Security Analysis of A Single Sign-On Mechanism for Distributed Computer Networks

Guilin Wang, Jiangshan Yu, and Qi Xie

***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 distributed computer networks. Recently, Chang and Lee proposed a new SSO scheme and claimed its security by providing well-organized security arguments. In this paper, however, we demonstratively show that 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 the other attack an outsider without any credential may be able to enjoy network services freely by impersonating any legal user or a nonexistent user. We identify the flaws in their security arguments to explain why attacks are possible against their SSO scheme. Our attacks also applies to another SSO scheme proposed by Hsu and Chuang, which inspires the design of Chang-Lee scheme. We promote the study of the soundness of authentication as one open problem.**

Keywords: Authentication, Single Sign-On, Attacks, Information Security.

I. Introduction

With wide spreading of distributed computer networks, it has become popular to allow users accessing various network services offered by distributed service providers [1], [2]. Consequently, user authentication (also called user identification) [3], [4] plays a crucial role in distributed computer networks to verify if a user is legal and then can be granted to access the services requested. To prevent bogus servers users usually need to authenticate service providers. After mutual authentication, a session key may be negotiated to keep the confidentiality of data exchanged between a user and a service provider [4], [5], [6]. In many scenarios, the anonymity of legal users should be protected as well [4], [7], [6]. However, practice has shown that it is a big intelligent challenge to design efficient and secure authentication protocols with these security properties in complex environments of computer networks.

In 2000, Lee and Chang [4] proposed a user identification and key distribution scheme to maintain user anonymity in distributed computer networks. Later, Wu and Hsu [8] pointed out that Lee-Chang scheme is insecure against both impersonation attack and identity disclosure attack. Meanwhile, Yang et al. [9] identified a weakness in Wu-Hsu scheme and proposed an improvement. In 2006, however, Mangipudi and Katti [10] pointed out that Yang et al.'s scheme suffers from DoS (Deniable of Service) attack and presented a new scheme. In 2009, Hsu and Chuang [11] showed that both Yang et al. and Mangipudi-Katti schemes were insecure under identity disclosure attack, and proposed an RSA-based user identification scheme to overcome this weakness.

On the other hand, it is usually not practical by asking one user to maintain different pairs of identity and passwords 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, single sign-on (SSO) mechanism [12] has been introduced so that after obtaining a credential from a trusted authority, each legal user can use this single credential to authenticate itself and then access multiple service providers. Intuitively, an SSO scheme should meet at least two basic security requirements, i.e., *soundness* and *credential privacy*. Soundness means that an unregistered user without a credential should not be able to access the services offered by service providers. Credential privacy guarantees that colluded dishonest service providers should not be able to fully recover a user's credential and then impersonate the user to log in other service providers. Formal security definitions of SSO schemes were given in [13].

In [14], Chang and Lee made a careful study of SSO mechanism. Firstly, they argued that Hsu-Chuang user identification scheme, actually an SSO scheme, has two weaknesses: (a) An outsider can forge a valid credential by mounting a credential forging attack since Hsu-Chang scheme employed naive RSA signature without any hash function to issue a credential for any random identity selected by a user (In fact, this feature inherits from [9].); and (b) Hsu-Chuang scheme requires clock synchronization since timestamp is used in their scheme. Then, Chang and Lee presented an interesting RSA-based SSO scheme, which is highly efficient in computation and communication (So it is suitable for mobile devices), and does not rely on clock synchronization by using nonce instead of timestamp. Finally, they presented well-organized security analysis to show that their SSO scheme supports secure mutual authentication, session key agreement, and user anonymity. In [13], Han et al. proposed a generic SSO construction which relies on broadcast encryption plus zero knowledge (ZK) proof [15] showing that the prover knows the corresponding private key of a given public key. So, implicitly each user is assumed to have been issued a public key in a public key infrastructure (PKI). In the setting of RSA cryptosystem, such a ZK proof is very inefficient due to the complexity of

Guilin Wang and Jiangshan Yu are with the Center for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong, Wollongong, NSW 2522, Australia, Email: guilin@uow.edu.au, jy898@uowmail.edu.au.

