ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

Secure Authentication of Distributed Networks by Single Sign-On Mechanism

Swati Sinha[1], Prof. Sheerin Zadoo[2]

P.G.Student, Department of Computer Application, TOCE, Bangalore, Karnataka, India[1]

Asst.Professor, Department of Computer Application, TOCE, Bangalore, Karnataka, India[2]

Abstract: Credential of the technology is missing in the recent system. So, to improve the authentication of the distributed networks or multiple applications we are making use of a single sign on mechanism. Previously, users were using n number of usernames and passwords to access different applications on network. This would lead to higher expense for the administrator as each and every account of the organization will be handled with their particular username and password. But, now user needs to remember just single secure credential to access the multiple service providers in a distributed network by using single sign-on mechanism. However, most existing systems which are using this mechanism have some disadvantage regarding security requirements. So through this paper we will discuss about the development of security from earlier stage to present stage. And also discuss about the structure of the mechanism's working strategy.

***Keywords*:** Single sign-on, Distributed system and Privacy.

I. INTRODUCTION

User identification plays key role in distributed networks to verify the user is legal or not and can therefore grant access to distributed service providers [3]. To avoid illegal user accessibility to the services we need proper user authentication [1], [2]. After mutual authentication between the user and the service providers, a session key should be negotiated to keep privacy of the data exchanged [2], [4], and [5]. It is difficult to remember the password with user identity which is required to access each service provider in the network. Hence, Single sign-on mechanism was proposed so that user with single credential can be authenticated by multiple service providers.

Single sign-on mechanism should meet two basic security requirements that is, credential privacy and soundness. Credential privacy guarantees that illegal service provider should not be able to fully recover a user's credential and then impersonate the user to login other service providers. Soundness means that unregistered user should not be able to access the services provided by the service providers [6]. This paper aims to provide the enhanced security from the previous stage to present stage.

II. RELATED WORKS

In 2000, Lee and Chang proposed a user identification and key distribution scheme to maintain user anonymity in the distributed networks [2]. Later, Wu and Hsu [7] pointed out that the Lee and Chang scheme is insecure against both impersonation attack and identity disclosure attack. Meanwhile, Yang et al. [8] identified a weakness in Wu-Hsu scheme and proposed for improvement. In 2006, Mangipudi and Katti [9] pointed out that Yang et al. scheme suffers from Denial of Service (DoS) attack and presented new scheme. In 2009, Hsu and Chuang [10] showed Yang et al. and Mangipudi – Katti scheme were insecure under identity disclosure and proposed an RSA based user identification scheme to overcome the drawbacks.

Hence, Single Sign-On mechanism was introduced and presented so that user can remember single username and password for the distributed service providers. A similar concept, called the Public/Private key was proposed to provide user identification and key agreement to access all applications.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

- When user registers, then with all the details it gives IP address, which is accepted if not occupied by other users.
- Administrator will have all the details regarding the IP. Administrator will then allocate different IP to all users. And according to it users will be bonded in the network. Registered users will have their own specific IP address which will be accessed by themselves.
- When registered user will send some message to the service provider it will change into encrypted signature which will have public key and to prove the service provider's identity, the service provider will verify and decrypt through the private key which he has.
- While registration, users will use special type of password which will have specific pattern. That special pattern will have Zero knowledge identity (ZKI) [11].
- With the complex password and public/private key the system will have credential users and privacy.
- Soundness will obviously be satisfied by the user by entering valid pair of username and password that is registered and maintained by the server.
- Third party will not be able to login as they are illegal to the application. As, he/she is not registered to the application, so credential forgery and recovery attacks from outsiders, users, service providers and potential collusion of them will not be possible.

