© 2017 IJSRSET | Volume 3 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Real-Time Detection from Various Social Network Using SSO

C. Jayaseelan, S. Murali, S. Viswanath

Information Technology, Anna University, SKP Engineering College, Tiruvannamalai, Tamil Nadu, India

ABSTRACT

Single sign-on(SSO) is a mechanism that uses a single action of validation to permit an authorized user to access all linked, but independent software systems or applications without being prompted to log in again at each of them during a particular session. Some user identification schemes have been proposed for distributed computer networks. Most existing schemes cannot preserve user anonymity when conceivable attacks occur and those schemes are unconfident. Based on the various cryptography techniques and methods there are few practical and secure single sign-on models are proposed. Specifically, we present two impersonation attack, the first attack is outsider without any credential may be able to enjoy network services, The second attack allows a malicious service provider. The objective is to make observations about how the security of this SSO scheme can be improved.

Keywords : Single Sign On, Validation, User Anonymity, Credential, Malicious Service Provider

I. INTRODUCTION

Single sign-on (SSO) is an validation process that allows a user to access various requests with one set of login credentials. SSO is a common procedure in enterprises, where a client accesses multiple resources associated to a local area network (LAN). Some advantages of SSO are Eliminates credential reauthentication and help desk requests; thus, improving efficiency. Rationalizes local and remote application and desktop workflow. Minimizes phishing. As IT systems proliferate to support business processes, users and system administrators are faced with an increasingly difficult interface to accomplish their work meanings. Users naturally have to sign-on to multiple systems, necessitating an equivalent number of sign-on dialogues, each of which may involve dissimilar usernames and validation information. System administrators are faced with managing user accounts within each of the multiple systems to be accessed in a coordinated manner in order to maintain the integrity of security policy enforcement.

Characteristics of SSO include the following

a) Enhanced user throughput: Manipulators are no longer bogged down by various logins and they are not compulsory to remember various IDs and passwords. Also, support personnel answer fewer requests to rearrange forgotten passwords.
b) Enhanced developer efficiency: SSO provides developers with a common validation framework. In fact, if the SSO mechanism is independent, then developers don't have to worry about validation at all. They can assume that once a request for an application is accompanied by a username, then validation has already taken place.
c) Simplified management. When applications participate in a single sign-on protocol, the management burden of managing user accounts is simplified. The degree of simplification depends on the requests since SSO only deals with authentication. So, applications may still require user-specific attributes (such as access privileges) to be set up

II. METHODS AND MATERIAL

A. Existing System

One user to maintain distinct pairs of identity and password for different service providers. Intuitively, an SSO scheme should meet at least three basic security requirements, enforceability is not able to forge a valid

credential for a new user, credential privacy then impersonate the user to log in to other service providers, soundness unregistered user without a credential should not be able to access the services offered by service providers.

DISADVANTAGES OF EXISTING SYSTEM:

- ✓ Actually, an SSO system, has two weaknesses an unidentified can forge a legal credential by mounting a credential forging attack since the system employed naïve RSA signature without using any hash function to subject a credential for any random identity.
- ✓ Their system is fit for mobile devices due to its high efficiency in calculation and communication.

B. Proposed System

We Overcome The first attack, the "credential recovering attack" compromises the credential privacy in the scheme as a malicious service provider is able to recover the credential of a legal user. We Overcome the other attack, an "impersonation attack without credentials," demonstrates how an outside attacker may be able to freely make use of resources and services offered by service providers.

Advantages:

- ✓ The authors claimed to be able to: "verify that and are able to validate each other using our protocol." but they provided no argument to show why each party could not be impersonated by an attacker. Second, the authors did discuss informally why their system could withstand impersonation attacks.
- ✓ The authors did not give details to show how the BAN logic can be used to prove that their system guarantees mutual validation.
- ✓ In other words, it means that in an SSO system suffering these attacks there are alternatives which enable passing through validation without credentials.

C. System Architecture

This SSO architecture showed in the below figure.

The whole structure of Single Sign-on is as Fig 1 shown.

