A SURVEY ON SECURITY ANALYSIS OF A SINGLE SIGN-ON MECHANISM FOR DISTRIBUTED COMPUTER NETWORKS

Ms. Vrushali S. Tapade
CSMSS'S CSCOE, Aurangabad, tapadevrushali@gmail.com

Abstract— With extensive spread use of distributed computer networks, it has become common to permit users to access different kinds of network services that are given by distributed service providers. User verification is a key process for the security in the distributed computer network. A new certification scheme is used which is called as Single sign-on mechanism, which facilitates the users with a single credential to be verified by multiple service providers. By providing structurally organized security arguments Chang and Lee proposed a novel SSO scheme and claimed its security. But their proposed scheme is actually not much secure as it fails to meet credential privacy and reliability of authentication. Here, we present two impersonation attacks. In the first attack a malicious service provider communicated with a legal user to gain the user's credential parameters and then take the control for accessing resources & different services offered by service providers. In second type of attack, an outsider who does not having any credential may be able to take the control of user account and can enjoy network services easily by impersonating any legal user or a nonexistent user. Particularly, this survey promote the formal study of the soundness of authentication.

Keywords— single sign-on (SSO), Authentication, distributed computer networks, Attacks, soundness, impersonation,

INTRODUCTION

Distributed system is a kind of network in which different systems are connected through some medium but can be handling from single computer system. There are various real time examples of Distributed system such telephone n/w, Google Cloud, Banks, etc. There are various software components in distributed computer system work from single system. In this kind of systems computers are connected through some network such as LAN, MAN, WAN or wireless. Distributed computer networks consist of clients and servers where they have their respective jobs to do, such as server will monitor all the activities of clients and client can send request to server. There are various advantages of Distributed systems such as more clients can be added effortlessly with less redundancy. But here the problem of security arises, so some security measures should be included in this network so that after completing proper verification process then only client will be added in the network .If verification fails he will not allowed to be part of the existing network. Our paper focuses on these security measures[4].

Various network services are provided by distributed network service providers to different users in Distributed Network. So in distributed n/w user verification is important to check whether he/she is valid user to the services requested. As well as user also required to verify the service provider to avoid fake service provider. Hence after this verification process, a session key may be assigned between user and service provider to keep the confidentiality of the data exchanged between them. In various circumstances, the legal user's privacy must be protected. So it is a big challenge to design efficient as well as secure verification protocols with these security properties in complex computer network environments [3].To maintain individual pair of identity & password for various service provider is difficult task for any user, because it would increases the workload of both service providers and user as well as the communication overhead of networks. This problem was tackled by the single sign-on (SSO) mechanism[5] , where verified user's agent can obtained their credential from a trusted party for a short period(may be one day),and complete verification process of user on behalf of the user to access services provided by multiple service providers. Three basic security requirements that should be meet by an SSO scheme are unforceability, credential privacy, and soundness. Un forgeability means that, a valid credential of a new user could not be forge by any no. of users and service provider except the trusted party. Credential privacy means that malicious service provider could not impersonate the legal user to log in to other service providers by recovering a legal user's credential's. Soundness means that the services offered by service providers should not be access by unregistered user [6].

2. Related work

To improve the security of distributed n/w various SSO mechanisms are suggested.

In 2013, G. Wang et al. [3], presented two attacks on Chang Lee scheme , to prove their scheme is insecure. These attacks are impersonation attack without credentials & credential recovery attack. In credential recovery attack the malicious service provider impersonate the legal user by recovering user's credential to access services provided by different service provider. In the impersonation attack services provided by various service providers could be accessed by unregistered user without credential by impersonating a legal or a non-legal user.

In 2008, W. Juang et al. [7], used Elliptic curve cryptosystem to provide identity protection, session key agreement, and squat communication and computation cost as well as prevent an offline dictionary attack & insider attack. It's a nonce-based scheme in which user can freely choose & change the password and have no time-synchronization problem when server & user can authenticate to each other.

In 2010, X. Li et al. [8], has presented a trick for transmission of data in randomized manner so that an opponent cannot link conversations over the channel. The author addressed the initiator traceability property. Hence author uses symmetric encryption decryption, hash function as well as security parameter such as session key agreement, authentication, and initiator secrecy.

In 2011, A.K. Das here the author, shows the scheme in which authentication is done by random nonce used by server & user, password, biometric. This process was done in four phases to secure various attacks are the registration phase, login phase, authentication phase and password changing phase.

In 2012, Chang-Lee has presented a new scheme to reduce the overhead of the system. & to solve timestamp problem, is RSA based Single Sign-On (SSO) scheme based on one-way hash functions and random nonce. Chang-Lee scheme taken communication cost and computation cost as a parameter but their scheme is actually insecure for impersonation attack, this was shown by the authors [3].

