International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 7 Issue 1 –MARCH 2014.

A SECURE SINGLE SIGN ON MECHANISM FOR DISTRIBUTED COMPUTER NETWORKS

V. Priya, M.E [1],A. Rajeswari [2], J. Nithya [3], P. Shrivithya [4]

Department of Information Technology,

K S Rangasamy College of Technology (Autonomous)

***Abstract*—Single sign-up (SSU) 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. Recently, Chang and Lee proposed a new SSU scheme and claimed its security by providing well-organized security arguments. In this paper, however, we describe that their scheme is actually insecure as it fail to meet credential privacy and soundness of authentication. Specifically, we represent two impersonation severities. The first attack allows a malicious service provider, who has easily communicated with a legal user twice, to resume the user's credential and then to impersonate the user to deal with the resources and services offered by other service providers. In next attack, an outsider without any credential may be able to enjoy network services freely by impersonating any legal user or a nonexistent user. Here, we identify the flaws in their security arguments to explain why attacks are possible against their SSU scheme. Our attacks also apply to another SSU scheme proposed by Hsu and Chuang, which has inspired the design of the Chang–Lee scheme. Moreover, by adapting an efficient verifiable encryption of RSA signatures proposed by Ateniese, we propose to improvement by repairing the Chang–Lee scheme. We project the formal study of the soundness of authentication as an open problem.**

***Index Terms*—Distributed computer networks, information security, security analysis, single sign-up (SSU).**

1. INTRODUCTION

With the widespread use of distributed computer networks, it has become regular 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 interactions, users usually need to authenticate service providers. After one-to-one authentication, a session key may be negotiated to maintain the confidentiality of the data exchanged between a user and a service provider.In many scenarios, the anonymity of legal users must be protected. 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.

This proposed a user identification and key distribution scheme to maintain user anonymity in distributed computer networks. On the other side, 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 users, service providers as well as the communication of networks. To tackle this problem, the single sign-up (SSU) mechanism has been introduced so that, after getting a credential from a trusted party for a short period (say 1 day), each legal user's authenticated agent can use this single credential to complete authentication on behalf of the user and then access multiple service providers. Intuitively, an SSU scheme should meet at least three basic security requirements, i.e., remembrance, credential privacy, and soundness. Remembrance demands that, except the trusted party, even a collusion of users and service providers are not able

to forge a valid credential for a new user. Credential privacy which guarantees 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 unauthorised and unregistered user without a credential should not be able to ac-cess the services offered by service providers. Formal security definitions of remembrance and credential privacy were given in.

A familiar concept, called the generalized digital certificate (GDC), was proposed in to provide user authentication and key agreement in wireless networks, in which a user, who holds a digital signature of his/her GDC issued by an authority, can authenticate him/herself to a verifier by proving the knowledge of the signature without revealing it.

A careful study of SSU mechanism. First, they argued that the Hsu–Chuang user identification scheme, actually an SSU scheme, has two weaknesses: 1) an outsider can forge a valid credential by mounting a credential forging attack since the Hsu–Chang scheme employed naive RSA signature without using any hash function to issue a credential for any random identity selected, 2) the Hsu–Chuang scheme requires clock synchronization since it uses a time stamp. Then, Chang and Lee presented an interesting RSA-based SSU scheme, which does not rely on clock synchronization by using a nonce instead of a time stamp. Their scheme is suitable for mobile devices due to its high efficiency in computation and communication. At last, they presented a well- organized security analysis to show that their SSU scheme supports secure mutual verification, session key agreement, and user anonymity secure.

In this paper, we show that the Chang–Lee scheme is actually insecure by presenting two impersonation type attacks, i.e., credential recovering attack and impersonation attack without credentials. In the first attacking, a malicious service provider who has communicated with a legal user twice can success-fully resume the user's credential. Then, service provider can impersonate the user to access resources and services provided by other service providers. The other 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. These two attacks imply that the Chang–Lee SSU scheme fails to meet credential privacy and soundness, which are essential requirements for SSU schemes and authentication protocols.

We also identify the flaws in their security arguments in order to explain why it is possible to mount our attacks against their scheme. Similar attacks can also be applied to the Hsu–Chuang scheme, on which the Chang–Lee scheme is based. Finally, to avoid these two impersonation attacks, we propose an improved SSU scheme to enhance the user authentication phase of the Chang -Lee scheme. To this end, we employ the efficient RSA-based verifiable encryption of signatures (VES) proposed by Ateniese to verifiably and securely encrypt a user's credential. In fact, Ateniese's VES was originally introduced to realize fair exchange.

