International Journal of Technology and Engineering System (IJTES)
Vol 6. No.1 – Jan-March 2014 Pp. 1-7
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-1345

SINGLE SIGN ON (SSO) MECHANISM ENHANCED WITH FIREWALL SECURITY IN MULTIPLE SERVICE PROVIDER

Padma Priya.C   Mrs.E.Indra
Computer Science and Engineering
Mailam Engineering College
sanpriya.c@gmail.com   indrae@gmail.com

ABSTRACT

Single 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, Chang and Lee proposed a new SSO scheme and claimed its security by providing well-organized security arguments. To demonstrative that their scheme is actually insecure as it fails to meet credential privacy and soundness of authentication. Specifically,presented 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. Identify the flaws intheir security arguments, to explain why attacks are possible against their SSO scheme. These attacks also apply to another SSO scheme proposed by Hsu and Chuang, which inspired the design of the Chang–Lee scheme. Moreover, by employing an efficient verifiable encryption of RSA signatures proposed by Ateniese, we propose an improvement for repairing the Chang–Lee scheme.To promote the formal study of the soundness of authentication as one open problem.

IndexTerms—Authentication, distributed computer networks, information security, security analysis, single sign-on (SSO).

1. INTRODUCTION

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. To avoid bogus servers, users usually need to authenticate service providers. After mutual authentication, a session key may be negotiated to keep the confidentiality of the data exchanged between a user and a service provider. In many scenarios, the anonymity of legal users must be protected as well. However, 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.

To maintain distinct pairs of identity and password for different service providers, since this could increase the workload of both users and service providers as well as the communication overhead of networks. To tackle this problem, the singlesign-on (SSO) mechanismhas been introduced so that, afterobtaining a credential from a trusted authority for a short period, each legal user's authentication agent can usethis single credential to complete authentication on behalf of theuser and then access multiple service providers. Intuitively, anSSO scheme should meet at least three basic security requirements,i.e., *unforgeability*, *credential privacy*, and *soundness*.

The generalized digital certificate(GDC), is to provide user authentication andkey agreement in wireless networks, in which a user, who holdsa 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. SSO scheme, has two weaknesses: 1) an outsider can forge a valid credential by mounting a credential forging attack since the Hsu–Chang scheme employed naïve RSA

International Journal of Technology and Engineering System (IJTES)
Vol 6. No.1 – Jan-March 2014 Pp. 1-7
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-1345

signature without using any hash function to issue a credential for any random identity selected by a user. 2) The Hsu–Chuang scheme requires clock synchronization since it uses a time stamp.

Finally, they presented a well-organized security analysis to show that their SSO scheme supports secure mutual authentication, session key agreement, and user anonymity.A generic SSO construction which relies on broadcast encryption plus zero knowledge (ZK) proof showing that the prover knows the corresponding private key of a given public key.

2. REVIEW OF THE CHANG–LEE SCHEME

Chang and Lee's single sign-on scheme 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, and service providers, denoted as Pj's.The Diffie–Hellman key exchange technique is employed toestablish session keys. In the Chang–Lee scheme, each user Uiapplies a credential from the trusted authority SCPC, whosigns an RSA signature for the user's hashed identity.On the other side, each P jmaintains its own RSAkey pair for doing server authentication. The Chang–Lee'sSSO 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.

Table.1 Notations

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_z	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

A. System Initialization Phase

The trusted authority SCPC first selects two large safe primesandthen sets N=pq. After that, SCPC determinesits RSA key pair(e,d) such thated=1modΦ(N), where Φ(N)=(p-1)(q-1).SCPC chooses a generator,gɛ 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) immediatelyonce this phase has been completed.

B. Registration Phase

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

C. User Identification Phase

To access the resources of service providerPj, user$U_i$needs to go through the authentication protocol specified in Fig. 1. Here, k and t are random integers chosen by Pj and U_i, respectively;n_1, n_2 and n_3 are three random nonces; and E(.) denotesa symmetric key encryption scheme which is used to protect theconfidentiality of user Ui's identityIDi .We highlight this phaseas follows.

