International Journal For Technological Research In Engineering
Volume 1, Issue 10, June-2014 *ISSN (Online): 2347 - 4718*

ENHANCED SIGNATURE BASED AUTHENTICATION SCHEME FOR DISPENSED NETWORKS

Naik D.C[1] (M-Tech 2nd Year), Dr. Suresh M.B[2]
[1]Department of Computer Network Engineering
[2]Prof & Head, Department Of Information
Science East West Institution of Technology,
Bangalore, India,

Abstract: Single sign-on (SSO) is an authentication mechanism which enables an authorized user with a onetime credential to be authenticated by many service providers in a scattered computer system. This project proposed a SSO mechanics that claimed its certificate by providing well-organized protection arguments. The old SSO system is actually unsafe as it fails to meet credential secrecy and soundness of certification. Specifically, the project presents the following impersonation attacks. The firstly attack allows a vicious service provider, who has successfully communicated with a valid user twice, to recover the user's vicious and then to impersonate the user to access resources and services offered by service provider. In secondly attack, an outsider without any vicious may be able to enjoy network services freely by impersonating any user or a nonexistence user. Project determines the flaws in their protection arguments to explain why attacks are possible against the old SSO scheme. By employing an efficient verifiable encryption of RSA signatures in this SSO mechanism to provide the best security issue.

Keywords: Authentication, Single sign-On, Attacks, Soundness.

I. INTRODUCTION

In the dispensed computer networks, it has become common to allow users to access various network services offered by dispensed service providers [1], [2]. A user certification (also called user identification) [3], [4] plays a important role in dispensed computer networks to verify if a user is effectual and that can be granted access to the services requested by the users. To avoid fake servers, users usually need to authenticate service after reciprocal authentication between the user and the service provider, a session key may be managed to keep the confidentiality of the data exchanged between a user and a service provider [4], [5]. In many assumptions, the anonymity of effectual users must be protected as well [4], [6]. The practice has shown that it is a big challenge to design efficient and secure certification protocols with these security properties in composite computer network systems. It is usually not virtual by asking one user to maintain distinct pairs of identity and password for dissimilar service providers, since this will leads to increase the workload of some users and service providers as well as the communication overload of networks. To undertake this problem, the single sign-on (SSO) mechanism [16] has been brought out so that, after getting a credential from a trusted authority for a short period, each effectual user‟s authentication agent can use this single credential to complete authentication on behalf of the user and then access multiple service providers. The SSO scheme should fill at least three introductory security requirements, i.e., unforgeability, credential privacy and soundness. Unforgeability demands that, except the trusted authority, even a connivance 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 unlisted user without a credential should not be able to access the services proposed by service providers. A standardized concept called the generalized digital certificate (GDC), was proposed in [18] to provide user authentication and key agreement in wireless networks, in which a user, who holds a digital signature of his/her GDC issued by an authority, can authenticate him/herself to a verifier by proving the knowledge of the signature without revealing it. Actually an SSO scheme, has two weaknesses: 1) an outsider can forge a valid credential by mounting a credential forging attack since the existing scheme employed naïve RSA signature without using any hash function to issue a credential for any random identity selected by a user and 2) the existing scheme requires clock synchronization since it uses a time stamp.

Then, the proposed system presented an interesting RSA-based SSO scheme, which does not rely on clock synchronization by using a nonce instead of a time stamp. Their scheme is suitable for mobile devices due to its high efficiency in computation and communication. Finally, they presented a well-organized security analysis to show that their SSO scheme supports secure mutual authentication, session key agreement, and user anonymity. In [17], Han et al. proposed a generic SSO construction which relies on broadcast encryption plus zero knowledge (ZK) proof [20] 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, the 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. The block digram is as shown in the Fig. 1.