TABLE I

SCPC	Smart Card Producing Center
U_i, P_j	User and Service provider, respectively
ID_i, ID_j	The unique identity of U_i and P_j, respectively
e_X, d_X	The public/private RSA key pair of identity X
S_i	The credential of U_i created by SCPC
S_x	The long term private key of SCPC
S_y	The public key of SCPC
$E_K(M)$	A symmetric key encryption of plaintext M using a key K
$D_K(C)$	A symmetric key decryption of ciphertext C using a key K
$\sigma_j(SK_j, M)$	The signature σ_j on M signed by P_j with signing key SK_j
$Ver(PK_j, M, \sigma_j)$	Verifying signature σ_j on M with public key PK_j
$h(\cdot)$	A given one way hash function
$\|\|$	The operation of concatenation

2. Our Contributions

In this paper, we propose a secure single sign-on mechanism to allow mobile users to use the unitary token to access service providers. In a real-life application, the mobile user can use the mobile device, e.g., a cell phone, with the unitary token to access multiservice, such as download music,

receive/reply electronic mails, order goods, or process online payment etc., from different service providers in distributed computer networks. Our scheme is based on one-way hash functions and random nonces to solve the weaknesses described above and to decrease the overhead of the system.

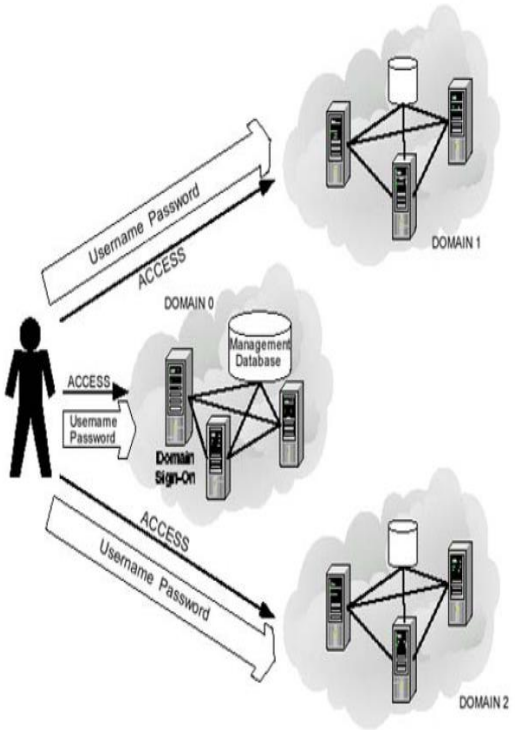

Fig 1 Overall system architecture

2.1 Review Of The Chang–Lee Scheme

Chang and Lee's single sign-up scheme [19] is a remote user authentication scheme, supporting session key establishment and user anonymity. In their scheme, RSA cryptosystems are used to initialize a trusted authority, called an SCPC (smart card producing centre), and service providers, denoted as 's. The Diffi e–Hellman key exchange technique is employed to establish session keys in this method. In the Chang–Lee scheme, each user applies a credential from the trusted authority called SCPC, who signs an RSA signature for the user's hashed identity. Then, uses a kind of knowledge proof to show that he/she is in possession of the valid credential without revealing his/her identity to eaves droppers. But, 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. On the other side, each maintains its own RSA key pair for doing server authentication. The Chang–Lee's SSU scheme consists of three phases: system initialization, registration, and user identification. Table I explains notations, and the details of Chang–Lee scheme are reviewed as follows.

B. Registration Phase

In this phase, each use U r chooses a unique identity with a fixed bit-length and sends it to SCPC,the SCPC will return the credential, where denotes a concatenation of two binary strings and is a hash function of collision-resistant cryptographic one-way. Here, both and must be transferred via a secure channel. At the same time, each service provider with identity should maintain its own RSA public parameters and private key as does by SCPC.

C. User Identification Phase

To access the resources of service provider, user ought to go through the authentication protocol specified in Fig. 1.the random integers chosen. A symmetric key encryption scheme is used to protect the confidentiality of user's identity. We highlight this phase as follows. It receives a service request message from user service provider generates and returns user message which is made up primarily by its RSA signature on

•. Once this signature is validated, it means that user has authenticated service provider successfully is the temporal Diffie–Hellman (DH) key exchange material..

