An Efficient Digital Verifiable Signature Scheme For User Authentication and Key Establishment in Secure Communication Network

Sharath A H[1] **Manasa M P[2]** **Dr Suresh L[3]**

[1] PG Scholar, Department of CSE, Cambridge Institute of Technology, India
[2] PG Scholar, Department of CSE, Cambridge Institute of Technology, India
[3] Principal, Cambridge Institute of Technology, India
[1] sharathah@outlook.com [2] manasa.m.p@outlook.com [3] principal@citech.edu.in

Abstract: In distributed computer networks, the network service providers allow users to access various services. In current application architecture user has to memorize and utilize different set of credentials E.g. Username/Password or token for each application he want to access. But it is usually not practical by asking one user to maintain distinct pair of identity and password for distributed service provider. Due to increased workload of both user and service provider, it causes communication overhead in the network. It is also inefficient and insecure with the exponential growth of number of application services user has to access.

To overcome this, a new authentication mechanism called Single Sign-on (SSO) was proposed in which single credentials is authenticated by multiple service providers in distributed networks. Chang and Lee proposed a new SSO scheme [1]. But, this scheme is insecure, as it fails to meet credential privacy and soundness of authentication. An improvement for Chang and Lee scheme is proposed by employing verifiable encryption of RSA signatures.

Index terms: Authentication, Distributed computer networks, Information security, Security analysis, SSO.

I. INTRODUCTION

Identification of a user is an important access control mechanism for client server network architecture. The SSO scheme is a method of access control which allows a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again. Single sign-off is the reverse process whereby a single action of signing out terminates access to multiple software systems.

There are three basic security requirements that should be met by an SSO scheme. They are unforgeability, credential privacy, and soundness. Unforgeability means 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.

As different applications and resources support different authentication mechanisms, SSO has to internally translate to and store different credentials compared to what is used for initial authentication.

The Chang–Lee scheme is an insecure scheme. It presents 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 have free access to the services.

These two attacks imply that the Chang–Lee SSO scheme cannot meet credential privacy and soundness, which are essential requirements for SSO schemes and authentication protocols. Many flaws are identified in their security arguments in order to explain why it is possible to mount the attacks against their scheme. Similar attacks can also be applied to the Hsu–Chuang scheme [9], on which the Chang–Lee scheme is based.

Finally, to avoid these two impersonation attacks, an improved SSO scheme was proposed to enhance the user authentication phase of the

Chang-Lee scheme. To this end, the efficient RSA- based Verifiable Encryption of Signatures (VES) proposed by Ateniese [2] to verifiably and securely encrypt a user"s credential is employed. In fact, Ateniese"s VES was originally introduced to realize fair exchange. COMMON FRAMEWORKS

Open SSO –Open Web SSO

The OpenSSO provides core identity services to simplify the implementation of transparent SSO as a security component in a network infrastructure. OpenSSO provides the foundation for integrating diverse web applications that might typically operate against a disparate set of identity repositories and are hosted on a variety of platforms such as web and application servers. This project is based on the code base of Sun Java System Access Manager, a core identity infrastructure product offered by Sun Microsystems.

JOSSO – Java Open Single Sign-On Project Home

JOSSO is an open source J2EE-based SSO infrastructure aimed to provide a solution for centralized, platform neutral, user authentication and authorization. The framework allows multiple web server/applications such as the Apache HTTP Server, Apache Tomcat, JBOSS, ASP, PHP etc. to authenticate users with credential store. JOSSO communicates with credential stores over the Lightweight Directory Access Protocol (LDAP) or a JDBC connection. JOSSO exposes SSO services using SOAP over HTTP protocol.

SAML SSO Service for Google Apps

Security Assertion Mark-up Language (SAML) is an XML standard that allows secure web domains to exchange user authentication and authorization data. Using SAML, an online service provider can contact a separate online identity provider to authenticate users who are trying to access secure content. Google Apps offers a SAML SSO service that provides partner companies with full control over the authorization and authentication of hosted user accounts that can access web-based applications like Gmail or Google Calendar. Using the SAML model, Google acts as the service provider and provides services such as Gmail and Partner Start Pages (PSP). Google partners act as identity providers and control usernames, passwords and other information used to identify, authenticate and authorize users for web applications that Google hosts.

II. LITERATURE SURVEY

In 2000, Lee and Chang [5] proposed a user identification and key distribution scheme to maintain user anonymity in distributed computer networks. Later, Wu and Hsu [6] pointed out that the Lee-Chang scheme is insecure against both impersonation attacks and identity disclosure attacks. Meanwhile, Yang et al. [7] identified a weakness in the Wu-Hsu scheme and proposed an improvement. In 2006, however, Mangipudi and Katti [8] 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 [9] 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.

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 users and service providers as well as the communication overhead of networks. To tackle this problem, the SSO mechanism has been introduced so that, after obtaining a credential from a trusted authority for a short period say one day, each legal user"s authentication agent can use this single credential to complete authentication on behalf of the user and then 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.

III. PROPOSED WORK

To overcome the flaws in the Chang-Lee scheme [1], an improvement was proposed by employing the RSA-based Verifiable Encryption of Signatures (RSA-VES), which is an efficient primitive introduced in [2] 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) to convince Bob that she has
signed the message and the trusted party can recover the signature from the cipher text. 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

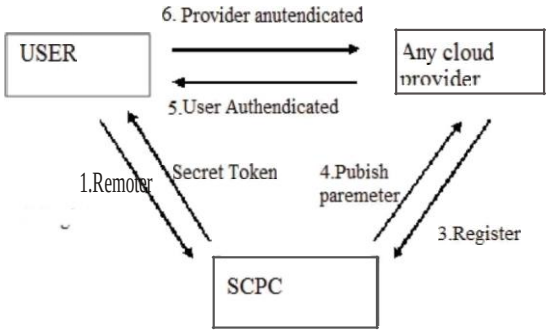


Fig 1. Block Diagram

The proposed scheme consisting of 4 phases

a. Initialization Phase

The user when request for server, to login to server and get service choose the unique identity and sends the ID to the third party server.

