NOVATEUR PUBLICATIONS
International Journal Of Research Publications In Engineering And Technology [IJRPET]
ISSN: 2454-7875
VOLUME 2, ISSUE 7, July -2016

A SECURE SYSTEM IN DISTRIBUTED COMPUTER NETWORKS USING SINGLE SIGN-ON MECHANISM

HARSHAL B TORVI
Department Of ComputerScience and Engineering. V.V.P.I.E.T.
Solapur, India harshal.torvi@gmail.com

SUPRIYA KULKARNI
Department Of Electrical Engineering. N.B.N.S.C.O.E
Solapur, India Kulkarnispriya.77@gmail. com

ABSTRACT:

In the distributed computer network environment, it is easy for user terminals to share information and computing power with hosts. Accessing of resources becomes efficient and convenient because of the distributed locations of service providers. A Single Sign-On is a method of access control that enables a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again. This scheme is based on one-way hash functions and randomly used to decrease the overhead of the system. In this Paper a secure system with single sign-on mechanism is proposed which allow mobile users to use the unitary token to access service providers.

KEYWORDS: Distributed Computer Networks, Algorithm, Security, Authenticity, RSA, User identification

INTRODUCTION:

Information plays an important role in business, work, and projects. The information should have good quality if it need to be distributed along the network. A distributed referred to computer system where individual computers are physically distributed within some geographic area. The computers that are in a distributed system can be physically close together and connected by a local network.

Distributed computer networks consist of clients- server Model. The simplicity client-server architecture allows clients to make requests that are routed to the appropriate server. Also it distributes processing of task to client systems and relieves servers of many tasks. It is possible to access data any sites over networks. Data may be replicated and distributed to other systems to provide protection from fault tolerance and from local disasters. In the distributed computer network environment, it is easy for user terminals to share information and computing power with hosts. Accessing of resources becomes efficient and convenient because of the distributed locations of service providers. Distributed systems have many advantages over centralized systems, such as *Scalability* where it allows the system to increase capacity by sites as needed. *Redundancy,* where several machines can provide the same services, so if one is failed; the system will not get affected, because other machines are ready to provide the services. A Single Sign-On is a method of access control that enables a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again. It will allow mobile users to use the unitary token to access software systems. In a real-world application, the user can use the mobile device, with the unitary token to access multiple services, such as sending e-mails, download movies, shop online, or process online payment etc., from different service providers in distributed computer networks.

In this paper the proposed system can be implemented by collecting the user id, password and generates the Encrypted key by using RSA Algorithm and by the Trusted Authority. This Encrypted key will be issued to the Authenticated Key Exchange and a Session Key is generated which is should be differentiate with Diffie-Hellmen if the matching founds then only the user is allowed to access the multiple services. Whenever user has to keep secret information security problems can occurs and increase the overhead of the networks.

A system based on Secure Electronic Mail (e-Mail), have been proposed by the author Lein Harn *et al.* [11] (PGP and S/MIME), it uses digital signature to provide message authentication, and it also provides the undesired non-repudiation evidence of the message sender. This paper concentrates on a fully deniable e-mail authentication service. The implemented design is easy to integrate with the current PGP and S/MIME to provide message authentication without non-repudiation evidence. This feature provides security by protecting personal privacy of the message sender in most personal communication**.**

Methodologies in single sign-on (SSO) to enable a legal single credential to be authenticated by a multiple service providers in a distributed computer network is presented by Gguilin Wang *et al.*[10] The techniques used earlier causes overhead in terms of costs and could not preserve when possible attacks occurred. These techniques were also not useful for battery limited devices. The existing solutions were consists of less RSA algorithm. The proposed system uses Single sign-on mechanism that allows users to sign on only once and have their identities automatically verified by every application the services they want to access afterwards. No additional cost are required for the intrinsic centralized access control functionality in the single sign on but provides an easy way to manage access policies rights revocation.

A practical anonymous user authentication scheme with security proof is proposed by Chenglian Liu *et al.* [9] in 2008. He used bitwise exclusive against multiplication attack and the exclusive or implants are easier and faster. But the order of operation in mathematical precedence is misused by him. The author would like to point out these errors in this paper.''