Qi Xie is with the School of Information Science and Engineering, Hangzhou Normal University, Hangzhou 310036, China, Email: qixie68@yahoo.com.cn.

interactive communications between the prover (a user) and the verifier (a service provider). Therefore, compared with Han et al.'s generic scheme, Chang-Lee scheme has several attracting features: less underlying primitives without using broadcast encryption, high efficiency without resort to ZK proof, and no requirement of PKI for users. Unfortunately, as we shall discuss later this efficient SSO scheme is not secure, contrary to the security claims made in [14].

Specifically, in this paper we show Chang-Lee scheme [14] is actually insecure by presenting two impersonation attacks, i.e., *credential recovering attack* and *impersonation attack without credentials*. In the first attack, a malicious service provider who has communicated with a legal user twice can successfully recover the user's credential. Then, the malicious 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 enjoy services freely. These two attacks imply that Chang-Lee SSO scheme fails to meet credential privacy and soundness, which are essential requirements for SSO schemes and authentication protocols. Moreover, we identify the flaws in their security arguments to explain why our attacks are possible to be mounted against their scheme. Similar attacks can also be applied to Hsu-Chuang scheme [11], which inspires the design of Chang-Lee scheme.

The rest of the paper is organized as follows. Section II reviews Chang-Lee scheme [14]. After that, we present two attacks against Chang-Lee scheme in Section III, and briefly analyze Hsu-Chuang scheme [11] in Section IV. Finally, the conclusion is given in Section V.

II. Review of Chang-Lee scheme

Chang and Lee single sign-on scheme [14] 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 $SCPC$ (smart card producing center), and service providers, denoted as P_j's. The Diffie-Hellman key exchange technique is employed to establish session keys. In Chang-Lee scheme, each user U_i 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 such a 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 as we shall show shortly. On the other hand, each P_j maintains its own RSA key pair for doing server authentication. Chang-Lee's SSO scheme consists of three phases: system initialization, registration, and user identification. The details are reviewed as follows.

A. System Initialization Phase

The trusted authority $SCPC$ first selects two large safe primes p and q, and then sets $N = pq$. After that, $SCPC$ determines its RSA key pair (e, d) such that $ed = 1 \mod \phi(N)$, where $\phi(N) = (p-1)(q-1)$. Furthermore, $SCPC$ chooses a generator $g \in \mathbb{Z}_n^*$, 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 completed.

B. Registration Phase

In this phase, each user U_i chooses a unique identity ID_i with a fixed bit-length, and sends it to $SCPC$. After that, $SCPC$ will returns U_i the credential $S_i = (ID_i || h(ID_i))^d \mod N$, where $||$ denotes a concatenation of two binary strings and $h(\cdot)$ is a collision-resistant cryptographic one-way hash function. Here, both ID_i and S_i should 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 a service provider P_j, a user U_i needs to go through authentication protocol specified by Fig.1. Here, k and t are random integers chosen by P_j and U_i respectively; n_1, n_2 and n_3 are three random nonces; and $E(\cdot)$ denotes a symmetric key encryption scheme which is used to protect the confidentiality of user U_i's identity ID_i. We highlight this phase as follows.

- Upon receiving a service request message m_1 from a user U_i, service provider P_j generates and returns the user message m_2 which mainly includes its RSA signature on (Z, ID_j, n_1). Once this signature is validated, it means that user U_i 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.
- After that, user U_i correspondingly generates his/her temporal DH key exchange material $w = g^t \mod n$ and issues a proof $x = S_i^{h(K_{ij}||w||n_2)}$, where $K_{ij} = h(ID_i||k_{ij})$ is the derived session key and $k_{ij} = Z^t \mod n = w^k \mod n = g^{kt} \mod n$ 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 P_j that U_i does hold a valid credential S_i without revealing the value of S_i. Namely, after receiving message m_3 service provider P_j can confirm x's validity by checking if $SID_i^{h(K_{ij}||w||n_2)} \mod N = x^e \mod N$, where $SID_i = (ID_i||h(ID_i))$. Once this quality holds, it means that user U_i has been authenticated successfully by service provider P_j. Moreover, note that proof x is designed in a particular way so that except P_j and U_i, anyone else cannot verify it as both U_i's identity ID_i and the newly established session key K_{ij} are used to produce x. This aims to achieve user anonymity as no eavesdropper can learn the values of ID_i and K_{ij}.
- Finally, message m_4 (i.e. $h(n_3)$) is employed to show that P_j has obtained message m_3 correctly, which implies the success of mutual authentication and session key establishment.

