IOSR IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. II (Mar-Apr. 2014), PP 80-86
www.iosrjournals.org

Soundness to Single Sign on Using OTP in Distributed Networks

Miss. Bhavana M. Bahikar, Prof. Praveen R. Barapatre
Department of computer engineering SKN-SITS, Lonavala
Asst. Prof., Department of Information Technology SKN-SITS, Lonavala

Abstract: *In a distributed system, there are numerous service provider. The user must be authenticated to entrance the services provided by the service provider. It is challenging to recall all secret words for users. So to clarify this problem single sign on is used which is an authentication contrivance in that permit a single license to be validated by multiple service provider. The Wang, Yu, and Qi Xie find that Chang – Lee Scheme undergoes from two attacks one of which is that the aggressor is outside service provider converses with the authenticated user twice and get the license necessary to right to use data in distributed systems. The second attack is the outsider easily receiving right to use to, use services without any license by mimicking authenticate user. This violence also associated with Hsu and Chang Scheme. To sidestep these attacks Wang, Yu, and Qi Xie employed RSA-VES. For enhancement and soundness of authentication, this paper services One Time Password to Wang, Yu, and Qi Xie Method. Now a days OTP plays important role in an authentication, so that using OTP for secure single sign on its easy to provide soundness for authentication.*

Index Terms:*Authentication, RSA-VES, distributed system, Security, Single Sign On(SSO),One Time Password(OTP).*

I. Introduction

In computer network, interchange information firmly between two users is a challenging task because there are probabilities that fraud users or service provider may enter into the system to use services without any license. To exchange information securely authentication is required. Authentication is the vital activity in the distributed system and fair exchange between two user and service provider. After mutual authentication, the next step is that we have to generate a session key for the privacy of data exchange by two users and also the service provider so that data can be sent on unsecure channelsecurely. It is difficult to design authentication because there are many chances of fraud users or service providers can generate duplicate license to right to use data in a distributed system.

In a distributed system, there are a number of service providers so that to right to use those service users must have authentication. And it is difficult for users to remember those secret words and also these increased overhead for the system. So that to reduce overhead as well as to reduce human efforts to remember all those secret words, there is an authentication mechanism called as SSO, SSO scheme allows single identity and secret word to right to use multiple services in the distributed system no need to create different identity and secret word for each service provider so that it reduces the overhead. There are three necessary requirements for SSO authentication, which require to be fulfill as unforgeability which means that user and service provider cannot forge a license for new user the right to forge new user is provided to only trusted authority. The another requirement is that license privacy means that unapproved users cannot recover all the license and mimic user to write to use services from different service provider by communicating with the approved user, and the last but not the least requirement is soundness it deals with only approved user able to write to use services provided by service provider it means an unapproved user cannot right to use services without any license [14]. These requirements indicate that SSO can work with the uniqueness and secret word, there is no need to keep different secret words for different service provider means using a single identity a user can right to use all approved services in the distributed system. To converse on a distributed system securely there is need of authentication that means users interacting are the intended user and also service provider is also authenticated that it should not be a fraud service provider then only we can establish a secure connection to share secret information in insecure channel. There is need of a third party, we can say that trusted party which has authority to provide licenses to the users and service providers so that when we want to converse we can verify that users and service provider are approved or not. It helps to find fraud users or service providers because the only main party has the power to add new user or new service provider.

The Chang –Lee scheme uses the secure SSO mechanism and they applied the RSA

algorithm to fair exchange of data, but these schemes are suffering from the certificate recovering attack that is when any unapproved service provider can converse with the approved user without any license twice or more than that then the service provider is able to recover a license. After getting authority to an unapproved service provider can forge a number of unapproved users. The second attack is an impersonation attack without any certificate, it indicates that any unapproved user without any license can be able to right to use the services provided by service provider this attack is applicable to Chang –Lee which is proven by Wang, Yu, and Qi Xie and they employed efficient verifiable encryption RSA signature to improve Change- Lee Scheme in soundness and certificate privacy. The Hsu and Chang scheme are also suffering from the certificate recovering attack and impersonation attack without any certificate. In this paper proposed that adding One Time Password to Wang, Yu, and Qi Xie so that it can provide soundness for authentication.

