ACCESSING DISTRIBUTED SERVICES WITH ONE TIME TOKEN GENERATION

Richie George
PG Student
Department of Computer Science and Engineering
Rajalakshmi Engg College
Chennai, India
richie.george88@gmail.com

Susmita Mishra
Assistant Professor
Department of Computer Science and Engineering
Rajalakshmi Engg College
Chennai, India
susmitamishra@hotmail.com

***Abstract*— Many services which we use today require us to login to ensure security and confidentiality. As the number of services increase, it has become quite difficult to remember the username and password for each of them. In this system, user can access different services in which he can log in securely once and can access different services through a trusted authority. Sign-on mechanism is an integrated system setup that allows users to access application services by logging only once. It allows users to use the unitary token to access the service provider in distributed computer network. The user has to authorize himself to a trusted third party which will grant him the permission to access all the services by issuing encrypted key known as token. The user acquires this secret key to logon to various services provided by the service provider. This application can be used in desktop/ laptop or mobile phones.**

Keywords- Token, Nonce, Trusted Authority, Anonymity

I. INTRODUCTION

Secure sign-on has seen a lot of implementations in the distributed services domain. A user can sign in to a common interface once, which will grant him direct access to several services hosted within the interface. Sign on is a concept which allows a user to get access to several systems at once, with a single authentication. There are a lot of interesting questions that sign on mechanism brings up, what number of systems the user will be able to access? What are the policies that govern granting access or denying the same to the user? What are the policies sign on is based on? What are the risks when it comes to security of the systems? In sign on, a user will sign in only once using a single user id and password. This single authentication will allow or deny one-click access to the services hosted based on some policies.

Authentication is the process by which a computer system confirms the identity of an individual user, usually based on a name and password. Sign-on is a specialized form of authentication that allows a user to authenticate once in a particular system and thereafter gain access to multiple systems and services. Single sign-on relieves the burden on the user of having to enter authentication information multiple times (e.g., once for every service accessed). In addition, sign-on mechanism facilitates the application of an authentication policy across a domain to be accessed based on centralized management of authentication.

An administrative domain in general, is a security provider for various services that holds security repositories, authenticates and authorizes clients with authentication procedures safely and easily. An administrative domain is a network of computers or a collection of networks and databases, which fall under a common administrator. These services share common security features, which are implemented across the network.

Numerous single sign-on solutions have been developed by industry and academia. Sign on can be organized into two main categories: those that deal with a single set of authentication procedure, and those that deal with multiple sets of authentication procedure. The difference between the two categories is the number of user authentication procedure handled by the sign on mechanism. A sign-on solution dealing with a single set of authentication procedure only has to handle one type of sign on procedure per user; for example, one common authentication mechanism is a username and password. So in single sign-on all the systems in the domain

generally support the same authentication mechanism and accept the same password for an individual user. Sign-on mechanism that handle multiple sets of user authentication procedures usually operate across separate domains that may each require a separate authentication procedure.

II. BACKGROUND WORK

Chin-Chen Chang et al[1] proposed that User identification is an important access control mechanism for client–server networking architectures. The sign-on mechanism can allow legal users to use the unitary token to access different service providers in distributed computer networks. Unfortunately, most of the existing systems cannot preserve user anonymity when possible attacks occur. The additional time-synchronized mechanisms they use may cause extensive overhead. To overcome these drawbacks, a secure sign-on mechanism that is efficient, secure, and convenient for mobile devices in distributed computer networks is been used.

In this paper, the some drawbacks of existing user identification scheme for disturbed computer networks is done. The intend is a secure single sign-on mechanism to overcome these potential drawbacks. In comparing this scheme with other published schemes, the proposed scheme is more suitable for mobile users who use battery-limited devices due to its lower computational cost and lower communication cost. In addition, without additional time-synchronized mechanisms, this scheme can be employed for distributed computer networks in which users are located in different time zones.

Juang et al[2] proposed a password authenticated key agreement scheme using smart cards. Although this scheme has many benefits, it suffers from three weaknesses: 1) inability of the password-changing operation; 2) the session-key problem; and 3) inefficiency of the double secret key. Therefore, an improved scheme to overcome the weaknesses and maintain the benefits of the original scheme is applied here.