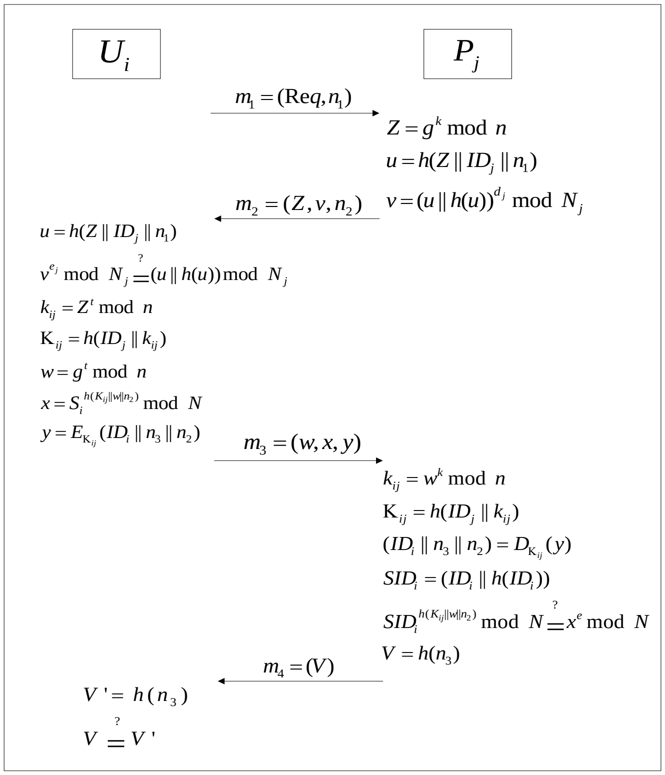
U_i
P_j
$m_1 = (\mathrm{Req}, n_1)$
$Z = g^k \bmod n$
$u = h(Z \| ID_j \| n_1)$
$v = (u \| h(u))^{d_j} \bmod N_j$
$m_2 = (Z, v, n_2)$
$u = h(Z \| ID_j \| n_1)$
$v^{e_j} \bmod N_j \overset{?}{=} (u \| h(u)) \bmod N_j$
$k_{ij} = Z^t \bmod n$
$\mathrm{K}_{ij} = h(ID_j \| k_{ij})$
$w = g^t \bmod n$
$x =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

Fig. 1. User Identification Phase of Chang-Lee scheme

III. Attacks Against Chang-Lee Scheme

According to the above review it seems that Chang-Lee SSO scheme achieves secure mutual authentication since server authentication is done via using traditional RSA signature issued by service provider P_j and without a valid credential S_i it looks impossible for an attacker to impersonate a legal user U_i by going through the user authentication procedure.

However, in the following we show that Chang-Lee scheme is actually not a secure SSO scheme by presenting two effective and concrete impersonation attacks. The first attack, called *credential recovering attack*, compromises the credential privacy in Chang-Lee scheme as a malicious service provider is able to recover the credential of a legal user. The other attack, called *impersonation attack without credentials*, demonstrates how an outside attacker may be able to enjoy resources and services offered by service providers freely, since the attacker can successfully impersonate a legal user without holding a valid credential and thus violate the requirement of soundness for an SSO scheme. In real life, these attacks may lead high risk to both users and service providers.

We now first 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 [14] are not enough to guarantee the security of Chang-Lee SSO scheme.

A. Credential Recovering Attack

Intuitively, Chang-Lee SSO scheme seemingly satisfies the requirement of credential privacy since receiving the credential proof $x = S_i^{h_2} \mod N$, 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 $S_i = x^{h_2^{-1}} \mod N$, where h_2^{-1} refers to $h_2^{-1} \mod \phi(N)$. In fact, the difficulty of calculating h_2^{-1} by given (e, N, x, h) is the exact rationale why 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 ciphertext). 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. Moreover, directly recovering S_i from $x = S_i^{h_2} \mod N$ also looks impossible as this seems equivalent to decrypt the RSA ciphertext x w.r.t. the (ephemeral) public key h_2.