3. Parameters and Attacks Considered for Better Security

To check the security of SSO following parameters are considered.

3.1 Parameters

A. Mutual Authentication

In mutual authentication user and server agree upon a common key (i.e. session key) , hence sever and the user is authenticated at the same time.

B. Initiator Privacy

Only the server knows the identity of the user, while anyone else cannot do this.

C. Initiator Untraceability

It is the toughest property than privacy because it is difficult for the opponent to trace who is the initiator, or whether the one or more conversations are initiated by same initiator. It prevents opponent form linking user & server interaction[10].

D. Password Change Phase

User can change his password by notifying to the authentication party in advance, so that the new hash code is generated for the password and can be used during login[11].

3.2 Attacks is To Be Prevented

A. Impersonation Attack

In this attack a rival assumes the identity of a legal user in a system and tries to change login request message. But he is unable to obtain the data of legal user so no changes will be done and detect the address.

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

This attack is done during login phase and authentication phase by detecting logon ID's and password of a legal user. The attacker tries to pretend as a authorized server by creating forged reply message which impersonate the user when received user login request message.

4. Methodology

A. System Initialization Phase

i. SCPC selects large prime p.

ii. SCPC now choosing a generator element g. This number must be between 1 and p − 1

iii. Then SCPC choosing the private key.

The private key d is any number bigger than 1 and smaller than p−1.

iv. The ElGamal public key consists of the three parameters (p, g, y). So Computing part of the public key, the value y is computed from the parameters p, g and the private key x as $y=g^d \bmod p$

v. Protect d, and publish Public key.

B. Registration Phase

In this phase user send its identity to SCPC. Then, SCPC returns Ui, the credential Si=(IDI||h(Idi))d mod N, || denotes a concatenation of strings and h(.) is a cryptographic one-way hash function.

SCPC	Smart Card Producing Centre
Ui , Pj	User & service provider
IDi , IDj	Unique identity of Ui & Pj
Si	Credential of Ui created by SCPC
h(.)	One way hash function

C. User Identification phase

In this phase, to authenticate user RSA-VES is employed and service provider is authenticated by normal signature.

D. Security Analysis

The user authentication plays crucial role to analyze the security of SSO ,specifically soundness and credential privacy . credential is secured by the unforgeability of RSA signatures, and the security of service provider verification is ensured by the unforgeability of the secure signature scheme chosen by each service provider.

CONCLUSION

In this paper, we presented two powerful impersonation attacks based on Chang and Lee's single sign-on (SSO) scheme. The first attack demonstrates that their scheme cannot defend the confidentiality of a user's credential, and because of that a wrong intentional service provider can copy a legal user to enjoy the resources and services from different service providers. The second attack disrupts the reliability of validation by giving an outside attacker without credential the chance to even impersonate a imaginary user and then easily access resources and services provided by service providers. We also discussed why their well-organized security arguments are not much powerful to assured the security of their proposed SSO scheme. As the future work, the open problems are to formally define authentication soundness and can build efficient and probably secure single sign-on schemes.

REFERENCES:

[1] A. C. Weaver and M. W. Condtry, “Distributing internet services to the network’s edge,” IEEE Trans. Ind. Electron., vol. 50, no. 3, pp.404–411, Jun. 2003.

[2] L. Barolli and F. Xhafa, “JXTA-OVERLAY: A P2P platform for distributed, collaborative and ubiquitous computing,” IEEE Trans. Ind.Electron., vol. 58, no. 6, pp. 2163–2172, Oct. 2010.

[3] G. Wang, J. Yu , Qi Xie, “Security analysis of a single sign-on mechanism for Distributed Computer Networks,” IEEE Trans. Ind. Informatics., vol. 9, Feb. 2013.

[4] L. Lamport, “Password authentication with insecure communication,”Commun. ACM, vol. 24, no. 11, pp. 770–772, Nov. 1981

[5] “Security Forumon Single Sign-On,” The Open Group [Online]. Avail- Dr. Wang has served as a programco-chair for six international security conable: http://www.opengroup.org/security/l2-sso.html

[6] J. Han, Y. Mu, W. Susilo, and J. Yan, “A generic construction of dy- workshops, and a reviewer for over 20 international journals.namic single sign-on with strong security,” in Proc. SecureComm’,2010, pp. 181–198, Springer.

[7] 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.

[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] Book on “Computer network “ by Andrew S. Tanenbaum.

[10] N. Gomathy , Dr. N. radha “ A survey on single sign-on mechanisms for distributed computer networks” IJCTT , vol.13 , no. 3 , jul-2014.

[11] Dr. D. G. Harkut , R.G. Chhatwani “ A review on single sign-on mechanism for distributed computing “ IJERT , vol.2 , no. 12, dec-2013