A SECURE AUTHENTICATION MECHANISM USING SINGLE SIGN ON IN COMPUTER NETWORKS

Thamaraiselvi.R[1], Vidhya.R[2],Nandhinidevi.L [3],Kowsalya.M[4],Somu.M[5]

[1,2,3,4]Department of Computer Science and Engineering
K.S.R College of Engineering,
Tiruchengode, India
[1]thamarai.ksr@gmail.com,
[2]vidhyar55@gmail.com,
[3]nnlnandhu@gmail.com,
[4]kowsalyaksr@gmail.com
[5]somumurugesan@gmail.com

Abstract:

Single Sign On mechanisms allow users to sign on only Once and have their identities automatically verified by each application or service they want to access afterwards .Recently, Chang and Lee suggested a new big plan for Single Sign On and claimed it's protection by providing well-organized security features. In this paper,however, we demonstrated that their plan is actually in secure as it does not meet user's credential privacy and soundness of verifying someone's identity. Here are few practical and Secure Single Sign On models, even though it is a great importance to the current distributed application environments.

Most of the current application requires user to memorize and utilize different set of the credentials (eg, user name / password) for each application they wants to access. However this approach inefficient and insecure with exponential growth in the number of the applications and the services user has to access both inside corporative environments and at internet. More than that, by employing an efficient able to be proven true turning messages into secret code of RSA signature propose by Ateniese,we propose an improvement for repairig the Chang and Lee big plan. This paper shows the Chang and Lee scheme and it aims to enhance the security using AES encryption and decryption.

Key Terms--**Certification, Computer networks, security analysis, single sign-on (SSO).**

I. INTRODUCTION

With the knowledge of computer networks, it has become common to allow users to access various network services offered by dispersed service providers.As a result, the user verifying someone's identity also called User identification [3], [4] plays an extremely important role in the distributed computer networks to check for truth/prove true if a user is legal and can therefore be granted access to the services requested.To avoid fake Servers,users usually need to verify someone's identity service providers .

After back and forth/equal between people (verifying someone's identity), a session key may be negotiated to stay confidentiality of the information changed between a user and a service supplier [4],In many situations,telling someone's name of legal users should be protected additionally [4]. However, the practice has shownthat it is a big challenge to design efficient and secure supportive for someone's identity rules of conduct with security properties in the advanced network environments. But it's sometimes not practical by as king one user to take care of the clear pairs of identity and password for different Service providers, since this could increase the workload of each users and service providers additionally as communication overhead of networks.

To tackle this drawback, the only Single Sign-On mechanism has been introduced in order that, afterobtaining a written document from trustedauthority for a brief period (say one day),a each legal users supportive someone an identity agent can use this single written document to finish supportive someone's identity for the user then access multiple service providers.

In 2000, Lee and Yangtzen[4] projected auser identification and key distribution to maintain user not knowing or telling some one's name in the computer networks. It should meet a Minimum of three basic security requirements, i.e.,unforgeability, written document privacy, and soundness. Unforgeability demands that, except the trusted authority even a valid users and service providers are not ready to produce a valid written document for a new user and written document privacy guarantees that dishonest service providers mustn't be ready to totally recover a user's written document then fake to be the user to log on to other service providers. Soundness means that unregistered user without a written document mustn't be ready toaccess the services offered by service providers.

A similar plan, known as the generalized digital certificate (GDC), to provide user supportive someone's identity and key agreement in wireless networks, during which a user, holds a digital signature of their GDC issued by authority, can verify someone's identity of themself to voucher by proving the data of the signature without showing/telling about it.

II.THE STAGES IN CHANG–LEE SCHEME:

Chang and Lee's proposed remote user authentication theme, supporting secret one- time key institution and user insignificance. In this theme there are 3 phases: checking, key generation,and user recognition phase.In their theme,the RSA cryptosystems initialize a trusted authority, known as a associate SCPC and service providers.The Diffie-Hellman key exchange technique is used to determine Session keys. Within the Chang Lee theme, an every user applies a credentials from the centre authority SCPC, signs associate RSA signature for the user's hashed an identity. After that,it uses a form of dataproof to point out that he/she is in possession of the valid credentials while not revealing his/ her identity to eavesdroppers. Actually, this can be the core plan of user authentication in their theme and explains why their theme fails to realize secure authentication. On the opposite aspect , every maintains it is own RSA key try for doing server authentication.

A. Checking phase

First initialization is carried. The trusty SCPC selects two safe primes. After that, SCPC determines its RSA key specified, where SCPC chooses generator, where ever is additionally an over sized prime quantity. Finally, SCPC publishes, keeps as a secret, and erases straight off once this section has been completed.

B. Key generation phase

ElGamal encryption is probabilistic, meaning that a single plaintext can been encrypted to many possible ciphertexts, with consequence that a general ElGamal encryption produces a expansion in size from plaintext to ciphertext.