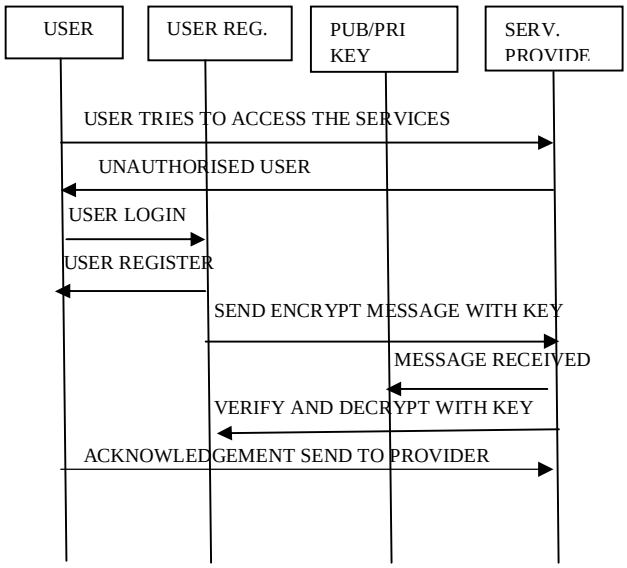

Fig 1: WORKING OF APPLICATION WITH SINGLE SIGN-ON

A. ALGORITHMS FOR PUBLIC /PRIVATE KEY:

Using an encryption key(e,n), the algorithm is as follow:

1. Represent the message as an integer between 0 and (*n*-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.
2. Encrypt the message by raising it to the *e*th power modulo *n*. The result is a cipher text message C.
3.To decrypt cipher text message C, raise it to another power *d* modulo *n*

The encryption key(e,n) is made public. The decryption key(d,n) is kept private by the user.

We can determine the appropriate values of e, n and d by:

1. Choose two very large (100+ digit) prime numbers. Denote these numbers as u and v.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

2. Set n=*u***v*
3. Choose any large integer, such that GCD(*d*, ((u-1) * (v-1))) = 1
4. Find e ;e*d=1 (**mod** ((*u*-1) * (*v*-1)))

III. SINGLE SIGN-ON

Single sign-on is also called Enterprise Single Sign-On or "ESSO". Single sign on can also be defined as user experiencing of logging once and navigating through multiple applications without giving credentials for each applications. In the enterprises, commonly departments have to take care of many applications running simultaneously for different business functions. So, single sign-on makes easy for the user to handle with security and privacy.
Single sign-on mechanism functionality and structure as given below:

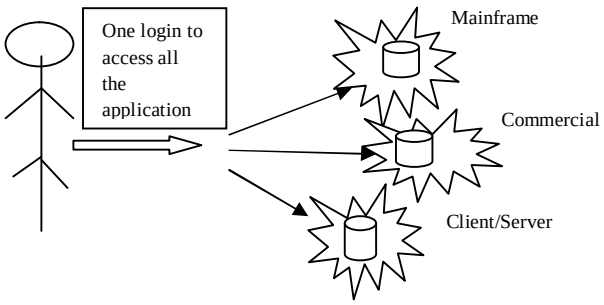

Fig 2: The Single sign on

Benefits:

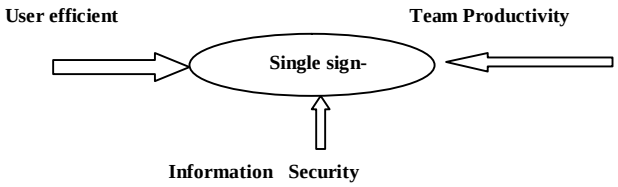

Fig 3: Benefits of Single Sign-On

- **From user view**
  The user has to register them just once. This frees user from remembering large number of passwords.

- **From enterprise view**
  For this, single sign-on delivers tremendous returns on their investment.

- **Increase the potentiality of the password**
  As user has to remember just one password so they construct the password very complex according to their choice.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

- **Improves productivity**
  With less time users can login into multiple applications.

- **Reduces cost**
  There is 33% reduction in help desk volume in the enterprise Single Sign–On solutions as estimated by Meta Group.
  Due to this it reduces password related help desk and lowers the cost.

