International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Enhancing Security and Authentication of Single Sign on Mechanism of Distributed Computer Networks

Bommasani Nagasai[1], P. Srilatha[2]

[1]M.Tech, Department of CSE, Anurag Group of Institutions, Hyderabad, India

[2]Assistant Professor, Department of CSE, Anurag Group of Institutions, Hyderabad, India

Abstract: ***With wide spreading of distributed computer networks, it has become trendy to allow users accessing various network services offered by distributed service providers. It is usually not recommended by asking one user to maintain different pairs of identity and passwords for different service providers, since this imposes a burden on both users and service providers as well as the communication overhead of computer networks. So, a single sign-on mechanism has been introduced so that after obtaining a credential from a trusted authority each legal user can use this single credential to authenticate itself and then access multiple service providers. There are various attacks and parameters that need to be considered while providing security to authentication system. In this paper, we endow with a comprehensive review of existing work done on Single sign-on. However, most existing Single sign-on schemes have not been proved to satisfy credential privacy and soundness of credential based authentication we formalize the security model of Single sign-on scheme with authenticated key exchange what parameters and attacks should be covered. Next, Implementation of Single Sign-on for distributed computing using user-id and password along with biometric verification and security analysis is done finally, we conclude, specifying the future work.***

Keywords: Authentication, Soundness, Anonymity, Single Sign-On, Biometrics, security.

1. Introduction

In a insecure network environments there is a requirement to be more vigilant about the security and privacy, user authentication plays a vital role. Communication securely through open network is one of the common necessities. Single Sign-on means that after obtaining a username and password from a trusted authority, each legal user can use this single username and password to authenticate itself and then access multiple service providers. Consequently, user authentication has been widely used in distributed computer networks to identify a legal user who requires accessing network services. Therefore mutual authentication is needed to prevent fake server attacks.

There are different methods that are well defined and are useful. An input is given by using smart card and nonces. Nonces are any randomized number which is used. We can use biometrics along with smart card which are advantageous too. In Biometric and smart cards, the input of a biometric can be taken by using a hardware device and feed along with the smart card input and then cryptography mechanism is applied to it. In this paper, we are taking credentials as input along with the biometric verification. Single Sign-On scheme should meet at least two security requirements. ie, Soundness and Credential Privacy [2][3]. Soundness means that A user without a credential should not be able to access the services offered by service providers. Credential privacy guarantees and colluded dishonest service providers should not be able to fully recover a user's credential and then impersonate the user to log in other service providers.

While providing various security parameters that need to be considered such as mutual authentication, Password Change phase, User anonymity, User untraceability. There are attacks that should be verified [1] [5] [6].

- Impersonation attack
- Replay attack
- Denial of service attack
- Credential privacy attack

The two concepts that should be focused for better security are Initiator anonymity and Initiator untraceability[7][8]. Initiator anonymity, says that where only the server knows the identity of the user no other user can identify or notice it. Initiator untraceability is a stronger property than initiator anonymity and requires that any opponent should be not only infeasible to infer the identity of the initiator but also prevent from linking one non-legal user interacting with the server to another transcript. In other words, the adversary is not able to identify or tell whether he has seen the same user twice. Kerberos is also an authentication scheme that we should concentrate, but if this unproven symmetric mechanism is used to authenticate users, which leads to potential security weakness. As authentication of users plays a vital role and major phase i.e., soundness, more improved mechanisms should be used. In this method, the phases used are the same for all the three schemes, but the input feed and processing is different from one another.

2. Related Work

In 2012, C. C. Chang et al. [11], Chang-Lee has introduced a new schema called Chang-Lee Scheme,which have presented an interesting RSA based Single Sign-On(SSO)

scheme based on one-way hash functions and random nonce to solve the weakness of timestamp and to decrease the overhead of the system. It is extremely efficient in computation and communication cost. Where Computation cost and Communication cost are taken as parameters. Chang-Lee scheme is actually insecure to impersonation attack; this was found out by the authors in [2].

In 2013, G. Wang et al. [2], showed that Chang Lee scheme is insecure by applying credential recovering attack and impersonation attack without credentials. The Credential recovery attack which will compromises credential privacy, permits a malicious service provider, who has effectively communicated with an authorized user twice, to recover the user's credential and then to impersonate the user to access resources and services offered by other service providers. In the impersonation attack without credential compromises Soundness, an unauthorized user without any credential may be able to use network services generously by impersonating any legal user or a non-legal user.