A one-time password (OTP) is the one in which secret word is valid for only for one login session if we want to login again we need new OTP. OTP is better than (static) secret words and there is no necessity to recall the secret word every time or create a new secret word for different service again and again. OTP is not vulnerable to replay attack because we cannot use the same secret word for new login so if anyone try to use the same secret word then session rejected. No one misuses OTP because it varies for each login it never valid for long duration. OTPs are very hard to learn by heart for human beings. One Time Password generation algorithms typically make use of uncertainty that is OTP is generated randomly there is no need of physical interaction. This is helpful otherwise anyone guesses future OTPs by noticing previous OTPs and can get right to use for the session.

Different methods for the generation of OTPs are given as:

- By using time-synchronization in-between the service provider and the users providing the secret word (it is valid only for a short period of time)
- By using a mathematical algorithm to create a new secret word which can be done by using previous secret words (These are effectively a chain and must be used in a predefined order).
- By using a mathematical algorithm where the new secret word is generated by a challenge (e.g., A random number chosen by the service provider) and/or using a counter.

The RSA algorithm is used for secure message between users. RSA algorithm deals with key generation, encryption and decryption are given as-

1. Choose two prime numbers p and q. For security purposes, the p and q should be chosen at random, and should be of similar bit-length.

2. n = pq. n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

5. Find d as $d^{-1} \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo φ(n)). d is kept as the private key exponent.

Plain Text (PT)

Cipher Text (CT)

6. $CT=(PT)^e \bmod n$
7. $PT=(CT)^d \bmod n$

NOTATIONS TABLE

SR. No.	Notation	Meaning
1	SCPC	Smart Card Producing Center, which is a trusted authority
2	Ui, Pj	User provider and Service provider
3	IDu, IDp	Identity of user and service provider
4	ei, di	Public/private key pair of RSA encryption, decryption algorithm of identity i.
5	Si	User (Ui) certificate, provide by SCPC
6	Sx	Long term private key of SCPC
7	Sy	Public key of SCPC

8	EK(P)	A symmetric key encryption of plain text P using key K
9	DK(C)	A symmetric key decryption of cipher text C using key K
10	σj(SKj,P)	The signature σj on P signed by Pj with signing key SKj
11	Ver(PKj,P,σj)	Verifying signature σj on P with public key PKj
12	h(·)	Used for One way Hash function
13	||	Used for concatenation

II. Literature Survey

In 2000, Lee and Chang [3] proposed a user identification scheme and also key distribution conserving user obscurity in distributed systems, for authentication it is necessary to identify users who are capable to right to use the services provided by a service provider, and, Lee and Chang are one who take steps just before user identification. The factoring problem and one way hash function is based of Security of the scheme. The service providers can only the one who acknowledged the approved user and able to establish a session key with, approved user, these all things is handled by the security scheme. One more thing that scheme does not need to

3. Compute $\varphi(n) = \varphi(p) \times \varphi(q) = (p-1)(q-1)$, where φ is Euler's quotient function.

4. Select an integer *e* such that $1 < e < \varphi(n)$ and $ed = 1 \bmod \varphi(n)$ is released as the public key exponent.

create secret word table. Afterward, in 2004, Wu and Hsu [6] find that the Lee–Chang's scheme is affected by a masquerade attack which deal with the banned user has assumed legal user identity and can right to use data which is that legal user is approved. In masquerade service provider can be masqueraded to interchange a session key with a user so unapproved service provider can take authorization so it will easily add the unapproved users in the system. Wu and Hsu make changes in Change-Lee scheme that is refining efficient user identification scheme and also key distribution. In 2004, Yang et al. [7] Prove that Wu-Hsu's scheme has some drawback so Yang et al. Make improvement in the Wu – Hsu scheme by adding more security requirement.

