Improving the Security of SSO in Distributed Computer Network using Digital Certificate and one Time Password (OTP)

Vishal Patel
Information Technology
Parul Institute of Engineering & Technology, Vadodara.

Riddhi Patel
Asst. Professor, CSE Dept
Parul Institute of Engineering & Technology, Vadodara

ABSTRACT
A Single Sign–on is a new authentication mechanism for user to use multiple services provided by service provider in distributed computer network. It is a one type of application in that allows users to log in once and access to multiple independent applications without being asked to log in again at every application. It enables a legal user with a single credential to be authenticated by multiple service providers in distributed computer networks. This scheme has security flaws. Service provider is fail to credential privacy and authentication. There is two types of impersonation attacks. First attack is credential recovery attack and impersonation. In this attack the attacker act as harm full service provider, who has successfully communicated with a legal user twice to get the identity of a legal user. In another attack the attacker use the services impersonating any legal user or a nonexistent user without credentials. In this we analyze those security flaws & propose solution for those flaws. We have to recover these two types of attacks.

Keywords
Credential, Impersonating, single sign on.

1. INTRODUCTION
The Single sign-on (SSO) is a new authentication mechanism that enables a legal user with a single credential to be authenticated by multiple service providers in a distributed computer network. With wide spreading of distributed computer networks, it has become popular to allow users accessing various network services offered by distributed service providers. Consequently, user authentication (also called user identification) plays a crucial role in distributed computer networks to verify if a user is legal and then can be granted to access the services requested. To prevent bogus server's users usually need to authenticate service providers.[1]. SSO mechanism is used to login once and use services of different service providers using centralize password in distributed computer network.

Nowadays use of multiple network services provided by different service provider using distributed computer network is very popular. Single sign-on is a mechanism which is very usefull to login once and use the different services at same time. It is very important but there is security flow in SSO. The increase of different network services it is very necessary to prevent the security flow for using these services very securely. The Single sign-on (SSO) is a new authentication mechanism that enables a legal user with a single credential to be authenticated by multiple service providers in a distributed computer network. The increasing use of different distributed computer network work load between user and service provider it is mainly to maintain the identity and password for difference service provider. To handle this problem SSO mechanism has been introduces so that after obtaining a credential from a trusted authority, each legal user can use this single credential to authenticate itself and then access multiple service providers. Example of SSO is that we can use a services of myntra.com and we don't have their account, but with the use of our facebook account we can use the myntra. com's services. This is the current example of single sign-on (SSO). [1]

1.1 Application of SSO [13]
Single sign-on is very useful to use different network services at the same time .different application of SSO is as below:

1.1.1 In client-server relationship
In any client/server relationship, SSO is a session and user authentication process This give permission to user use a different network services and application using one Id and Password.e.g we can use services of Google by entering the one password.

1.1.2 In E-commerce
In E-commerce, the SSO scheme is designed to login centrally and consumer secrete data (information) on one server not only for the consumer's facility, but also offer the increasing the security in system. The consumer enters (credit card numbers) secrete data or other sensitive information used in billing. On line internet banking is the best example of it.

1.1.3 Organization
In organization SSO is very useful to user a different services at the same time. Employee can use these services to achieve the or goal or to finish their works.

2. COMPARASION OF DIFFERENT SSO SCHEME
There are different SSO scheme which are describing below.

2.1 Authentication information and replication
The simple SSO scheme (architecture) is authentication database replication. Clients can authenticate to a centralized authentication system (server) and the server stores information for current time logged in clients (online clients)in a session database. This database is send all the data to all the server. In essence, the authentication server acts as the "master" server (holder) of the authentication database and all the other servers are the "slaves"server (holder). When a client contacts another server to request for a service, the

server authenticates the client based on its copy of the authentication database (which store in master server(holder)) and allows the client to connect if the client is found in the replicated database[16]

2.2 Token based

In token based SSO scheme a client can authenticate to authorization system (server) and server send a token to client. It is one type of cryptographic token it is like a secrete key. The client uses this token to prove the identity to each application serve it wants to access. The server does some mathematical calculation (cryptographic processing), some calculation on the token to verify the identity of the client and validate of the token which is created by server. Tokens are rely on shared secret keys. Token describe the trust between two parties (application server and the authentication server). The basic example of a token-based SSO scheme is the Kerberos authentication protocol it describe additional tokens called tickets in Kerberos and in addition client server messages for single sign on.[16]