The system may be compromised by extracting information from the smart card in order to falsify server authentication. The attacker can seek out the secret server key *s* using offline attack. After the secret value *s* is known, the attacker can easily tamper with the internal value, compromising the security of the entire system.

Xiangxue Li [3] proposed a system for exploiting smart card; it presents a robust and efficient password-authenticated key agreement scheme. It help to strengthens the security of the scheme by addressing untraceability property such that any third party over the communication channel cannot tell whether or not he has seen the same (unknown) smart card twice through the authentication sessions. It also prevents a kind of denial of service attack found in the original scheme, also the performance is higher and other good functionalities are preserved.

This paper has presented a remedy to by addressing the initiator untraceability property. The trick is to randomize the transmitted data in a manner that the adversary over the channel cannot link different conversations and that the communicating parties can recognize the received messages. It is believed that untraceability property should also be addressed in the design of authentication schemes for wireless communications. As a conclusion, the password-authenticated key agreement scheme using smart cards has been really efficient and effective. In terms of efficiency, besides the low communication costs, this solution builds on the efficient cryptographic primitives of secure hash function and symmetric cipher, which may be easily instantiated in and thus inherently viable for smart card environment. In terms of effectiveness, this solution not only preserves mutual authentication, key agreement, initiator anonymity and the functionality of password updating but also can prevent initiator traceability, insider attack, offline password-guessing attack, and DoS attack.

Kyawt Kyawt Khaing et al[4] proposed a Modern cryptography which offers a variety of encryption schemes for the protection of information. Each scheme requires keys to encrypt and decrypt information. Encryption works by scrambling information into unintelligible cipher text by using an encryption algorithm and a short cryptographic key. Decryption restores original information from cipher text by using a com-plementary decryption algorithm and a decryption key. Although many efficient and iron-clad secure encryption solutions have been standardized, these solutions are not generally used in miniature devices and computer systems. The main reason is the lack of generic, easy-to-deploy, and easy-to-use solutions for key management.

Leonard Barolli[5] proposed With the fast growth of the Internet infrastructure and the use of large-scale complex applications in industries, transport, logistics, health, and businesses, there is an urgent need to design and deploy multi-featured networking applications. Some of the features of such applications include the capability to be self-organized, distributed, integrate different types of resources (computers, laptops, and mobile and sensor devices etc), and provide transparent, and secure access to resources. Such applications should not only support traditional forms of reliable distributing computing and optimization of resources but also various forms of collaborative activities, like business, online learning, and social networks in an secure

environment. Here, the Juxtapose (JXTA)-Overlay, which is a based on JXTA peer-to-peer (P2P) platform designed with the aim to leverage capabilities of Java, JXTA, and peer to peer technologies to support distributed and collaborative systems. The platform can be used for collaborative activities and ubiquitous computing by integrating in the platform end devices. The design of a user interface helps to tackle security issues.

P2P systems have evolved from simple systems of file sharing among Internet users to a disruptive technology for collaborative and social activities. Such systems are capable to deliver content, profiling, grouping, and give control to the ordinary users in intelligent and interactive environments. In this paper, we have presented the JXTA-Overlay, which is a JXTA-based P2P platform designed with the aim to leverage capabilities of Java, JXTA, and peer to peer technologies to support distributed and collaborative systems in a decentralized and self organized manner, capable of integrating different types of peers. 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 also end devices.

III. DESIGN AND IMPLEMENTATION OF SIGN-ON MECHANISM

In this project, a secure single sign-on mechanism is used to allow users to use the unitary token to access service providers. In a real-life application, the user can use the mobile device, e.g., a cell phone, with the unitary token to access multiple services, such as download music, receive/reply electronic mails, order goods, or process online payment etc., from the service provider in distributed computer networks as shown in figure 1.This scheme is based on one-way hash functions and random nonce. The user first registers with the trusted authority and the trusted authority verifies the identity of the user. The trusted authority provides the session key to the user. Using this session key the user registers with the service provider. The trusted authority authenticates the user to the service provider. Once the identity of the user is verified by the service provider, it allows the user to access various services authorized by service provider. The steps involved are

