ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Implementation on Distributed Network Services Using SSO for Secure Mechanism

Mr. D.S.Baravde*, Prof. S.S.Bere
*Research Scholar –ME 2nd yr, DKCOE, Bhigvan
H.O.D.(IT)-DKCOE,Bhigvan

Abstract

Key Agreement and User Authentication is an prime issues for creating and maintaining a security in distributed network .Legal User may able to access services of different providers. Recently there are some user Authentication and key agreement schemes has been proposed for distributed computer network. SSO is a Authentication mechanism which provides , the legal user authenticated by multiple service providers in distributed computer network, with a Single Authentication information. Goal of this paper are focused on improving and to reveal security weakness in services using Single sign On (SSO) secure mechanism, In this paper we provide comparative review of existing work done on SSO. Next we discuss mechanisms in which SSO is carried out to provide well Security. Idea provided by Chang and Lee for SSO mechanism, the authorized user privacy and easiness of authentication is not that much secure, as it fail to meet the security needs.

Keyword: Public key distribution, RSA and SSO Authentication, Distributed Computer Network, Attacks.

Introduction

With wide use of distributed network authentication plays an important role for secure communication, authentication gives assurance that two communicating parties such as user and Distributed service providers [i],[ii] are authenticate each other for proper communication.To maintain different pairs of identity and passwords for different service providers is very difficult task , since this could increase the workload of both users and service providers , So for thatsingle sign-on authentication mechanism is introduced ,in which multiple service providers in distributed network authenticate to legal user with single credential may able to access the services without increase the workload on networks .Few days ago ,Chang and Lee presents new SSO mechanism for security, the authorized user privacy and easiness of authentication is not that much secure, as it fail to meet the security needs. So we introduced two new attacks...

I) First attack :- Service provider who has communicated with authorized user more than once, can recover the user authentication information and impersonate the user to access services offered by other service providers.

II) Second attack :-An outsider without any authentication can use network services freely by impersonating any authorized user. Soundness and Credential Privacy [iii], [v] are two important concepts comes in SSO mechanism for security concerned[vi]. The purpose of this review paper is to investigate an improvement by employing an RSA-based verifiable encryption of signatures (RSA-VES), which is an efficient primitive introduced for realizing fair exchange of RSA signatures. VES comprises three parties:

1) Trusted party
2) Service Provider
3) User

The basic idea of VES is that Service Provider who has a key pair of signature scheme signs a given message and encrypts the resulting signature under the trusted party's public key[ix], and uses a no interactive zero-knowledge (NZK) proof to convince User that He has signed the message and the trusted party[x] can recover the signature from the cipher text. After validating the proof, User can send his signature for the same message to Service Provider. For the purpose of fair exchange, Service Provider should send her signature in plaintext back to User after accepting User's signature. If He refuses to do so, however, User can get her signature from the trusted party by providing Service Provider's encrypted signature and his own signature, so that the trusted party can recover Service Provider's signature and sends it to User, meanwhile, forwards User's signature to Service Provider. Thus, fair exchange is achieved.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

We identify the flaws in their security arguments to explain why attacks are possible against their SSO scheme. Our attacks also apply to another SSO scheme proposed by Hsu and Chuang, which inspired the design of the Chang–Lee scheme [iv]. Moreover, by employing an efficient verifiable encryption of RSA signatures proposed by Ateniese, we propose an improvement for repairing the Chang–Lee scheme. Chang and Leeproposed a new SSO scheme and claimed its security by providing well-organized security arguments. In this paper, however, we demonstrative that their scheme is actually insecure as it fail to meet credential privacy and soundness of authentication. Specifically, we present two impersonation attacks. 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 another attack, an outsider without any credential may be able to enjoy network services freely by impersonating any legal user or a nonexistent user .

Methodology

Some author's SSO Mechanism consists of three phases: system initialization,registration, and user identification. Table I explains notations,and the details of Their scheme are reviewed as follows.

TABLE I: Notations

U_i, P_j	User and Service Provider
S_i	The Credential of U_i,Created by SCPC
S_x	The long term private key of SCPC
S_y	The public key of SCPC
E_k(M)	A symmetric key encryption of plain text M using a key K
e_X,d_X	The public /private RSA key pair of identity X
$ID_i ID_j$	The unique identity of U_i,and P_j

A. ***System Initialization Phase***

SCPC does the following

1. Selects large two primes p, q and computes p*q.
2. Determines the key pair (e,d) such that e *d ≡ 1mod φ(N),where φ(N)=(p − 1)*(q − 1).
3. Chooses a generator g over the finite field Z∗n, where n is a large odd prime number.
4. SCPC protects the secrecy of d and publishes

B. ***Registration Phase***

1. Each user U_i,registers a unique identity ID_i with a fixed bit length.
2. Obtain a secret token S_iSi=(ID_i||h(ID_i))d mod N, from the SCPC through a secure channel where *H(.)* is a cryptographic one-way hash function.

