)$

i mod *N* of credential *Si*, where *k*2 is user's session key material and *n*2 is a random nonce selected by the user. For the purpose of anonymity, the random nonce *n*3 and user identity which used for proof checking has been encrypted via symmetric key encryption scheme with session key *Kij* (treated as encryption key). The user can pass authentication if *ze* mod *N* = *SIDh*(*Kij* ||*k*2||*n*2) *i* mod *N* dose hold, and the user believes that they are share the same session key if the hashed *n*3 has been received.

I. TABLE

NOTATION USED IN THE SCHEME

TCP	The trusted credential provider
P_j	A service provider
U_i	A User
SID_j	The unique identity of P_j
Id_i	The Unique identity of U_j
C_i	The credential of U_i
x	The long term private key of TCP
y	The public key of TCP
$E_k(M)$	**Symmetric** Encryption of message M using key k
$D_k(C)$	**Symmetric** decryption of message C using key k
h(.)	**A secure hash function**

B. Review of Attacks

Two high risky attacks are identified in on Chang-Lee scheme. The former allows a malicious *Pj* to recover user credential; the latter enables an adversary passing user authentication without a valid credential. They are briefly reviewed below.

1) Credential Recovering Attack: A user *Ui* can pass authentication if he provides the valid proof *z* of knowledge *Ci*. To simplify the discussion, we use *h*2 to denote *h*(*Kij* ||*k*2||*n*2). So proof *z* = *Sh*2 *i* . It is easy to see that for different proofs in different session, the same credential *Si* has been encrypted multiple times with different *h*2 but the same modulo *N*. Thus, if a malicious *Pj* has been accessed twice with the same user *Ui*, then *Pj* is able to recover *Ui*'s credential *Si* by using extended Euclidean algorithm. Let us suppose that (*z*_, *z*__) and (*h*_2, *h*__ 2), the proofs and hash values in two different sessions, satisfy *gcd*(*h*_2, *h*__ 2) = 1. Then we can find two integers *a* and *b* such that *a* · *h*_2 + *b* · *h*__ 2 = 1
(in Z) due to the extended Euclidean algorithm. Finally, the *Pj* can recover user credential by computing *z*_*a* · *z*__*b* mod *N* = *Sh*_2·*a*+*h*__ 2 ·*b i* mod *N* = *Si*. The success rate of this attack is about 60% .

2) Impersonation Attack without Credentials: A small RSA public key *e* has been assumed in this attack, where the "small"requires the binary length of *e* is much less than the output length of hash function *h*. In the conversation, if the *h*2 is divisible by*e*, then the adversary computes an integer *b* such that *h*2 =*e* · *b*, and calculates proof *z* by *z* = *SIDbi* , where *SIDi* =*IDi*||*h*(*IDi*). The verification holds as *SIDh*2 *i* mod *N* =*SIDb*· *i* mod *N* = *ze* mod *N*. Thus, the adversary can pass user authentication without a valid credential. The success rate of the attack is about 1*/e* . Chang and Lee provided a well-organized securityanalysis to show that their SSO scheme is secure. However, the two impersonation attacks presented in the previous section mean that their SSO scheme is actually not secure. So, why is their analysis not enough to guarantee the security of their scheme?What is the security flaw in their scheme leading to the above attacks? And what could we learn from these attacks to prevent similar situations in the future design of SSO schemes?
These are the topics of this section.
The security of the Chang–Lee SSO scheme has been analyzed in three different ways: 1) BAN logic was used to show the correctness of the Chang–Lee schemes;
2) informal security arguments were given to demonstrate that their scheme can resist some attacks, including impersonation attacks; and 3)a formal security proof was given to prove that their scheme is asecure authenticated key exchange (AKE) protocol . However,these security analyses and proofs still do not guarantee thefull security of the Chang–Lee scheme and there are a numberof reasons for this. First, as early as the 1990s, it was known that although BAN logic had been shown useful to identify some attacks, it could approve protocols which are actually unsound in practice because of some technical weaknesses in the Ban logic.
Moreover, The authors did not give details to show how the BAN logic can be used to prove that their scheme guarantees mutual authentication. In fact, at the end of Section V-A of Chang and Lee, the authors claimed to be able to: "prove that Ui and Pj 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 with stand impersonation attacks by considering two scenarios, for example, an attacker re-uses previous
nonce n2 to forge message m3 or selects random credential Si to compute SID_i by $SID_i=S^e_i$ mod N However, such informal arguments neither strongly confirm their scheme's security against these two concrete attacks nor exclude the existence of other scenarios of impersonation attacks, such as those presented in previous sections. Finally, their formal proof about AKE only focuses on the session key security, i.e., an attacker with all reasonable resources is not able to know the session key established between the two parties under the computationalDH (CDH) assumption , and not the security of mutual authentication. According to the

