www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 3 March 2015, Page No. 10823-10826

Single Sign on Mechanism

Priyanka Jagtap, Shraddha Karande, Pratibha Kohinkar,Tazeen Mansuri

[1]Savitribhai phule University, Sharchandra Pawar Collage Of Engginering,
Dumberwadi,Otur
Priyankajagtap1818@gmail.com

Savitribhai phule University, Sharchandra Pawar Collage Of Engginering,
Dumberwadi,Otur
karandeshraddha00@gmail.com

Savitribhai phule University, Sharchandra Pawar Collage Of Engginering,
Dumberwadi,Otur
pratibha.kohinkar@gmail.com

[1]Savitribhai phule University, Sharchandra Pawar Collage Of Engginering,
Dumberwadi,Otur
tazint20@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 SSOscheme and claimed its security by providing well-organized security arguments. In this paper, however, we demonstrative 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 another 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 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. We promote the formal study of the soundness of authentication

Keywords: 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 (alsocalled 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 Manuscript received February 01, 2012; revised May 15, 2012; accepted July24, 2012. Date of publication August 28, 2012; date of current version December 19, 2012. The work of G. Wang was supported in part by the National Natural Science Foundation of China under Grant 61070153. The work of Q. Xie was supported in part by the National Natural Science Foundation of China under Grant 61070153 and the Natural Science Foundation of Zhejiang Province under Grant LZ12F02005. Paper no. TII-12-0047. G. Wang and J. 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 (e-mail: guilin@uow.edu.au;jy898@uowmail.edu.au).
Q. Xie is with the School of Information Science and Engineering, Hangzhou Normal University, Hangzhou 310036, China (e-mail: qixie68@yahoo.com.cn). Digital Object Identifier 10.1109/TII.2012.2215877
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 .In 2000, Lee and Chang proposed a user identification and key distribution scheme to maintain user anonymity in distributed computer networks. Later, Wu and Hsu pointed out that the Lee–Chang scheme is insecure against both impersonation attacks and identity disclosure attacks. Meanwhile, Yang *et al.* identified a weakness in the Wu–Hsu scheme and proposed an improvement. In 2006, however, Mangipudi and Katti pointed out that Yang *et al.*'s scheme suffers from Deniable of Service (DoS) attacks and presented a new scheme. In 2009, Hsu and Chuang 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. Recently, authentication and privacy have been attracted a lot of attentions in RFID systems , industrial networks , as well as general computer networks

2. Usable Notation:

Table Show

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

3 .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 (smart card producing center), and service providers, denoted as 's. The Diffient –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. Table I explains notations, and the details of Chang–Lee scheme are reviewed as follows.

3.1. System Initialization Phase

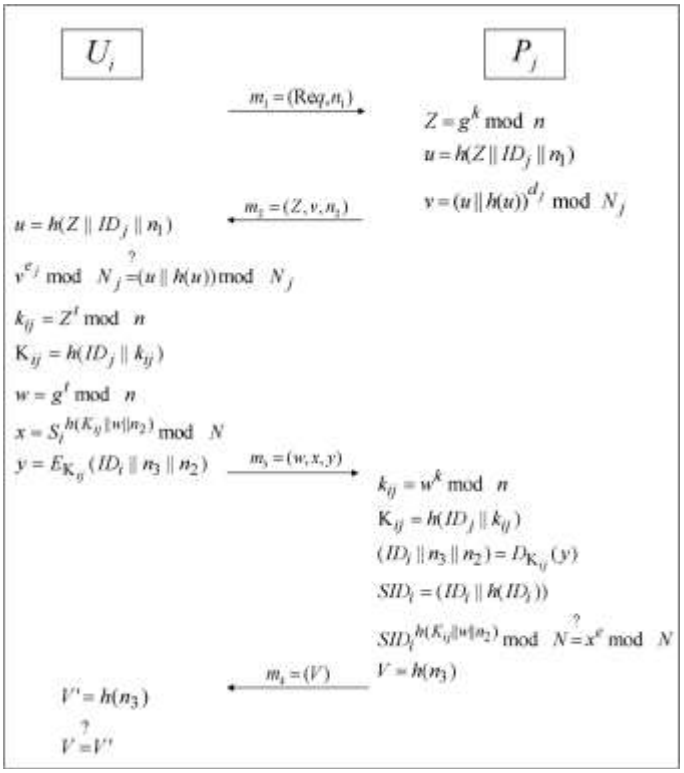
The trusted authority SCPC first selects two large safe primes and and then sets . After that, SCPC determines its RSA key pair such that , where . SCPC chooses a generator ,where is also a large prime number. Finally, SCPC publishes , keeps as a secret, and erases immediately once this phase has been completed.

3.2. Registration Phase

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

3.3. User Identification Phase

To access the resources of service provider , user needs to go through the authentication protocol specified in Fig. 1.Here, and are random integers chosen by and , respectively;
, and are three random nonces; and denotes a symmetric key encryption scheme which is used to protect the confidentiality of user 's identity .We highlight this phase as follows.
• Upon receiving a service request message from user, service provider generates and returns user message which is made up primarily by its RSA signature on .Once this signature is validated, it means that user has authenticated service provider successfully. Here, is the temporal Diffie–Hellman (DH)
key exchange material issued by .
• After that, user correspondingly generates his/her temporal DH key exchange material and issues proof , where is the derived session key and is the raw key obtained by using the DH key exchange technique.
• Proof is used to convince that does hold valid credential without revealing the value of . Namely, after receiving message service provider can confirm 's validity by checking if , where if this quality holds, it means that user has been authenticated successfully by service provider . It worth noting that proof is designed in a particular way so that except and , no one else
can verify it as both 's identity and the newly established session key are used to produce . This aims to achieve user anonymity as no eavesdropper can learn the values of and .
• Finally, message (i.e.) is employed to show that has obtained message correctly, which implies the success of mutual authentication and session key establishment.