Nevertheless, there is a pitfall in the produce of proof $x = S_i^{h_2} \mod N$ as here the same credential S_i is encrypted multiple times under different (ephemeral) public key h_2 w.r.t. the same RSA modulus N. Consequently, under the assumption that a 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 a certain high probability by using extended Euclidean algorithm. Namely, P_j can solve S_i from two equations $x = S_i^{h_2} \mod N$ and $x' = S_i^{h'_2} \mod N$. The details of the attack are given as follows.

1) After successfully running Chang-Lee SSO scheme twice with the same user U_i, a malicious service provider P_j stores all messages exchanged in these two instances, denoted them as $(ID_i, x, K_{ij}, w, n_2, \cdots)$ for the first instance, and $(ID_i, x', K'_{ij}, w', n'_2, \cdots)$ 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 $\gcd(h_2, h'_2) = 1$. In the case that $\gcd(h_2, h'_2) = 1$, P_j then runs the extended Euclidean algorithm to compute two integers a and b such that $a \cdot h_2 + b \cdot h'_2 = 1$ (in $\mathbb{Z}$). Finally, malicious P_j can recover U_i's credential S_i by computing
$$S_i = x^a \cdot x'^b \mod N. \tag{1}$$
Eq. (1) is justified by the following equalities:
$$\begin{aligned} x^a \cdot x'^b \mod N &= (S_i^{h_2})^a \cdot (S_i^{h'_2})^b \mod N \\ &= S_i^{a \cdot h_2 + b \cdot h'_2} \mod N \\ &= S_i^1 \mod N \\ &= S_i. \end{aligned}$$
3) If $\gcd(h_2, h'_2) \neq 1$, P_j needs to run more instances with U_i so that it can get two instances such $\gcd(h_2, h'_2) = 1$.

We give a few remarks on the above attack. Firstly, the above attack has a success rate about 60% due to two facts: (a) For two randomly selected integers u and v, the probability of $\gcd(u, v) = 1$ holds with probability $6/\pi^2 \approx 0.6$ [16][17]; and (b) As the outputs of hash function h, h_2 and h'_2 can be regarded as random numbers. This means that after executing the Chang-Lee SSO scheme with the same user U_i twice, malicious P_j will be able to recover U_i's credential S_i with probability about 0.6. Consequently, it is trivial to see that after running the scheme with U_i a couple of times, P_j can recover S_i almost certainly. Secondly, 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 h_2 together. Finally, the attack will lead to a serious consequence since after recovering a valid credential of a legal user, a malicious P_j can impersonate this user by trivially running Chang-Lee SSO scheme as does by the legal user to freely enjoy the services offered by other service providers.

Now, we discuss why a service provider P_j could be malicious and then mount the above attack. On the one hand, Chang-Lee SSO scheme just specifies that $SCPC$ is the trusted party (refer to Section IV A [14]). So, this implies that service providers are not trusted parties and then they could be malicious. In addition, on page 629 of [14] the authors summarized: Yang et al. [9] "*showed that Wu-Hsu's modified version cold not protect the user's token against a malicious service provider, ...*". This also implicitly means that the authors agree the existence of attacks from malicious service providers against SSO schemes. Moreover, if all service providers are assumed to be trusted, to identify him/herself user U_i can simply encrypt his/her credential S_i under the RSA public key of a service provider P_i. Then, P_i can trivially decrypt this ciphertext to get U_i's credential and verify its validity by checking if it is a correct signature issued by $SCPC$. In fact, such a straightforward scheme with strong assumption is much simpler, more efficient and has better security (At least, the attacks discussed here do not work anymore).

On the other hand, according to the security models given in [9] and [13], malicious service providers could be attackers in SSO 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 $SCPC$, all service providers are also trusted. The basic reason is that assuming the existence of a trusted party is the strongest supposition in cryptography which usually requires very expensive costs to develop and maintain. In particular, Han et al. [13] defined the collusion impersonation attacks to capture the scenarios in which malicious service providers may recover a user's credential and then impersonate the user to login other service providers. It is easy to see that the above credential recovering attack is just a special case of collusion impersonation attacks where only one malicious service provider can recover a user's credential.

B. Impersonation Attack Without Credentials

We now study the soundness of Chang-Lee SSO scheme, which looks respecting this security property as well. The main reason is that to get a valid proof x satisfying $SID_i^{h_2} \mod N = x^e \mod N$ for a random hash output h_2, there seems no any other way but to compute x by $x = SID_i^{h_2 \cdot e^{-1}} \mod N$, i.e., $x = (SID_i^d)^{h_2}$ or $x = (S_i)^{h_2} \mod N$. Therefore, an attacker should be not able to log in 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.