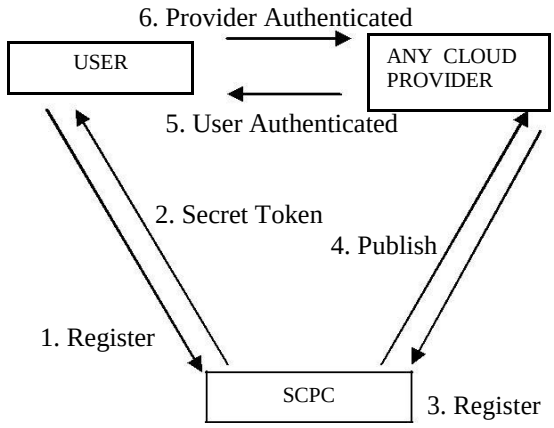

Fig. 1. Block Diagram

In this paper, we show that the existing (Chang–Lee) scheme [19] is actually insecure by presenting two imitation attacks, i.e., credential recovering attack and impersonation attack without credentials. In the first attack, a venomous service provider who has communicated with a effective user twice can successfully recover the user‟s information. Then, the malicious service provider can impersonate the user to approach resources and services provided by other service providers.

The another attack may enable an outside attacker without any valid information to impersonate a legal user or even a nonexistent user to have free access to the services. These two attacks imply that the previous (Chang–Lee) SSO scheme fails to meet credential privacy and soundness, which are essential requirements for SSO schemes and authentication protocols. We also identify the flaws in their security arguments in order to explain why it is possible to mount our attacks against their scheme.

Finally, to avoid these two impersonation attacks, propose an improved SSO scheme to enhance the user authentication phase of the previous scheme. To this end, we employ the efficient RSA-based verifiable encryption of signatures (VES) proposed by Ateniese [21] to verifiably and securely encrypt a user‟s credential. In fact, Ateniese‟s VES was originally introduced to realize fair exchange between the user and the service provider. There are no similar attacks in the setting of SSO and this is also the first time of using VES to design an SSO scheme, to the best of our knowledge.

TABLE I. NOTATIONS

SCPC	Smart Card Producing Center
U_i, P_i	User and Servive Provider respectively
ID_i, ID_i	The unique identity of U_i and P_i 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
$\sigma_i (SK_i , M)$	The signature σ_i on M signed by P_i with signing key SK_i
$Ver (PK_i, M, \sigma_i)$	Verifying signature σ_i on M with public key PK_i
$h (\cdot \quad)$	A given one way hash function
‖	The operation of cancatenation

II. LITERATURE SURVEY

A distributed computer system has the many software elements that are on many computers but run as a single system. The computers which are in a distributed system can be physically associated by a local network or they can be geographically distant and connected by a wide region network. The distributed scheme can consist of whatever number of potential configurations such as, minicomputers, workstations, personal computers and so on. The agenda of distributed computer network is to make such a network work as a single computer and in an distributed computing system can run on hardware that is provided by many sellers and can use a variety of standards based software portions, Such schemes are independent of the fundamental software. They can run on many operating systems and can use different communications protocols.

A. NEED of SSO.

The main object of SSO mechanism is to access users admittance to many applications from one login which allows a unified mechanism to handle the authentication of users and implement business patterns checking user access to applications and data. Sometimes a coherent authentication strategy or a solid authentication framework is missing during the mechanism which leads to a development of applications, each of which comes with their own authentication needs and user repositories. In some situations every user needs to remember multiple usernames and passwords to access different applications in a distributed computer networks. This goes up a huge cost for the administration and support department‟s accounts. The system have to set up in such a way that each application for each employee can be accessed the service from the service provider. Authentication is required across multiple applications, platforms, and infrastructures.

B. Single sign on benefits

- Improved user productivity. Users are no longer have to stuck by multiple logins and they are not required to remember many identity keys and passwords and also that will support personal answer by the requests from the user to reset forgotten password.

- Improved developer productivity. SSO mechanism provides a secure way for the developers with a same authentication framework. Since the Single sign on mechanism is an independent, then programmers don't have to worry about authentication at all. The developers can adopt that once a request from user to the service provider for an application that is attended by a username, then authentication has already taken place.

- Simplified administration. The services which are given by the service provider by the single sign-on mechanism, the administration task is to manage user accounts in simplified way to keep the data. The grade of reduction by the service provider depends on the applications which are used by the user. since SSO only deals with authentication. So, applications which are given by the service provider may still need user specific attributes (such as access privileges) has to be set up by the service provider.

III. PROPOSED IMPROVEMENT

To overcome the flaws in the existing scheme [19], now the paper shows an improved scheme 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 represents three parties such as trusted party and two users say Alice and Bob. The introductory 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 noninteractive zero-knowledge (NZK) proof to convince Bob that she has signed the message and the trusted party can recover the signature from the ciphertext which has send by the Alice. After verifying the proof, Bob can send his signature for the same message to Alice.