Encryption under ElGamal requires twoexponentiations; these exponentiations are independent of the message and can be computed ahead of time if need be.An RSA Public key algorithm is used .It uses two exponents e and d.,where e is public key and d is secret key. By using two large primes p and q.Then n computed as

$$n=p*q$$

If P is plaintext and C is ciphertext means, C is Created by

$$C=P^{e} \bmod n$$

then P decrypted from Ciphertext ,

$$P=C^{d} \bmod n.$$

C. User recognition section

To access the resources of service provider,user needs to go through the authentication protocol. Here, the random integers chosen. Upon receiving a service request message from user, service provider generates and returns user message that is formed up primarily by its RSA signature on. Once this signature is valid, it implies that user has authenticated service provider successfully . Here, is that the temporal Diffie–Hellman key exchange material issued.

Finally, message is utilized to point out that has obtained message correctly, which suggests the success of mutual authentication and session key institution.

III.PROBLEM STATEMENT

As shown above, it appears that Chang Lee SSO theme achieves secure mutual authentication , since server authentication is completed by mistreatment of RSA signature issued by Service supplier. This theme is really not a Secur SSO theme as a result of there are two potential attacks. The primary attack, the“credentialunwell attack”compromises the certificate privacy with in the Chang Lee theme as a malicious service supplier is ready to recover the certificate of a legal user.The opposite attack,associate“impersonation attack while not credentials” demonstrates however outdoor attacker is also able to freely create use of the resources and services offered by service suppliers,since Hacker successfully impersonate legal user while not holding legitmate certificate associate therefore violate the need of soundness for an SSO theme. In reality , these attacks could place each users and repairs suppliers at high risk.

A.CREDENTIAL RECOVERING ATTACK

Intuitively, the Chang Lee SSO theme appears to satisfy the need of certificate privacy since receiving certificate proof, wherever it doesn't enable service supplier to recover user’s certificate by computing. Consequently , beneath the belief malicious service provider has run the Chang–Lee SSO theme with constant user twice, are going to be able to recover’s credential with high probability by discrimination the extended Euclidean rule.

Once with success running the Chang–Lee SSO theme twice with constant user, the malicious service supplier.

B.IMPERSONATION ATTACK

We currently study the soundness of the Chang Lee SSO scheme , that looks satisfy this security necessities as well. The most reason is that to get valid proof. This also implies that if is tiny whole number will even impersonate a non existent user to make use of resources and services offered by service suppliers. Finally, it should be emphasized that impersonation attacks while not valid document seriously isolate the safety of SSO schemes .

As it allows attackers to be with success genuine while not first getting a sound credential from the sure authority when registration.

C.DISCUSSION

In Chang and Lee provided a well-organized security analysis to point out that their SSO theme is secure.However,the two impersonation attacks presented in the previous section mean that their SSO theme is actually not secure.The safety of the Chang Lee SSO theme has been analyzed in 3 completely different ways: 1)BAN logic was wont to show the correctness of the Chang–Lee themes; 2)Informal security arguments got to demonstrate that their scheme will resist some attacks, as well as impersonation attacks;3) A proper security proof was given to prove that their theme is a secure genuinekey. Finally, it must be noted that the analysis higher than shows solely that Chang Lee SSO theme fails to realize secure authentication, without violating its security for achieving user anonymity And session key privacy.

IV.ATTACKS ON THE HSU CHUANG SCHEME

Here, we concisely highlight the difference betwe en the Chang Lee themeand the Hsu Chuang theme to see why the above describe impersonation attacks apply to the present latter yet. The twoschemes have similar structures and use similar notations, however the technical details differ. In summary, the Hsu Chuang theme is differs from the Chang Lee theme in three ways.

First, within the Hsu–Chuang scheme user's credential is a naïve RSA signature signed by the trustworthy party, where is identity elect by him/herself.

Second, to authenticate itself, service provider sends signature, where is that the DH key material generated by , is that the current timestamp, and is identity's.

Finally, for user authentication userproblems and sends proof to,who validate by checking if. The Hsu–Chuang theme is vulnerable to impersonation attack as the associate assaulter can forge a valid credential with respect to identity by merely selecting random and computing.
This attack can be excluded if specific encryption format is required for identities and the credential is issued by mistreatment a secure hash,i.e.,as in the Chang Lee theme. In line with the discussion in Section III,the Hsu Chuang the me remains not secure even with such a step. The reason is that our two attacks against the Chang Lee theme apply to the Hsu- Chuang theme yet.
This suggests that Hsu chuang theme additionally fails to satisfy both written document privacy and soundness of authentication.In addition, there's anotherflaw with in the Hsu Chuang theme.
Assaulter can impersonate service the supplier to cheat legal users, as service authentication is conducted by employing a non traditional RSA signature. By act with twice attacker can get messages and satisfying once can run extended Euclidean algorithm to find two integers and such that in (without knowing the factors of RSA modulus).
Hence,will recover by computing. Afterthat, will impersonate to any legal user byexploitation the worth of issue signature , without knowing RSA private key .