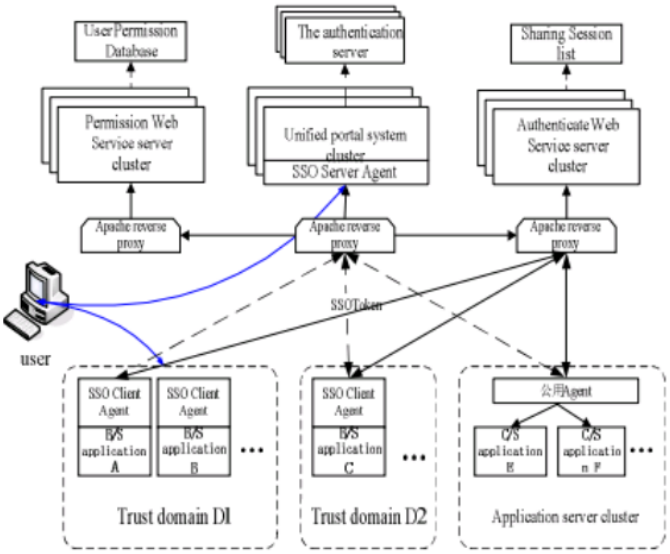


Figure 1: The Structure of Single Sign-on

The procedures are:

Step 1 : The user enters into the unified portal system (it is a cloud account), it contains a authentication server. It fetches the user details from the user database through the permission web service server cluster which requested for where to get in.

Step 2 : After entering into the first service, the authenticate web service server cluster authenticates user then it sends OTP along with the registered number to the user.If the OTP is valid ,it creates the session for the users.

Step 3 : Now users enter into a multiple service with the single-credentials.

Multiple Service with Single Sign On

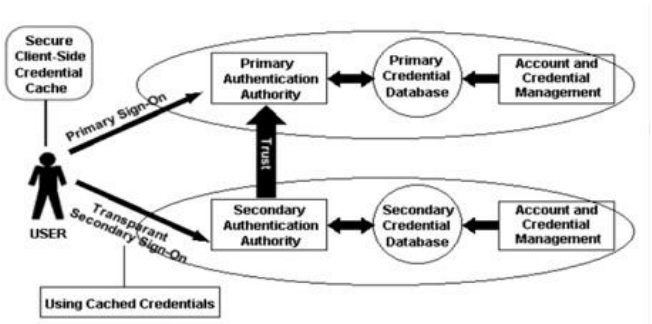
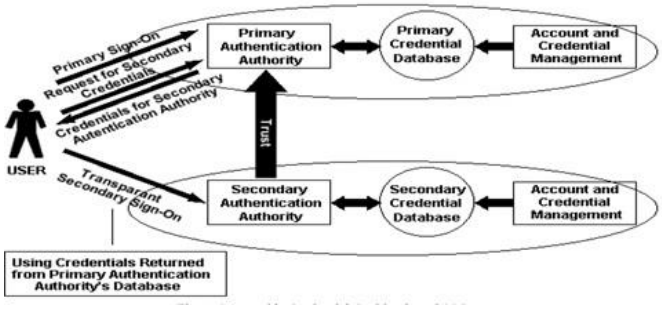


Figure 2. Client Credential Caching Mechanism



D. Modules

The list of modules are

- ✓ User Identification Phase
- ✓ Attacks against the Chang–Lee Scheme
- ✓ Recovering Attack
- ✓ Non-interactive zero-knowledge(NZK)
- ✓ Security Analysis

Module Description

1. User Identification Phase

To access the resources of service provider, user requirements to go through the validation protocol specified. Here, and are random integers selected by and, respectively; and are three random nonce; and denotes a symmetric key encryption system which is used to defend the privacy of user's individuality.

2. Attacks against the Chang–Lee Scheme

The Chang–Lee system is truly not a secure SSO system because there are two potential effective and tangible impersonation attacks.

3. Recovering Attack

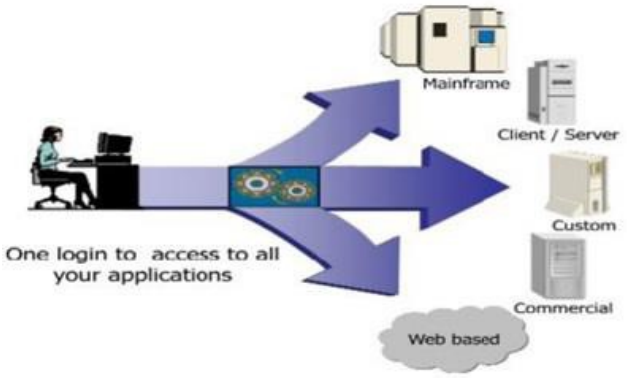
The malicious and then mount the above attack. On the one hand, the Chang–Lee SSO system specifies that is the reliable party. So, this implies that service providers are not reliable parties and that they could be malicious.

4. Non-interactive zero-knowledge (NZK)

The basic idea of VES is that Alice who has a key pair of signature system signs a given message and encrypts the resulting signature under the reliable party's public key, and uses a non-interactive zero-knowledge (NZK) proof to convince Bob that she has signed the message and the reliable party can recover the signature from the cipher text. After authenticating 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.