Later, in 2006 Mangipudi and Katti [8] have find out that Yang et al.'s scheme is affected by a denial of service attack in which unapproved user can continuously send packet to the server so that server will blocked and approved user cannot able to right to use the services provided by the service provider. To improve such a DoS attack, Mangipudi and Katti further proposed a secure identification and key agreement protocol with user anonymity (SIKA). In 2009 Hsu and Chuang [9] find that both Yang et al.'s and Mangipudi–Katti's scheme can be affected by identity disclosure attack any outsider user can easily crack the identity of the approved user and proposed an improvement in Yang et al.'s and Mangipudi–Katti's scheme. In 2012 Chang – Lee [13], proposed secure single sign-on mechanism using RSA, which allow mobile users to use the single identity and secret word to right to use multiple services in the distributed system. There is no need to create different identity and secret word for every service provider with one identity and secret word can right to use to multiple services called as SSO.

In 2013 Wang, Yu, and Qi Xie [15] find drawback in Change-Lee Scheme that it is affected by certificate recovering attacks and impersonation attack without certificate also they improve it by adding soundness and certificate privacy.

REVIEW OF WANG, YU, AND QI XIE SCHEME

To improve the Chang-Lee scheme Wang [13], Yu, and Qi Xie [15] design an RSA-based verifiable encryption of signatures (RSA-VES), which is used to secure exchange of RSA signatures and provide soundness and certificate privacy. The working of VES includes three parameters a SCPC and two users we can say u1 and u2. When u1 want to send message to u2 it first encrypt message with SCPC's public key and send message to u2. Then u2 again directs the same message back to u1, so u2 send same message to m2 this for protected communication. Then u2 gets u1 key from SCPC or u1 itself. This process is for secure communication. The algorithm is given as:

A. Initialization Phase

SCPC (Smart Card Producing Centre) selects two large safe primes p and q to set N = p X q. Then, there are two primes p' and q' such that p = 2p' + 1 and q = 2q' + 1. SCPC has two sets its RSA public/private key pair (e, d) such that e X d = 1 mod 2p'q', where e is a prime use for encryption and decryption. Let QN be the subgroup of squares in Ƶ*N whose order #G = p'q' is unknown to public but its bit length lG = |N| - 2 is publically known. SCPC randomly choose generator g of QN, choose an ElGamal decryption key u, and calculate the equivalent public key $y = g^u \bmod N$. To do the Diffie-Hellman key give-and-take SCPC selects generator $\bar{g} \in Ƶ^* N$, where n is a new large prime number. SCPC also select a cryptographic hash function $h(\cdot) : \{0,1\}^K$, where security parameter $\epsilon > 1$ is chosen to control the tightness of the ZK proof. Finally, SCPC publishes (e, N, h(·), ϵ, g, y, $\bar{g}$, n), and keeps (d, u) secret.

B. Registration Phase:

In registration, after receiving a request, SCPC provide Ui fixed-length unique identity IDi also issues certificate $Si = h(IDi)^{2d} \bmod N$. SCPC's RSA signature on $h(IDi)^2$ is a method to compute Si, which is an element of QN, which will be the main thing we computed.

In Chang –lee Scheme, for every service provider, Pj whose identity IDj has to preserve a pair of signing keys which is required for a secure signature scheme (not necessarily RSA). σj(SKj, P) indicate that the signature σj on plain text signed by Pj using signing key SKj. Ver(PKj, P,σj) indicate that verifying of signature σj with public key PKj, gives outputs as "1" or "0" to understand that signature is valid or not.

C. Authentication Phase

In authentication phase, using RSA-VES, we authenticate the user and for service provider uses signature for authentication. In detail it is given as,

I. User Ui request to the service provider Pj with nonce n1.

II. After getting request (Req,n1) to service provider Pj, Pj has to calculate the session key $Z=g^k \bmod n$ where k is a random number and $K \in Ƶ$, sets u = Z || IDj || n, then send message m2 to user as m2 = (Z, v, n2) where n2 is nonce2 set by service provider Pj, after issuing signature v = σj(SKj, u).