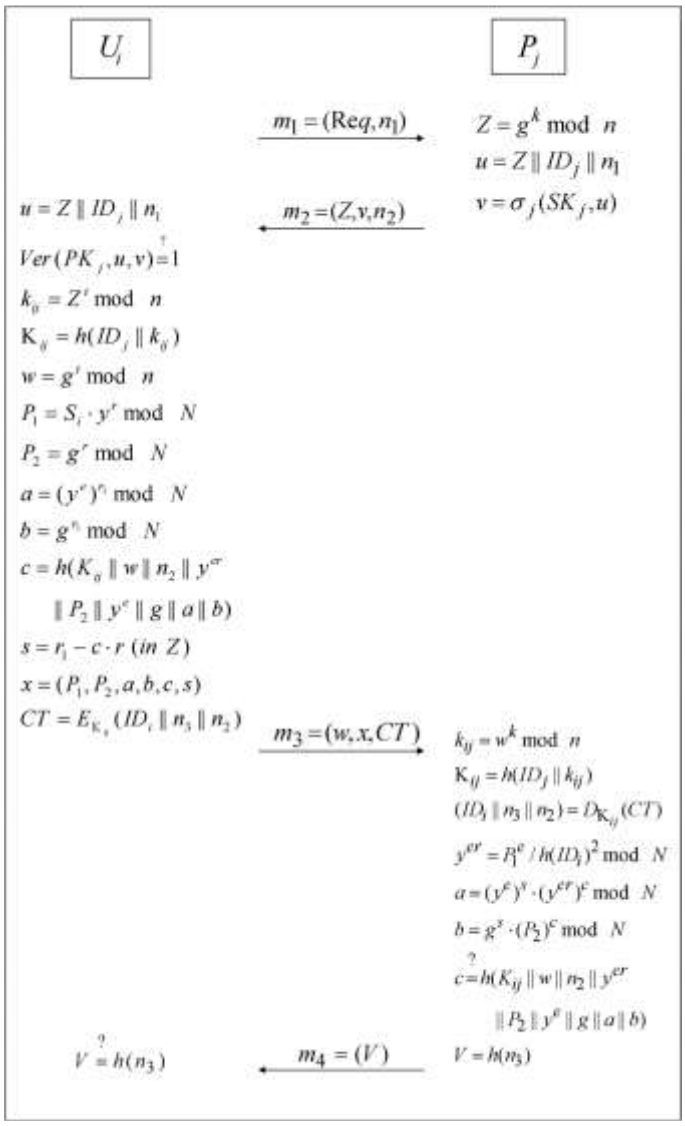
User identification phase of the Chang–Lee scheme

4. 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. Fig. 1. User identification phase of the Chang–Lee scheme. It can be seen from the following, however, that the Chang–Lee scheme is actually not a secure 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. 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 are not enough to guarantee the security of the Chang–Lee.

5. 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 in for realising 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 ciphertext. 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



.Fig refer improved scheme

6. 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 and the corresponding parts of the Chang–Lee scheme are kept unchanged. Soundness requires that without holding valid credential corresponding to a target user , an attacker, who could be a collusion of users and service providers, has at most a negligible probability of generating proof and going through user authentication by impersonating user . The soundness of the above improved 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 1 in . 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 given .

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 1 in . 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. More rigorous security proofs are interesting topics for further study by considering formal definitions first.

CONCLUSION

In this paper, we 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. 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 is also vulnerable to these attacks. Furthermore, by employing an efficient verifiable encryption of RSA signatures introduced by Ateniese , we proposed 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 formal model addressing the soundness of SSO has been proposed in. Further research is necessary to investigate the maturity of this model and study how the security of the improved SSO scheme proposed in this paper can be formally proven.

References

[1] A. Bonnaccorsi, "On the Relationship between Firm Size and Export Intensity," Journal of International Business Studies, XXIII (4), pp. 605-635, 1992. (journal style)

[2] R. Caves, Multinational Enterprise and Economic Analysis, Cambridge University Press, Cambridge, 1982. (book style)

[3] M. Clerc, "The Swarm and the Queen: Towards a Deterministic and Adaptive Particle Swarm Optimization," In Proceedings of the IEEE Congress on Evolutionary Computation (CEC), pp. 1951-1957, 1999. (conference style)

[4] H.H. Crokell, "Specialization and International Competitiveness," in Managing the Multinational Subsidiary, H. Etemad and L. S, Sulude (eds.), Croom-Helm, London, 1986. (book chapter style)

[5] K. Deb, S. Agrawal, A. Pratab, T. Meyarivan, "A Fast Elitist Non-dominated Sorting Genetic Algorithms for Multiobjective Optimization: NSGA II," KanGAL report 200001, Indian Institute of Technology, Kanpur, India, 2000. (technical report style)

[6] J. Geralds, "Sega Ends Production of Dreamcast," vnunet.com, para. 2, Jan. 31, 2001. [Online]. Available: http://nl1.vnunet.com/news/1116995. [Accessed: Sept. 12, 2004]. (General Internet site)