5. Security Analysis

The security of the enhanced SSO system by focusing on the safety of the user validation part, particularly soundness and credential privacy due to two reasons. importantly the unforgeability of the credential is assured by the unforgeability of RSA signatures, and the safety of service provider validation is ensured by the unforgeability of the secure signature system chosen by each service provider.

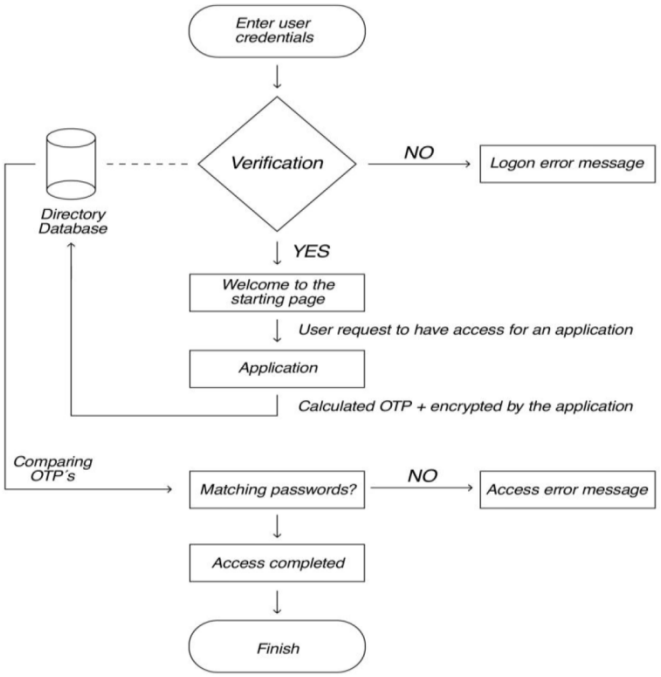


III. RESULTS AND DISCUSSION

A. Security Mechanism

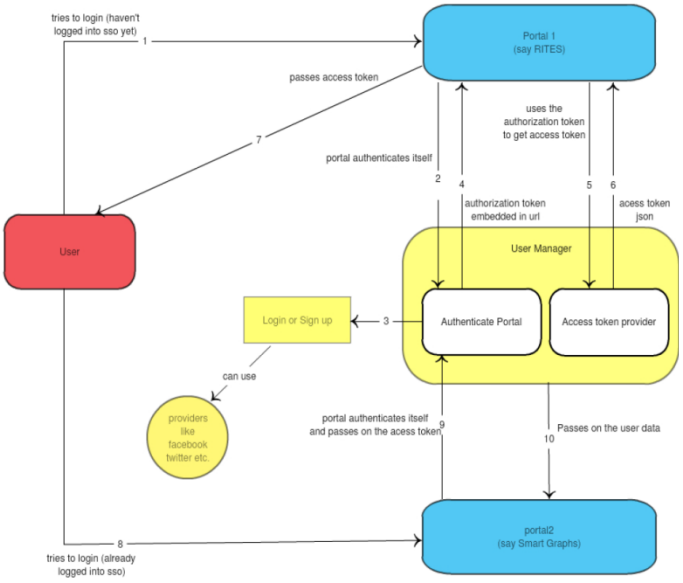
OTP (One Time Password) is another mechanism for the user authentication. OTP is changing every time when it is used. This increases the complexity of the password. This approach used to build a communication between the user and the applications. Combination of OTP with SSO is explained in Figure 3.1. First of all, user needs to enter the credentials to get an access. That username and OTP password verified from a directory database. This database contains username, password, number of how many times OTP should be generated for that user, and secret questions for each user. User and the database both have the same list of passwords. User is able to get that generated OTP by using a password token. That token might be a device like mobile phones or remote hand devices which are unpredictably create a password. If the password is correct than the user directed to a starting page including the applications that permitted to get an

access. If the password is not correct then a warning message pops up in the screen. Each link on the welcome page sends the user credentials to the application that user clicked. After that, some specific algorithms calculate the OTP and encrypt it before sending back to the database. Here OTP computed again with the same algorithms and encrypted. If two passwords are equal which OTP sent by the user and other OTP computed by the application, then the login accessed securely. If they don't match, then the login is not successfully completed. Each successful login decreases the number of logins in the database.



B. Unified Modeling Language(UML)

DataFlow Diagram



Authentication Algorithms

Validation is the process of verifying the identity of the sender request. Validation algorithms use a shared key to verify the current user. Validation algorithms authenticates users credential before entering into the service. If the user enters correct details entering into the service. otherwise it sends the invalid details to the user. And it also authenticates the OTP password.