III. Here Ui get the message m2 from Pj, and sets u = Z || IDj || n. Ui stop communication if Ver(PKj, u ,v) = 0 cause signature is invalid. In other case Ver(PKj, u ,v) ≠ 0 Ui accept the request, then Ui select random number $t \in Ƶ^* n$ and compute $w = g^t \bmod n$, $kij = Z^t \bmod n$, Kij = h(Idj || kij) which is a session key. The user authentication process is that user encrypt message(certificate) Si that is $P1 = si.y^r \bmod N$, $p2 = g^r \bmod N$, where r is with binary length l and r is any random integer number. Then Ui calculate $a = (y^e)^{r1} \bmod N$ and $b = g^{r1} \bmod N$ where a & b are the commitments, in that r1 is random integer given as $r1 \in \pm\{0,1\}^{\epsilon (lG+k)}$. Later on Ui calculate the evidence by proving that Si (certificate) is encrypted (P1,P2) with public key y. For that Ui compute c = h(Kij || w || n2 || y^{er} || P2 || y^e || g || a || b) ,

S = r1 – c.r(in Ƶ). After that, user authentication proof for NIZK is x= (P1, P2, a, b, c, s). At last Ui send encrypted message to Pj as m3 = (w, x, CT) where $CT = E_{Kij}$ (IDi || n3 || n2) where n3 is new nonce with user identity and n2 is Pj's nonce with key.

IV. For verification process compute $kij = w^k \bmod n$, from these we can calculate session key as Kij = (IDj || kij), after that using this session key to decrypt CT we can recover PT as (IDi, n3, n2). Also the Pj calculate

$y^{er} = P1^e / h(IDi)^2 \bmod N$, $a= (y^e)^s . (y^{er})^c \bmod N$, $b = g^s . P2^c \bmod N$, then verify that if $(c,s) \in \{0,1\}^k \quad X \pm \{0,1\}^{\epsilon (lG+k)+1}$, c = h(Kij || w || n2 || y^{er} || P2 || y^e || g || a || b) is satisfied or not, if result is non- negative indicate that Pi and Ui shared same session key Kij so confirm request sending message to Ui as m4= (V) here V = h(n3), otherwise communication stop if value is negative.

V. Ui receives m4 from Pj then Ui verify message if he found that it is right message means that they shared samesession key Kij otherwise Ui stop communication.

III. Proposed System

- *HMAC*(*K*,*C*) = SHA1(*K* ⊕ 0x5c5c… ‖ SHA1(*K* ⊕ 0x3636… ‖ *C*)) be an HMAC calculatedwith the SHA-1 cryptographic hash algorithm
- *Truncate* is a function that selects 4 bytes from the result of the HMAC in a defined manner

Then HOTP(*K*,*C*) is mathematically defined by

HOTP(*K*,*C*) = *Truncate*(*HMAC*(*K*,*C*)) &

0x7FFFFFFF

The mask is to disregard the most significant bit to provide better interoperability between processors

For HOTP being useful for an individual to input to a system, the result must be transformed into a HOTP value, a 6–8 digit number that is As Wang, Yu, and Qi Xie [15] work on soundness and certificate privacy of SSO requirement, but still the scheme required reliability for validation to secure SSO. So for this paper proposed work is to provide authentication reliability to make a secure SSO strong which is possible using One Time Password.

Validation is the first step for a secure communication so it is necessary to provide strong validation, so that unapproved user cannot rip-off the certificate from approved user and can able to right to use the services. To provide strong authentication One Time Password is helpful cause it never generate same secret word and secret word is sent to the approved user so that illegal user cannot right to use data. There is a different method of One Time Password this paper uses timestamp method that is used counter, which decrement when secret word is sent to user if user is logging in that period then only he/she can right to use the facilities otherwise session terminated.

The algorithm is given as follows: implementation dependent.

HOTP-Value = HOTP(*K*,*C*) mod 10^d, where *d* is the desired number of digits

In the above algorithm HMAC and SHA algorithm is used to compare OTP sent and received from client are same or not.

