RESEARCH ARTICLE OPEN ACCESS

Efficient and Secure Single Sign on Mechanism for Distributed Network

Madhavi A. Indalkar*, Prof. Ram Joshi**
*(Department of Computer Engineering. Pune University, ME II Year MMCOE)
** (Department of Computer Engineering, Pune University, Assistant Professor MMCOE)

ABSTRACT
Distributed network act as core part to access the various services which are available in the network. But the security related to distributed network is main concern. In this paper single sign-on SSO mechanism is introduced which gives access to all services by allowing to sign on only once by users. In this mechanism once user logs in to the Trusted Authority Center TAC then application or services which are register to trusted center will automatically verifies the user's credentials details and these credentials like password or digital signature will be only one for all applications or services. Unlike all other previous mechanisms where in, if user wants to have access multiple services then for every service distinct user credentials (username, password) must be required. SSO act as single authentication window to user for admittance multiple service providers in networks. Previously introduced technique based SSO technology proved to be secure over well-designed SSO system, but fails to provide security during communication. So here emphasis is given on authentication as open problem and on to refining the already proposed SSO process. And to do this along with RSA algorithm which was used in previous SSO process, we will be using MAC algorithm, which is intended to provide secured pathway for communication over distributed network.TAC i.e. Trusted Authority Center is used for sending token integrated with private and shared public key to user.

Keywords - Authentication, Attacks, Distributed network services, Single Sign on mechanism, SSO

I. INTRODUCTION

User authentication [4][5] is an important task in distributed network services. As distributed network is a broadly spreading technology for accessing various types of services by users. So need to provide security with respect to user as well as provider. The aim of a single sign on mechanism is to provide centralized verification and access control management. In SSO the user is registered to any trusted authority center TAC and after verifying details of users TAC gives unique token by which user can able to access the services which also registered to TAC. The service provider verifies details of user by TAC only. However, in existing system, to access the multiple services user need to sign in again and again for each service using the same set of identification details i.e. user id & password, which are validated at the identity provider by each service. Also to prevent/secure from bogus servers, users need to validate service providers every time when want to access the services. After mutual authentication, a session key may be negotiated to keep the privacy of data exchanged between a user and a provider [5], [6], [7]. In many scenarios, the confidentiality of legal users should be protected [5], [8], [7]. But this is big task to design well-organized and protected authentication protocol. This paper aims to ensure more security to the existing Chang Lee SSO scheme [5] and Hsu and Chuang's scheme [9]. The main purpose of this paper is to improvise security for single sign-on solutions and reduce the need for users to frequently prove their identities to different applications and hold different credentials for each application. Also it aims to add additional security during communication between user and provider and security during passing of secrete token.

II. LITERATURE SURVEY

In the literature survey we are going to discuss various existing methods which allow user to access the services from multiple service providers in distributed network. Below in literature we are discussing some of them.

1. Chang and Lee [5] proposed a new SSO scheme. But in that scheme two attacks are found as the first attack allows a malicious/bogus service provider to pick up the user's secrete credential details and then it act as a genuine service provider for user to access resources and services. In another attack, an unregistered user without any credential details able to access services offered by service provider. This leads to soundness attack.
2. L. Harn and J. Ren [10] proposed a similar concept like SSO known as generalized digital certificate (GDC), in this system authentication is done by digital certificate. It is used in wireless network system. In this system a user

will get the digital signature GDC which is provided by a trusted authority center, then user can authenticate itself with the help of GCD signature only. Every user will get unique GCD Signature.

3. Hsu–Chuang user identification scheme [9] is also based on single sign on mechanism. There are two weaknesses found in scheme as 1) an outside user can able to create a valid authentication details without registered to any trusted authority and with that details also able to access the services. 2) Scheme requires clock synchronization as it is based on time stamp.
4. Han [12] proposed a generic SSO structure which is based on broadcast encryption in addition with zero Knowledge (ZK) proof [20]. In this scheme user knows the equivalent private key of a given public key. By this each user is assumed to have been issued a public key in a public key infrastructure (PKI). By making use of RSA cryptosystem ZK proof is very inefficient and unproductive due to the complexity of interactive communications between the a user and the verifier (a service provider).
5. A. C. Weaver and M. W. Condtry[2] propose an alternative- a client server architecture that can assign some multifaceted data processing and device interface tasks to a network edge device, the Net Edge. This device can support services thought to be useful to the industrial environment like language translation technique, image translating scheme, access device adaptation/revision system, virus scanning processor device, content assembly method, local content insertion method, and caching.
6. L. Lamport [4] propose password authentication with insecure communication scheme. This system is secure even if an intruder can read the system's data, and can tamper or corrupt with or snoop on the communication between the user and the system/server. The method uses a secure one-way encryption function and can be implemented with a microcomputer in the user's terminal.

