I.J. Information Technology and Computer Science, **2014, 07, 40-46**
Published Online June 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2014.07.06

Confidence Analysis of a Solo Sign-On Device for Distributed Computer Networks

Sumanth C M
Dept. of CSE, Canara Engineering College, Mangalore, India
Email: sumanthcm4@gmail.com

Adithyan B
Dept. of CSE, Canara Engineering College, Mangalore, India
Email: adithyan.it@gmail.com

Abstract— Solo 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. Recently, a SSO scheme proposed and claimed its security by providing well organized security arguments. But their scheme is actually insecure as it fails to meet credential privacy and soundness of authentication. Specifically, we present two impersonation attacks i.e., credential recovering attack and impersonation attack without credentials. So we propose a more authentication scheme that overcomes these attacks and flaws by make use of efficient verifiable encryption of RSA signatures. We promote the formal study of the soundness of authentication as one open problem.

Index Terms— Authentication, Distributed computer networks, Information security, Security analysis, Solo Sign-On

I. INTRODUCTION

Solo sign-on (SSO) is a property of access control, with this property a user logs in once and gains access to all systems without being prompted to log in again at each of them in a distributed computer network.

In distributed computer networks, it has become common to allow users to access various network services offered by distributed service providers [3]. Consequently, user authentication (also called user identification) [1], [2] 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 obtained to keep the confidentiality of the data exchanged between a user and a service provider [10]. In many scenarios, the anonymity of legal users must be protected as well [2], [8], [9]. However, big challenge is to design efficient and secure authentication protocols in the complex computer network environments [10].

The SSO mechanism [13] has been introduced so that, after obtaining a credential from a trusted authority for a short for a new user. Credential privacy guarantees that malicious service provider's 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. Unforgeability except the trusted authority, even a collusion of users and service providers are not able to make progress that valid credential should not 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.

We intend to design a secure key agreement protocol for distributed computer networks, which is expected to inherit all the good virtues of the previous schemes and some added security properties. Here we summarize all these requirements to evaluate our new scheme as follows.

User Anonymity: The scheme should preserve the user's identity, namely, a server could not tell a user's identity. Once the connection between the user and the server has been established, the probability of the server to guess the user's identity is $1/n$, where n is the number of ring members.

Security of Session Key: The scheme should preserve the security of session key, that is to say, when executing our improved protocol, except the correspondence patties nobody outside could acquire the session key.

Mutual Authentication: The scheme should assure that not only can the server verify the legal user, but the user can also verify the server. In authenticated protocols, mutual authentication is an important attribute, so our scheme should also be in favor of it perfectly.

Forward Secrecy and Backward Secrecy: The scheme should satisfy forward secrecy and backward secrecy, namely, if the session key generated in j period has been leaked, the attacker can't forge any session key generated before j period or after j period. Therefore, the scheme should defeat some attacks like replay attack and so on.

The remainder of this paper is organized as follows. Section III reviews existing system [12]. After that, we present two attacks against the Chang–Lee scheme in Section IV. Then, the improved SSO scheme using VES is given in Section V. Finally, Section VI gives the conclusion.

II. Literature Survey

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.

In 2000, Lee and Chang [2] proposed a user identification and key distribution scheme to maintain user anonymity in distributed computer networks. This user identification scheme is based on the security of the factoring problem and the one way hash function. Their scheme has the following advantages: (1) users can request services without revealing their identities to the public; (2) each user needs to maintain only one secret; (3) it is not required for service providers to record the password files for the users; (4) no master key updating is needed if a new service provider is added into the system. But this scheme is insecure against both impersonation attacks and identity disclosure attacks.