C. User Identification Phase

User go through authentication process. To use the resources of service provider

D. ***Encryption and Decryption Phase:***

Encryption and Decryption between user and provider is ensured using AES algorithm which is more secure than DES and there are currently no known non-brute-force attacks against AES. Data which is send from each provider to user is encrypted and send to the user, then the user decrypts it and the original data is retrieved. All these encryption and decryption are done using the more secure Advanced Encryption Algorithm (AES). The implementation is done using socket programming in Java and it uses server programs and client programs. To run in different machines, programming is based on IP address of the systems. Using the multithreading features of Java, all the providers can be run in parallel

Results

In this system we proposed that Chang and Lee's SSO scheme is insecure. Since their credential privacy and authentication mechanism is fails to achieve security in distributed network. Initially we introduced two different attacks. In first attack malicious server (Service provider) may successfully communicate many times with a legal user and recover their credential. Then this malicious service provider may create another user to access all the resources and services given by another service provider. In Second attack outsider user impersonate any legal user and uses their services without any authentication To overcome theirs drawback we implement new security mechanism specifically We propose an improvement by employing an RSA-based verifiable encryption of signatures (RSA-VES), which is an efficient primitive introduced for realizing fair exchange of RSA signatures. VES comprises three parties: a trusted party and two users say Alice and Bob. The basic idea of VES is that Alice who has a key pair of signature scheme signs a given message and encrypts the resulting signature under the trusted party's public key, and uses a no interactive zero-knowledge (NZK) proof to convince Bob that she has signed the message and the trusted

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

party can recover the signature from the cipher text. After validating 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. If she refuses to do so, however, Bob can get her signature from the trusted party by providing Alice's encrypted signature and his own signature, so that the trusted party can recover Alice's signature and sends it to Bob, meanwhile, forwards Bob's signature to Alice. Thus, fair exchange is achieved.

Conclusion

We reached the end of this work the overall work can be summed up with the following statements. The task consisted first of researching and investigating within the around protocol with the focus on its aspect of single sign on mechanism. Also this work proposes further research into more efficient enhancements for security of single sign on for distributed computer networks. For third-party sites, credential generation and synced, cloud-based storage can be provided. Auto login, Smart cards, Biometrics are other methods to enhance security for single sign on mechanism for distributed computer networks. As the future work, the open problems are to formally define authentication soundness and construct efficient and provably secure single sign-on schemes.

Acknowledgement

We would like to thank you Prof. Dhaigude S.S & Prof Dr. Mankar M.V. Sir [PG-Coordinator & Principal Dattakala College of Engineering, Bhigvan.] For his Encouragement, kindness, support, patience and valuable guidance throughout this work.

References

1. C. Weaver and M. W. Condtry, "Distributing internet services tothe network's edge," IEEE Trans. Ind. Electron., vol. 50, no. 3, pp.404–411, Jun. 2003.
2. 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
3. Gulin Wang, Jianghan Yu,and Qi Xie, 2013. Securityanalysis of a single sign-on mechanism for distributedcomputer networks, 9(1): 294-302.
4. C.-C. Chang and C.-Y. Lee, "A secure single sign-on mechanism fordistributed computer networks," IEEE Trans. Ind. Electron., vol. 59, no. 1,pp. 629–637, Jan. 2012.
5. J. Yu, G.Wang, and Y.Mu, "Provably secure single sign-on scheme indistributed systems and networks," in Proc. 11th IEEE TrustCom,Jun.2012, pp. 271–278.
6. G. Wang, J. Yu, and Q. Xie, Security analysis of a single sign-on mechanism for distributed computer networks Cryptology ePrint Archive, Rep. 102, Feb. 2012 [Online]. Available: http://eprint.iacr.org/2012/107
7. Li X, Niu J-W, Ma J, Wang W-D, Liu C.-L. 2011. *Cryptanalysis and further improvement of a biometricbased remote user authentication scheme using smartcards.* Journal of network and computer applications;
8. W. Juang, S. Chen, and H. Liaw, 2008. Robust and efficient password authentication key agreement using smart cards, IEEE Trans. Ind. Electron, 15(6): 2551- 2556.
9. Xinyi Hunag, Y. Xiang member, IEEE, Ashley Chonka, J. Zhou, and R. H. Deng Senior member, IEEE,2010. A generic framework for three-factor authentication: Preserving security and privacy in distributed systems, IEEE Transactions on Parallel and Distributed System.
10. Jingquan Wang, Guilin Wang and Willy Susilo, 2013. Anonymous single sign-on schemes transformed from group signatures, International conference of intelligent networking and collaborative systems.