A. Key Generation Phase-

A Trusted Authority is such a powerful concept, and it is possible to use the strategy in almost any business or organization and is required to generate the system parameters for each participant in system initialization phase by keeping secrecy of one and publishes the other. It means the original information that feed into system is hided and the other information which is changed, send to the other system. The trusted authority issues the key to the user, using this key the user is authenticated with the service provider. In key generation phase, the trusted authority computes $N = p \cdot q$, where p and q are two large primes, and determines the key pair (e, d) such that $e \cdot d \equiv 1 \bmod \varphi(N)$, where $\varphi(N) = (p - 1)(q - 1)$. The trusted authority protects the secrecy of (d, p, q) and publishes (e, g, N). This working model is shown in Figure 2.

B. Registration Phase-

In the registration phase, each user registers a unique identity with fixed bit length and obtains a secret token from the trusted authority through a secure channel. The secret token is a collision resistant cryptographic one way hash function. In addition it also maintains its public and private parameters to maintain and to withstand the DoS attacks presented on the network. In which the server for that service collects all the data of the network which is connecting the service. With the details registered in the server on the service it allows the user to access the services securely. Here each participant must select a unique identity and send the unique identity to the trusted authority for registration. Upon receiving the unique identity, the trusted authority uses the private key *d* to generate user's secret token. Finally, the trusted authority delivers the secret token to the user through a secure channel. To withstand a DoS attack that is presented, each service provider must maintain its own public and private parameters similar to trusted authority.

C. User Authentication Phase-

In user identification phase, if the user want to access the resources, the user's legitimacy must be authenticated and need to follow the authentication process to work out and to find whether the user is legitimate. The service providers must authenticate, common session key must appropriately established and privacy of legal users must be ensured. The user submits the request with a random nonce. After receiving the request by selecting a random number, a random nonce has been generated. If someone tampered the protocol or the private key another random nonce is generated by selecting another random number and this is computed to generate a session key for the user and decrypt cipher text and give validity for the user identity. The service provider after authenticating the user generates the key as shown in Figure 3. This key is given to the user for accessing various services provided by the server.

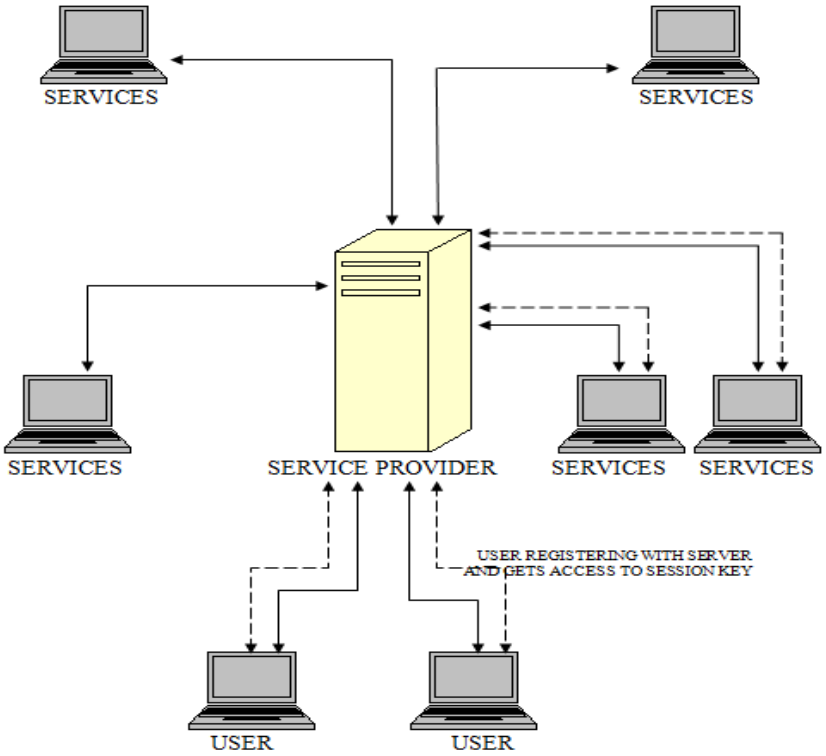

Figure 1. Secure sign-on in distributed networks

IV. RESULT

In this section, we present a screenshot of the key generation phase. The implementation of the system is done in java, where the trusted authority generates the secret keys.

