International Journal of Engineering Technology, Management and Applied Sciences

IJETMAS

www.ijetmas.com March 2015, Volume 3, Issue 3, ISSN 2349-4476

Single sign on mechanism using M-RSA-VES for network security

Amruta Nerlekar
BE.IT Pune university

Pradnya Janrao
BE.IT Pune university

Ankita Patil
BE.IT Pune university

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. Chang and Lee proposed a new SSO scheme and provided well-organized security arguments. Their scheme is actually insecure as it fails to meet credential privacy and soundness of authentication. We present two impersonation attacks. We identify the faults in their security arguments to explain why attacks are possible against their SSO scheme. By employing an efficient verifiable encryption of RSA signatures, we propose an improvement for repairing the Chang–Lee scheme. To overcome this problem we are modifying RSA VES algorithm and increasing security, efficiency and decreasing time of execution.
keywords— distributed computer networks,,Authentication,information security,security analysis

I.INTRODUCTION

With the wide 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 (also called 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 both authentication session key may benegotiated to keep the confidentiality of the data exchanged betweena user and a service provider However, practice has shown that it is a big challenge to designefficient and secure authentication protocols with these security properties in complex computer network environments.

II.EXISTING SYSTEM

Chang and Lee proposed a new SSO scheme and claimed its security by providing well-organized security. In this paper we demonstrative that their scheme is actually insecure as it fails to meet credential privacy and soundness of authentication. we present two impersonation attacks,first attack allows a malicious service provider, who has successfully communicated with a legal user,to recover the user's credential and then to impersonate the user to access resources and services offered by other service providers. In second attack, an outsider without any credential may be able to enjoy network services freely by impersonating any legal user or a illegal user.

III.ADVANTAGES

1. Reduce password related headache
2. Using SSO system user does not need to enter a password for different service

www.ijetmas.com March 2015, Volume 3, Issue 3, ISSN 2349-4476

providers, user can access all service providers with entering only one password.

3. Lower IT security risk

4. Keeping all technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal system.

5. Increase employee productivity

6. Unsafe user behavior can leave sensitive corporate information behind on public machine, easily accessible to curious outsider. To protect from such access SSO can be used.

IV . PROPOSED SYSTEM

propose an improvement by employing an RSA-based verifiable encryption of signatures (RSA-VES), which is an efficient primitive introduced for realising fair exchange of RSA signatures. VES comprises three parties: a trusted party and two users, say Alice and Bob. The 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, 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 cipher text. After checking the proof, Bob can send his signature for the same message to Alice. For the purpose of fair exchange, Alice need to send her signature in plaintext back to Bob after accepting Bob's signature. If she refuses to do so,Bob can get her signature from the trusted party by providing Alice's encrypted signature and his own signature, so the trusted party can recover Alice's signature and sends it to Bob,forwards Bob's signature to Alice so fair exchange is achieved.

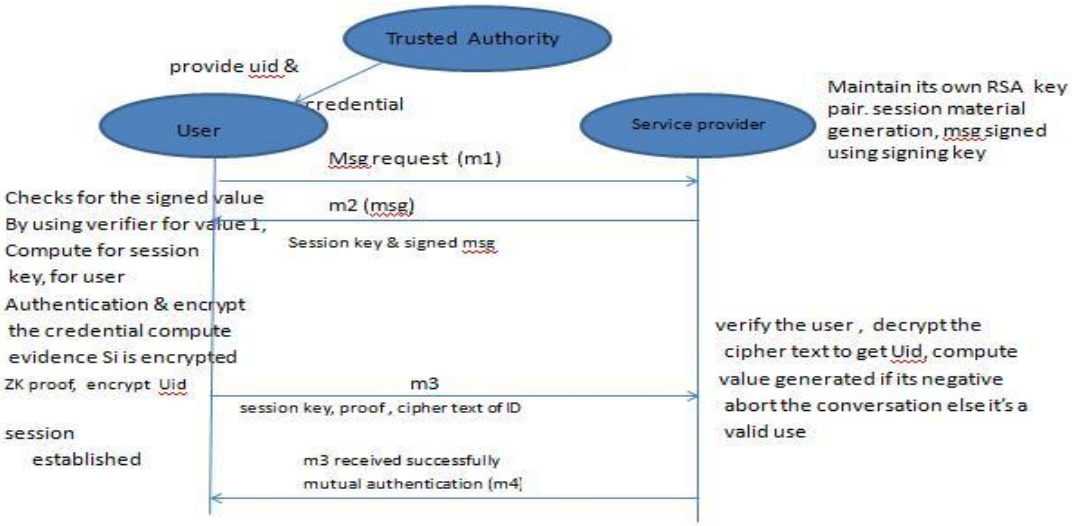


Fig: Propose improvement

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 2 ′ ′ , where e is a prime. Let be the subgroup of squares in $\mathbb{Z}^*$ whose order #G=p'q' is unknown to the public but its bit-length $\mathcal{J}$ = | | − 2 is publicly known.