Alice should send her signature in plaintext back to Bob after accepting Bob‟s signature, For the purpose of correct exchange between the Alice and Bob. If she refuses to accept the signature, 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, interim, forwards Bob‟s signature to Alice.

Thus, correct exchange is achieved. The basic idea of the improved scheme can be highlighted as follows. User Ui ‟s credential is Si = h (IDi)2d mod N , i.e ., SCPC‟s RSA signature on the square of the hashed user identity (in contrast to Si = h (IDi)d mod N in [19]). For user authentication, Ui will encrypt his/her credential Si using ElGamal encryption of SCPC‟s other public key y = gu by computing A1 = Si · y r mod N and A2 = g r mod N , where g € ZN 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 (A1, A2) does encrypt his/her credential Si (i.e. SCPC‟s RSA signature for IDi), Ui must also provide an NZK proof x to show that he or she knows a secret r such that A1 e / h(IDi) 2 = (y e) r mod N and A2 = g r mod N . Such a proof x , 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 Ui‟s credential Si . 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 existing scheme.

A. Initialization Phase

SCPC selects two large safe primes p and q to set N = pq. Namely there are two primes p‟ and q‟ such that p = 2p‟+1 and q = 2q‟+1. SCPC now sets its RSA public private key pair (e, d) such that ed ≡ 1 mod 2p‟q‟ , where e is a prime. Let QN be the subgroup of squares in ZN whose order #G = p‟q‟ is unknown to the public but its bit-length lG = | N | - 2 is publicly known.

SCPC randomly picks generator g of QN, selects an ELGamal decryption key u, and computes the corresponding public key y = g u mod N. In addition for completing the Diffie-Hellman key exchange SCPC chooses generator g̃ € Z N, where n is another large prime number. SCPC also chooses a cryptographic hash function h(·) : {0, 1}*→ {0, 1}k , where security parameter k satisfies 160 ≤ k ≤ı N ı-1. Another security parameter € > 1 is chosen to control the tightness of the ZK proof [34]. Finally SCPC publishes (e, N, h (·), €, g, y, g̃, n), and keeps (d, u) secret.

B. Registration Phase

In this phase, upon receiving a register request from the user, SCPC gives Ui fixed-length unique identity IDi and issues credential Si = h (IDi) 2d mod N. Si calculates as SCPC‟s RSA signature on h (IDi) 2 is an element of QN, which will be the main group we are calculating. As in [19], each service provider Sj with identity IDj should maintain a pair of signing/verifying keys for a secure signature scheme (not necessarily RSA). σ j (SKj , Msg) denotes the signature σj on message Msg signed by Sj using signing key (SKj). Ver (PKj, Msg , σj)denotes verifying of signature σj with public key PKj , which outputs “1” or “0” to indicating if the signature is legal or illegal, respectively.

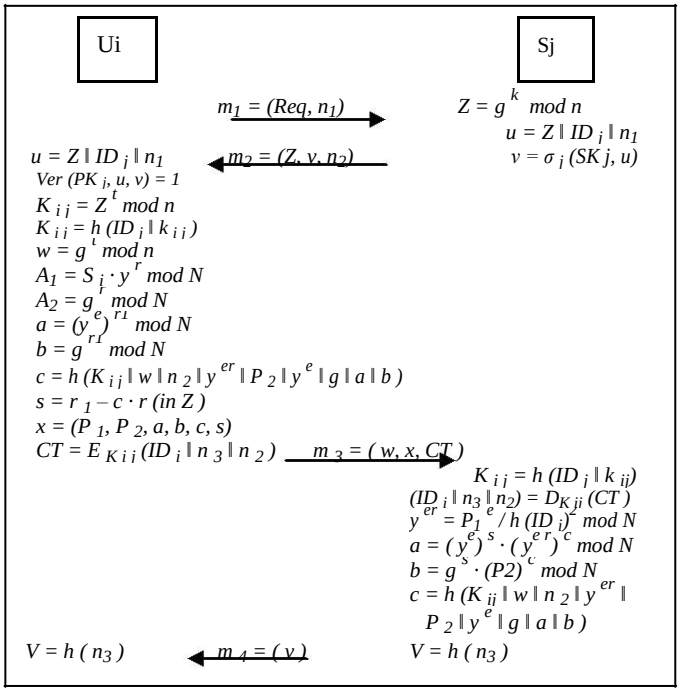

Fig. 3. Authentication phase

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.3. and further explained as follows

