ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Efficient Single Sign on Scheme for Distributed Networks

N. Rubiya (M.E-CSE), M. Arulprakash M.TECH.,

PG Student, Sri Subramanya College of Engineering and Technology, palani, Tamilnadu, India[1]

Assistant Professor, Sri Subramanya College of Engineering and Technology, palani, Tamilnadu, India[2]

ABSTRACTt- 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. The existing Chang-Lee scheme is actually insecure by presenting two attacks i.e credential recovering attack, impersonation attack without credentials. 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. In the Enhancement phase the work is based on to avoid the previous attacks that is impersonation and mounting. Once user enters into the service the portal will assign unique session id for each users with the unique key assignment for every machine. Once user request the service the portal will check the session id and the unique key (RSA signature scheme) for each request. If the authentication fails the user will not enjoy the distributed services.

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

I. INTRODUCTION

With the development of distributed computer networks, it has become common to allow users to access 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 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 [4], [5]. In many scenarios, the anonymity of legal users must be protected as well [4], [6].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 [7], [8].

In 2000 Lee and Chang first proposed a user identification protocol that provides session key establishment and user anonymity for distributed computer networks. Since that time many improvements for dealing with possible attacks have been proposed. In 2004, Wu and Hsu pointed out that Lee and Chang's protocol might suffer from masquerading attacks, and they proposed a modification to correct this issue .Later Yang *et al.* showed that Wu–Hsu's modified version could not protect the user's secret token against a malicious service provider, and they proposed an enhancement to prevent this kind of attack. In 2005, Lee demonstrated two possible attacks on Wu–Hsu's scheme. Under these attacks, the adversary can forge a legal token to cheat the service provider. In 2006, Mangipudi and Katti presented a denial-of-service (DoS) attack on Yang *et al.*'s scheme and proposed an improvement to overcome this drawback. Recently, Hsu and Chuang demonstrated that both Yang *et al.*'s and Mangipudi – Kati's schemes are vulnerable to identity disclosure attacks and proposed an improvement to prevent such attacks. Although Hsu and Chuang's scheme has many attractive features; in fact, it does not provide all of the security properties that they claimed. We demonstrated that Hsu–Chuang's scheme might be vulnerable to impersonation attacks since it employs an analogous RSA signature to generate secret tokens. In this kind of attack, an attacker can masquerades a legal user to cheat the service provider. In addition, Hsu–Chuang's scheme uses time stamps to avoid replay attacks and unfortunately, it is difficult to verify the timestamp when entities are located in different time zones or when there is a congested network environment that has unstable latency. Therefore, additional time-synchronized mechanisms are

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

needed to adjust the clock between the two parties .We propose a secure single sign-on mechanism to allow mobile users to use the unitary token to access service providers..The proposed scheme is based on one-way hash functions and random nonce to solve the weaknesses described above and to decrease the overhead of the system.

The remainder of this paper is organized as follows. Section II reviews Chang–Lee scheme [19]. After that, we present two attacks against the Chang–Lee scheme in Section III and proposed improvement in Section IV. Then, the details of improved scheme are given in Section V. Finally, the conclusion is given in Section VI.

II. REVIEW OF THE CHANG–LEE SCHEME

Chang and Lee's single sign-on scheme [19] is a remote user authentication scheme, supporting session key establishment and user anonymity. In their scheme, RSA cryptosystems are used to initialize a trusted authority, called an SCPC (smart card producing center), and service providers, denoted as Pj's. 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, 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 as we shall show shortly. On the other side, each 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.

III. ATTACKS AGAINST THE CHANG–LEE SCHEME

As can be 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. Without valid credential it looks impossible for an attacker to impersonate a legal user by going through the user authentication procedure. It can be seen from the following, 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, the "credential recovering attack" compromises the credential privacy in the Chang–Lee scheme as a malicious service provider is able to recover the credential of a legal user. The other attack, an "impersonation attack without credentials," 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 violate 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 , does not allow service provider p_j to recover user 's credential by computing S_i , where refers to $x=s_i^{h2-1} \bmod N$. In fact, the difficulty of calculating from the given is the exact rationale why the RSA cryptosystem is secure, i.e, it should be intractable for an attacker to derive the RSA private key from the public key.

