ADVANCED MECHANISM FOR SINGLE SIGN-ON FOR DISTRIBUTED COMPUTER NETWORKS

Niranjan Reddy Kurelli

Student, Dept. of I.T., VNR Vignana Jyothi Institute of Engineering and Technology, Bachupally, Hyderabad, Telangana India.
niranjan.6k6@gmail.com

Abstract

A distributed computer networks could be a special form of the network that facilitates the purchasers to use completely different network services that is provided by the service suppliers. Within the distributed computer networks, user verification is a crucial method for the protection. Within the verification, the choice is taken whether the user is legal or not and then enabled the users to access the service. In general users are using multiple usernames and passwords for to access different applications on a distributed computer network. This increase the burden of the user and organization administrator as each and every account of the organization is going to be handled with their explicit username and credential. A new certification plan that is named as single sign-on mechanism that facilitates the users with one identity token to be verified by multiple service suppliers. Single sign-on is one of user authentication method that allows a user to enter one name and identity token so as to access multiple applications. The method authenticates the user for all the applications they have been offered access to and eliminates additional prompts after they switch applications throughout a specific session.
However, existing approaches which are utilizing single sign-on scheme have some drawbacks relating to security needs. Thus, through this paper, we will discuss regarding the event of security from earlier stage to present stage. And clearly discuss regarding the authentication steps between user and service supplier.

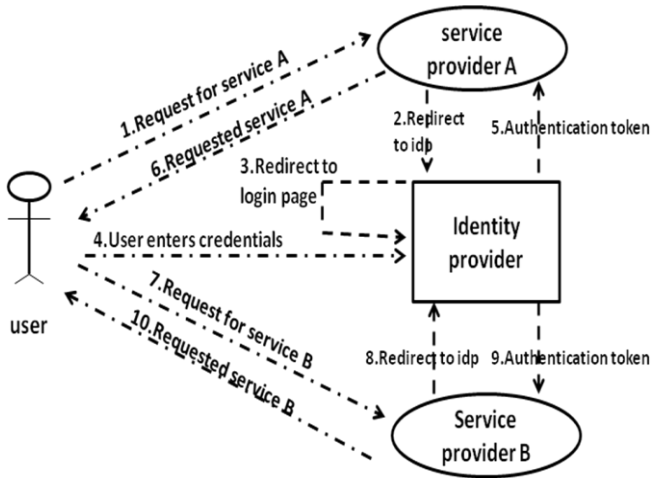
Keywords — *single sign-on, authentication token , mutual authentication*

----------***----------

1. INTRODUCTION

User authentication is a major part in distributed networks to confirm the user is legitimate or not and can in this way allow access to conveyed service suppliers [3]. To keep away from illicit user access to the services we require strong user verification [1], [2]. In addition to the user authentication, service supplier authentication is additionally vital to avoid bogus servers. After finishing of the client and the service supplier check, a session key is given to keep up the confidentiality of the information interchanged between a user and a service supplier. After common confirmation between the user and the service supplier, a symmetric key ought to be arranged to keep the protection of the information is interchanged [2] between user and service supplier, [3], and [4]. It is complex to store and remember the password with user identity token which is required to access to authorized services in the network. Consequently, Single sign-on mechanism was proposed so that user with single certification can be authenticated by numerous service suppliers. Single sign-on mechanism ought to meet two essential security necessities that are, certification protection and soundness. Certification protection ensures that any service supplier ought not have the capacity to completely recover user confidential information from that certificate and afterward imitate the user to login other services on which user has access. Soundness implies that an unregistered client ought not have the capacity to get to the services gave by the service suppliers [5]. This paper intends to give the upgraded security from the past stage to the present stage.

Verifiable a distributed computer network has been gained from domains that go about as autonomous security areas. These domains include singular stages with related working framework and applications. These domains go about as free spaces as in an end-client needs to recognize and validate himself autonomously to each of the areas with which he wishes to collaborate. From the administration point of view, this methodology obliges autonomous administration of every area and the utilization of different client account administration interfaces. Contemplations of both use and security offer ascent to a need to co-ordinate and where conceivable coordinate client sign-on capacities and client account administration capacities for the huge number of diverse areas now found inside of an enterprise.
The following picture presents the common overall idea behind basic SSO



In the displayed graph we have 4 fundamental elements Client
Two administration applications: A and B.
Identity Provider
Both administration applications (A & B) are arranged to utilize a solitary Identity Provider– so when individual logs in any of the applications, he ought to have the belief that he is as of now signed in the second one.

