A Review on Distributed Network Services Using SSO for Secure Mechanism.

Mr.D.S. Baravde,Prof. S.S Bere

Abstract— **The Goal & the research of this paper are focused on improving & to reveal security weakness in distributed network services using Single sign On (SSO) for secure mechanism. SSO is a method of access to the resources of the multiple software system without being prompted to log in again .Authentication is very much important issue in creating and maintaining privacy in large area distributed network In this paper we presents the security problems occurs during secure communication. The main focus is on improving and reveal security drawback in single sign on mechanism .We also demonstrate comparable reviewer of existing work done on this drawbacks to achieve well security over the distributed networks for secure communication . However, by implementing an efficient verifiable encryption of RSA signatures, we propose an improvement for repairing the previous idea. We are also presents the simple way of authentication in this mechanism.**

IndexTerms—**SSO, RSA, Session key Management, Authentication, credential .**

I. INTRODUCTION

In large area of Distributed Computer Network [1] security is major issue faced by different service provider as well as legal user[9]. In general user may register with different service provider's with different authentication information .This makes very tedious task on network also this is complicated to keep authentication information of each service provider[1].To avoid this problem SSO(Single Sign-On)mechanism has been introduced .SSO is mechanism of access control; that enables a user to log in once and gain of different service provider.SSO Uses session authentication process that permits a user to enter one credential in order to access multiple application or services provider's. Which increases the overhead on network as well on user. However, SSO mechanism required strong security policies. otherwise attackers may break this system and uses services of different service provider. Chang and Lee planned a new SSO scheme for secure communication. The single sign-on (SSO) mechanism has been introduced so that, after obtaining a credential from a trusted authority for a short period , each legal user's authentication agent can use this single credential to complete authentication on behalf of the user and then access multiple service providers. Intuitively, an SSO mechanism should meet at least three basic security policies, i.e., Unforgeability , credential privacy[6], and soundness. Unforgeability demands that, except the trusted authority, even a collusion of users and service providers are not able to forge a valid credential for a new user. Credential privacy guarantees that colluded corrupted service providers should not be able to fully recover a user's credential and then impersonate the user to log in to other service providers. Soundness terms mean that an unregistered user without a credential should not be able to access the services offered by service providers. Recently some author presents authorized user privacy and easiness of authentication. However this SSO mechanism is not that much secure, as it fails to achieve the security. The purpose of this research paper is to investigate an improvement by employing an RSA-based verifiable encryption of signatures (RSA-VES), which is an efficient primitive introduced for realizing fair exchange of RSA signatures. VES comprises three parties: a trusted party& two users say Alice and Bob. The main idea of VES is that Alice who has a key pair of signature scheme signs a given message and encrypts the resulting signature under the trusted party's public key, and uses a no interactive zero-knowledge (NZK) proof to convince Bob that she has signed the message and the trusted party can recover the signature from the cipher text. After checking the proof, Bob can send his signature for the same message to Alice. For the purpose of fair exchange, Alice should send her signature in plaintext back to Bob after accepting Bob's signature. If she refuses to do so, however, Bob can get her signature from a trusted party by providing Alice's encrypted signature and his own signature, so that the trusted party can recover Alice's signature and sends it to Bob, meanwhile, forwards Bob's signature to Alice. Thus, fair exchange is achieved. We identify the flaws in their security arguments to explain why attacks are possible against their SSO scheme. Our attacks also apply to another SSO scheme proposed by Hsu and Chuang, which encouraged the design of the Chang–Lee scheme. Moreover, by deploying an efficient verifiable encryption of RSA signatures proposed by Ateniese, In this article we propose an improvement for repairing the Chang–Lee scheme.Chang and Lee proposed a new SSO scheme and claimed its security by providing well-organized security advice. In this paper, however, we demonstrative that their scheme is actually insecure as it fail to meet credential privacy and soundness of authentication. Particularly, we present two impersonation attacks. Here, The first attack allows a illegal service provider, who has successfully communicated with a legal user twice, to recover the user's authentication information and then to impersonate the user to access resources and services offered by other service providers. In second attack, an outsider without any credential may be able to benefit from network

Manuscript received Nov, 2014.