On the other hand, according to the security models given in [10] and [17], 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, all service providers are also trusted. The basic reason is that assuming the existence of a trusted party is the strongest supposition in cryptography but it is usually very costly to develop and maintain. In particular, Han *et al.* [17] defined collusion impersonation attacks as a way to capture the scenarios in which malicious service providers may recover a user's credential and then impersonate the user to login to other service providers. It is easy to see that the above credential recovery attack is simply a special case of collusion impersonation attack where a single malicious service provider can recover a user's credential.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

B. Impersonation Attack Without Credentials

We now study the soundness of the Chang–Lee SSO scheme, which seems to satisfy these security requirements as well. The main reason is that to get valid proof x satisfying SIDih2.e^{-1}mod N =x^e mod N fo r a random hash output h_2 , there seems no other way but to compute x . Therefore, an attacker should not be able to log in to any service provider if it does not have the knowledge of either's RSA private key or user 's credential .

Again, however, such a plausible discussion simply explains the rationale of the Chang-Lee SSO scheme but cannot guarantee its security w.r.t. the soundness. This is also the essential reason why the current focus of research in information security is on formal proofs which rigorously show the security of cryptosystems. Indeed, no one can formally prove that without knowing either 's RSA private key or user 's credential , it is unfeasible to compute a proof that passes through authentication, as an outside attacker is able to get a shortcut if the 's RSA public key

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.

IV. PROPOSED IMPROVEMENT

To overcome the flaws in the Chang-Lee scheme [19], we now propose an improvement by employing an RSA-based verifiable encryption of signatures (RSA-VES), which is an efficient primitive introduced in [21] for realizing fair exchange of RSA signatures. VES comprises three parties: a trusted party and two users.

A. Main Idea

The basic idea of the improved scheme can be highlighted as follows. User's credential is $S_i = h(ID_i)^{2d}$ mod N., SCPC's RSA signature on the square of the hashed user identity. For user authentication, will encrypt his/her credential using ElGamal encryption of SCPC's other public key $y=g^u$ by computing $P1=s_i .y^r$ mod N and $P_2=g^r$ mod N, where g €Z*n of big order and U is SCPC's secret decryption key. In this improvement, SCPC also plays the role of the trust authority in VES. To convince a service provider that (P_1 and P_2)does encrypt his/her credential $S_i .U_i$ must also provide an NZK proof to show that he or she knows a secret r and P_2.Such a proof , is called 'proving the equality of two discrete logarithms in a group of unknown order' [21], will convince the service provider without leaking any useful information about's credential . For server authentication, service providers can simply issue signatures as the work in [19] did, though the proposed changes give service providers the freedom to employ any secure signature scheme. The other procedures are the same as in the Chang-Lee scheme.

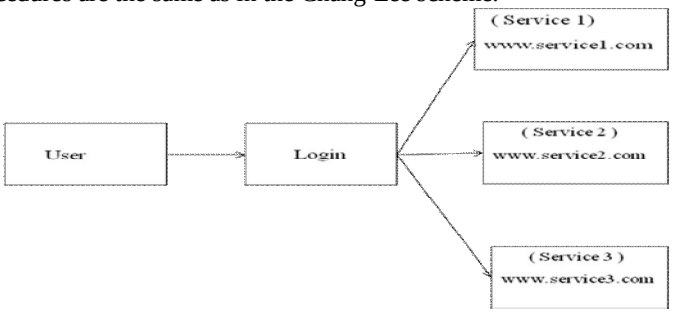

Fig. 1 The block diagram of proposed scheme

Frequently used notation are given in the below table.1

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

NOTATION	DESCRIPTION
SCPC	Smart Card Producing Centre
U_i,P_j	User and Service Provider
ID_i,ID_j	A unique identity of U_i, and P_j
e_x, ,d_x	The RSA key pair of identity x
S_i	The credential of U_i
S_x	The secret key of SCPC
S_y	The public key of SCPC
H(.)	One way hash function

Table.1Frequently used Notation in our scheme description

V. DETAILS OF THE PROPOSED SYSTEM

In our framework, there are multiple owners, multiple AAs, and multiple users in addition, DMA-ABE is used. The framework is illustrated in Fig. 1. We term the users having read and write access as data readers and contributors, respectively.

A. 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 φ(N), where φ(N)=(p-1)(q-1). SCPC chooses a generator g,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.

B. Registration Phase

In this phase, upon receiving a register request, SCPC gives Ui, 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 , which Q_n ill be the main group we are calculating. each service provider with identity IDj should maintain a pair of signing/verifying keys for a secure signature scheme (not necessarily RSA).

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.

User first send request m1with nonce n1 to provider. upon receiving request from user the provider calculates Session key material Z and issues signature then sends message m2 with nonce n2.where n2 refers
Nonce selected by provider.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Upon receiving message m2 the user verify the signature. it terminate the conversation if the verification process is zero. otherwise it continues the conversation.