Later in 2004, Wu and Hsu [5] proposed scheme that overcomes drawbacks of Lee Chang scheme, that is not only effectively eliminates the security leaks of the Lee Chang scheme, but also reduces computational complexities and communication costs as compared with their scheme. The main objective of the Wu-Hsu scheme is to provide user identification and key exchange between parties at both ends of the communication, while preserving user anonymity from the public. We must point out that in scenarios such as a user requesting services from a service provider, anonymity of the service provider is not necessary since whom providing what service is a public knowledge. Participants involved in the Wu-Hsu scheme include a Smart Card Producing Centre (SCPC), users and service providers. The SCPC is responsible for setting up the system parameters and assigning a secret token to each user and each service provider. Based on the respective secret tokens, a user and a service provider can authenticate each other and exchange a common session key. But Wu and Hsu scheme has a serious weakness, by which the service provider can learn the secret token of the user who requests services from him.

Later Yang et al. [6] proposed a protocol that overcomes the weakness of Wu–Hsu's protocol and achieves user anonymity, user identification and key agreement. As mentioned by Yang et al., these three protocols (Lee–Chang, Wu–Hsu and Yang) have the following attractive features apart from achieving user anonymity: (1) each user is required to maintain only one secret irrespective of the number of servers he is accessing; (2) the server is not required to maintain a list of passwords; (3) the system is scalable as new servers can be added without requiring to update the master key. Unfortunately, Yang's scheme suffers from Denial-of-Service (DoS) attack.

In 2006, Mangipudi and Katti [8] proposed a Secure Identification and Key agreement protocol with user Anonymity (SIKA) that overcomes the limitations of Yang et al scheme while achieving security features like identification, authentication, key agreement and user anonymity. This scheme showed that their protocol is as efficient as the previously proposed protocols with a modest increase in communicational and computational cost. But it is insecure under identity disclosure attack.

In 2009, Hsu and Chuang [9] showed that the schemes of both Yang *et al.* and Mangipudi–Katti were insecure under identity disclosure attack and proposed an RSA-based user identification scheme to overcome this weakness, they proposed scheme can easily overcomes DoS attack demonstrated by Mangipudi and Katti by appending a digital signature to the service provider's message, outperforming the previously proposed schemes in terms of security, communication costs, and computational complexities. It, in fact, does not provide all of the security properties that they claimed and that Hsu–Chuang's scheme might be vulnerable to impersonation attacks since it employs an analogous RSA signature to generate secret tokens.

Recently, Chang and Lee [12] proposed A Secure Single Sign-On Mechanism for Distributed Computer Networks. The concept of single sign-on can allow legal users to use the unitary token to access different service providers in distributed computer networks. Recently, some user identification schemes have been proposed for distributed computer networks. Unfortunately, most existing schemes cannot preserve user anonymity when possible attacks occur. Also, the additional time-synchronized mechanisms they use may cause extensive overhead costs. To overcome these drawbacks, Chang and Lee propose a secure single sign-on mechanism that is efficient, secure, and suitable for mobile devices in distributed computer networks. But their scheme is actually insecure as it fails to meet credential privacy and soundness of authentication. Specifically, we present two impersonation attacks. The first attack allows a malicious service provider, who has successfully communicated with a legal user twice, to recover the user's credential and then to impersonate the user to access resources and services offered by other service providers. In another attack, an outsider without any credential may be able to enjoy network services freely by impersonating any legal user or a nonexistent user.

III. Existing System

The existing Chang–Lee scheme is a remote user authentication scheme, supporting session key establishment and user anonymity. In this scheme, RSA cryptosystems are used to initialize a trusted authority, called an SCPC (smart card producing center), and service providers. The Diffie–Hellman key exchange technique is employed to establish 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, U_i 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. On the other side, each service provider maintains its own RSA key pair for doing server authentication. The Chang–Lee's SSO scheme consists of three phases: system initialization, registration, and user identification. Table 1 explains notations, and the details of Chang–Lee scheme are reviewed as follows.

A. System Initialization Phase:

The trusted authority SCPC first selects two large safe primes *p and q* then sets *N=pq*. After that, SCPC determines its RSA key pair *(e,d)* such that *ed=1mod φ(N),* where *φ(N)=(p-1)(q-1).* SCPC chooses a generator g Є Z_n^*, where n is also a large prime number. Finally, SCPC publishes *(e, g, n, N)* keeps *d* as a secret, and erases *(p, q)* immediately once this phase has been completed.