The third party selects two prime number p and q. The third party server sets its RSA parameter such as private and public key pair (e,d) where 'e' is prime number. It also generates the prime number for Diffie-Hellman key exchange. Third party also chooses a cryptographic hash function.

b. Registration Phase

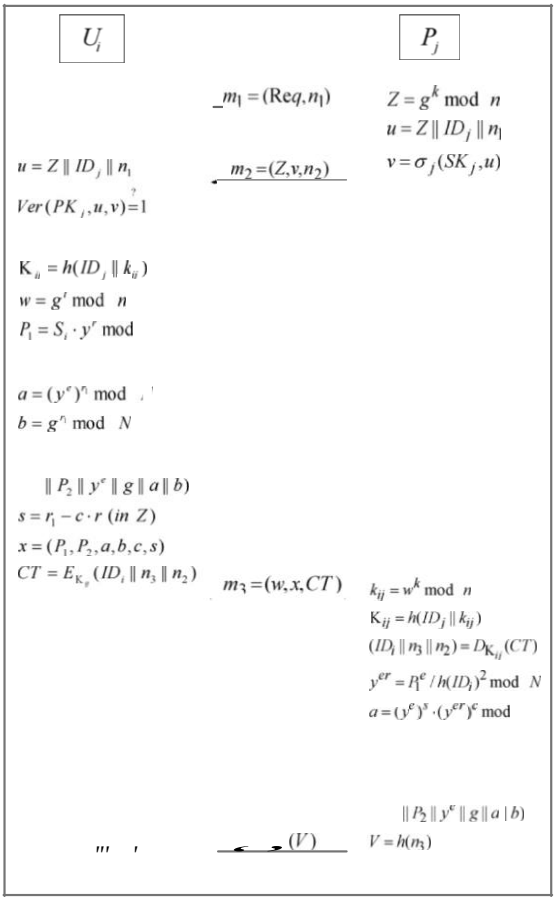
The third party server receives the register request. It then issues a user credential. The user credential is calculated as RSA's signature. Each service provider has unique identity and it should maintain a pair of signing/verifying keys for a secure signature scheme. Verification function is used to verify the signature with the public key.

c. Authentication Phase

In this phase, RSA-VES is employed to authenticate a user, and normal signature is used for service provider authentication.

sends it to Bob, meanwhile, forwards Bob's signature to Alice. Thus, fair exchange is achieved.a signature and then sends the message which contains session key signature, nonce value which is selected by service provider. The client upon receiving the message from service provider terminates the conversation if the verification is failed. Otherwise, the client accepts service provider because the signature is valid. The client selects a random number and generates the session key. The client computes the evidence showing that the credential has encrypted using public key. Finally the client encrypts user's identity, new nonce value and server's nonce using session key to get cipher text.

To verify the client, the service provider uses the session key of the client to decrypt the message sent by client and to recover the client ID, nonce value of client and server. If the verification fails, the service provider aborts the conversation. Otherwise, the service provider accepts the client and believes that they shared the same session key by sending the message to client. After the client receives the verify message from service provider, it checks whether it is equal to nonce value created by client. On successful verification, the client believes that they shared the same session key. Otherwise it terminates the conversation.



The user sends a service request with

nonce to service provider. Upon receiving the request, server calculates its session key and issues Fig 2. RSA VES scheme

d. Encryption and Decryption Phase

Encryption and Decryption between user and provider is ensured using AES algorithm which is more secure than DES and there are currently no known non-brute-force attacks against AES. Data which is send from each provider to user is encrypted and send to the user, then the user decrypts it and the original data is retrieved.

Security Analysis

The security of the improved SSO scheme is analyzed by focusing on the security of the user authentication part, especially soundness and credential privacy due to two reasons. On 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 like user anonymity and session key privacy are preserved, since these properties have been formally proved in [1] and the corresponding parts of the Chang−Lee scheme are kept unchanged.

Soundness requires that without holding valid credential S* corresponding to a target user U*, an attacker, who could be a collusion of users and service providers, has at most a negligible probability of generating proof x* and going through user authentication by impersonating user U*. 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 [2]. Namely, if the user authentication part is not sound, i.e., an attacker can present valid proof x* without holding the corresponding credential S* 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 in [2].

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 [2]. 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 [2].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.

VI. CONCLUSION

There are two effective impersonation attacks on Chang and Lee"s SSO scheme [1].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 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 anon-existent user and then freely access resources and services provided by service providers. An efficient digital verifiable signature scheme based on RSA algorithm can overcome these attacks. In the future work, the open problems are to formally define authentication soundness and construct efficient and provably secure SSO schemes.

REFERENCES

[1] 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.

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

[3] A. C. Weaver and M. W. Condtry, "Distributing internet services tothe network"s edge," IEEE Trans. Ind. Electron., vol. 50, no. 3, pp.404–411, Jun. 2003.

[4] L. Lamport, "Password authentication with insecure communication," Commun. ACM, vol. 24, no. 11, pp. 770–772, Nov. 1981.

[5] W. B. Lee and C. C. Chang, "User identification and key distribution maintaining anonymity for distributed computer networks," Comput.Syst. Sci. Eng., vol. 15, no. 4, pp. 113–116, 2000.

[6] 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.

[7] 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.

[8] 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.

[9] 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.