V. PROPOSED IMPROVEMENT

To overcome the failings in the existing system we tend to now show improvement by employing RSA primarily based verifiable encoding of signatures (RSA─VES) which includes three parties: a trustworthy party and two users, say Alice and Bob .

The fundamental plan of VES is that Alice contains a key pair of signature scheme signs given message then encrypts ensuring signature below the trustworthy party's public key,and uses a non interactive zero knowledge (NZK) proof to convince Bob that she has signed the message and therefore the trustworthy party can recover the signature from the ciphertext . When confirmatory the proof, Bob can send his signature for the same message to Alice. For the aim of fair exchange, Alice should send her signature in plaintext to Bob when acceptingBob's signature.If she refuse to do thus, even so, Bob can get her signature from the trustworthy party by providing Alice's encrypted signature and his own the signature, so that the trustworthy party can recover Alice's signature and sends it to Bob meanwhile, forwards Bob's signature to Alice. Thus, fair exchange is achieved.

For user authentication, can cipher their credential using ElGamal encryption of SCPC's alternative public key by the computing and ,where of big order and is SCPC's secret coding key . In this improvement, SCPC also plays the role of the trust authority in VES.

A. INITIALIZATION PHASE

SCPC selects two large safe primes and to set.Namely, there are two primes and such that and SCPC now sets its RSA public or private key pair such that,where is a primary every which way picks generator of, selects an ElGamal decipherment key,computes corresponding public key .

Additionally, for finishing Diffie Hellman key exchange SCPC choose the generator where is another large prime.SCPC additionally chooses cryptographic hash function, where security parameter satisfies. Another security parameter is chosen to control the tightness of the ZK proof Finally, SCPC publishes, and keepssecret.

B.REGISTRATION PHASE

In this phase, upon receiving a register request, SCPC gives fixed length Distinctive identity calculated as SCPC's RSA signature which is a component of,which canbe A in the group we tend to scheming. Each service providerwith the identity should maintain a pair of signing/verifying keys for a secure signature scheme(not necessarily RSA). It denotes the signature on message signed by using sign language key denotes verificatory of signature with public keywhich outputs "1" or "0" to indicating if the signature is valid or invalid, severally.

C.AUTHENTICATION PHASE

In this phase, RSA VES is utilized to demonstrate a user, where as traditional signature is used for service supplier authentication. First user sends a service request with nonce to service supplier.Second upon receiving and calculates it is session key material where is a random number, sets a signature and then sends to the user, where is a nonce designated by.Otherwise, accepts service provider because the signature is valid.During this case, selects a random range to computes and the session key.For user authentication initial encrypts his/her credential as where is a random integer with binary length.

Next, Computes two commitments and,where is additionally a random range. After that, computes the proof showing that credential has been encrypted in under public key.

For this purpose, calculates and then the NIZK proof for user authentication. In fact, it's exactly, the process of generating which is that the proof a part of RSA-VES.

Finally, encrypts his/her identity, new nonce, and 's nonce using session key. Signature activity implies that associate offender cannot extract a signature from VES with out help from the user encryptedt he signature or the trusted authority can decode a VES.So, if this improved SSO scheme fails to meet document privacy,it implies that Ateniese's RSA-VES fails to satisfy signature activity.

In fact, soundness and signature activity are the two core security properties to guarantee the fairness of digital signature exchange using VES.

VI.CONCLUSION

In this paper, we have a tendency to demonstrated two attacks on Chang and Lee's Single Sign On (SSO) scheme. The first attack shows that their scheme cannot shield privacy of a user's document and thus a spiteful service supplier can act as a legal user in order to relish resources and the services from different serviceproviders and the second attack can be effects the soundness of authentication by giving an out door offender without document the prospect to impersonate even a non existent user to freely access resources. We have a tendency to also mentioned why their well-organized the security arguments don't seem to be robust enough to guarantee the safety of their SSO scheme. As future work,it's interesting to formally define Authentication Soundness construct efficient and incontrovertibly 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 additional analysis is critical to an investigate the maturity of this model and study however the safety of the improved SSO scheme proposed in this paper can be formally well-tried.

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, "JXTAOVERLAY: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.770772, Nov.1981. IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL.9,NO.1,FEBRUARY 2013

[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]. Bellare and P. Rogaway, “Entity authentication and key distribution,”in *Proc. of CRYPTO’*, 1993, pp. 232–249.

[6] C. Boyd and W. Mao, “On a limitation of BAN Logic,” in *Proc. Of EUROCRYPT*, 1994, pp. 240–247.

[7] N. Asokan, V. Shoup, and M. Waidner, “Optimistic fair exchange of digital signatures,” *IEEE J. Sel. Areas Commun.*, vol. 18, no. 4, pp. 591–606, Apr. 2000.