Table 1. list of notations.

SCPC	Smart Card Producing Center
$U_{i,}$ P_j	User and Service provider respectively
I D_i, I D_j	Unique identity of U_i and P_j respectively
$e_{x.,}$ d_o	The public/private RSA key pair of identity X
S_i	The credential of U_i created by SCPC
Sx	The long term private key of SCPC
Sy	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 plaintext 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 (.)	A given one way hash function
||	The operation of concatenation

B. Registration Phase:

In this phase, each user U_i chooses a unique identity ID_j with a fixed bit-length and sends it to SCPC. After that, SCPC will return the credential S_i = (Id || $h(ID_i))^d$ mod N, where || denotes a concatenation of two binary strings and h(**.**) is a collision-resistant cryptographic one-way hash function. Here, both Id_i and S_i must be transferred via a secure channel. At the same time, each service provider P_j with identity ID_j should maintain its own RSA public parameters (e_j, N_j) and private key d_j as does by SCPC.

C. User Identification Phase:

To access the resources of service provider P_j, user U_i needs to go through the authentication protocol specified in Fig. 1. Here, k and t are random integers chosen by P_j and U_i respectively, n1, n2, and n3 are three random nonces and E (**.**) denotes a symmetric key encryption scheme which is used to protect the confidentiality of user U_i's identity ID_i.

1) Upon receiving a service request message m1 from user U_i, service provider P_j generates and returns user message m2 which is made up primarily by its RSA signature on (Z, IDj, and n1). Once this signature is validated, it means that user has authenticated service provider P_j successfully. Here, Z = (g^k mod n) is the temporal Diffie–Hellman (DH) key exchange material issued by P_j.
2) After that, user U_i correspondingly generates his/her temporal DH key exchange material w = (g^t mod n) and issues proof x= $S_i^{h(Kij \parallel w \parallel n2)}$, where K_{ij} = h(ID_i || k_{ij}) is the derived session key and K_{ij} = (Z^t mod n) = (w^k mod n) = (g^{kl} mod n) is the raw key obtained by using the DH key exchange technique.
3) Proof x= $S_i^{h(Kij \parallel w \parallel n2)}$ is used to convince P_j that does hold valid credential S_i without revealing the value of S_i. Namely, after receiving message m3 service provider P_j can confirm x's validity by checking,

   If (SID_i $^{h\ (Kij \parallel w \parallel n2)}$ mod N) = (x^e mod N),
   Where SID_i = (Id || h (ID_i)).

4) If this quality holds, it means that user U_i has been authenticated successfully by service provider P_j. It is nothing but that proof x is designed in a particular way so that except U_i and P_j, no one else can verify it as both U_i's identity ID_i and the newly established session key K_{ij} are used to produce. This aims to achieve user anonymity as no eavesdropper can learn the values of ID_i and $K_{ij.}$
5) Finally, message m4 (i.e. h (n3)) is employed to show that P_j has obtained message m3 correctly, which implies the success of mutual authentication and session key establishment.