2.3 PKI-based

Public key infrastructure (PKI)-based Security technique is secure method in network security. In this scheme SSO require that user register to a certification authority(CA) themselves. In this process registration it is validate(identify) with credential generation of private key, public key and the creator of user certificate by CA. Digital certificate contains their unique public key and serial number. Here the CA is the main trusted party(authority) which gives a digital certificate.[14]With the use PKI we can generate the digital certificate. Digital certificate is a small file in there is a public key and serial number. digital certificate establish a connection between a user and a public key ,so digital certificate must contain user name and user's public key. There are different method for sending a data from one client and server. Client can encrypt there data and send to the server. Encryption is the process to convert our data in to the not readable from using the private key. In the other end server can decrypt their data using his public key. Decryption is the process of changing the cipher text in to the original form. In PKI based SSO scheme the main process is user registration IN this method we need to require support of certificate by client and server. Most popular solution that combination of token-based authentication of Kerberos and PKI is Secure European System for Applications in a Multivendor (SESAME) Environment. SESAME also has an option that only uses a PKI based scheme [16].

2.4 Proxy-based

In a proxy-based SSO scheme, the user authenticates to the centralized authentication system(server), and the authentication server itself supplies the user personal data (e.g., username and password) to the similar (appropriate) server whenever the user can send requests for use an application services on another server. Proxy-based SSO is used often when different servers have different authentication mechanisms to use the services and the client(user)has multiple sets of credentials(e.g., username and password) to authenticate their identity. The authentication proxy server uses a database to maintain all the credentials (e.g. username and passwords) for the user. However, proxy-based SSO can still be used when there is one set of credentials each user; the database on the proxy server would simply maintain whole the identity of client (a single set of credentials for each and every user) Proxy-based SSO solutions are popular since they do not require much modification to the end systems to enable single sign-on(SSO)[16]

Table 1. Describe comparison of all the SSO scheme

SSO method	Performance bottlenecks	Scalability Mechanism	Implement ation requireme nt
Authentica tion informatio n and replication	Frequency of authorization database update	Addition of more slave server	All server need to understand the authenticati on format
Token based	Authenticated server need to be contacted for each application request	Replicates authentication server	Additional code required at application server &client
PKI-based	Checking of revoked certificate	Changing of certificate from different CAs	Require support certificate from client and server
Proxy-based	Authentication at the identity provider	Replication of authentication servers at the identity provider	Web based services standard web browser for clients

3. ATTACKS AGAINST EXISTING SCHEME

According to the recent research paper SSO scheme achieves secure mutual authentication since server authentication is done via using traditional RSA signature issued by service provider Pj and without a valid credential Si it looks impossible for an attacker to impersonate a legal user Ui by going through the user authentication procedure. Intuitively, an SSO scheme should meet at least two basic security requirements, i.e., soundness and credential privacy. Soundness means that an unregistered user without a credential should not be able to access the services offered by service providers. Credential privacy guarantees that colluded dishonest service providers should not be able to fully recover a user's credential and then impersonate the user to log in other service providers [1] However, in the following we show that Chang-Lee scheme is actually not a secure SSO scheme by presenting two effective and concrete impersonation attacks. The first attack, called credential recovering attack, compromises the credential privacy in Chang-Lee scheme as a malicious service provider is able to recover the credential of a legal user. The other attack, called impersonation attack without credentials, demonstrates how an outside attacker may be able to enjoy resources and services offered by service providers freely , since the attacker can successfully impersonate 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 lead high risk to both users and service providers. There are two attacks in SSO they are below:

3.1 Credential Recovering Attack

In this type of attack attacker can automatically fetch the user id and password of the user and it login many times and uses the service of the service provider. In this attack attacker has the different type of techniques to get identity. This technique like spoofing ,in this attacker can observe the process of registration or login and then he can fetch their private data.[1]

3.2 Impersonation Attack without Credentials

In this type of attack the attacker is non another but he is a fake or dishonest service provider. If we can log in into this service provider's service our cranial like user id and password can be cracked and our account or our private data can be hacked or stolen by the attacker [1]

4. LIMITATION OF EXISTING SCHME

Single sign-on (SSO) is a new authentication mechanism that enables a legal user with a single credential to be authenticated by multiple service providers in distributed computer networks. Recently, Chang and Lee proposed a new SSO scheme and claimed its security by providing well-organized security arguments. But their scheme has security flaws. hang and Lee single sign-on scheme is a remote user authentication scheme, supporting session key establishment and user anonymity. In their scheme, RSA cryptosystems are used to initialize a trusted authority, called SCPC (smart card producing center), and service providers, denoted as Pj's. Key exchange method is employed to establish session keys. In Chang-Lee scheme, each user Ui applies a credential from the trusted authority SCPC, who signs an RSA signature for the user's hashed identity. After that, Ui uses a kind of knowledge proof to show that he/she is in possession of such a valid credential without revealing his/her identity to eavesdroppers. Actually, this is the core idea of user authentication in their scheme and also the reason why their scheme fails to achieve secure authentication as we shall show shortly. On the other hand, each Pj maintains its own RSA key pair for doing server authentication[1,2].