In this paper we are promoting the formal study of the soundness of authentication as one open problem. By using an efficient encryption of MAC (Message Authentication Code) algorithm we provide high level of security. Instead of using only RSA signatures which is use in previous paper we propose MAC (Message Authentication Code) algorithm for better performance and improving the security of the system during communication. Also encryption and decryption technique is used for transfer the secrete token from Trusted Authority Center (TAC).

III. SYSTEM DESIGN

3.1 Problem Definition

In Single Sign on mechanism the trusted authority center send the secrete token to user by which user can able to access the services from authorized services providers which are already registered to TAC.

3.2 System Design and Working of System

The system is divided into three phase as TAC Initialization phase, User & providers Registration phase and User & providers authentication phase.

3.2.1 System Initialization Phase

Trusted Authority Center TAC initialization is done in the initialization phase. This phase is required for TAC to calculate secrete token value for user and parameters for providers. It is based on RSA cryptographic systems.

Steps:

1. Selects large two primes p, q and computes p*q.
2. Determines the key pair (e, d) such that

(1)e *d ≡ 1mod φ (N), where φ(N)=(p − 1)*(q − 1).

3. Chooses a generator g and ElGamal decryption key u and compute the value of y as

(2) y= $g^{u} \bmod N$

4. Chooses a cryptographic hash function h(.)
5. TAC publishes the value as (e, g, y, h (.), n, N) and protects the confidentiality of d and u.

3.2.2 Registration Phase

There are many users which want to access the services from TAC. All users are registered itself to TAC. Also there are various providers which also authenticated by TAC to provide the services.

Steps:

1. On receiving request from user, TAC gives fixed length unique identity IDi and a secret token

(3) $Si = h(IDi)^{2d} \bmod N$

At the same time each service provider keeps a pair of signing signature value σ_j and verifying signature value v_j keys for secure signature scheme.

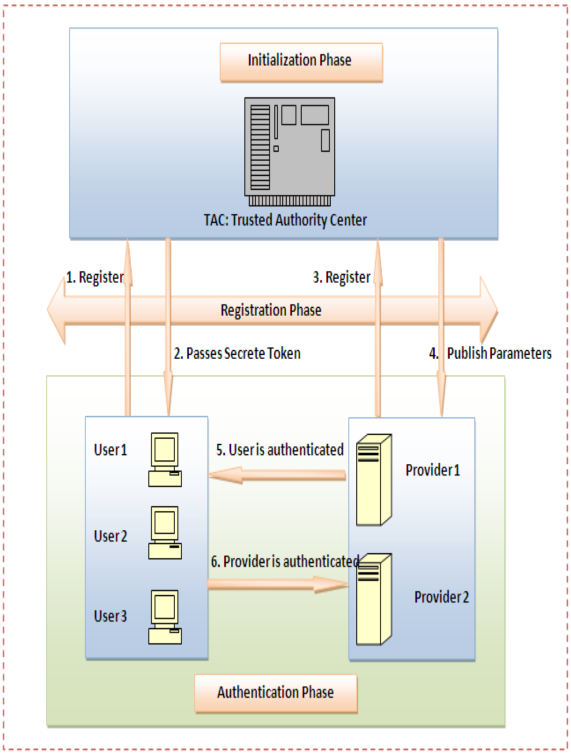

Fig. 1: System Design

3.2.3 User Authentication Phase

Authentication is done between user and service provider. Before granted the access to user first user is authenticated by service provider. Then before accessing the services, user checks the provider's authentication details.

Steps:

1. User send request message to service provider

2. After receiving, provider calculates Diffie Hellman key exchange material Z as (4) $Z = g^k \bmod N$ an issue signing signature v and sends this parameter to user.