definitions given by Bellare and Rogaway , one fundamental requirement of a secure AKE protocol is that there be a secure mutual authentication
in the first place. From the above, we can see that it is the use of credential
Proof $x=S^{h2}_{i}$ mod N which leads to the above two attacks against the Chang–Lee SSO scheme.

III. PROPOSED SYSTEM

To overcome the flaws in the Chang-Lee scheme, We now propose an improvement by employing an RSA-based verifiable encryption of signatures (RSA-VES), which is an efficient primitive introduced for realizing fair exchange of RSA signatures. VES comprises three parties: a trusted party and two users, say Alice and Bob. The basic idea of VES is
that Alice who has a key pair of signature scheme signs a given message and encrypts the resulting signature under the trusted party's public key, and uses a no interactive zero-knowledge (NZK) proof to convince Bob that she has signed the message and the trusted party can recover the signature from the cipher text. After validating the proof, Bob can send his signature for the same message to Alice. For the purpose of fair exchange, Alice should send her signature in plaintext back to Bob after accepting Bob's signature. If she refuses to do so, however, Bob can get her signature from the trusted party by providing Alice's encrypted signature and his own signature, so that the trusted party can recover Alice's signature and sends it to Bob, meanwhile, forwards Bob's signature to Alice. Thus, fair exchange is achieved.

RSA-VES Algorithm:

1) Each user generates a public/private key pair by:
2) Selecting two large primes at random - p, q
3) Computing their system modulus N=p.q
   - note ø(N)=(p-1)(q-1)
4) Selecting at random the encryption key e
   - where 1<e<ø(N), gcd(e,ø(N))=1
5) Solve following equation to find decryption key d
   - e.d=1 mod ø(N) and 0≤d≤N
6) Publish their public encryption key: KU={e,N}
7) Keto encrypt a message M the sender:
8) Obtains **public key** of recipient KU={e,N}
9) Computes: $C=M^e$ mod N, where 0≤M<N
10) To decrypt the ciphertext C the owner:
11) Uses their private key KR={d,p,q}
12) Computes: $M=C^d$ mod N
13) Ep secret private decryption key: KR={d,p,q}

In this system there are three phases

A. *Initialization phase*

SCPC selects two large safe prime number, then SCPC set its RAS public or private key there
SCPC produce some public key and some secret key

B Registration phase

In this phase upon receiving register request SCPC gives fix length unique identity and issue credential. Each service provider with unique identity should maintain a pair of signing/verifying keys for a secure signature scheme. This signatures with public key gives outs 1 or 0 to indicating if the signature is valid or invalid.

C. Authentication Phase

In this phase RSA-VES is employed to authenticate a user, while a normal signature is used for service provider authentication.
1) User sends the service request with nonce to service provider.

2) Upon receiving request service provider calculate its session key material then issue a signature key and then sends a message to user where another nonce is selected by service
provider

3) Upon receiving the message the user terminates the conversation if session key is invalid other user accept service provider is valid. For user authentication user first encrypts his or her credentials then it gives some NIZK proof for user authentication, In fact it is a proof part of RSA-VES.
Then using session key user gat n cipher text and sends a message to service provider

4) To verify user and service provider calculates session key and then use this session key to decrypt cipher text and recover ID if the session key is valid then, Service provider aborts conversation. Otherwise service provider accept user interface and believes that they share same session key

5) After user receive valid Id, then user believes that they have shared same session key otherwise user terminates the conversation