Mr.Baravade D.S *Department of Information Technology,Pune University/ DKGOI,Bhigavan/ , Pune, India, 9766129140*
Prof.S.S.Bere*, Department of Information Technology,Pune University/ DKGOI,Bhigavan/ , Pune,982244957.*

services freely by impersonating any legal user or a nonexistent user.

II RELATED WORK

In [1] Chin-Chen Chang et al. presents the new scheme called Single Sign-On (SSO), which is mainly used for user identification scheme. The prime concept of SSO can permit the legitimate users to use the unique credential to access different service providers in the distributed systems and networks. They use one-way hash functions with random nonces and Data Encryption Standards (DES) for user identification scheme. Hence, the technique is more suitable and efficient for mobile devices. It also provides high security among the mobile users

In [2] Lein Harn et al. described a technique called Generalized Digital Certificate (GDC) which is used to provide user authentication and key agreement. The GDC contains only user's public information. It does not have any user's public key. Here, the digital signature of the GDC is used as a secret token that will never be made public and the secret token will not be given to the verifier. Instead of that, the owner of the secret token will proves to the verifier that he has the knowledge of the signature. Hence, the digital certificate based on this technique is much easier to manage than the X.509 public-key digital certificates.

In [3] Guilin Wang et al. introduced a Single Sign-On technique as a access control method, that allows a user to login once and enables a user with a unique credential to be authenticated by multiple service providers. Here, Guilin Wang et al. identify that the Chang-Lee scheme suffers from two impersonation attacks. Hence, there arises a security flaws. To address this problem, Guilin Wang et al. proposed the new security method based on the verifiable encryption of RSA signatures. The generation of keys and the encryption of signatures are based on the RSA algorithm. Hence, the more secured mutual authentication is achieved. The proposed remedy also prevents a kind of denial of service attack found in the actual scheme. Single Sign-On Mechanism can be done by Cryptography based[10] Single Sign-On, Smart Card based Single Sign-On, Biometric based Single Sign-On.

Smart Card Based SSO

In this smart card based method [8], user inserts smart card into the card reader and submits user credential, card reader computes and checks that the feed data is the same, if yes then further processing is done and message is hashed and send to the server.

Biometric based SSO

Biometric is used in SSO mechanism as biometrics is more advantageous because of its properties [7]. It provides better security as is required for the authentication phase. User inputs the personal biometrics on the input device, if the biometric does not match the template that is stored in the system then no further procedure is carried out.

JXTA-based peer-to-peer (P2P) platform

This platform designed [5] with the aim to leverage capabilities of, P2P, JXTA, and Java technologies to support distributed systems. The platform can be used not only for efficient and reliable distributed computing but also for collaborative activities and ubiquitous computing by integrating in the platform end devices. We calculate the proposed system by experimental study and show its usefulness for massive processing computations and e-learning applications.

S*ecurity Consideration in Distributed Network*

Following are the parameter considered while checking the security of Single Sign-On Mechanism .

- Mutual Authentication
- Session Key Agreement
- Initiator Anonymity
- Initiator Untraceability.
- E. Password Change Phase

Attacks against Chang-Lee Scheme

It can be seen , that the Chang–Lee scheme is actually not a secure SSO scheme because there are two attacks. The first attack, the "credential recovering attack" compromises the credential privacy in the Chang–Lee scheme as a malicious service provider is able to recover the credential of a legal user. The other attack, an "impersonation attack without Id and password," demonstrates how an outside attacker may be able to make use of resources and services offered by service providers, ever since the attacker can successfully masquerade as a legal user without holding a valid credential and thus violate the requirement of soundness for an SSO scheme. In real life, these attacks may put both users and service providers at high risk. Now first describe the attacks together with the assumptions required, justify why these assumptions are reasonable, and finally discuss why the security analysis and proofs are not enough to guarantee the security of the Chang–Lee SSO scheme

III .PROBLEM STATEMENT

Few years back, Chang-Lee offered a new way for single user login and provided some security schemes without having any proof. Their scheme is not secure because, the two types of masquerade attacks are identified

.