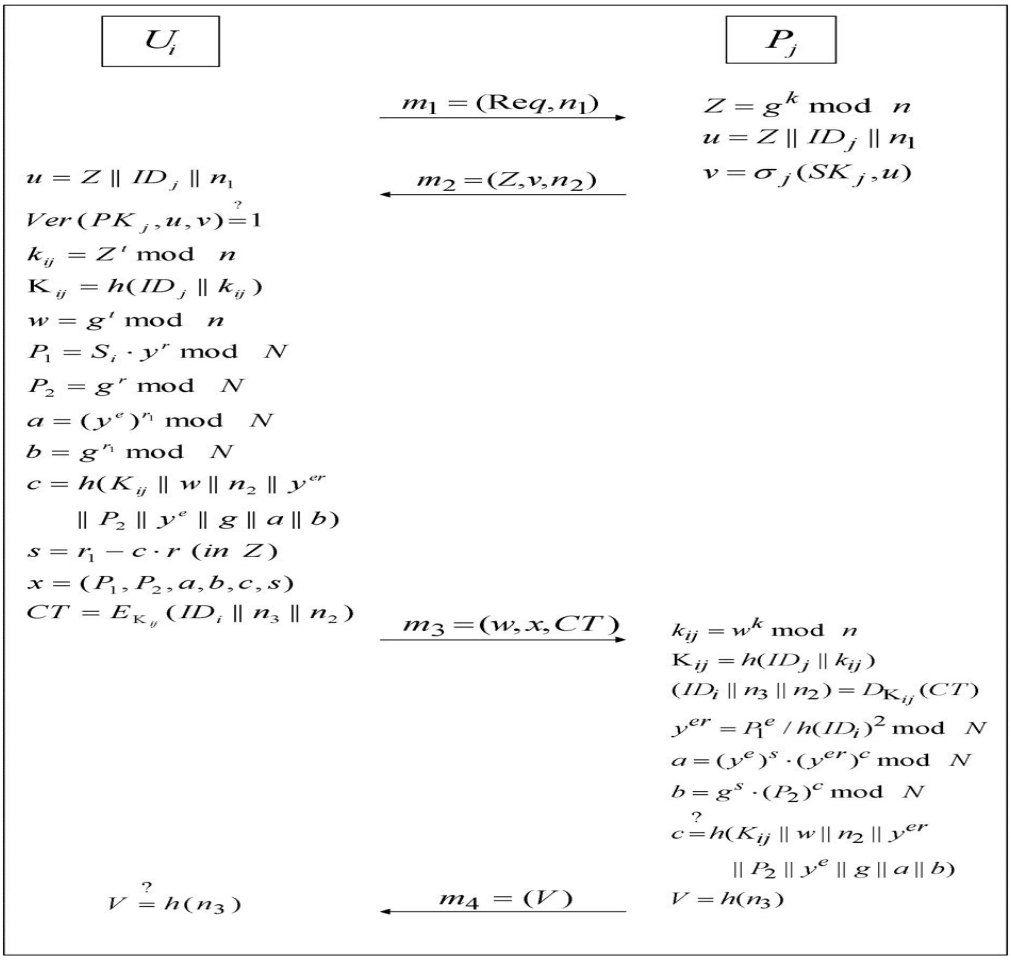

Fig. 2. Our improved scheme

D. Security Analysis

We now analyze the security of the improved SSO scheme by focusing on the security of the user authentication part, especially soundness and credential privacy due to two reasons. On the one hand, the unforgeability of the credential is guaranteed by the unforgeability of RSA signatures, and the security of service provider authentication is ensured by the unforgeability of the secure signature scheme chosen by each service provider. On the other hand, other security properties (e.g., user anonymity and session key privacy) are preserved, since these properties have been formally proved in [19] and the corresponding parts of the Chang–Lee scheme are kept unchanged.

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

hiding property of RSA-VES, defined as the third property of Definition 1 in [21].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 given. 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 demonstrated two effective impersonation attacks on Chang and Lee's single sign-on (SSO) scheme [19].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. By employing an efficient verifiable encryption of RSA signatures the attacks were avoided and an improved Chang–Lee scheme to achieve soundness and credential privacy was proposed.

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] 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.

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

[4] Y. Xu, R. Song, L. Korba, L. Wang, W.Shen, and S. Y. T. Lang, "Distributed device networks with security constraints," IEEE Trans. Ind. Inf., vol. 1, no. 4, pp. 217–225, Nov. 2005

[5] 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.

[6] A.Valenzan ,L.Durante, and M.Cheminod, "Review of security issues in industrial networks" IEEE Trans. Ind. Inf., vol. PP, no. 99, 2012, DOI 10.1109/TII/2012.2198666.

[7] 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.