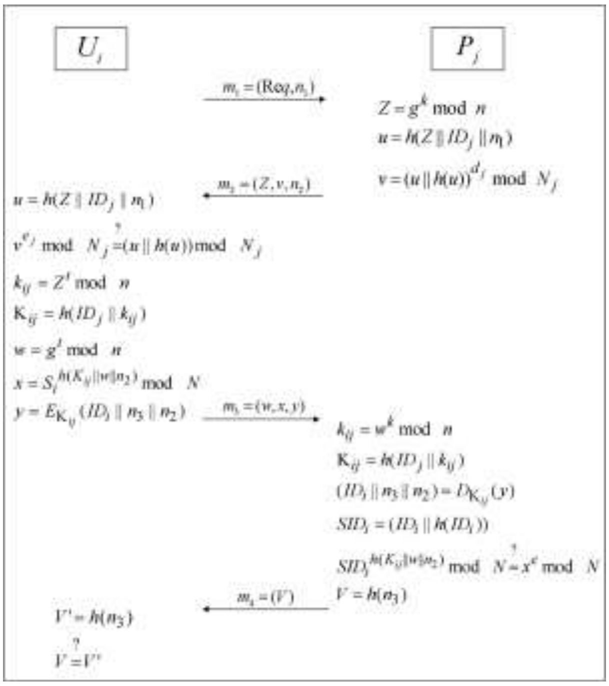
U_i
P_j
$m_1 = (Req, n_1)$
$Z = g^k \bmod n$
$u = h(Z \parallel ID_j \parallel n_1)$
$v = (u \parallel h(u))^{d_j} \bmod N_j$
$m_2 = (Z, v, n_2)$
$u = h(Z \parallel ID_j \parallel n_1)$
$v^{e_j} \bmod N_j \overset{?}{=} (u \parallel h(u)) \bmod N_j$
$k_{ij} = Z^t \bmod n$
$K_{ij} = h(ID_j \parallel k_{ij})$
$w = g^t \bmod n$
$x = S_i^{h(K_{ij} \parallel w \parallel n_2)} \bmod N$
$y = E_{K_{ij}}(ID_i \parallel n_3 \parallel n_2)$
$m_3 = (w, x, y)$
$k_{ij} = w^k \bmod n$
$K_{ij} = h(ID_j \parallel k_{ij})$
$(ID_i \parallel n_3 \parallel n_2) = D_{K_{ij}}(y)$
$SID_i = (ID_i \parallel h(ID_i))$
$SID_i^{h(K_{ij} \parallel w \parallel n_2)} \bmod N \overset{?}{=} x^e \bmod N$
$V = h(n_3)$
$m_4 = (V)$
$V' = h(n_3)$
$V \overset{?}{=} V'$

Fig. 1. Chang–Le's user identification phase

IV. Attacks against the Chang–Lee Scheme

As we seen from the previous section, it seems that the Chang–Lee SSO scheme achieves secure mutual authentication, since server authentication is done by using traditional RSA signature issued by service provider P_j. Without valid credential S_i it is impossible for an attacker to impersonate a legal user U_i by going through the user authentication procedure.

However, that the Chang–Lee scheme is actually not a secure SSO scheme because there are two potential effective and concrete impersonation attacks. The first attack is 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 is "impersonation attack without credentials," demonstrates how an outside attacker may be able to freely make use of resources and services offered by service providers, since the attacker can successfully impersonate a legal user without holding a valid credential and thus violates the requirement of soundness for an SSO scheme. In real life, these attacks may put both users and service providers at high risk.

A. Credential Recovering Attack:

Intuitively, the Chang–Lee SSO scheme seems to satisfy the requirement of credential privacy since receiving credential proof $x = (S_i^{h2} \bmod N)$, where h_2 denotes $h(K_{ij} \| w \| n_2)$ does not allow service provider P_j to recover user U_i's credential S_i by computing $S_i = (x^{h2\text{-}1} \bmod N)$, where h_2^{-1} refers to $(h_2^{-1} \bmod \varphi(N))$. In fact, the difficulty of calculating h_2^{-1} from the given (e, N, x, h_2) 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 (and a given cipher text). This is because here we could treat (h_2, h_2^{-1}) as another RSA public/private key pair with respect to the same RSA modulus. Moreover, directly recovering Si from $x = (S_i^{h2} \bmod N)$ also looks impossible as this seems equivalent to decrypt the RSA cipher text with respect to the public key h_2.

Nevertheless, there is a pitfall in the production of proof $x = (S_i^{h2} \bmod N)$ as here the same credential S_i is encrypted multiple times under different public keys h_2 w.r.t the same RSA modulus N. Consequently, under the assumption that malicious service provider P_j has run the Chang–Lee SSO scheme with the same user U_i twice, P_j will be able to recover U_i's credential S_i with high probability by using the extended Euclidean algorithm, P_j can solve S_i from two equations $(S_i^{h2} \bmod N)$ and $x` = (S_i^{h2`} \bmod N)$. The details of this attack, which share some features of common-modulus attacks against RSA, are given as follows.