[1]. Client request a service from administration Application A.
[2]. Anyway client is not yet verified in administration Application A, the client is diverted to the Identity Provider.
[3]. As the client is not yet verified in Identity Provider side, Identity Provider redirects the client to Identity Providers' login page.
[4]. The client enters credentials and after that is authenticated in the Identity Provider area.
[5]. Identity Provider makes and sends validation token to the administration Application A.
[6]. As soon as administration Application A validates User using the received validation token, the initially requested service page A is returned to the client.
[7]. So far so great, yet there is no genuine SSO with a solitary application, so now client requests service page B from administration Application B.
[8]. As the client is not yet verified in administration Application B, the client is diverted to the Identity Provider.
[9]. As the client is as of now, confirmed in Identity Provider, Identity Provider produces and sends validation token to administration Application B.
[10]. The client becomes validated in administration Application B and page B can come back to the client.

2. RELATED WORK

2.1 Lee and Chang user Authentication scheme

Lee and Chang proposed a user authentication plan which also can useful for key interchange requirement while keeping the user as an unknown person. This plan is very helpful in some applications like e-banking where the identity of user should not reveal to the public in the distributed computer networks. This paper proves that their plan has two drawbacks, to eliminate these two drawbacks a we proposed standard authentication scheme. With the fast development of computer network, individuals depend more on advanced communication mechanisms. The present computer network is formed by joining different types of networks which themselves contain hosts and user terminals to use the advantages of distributed computing environment like sharing information and competence power. On the other hand, there might exist some potential issues that need to be considered seriously e.g., who can have entry to the data and up to what level he has authorization. It is necessary to construct few standard mechanisms to secure the networks from attackers. User authentication is the primary approach to detect unauthorized adversary from the network which leads to secure system resources. User anonymity is maintained in a distributed computing environment. This is the reason that service supplier can only detect user using user identity.

Lee and Chang user authentication scheme has the following advantages: (1) user can get the services from different service providers only using zero knowledge proof identity; (2) user no need to maintain multiple passwords and usernames with the single credential user can get services from different service providers; (3) service providers, no need to maintain database of password records; (4) no need to change the authentication token if a new service provider is added into the system

3. DATA INTERCHANGE USING GENERALIZED DIGITAL CERTIFICATE

A digital certificate can be defined as the concatenation of plaintext and signature of the plaintext, created by a trusted identity provider. Using this standard digital signature concept we can complete user authentication and key negotiation for safe communication between user and service provider. Digital certificate contains the information like certificate version number, license code provided by the identity provider and the profile information of certificate holder which is public.

The existence of public key pairs and private key sets is avoided in the GDC model. The user does not have to worry about key management. The verifying party will not be revealed about the digital signature component, as it acts as a secret token of the user. However, the verifying authority will understand the knowledge of the signature by requesting the owner to solve its challenge. The session key, which is generated during the above process, can act as a secure medium for communication among the involved parties.

NOTATION	
TIP	Trusted Identity Provider
C_i,SS_j	Client and service supplier
A_i, B_j	Identification number of C_i, SS_j respectively
pu_X,pr_X	The RSA key pair of identity X
V_i	The credential of C_i created by TIP
T_x,T_y	private and public key pair of TIP
E_k(msg) msg	A symmetric key encryption of plaintext Using a session key K
D_k(cpr) cpr	A symmetric key decryption of ciphertext Using a session key K

4. PROPOSED APPROACH

4.1 System Commencement Phase

System initialization phase involves the process of generating key pair by TIP

The TIP will do the following steps

[1]. Select two large prime numbers a, b next compute N= ab

[2]. Find the key pair (pu, pr) such that pu*pr ≡ 1 mod φ (N), where φ (N) = (a − 1) * (b − 1).

[3]. Picks a generator g over the limited field Z*n, where n is a huge odd prime number.

[4]. SCPC ensures the confidentiality of pr and publishes (pu, g, n, N).