Two impersonation attacks are present in SSO scheme. The first attack allows malicious service provider, who has successfully communicated with a legal user twice, to recover the user's credential and then to impersonate the user to access resources and services offered by other service providers. In the other attack an outsider without any credential may be able to enjoy network services freely by impersonating any legal user or a nonexistent user. In recent research paper this security flow is not solved. There is no secure SSO scheme which is prevent this attacks purely[1]

5. PROPOSED SCHME

The overview of proposed work will start from the basic concept of the how the security mechanisms have been proposed earlier in the different research papers that I have studied. My proposed work is present Two impersonation attacks are SSO scheme :The first attack allows a malicious service provider, who has successfully communicated with a legal user twice, to recover the user's credential and then to impersonate the user to access resources and services offered by other service providers. In the other attack an outsider without any credential may be able to enjoy network services freely by impersonating any legal user or a nonexistent user. This two attacks can be solved by a method one time password generater.In this we have to register our mobile number at the time of registration process. At the time of login the one time password(OTP) can be send in our mobile no and we can enter it to use the services and for the dishonest service provider we can have to validate the their digital certificate with public key and serial number.

5.1 Flow chart of SSO mechanism

Flow chart of SSO mechanism is shown in figure 1.the different step of this mechanism is below.

- In first step the user is log in into the main service provider's services
- then user have to validate that SP is honest or dishonest. so it can check the digital certificate which is generated by the trusted service provider which can be used by user.
- If the certificate is illegal or expired the use can not go forward and it redirect to the login page and if certificate is valid user can enter their user id or password.
- User enter their id and password to the filed and then generate the one time password which is send to your mobile number which is registered to the trusted service provider.
- Enter the one time password if password is correct the user can use the services and if password is wrong user redirect to the main login page

5.2 System Architecture of SSO Mechanism

Figure 2 describe system architecture of SSO.

[1] User is use the service of service provider A(e.g.myntra.com).User login into the sp A.It redirect to the service provider B(e.g. facebook.com).

[2] There is seen a digital certificate of the service provider A. cretificate authority can check the serial number and the public key of the certificate. If it is valid the whole process is going on otherwise it is terminated and redirect to the login page of sp A.

[3]Validate the digital certificate and redirect to the service provider B.

[4] User enter their user id and password and login into the service provider B. there is a onetime password can be generated on our mobile number which is registered to the service provider B.

[5] If onetime password is correct it redirect to the service provider B.

[6] User successfully login with the service provider B .

[7] User use the services of service provider A using the id and password of service provider Bfacebook.com).