D. Security Analysis

We now analyze the security of the improved SSO scheme by focusing on the security of the user authentication part, especially soundness and credential privacy due to two reasons. On the one hand, the unforgeability of the credential is guaranteed by the unforgeability of RSA signatures, and the security of service provider authentication is ensured by the unforgeability of the secure signature scheme chosen by each service provider. On the

other hand, other security properties (e.g., user anonymity and session key privacy) are preserved, since these properties have been formally proved and the corresponding parts of the Chang–Lee scheme are kept unchanged. Soundness requires that without holding valid credential corresponding to a target user, an attacker, who could be a collusion of users and service providers, has at most a negligible probability of generating proof and going through user authentication by impersonating user . The soundness of
the above improved SSO scheme relies on the soundness of the NIZK proof, which also guarantees the soundness of RSA-VES, defined as the second property of Definition 1 in Namely, if the user authentication part is not sound, i.e., an attacker can present valid proof without holding the corresponding credential in non-negligible probability, then this implies the NIZK proof of proving equality of two discrete logarithms in a group of unknown order is not sound, contradictory to the analysis. Credential privacy or credential irrecoverableness requires that there be a negligible probability of an attacker recovering a valid credential from the interactions with a user. Again this property can be deduced from the signature hiding property of RSA-VES, defined as the third property of Definition 1. Signature hiding means that an attacker cannot extract a signature from VES without help from the user who encrypted the signature or the trusted authority who can decrypt a VES. So, if this improved SSO scheme fails to meet credential privacy, it implies that Ateniese's RSA-VES fails to satisfy signature hiding. In fact, soundness and signature hiding are the two core security properties to guarantee the fairness of digital signature exchange using VES.
More rigorous security proofs are interesting topics for further
study by considering formal definitions first.

IV. CONCLUSION

In this paper, we demonstrated two effective impersonation attacks on Chang and Lee's single sign-on (SSO) scheme. The first attack shows that their scheme cannot protect the privacy of a user's credential, and thus, a malicious service provider can impersonate a legal user in order to enjoy the resources and services from other service providers. The secondattack violates the soundness of authentication by giving anoutside attacker without credential the chance to impersonateeven a non-existent user and then freely access resources andservices provided by service providers. We also discussed whytheir well-organized security arguments are not strong enoughto guarantee the security of their SSO scheme. In addition,we explained why Hsu and Chuang's scheme is also vulnerable to these attacks. Furthermore, by employing an efficient verifiable encryption of RSA signatures introduced by Ateniese, we proposed an improved Chang–Lee scheme to achieve soundness and credential privacy. As future work, it is interesting to formally define authentication soundness and construct efficient and provably secure single sign-on schemes.
Based on the draft of this work, a preliminary formal model addressing the soundness of SSO has been proposed in G.Wang. Further research is necessary to investigate the maturity of this model and study how the security of the improved SSO scheme proposed in this paper can be formally proven

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] L. Lamport, "Password authentication with insecure communication," Commun. ACM, vol. 24, no. 11, pp. 770–772, Nov. 1981.

[4] 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.

[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] 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.

[7] M. Cheminod, A. Pironti, and R. Sisto, "Formal vulnerability analysis of a security system for remote fieldbus access," IEEE Trans. Ind. Inf.,vol. 7, no. 1, pp. 30–40, Feb. 2011.

[8] 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.

[9] Y. Yang, S. Wang, F. Bao, J. Wang, and R. H. Deng, "New efficient user identification and key distribution scheme providing enhanced security," *Comput. Security*, vol. 23, no. 8, pp. 697–704, 2004.

[10] K. V. Mangipudi and R. S. Katti, "A secure identification and key agreement protocol with user anonymity (SIKA)," *Comput. Security*, vol. 25, no. 6, pp. 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*., vol. 179, no. 4, pp. 422–429, 2009.

[12] B.Wang and M. Ma, "A server independent authentication scheme for RFID systems," *IEEE Trans. Ind. Inf*., vol. 8, no. 3, pp. 689–696, Aug. 2012.

[13] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.

[14] C. Boyd and W. Mao, "On a limitation of BAN Logic," in *Proc. Of EUROCRYPT*, 1994, pp. 240–247.

[15] J. Camenisch and M. Michels, "Confirmer signature schemes secure against adaptive adversaries," in *Proc. EUROCRYPT*, 2000, pp. 243–258.

[16] 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

[17] 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.