International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Single Sign-on Secure Password Mechanism for Distributed Computer Networks

Deepali M. Devkate[1], N. D. Kale[2]

ME Student, Department of Computer Engineering, PVPIT, Bavdhan, Pune, Savitribai Phule Pune University, Pune, Maharashtra, India

Assistant Professor, Department of Computer Engineering, PVPIT, Bavdhan, Pune,
Savitribai Phule Pune University, Pune, Maharashtra, India

Abstract: ***Single sign-on mechanism is an authentication mechanism in which user sign on only once but their identities verified by many services they want to access later. Practically, it happens that if you wish to access any service then identification of user is an important task. So first you have to register for that service then you become authenticated user. Suppose you want to access many services then you have to create different set of credentials and memorize it. But in proposed system user need only one credential to access many services in distributed computer network. In existing system two types of attacks are found .i.e. impersonation attack and session attack. In impersonation attack , a bogus service provider is able to hack up the credential of authorized user. In session attack, an unauthorized user is able to enjoy the resources and services accessible by service providers. In proposed research work, credential privacy and soundness is protected. By using Diffie-Hellman Key Exchange and Elliptic curve Encryption Algorithm authentication is secure.***

Keywords: Credential privacy, soundness, diffie-hellman key exchange, elliptic curve cryptography.

1. Introduction

Single sign on mechanism is an authentication mechanism in which user sign on only once but their identities verified by many services they want to access later. Practically, it happens that if you wish to access any service then identification of user is an important task. So first you have to register for that service then you become authenticated user. Suppose you want to access many services then you have to create different set of credentials and memorize it. But in proposed system user need only one credential to access many services in distributed computer network. In existing system two types of attacks are found .i.e. impersonation attack and session attack. In impersonation attack ,a bogus service provider is able to hack up the credential of authorized user. In session attack, an unauthorized user is able to enjoy the resources and services accessible by service providers. In proposed research work, credential privacy and soundness is protected. By using Diffie-Hellman Key Exchange and Elliptic curve Encryption Algorithm authentication is secure.

2. Related Work

A. Initialization

1. Select two large prime p and q and calculate N=p*q
2. Determine key pair (e, d), ed= 1 mod Φ(N)
   a.Where , Φ(N)=(p-1)*(q-1)
3. Select generator g over fields Z*n
   a.Where, n is large odd prime number
4. Protect d, and publish (e, g, n, N).

B. Registration

1. After request of user U_i SCPC gives ID_i to user and $S_i = h(ID_i)^{2d} \bmod N$

2. As user Service provider is also register to SCPC and each Service Provider P_j with the identity ID_j maintain key pairs of signing and verifying keys.
   a. $\sigma_j(SK_j, msg)$ signing key,
   b. $Ver(PK_j, msg, \sigma_j)$ verifying key.

Output is 0 or 1, signature is invalid or valid respectively.

C. Authentication

1. User U_i send request to Service provider P_j. $msg1(req, n1)$
2. P_j calculate its session key $Z = g^k \bmod n$
3. Set $u = Z||ID_j||\ n1$ and issue $v = \sigma_j(SK_j, u)$.
4. P_j send msg to U_i. $msg2(Z, v, n2)$
5. User sets $u = (Z||ID_j||n1)$ and verify $Ver(PK_j, u, v) = 0$ if output is 0 signature is invalid user terminate conversation or accept signature of P_j.
6. User select random number r and calculate w, k_{ij}, K_{ij}.
   Where, $w = g^r \bmod n.\ , k_{ij} = Z^r \bmod n., K_{ij} = h(ID_j||k_{ij})$
7. For authentication user encrypt signature S_i.
   $P_1 = S_i \cdot y^r \bmod N$ and $P_2 = g^r \bmod N$. Where r is random integer with fixed length.
8. Then user calculate two commitment
   $a = (y^e)^{r1} \bmod N$
   $b = g^{r1} \bmod N.$
9. For NIZK proof calculate.
   $c = h(K_{ij}||w||n2||y^{er}||P_2||y^e||g||a||b)$
   $s = r1 - c \cdot r$
   Then $x = (P_1, P_2, a, b, c, s)$
10. User encrypt his ID_i , new nonce $n3$, $P_j's$ nonce using session key K_{ij}.
    a..Cipher text $C = E_{K_{ij}}(ID_i||n2||n3)$.
11. U_i send msg to P_j. $msg3(w, x, C)$.

12. P_j decrypt cipher text received by user and recover $(ID_i||n2||n3)$

13 .And compute $y^{er} = \frac{P_1{}^s}{h(ID_i)^2 mod} N$

$a = (y^e)^s \cdot (y^{er})^c mod\ N$

$b = g^s \cdot P_2{}^c mod\ N$

14.P_j verify $(c,s) \in \{0,1\}^k \times \pm\{0,1\}^{\in(l_c+k)+1}$. if output is negative terminate conversation otherwise accept msg to user with nonce $V = h(n3)$.