1) After successfully running the Chang–Lee SSO scheme twice with the same user U_i, malicious service provider P_j stores all messages exchanged in these two instances, denoted as $(ID_i, x, K_{ij}, w, n_2 \ldots.)$ for the first instance, and $(ID_i, x`, K`_{ij}, w`, n`_2 \ldots.)$ for the second instance.
2) By denoting $h_2 = h(K_{ij} \| w \| n_2)$ and $h`_2 = h(K`_{ij} \| w` \| n`_2)$, P_j first checks if h_2 and $h`_2$ are co-prime, i.e. if $\gcd(h_2, h`_2) = 1$. If $\gcd(h_2, h`_2) = 1$, $P_j$ then runs the extended Euclidean algorithm to compute two integers a and b such that $(a.h_2 + b.h`_2 = 1)$. Finally, malicious P_j can recover U_i's credential S_i by computing

$$S_i = x^a\, x`^b \bmod N. \tag{1}$$

Equation (1) is justified by the following equalities:

$$\begin{aligned} x^a\, x`^b \bmod N &= (S_i^{h2})^a \,.\, (S_i^{h2})^b \bmod N \\ &= S_i^{a.h2+b.h`2} \bmod N = S_i^1 \bmod N \\ &= S_i \end{aligned}$$

3) If $\gcd(h_2, h`_2) \neq 1$, $P_j$ then needs to run more instances with $U_i$ so that it can get two instances such that $\gcd(h_2, h`_2) = 1$.

B. Impersonation Attack without Credentials:

The soundness of the Chang–Lee SSO scheme, which seems to be satisfy this security requirement as well. The main reason is that to get valid proof x satisfying $(SID_i^{h2} \bmod N)$ for a random hash output h2 , there seems no other way but to compute x by $x = (SID_i^{h2.e\text{-}1} \bmod N)$, i.e. $x = (SID_i^d)^{h2}$ or $x = ((S_i)^{h2} \bmod N)$. Therefore, an attacker should not be able to log in to any service provider if it does not have the knowledge of either SCPC's RSA private key d or user U_i's credential S_i.

However, the Chang-Lee SSO scheme 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 SCPC's RSA private key d or user U_i's credential S_i, it is unfeasible to compute a proof x that passes through authentication, as an outside attacker is able to get a shortcut if the SCPC's RSA public key e is a small integer so that e's binary length is less than the output length of hash function h, i.e., $|e| < |h(.)|$. The attack is explained in detail as follows.

1) To impersonate legal user Ui with identity IDi for accessing service provider P_j, an attacker E first sends request message m1 normally, as U_i does.
2) Upon receiving message m2 from P_j, then checks P_j's signature and chooses a random integer t to compute (k_{ij}, K_{ij}, w). Before moving on to the next step, attacker E needs to check whether $h(K_{ij} \| w \| n2)$ is divisible by e. If not, E has to choose another t or start a new session to satisfy this condition.
3) As $h(K_{ij} \| w \| n2)$ is divisible by e, let $h(K_{ij} \| w \| n2) = e.b$ for some integer $b \in Z$. Now, E sets $x = (SID_i^b \bmod N)$, where $SID_i = (ID_i \| h(ID_i))$.
4) Finally, E can impersonate user U_i to pass the authentication by sending $m3 = (w, x, y)$ to P_j, since P_j will notice that $SID_i^{h(Kij \| w \| n2)} \bmod N = x^e \bmod N = SID_i^{b.e} \bmod N = x^e \bmod N$. This is because we have: $SID_i^{h(Kij \| w \| n2)} \bmod N = SID_i^{b.e} \bmod N$.

In the above attack we assume that e is a small integer and attacker E may know the value of one legal user's identity IDi. This is reasonable as explained below. On the one hand, in the system initialization phase Chang-Lee scheme just specifies that the trusted party SCPC needs to set its RSA key pair (e, d) but does not give any limitation on the length of public exponent e. So, e could be a small integer with binary length less than the output length of hash function h, i.e., |e| < |h (.)|. Moreover, in practice this is likely to happen due to the following two reasons: (a) to speed up the RSA signature verification, some security standards (e.g. PKCS [15]) and popular web sites (e.g. Wikipedia [14]) suggest that e can be set as 3 or 65537 and (b) as Chang-Lee scheme is claimed to be efficient even for mobile devices in distributed networks, using small exponent e can provide further computational advantage for these devices as they usually have limited resources for computation and storage.