- Ui sends a service request with nonce to service provider Sj .
- Upon receiving (Req, n1), Pj calculates its session key material Z = g k mod n where k € Zn* is a random number, sets u = Z ‖ IDj ‖ n1, issues a signature v = σj (SKj ,u), and then sends m2 = (Z, v, n2) to the user, where n2 is a nonce selected by Sj.
- Upon receiving m2 = (Z, v, n2), Ui sets u = Z ‖ IDj ‖ n1 . Ui terminates the conversation if Ver (PKj, u, v) = 0. Otherwise, Ui accepts service provider Sj because the signature v is valid. In this case, Ui selects a random number t € Zn* to compute w = g t mod n, kij = Z t mod n, and the sesson key Kij = h(IDj ‖ kij). For user authentication, Ui first encrypts his/ her credential Si as (A1 = Si · y r mod N, A2 = g r mod N), where r is a random integer with binary length lG. Next Ui computes two commitments a = (y e) r1 mod N and b = g r 1mod N, where r1 € ± {0, 1} € (lG + k) is also a random number. After that, Ui computes the evidence showing that credential Si has been encrypted in (A1, A2) under public key y. For this purpose Ui calculates c = h(kij ‖ w ‖ n2 ‖ yer ‖ A2 ‖ ye ‖ g ‖ a ‖ b) and s = r1 – c · r (in Z). Then x = (A1, A2, a, b, c, s) is the NIZK proof for user authentication. In fact it is precisely the process of generating x which is the proof part of RSA-VES[21]. Finally Ui encrypts his/her identity IDi, new nonce n3 and Pj"s nonce n2 using session key Kij to get ciphertext CT = Ekij (IDi ‖ n3 ‖ n2), and thereafter sends m3 = (w, x, CT) to service provider Pj.
- To verify Ui, Sj calculates kij = w k mod n, the session key Kij = h (IDj ‖ kij), and then uses Kij to decrypt CT and recover (IDi, n3, n2). Then Sj computes y e r = A1 e / h (IDi) 2 mod N, a = (y e) s· (y e r) c mod N, b = g s · P2 c mod N, and checks if (c, s) € {0, 1} k X ± {0, 1} € (lG + k) + 1 and c = h (Kij ‖ w ‖ n2 ‖ ye r ‖ A2 ‖ y e ‖ g ‖ a ‖ b ‖). If the output is negative Sj aborts the conversation. Otherwise Sj accepts Ui and believes that they have shared the same session key kij by sending Ui m4 = (V) where V = h (n3).
- After Ui receives V, he checks if V = h (n3). If this is true, then Ui believes that they have shared the same session key Kij. Otherwise Ui terminates the conversation.

IV. PARAMETERS CONSIDERED FOR BETTER SECURITY

A. Mutual Authentication

Mutual authentication is to establish the agreement between the user and the server, so that the user and the server agree upon a common key known as session key. Let A mean the user, B mean the server, and A, B share a common session key Sk. If there is an Sk such that A believes A←Sk→ B and B believes A ← Sk → B for the transaction, we can say that the mutual authentication is finished between A and B.

B. Session Key Agreement

It is an interactive method in which for two or more parties needs to share some session key in secret. Attributes of key agreement protocols are known session key, At each run of key agreement protocol, user and server should produce a unique secret key and achieves its goal even in face of adversary is successful in achieving the previous session keys. The goal is even if one key compromise at one point should not expose the key of another point. Forward secrecy says that the secrecy of previous session keys is not affected even if long-term secrets of one or more entities are compromised.

C. Password change phase

Password change phase is necessary phase that should be included in the methodology as the user needs to update password so as to agree on a session key with the server through the log-in phase in advance. If user U wants to change his password from PW to PW*, user U inserts the smart card into card reader and keys in ID and PW* then the card reader checks that the user is legitimate user or not, if yes then asks the user to enter new password, then the card reader does the further processing in smart card.