PRINCIPLE OF OPERATION OF SECURITY MECHANISM:

Security problems can occurs and increase the overhead of the networks whenever user has to keep secret information.The problems that the user wants to deal with are to determine whether the user is legitimate or not, service providers should be authenticated, a common session key must be established appropriately and to ensure the privacy of legal users. Recently much research has been proposed a user identification protocol that establish a session key and user anonymity for distributed computer networks. But it suffers from masquerading attacks, and the modified versions are not able to preserve the user's secret token against a malicious service provider. These attacks, the adversary can forge a legal token to cheat the service provider. Afterwards several schemes are proposed which are vulnerable to identity disclosure attacks and proposed an improved prevention mechanism from such attacks. Hsu–Chuang's scheme employs an analogous RSA signature to generate secret tokens, might be vulnerable to impersonation attacks. An attacker can cheat the service provider by masquerading as a legal user but unfortunately, to verify the timestamp when entities are located in different time zones or when there is a congested network environment that has unstable latency is very difficult.

THE PROPOSED RSA ALGORITHM:

RSA was described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman, It is algorithm for public-key cryptography, also known as asymmetric cryptography. The RSA algorithm is the most commonly used encryption and authentication algorithm involves two different but mathematically linked keys, one public and one private. In this algorithm two large prime numbers are multiplied (a prime number is a number divisible only by that number and 1) and through additional operations a set of two numbers are derived that forms the public key and another set that is the private key. After the development of the keys, the original prime numbers are no longer needed and can be discarded. Public and the private keys both are needed for encryption /decryption but only the owner of a private key ever needs to know it.

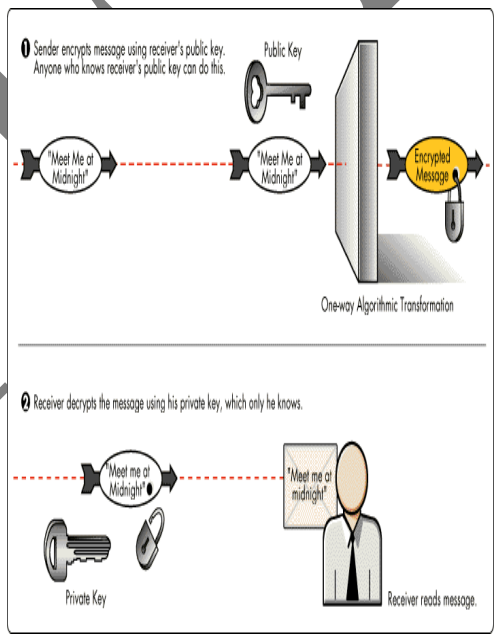

Figure 3.1 RSA algorithm showing Encryption and decryption

In the RSA system, the private key is never sent across the Internet. The text is encrypted with the public key and the private key is used to decrypt the text. Thus, if I wants to send you a message, from a central administrator I can find out your public key (but not your private key) and encrypt a message by using your public key. When the message is received by you, it can be decrypted it with your private key. In addition to this (which ensures privacy), you can authenticate yourself to me (so I know that it is really you who sent the message) by signing a digital certificate by using your private key for encryption. After receiving it, I can use your public key decryption.

SINGLE SIGN-ON MECHANISM (SSO):

In this paper the idea of a Single Sign-On (SSO) platform is used to address the problem by using only one unique central account database and one login procedure for authentication to different software systems. SSO allows users to access all applications from one login. The unified mechanism is provided to manage the user authentication and to implement business rules determining user access to applications and data.

SSO mechanism is a seamless process of authentication performed at various levels. The signed tokens are delivered during the network access phase to provide the desired functionality in SSO system. A SSO according to The Open Group is, It is a mechanism whereby a single action of user authentication and authorization can permit a user to access all computers and systems where he has access permission, without the need to enter multiple passwords. Single Sign-On provides a secure, transparent login which significantly simplifies user identification.

In Single Sign-On (SSO) mechanism the user have to authenticate himself for once and he can access all the resources in an application where he has access permission and there is no need to enter multiple passwords also. The SSO concept can be applied to cross-organizational relationships also, where users are able to travel freely among partner sites within a "boundary of trust". Basically, Single Sign-On authentication is used for sharing of authentication data.

The use of Single Sign-On mechanism eliminates the need of users to remember the number of usernames and passwords apart from their initial network login. The usernames and passwords are securely stored in Single Sign-On mechanism which can be retrieved automatically as and when required by the user. In this way the problem related with users to remember their login credentials is solved.