V. Proposed Improvement

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 non-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.

A. System Initialization Phase

SCPC selects two large safe primes p and q to set N= pq. Namely, there are two primes p' and q' such that p= 2p' + 1 and q= 2q' + 1. SCPC now sets its RSA public/private key pair (e, d) such that ed = 1 mod 2p'q', where e is a prime. Let Q_N be the subgroup of squares in Z^*_N whose order is G =p'q' unknown to the public but its bit-length l_G= |N| - 2 is publicly known. SCPC randomly picks generator g of Q_N, selects an ElGamal decryption key u, and computes the corresponding public key y = g^u mod N. In addition, for completing the Diffie-Hellman key exchange SCPC chooses generator g' Є Z*N, where n is another large prime number. SCPC also chooses a cryptographic hash function h (.): {0, 1}* -> {0, 1} ^{k}, where security parameter k satisfies 160 <= k <= |N|-1. Another security parameter e >1 is chosen to control the tightness of the ZK proof. Finally, SCPC publishes (e, N, h (.), g, y, g', n), and keeps (d, u) secret.

B. Registration Phase

In this phase, upon receiving a register request, SCPC gives U_i fixed-length unique identity IDi and issues credential S_i = h (ID_i) ^{2d} mod N. Si calculated as SCPC's RSA signature on h $(ID_i)^2$ is an element of Q_N, which will be the main group we are calculating. Each service provider with identity ID_i should maintain a pair of signing/verifying keys for a secure signature scheme (not necessarily RSA). $\sigma_j(SK_j$, Msg) denotes the signature σ_j on message Msg signed by P_j using signing key SK_j. Ver $(PK_j$, Msg, $\sigma_j)$ denotes verifying of signature σ_j with public key PK_j, which outputs "1" or "0" to indicating if the signature is valid or invalid, respectively.

C. Authentication Phase

In this phase, RSA-VES is employed to authenticate a user, while a normal signature is used for service provider authentication. The details are illustrated in Fig. 2 and further explained as follows.