IV. PERFORMANCE AND ANALYSIS

When we compare previous and present phase's security then we come to know that:

1. **Implementation:** Previous security was complex as compared to present single sign-on signature. Now it's easy to implement.
2. **Process:** Previously, using single username and password to login to one specific server which will take charge of the client authentication to all the other servers.
   Whereas, now simply changing all applications to use the same passwords.
3. **Login Accessibility:** Before, the user only needs to login primary authentication authority once. Whereas, now user has to give same password for each and every system.
4. **Manage Credential Data:** Presently only passwords are managed whereas before client authentication was managed using specific protocols and secrete information.
5. **Password:** Before, strong password would provide only confidentiality. Whereas AK algorithm can assure authentication and confidentiality.
6. **Security:** Presently, credentials are identical so it's far more secure than previous security.

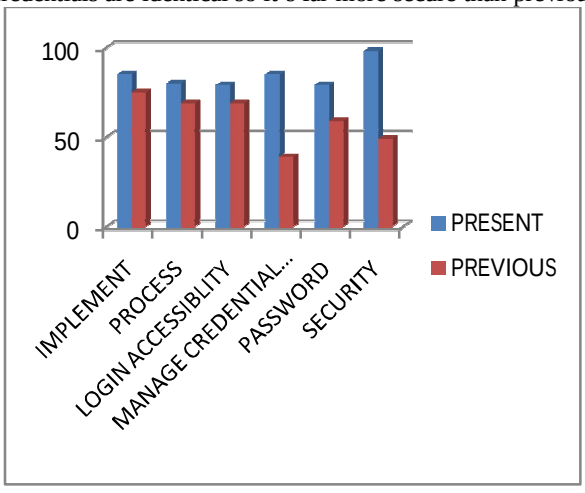

Fig 4: Graph shows the performance of security

Above graph shows the performance of single sign on mechanism from the previous to present.

A. MAINTENANCE:

As we know as time passes there is no stop for new vulnerabilities to occur. So secure architecture of a system is not destination, it changes accordingly. To ensure security to the system we should take care of some measures:

- Software updates and deploy all supportive security fixes.
- Vulnerability scans performed regularly.
- Interact with IT security teams to get recent updates regarding software.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

V. CONCLUSION

In this paper , we discussed how the two attacks can be saved from the application. Using, Single sign-on mechanism how credential user can access the services provided be service providers by giving authentication keys(AK) and complex format of password which contains Zero knowledge Identity(ZKI) pattern to make the identity stronger. And also, described the working of Single sign-on mechanism , comparative study of previous stage and present stage performance using this mechanism. In addition, discussed the maintenance of the system to get alert from vulnerabilities.

REFERENCES

[1]. L.Lamport,"Password authentication with insecure communication",Commun.ACM,24(11):pp770-772,NOV 1981.
[2]. Chin-Chen Chang ,"A secure single mechanism for distributed computer networks", IEEE Trans. On Industrial Electronics, Vol.59, No.1, Jan 2012.
[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]. W.B.Lee and C.C.Chang," User authentication and key distribution maintaining anonymity for distributed computer networks", Computer System and Science and Engineering 15(4):113-116, 2000.
[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]. 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.
[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]. 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.
[9]. 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.
[10]. C.-L. Hsu and Y.-H. Chuang, "A Novel User Identification Scheme with Key Distribution Preserving User Anonymity for Distributed Computer Networks", Inf. Sci., vol. 179, no. 4, pp. 422-429, 2009.
[11]. U. Feige. A. Fiat, and A. Shauin," Zero knowledge proofs of identity", Journal of Cryptography1(2):77-94,1988

.

BIOGRAPHY

Swati Sinha is a student of The Oxford College Of Engineering,Bangalore,India She is pursuing MCA from VISVESVARAYA TECHNOLOGICAL UNIVERSITY,BELGAUM. She is interested in doing research in Computer Networks.