Design and Analysis of Multi-Secured Signatures of a Single Sign- on Mechanism for Distributed System

Sumangala Patil[1] Niharika Kumar[2]
[1]M.Tech Scholar [2]Assistant Professor
[1,2]Department of Information Science
[1,2]RNS Institute of Technology Bangalore, Karnataka, India

Abstract— Single Sign–on is a new authentication mechanism for user to use multiple services provided by service provider in distributed computer network. It is a one type of application in that allows users to log in once and access to multiple independent applications without being asked to log in again at every application. It enables a legal user with a single credential to be authenticated by multiple service providers in distributed computer networks. In this paper, however, it is shown that most existing SSO schemes have not been formally proved to satisfy credential privacy and soundness of credential based authentication. To overcome this drawback an efficient verifiable encryption of RSA signatures has been proposed.

Keywords: Authentication, Credential, Distributed System, single sign-on(SSO).

I. INTRODUCTION

Single sign-on (SSO) is a mechanism whereby a single action of user authentication and authorization allows to all computers and systems where authorization rights have been verified, without the need to enter multiple passwords. Single sign-on reduces human error, a major component of systems failure and is therefore highly desirable. 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. Identification of user is an important access control mechanism for client–server networking architectures.

The goal of a single sign on platform is to eliminate individual sign on procedures by centralizing user authentication and identity management at a central identity provider. In a single sign-on solution, the user should seamlessly authenticated to his multiple user accounts (across different systems) once he proves his identity to the identity provider. Nevertheless, in many current solutions, the user is required to repeat sign on for each service using the same set of credentials, which are validated at the identity provider by each service.

Consequently, user authentication plays an important 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 negotiated to keep the confidentiality of the data exchanged between a user and a service provider.

On the other side, it is usually not practical by asking one user 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 single sign-on (SSO) mechanism has been introduced, as it allows a user with a single credential to access multiple service providers. Intuitively, an SSO scheme should meet at least three basic security requirements, i.e., unforgeability, credential privacy, and soundness. Unforgeability demands that, except the trusted authority, even a collusion of users and service providers are not able to forge a valid credential for a new user. 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 to other service providers. Soundness means that an unregistered user without a credential should not be able to access the services offered by service providers.

II. RELATED WORK

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 ; 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.

User authentication and key establishment are two fundamental services in secure communication. Extensive research has been conducted in both areas. In 2000, Lee and Chang [1] 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 the drawbacks.

In [8], Han et al. proposed 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. 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 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.

Han et al. 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.

A. 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_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

III. PROPOSED WORK

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 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. Organizing The notations used in the algorithm are explained in Table I. The scheme consists of three phases:

A. System Initialization Phase

SCPC does the following

- selects large two primes p, q and computes p*q. determines the key pair (e,d) such that e *d ≡ 1mod φ(N),where φ(N)=(p − 1)*(q − 1).
- chooses a generator g over the finite field Z∗n, where n is a large odd prime number.
- SCPC protects the secrecy of d and publishes (e,g,n,N).

B. Registration Phase

- Each user Ui registers a unique identity ID I with a fixed bit length.
- Obtain a secret token Si=(IDi||h(IDi)) dmod N, from the SCPC through a secure channel where h(·) is a cryptographic one-way hash function.