TOTP and HOTP are two variables. TOTP is based on HOTP where timestamp substitutes the incrementing counter. The current timestamp is turned into a time-counter by defining the start of an epoch (T0) and counting in units of a time step (TS). For example, TC = (unixtime(now) - unixtime(T0)) / TS

TOTP = HOTP (SecretKey, TimeCounter), where HOTP is defined below.

TOTP-Value = TOTP(*K*,*TC*) mod 10^d, where *d* is the desired number of digits

Let:

- K be a secret key
- C be a counter

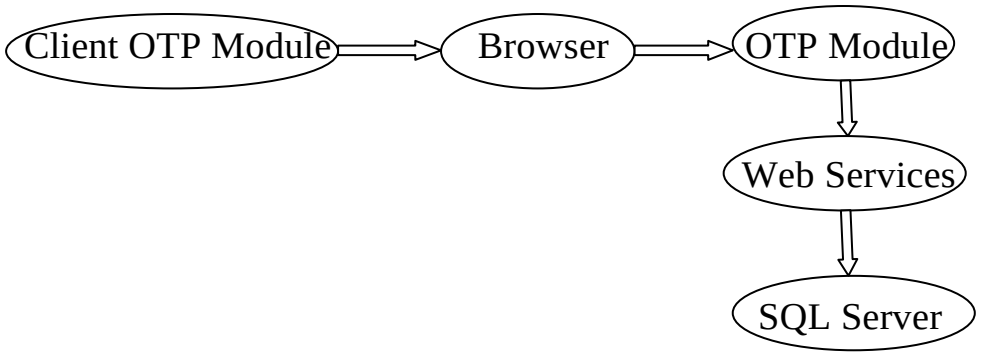

Figure 1: Flow of System

Figure 1 shows the flow of the system in which first part is a Client OTP generator which will generate an OTP and send to the client and wait for limited timestamp. The borrower is the interface between the

user and the client. Next is the OTP module this module is the one which check that whether the enter OTP and sent OTP are the same or not in that timestamp if it is true then only the client get right to use to the web services otherwise period rejected. And the SQL server is used for the storage purpose.

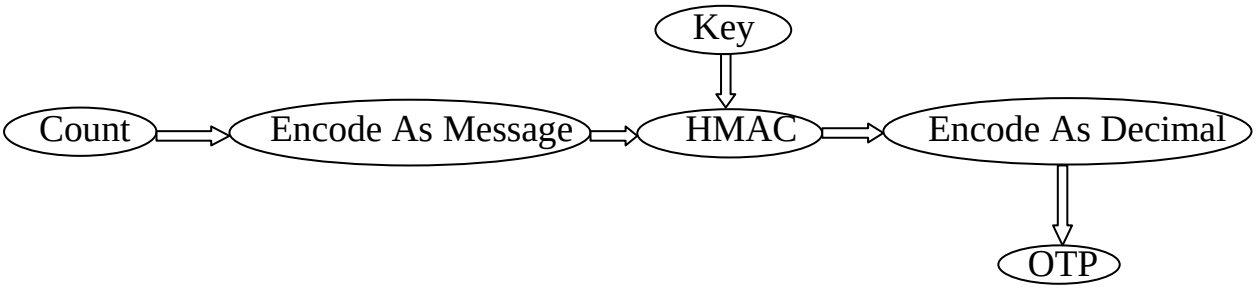

Figure 2: OTP generation

Figure 2 shows that one counter is set for the OTP which casually generate a number. Because of OTP is valid only for a small duration of time and if in that duration OTP doesn't enter then the session is rejected. So first initialize the counter, then encrypts the message using HMAC and the key that message is again encoded with decimal from which we get the OTP.

This paper uses the algorithm for key selection for HMAC. In Fig: OTP generation is given as algorithm they first check that the size of the key and the block size/ message size are the same or not if it is not same then we have equalized the key to block size if it is less than a block size, then by adding more zero to the key if is greater than block size then it is shortened to block size. And then apply the HMAC algorithm.

