Single Sign-on Secure Password Mechanism for Distributed Computer Networks

Deepali M. Devkate¹, N. D. Kale²

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).

B. Registration
1. After request of user U, SCPC gives ID to user and
   \[ S = h(ID)^{2^a} \mod N \]
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. \( a_j \) (SK, msg) signing key,
   b. \( V \) (PK, msg, a_j) verifying key.

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

C. Authentication
1. User \( U \) send request to Service provider \( P_j \) msg1(req, n1)
2. \( P_j \) calculate its session key \[ Z = g^a \mod n \]
3. Set \( u = Z || ID_j || n1 \) and issue \( v = a_j (SK_j, u) \)
4. \( P_j \) send msg to \( U \) msg2(Z, v, n2)
5. User sets \( u = (Z || ID_j || n1) \) and verify \( V (PK_j, u, v) \) if output is 0 signature is invalid user terminate conversation or accept signature of \( P_j \).
6. User select random number \( t \) and calculate \( w, k_{ij}, K_{ij} \)
   Where, \( w = g^t \mod n \), \( k_{ij} = Z^m \mod n \), \( K_{ij} = h(ID_j || k_{ij}) \)
7. For authentication user encrypt signature \( S_t \)
   \[ R_t = S_t \cdot y^t \mod N \]
8. Then user calculate two commitment
   a. \( (y^t)^{r^2} \mod N \)
   b. \( g^{r^2} \mod N \)
9. For NIZK proof calculate,
   \[ c = h(K_{ij} || w || n2 || y^t || P_j || y_i || g || a || b) \]
   \[ s = r1 - c \cdot r \]
   Then \( x = (P_j, P_r, c, b, c.s) \)
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. \( U \) send msg to \( P_j \) msg3(w, x, c).


www.ijsr.net

Paper ID: SUB156557

Licensed Under Creative Commons Attribution CC BY
12. $P_j$ decrypt cipher text received by user and recover 
\[(ID_2)[n2][n3]\]
13. And compute $y^{er} = \frac{P_j^e}{(ID_2^{mod\ N}}$
\[a = (y^{er})^x \mod N\]
\[b = g^a \cdot P_j^{mod\ N}\]
14. $P_j$ verify $(c.s) \in \{0,1\}^k \times \pm \{0,1\}^k \cdot (c,s) + k + 1$ if output is 
   negative terminate conversation otherwise accept msg to user 
   with nonce $V = h(n3)$
15. $msg4(x)$ 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](image1)

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](image2)

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).
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 user’s 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 outsider attacker without credential the chance to impersonate even a real 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 assure the security of their SSO scheme. In addition, we clarified why Hsu and Chuang’s 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 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