• After that, user correspondingly generates his/her temporal DH key exchange material and issues proof is the derived session key and is the raw key obtained by using the DH key exchange technique.

$$S_i = x^a \cdot x'^b \bmod N.$$

Equation (1) is justified by the following equalities:

$$\begin{aligned} x^a \cdot x'^b \bmod N &= \left(S_i^{h_2}\right)^a \cdot \left(S_i^{h_2'}\right)^b \bmod N \\ &= S_i^{a \cdot h_2 + b \cdot h_2'} \bmod N \\ &= S_i^1 \bmod N \\ &= S_i. \end{aligned} \tag{1}$$

• Proof $\tilde{x} = S_i^{h(K_{ij} \| w \| n_2)}$ is used convince Pj that Ui does hold valid credenttail Si without revealing the value of Si.after receiving message M3 Service provider Pj can confirm x's validity by checking if this quality holds, it means that user Ui has been authenticated successfully by service Pj provider .

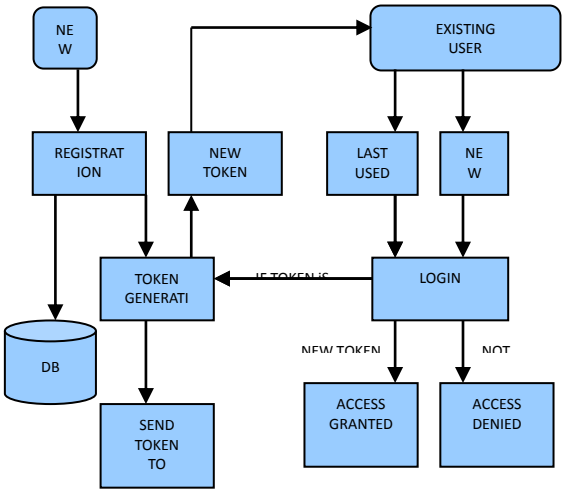

Fig 2 Dataflow Diagram of Chang–Lee Scheme

3. Attacks Against the Chang–Lee Scheme

As can be seen from the previous section, it seems that the Chang–Lee SSU scheme achieves secure mutual authentication, since server authentication is

done by using traditional RSA signature issued by service provider . Without valid credential it looks impossible for an attacker to impersonate a legal user by representing the user authentication procedure.

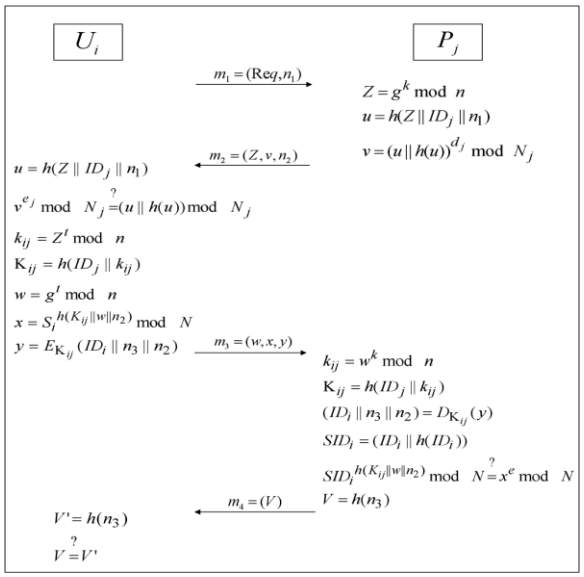

Fig 3. User identification phase of the Chang–Lee scheme.

It can be seen from the following, however, that the Chang–Lee scheme is actually not a secure SSU scheme because there are two potential effective and concrete impersonation attacks. The first attack, the "credential recovering attack" compromises the credential privacy in the Chang–Lee scheme as a malicious service provider is able to recover the credential of a legal user. The other attack, an "impersonation attack without credentials," tells that how an outside attacker may be able to freely make use of resources.

We now describe our attacks together with the assumptions required, justify why these assumptions are reasonable, and finally discuss why the security analysis and proofs given in are not enough to guarantee the security of the Chang–Lee SSU scheme.