MATHEMATICAL MODEL

Let ,
O : One Time Password S : Single Sign On
D : Distributed System SP : Service provider
SP = {SP1, SP2, SP3, SP4,…..SPn)
L : Login credential
L = {L1, L2, L3, L4,……Ln}
In Distributed system there are no. of service provider so that,
. . . .
SPn=Ln

Which is difficult to remember to avoid this paper uses Single Sign On.
Therefore, SP1=SP2=SP3=SP4=……=SPn = S
But still SSO cannot provide complete soundness to authentication it required some extra security,

SP1=SP2=SP3=SP4=……=SPn = O(S)

The above equation provide soundness to authentication.
D = nSP

Each service provider can have separate login credential it can be represented as,
SP1= L1
SP2= L2
. . . .
SPn= Ln

Which is difficult to remember to avoid this paper uses Single Sign On.
Therefore, SP1=SP2=SP3=SP4=……=SPn = S
But still SSO cannot provide complete soundness to authentication it required some extra security,

SP1=SP2=SP3=SP4=……=SPn = O(S)

The above equation provide soundness to authentication.

IV. Conclusion

This paper offers soundness to the authentication which is crucial in Wang, Yu, and Qi Xie scheme because they only offer soundness and certificate privacy to their scheme which need more safety for certification. The Wang, Yu, and Qi Xie scheme uses RSA-VES algorithm which improve the Chang – Lee scheme by providing user certificate privacy. But for assuring the validation some extra technique is needed. For that One Time Password is used with SSO. This paper explains how the security can be upgraded using One Time Password. OTP can valid only for tiny period of time, so that any new user or invader if try to use the old secret word then the operation is terminated. In this way One Time Password provide reliability for the authentication.

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. Lamport, "Secret word authentication with insecure communication," Commun. ACM, vol. 24, no. 11, pp. 770–772, Nov. 1981.
[3] W. B. Lee and C. C. Chang, "User identification and key distribution maintaining anonymity for distributed systems," Comput. Syst. Sci. Eng., vol. 15, no. 4, pp. 113–116, 2000.
[4] W. Juang, S. Chen, and H. Liaw, "Robust and efficient secret word authenticated key agreement using smart cards," IEEE Trans. Ind. Electron., vol. 15, no. 6, pp. 2551–2556, Jun. 2008.
[5] X. Li,W. Qiu, D. Zheng, K. Chen, and J. Li, "Anonymity enhancement on robust and efficient secret word-authenticated key agreement using smart cards," IEEE Trans. Ind. Electron., vol. 57, no. 2, pp. 793–800, Feb. 2010.
[6] T.-S.Wu and C.-L. Hsu, "Efficient user identification scheme with key distribution preserving anonymity for distributed systems," Comput. Security, vol. 23, no. 2, pp. 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, Vol. 23, No. 8, pp. 697-704, 2004.
[8] 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.
[9] C.-L. Hsu and Y.-H. Chuang, "A novel user identification scheme with key distribution preserving user anonymity for distributed systems," Inf. Sci., Vol. 179, No. 4, pp. 422-429, 2009.
[10] H.-M. Sun, Y.-H. Chen, and Y.-H. Lin, "oPass: A user authentication protocol resistant to secret word stealing and secret word reuse attacks," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 651–663, Apr. 2012.
[11] "Security Forumon Single Sign-On," TheOpenGroup [Online].Available:http://www.opengroup.org/security/l2-sso.htm
[12] J. Han, Y. Mu, W. Susilo, and J. Yan, "A generic construction of dynamic single sign-on wit strong security," in Proc. SecureComm', 2010, pp. 181–198, Springer.
[13] C.-C. Chang and C.-Y. Lee, "A secure single sign-on mechanism for distributed systems", IEEE Trans. Ind. Electron., vol. 59, no. 1, pp. 629–637, Jan. 2012.
[14] G. Ateniese, "Verifiable encryption of digital signatures and applications," ACM Trans. Inf. Syst. Secur., vol. 7, no. 1, pp. 1–20, 2004.
[15] Guilin Wang, Jiangshan Yu, and Qui Xie,"Security Analysis of a SSO mechanism for Distributed systems", IEEE Trans. In industrial informatics, vol.9, no.1,Feb.2013