C. User Identification Phase

Ui submits the request with a random nonce n1, m1 to Pj. On receiving m1, Pj chooses a random number k and then generates a random nonce n2. Pj calculates Z = gk mod n, u = h(Z||IDj||n1),and the signature v =(u||h(u))dj mod Nj.Next, Pj sends the message m2 = {Z,v,n2} back to Ui. After receiving m2 from Pj, Ui computes u =h(Z||IDj||n1) and performs the next step. Ui verifies the signature v by checking the equivalency of vej mod N?=(u||h(u))mod Nj. Otherwise, Ui informs Pj that someone has tampered with Z and aborts the protocol. Otherwise, Ui chooses a random number t to be his short-term private key and computes w =gt mod n. Ui calculates the parameter kij as kij= Zt mod n. Ui generates a random nonce n3 and calculates three parameters Kij, x and y in accordance with the following equations: Kij= h(IDj||kij), the session key, x = Si h(Kij ||w||n2)mod N, y = EKij (IDi||n3||n2), where E(·) is a symmetric crypto system such as DES or AES. Ui sends m3 = {w,x,y} to Pj After receiving m3, Pj computes kij as kij= wkmod n. Pj can obtain the session key Kij by computing Kij=h(IDj|| kij). Pj uses Kij to decrypt cipher text y and retrieves IDi, n3, and n2. If n2 is valid, Pj computes SIDi = (IDi||h(IDi)). Pj verifies the validity of the identity IDi by checking SIDi h (Kij ||w||n2)mod N ?= xe mod N. If the equation holds, Pj trusts that Ui is a legal user. Pj computes V = h(n3) and sends m4 = {V } to Ui. After receiving m4 from Pj, Ui computes V ||= h(n3) and confirms that V? = V „. When both the equations are same, Ui trusts that Pj is an authorized service provider and Pj has really calculated the common session key Kij.

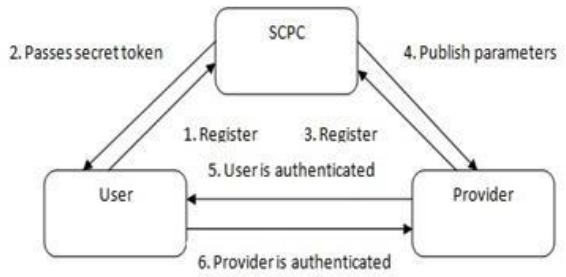

Fig. 1.checking Authentication of User and Provider

D. ADVANTAGES OF SSO

- Users need only one password for access to all applications and systems.
- Users can access the corporate network at the start of their workday.

- Users have immediately have access to all
- necessary password-protected applications.
- Users don't need to remember multiple passwords.
- Users don‟t have to write down their passwords.
- Users don't have to guess passwords, which potentially expose applications to unauthorized users.

IV. METHODOLOGY

In the existing system, different security schemes are proposed by many researchers. In the proposed system, various Client-Server programs are written to implement the project using programming in .Net. Chang-Lee algorithm is used for user identification phase. But, it is using a less secure DES algorithm. This paper user a more secure RSA-VES algorithm to enhance the security features. So, this scheme is more secure than Chang-Lee scheme.

V. CONCLUSIONS

Most existing single sign-on schemes suffer from various security issues and are vulnerable to different attacks. 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. This paper propose an improved Chang–Lee scheme to achieve soundness and credential privacy by employing an efficient verifiable encryption of RSA signatures. Thus the proposed scheme reduces the computation cost, enhances the confidentiality, and preserves soundness and credential privacy.

ACKNOWLEDGMENT

I take this Opportunity to express my profound gratitude and deep regards to my guide Ms. Niharika Kumar, Assistant Professor, RNS Institute of technology, Bangalore, for her exempla nary guidance, and constant encouragement throughout.

I would also like to thank Director Dr. H N Shivashankar, Principal Dr. M K Venkatesha and Dr. M V Sudhamani, professor and Head, Dept of Information Science and engineering, RNSIT, for constant encouragement in implementing this paper and pursuing this paper.

REFERENCES

[1] Chin-Chen Chang, A secure single mechanism for distributed computer networks, IEEE Trans. On Industrial Electronics ,vol. 59,no. 1, Jan 2012.
[2] 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.
[3] 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.
[4] 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.
[5] 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.
[6] 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.
[7] G. Ateniese, Verifiable encryption of digital signatures and applications, ACM Trans. Inf. Syst. Secur., vol. 7, no. 1, pp. 1–20, 2004.
[8] Advanced Encryption Standard, NIST Std. FIPS PUB 197, 2001.