A. Credential Recovering Attack

Intuitively, the Chang–Lee SSU scheme seems to satisfy the requirement of credential privacy since receiving credential denotes does not allow service provider to recover user x's credential by computing In fact, the difficulty of calculating from the given is the exact rationale why the RSA cryptosystem is

secure, i.e., it should be intractable for an attacker to derive the RSA private key from the public key.). This is because here we could treat as an- other RSA public/private key pair w.r.t the same RSA modulus Moreover , directly recovering from also looks impossible as this seems equivalent to decrypt the RSA cipher text w.r.t. the (ephemeral) public key .

There is a pitfall in the production of proof as here the same credential is encrypted multiple times under different (ephemeral) public keys w.r.t. the same RSA modulus. Consequently, under the assumption that malicious service provider has run the Chang–Lee SSU scheme with the same user twice, will be able to recover x's credential with high probability by using the extended Euclidean algorithm. It can solve from two equations. The details of the attack, which share some features of common-modulus attacks against RSA.are given as follows.1) After successfully running the Chang–Lee SSU scheme twice with the same user, malicious service provider stores all messages exchanged in these two instances, denoted as for the first instance, and for the second instance.

There are a number of comments to be made regarding the above attacks. First, it has a success rate of about 60% due for two reasons: 1) for two randomly selected integers and , the probability that holds and 2) as the outputs of hash function , and can be re- graded as random numbers. This means that after executing the Chang–Lee SSU scheme with the same user twice, malicious will be able to recover Pj's credential with a probability of about 0.6. Consequently, it is easy to see that after running the scheme with a couple of times, can recover almost certainly. Second, it is not hard to see that the above attack could be mounted by two or multiple malicious service providers who collude together once they put the values of together. Finally, the attack will lead to serious consequences since after recovering the valid credential of a legal user, malicious can impersonate this user by running the Chang–Lee SSU scheme in the same way as a legal user does to freely make use of the services offered by other service providers.

How could service provider be malicious and then mount the above attack?On the one hand, the Chang–Lee SSU scheme specifies that is the trusted party. So, this implies that service providers are not trusted par- ties and that they could be malicious. By agreeing with Yang et al. [10], when they said that "the Wu–Hsu's modified version cold not protect the user's token against a malicious service provider...", the work in also implicitly agrees that there is the potential for attacks from malicious service providers against SSU schemes. Moreover, if all service providers are assumed to be trusted, to identify him/her user can simply encrypt his/her credential under the RSA public key of ser- vice provider . Then, can easily decrypt this cipher text to get's credential and verify its validity by checking if it is a correct signature issued by them. In fact, such a straightforward scheme with strong assumption is much simpler, more efficient and has better security, at least against this type of attack.

On the other hand, according to the security models malicious service providers could be attackers in SSU schemes. In fact, this is a traditional as well as prudential way to deal with trustworthiness, since we cannot simply assume that beside the trusted authority , all service providers are also trusted. The basic reason is that assuming the existence of a trusted party is the strongest supposition in cryptography but it is usually very costly to develop and maintain.the collusion impersonation attacks as a way to capture the scenarios in which malicious service providers may recover a user's credential and then impersonate the user to login to other service providers. It is easy to see that the above credential recovery attack is simply a special case of collusion impersonation attack where a single malicious service provider can recover a user's credential.

B. Impersonation Attack without Credentials

We now study the soundness of the Chang–Lee SSU scheme, which seems to satisfy this security requirements as well. The main reason is that to get valid proof satisfying for a random hash output, there seems no other way but to compute, an attacker should not be able to log in to any service provider if it does not have the knowledge of either

RSA private key or user's credential. Again, however, such a plausible discussion simply explains the rationale of the Chang-Lee SSU scheme but cannot guarantee its security w.r.t. the soundness. This is also the essential reason why the current focus of research in information security is on formal proofs which rigorously show the security of cryptosystems.

Indeed, no one can formally prove that without knowing either user's RSA private key or user's credential , it is unfeasible to compute a proof that passes through authentication, as an outside attacker is able to get a shortcut if the 's RSA public key is a small integer so that 's bi- nary length is less than the output length of hash function. The attack is explained in detail as follows.

1) To impersonate legal user with identity for ac-cessing service provider an attacker first sends request message normally.

2) Upon receiving message from, thenchecks's signature and chooses a random integer to computation. . Before moving on to the next step, attacker needs to check whether it is divisible by this variable. If not, has to choose another or start a new session to satisfy this condition.