3. Depending upon received parameter user check verifying signature value is 1 or not. If verifying signature value v =1 then it calculates its own Diffie Hellman key exchange material W as (5) $W = g^t \bmod N$ and credential details are encrypted into x and send it to provider along with cipher text CT.

But If verifying signature value v =0 then user terminate the connection

4. Provider checks the validity of user depending upon user's credential details. Provider decrypts text using session key K_{ij} and validate the user by checking value of C. Value of C is nothing but concatenated hash function value. If C value is positive then assume that it is valid user then provider grants the access of services. And send the session key hash value V to user. But if C value is negative then provider terminate the connection.

5. User check the value of V. If value is true then user believes that they have shared the same session key to authenticate provider. If value is false then user terminates the conversation

The proposed scheme uses the MAC algorithm to provide the services during the communication between User and Provider and Encryption / Decryption technique to pass the secrete token.

3.3 Use of Message authentication Code (MAC)

MAC is used for better performance and improving the security of the system during communication, because communication between user and provider is done through only message passing. So it is also important task to check the message receive is changed during transmission or not.

TAC creates the symmetric secret key for user and service provider. Depending upon shared symmetric secrete key hash value h1 is calculated and original message and hash value h1 send to provider.

Then provider calculate its own hash value h2 depending upon shared symmetric secrete key which is provided by TAC. IF h1=h2 then provider conclude that the message is not changed during transmission

3.4 Use of Encryption / Decryption technique

Trusted authority center TAC send the token along with private key and shared public key to user. By which the key is encrypted by private key and send to provider for authentication and provider will decrypt key with the help of shared public key which is send by TAC to service provider.

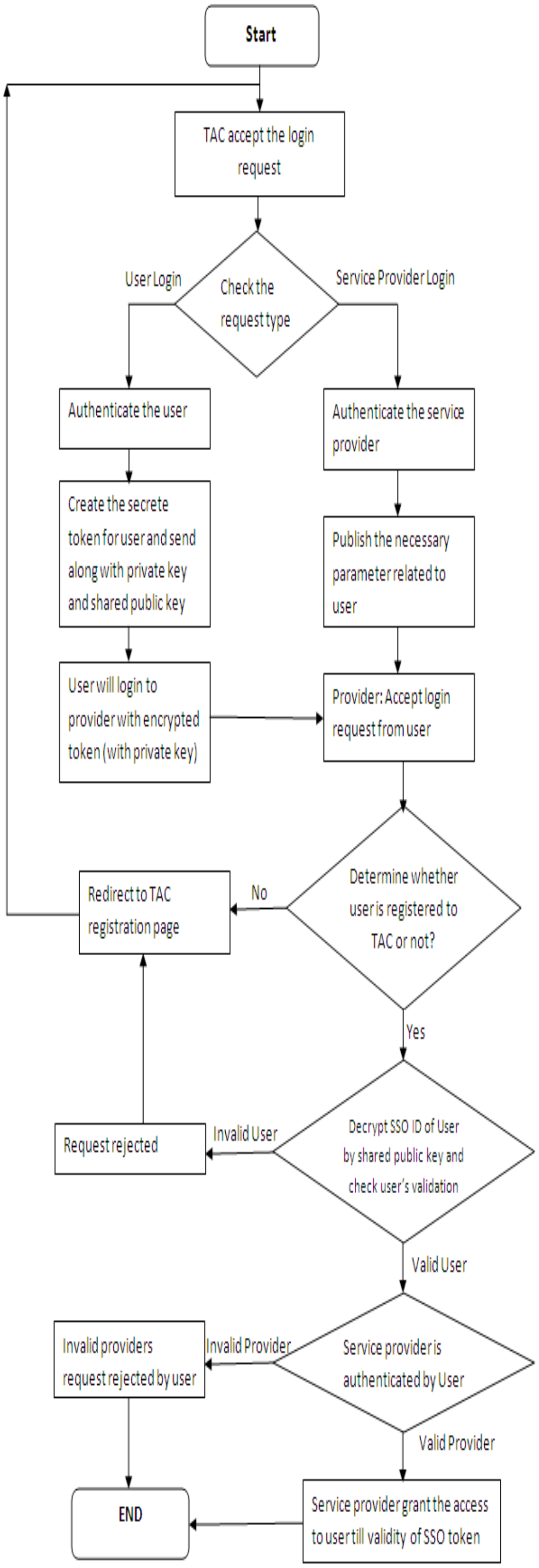
Start
TAC accept the login request
Check the request type
User Login
Service Provider Login
Authenticate the user
Authenticate the service provider
Create the secrete token for user and send along with private key and shared public key
Publish the necessary parameter related to user
User will login to provider with encrypted token (with private key)
Provider: Accept login request from user
Determine whether user is registered to TAC or not?
No
Redirect to TAC registration page
Yes
Decrypt SSO ID of User by shared public key and check user's validation
Invalid User
Request rejected
Valid User
Service provider is authenticated by User
Invalid Provider
Invalid providers request rejected by user
Valid Provider
Service provider grant the access to user till validity of SSO token
END