In 2008, W. Juang et al. [9], the authors have used Elliptic curve cryptosystem and key agreement. It does not endow with user anonymity. The main virtues include, a user can freely choose and can change the password, it is a nonce based scheme that does not have a serious time-synchronization problem, where servers and users can authenticate to each other. It can provide identity protection, session key agreement, and squat communication and computation cost by using elliptic curve cryptosystems and can also prevent the insider attack and offline dictionary attack.

In 2010, X. Li et al. [8], has presented a remedy by addressing the initiator in traceability property. The deception is to randomize the transmitted data in a manner such that the adversary over the channel cannot link various conversations and where the communicating parties can recognize the received messages. It said that in traceability property would also be addressed in the design of authentication schemes for wireless communications. The authors utilized hash function and, symmetric encryption and decryption and the parameters that were checked for security analysis were Mutual authentication, session key agreement, initiator anonymity, Initiator intractability.

In 2011, A.K. Das Here the author, shows that the scheme which is improved provides strong authentication by biometric, password as well as random nonce produced by the user and the server. The author has enlightened the proposed scheme in four phases that is the registration phase, login phase, authentication phase and password changing phase. Which are secure against attacks like masquerading server attacks, parallel session attacks, lost smart card attack. In 2012, G. Dong et al. [10], the authors analyzed that the Das's scheme [2], is insecure and against the user impersonation attack, the server spoofing attack, the off-line password guessing attack and insider attack, authors have found security weaknesses in Das's scheme.

In 2010, 2012 , Eun-Jun Yoon et al. [12] [13**],** the paper anticipated by Kim, Lee and Yoon, two ID-based password authentication schemes are insecure and vulnerable with smart card and fingerprints leads to impersonation attack. Without passwords or verifying tables, In further paper, the authors have given an idea about Khan-Zhang's biometric remote user authentication scheme is vulnerable to a privileged insider's attack and Parallel session attack. So the authors have projected a new robust authentication scheme using bit-wise exclusive- OR (XOR) operation and collision-free one-way hash functions as which has main cryptographic operations without additional requirements such as using server's public key and digital signatures. This scheme can withstand with various attacks like replay attack, guessing attack, insider attack and impersonation attack and also provides mutual authentication, secure password change function without helping of the remote server. This scheme is useful for wired/wireless environment and for smart card based schemes as it provides the security, dependability and efficiency.

3. Parameters and Attacks Considered for Better Security

In order to check the security of Single Sign-On Mechanism the parameters considered confirmed that the security is not hindered.

3.1 Parameters

A. Mutual Authentication

Mutual authentication is that the user and the server are validated at the same time. Mutual authentication is to set up the agreement between the user and server, so that the user and server agree upon a common key known as a session key.

B. Initiator Anonymity

Initiator anonymity is an important property that must be addressed [7] [15]. It says that only server knows the identity of the user with whom he/she is interacting, while any third party cannot do this [27]. If the Trusted Third Party (TTP) concept is considered, to each and every access to service providers a user will use varied IP addresses of the service providers to benefit from different services, and the authentication party will provide the required data, so in this way the user is unspecified to the service provider also.

C. Initiator Untraceability

Initiator untraceability, is the tougher property than initiator anonymity. It means that the opponent can neither know who the initiator is, nor whether the two conversations initiate from the same initiator. This is an important property that requires to be concentrated on. In simplest terms, it involves that any opponent should be avoided from linking one (unknown) user interacting with the server to another transcript. Namely, the opponent is not capable of telling whether he/she has seen the same user twice.

D. Password Change Phase

Password change phase is essential phase that must be included in the methodology as the user requires to update password so as to concur on a new same password to the authentication party through the log-in phase in advance. It must be included as every time the message is sends new hash code is created of the new password and then that password is used during login.

3.2 Attacks is To Be Prevented

A.Impersonation Attack

An impersonation attack is an attack in which a challenger successfully assumes the identity of one of the genuine in a system or in a communication protocol. So, as the identity is achieved the illegitimate user tries to modify a login request message, but the illegal user will be unable to obtain the data so no modification will be done and the address must be detected.

B. Credential Privacy Attack

A masquerade attack is throughout the use of stolen logon IDs and passwords, it is one type of attack where the attacker pretends to be an authorized server on a system in order to achieve access to it or to achieve greater privileges than they are authorized for. This process obtains a place during login phase and authentication phase. To masquerade as the legal server, an attacker attempts to create the forged reply message which can be masqueraded to the user when receiving the user's login request message.