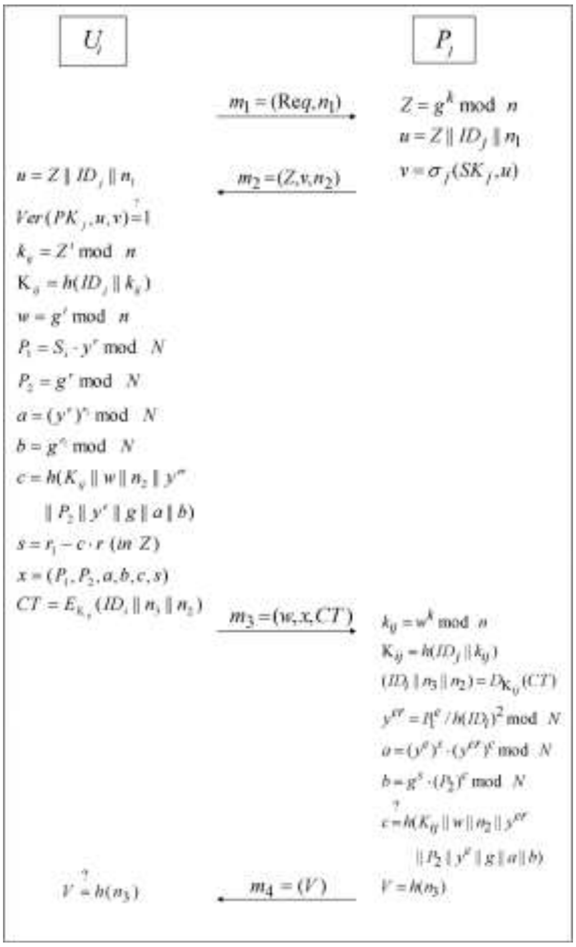
U_i
P_j
$m_1 = (Req, n_1)$
$Z = g^k \bmod n$
$u = Z \| ID_j \| n_1$
$v = \sigma_j(SK_j, u)$
$m_2 = (Z, v, n_2)$
$u = Z \| ID_j \| n_1$
$Ver(PK_j, u, v) \overset{?}{=} 1$
$k_v = Z^t \bmod n$
$K_{ij} = h(ID_j \| k_v)$
$w = g^t \bmod n$
$P_1 = S_i \cdot y^r \bmod N$
$P_2 = g^r \bmod N$
$a = (y^e)^{r_1} \bmod N$
$b = g^{r_1} \bmod N$
$c = h(K_v \| w \| n_2 \| y^{er} \| P_2 \| y^e \| g \| a \| b)$
$s = r_1 - c \cdot r$ (in Z)
$x = (P_1, P_2, a, b, c, s)$
$CT = E_{K_v}(ID_i \| n_1 \| n_2)$
$m_3 = (w, x, CT)$
$k_{ij} = w^k \bmod n$
$K_{ij} = h(ID_j \| k_{ij})$
$(ID_i \| n_3 \| n_2) = D_{K_{ij}}(CT)$
$y^{er} = P_1^e / h(ID_i)^2 \bmod N$
$a = (y^e)^s \cdot (y^{er})^c \bmod N$
$b = g^s \cdot (P_2)^c \bmod N$
$c \overset{?}{=} h(K_{ij} \| w \| n_2 \| y^{er} \| P_2 \| y^e \| g \| a \| b)$
$V \overset{?}{=} h(n_3)$
$m_4 = (V)$
$V = h(n_3)$

Fig. 2. Improved user identification phase

1) U_i sends a service request with nonce n1 to service provider P_j.
2) Upon receiving (Req, n1), P_j calculates its session key material Z = g^k mod n where k Є Z^*_n is a

random number, sets u = Z||ID_j||n1, issues a signature v= $\sigma_j(SK_j, u)$ and then sends m2 = (Z,v, n2) to the user, where n2 is a nonce selected by P_j .

3) Upon receiving m2= (Z, v, n2), U_i sets u= (Z|| Id_j || n1). Ui terminates the conversation if Ver(PK_j, u,v) = 0 . Otherwise, U_i accepts service provider P_j because the signature v is valid. In this case, U_i selects a random number t Є Z^*_u to compute w =g^t mod n, $k_{ij} = Z^t$ mod n, and the session keyK_{ij} = h (ID_j || k_{ij}). For user authentication, Ui first encrypts his/her credential S_i as (P1 = S_i. y^r mod N, P2 = g^r mod N), where r is is a random integer with binary length l_G. Next, U_i computes two commitments a= $(y^e)^{r1}$ mod N and b=g^{r1} mod N, where r1 Є ± {0, 1} $^{Є\ (lG+k)}$ is also a random number. After that, U_i computes the evidence showing that credential S_i has been encrypted in (P1, P2) under public key y. For this purpose, U_i calculates c= h (K_{ij}|| w || n2 ||y^{er} || P2 ||y^e ||g ||a ||b) and s = r1 –c.r. Then, x = (P1, P2, a, b, c, s) is the NIZK proof for user authentication. In fact, it is precisely, the processes of generating which is the proof part of RSA-VES. Finally, encrypts his/her identity ID_i, new nonce n3, and P_j's nonce n2 using session key K_{ij} to get cipher text CT = E_{Kij} (ID_i || n3 ||n2), and thereafter sends m3 = (w, x, CT) to service provider P_j.