3) As it is divisible by, let for some integer.

4) Finally, can impersonate user to pass the authentication by sending.it must be emphasized that impersonation attacks without valid credentials seriously violate the security of SSU schemes as it allows attackers to be successfully authenticated without first obtaining a valid credential from the trusted authority after registration. In other words, it means that in an SSU scheme suffering these attacks there are alternatives which enable passing through authentication without credentials.

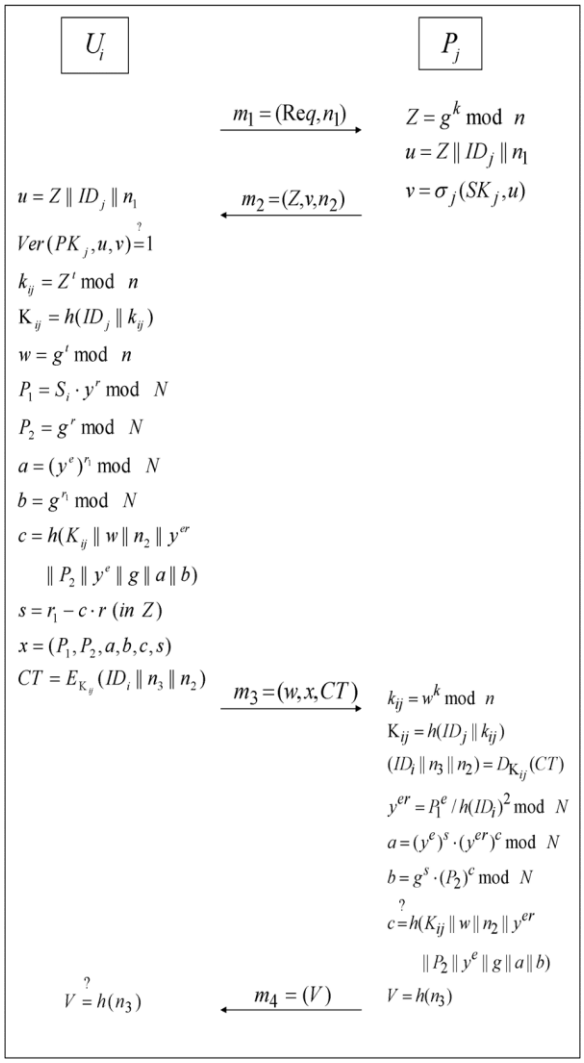

Fig 4. Impersonation of attack

4. Security Analysis

We now analyze the security of the improved SSU scheme by focusing on the security of the user authentication part, that is soundness and credential privacy due to two reasons. On the one hand, the remembrance of the credential is guaranteed by the remembrance of RSA signatures, and also the security of service provider authentication is ensured by the remembrance 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 SSU scheme relies on the soundness of the NIZK proof, which also guarantees the soundness of RSA-VES, defined as the second property. 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 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 SSU scheme fails to meet credential privacy, it implies that Ateniese's RSA-VES fails to satisfy signature hiding, which is contrary to the analysis. In fact, soundness and signature hiding are the two core security properties to guarantee the fairness of digital signature exchange using VES.

5. CONCLUSION

In this paper, we demonstrated two effective impersonation attacks on Chang and Lee's single sign-up (SSU) scheme. Thus, the first attack shows that their scheme cannot protect the privacy of a our credential, and a malicious service provider can impersonate a legal user in order to enjoy the resources and services from other service providers. The next attack violates the soundness of authentication by giving an outside attacker without credential the chance to impersonate even a non-existent user and then freely access resources and services provided by service providers. We also discussed why their well-designed security arguments are not strong enough to guarantee the security of their SSU scheme. In addition, we explained why Hsu and Chuang's scheme is also vulnerable to these attacks. By adapting an efficient verifiable encryption of RSA signatures introduced by Ateniese, we proposed an improved Chang–Lee scheme to achieve both securities. As future work, it is interesting to formally define authentication soundness and construct efficient and provably secure single sign-up schemes. Based on the draft of this work, a preliminary formal model addressing the soundness of SSU has been proposed. Further research is necessary to investigate the maturity of this model and study how the security of the improved SSU scheme of 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. 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. 302 IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 9, NO. 1, FEBRUARY 201

[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.