Credential Recovering Attack

In this attack, a malicious service provider who has communicated with a legal user twice can successfully recover the user's authentication information. Then, the malicious service provider can impersonate the user to access resources and services provided by other service providers.

Impersonation Attack without Credential

We now study the soundness of the Chang–Lee SSO scheme, which seems to satisfy this security requirement as well. In this attack may enable an outside attacker without any valid credential to impersonate a legal user or even a nonexistent user to have free access to the services. Finally, it must be noted that the an analysis above shows only that the Chang–Lee SSO scheme fails to achieve secure authentication, without disturbing its security for achieving user anonymity and session key privacy.

IV. PROPOSED SYSTEM

We propose an improvement by employing an RSA-based verifiable encryption of signatures (RSA-VES), which is an efficient primitive introduced for realising fair exchange of RSA signatures. VES comprises three parties: a trusted party [10]and two users, say Alice and Bob. The basic idea of VES is that Alice who has a key pair of signature scheme signs given message and encrypts the resulting signature under the

ISSN: 2278 – 1323

trusted party's public key, and uses a no interactive zero-knowledge (NZK) proof to convince Bob that she has signed the message and the trusted party can recover the signature from the cipher text. After validating the proof, Bob can send his signature for the same message to Alice. For the purpose of light exchange, Alice should send her legal signature in plaintext back to Bob after accepting Bob's signature. Next, If she refuses to do so, however, Bob can get her signature from the trusted party by providing Alice's encrypted signature and his own signature, so that the trusted party can recover Alice's signature and sends it to Bob, meanwhile, forwards Bob's signature to Alice. Thus, fair exchange is achieved.

V. CONCLUSION

Most Single sign-on schemes undergo from different security issues and are at risk to different attacks .In this paper, we have discussed existing work done on SSO, and attacks that should be legitimate to provide security to SSO scheme. Next, we discuss various mechanisms through which SSO can be passed out .Auto login, Smart cards, Biometrics are other methods to enhance security for single sign on mechanism for distributed computer networks. As the future work, the open problems are to formally define authentication soundness and construct efficient and provably secure single sign-on schemes. We also discussed why their well-organized security arguments are not strong enough to guarantee the security of their SSO scheme. In addition, .Furthermore, by employing an efficient verifiable encryption of RSA signatures, We demonstrate that how security is achieved

.

ACKNOWLEDGMENT

We would like to thank you Prof.S.S.Bere. Prof. Dhaigude S.S & Prof Dr. Mankar M.V. Sir [HOD,PG-Coordinator & Principal Dattakala College of Engineering, Bhigvan.] For his Encouragement, kindness, support, patience and valuable guidance throughout this work

.

REFERENCES

[1] C.-C. Chang and C.-Y. Lee, "A secure single sign-on mechanism for distributed computer networks," IEEE Trans. Ind. Electron., vol. 59, no. 1, pp. 629–637, Jan. 2012.

[2] L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications," IEEE Trans. Wireless Commun., vol. 10, no. 7, pp. 2372–2379, Jul. 2011.

[3] 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.

[4] 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.

[5] 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.

[6] J. Yu, G.Wang, and Y.Mu, "Provably secure single sign-on scheme in distributed systems and networks," in Proc. 11th IEEE TrustCom, Jun.2012, pp. 271–278.

[7] Li X, Niu J-W, Ma J, Wang W-D, Liu C.-L. 2011. Cryptanalysis and further improvement of a biometricbased remote user authentication scheme using smart cards. Journal of network and computer applications;

[8] 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.

[9] Xinyi Hunag, Y. Xiang member, IEEE, Ashley Chonka, J. Zhou, and R. H. Deng Senior member, IEEE, 2010. A generic framework for three-factor authentication: Preserving security and privacy in distributed systems, IEEE Transactions on Parallel and Distributed System.

[10] Jingquan Wang, Guilin Wang and Willy Susilo, 2013. Anonymous single sign-on schemes transformed from group signatures, International conference of intelligent networking and collaborative systems.