Again, however, such a plausible discussion just explains the rationale of Chang-Lee SSO scheme but cannot guarantee its security w.r.t. the soundness. This is also the essential reason why the current stream of research in information security focuses on formal proofs showing the security of cryptosystems rigorously. Indeed, nobody can formally prove that without knowing either $SCPC$'s RSA private key d or user U_i's credential S_i, it is infeasible 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., $|e| < |h(\cdot)|$. The attack is explained in detail as follows.

1) To impersonate a legal user U_i with identity ID_i for accessing service provider P_j, an attacker E first sends P_j request message m_1 normally as U_i does.
2) Upon receiving message m_2 from P_j, E then checks P_j's signature and chooses a random integer t to computes (k_{ij}, K_{ij}, w). Now, attacker E needs to check whether $h(K_{ij}||w||n_2)$ is divisible by e. If not, E has to choose another t or start a new session to satisfy this condition. Otherwise, continues the next step.
3) As $h(K_{ij}||w||n_2)$ is divisible by e, let $h(K_{ij}||w||n_2) = e \cdot b$ for some integer $b \in \mathbb{Z}$. Now, E computes x by $x = SID_i^b$, where $SID_i = ID_i||h(ID_i)$
4) Finally, E can impersonate user U_i to pass the authentication by sending $m_3 = (w, x, y)$ to P_j, since P_j will notice that $SID_i^{h(K_{ij}||w||n_2)} \mod N = x^e \mod N$. This is because we have: $SID_i^{h(K_{ij}||w||n_2)} \mod N = SID_i^{b \cdot e} \mod N = x^e \mod N$.

We now give a few comments on the above impersonation attack without credentials. Firstly, the attack will succeed at rate about $1/e$ for one random number t in a new session. The reason is that $e|h(K_{ij}||w||n_2)$ holds with probability about $1/e$, since $|e| < |h(\cdot)|$ and the output of hash function h can be treated as random numbers. Consequently, if $e = 3$ the above attack can succeed once by trying about three values of t on average. Even if e is as large as $65537 (= 2^{16}+1)$, trying 65537 times to get a successful impersonation seems not an issue for attacker E as it may explore a machine, which can be much more powerful that a mobile device, to do the computations needed for each try, i.e., two modular exponentiations and two hash evaluations. Moreover, even timeout was introduced in Chang-Lee scheme it may be not a real obstacle for attacker E as it can initialize new sessions (w.r.t. the same or different identities).

Secondly, 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 ID_i. This is reasonable as explained below. On the one hand, in the system initialization phase (Section IV-A) 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., $|e| < |h(\cdot)|$. 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 #1 [18]), academic papers (e.g. [19]) and popular web sites ((e.g. wikipedia [20])) 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. In addition, the security analysis given in [14] neither excludes the case of small e nor relies on the concrete procedure of setting $SCPC$'s RSA key pair (e, d).

On the other hand, in Chang-Lee SSO scheme users' identities are not crucial as their credentials, though the identities are transferred in ciphertext to provide user anonymity. So, users' identities could be known by an attacker due to different reasons, like users' negligence. At least, service providers know users' identities. Moreover, even if users' identities are well protected so that attacker E cannot impersonate a registered user U_i as above, E can freely forge an identity ID. This is possible because in Chang-Lee scheme, each user selects his/her identity by following only one requirement: each identity is a string with fixed bit-length. Therefore, even an outside attacker E can use an arbitrary such string as an identity to mount the above attack, since the service providers are not provided any additional mechanism to check whether an identity ID has been registered with $SCPC$. This also implies that E can even impersonate a nonexistent user to freely enjoy resources and services offered by service providers, if e is a small integer.

Finally, we would like to emphasize that impersonation attacks without valid credentials seriously violate the security of SSO schemes as it allows attacker 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 to pass through authentication without credentials.

C. Discussions

In [14], Chang and Lee provided well-organized security analysis to show that their SSO scheme is secure. However, the two impersonation attacks presented in 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 happening again in the future design of SSO schemes? We now discuss these issues in this section.