C. Replay Attack

A replay attack is a type of network attack in which a legal data transmission is maliciously or fraudulently repeated or delayed. This is accepted out either by the originator or by an opponent, who captures the data and retransmits it [9].

D. Denial of service attack

In this denial of service attack, the attacker normally sends excessive messages requesting the network or server to authenticate requests that have unacceptable return addresses. The network or server will not be capable to find the return address of the attacker when sending the authentication endorsement, causing the server to wait before closing the connection. When the server will closes the connection, the attacker can send more authentication messages among invalid return addresses. Hence, the process of authentication and server wait will begin again, staying the network or server busy.

The Notations:
Ri – Receiver; **PWi** – generated by AP; **Si** – Server; **AP** – Authentication party; **PW*-** Password choose by Receiver.

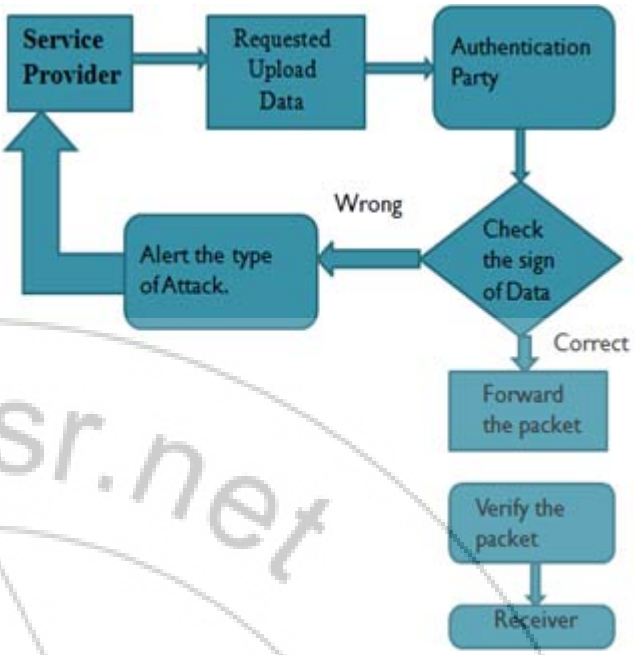

Figure 4.1: System Flow Diagram

4. Implementation of Single Sign-on Mechanism

There are various phases in which the method is carried out:

- Registration Phase
- Login Phase
- Authentication Phase
- Password changing Phase.

A. Registration Phase

In this Phase of work, Receiver Ri opens the file and registers to the authentication party by giving input to user-id and face through a data set that is stored in, the file. Here we are doing it by simulation. The authenticated party provides the password to the receiver. So the APi computes the hash of UDi and password and stores in it. This is done through a secure channel as the random number that is once is added to the message along with the facial Biometric. This hash code of UDi and PWi and face data is stored at the APi.

B. Login Phase

Receiver Ri wants to login in the System to get the service, this phase provides the provision of a secure login request to authentication Party APi. When the receiver inputs the UDi and PWi along with the facial data, the authentication party calculates the hash function of the user-id and password and merges the message with the face data along with the random number and the message digest created is checked with the message digest stored at the APi. If its true then the receiver is the legitimate user else it ends the login phase and asks to login again. If the receiver is the legitimate user then,the IP address is asked to the service provider and the receiver's IP address.

C. Authentication Phase – Receiver authentication

After the login request is done the authenticated party authenticates the receiver. APi already has the list of file names and its signature created. Authentication party asks the receiver of file data needed from DB on the server from the IP address and also gives him own IP address. One of the application is File operation and chat. If the receiver is login, he is connected online to both the applications that is the file operation and chat application. APi asks the receiver of the file needed. **Server Authentication-** As the APi has the list of the File name along with AES encryption/Decryption sign generated. APi asks the server for the file, file stored in the server sends the requested encrypted file along with the random number that is known only to the legitimate server. File is sent to the APi. And does the AES decryption sign. If the sign and random number is same as stored in the APi and the time is also noted then the server is the admissible server. Server and receiver both are authenticated by the authentication party (APi).