4) To verify U_i, P_i calculates k_{ij} = wk mod n , the session key K_{ij} = h (ID_j || k_{ij}) , and then uses k_{ij} to decrypt CT and recover (ID_i, n3, n2). Then, computes $y^{er} = P1^e/h\ (ID_j)^2$ mod N, a = $(y^e)^s. (y^{er})^c$ mod N, b= $g^s . P_c^2$ mod N, and checks if (c, s) Є {0, 1} ^{k}. ± {0, 1} $^{Є\ (lG+k)+1}$ and c= h(K_{ij}|| w || n2 ||y^{er} || P2 ||y^e ||g ||a ||b). If the output is negative, P_j aborts the conversation. Otherwise, P_j accepts U_i and believes that they have shared the same session key K_{ij} by sending U_im4 = (V) where V= h (n3).

5) After U_i receives V, he checks if V= h (n3). If this is true, then U_i believes that they have shared the same session key K_{ij}. Otherwise, U_i terminates the conversation

Security Analysis:

The security analysis of the improved SSO scheme is focusing on the security of the user authentication part, especially soundness and credential privacy due to two reasons. First, 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 S^* corresponding to a target user U^*, an attacker, who could be a collusion of users and service providers, has at most a negligible probability of generating proof x^* and going through user authentication by impersonating user U^*.

The soundness of the above improved SSO scheme relies on the soundness of the NIZK proof, which also guarantees the soundness of RSA-VES. Namely, if the user authentication part is not sound, i.e., an attacker can present valid proof x^* without holding the corresponding credential S^* 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.

Credential privacy or credential irrecoverableness requires that there would 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. 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 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.

VI. Conclusion

In this paper, we identified 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 second 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 studied why their SSO scheme is not strong enough to guarantee the security for well-organized security arguments. In addition, we employed an efficient verifiable encryption of RSA signatures and we proposed that RSA-VES for an improved Chang–Lee scheme to achieve soundness and credential privacy.

As future work, it provides interests for researchers to formally define authentication soundness and constructing efficient and provably secures SSO schemes.

References

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

[2] 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.

[3] 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.

[4] G. Ateniese, "Verifiable encryption of digital signatures and applications," ACM Trans. Inf. Syst. Security., vol. 7, no.1, pp. 1–20, 2004.

[5] T.-S.Wu and C.-L. Hsu,"Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks," Computer Security, vol. 23, no. 2, pp. 120–125, 2004.
[6] Y. Yang, S. Wang, F. Bao, J. Wang, and R. H. Deng, "New efficient user identification and key distribution scheme providing enhanced security," Computer Security, vol. 23, no. 8, pp. 697–704, 2004.
[7] K. V. Mangipudi and R. S. Katti, "A secure identification and key agreement protocol with user anonymity (SIKA)," Computer Security, vol. 25, no. 6, pp. 420–425, 2006.
[8] C.-C. Lee, M.-S. Hwang and I-E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," IEEE Trans. Ind. Electron., 53(5): 1683-1687, Oct. 2006.
[9] 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.
[10] 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.
[11] 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.
[12] 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.
[13] The Open Group, "Security Forum on Single Sign-on", http://www.opengroup.org/security/l2-sso.html.
[14] Wikipedia, RSA (algorithm). [online]. http://en.wikipedia.org/wiki/RSA_ (algorithm).
[15] PKCS, "Public key cryptography standards, PKCS #1 v2.1," RSA Cryptography Standard, Draft 2, 2001.Available at http://www.rsasecurity.com /rsalabs/ pkcs/

Authors' Profiles

Mr. Sumanth C M received his B.E degree in Computer Science and Engineering from Sai Vidya Institute of Technology, Bangalore in 2012. Currently he is perusing M.Tech degree in Computer Science and Engineering at Canara Engineering College, Mangalore. His areas of interest are Network Security, Information Security and web design.

Mr. Adithyan B had done his B.E and M.Tech degree in Computer Science & Engineering. Currently he is working as Asst. Professor at Canara Engineering College, Mangalore. His area of interest is Cryptography, Computer Networks, Information security.

How to cite this paper: Sumanth C M, Adithyan B,"Confidence Analysis of a Solo Sign-On Device for Distributed Computer Networks", International Journal of Information Technology and Computer Science(IJITCS), vol.6, no.7, pp.40-46, 2014. DOI: 10.5815/ijitcs.2014.07.06