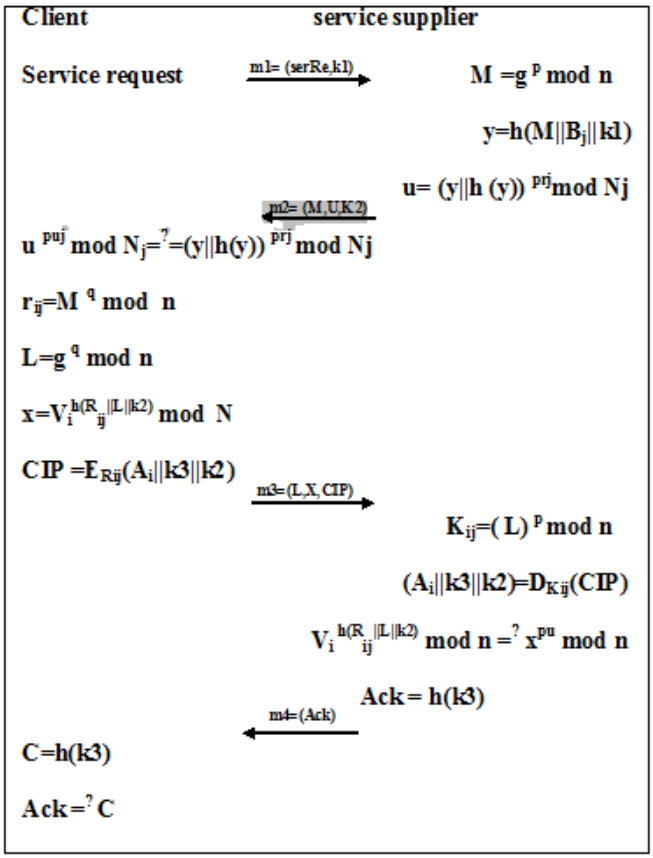
4.2 Registration Phase

At this stage, every client C_i picks an extraordinary character A_i with a strong bit-length, and sends it to TIP. After that, TIP will returns A_i the validation token $V_i = (A_i \| h(A_i))^{pr} \bmod N$, where || indicates a connecting of two strings and h (.) is a hash function to generate hash of identifying number. Here, both C_i and V_i ought to be exchanged by means of a safe channel. In the meantime, every service supplier SS_j with character B_j ought to keep up its own RSA open parameters (pu_j, Nj) and private key pr_j as does by TIP.

4.3 Mutual Authentication Phase

To get the services of service supplier SS_j, Client C_i needs to follow the Identification protocol described in the figure. In this stage client and service supplier will select the two random integers p and q respectively; to prove the identity of messages interchanged between client and service supplier they have to take the three random nonces k1, k2, k3 respectively; and E (msg) indicates the symmetric key encryption scheme to protect the confidentiality of messages interchanged between client C_i and service supplier SS_j.

- In the first step client C_i send the service
- request to service supplier SS_j



- Service supplier considers the service request received from client, he creates and sends user message which is useful to prove the identity of service supplier. The user message is signed by service supplier RSA private key which includes (M, B_j, k1). This signature is validated by client C_i. M= $g^p \bmod n$ is the Diffie-Hellman session key generation material created by SS_j
- Upon receiving a reply message from service supplier SS_j, client C_i also creates Diffie-Hellman session key generation material $L=g^q \bmod n$ and generates validation proof
- $x=V_i^{h(R_{ij}||L||k2)}$ here $R_{ij}=h(A_i||r_{ij})$ is the generated session key from $r_{ij}=M^q \bmod n = g^{pq} \bmod n$ using Diffie-Hellman key exchange technique.
- Validation proof $x= V_i^{h(R_{ij}||L||k2)}$ is the signature generated from client details which is used to prove the client identity, such that the client hold valid validation token without giving a value of the validation token by following statement

$$V_i^{h(R_{ij}||L||k2)} \bmod n = x^{pu} \bmod n$$

- If this statement is verified it means that the service supplier SS_j validated the user successfully.
- In the last step service supplier sends the acknowledgement message which indicates the acceptance of service supplier.

5. CONCLUSIONS

Here, the methodology is discussed where the application can be secured from two attacks. With the help of single sign-on approach, the authorised user can gain access to facilities provided by The service supplier. This can be enabled by passing on the authentication keys and a complicated form of password. The password consists of Zero Knowledge Proof (ZKP) pattern to strengthen the actual identity. The above explained methodology also describes the following stages: operational procedures of single sign on approach, analytical study of the previous phase and present phase execution. In this connection, the maintainability of the system by receiving notifications and alerts is also analysed.

REFERENCES

[1]. L.Lamport,"Password authentication with insecure communication",Commun.ACM,24(11):pp770-772,NOV 1981.Chin-Chen Chang ,"A secure single mechanism for distributed computer networks", IEEE Trans. On Industrial Electronics, Vol.59, No.1, Jan 2012.

[2]. W.B.Lee and C.C.Chang," User authentication and key distribution maintaining anonymity for distributed computer networks", Computer

[3]. A.C.Weaver and M.W.Coudtry," Distributing Internet services to the networks edge", IEEE Trans. And Electron 50(3):pp 404-411;Jun2003.

[4]. Guilin Wang,Jiangshan Yu, and Qi,"Security analysis of a single sign-on mechanism for distributed computer networks,"IEEE Trans. Industrial Informatics.,vol. 9,no. 1,Feb 2013.

[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. 2551–2556, Jun. 2008.

[6]. 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 23(8):697-704,2004.

[7]. T.-S.Wu and C.-L. Hsu, "Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks", Comput. Security, vol. 23, no. 2, pp. 120– 125, 2004.

[8]. K.V. Mangipudi and R.S.Katti, "A secure identification and key agreement protocol with user anonymity(sika)", Computer and Security , 25(6):420-425,2006.

[9]. U. Feige. A. Fiat, and A. Shauin," Zero knowledge proofs of identity", Journal of Cryptography1(2):77-94,1988