IV. CONCLUSION

A well-planned and carefully deployed Single Sign-on product can be a great complement to the other security measures which were placed already in an organization. By weighing the risk factors associated with implementing each SSO product against the advantages and by keeping the expectations aligned with realistic planning, an SSO product implementation to satisfy your requirements is achievable.

V. REFERENCES

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

[2]. L. Barolli and F. Xhafa, "JXTA-OVERLAY: A P2P platform for distributed, collaborative and ubiquitous computing", IEEE Trans. Ind. Elect ron., 58(6): 2163-2172, Oct. 2010.

[3]. L. Lamport, "Password authentication with insecure communication", Commun. ACM, 24(11): 770-772, Nov. 1981.

[4]. W. B. Lee and C. C. Chang, "User identification and key distribution maintaining anonymity for distributed computer networks," Computer Systems Science and Engineering, 15(4): 113-116, 2000.

[5]. W. Juang, S. Chen, and H. Liaw, Robust and efficient password authenticated key agreement using smart cards, IEEE Trans. Ind. Electron., 15(6): 2551-2556, Jun. 2008.

[6]. 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 Trans. Ind. Electron., 57(2): 793-800, Feb. 2010.

[7]. 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., 53(5): 1683-1687, Oct. 2006.
[8]. T.-S. Wu and C.-L. Hsu, "Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks," Computers and Security, 23(2): 120-125, 2004.
[9]. Y. Yang, S. Wang, F. Bao, J. Wang, and R. H. Deng, "New efficient user identification and key distribution scheme providing enhanced security," Computers and Security, 23(8): 697-704, 2004.
[10]. K. V. Mangipudi and R. S. Katti, "A secure identification and key agreement protocol with user anonymity (sika)," Computers and Security, 25(6): 420-425, 2006.
[11]. C.-L. Hsu and Y.-H. Chuang, "A novel user identification scheme with key distribution preserving user anonymity for distributed computer networks," Inf. Sci., 179(4): 422-429, 2009.
[12]. The Open Group, "Security Forum on Single Sign-on", http://www. opengroup.org/security/l2-sso.htm
[13]. J. Han, Y. Mu, W. Susilo, and J. Yan, "A generic construction of dynamic single sign-on with strong security," in Proc. of SecureComm'10, pp. 181-198, LNICS 50, Springer, 2010.
[14]. C.-C. Chang and C.-Y. Lee, "A secure single sign-on mechanism for distributed computer networks," IEEE Trans. Ind. Electron., 59(1): 629- 637, Jan. 2012.
[15]. U. Feige, A. Fiat, and A. Shamir, "Zero-knowledge proofs of identity," Journal of Crytography, 1(2): 77-94, 1988.
[16]. G. Tenenbaum. Introduction to Analytic and Probabilistic Number Theory (Theorem 5, page 41). Cambridge studies in advanced mathematics, Vol. 46. Cambridge University Press, 1995.
[17]. E. W. Weisstein, "Relatively prime," MathWorld-A Wolfram Web Resource. Online]. Available at http://mathworld.wolfram. com/RelativelyPrime.html
[18]. PKCS, "Public key cryptography standards, PKCS #1 v2.1," RSA Cryptography Standard, Draft 2, 2001. Available at http://www.rsasecurity.com/rsalabs/pkcs/
[19]. D. Boneh, "Twenty years of attacks on the RSA cryptosystem, " Notices of the American Mathematical Society, 46(2): 203-213, 1999.
[20]. Wikipedia, RSA (algorithm). online]. http://en.wikipedia.org/wiki/RSA_(algorithm)
[21]. M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," ACM Trans. Comput. Syst., 8(1): 18-36, 1990.
[22]. M. Bellare and P. Rogaway, "Entity authentication and key distribution," in Proc. of CRYPTO'93, pp. 232-249, LNCS 773, Springer, 1993.
[23]. C. Boyd and W. Mao, "On a limitation of BAN Logic," in Proc. of EUROCRYPT'93, LNCS 765, pp. 240-247, Springer, 1994.
[24]. N. Asokan, V. Shoup, and M. Waidner, "Optimistic fair exchange of digital signatures," IEEE Journal on Selected Areas in Communications, 18(4): 591-606, 2000.
[25]. J. Camenisch and M. Michels, "Confirmer signature schemes secure against adaptive adversaries," in Proc. of EUROCRYPT 2000, LNCS 1807, pp. 243-258, Springer, 2000.