- Upon receiving a service request message m_1 from user Ui, service provider Pj generates and returns user message m_2 which is made up primarily by its RSA signature on (Z, IDj ,n_1).Once this signature is validated, it means that user Uj has authenticated service provider Pj successfully. Here,Z=g^kmod n is the temporal Diffie–Hellman (DH) key exchange material issued by Pj.
- After that, user Ui correspondingly generates his/her temporal DH key exchange material w=g^tmod n and issues proof x=$S_i^{h(K_{ij}||w||n_2)}$, whereK_{ij}=h(IDi|| K_{ij}) is the derived session key andK_{ij}= Z^tmod n= w^kmod n= g^{kt}mod n is the raw key obtained by using the DH key exchange technique.
- Proof x=$S_i^{h(K_{ij}||w||n_2)}$ is used to convince Pj that Ui does hold valid credential Si without revealing the value of Si. Namely, after receiving message m_3 service provider Pj can confirm x's validity by checking if $SID_i^{h(K_{ij}||w||n_2)}$ mod N= x^emod N,

International Journal of Technology and Engineering System (IJTES)
Vol 6. No.1 – Jan-March 2014 Pp. 1-7
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-1345

where$SID_i=(ID_i||h(ID_i))$. If this quality holds, it means that userUi has been authenticated successfully by service providerPj. It worth noting that proof x is designed in a particular way so that except PjandUi, no one else can verify it as both Ui's identityIDi and the newly established session key Kij are used to produce x. This aims to achieve user anonymity as no eavesdropper can learn the values ofIDi andKij.

- Finally, message m_4 (i.e.$h(m_3)$) is employed to showthat P_i has obtained message correctly, which impliesthe success of mutual authentication and session keyestablishment.

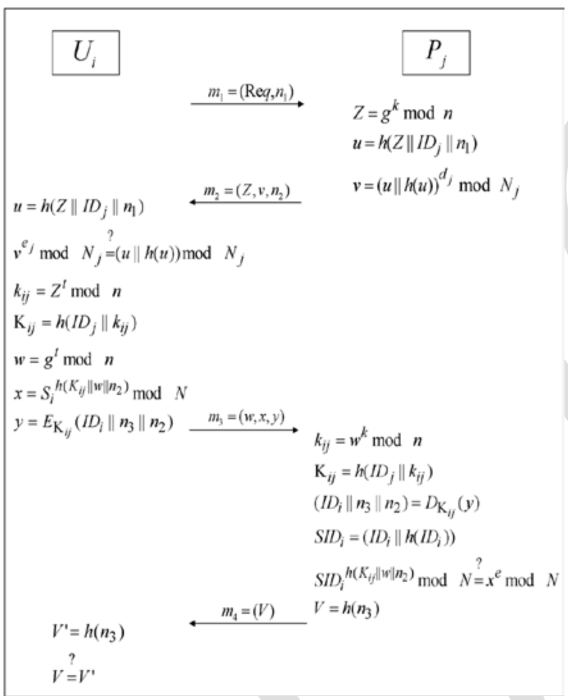

Figure.1.User identification phase of the Chang–Lee scheme.

3. ATTACKS AGAINST THE CHANG–LEE SCHEME

SSO scheme achieves secure mutual authentication, since server authentication is done by using traditional RSA signature issued by service provider Pj. Without valid credential Si it looks impossible for an attacker to impersonate a legal user Ui by going through the user authentication procedure.

A. Credential Recovering Attack

To satisfy the requirement of credential privacy since receiving credential proof $x=S_i^{h2}$ mod N, where h_2 denotesh(Kij||w||n_2) , does not allow service providerPj to recover user Ui's credential Si by computing $x=S_i^{h_2^{-1}}$ mod N , where h_2^{-1} refers to h_2^{-1}mod Φ(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.This is because here we could treat(h_2,h_2^{-1}) as another RSA public/private key pair w.r.t the same RSA modulus$N$.

Consequently, under the assumption that malicious service providerPj has run the Chang–Lee SSO scheme with the same user Uitwice, Pjwill be able to recoverUi credential with high probability by using the extended Euclidean algorithm. 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 SSO scheme twice with the same userUi, malicious service providerPj stores all messages exchanged in these two instances, denoted as(IDi,x,Kij,,w,$n2$,..)for the first instance, and (IDi,x\`,Kij,,$w$\`,$n2$\`,..)for the second instance.