D. Password Change Phase

This phase provides the facility of update password by the receiver R, if receiver R wants change his/her password PWi to PW*. First the receiver has to login through his old password. Then there is option for change password, the receiver then inputs his new password and the receiver is free to choose any password as his PW*. Once its updated, receiver is now free to login with his new password. Now every time he is login, this new password is used for creating hash and every time the message is sent. Whole further processing is done through this password.

5. Conclusion

Many Single Sign On Schemes may have security problems and are defenseless to different attacks. In this paper, we have conversed about the existing system and the parameters which are used, and the attacks that should be prohibited during the single sign on mechanism to provide security for single sign on scheme. We have implemented credentials along with the biometric based SSO authentication scheme. We have applied one way hash function and AES Encryption / Decryption algorithm for the file operation that is in the application. We have presented parameters and attacks considered for better security.

References

[1] Chun-Ta Li and Cheng-Chi Lee, 2011.A robust remote user authentication scheme using smart card, Information Technology and Control, Vol.40, No.3.
[2] Gulin Wang, Jianghan Yu,and Qi Xie, 2013, ―Security analysis of a single sign-on mechanism for distributed computer networks‖, 9(1): 294-302.
[3] J. Yu, G. Wang, Y. Mu. 2012. ―Provably secure single sign-on scheme in distributed systems and networks‖. In. Proc. 11th IEEE International Conference On Trust, Security and Privacy in Computing and Communication (TrustCom'12), pp 271-278, IEEE Computer Society.
[4] S. S. Sonwanshi, R. R. Ahirwal, Y. K. Jain, 2012, ―An efficient smart card based remote user authentication scheme using hash function‖, IEEE students' conference on electrical, electronics and computer science, 1-4.
[5] Kee-Young Yoo, Eun-Jun Yoon , and Sung-Ho Kim ,2012, ―A Security Enhanced remote user authentication scheme using smart cards‖, International Journal of Innovative Computing, Information and Control, vol. 8,no.5(B), pp. 3661-3675.
[6] P.Premchand2, A.Govardhan, Mohammed Misbahuddin, 2008, ―A smart card based remote user authentication scheme‖, Journal of Digital Information Management ‰ Volume 6 Number 3, pp.256-261.
[7] C. S. Bindu, P. C. S. Reddy and B. Satyanarayana, 2008, ―Improved Remote User Authentication Scheme Preserving User Anonymity‖, International Journal of Computer Science and Network Security, vol. 8, no. 3, pp. 62-66.
[8] X. Li, W. Qiu , S. Zheng, K. Chen, and J. Li, 2010. ―Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards‖, IEEE Trans. Ind. Electron, 57(2): 793-800.
[9] W. Juang, S. Chen, and H. Liaw, 2008, ―Robust and efficient password authentication key agreement using smart cards‖, IEEE Trans. Ind. Electron, 15(6): 2551-2556.
[10] Jacob Bellamy-McIntyre, Christof Luterroth, Gerald Weber, 2011, ―OpenID and the Enterprise: A Model-based Analysis of Single Sign-On Authentication‖, IEEE computer society.
[11] C.-C. Chang and C.-Y. Lee, 2012,―A secure single sign-on mechanism for distributed computer networks‖. IEEE Trans. Ind. Electron., 59(1): 629-637.
[12] Justie Su-Tzu Juan, Ming-Jhengli, 2010, ―New Cryptanalysis of an ID-based Password Authentication Scheme using Smart Cards and Fingerprints‖, International Journal of Engineering Science and Technology Vol. 2(11), 6840-6844.
[13] Kee-Young Yoo, Eun-Jun Yoon, 2012, ―A Robust and flexible biometrics remote user authentication scheme, International Journal of Innovative Computing‖, Information and Control, Volume 8, Number 5(A), pp. 3173-3188.

Author Profile

Bommasani NagaSai received the Bachelor Degree in Computer Science and Maintenance. and Master of Science Degree in Computer Science from Osmania University Hyderabad. Currently Pursuing Master of Technology in Computer Science and Engineering from Anurag Group of Institutions Ghatkesar, JNTU Hyderabad, India

P. SriLatha is a Assistant Professor in Anurag group of Institutions (formerly CVSR College of Engineering), JNTU Hyderabad, Before this she was a lecturer in Eswari Engineering College, Chennai. She has received the Bachelor of Technology in Computer Science and Engineering from Shadan College, JNTU, Hyderabad and M. Tech in Software Engineering from School of IT, JNTUH, Hyderabad, India