Fig. 2: Flow of the System

IV. Hardware and Software Used

Hardware Configuration
- Processor - Pentium –IV 2.6 ghz
- Speed - 1.1 GHz
- RAM - 512 mb dd ram
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Monitor - 15” color

Software Configuration
- Operating System: Windows XP/7/8
- Front End: Java and J2EE
- DATABASE: MYSQL Server 2008
- Tools Used: Eclipse

V. CONCLUSION AND FUTURE WORK

This paper proposes efficient a secure single sign-on mechanism based on Message Authentication Code MAC to solve the weaknesses of existing system and also provide the better security during message passing i.e. during communication. Encryption and decryption technique is used by User and service provider in authentication phase. User login with encrypted token and for authentication Provider decrypt token then check the validity of user. This technique is achieving security of token from bogus service provider. By using this proposed SSO scheme, users need only one password from trusted authority center for secure access to all applications available in distributed network and would restrict the hackers entering into the system. But there is some openness in the system and there should be a requirement of best password which is very hard to crack. This paper proposes further study into more well-organized enhancements for security of single sign on for distributed computer networks. Future scope will be leads to Biometric Application.

REFERENCES

[1] 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

[2] A. C. Weaver and M. W. Condtry, “*Distributing internet services to the network edge*” IEEE Transaction Ind. Electron, volume 50 no. 3pp. 402 to 413, June 2003.

[3] L. Barolli and F. Xhafa, “*JXTA-OVERLAY A P2P platform for distributed, collaborative and ubiquitous computing system*” IEEE Transaction Ind. Electron. Volume 58 no. 6 pp. 2160 to 2174 October 2010.

[4] L. Lamport, “*Password authentication with insecure communication*” Communication.

ACM volume 24 no 11 pp 770 to 774, November 1981.

[5] W. B. Lee and C. C. Chang, "*User identification and key distribution maintaining anonymity for distributed computer networks*" Computation System Science Engineering volume 15 no. 4, pp. 113 to 116, February 2000.

[6] W. Juang, S. Chen, and H. Liaw, "*Robust and efficient password authenticated key agreement using smart cards,*" IEEE Transaction Ind. Electron. Volume 15 no. 6 pp. 2553 to 2558, June 2008.

[7] X. Li,W. Qiu, D. Zheng, K. Chen, and J. Li, "*Anonymity enhancement on robust and efficient password authenticated key agreement using smart cards,"* IEEE Transaction Ind. Electron. Volume 57 no. 2, pp. 793 to 800, February 2010.

[8] M. Cheminod, A. Pironti, and R. Sisto, "*Formal vulnerability analysis of a security system for remote field bus access*" IEEE Transaction Ind. Inf. volume 7 no. 1 pp. 30 40, February 2011.

[9] C.L. Hsu and Y.H. Chuang, "*A novel user identification scheme with key distribution preserving user anonymity for distributed computer networks,*" Inf. Science volume 179 no. 4 pp. 422 to 429, February 2009.

[10] L. Harn and J. Ren, "*Generalized digital certificate for user authentication and key establishment for secure communications*" IEEE Transaction for Wireless Communication, volume 10, no. 7, pp. 2372 to 2379, July 2011.

[11] U. Feige, A. Fiat, and A. Shamir, "*Zero-knowledge proofs of identity*" J. Cryptography, volume 1, no. 2, pp. 77 to 94, 1988.

[12] J. Han, Y. Mu, W. Susilo, and J. Yan, "*A generic construction of dynamic single sign on with strong security,*" in Proc. Secure Communication pp. 181 to198, Springer, 2010.