15.$msg4(v)$ *to user.*

16. User check $V = h(n3)$.*true or not* . if true then proceed otherwise terminate conversation.

3. Mathematical Model

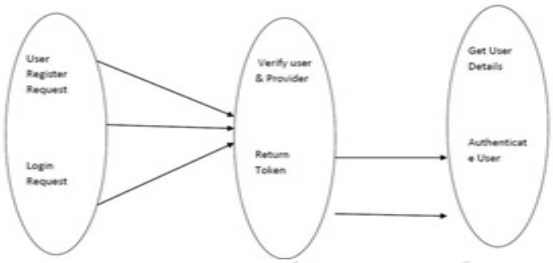

Figure 1: Mathematical Model

Since,
Input= {Fm}
Output= {Fma}
Success Condition,
{Fm} = NULL
Failure Condition
{Fm} = NULL U represent the set of users as clients
U= {u1,u2, u3. un}
These are the RSA keys and signatures
Keys= {pubkey, prikey, sign}
These are the services
S= {s1, s2,s3.sn}
SCPC publish parameters
publishParams ={e, N, h(.),g ,y, g, n}
SCPC secrete parameters
NonPub = {d, u}
When SCPC communicate with client ans service
Sends= {publishParams, Keys}

4. Results

Following snapshot shows the homepage of proposed system. When any new user wants to login, first he have to register his information. Then he became authenticated user. In case of already registered user he can access services which he wants through single-sign on.

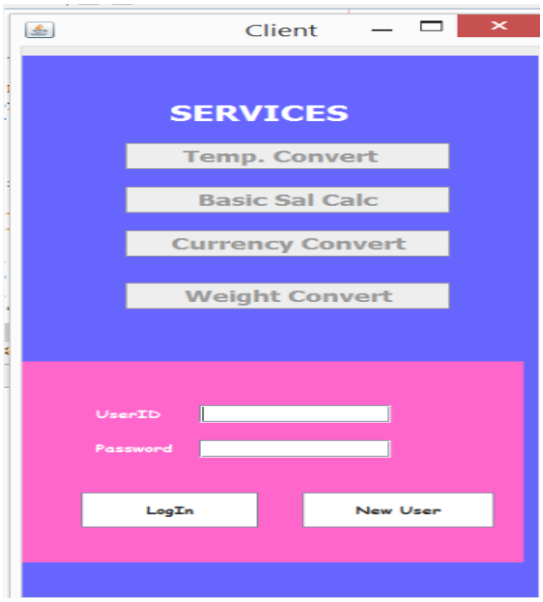

Figure 2: Snapshot of homepage

When user sign in and access any service then that service opens for the user. Following fig. shows the snapshot for that service.

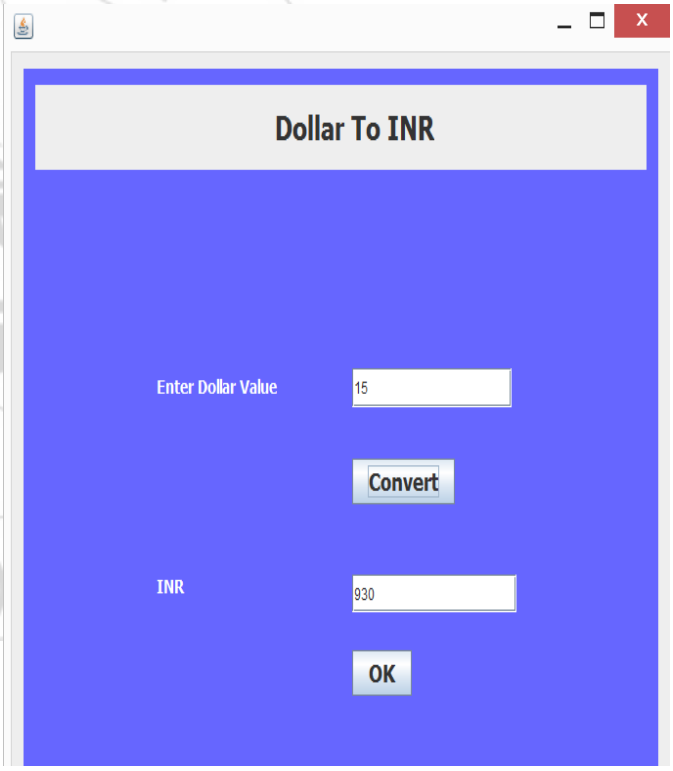

Figure 3:Snapshot of service

4.1 Result Analysis

When we analyse the time required for ECC algorithm for encryption and decryption as compared to other algorithms. We observed that ECC algorithm takes less time.(time taken in milliseconds).