In [14], the security of Chang-Lee SSO scheme has been analyzed in three different ways: (a) The BAN logic [21] was used to show the correctness of Chang-Lee scheme; (b) Informal security arguments were given to demonstrate that their scheme can resist some attacks, including impersonation attacks; and (c) A formal security proof was given to prove that their scheme is a secure authenticated key exchange (AKE) protocol [22]. However, these security analysis and proof are still not enough to guarantee the full security of Chang-Lee scheme, as explained below. Firstly, as early as in 1990s it has been known that though the BAN logic has been shown useful to identify some attacks, it may approve protocols that are actually unsound in practice due to some technical weaknesses in the logic [23]. Moreover, in [14] 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 [14], the authors just simply mentioned: "*Also, we can prove that U_i and P_j are able to authenticate each other using our protocol.* " without arguments showing why each party cannot be impersonated by an attacker. Secondly, the authors did discuss informally why their scheme can withstand impersonation attacks by considering two scenarios, i.e., an attacker re-uses a previous nonce n_2 to forge message m_3 or selects a random credential S_i to compute SID_i by $SID_i = S_i^e \mod N$. However, such informal arguments neither firmly confirm their scheme's security against these two concrete attacks nor exclude the existence of other scenarios of impersonation attacks, like our attacks 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 computational Deffie-Hellman (CDH) assumption (refer to Theorem 1 in [14], not the security of mutual authentication. According to the definitions given by Bellare and Rogaway [22], one fundamental requirement of a secure AKE protocol is that the protocol should be a secure mutual authentication in the first place.

From the above discussions, we can see that it is the use of credential proof $x = S_i^{h_2} \mod N$ leading to the above two attacks against Chang-Lee SSO scheme. More specifically, $x = S_i^{h_2} \mod N$ is a kind of knowledge proof which shows that a prover (played by user U_i usually) knows the credential S_i. However, this is not a secure proof as a malicious verifier (i.e. service provider P_j) can recover S_i and an outside attacker may be able to get authenticated without a credential. Based on this observation, a natural improvement on Chang-Lee scheme is to replace non-interactive proof x by a rigorous but interactive zero knowledge (ZK) proof [15] that shows the prover's knowledge of secret $S_i = SID_i^d \mod N$ without revealing any additional information about credential S_i. In more detail, using the verifiably encrypted signature introduced in [25] a user U_i can encrypt his/her credential S_i under the public key of a trusted party and verifiably convinces a service provider P_j that the ciphertext does contain S_i w.r.t. U_i's identity ID_i without allowing P_j to get any additional information about credential S_i. Compared with two modulo exponentiations used for generating and verifying proof x, however, ZK proofs for showing the possession of an RSA signature usually require hundreds of modulo exponentiations [24], [25] since these proofs rely on inefficient "cut and choose" method, i.e., binary challenges.

From the two attacks presented above, we can learn that both credential privacy and soundness are crucial for SSO schemes. As mentioned in Section III-A, credential privacy has been studied in Yang et. al [9] and Han et al. [13]. Surprisingly, however, this is no existing research which has given a careful treatment on soundness, to the best of our knowledge. For example, Han et al. [13] neither investigated soundness, thought they did carefully study how to formally define credential forgery and recovery attacks from outsiders, users, service providers and potential collusion of them. In the most traditional way of authentication in which a user will be authenticated if he/she can provide a valid pair of user name and password (i.e. credential), soundness is obviously satisfied as a user is not able to go through authentication without providing a valid credential that is registered and maintained by a server. In complex scenarios, like Chang-Lee scheme, the situation may become not obvious, subtle or even challenging. Due to this reason, we promote this as an open problem for attracting future study. Namely, it is an interesting and important question to formally define soundness of SSO/authentication schemes and rigorously prove this property for concrete solutions.

Finally, we remark that our analysis above just shows that Chang-Lee SSO scheme fails to achieve secure authentication, without violating its security for achieving user anonymity and session key privacy.