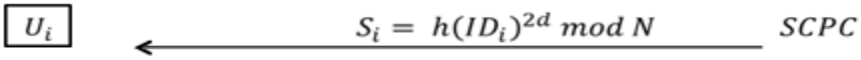
www.ijetmas.com March 2015, Volume 3, Issue 3, ISSN 2349-4476

SCPC randomly picks generator of , selects an ElGamal decryption key u, and computes the corresponding public key = . In addition, for completing the Diffie -Hellman key exchange SCPC chooses generator , ∈ $\mathbb{Z}^*$ where n is another large prime number. SCPC also chooses a cryptographic hash function $h(.)$: $\{0,1\}^* \rightarrow \{0,1\}$, where security parameter k satisfies 160≤ ≤ | | − 1

. Another security parameter > 1 is chosen to control the tightness of the ZK proof [14]. Finally, SCPC publishes (, , $h(.)$, , , , ,) and keeps (d,u) secret.

Registration Phase

In this phase, upon receiving a register request, SCPC gives Ui fixed-length unique identity IDi and issues credential Si=$h(IDi)$ $2dmod\ N$, Si calculated as SCPC's RSA signature on $h(IDi)$ $d$is an element of QN, which will be the main group we are calculating.



Each service provider P_j keeps a pair of signing/verifying keys for a secure signature scheme.

$\sigma_j(SK_j, Msg)$: signature σ_j on message Msg
$Ver(PK_j, Msg, \sigma_j)$: verifying of signature σ_j

Fig .1.1. Registration Phase of Proposed Scheme.

As each service provider Pj with identity IDj should maintain a pair of signing/verifying keys for a secure signature scheme (not necessarily RSA).$\sigma j(SKj,Msg)$ denotes the signature σj on message Msg signed by Pj using signing key SKj. $Ver(PK$槓$,Msg, \sigma j)$ denotes verifying of signature σj with public key PKj , which outputs "1" or "0" to indicating if the signature is valid or invalid, respectively.

Authentication Phase

.