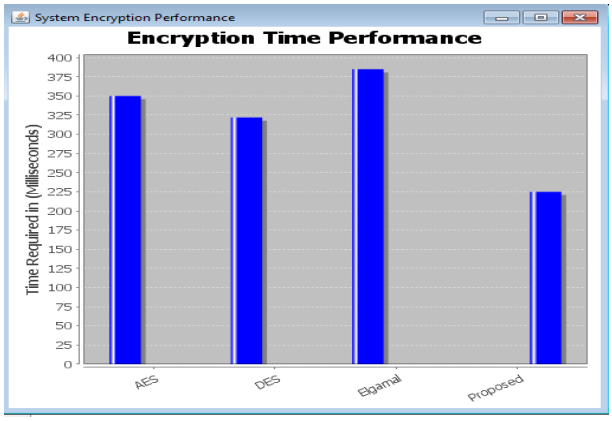

Figure 4 : Comparison of time required for encryption

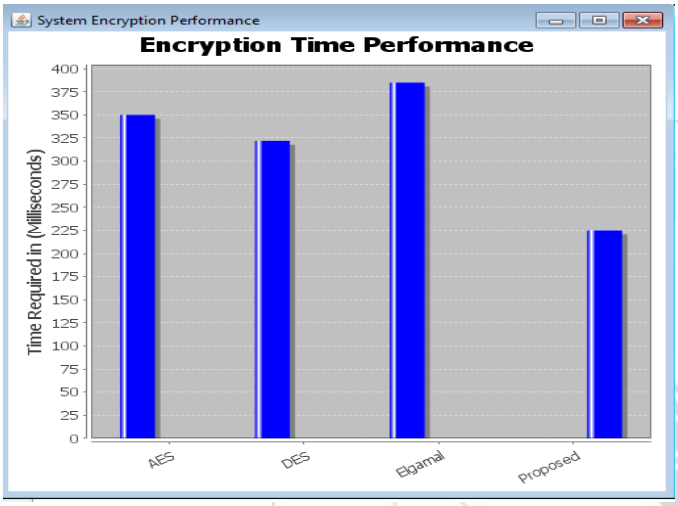

Figure 4: Comparison of time required for decryption

5. Conclusion

In this paper, we validated two effective impersonation attacks on Chang and Lees SSO scheme [19]. The first attack shows that their proposed scheme cannot preserve the privacy of a users credential, Therefore, a malicious service provider can imitate a legal user in order to enjoy the resources and services from other service providers. The second attack interrupts the soundness of authentication by giving an outside attacker without credential the chance to impersonate even a unreal user and then easily access resources and services provided by service providers. We also debated why their well-organized security arguments are not strong enough to assurance the security of their SSO scheme. In addition, we clarified why Hsu and Chuangs scheme is also vulnerable to these attacks. Also, by employing an efficient verifiable encryption of RSA signatures introduced by Atenies, we proposed an upgraded Chang Lee scheme to achieve soundness and credential privacy. As future work, it is stimulating to formally define authentication soundness and construct efficient and provably secure single sign-on schemes. Based on the draft of this work, a initial formal model addressing the soundness of SSO has been proposed. Further research is essential to inspect 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] Guilin Wang , Jiang Yu and Qi Xie ,Security analysis of a single sign-on scheme for distributed computer networks ,IEEE Transactions on Industrial Informatics, Vol. 9, No. 1, February 2013
[2] C. Ramkrishnan, S. Dhanabal, Security analysis of a single sign-on scheme for distributed computer networks, IOSR Journal of Computer Engineering (IOSR-JCE), vol. 16, pp146-149,June 2014
[3] Jean Jacob, Mary John , Security enhancement of a single sign-on scheme for distributed computer networks ,IJMER, vol. 3, pp-1811- 1814, June 2013
[4] 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. 793800, Feb. 2010.
[5] W. Juang, S. Chen, and H. Liaw, Robust and efficient password authenticated key agreement using smart cards, IEEE Trans. Ind. Electron., vol. 15, no. 6, pp. 25512556, Jun.2008.
[6] M. Cheminod, A. Pironti, and R. Sisto, Formal vulnerability analysis of a security system for remote field bus access, IEEE Trans. Ind. Inf., vol. 7, no. 1, pp. 3040, Feb. 2011
[7] A. Valenzano, L. Durante, and M. Cheminod, Review of security issues in industrial networks, IEEE Trans. Ind. Inf., vol. PP, no. 99, 2012]
[8] A. C. Weaver and M. W. Condtry, Distributing internet services to the networks edge, IEEE Trans. Ind. Electron., vol. 50, no. 3, pp. 404411, Jun. 2003
[9] A. C. Weaver and M. W. Condtry, Distributing internet services to the networks edge, IEEE Trans. Ind. Electron., vol. 50, no. 3, pp. 404 411, Jun. 2003.
[10] Xun Yi, San Ling and Huaxiong Wang, Efficient Two-server Password only authenticated key exchange, IEEE transactions on parallel and distributed systems, vol. 24, no. 9, Sep 2013.
[11] Basel Alomair, RadhaPoovendran, Senior Member, IEEE, Efficient Authentication for Mobile and Pervasive Computing, IEEE transactions on mobile computing, vol. 13, March 2014
[12] PawaniPorambage, Corinna Schmitt, Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications IEEE, 2014.
[13] Sanjeet Kumar, Nayak, SubasishMohapatra, BanshidharMajhi An Improved Mutual Authentication Framework for Cloud Computing International Journal of Computer Applications, Volume-5, August 2012.
[14] S. Bhuvanesh, L. Anita Elizabeth, Improving Service Credibility in Password Authentication Peer Service, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, May- 2014.
[15] Jonathan Katz, Philip MacKenzie, Two-server password-only authenticated key exchange, 2011, Elsevier.