2) By denoting $h2$=h(Kij||w||$n2$)and$h2$\`=$h$(Kij\`||w\`||$n2$\`),Pj first checks if$h2$and $h2$\`are co-prime, i.e. ifgcd($h2$,$h2$\`)=1.In the case thatgcd($h2$,$h2$\`)=1, Pjthen runs the extended Euclidean algorithm to compute two integers a and b such thata.$h2$+b.$h2$\`=1 . Finally, maliciousPjcan recoverUi 's credentialSi by computing,

$$S_i = x^a . x'^b \bmod N \qquad (1)$$

Equating (1) is justified by the following equalities:

$$\begin{aligned} x^a . x'^b \bmod N &= (S_i^{h2})^a \cdot (S_i^{h2'})^b \bmod N \\ &= S_i^{a h2 + b.h2'} \bmod N \\ &= S_i^{1} \bmod N \\ &= S_i \end{aligned}$$

3) Ifgcd($h2$,$h2$\`)≠1 , thenPj needs to run more instanceswith Uiso that it can get two instances such that gcd($h2$,$h2$\`)=1.

B. Impersonation Attack Without Credentials

To study the soundness of the SSOscheme, which seems to satisfy these security requirements as well. The main reason is that to get valid proof$x$ satisfyingSID_i^{h2}mod N= x^e mod N for a random hashoutputh_2, there seems no other way but to

International Journal of Technology and Engineering System (IJTES)
Vol 6. No.1 – Jan-March 2014 Pp. 1-7
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-1345

compute*x*by x=$SID_i^{h2.e1}$ mod N i.e., $x=(SID_i^{d})^{h2}$or $x=(S_i)^{h2}$ mod N. Therefore, an attacker should not beable to log in to any service provider if it does not have theknowledge of either SCPC's RSA private key d or userUi'scredential Si.

Again, however, such a plausible discussion simply explainsthe rationale of the Chang-Lee SSO scheme but cannot guaranteeits security w.r.t. the soundness.Indeed, no one can formally prove that withoutknowing eitherSCPC's RSA private key *d* or userUi's credential Si, it is unfeasible to compute a proof that passes throughauthentication, as an outsideattacker is able to get a shortcut ifthe SCPC's RSA public key*e* is a small integer so that *e*'s binarylength is less than the output length of hash function*h*. The attack is explained in detail as follows.

1) To impersonate legal user Uiwith identityIDi for accessing service provider Pj, an attacker E first sendsPj request messagem1 normally, as Ui.

2) Upon receiving message m2 from Pj,E then checksPj'ssignature and chooses a random integer*t* to compute(kij,Kij,*w*). Before moving on to the next step, attacker E needs to check whetherh(Kij||*w*||n_2) is divisible by *e*. If not, E has to choose another*t* or start a new session to satisfy this condition.

3)Ash(Kij||*w*||n_2) is divisibleby *e*, leth(Kij||*w*||n_2) =*e.b* for some integerb$\in$ Z. Now, Esets $x=SID_i^{b}$ mod N, where $SID_i = ID_i \|h(ID_i)$.

4)Finally, E can impersonate userU_i to pass the authentication by sending $m_3=(w,x,y)$ toP_j, sinceP_j will notice that $SID_i^{h(Kij\|w\|n2)}$ mod N= x^e mod N.

Finally, it must be emphasized that impersonation attacks without valid credentials seriously violate the security of SSO 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 SSO scheme suffering these attacks there are alternatives which enable passing through authentication without credentials.

4. ATTACKS ON THE HSU–CHUANG SCHEME

First, in the Hsu–Chuangscheme user U_i's credential $S_i$is a naive RSA signaturesigned by the trusted party SCPC, i.e.,$S_i=ID_i^{d}$mod N where $ID_i$is U_i's identity selected by him/herself. Second,to authenticate itself, service provider$P_j$sends signature$u=g_i^{h(Z\|T1\|IDj).dj}$mod Nj, where Z is the DH key materialgenerated by Pj,T1 is the current timestamp, andIDj isPj'sidentity. Finally, for user authentication userUi issues andsends proof$x=S_i^{h(Kij\|Z\|w\|T2)}$mod N toPj, who validates*x*by checking if $ID_i^{h(Kij\|Z\|w\|T2)}$ $=x^e$mod N.