IV. Attacks on Hsu-Chuang Scheme

In this section, we briefly highlight the difference between Chang-Lee scheme [14] and Hsu-Chuang scheme [11] to see why our impersonation attacks apply to Hsu-Chuang scheme as well. The two schemes have similar structures and use similar notations, but the technical details differ. In a summary, Hsu-Chuang scheme is mainly different from Chang-Lee scheme in the following three aspects. Firstly, in Hsu-Chuang scheme a user U_i's credential S_i is a naive RSA signature signed 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. Secondly, to authenticate itself a service provider P_j sends a signature $u = g_j^{h(Z||T_1||ID_j)\cdot d_j} \mod N_j$, where Z is the DH key material generated by P_j, T_1 is the current timestamp, and ID_j is P_j's identity. Finally, for user authentication the user U_i issues and sends a proof $x = S_i^{h(K_{ij}||Z||w||T_2)} \mod N$ to P_j, who validates x by checking if $ID_i^{h(K_{ij}||Z||w||T_2)} = x^e \mod N$. For more detail, please refer to [11] or Section II of [14].

As pointed out in [14], Hsu-Chuang scheme is vulnerable to impersonation attack as an attacker can forge a valid credential S_i w.r.t. an identity ID_i by simply selecting a random $S_i \in \mathbb{Z}_N^*$ and then computing $ID_i = S_i^e \mod N$. This attack can be excluded if a specific encoding format is required for identities and the credential is issued by using a secure hash h, i.e., $S_i = h(ID_i)^d \mod N$, as did in Chang-Lee scheme. According to the discussions in Section III, Hsu-Chuang scheme is still not secure even with such a countermeasure. The reason is that our two attacks against Chang-Lee scheme apply to Hsu-Chuang scheme directly. This means that Hsu-Chuang scheme also fails to satisfy both of credential privacy and soundness of authentication. Moreover, we identify another flaw in Hsu-Chuang scheme: An attacker E can impersonate a service provider P_j to cheat legal users, as the service authentication is conducted via using a non-traditional RSA signature, $u = g_j^{h(Z||T_1||ID_j)\cdot d_j} \mod N_j$. Namely, by communicating with P_j twice an attacker E can get messages (Z, T_1, ID_j, u) and (Z', T_1', ID_j, u') so that $u = g_j^{h(Z||T_1||ID_j)\cdot d_j} \mod N_j$ and $u = g_j^{h(Z'||T_1'||ID_j')\cdot d_j} \mod N_j$. Once $\gcd(h(Z||T_1||ID_j), h(Z||T_1||ID_j)) = 1$ (recall that this holds with probability about 0.6), E can find two integers a and b such that $a \cdot h(Z||T_1||ID_j) + b \cdot h(Z||T_1||ID_j) = 1$. Hence, E can recover $g_j^{d_j} \mod N_j$ by computing $g_j^{d_j} \mod N_j = u^a u'^b \mod N_j$. After that, E can impersonate P_j to any legal user by using the value of $g_j^{d_j} \mod N_j$ to issue a signature $u = (g_j^{d_j} \mod N_j)^{h(Z||T_1||ID_j)}$, without knowing P_j's RSA private key d_j.

V. Conclusion

In this paper, we demonstrated two effective impersonation attacks on Chang and Lee's single sign-on (SSO) scheme [14]. The first attack shows that their scheme can not protect the privacy of a user's credential, and thus, a malicious service provider can impersonate a legal user 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 even impersonate a nonexistent user and then freely access resources and services provided by service providers. We also discussed why their well-organized security arguments are not strong enough to guarantee the security of their SSO scheme. In addition, we explained why Hsu and Chuang's scheme [11] is also vulnerable to these attacks. As the future work, the open problems are to formally define authentication soundness and construct efficient and provably secure single sign-on schemes.

References

[1] A. C. Weaver and M. W. Condtry, "Distributing Internet services to the network's edge", *IEEE Trans. Ind. Electron.*, 50(3): 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.*, 58(6): 2163-2172, Oct. 2010.

[3] L. Lamport, "Password authentication with insecure communication", *Commun. ACM*, 24(11): 770-772, Nov. 1981.

[4] W. B. Lee and C. C. Chang, "User identification and key distribution maintaining anonymity for distributed computer networks," *Computer Systems Science and Engineering*, 15(4): 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.*, 15(6): 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.*, 57(2): 793-800, Feb. 2010.

[7] 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.

[8] T.-S. Wu and C.-L. Hsu, "Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks," *Computers and Security*, 23(2): 120-125, 2004.

[9] Y. Yang, S. Wang, F. Bao, J. Wang, and R. H. Deng, "New efficient user identification and key distribution scheme providing enhanced security," *Computers and Security*, 23(8): 697-704, 2004.