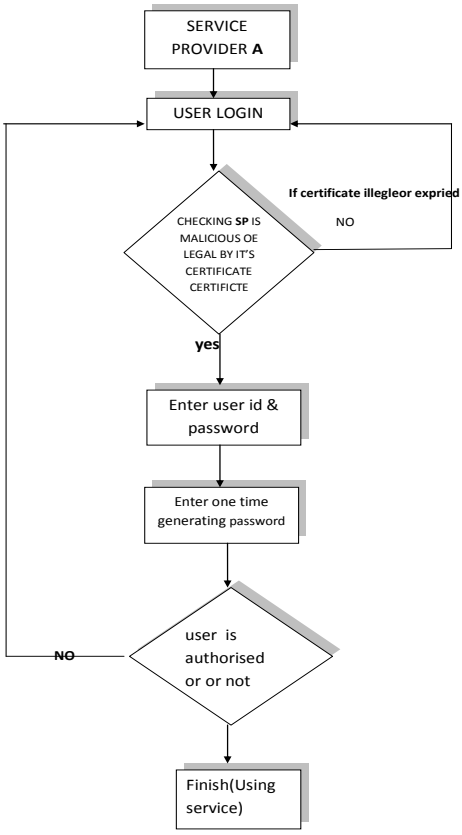

Fig 1.Flowchart of SSO scheme

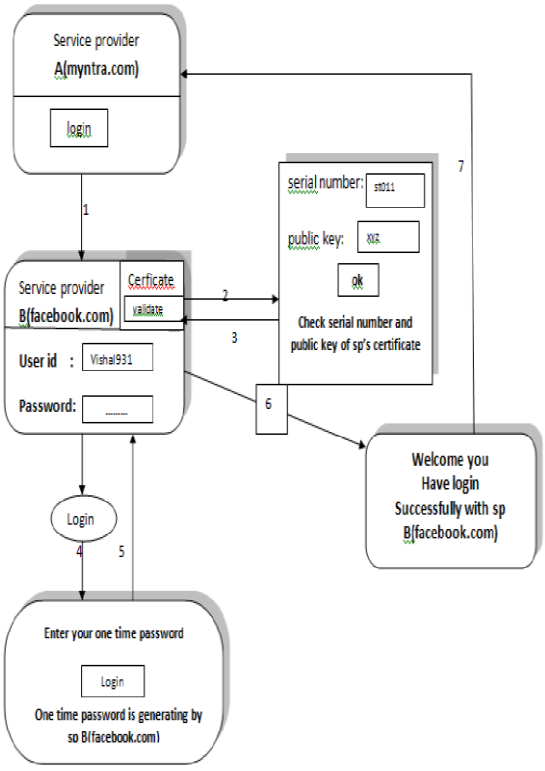

Fig 2.System architecture of SSO scheme

6. CONCLUSION

In this paper, we demonstrated two effective impersonation attacks on Chang and Lee's single sign-on (SSO)scheme. The Single sign-on (SSO) is a new authentication mechanism that enables a legal user with a single credential to be authenticated by multiple service providers in a distributed computer network. There is a security flow in this mechanism. The security flow is preventing by the attacks occurs in this mechanism for that we need to overcome this attacks. Propose solution for solving the two types of attacks . We also discussed why their ell-organized security arguments are not strong enough to guarantee the security of their SSO scheme. As the future work, the open problems are to formally define authentication soundness and construct efficient and provably secure single sign-on schemes

7. REFERENCES

[1] "Security Analysis of A Single Sign-On Mechanism for Distributed Computer Networks", Guilin Wang,Jiangshan Yu, and Qi Xie IEEE TRANSACTIONS ON NETWORKING FEB 2013.

[2] "A secure single sign-on mechanism for distributed computer networks," C.-C. Chang and C.-Y. Lee, IEEE Trans.On Industrial Electronics ,vol. 59, no. 1, Jan 2012.

[3] "Research on the solution of PKI interoperability based on validation authority" yongli Ma;Beijing GFA E-commerce Security CA CO;ltd Beijing , china June 2011

[4] "A generic construction of dynamic single sign-on with strong security" J. Han, Y. Mu, W. Susilo, and J. Yan, SECURECOMM – 2010.

[5] "A novel user identification scheme with key distribution preserving user anonymity for distributed computer networks," C.-L. Hsu and Y.-H. Chuang, Inf. Sci., 179(4): 422-429, 2009

[6] "Distributing Internet services to the network's edge", A. C. Weaver and M. W. Condtry, IEEE Trans. Ind. Electron., 50(3): 404-411, Jun. 2003

[7] "Password authentication within secure communication", L.Lamport, Commun.ACM, 24(11): 770-772, Nov. 1981.

[8] "A secure identification and key agreement protocol with user anonymity (sika)"K. V. Mangipudi and R. S. Katti, Computers and Security, 25(6): 420-425, 2006. [6] X. Li, W. Qiu, D. Zheng, K. Chen, and J. Li, "Anonymity enhancement

[9] "New efficient user identification and key distribution scheme providing enhanced security" ,Y. Yang, S. Wang, F. Bao, J. Wang, and R. H. Deng, "Computers and Security, 23(8): 697-704, 2004.

[10] A generic construction of dynamic single sign-on with strong security",J. Han, Y. Mu, W. Susilo, and J. Yan, secure pro communication spinger 2010

[11] "A logic of authentication," M. Burrows, M. Abadi, and R. Needham, ACM Trans. Comput. Syst., 8(1): 18-36, 1990.

[12] PKCS, "Public key cryptography standards, PKCS #1 v2.1," RSA Cryptography Standard, Draft 2, 2001. Available at http://www.rsasecurity.com/rsalabs/pkcs/

[13] Wikipedia,RSA(algorithm)http://en.wikipedia.org/wiki/RSA_(algorithm http://nile.wpi.edu/NS2

[14] W. Stallings, Cryptography and Network Security, 4th ed. Upper Saddle River, NJ: Pearson, Nov. 2005, pp. 334–340.

[15] Prof M.T. Savaliya Advance java technology dream tech publication.

[16] single sign-on solution for mysea servicesby Sonia Bui September 2005