This attack can be excluded if a specific encoding format isrequired for identities and the credential is issued by using a secure hash h, i.e.,$S_i=h(ID_i)^d$ mod N, as in theChang–Lee scheme.This means that the Hsu–Chuang scheme also fails to satisfyboth credential privacy and soundness of authentication. Inaddition, there is another flaw in the Hsu–Chuang scheme.Attacker E can impersonate service providerPj to cheatlegal users, as service authentication is conducted by using a non-traditional RSA signature,$u=g_i^{h(Z\|T1\|IDj).dj}$mod Nj. By communicating withPjtwice attacker E can get messages(Z,T1,IDj,u) and(Z`,T1`,IDj,u`) satisfying$u=g_i^{h(Z\|T1\|IDj).dj}$mod Njand $u`=g_i^{h(Z`\|T1`\|IDj).dj}$ mod Nj.Oncegcd(h(Z||T1||IDj),h(Z`||T1`||IDj))=1, E can run the extended Euclidean algorithmto find two integers a and bsuch that a.h(Z||T1||IDj) + b.h(Z`||T1`||IDj)=1in Z.Hence, E can recover g_i^{dj}mod Njby computingg_i^{dj}mod Nj=$u^a u`^b$mod Nj. After that, Ecan impersonatePjto any legal user by using the value ofg_i^{dj}mod Nj to issuesignature$u=(g_i^{dj}\text{mod Nj})^{h(Z\|T1\|IDj}$, without knowingPj'sRSA private keydj.

5. PROPOSED IMPROVEMENT

To overcome the flaws in the Chang-Lee scheme, an improvement by employing an RSA-based verifiableencryption of signatures (RSA-VES), which is an efficient primitive introduced forrealizing fair exchange ofRSA signatures.

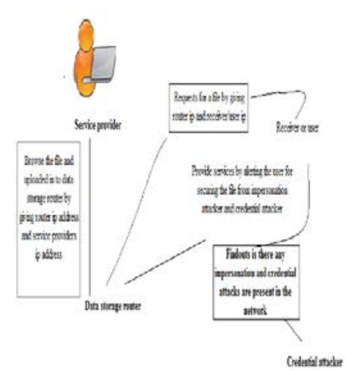

Figure.2 Architecture of sso schema

International Journal of Technology and Engineering System (IJTES)
Vol 6. No.1 – Jan-March 2014 Pp. 1-7
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-1345

The basic idea of the improved scheme and architecture can be highlighted as follows in fig.2. User U_i's credential is $S_i = h(ID_i)^{2d}$mod N, i.e., SCPC's RSA signature on the square of the hashed user identity. For user authentication, $U_i$will encrypt his/her credential S_i using ElGamal encryption of SCPC's other public key $y= g^u$ by computing$P_1= S_i$. y^rmod N and $P_2= g^r$mod N, where g ε Zn* of bigorder and *u*is SCPC's secret decryption key. In this improvement,SCPC also plays the role of the trust authority in VES. Toconvince a service provider that(P_1,P_2) does encrypt his/hercredentialS_i, $U_i$must alsoprovide an NZK proof *x* to show that he or she knows a secret*r* such that$P_i^e / h(ID_i)^2 = (y^e)^r$mod N.Such a proof*x*, is called 'proving the equality of two discretelogarithms in a group of unknown order, will convince theservice provider without leaking any useful information aboutU_i's credentialS_i.

A. 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 keypair(e,d) such thated=1 mod 2 p`q` , where is a prime. Let Q_N be the subgroup of squares in Z^*_N whose order #G=P`Q` is unknown to the public but its bit-length I_G=|N|-2 is publiclyknown. SCPC randomly picks generator g of Q_N, selectsan ElGamal decryption key*u*, and computes the corresponding public key*y* =g^emod N. In addition,for completing theDiffie-Hellman key exchange SCPC chooses generator ḡ Z^*_N,where *n*is another large prime number. SCPC also chooses acryptographic hash function*h*(.):$\{0,1\}^* \rightarrow \{0,1\}^K$, wheresecurity parameter*k* satisfies 160≤ *k*≤ |N|-1.

B. Registration Phase

In this phase, upon receiving a register request, SCPC gives$U_i$fixed-length unique identity ID_i and issues credential $S_i=h(ID_i)^{2d}$ mod N. S_i calculated as SCPC's RSA signature on $h(ID_i)^2$ is an element of Q_N , which will be the main group weare calculating.

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. 3 and further explainedas follows.

1) $U_i$sends a service request with nonce n_1 to serviceprovider P_j.

2) Upon receiving (Req, n_1), P_j calculates its session key Z= g^kmod n where*k*$Z^*_N$is a randomnumber, sets*u* =Z $\|ID_i\|$ n_1, issues a signature*v* =σj (SK_i,*u*), and then sends $m_2=(Z,v,n_2)$ to the user,wheren_2 is a nonce selected by P_j.