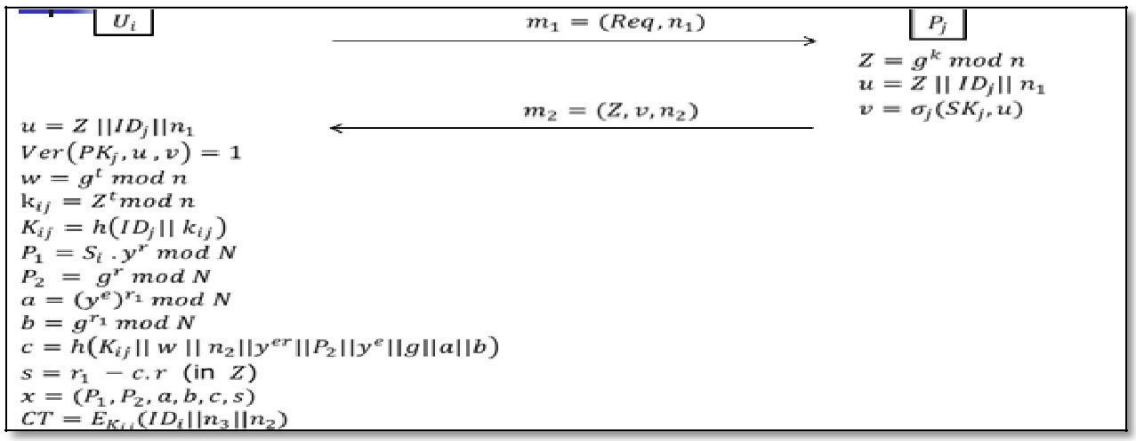


Fig.1.2(a).Proposed Scheme

IJETMAS
www.ijetmas.com March 2015, Volume 3, Issue 3, ISSN 2349-4476

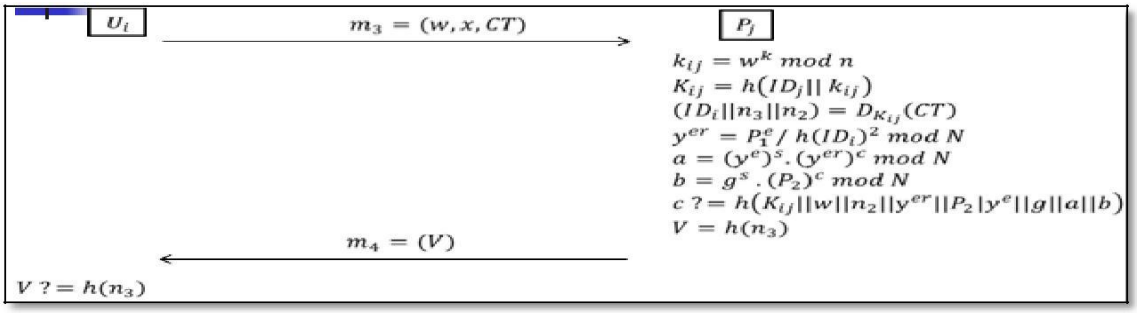


Fig.1.2(b). Proposed Scheme

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. 1.2(a) and 1.2(b) further explained as follows.

1) Ui sends a service request with nonce $n1$ to service provider Pj .

2) Upon receiving(Req, $n1$), Pj calculates its session key material Z=$gt \bmod n$ where $k \epsilon \mathbb{Z}N*$ is a random number, sets u=Z|| IDj ||$n1$, issues a signature v=$\sigma j(SK㈱,u)$, and then sends $m2$=(Z,v,$n2$) to the user, where $n2$ is a nonce selected by Pj.

3) 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 Pj because the signature v is valid. In this case, Ui selects a random number $t \epsilon \mathbb{Z}N*$ to compute , w=$gt \bmod n$,kij=$Zt \bmod n$ and the session key Kij=h(IDj||kij) . For user authentication, Ui first encrypts his/her credential Si as ($P1$=$Si.yr \bmod N$,$P2$=$gr \bmod N$), where r is a random integer with binary length . Next, Ui computes two commitments =(ye) $r1 mod\ N\ and\ b$=$gr1 mod\ N$, where $r1\epsilon\pm\{0,1\}$ $\epsilon(\iota g+k)$is also random number. After that, Ui computes the evidence showing that credential Si has been encrypted in($P1$,$P2$) under public key y . For this purpose, Ui calculates c=h(Kij||w||$n2$||yer||$P2$||ye||g||a||b) and =$r1-c.r$. Then, x=($P1$,$P2$,a,b,c,s) is the NIZK proof for user authentication. In fact, it is precisely, the processes 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 there after sends $m3$=(w,x,CT)to service provider.

4) To verify Ui , Pjcalculates kij=$wk \bmod n$ the session key Kij=h(IDj||kij) , and then uses Kij to decrypt CT and recover (IDi||$n3$ ||$n2$). Then, Pj computes ,yer=$P1eh(IDi)$ $2\diagup \bmod N$,a=(ye) s.(yer) $cmod\ N$,b=$gs.P2c$ mod N, and checks if (c,s)ϵ\{0,1\} $k\times\pm$\{0,1\} $\epsilon(\mathcal{J}G+k)$+1 and c=h(Kij||w||$n2$||yer||$P2$||ye||g||a||b). If the output is negative , Pj aborts the conversation. Otherwise, Pj accepts Ui and believes that they have shared the same session key Kij by sending Ui $m4$=(V) where V=h($n3$).