Figure 2. Key Generation by trusted authority

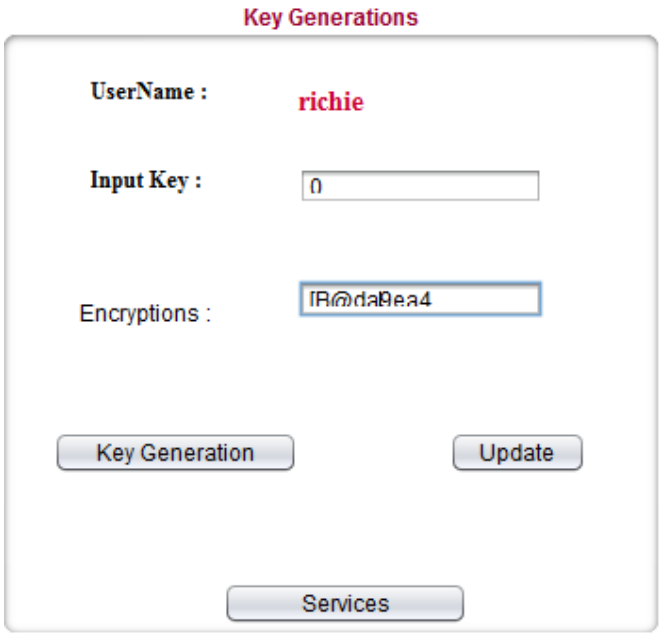

Figure 3. Secret key for accessing multiple services

V. CONCLUSION

We presented a new approach for practical, efficient and secure sign-on frameworks based on token schemes. The proposed framework provides seamless and transparent sign-on mechanism without undermining overall network security. Additionally, it reduces the risk of security threat by providing token based authentication for the application server. These results represent an important step towards the formalization of single sign-on and user authentication protocols, and the construction of provably secure schemes for these practical applications.

REFERENCES

[1] Chin-Chen Chang, Fellow, IEEE, and Chia-Yin Lee, Member, IEEE" A Secure Single Sign-On Mechanism for Distributed Computer Networks", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 59, NO. 1, JANUARY 2012.

[2] *Juang*, Jin-Peng Huai, Ji-Zhou Sun, Jian-Xin Li, Jia-Wan Zhang, Member, *IEEE*, and Zhi-Yong Feng," Improvements of Juang et al.'s Password-Authenticated Key Agreement Scheme Using Smart Cards", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 56, NO. 6, JUNE 2009.

[3] Xiangxue Li, Weidong Qiu, Dong Zheng, Kefei Chen, and Jianhua Li," Anonymity Enhancement on Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 57, NO. 2, FEBRUARY 2010.

[4] Kyawt Kyawt Khaing, Khin Aung, "Secured Key Distribution Scheme for Cryptographic Key Management System" , Availability, Reliability, and Security, 2010. ARES '10 International Conference, Feb. 2010.

[5] Leonard Barolli, , and FatosXhafa, "JXTA-Overlay: A P2P Platform for Distributed, Collaborative, and Ubiquitous Computing", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 58, NO. 6, June 2011 .

[6] Ernie Brickell and Jiangtao Li," Enhanced Privacy ID: A DirectAnonymous Attestation Scheme with Enhanced Revocation Capabilities", IEEE TRANSACTIONS, June 2012 .

[7] Zhen-Yu Wu, Dai-Lun Chiang,Tzu-Ching Lin,Yu-Fang Chung, "A Reliable Dynamic User-Remote Password Authentication Scheme over Insecure Network", 2012.

[8] A. Waluyo, W. Rahayu, D. Taniar, and B. Srinivasan, "A novel structure and access mechanism for mobile broadcast data in digital ecosystems", IEEE Trans. Ind. Electron, Jun. 2011.

[9] Wang, Y.Y., Liu, J.Y., Xiao, F.X., & Dan, J., "A more efficient andsecure dynamic ID-based remote user authentication scheme", Computer Communications, 2009.