D. Initiator Anonymity

Initiator anonymity says that only the server knows the identity of the user with whom he is interacting. If the Trusted Third Party (TTP) concept is considered, to each access to a service provider a user will use a different temporary identity

to authenticate himself to the TTP and TTP then forwards the users request to service provider.

So, the service provider knows only the temporary identity of the user not the real identity, so in this the user is anonymous to the service provider also.

V. ATTACKS IS TO BE PREVENTED

A. Impersonation Attack

An impersonation attack is an attack in which an adversary successfully assumes the identity of one of the legitimate in a system or in a communication protocol. So, as the identity is obtained the illegal user tries to modify a login request massage, but the illegal user will be unable to acquire the secret key so no modification will be done. In this way impersonation attack can be prevented.

B. Denial of service attack

In a denial of service attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy. There are various measures to prevent this attack, one of them is that in login phase the card reader checks the valid user id and password, so it prevents the attack during this process.

C. Insider attack

The insider attack is when the user‟s password is obtained by the server in the registration phase. Therefore user password should not be known to the server. So, here the trick used to prevent the Insider attack is to use random number that is nonce and send in the massage that is hashed. So the server will be unable to get the user password.

VI. CONCLUSION

Proposed system demonstrates the two effective imitations of attacks on existing single sign-on scheme [19]. The first attack shows that their scheme cannot protect the privacy of a user‟s information and thus, a vicious 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 external attacker without credential to the chance to impersonate even a non-existent user and then freely access resources and services provided by service providers. The paper will also discuss why the existing scheme is not well-organized security arguments are not strong enough to guarantee the security of their SSO scheme. Furthermore, by employing an efficient verifiable encryption of RSA signatures introduced in the proposed system by Ateniese [21], the proposed system is an improved existing 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 [22]. 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. 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] L. Barolli and F. Xhafa, “JXTA-OVERLAY: A P2P platform for distributed,collaborative and ubiquitous computing,” IEEE Trans. Ind. Electron., vol. 58, no. 6, pp. 2163–2172, Oct. 2010.

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

[4] 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.

[5] [5] W. Juang, S. Chen, and H. Liaw, “Robust and efficient password authenticatedkey agreement using smart cards,” IEEE Trans. Ind. Electron., vol. 15, no. 6, pp. 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., vol. 57, no. 2, pp. 793–800, Feb. 2010.

[7] M. Cheminod, A. Pironti, and R. Sisto, “Formal vulnerability analysis of a security system for remote fieldbus access,” IEEE Trans. Ind. Inf., vol. 7, no. 1, pp. 30–40, Feb. 2011.

[8] A. Valenzano, 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.

[9] T.-S.Wu and C.-L. Hsu, “Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks,” Comput. Security, vol. 23, no. 2, pp. 120–125, 2004.

[10] Y. Yang, S. Wang, F. Bao, J. Wang, and R. H. Deng, “New efficient user identification and key distribution scheme providing enhanced security,” Comput. Security, vol. 23, no. 8, pp. 697–704, 2004.

[11] K. V. Mangipudi and R. S. Katti, “A secure identification and key agreement protocol with user anonymity (SIKA),” Comput. Security, vol. 25, no. 6, pp. 420–425, 2006.

[12] C.-L. Hsu and Y.-H. Chuang, “A novel user identification scheme with key distribution preserving user anonymity for distributed computer networks,” Inf. Sci., vol. 179, no. 4, pp. 422–429, 2009.

[13] B.Wang and M. Ma, “A server independent authentication scheme for RFID systems,” IEEE

Trans. Ind. Inf., vol. 8, no. 3, pp. 689–696, Aug. 2012.

[14] B. Fabian, T. Ermakova, and C. Muller, "SHARDIS: A privacy-enhanced discovery service for RFID-based product information," IEEE Trans. Ind. Inf., vol. 8, no. 3, pp. 707–718, Aug. 2012.

[15] H.-M. Sun, Y.-H. Chen, and Y.-H. Lin, "oPass: A user authentication protocol resistant to password stealing and password reuse attacks," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 651–663, Apr. 2012.

[16] ["Security Forumon Single Sign-On," The Open Group[Online].Available: http://www.opengroup.org/security/l2-sso.html