3) Upon receiving$m_2=(Z,v,n_2)$,$U_i$sets*u* =Z $\|ID_i\|$ n_1. $U_i$terminates the conversation if Ver(PK_j.,*u*,*v*)=0. Otherwise, $U_i$accepts service providerP_j because the signature*v*is valid. In this case, $U_i$selects a random numbert $Z^*_N$to compute*w*= g^tmod n, K_{ij} = Z^tmod nand the session key$K_{ij}=h(ID_i\|K_{ij})$. Next, $U_i$computes two commitments $a=(y^e)^{r1}$ mod N and $b=y^{r1}$mod N, where r1 $\pm\{0,1\}^{e(lG+k)}$is also a random number. After that,$U_i$computes the evidence showing that credentialS_i hasbeen encrypted in (P_1,P_2) under public key*y*. For this purpose,$U_i$calculates c= $h(K_{ij}\|w\|n_2\| y^{er} \|P_2\|y^e\|g\|a\|b)$ and $s=r_1-c.r$(in Z). Then, $x=(P_1,P_2,a,b,c,s)$ is theNIZK proof for user authentication.

4) To verifyU_i ,P_j calculates$K_{ij}=w^k$ mod n,thesession key$K_{ij} = h(ID_j\| K_{ij})$, and then uses$K_{ij}$to decrypt CT and recover(ID_i, n_2 , n_3). Then,$P_j$computes$y^{er}=P_1^e/h(ID_i)^2$ mod N, $a= (y^e)^s.(y^{er})^c$ mod N,$b=g^s$. P_2^cmod N, and checks if $(c,s)$$\{0,1\}^k$x $\pm\{0,1\}^{e(lG+k)+1}$ and $c= h(K_{ij}\|w\|n_2\| y^{er} \|P_2\|y^e\|g\|a\|b)$. If the output isnegative, $P_j$aborts the conversation. Otherwise,P_j accepts$U_i$and believes that they have shared the same sessionkeyK_{ij} by sending $U_i$$m_4$=(V)where V=h($n_3$).

5) AfterU_i receives V, he checks if V=h(n_3). If this is true,thenU_i believes that they have shared the same session keyK_{ij}. Otherwise,U_i terminates the conversation.

D. Security Analysis

To 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 guaranteedby 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.

International Journal of Technology and Engineering System (IJTES)
Vol 6. No.1 – Jan-March 2014 Pp. 1-7
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-1345

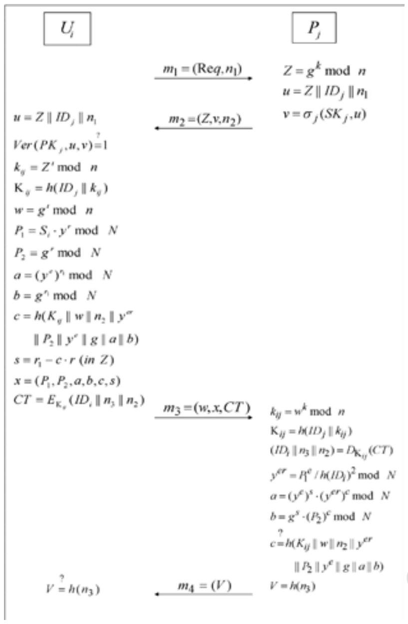

Figure. 3.Our improved scheme.

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. 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. 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, 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.

6. CONCLUSION

To 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 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. Discussed why their well-organized security arguments are not strong enough to guarantee the security of their SSO scheme. In addition, to 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, 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 formalmodel addressing the soundness of SSO has been proposed. Further research is necessary to investigate the maturityof this model and study how the security of the improved SSOscheme proposed can be formally proven. To provide a well organized security on SSO schema by using the firewall techniques.

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

International Journal of Technology and Engineering System (IJTES)
Vol 6. No.1 – Jan-March 2014 Pp. 1-7
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-1345

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, "Formalvulnerability analysisof a security system for remote fieldbus access," *IEEE Trans. Ind. Inf.*,vol. 7, no. 1, pp. 30–40, Feb. 2011.
[8] A. Valenzano, L. Durante, and M. Cheminod, "Review of security issuesin industrial networks," *IEEE Trans. Ind. Inf.*, vol. PP, no. 99,2012, DOI 10.1109/TII/2012.2198666.
[9] T.-S.Wu and C.-L. Hsu,"Efficient user identification scheme with keydistribution preserving anonymity for distributed computer networks,"*Comput.Security*, vol. 23, no. 2, pp. 120–125, 2004.
[10] Y. Yang, S. Wang, F. Bao, J. Wang, and R. H. Deng, "New efficientuser identification and key distribution scheme providing enhanced security,"*Comput. Security*, vol. 23, no. 8, pp. 697–704, 2004.