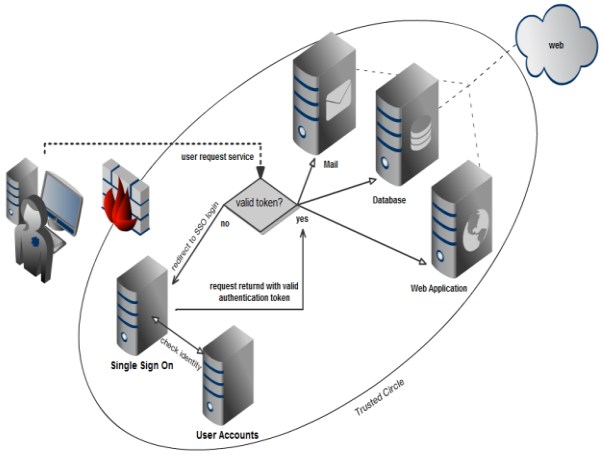

Figure: 4.1 A simple Example of SSO Infrastructure

AUTHENTICATED KEY EXCHANGE (AKE):

Authenticated key exchange (AKE) allows two or more parties to compute the shared key and also ensures authenticity of the parties. Only the authenticated parties can compute a shared key. AKE protocols use a public key environment and the parties use each other's public keys for the construction of a shared secret key. Authenticated Key exchange (KE) protocol enables two or more parties based on their knowledge of a password, establish a cryptographic key using an exchange of messages, such that an unauthorized party (one who controls the communication channel but does not possess the password) cannot participate in the method and is constrained as much as possible from brute force guessing the password. The session key plays an important role in ensuring data confidentiality and integrity between the parties involved in the communication by using effective symmetric encryptions and message authentication codes.

Diffie–Hellman key exchange (D–H) is a specific method that allows parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key is used to encrypt the messages using a symmetric key cipher. But Diffie-Hellman (DH) key exchange protocol is vulnerable to man-in-the-middle attacks hence the DH Protocol must be strengthen against these types of attacks. For this purpose authenticated key exchange (AKE) is used in which both parties must be assured that no other parties aside from their intended peers may know the established session key.

The idea behind the AKE-security is that a passive adversary should not learn the session key and the idea of mutual authentication describes that parties should produce identical session keys, which complete the protocol execution and that each participating party should be ensured of the identity of the others.

In Diffie–Hellman key exchange protocol allows two users to generate a shared private key with which they can then exchange information across an insecure channel. Let the users are Alice and Bob first they agree to use a two prime numbers p and g where Alice chooses secrete key a, and calculates $g^a \pmod p = A$. Bob uses a secret key b, and calculates $g^b \pmod p = B$. After calculating A, B both Alice and Bob calculates the value of s (secrete key) by using $s = B^a \pmod p$ and $s = A^b \pmod p$. The value of s is same for both the parties.

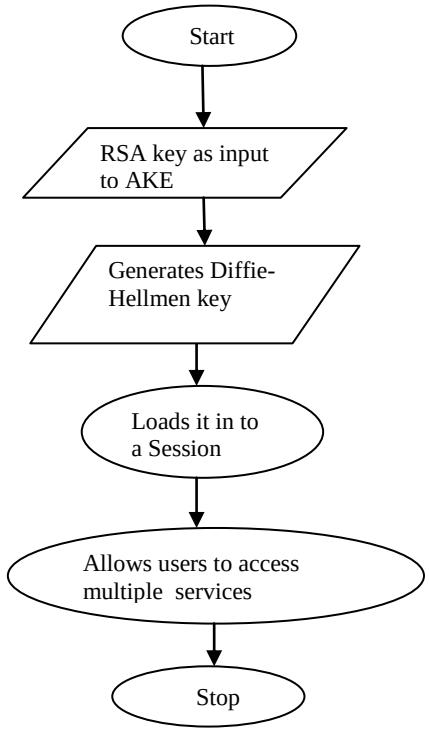

Figure 5.1: Data Flow Diagram for Authenticated Key Exchange

RESULTS:

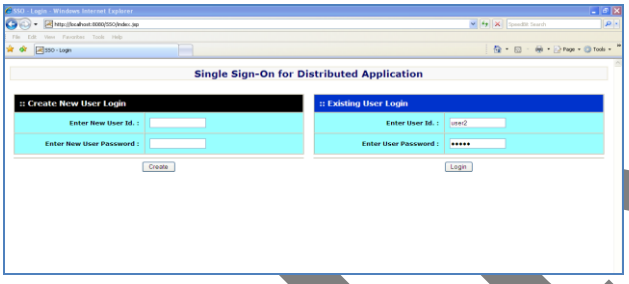

Figure 6.1: SSO Login using user id as "user2"

Figure 6.2 Successful Login for user id as "user2" and New Session DH Key as "13#21"

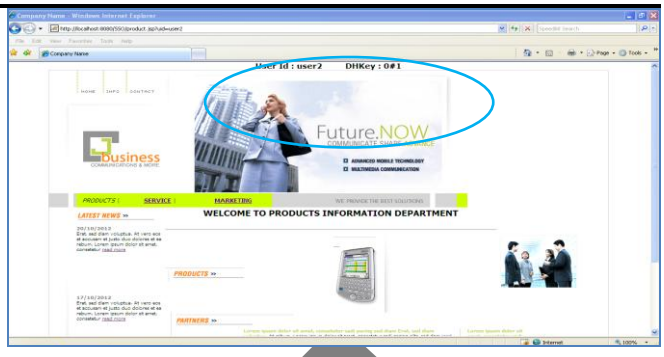

Figure 6.3 switching to "Product" service with New Session DHKey as "0#1"

In the above diagrams you can see how the security is enhanced with the use of Diffie-Hellman Protocol in fig 6.2 user successfully logged in with the session key as "13#21" but when it switches to other services like "Product" as shown in fig 6.3 new session key is created i.e. "0#1". Like this whenever a user wants to switch the service a new session key is created.

ACKNOWLEDGMENTS:

I wish to thank to all my friends for their help and support. I thank god for blessing me with health and determination towards my project. And also my family for their unfailing moral support, guidance and encouragement conformed upon me.

CONCLUSION:

The paper implements a secure system using a single sign-on mechanism to allow users to use the unitary token to access service providers. Our scheme is based on one-way hash functions and random DHKey to solve the multiple service accessing described above and to decrease the overhead of the system.

REFERENCES:

1) A. C. Weaver and M. W. Condry, *"Distributing Internet services to the network's edge,"* IEEE Trans. Ind. Electron., vol. 50, no. 3, pp. 404–411, Jun. 2003.
2) K. Bouyoucef and K. Khorasani, *"A robust distributed congestion-control strategy for differentiated-services network,"* IEEE Trans. Ind. Electron.,vol. 56, no. 3, pp. 608–617, Mar. 2009.
3) A. G. Vicente, I. B. Muñoz, J. L. L. Galilea, and P. A. R. del Toro, *"Remote automation laboratory using a cluster of virtual machines,"* IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3276–3283, Oct. 2010.
4) 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.

5) C. C. Lee, M. S. Hwang, and I. E. Liao, "*Security enhancement on a new authentication scheme with anonymity for wireless environments,"* IEEE Trans. Ind. Electron., vol. 53, no. 5, pp. 1683–1687, Oct. 2006.
6) W. C. Ku and S. M. Chen, "*Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards,"* IEEE Trans. Consum. Electron., vol. 50, no. 1, pp. 204–207, Feb. 2004.
7) K. Saeed and M. Nammous, *"A speech-and-speaker identification system: Feature extraction, description, and classification of speech-signal image,"* IEEE Trans. Ind. Electron., vol. 54, no. 2, pp. 887–897, Apr. 2007.
8) W. S. Juang, S. T. Chen, and H. T. Liaw, *"Robust and efficient passwordauthenticated key agreement using smart cards,"* IEEE Trans. Ind. Electron., vol. 55, no. 6, pp. 2551–2556, Jun. 2008.
9) Chenglian Liu, Changlu Lin and Shuliang Sun *"Security Analysis of Practical Anonymous User Authentication Scheme with Security Proof"* Information Technology Journal, Vol 12, Issue 3, 2013
10) Guilin Wang, Jiangshan Yu, and Qi Xie "*Security Analysis of a Single Sign On Mechanism For Distributed Computer Networks"*,IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL 9 NO 1 FEBRUARY 2013.
11) L. Harn and J. Ren, "*Design of fully deniable authentication service for e-mail applications,"* IEEE Commun. Lett., vol. 12, no. 3, pp. 219–221, Mar. 2008.