[10] K. V. Mangipudi and R. S. Katti, "A secure identification and key agreement protocol with user anonymity (sika)," *Computers and Security*, 25(6): 420-425, 2006.

[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.*, 179(4): 422-429, 2009.

[12] The Open Group, "Security Forum on Single Sign-on", `http://www.opengroup.org/security/l2-sso.htm`

[13] J. Han, Y. Mu, W. Susilo, and J. Yan, "A generic construction of dynamic single sign-on with strong security," in *Proc. of SecureComm'10*, pp. 181-198, LNICS 50, Springer, 2010.

[14] C.-C. Chang and C.-Y. Lee, “A secure single sign-on mechanism for distributed computer networks,” *IEEE Trans. Ind. Electron.*, 59(1): 629-637, Jan. 2012.

[15] U. Feige, A. Fiat, and A. Shamir, “Zero-knowledge proofs of identity,” *Journal of Crytography*, 1(2): 77-94, 1988.

[16] G. Tenenbaum. *Introduction to Analytic and Probabilistic Number Theory* (Theorem 5, page 41). Cambridge studies in advanced mathematics, Vol. 46. Cambridge University Press, 1995.

[17] E. W. Weisstein, “Relatively prime,” MathWorld-A Wolfram Web Resource. [Online]. Available at `http://mathworld.wolfram.com/RelativelyPrime.html`

[18] PKCS, “Public key cryptography standards, PKCS #1 v2.1,” RSA Cryptography Standard, Draft 2, 2001. Available at `http://www.rsasecurity.com/rsalabs/pkcs/`

[19] D. Boneh, “Twenty years of attacks on the RSA cryptosystem, ” *Notices of the American Mathematical Society*, 46(2): 203-213, 1999.

[20] Wikipedia, RSA (algorithm). [online]. `http://en.wikipedia.org/wiki/RSA_(algorithm)`

[21] M. Burrows, M. Abadi, and R. Needham, “A logic of authentication,” *ACM Trans. Comput. Syst.*, 8(1): 18-36, 1990.

[22] M. Bellare and P. Rogaway, “Entity authentication and key distribution,” in *Proc. of CRYPTO’93*, pp. 232-249, LNCS 773, Springer, 1993.

[23] C. Boyd and W. Mao, “On a limitation of BAN Logic,” in *Proc. of EUROCRYPT’93*, LNCS 765, pp. 240-247, Springer, 1994.

[24] N. Asokan, V. Shoup, and M. Waidner, “Optimistic fair exchange of digital signatures,” *IEEE Journal on Selected Areas in Communications*, 18(4): 591-606, 2000.

[25] J. Camenisch and M. Michels, “Confirmer signature schemes secure against adaptive adversaries,” in *Proc. of EUROCRYPT 2000*, LNCS 1807, pp. 243-258, Springer, 2000.

Guilin Wang is currently a senior lecturer in the School of Computer Science and Software Engineering, University of Wollongong, Australia. Before this, he was a lecturer in the School of Computer Science, University of Birmingham, UK, a research scientist in the Institute for Infocomm Research (I^{2}R), Singapore, and an assistant professor in the Institute of Software, Chinese Academy of Sciences, where he received his PhD degree in computer science in March 2001. Up to now, he has published more than 60 research publications in the areas of applied cryptography, information security, and electronic commerce. His main research interests include the analysis, design, and applications of digital signatures and security protocols. Dr. Wang has served as a program co-chair for six international security conferences, a committee member for more than 40 international conferences or workshops, and a reviewer for over 20 international journals. His homepage is `http://www.uow.edu.au/~guilin/`.

Jiangshan Yu is a research master student in the Center for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong, Australia, where he received his computer science master degree by course in computer science in 2011. His research topic is authentication in distributed computer networks.

Qi Xie is a professor in in the School of Information Science and Engineering, the Institute of Cryptology and Its Applications, and the Key Lab of E-Business and Information Security, and the vice dean of graduate school, Hangzhou Normal University, China. He received his PhD degree in applied mathematics from Zhejiang University, China, in March 2005. His research area is applied cryptography, including digital signatures, secret sharing, authentication protocol, key agreement protocols etc. He has published over 30 research papers in international and domestic journals and conferences.