5) 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.

www.ijetmas.com March 2015, Volume 3, Issue 3, ISSN 2349-4476

V. OBJECTIVES

1. More secure than RSA-VES
2. More efficient
3. Requires less time execution
4. Recovering attacks

VI. ARCHITECTURE OF SYSTEM

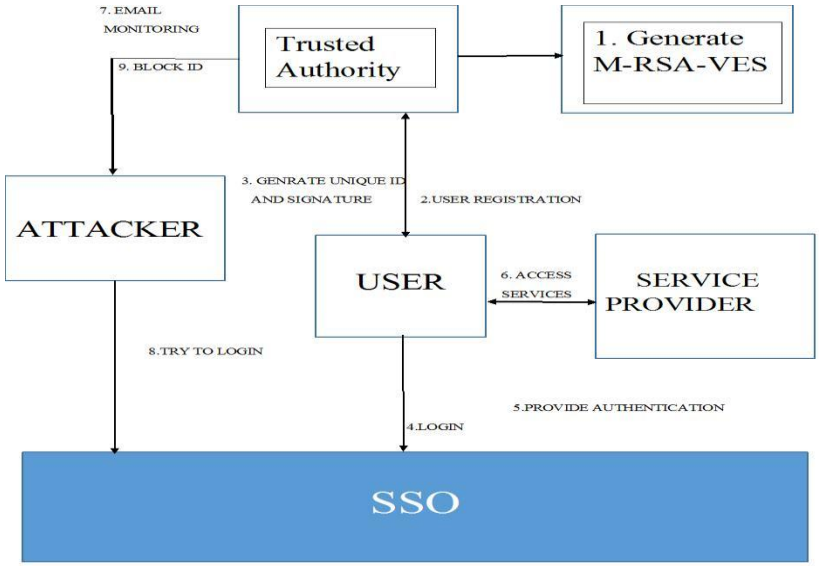


Fig:Architucture of Sysyem

The single sign-on (SSO) mechanism has been introduced so that, after obtaining a credential from a trusted authority for a short period, 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.

1.Credential recovery attack

In this 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.

2.Impersonation Attack:

In this 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.

3.Smart card producing center:

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 Diffie–Hellman key

exchange technique is employed toestablish 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.

VI .FUTURE SCOPE

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 by employing an efficient verifiable encryption of RSA signatures.we propose an improvement for repairing the Chang–Lee scheme.

VII.CONCLUSION

In this paper, we demonstrated two effective impersonationattacks on Chang and Lee's single sign-on scheme,first attack shows that their scheme cannot protect theprivacy of a user's credential, and thus, a malicious serviceprovider can impersonate a legal user in order to enjoy theresources and services from other service providers. The second attack violates the soundness of authentication by giving anoutside attacker without credential the chance to impersonateeven a non-existent user and then freely access resources andservices provided by service providers.. In addition,we explained why Hsu and Chuang's scheme is also vulnerable to these attacks.

Furthermore, by employing anefficient verifiable encryption of RSA signatures,we proposed an improved Chang–Lee scheme to achieve soundness and credential privacy. As future work, itis interesting to formally define authentication soundness andconstruct efficient and provably secure single sign-on schemes.Based on the draft of this work , a preliminary formalmodel addressing the soundness of SSO has beenproposed in.

REFERENCES

[1].W.Juang,S.Chen,andH.Liaw,"Robustandefficient password authenticated key agreement using smart cards," IEEE Trans. Ind. Elec-tron., vol. 15, no. 6, pp. 2551–2556, Jun. 2008.

[2]. X. Li,W. Qiu, D. Zheng, K. Chen, and J. Li, "Anonymity enhancement on robust and efficient password-authenticated key agreement usingsmart cards," IEEE Trans. Ind. Electron., vol. 57, no. 2, pp. 793–800 Feb. 2010.

[3]. 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.

[4]. L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications," IEEE Trans. Wireless Commun., vol. 10, no. 7, pp. 2372–2379, Jul. 2011.

[5]. J. Yu, G.Wang, and Y.Mu, "Provably secure single sign-on scheme indistributed systems and networks," in Proc. 11th IEEE TrustCom, Jun.2012, pp. 271–278.

www.ijetmas.com March 2015, Volume 3, Issue 3, ISSN 2349-4476

[6]. B.Wang and M. Ma, "A server independent authentication scheme fo RFID systems," IEEE Trans. Ind. Inf., vol. 8, no. 3, pp. 689– 696, Aug 2012.

[7]. 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.

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

[9]. D. Boneh, "Twenty years of attacks on the RSA cryptosystem," Notices Amer. Math. Soc., vol. 46, no. 2, pp. 203–213, 1999.

[10]. Y. Xu, R. Song, L. Korba, L.Wang,W. Shen, and S. Y. T. Lang, "Distributed device networks with security constraints," IEEE Trans. Ind. Inf., vol. 1, no. 4, pp. 217–225, Nov. 2005.