Analyzing Security of Single Sign on System through Advanced Encryption Standard

P.Manju Bala[1] M.O.Ramkumar[2]
[1]Senior Assistant professor, [2]Assistant professor
Department of Computer science and Engineering
IFET College of Engineering
Villupuram, Tamilnadu

Received: 14-01-2014, **Revised:** 25-03-2014, **Accepted:** 07-05-2014, **Published online:** 20-06-2014

ABSTRACT:- Single sign-on mechanisms allow users to sign on only once and have their identities automatically verified by each application or service they want to access afterward. Most of current application architectures require the user to memorize and utilize a different set of credentials (e.g., username/password or tokens) for each application he/she wants to access. In this paper, however, it is shown that their scheme is actually insecure as it fails to meet security during communication. This paper illustrates the Chang & Lee scheme and it aims to enhance security using AES encryption and decryption. The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data recognized by the U.S. National Institute of Standards and Technology. It is expected to become the accepted means of encrypting digital information, telecommunications, including financial, and government data.

KEYWORDS:-*Authentication, Attacks, Decryption, Encryption, Single Sign on*

I. INTRODUCTION

In the distributed computer networks, allow users to access 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 can therefore be granted access to the services requested. To avoid bogus servers, users usually need to authenticate service providers. After mutual authentication, a session key may be negotiated to keep the confidentiality of the data exchanged between a user and a service provider. In many scenarios, the anonymity of legal users must be protected as well. However, practice has shown that it is a big challenge to design efficient and secure authentication protocols with these security properties in complex computer network environments.

Lee and Chang [4] proposed a user identification and key distribution scheme to maintain user anonymity in distributed computer networks. Wu and Hsu pointed out that the Lee–Chang scheme is insecure against both impersonation attacks and identity disclosure attacks.

It is not practical by asking one user to maintain distinct pairs of identity and password for different service providers, since this could increase the workload of both users and service providers as well as the communication overhead of networks. To tackle this problem, the single sign-on (SSO) mechanism has been introduced so that, after obtaining a credential from a trusted authority for a short period (say one day), each legal user's authentication agent can use this single credential to complete authentication on behalf of the user and then access multiple service providers. Intuitively, an SSO scheme should meet at least three basic security requirements, i.e., *unforgeability*, *credential privacy*, and *soundness*. Unforgeability demands that, except the trusted authority, even a collusion of users and service providers are not able to forge a valid credential for a new user. 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 to other service providers. Soundness means that an unregistered user without a credential should not be able to access the services offered by service providers. Formal security definitions of unforceability and credential privacy.

Chang and Lee made a careful study of SSO mechanism. First, they argued that the Hsu–Chuang user identification scheme, actually an SSO scheme, has two weaknesses: 1) an outsider can forge a valid credential by mounting a credential forging attack since the Hsu–Chang scheme employed naive RSA signature without using any hash function to issue a credential for any random identity selected by a user (in fact, this feature inherits from) and 2) the Hsu–

Chuang scheme requires clock synchronization since it uses a time stamp. Then, Chang and Lee presented an interesting RSA-based SSO scheme, which does not rely on clock synchronization by using a nonce instead of a time stamp. Finally, they presented a well-organized security analysis to show that their SSO scheme supports secure mutual authentication, session key agreement, and user anonymity.

In this paper, we show that the Chang–Lee scheme is actually insecure by presenting two impersonation attacks, i.e., credential recovering attack and impersonation attack without credentials. In the first attack, a malicious service provider who has communicated with a legal user twice can successfully recover the user's credential. Then, the malicious service provider can impersonate the user to access resources and services provided by other service providers. The other attack may enable an outside attacker without any valid credential to impersonate a legal user or even a nonexistent user to have free access to the services. These two attacks imply that the Chang–Lee SSO scheme fails to meet credential privacy and soundness, which are essential requirements for SSO schemes and authentication protocols. We also identify the flaws in their security arguments in order to explain why it is possible to mount our attacks against their scheme this paper aims to ensure more security to the existing Chang Lee SSO scheme. It also aims to add additional security during data transfer between user and provider. It also proposes further research into more efficient enhancements to the current work. The main objective of this paper is to enhance security for single sign-on solutions and eliminate the need for users to repeatedly prove their identities to different applications and hold different credentials for each application.

II.RELATED WORK

Lee and Chang[4] proposed a user identification and key distribution scheme to maintain user anonymity in distributed computer networks. Later, Wu and Hsu pointed out that Lee-Chang scheme is insecure against both impersonation attack and identity disclosure attack. Meanwhile, Yang et al.[10] identified a weakness in Wu-Hsu scheme and proposed an improvement. However, Mangipudi and Katti [9] pointed out that Yang et al."s scheme suffers from DoS (Deniable of Service) attack and presented a new scheme. Hsu et al. [7] showed that both Yang et al. and Mangipudi-Katti schemes were insecure under identity disclosure attack, and proposed an RSA-based user identification scheme to overcome the drawbacks.

On the other hand, it is usually not practical by asking one user to maintain different pairs of identity and passwords for different service providers, since this could increase the workload of both users and service providers as well as the communication overhead of networks. To tackle this problem, single sign-on (SSO) mechanism has been introduced 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. 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. Formal security definitions of SSO schemes were given in. Chang and Lee made a careful study of SSO mechanism. Firstly, they argued that Chin-Chen Chang [3] user identification scheme, actually an SSO scheme, has two weaknesses: (a) An outsider can forge a valid credential by mounting a credential forging attack since Hsu-Chang scheme employed naive RSA signature without any hash function to issue a credential for any random identity selected by a user; and (b) Chin-Chen Chang [3] scheme requires clock synchronization since timestamp is used in their scheme. Then, Chang and Lee [4] presented an interesting RSA based SSO scheme, which is highly efficient in computation and communication (So it is suitable for mobile devices), and does not rely on clock synchronization by using nonce instead of timestamp. Finally, they presented well-organized security analysis to show that their SSO scheme supports secure mutual authentication, session key agreement, and user anonymity. In, Hanet.al. Proposed a generic SSO construction which relies on broadcast encryption plus zero knowledge (ZK) proof showing that the prover knows the corresponding private key of a given public key. So, implicitly each user is assumed to have been issued a public key in a public key infrastructure (PKI). In the setting of RSA cryptosystem, such a ZK proof is very inefficient due to the complexity of interactive communications between the prover (a user) and the verifier (a service provider). Therefore, compared with generic scheme, Chang-Lee scheme[4] has several attracting features: less

underlying primitives without using broadcast encryption, high efficiency without resort to ZK proof, and no requirement of PKI for users.

Notations	Descriptions
SCPC	A trusted authority
U_i, P_j	The user and the service provider, respectively
ID_X	The identity of the entity X
S_X	The secret token of the entity X
e_X	The public key of the entity X
d_X	The private key of entity X
$E_K(M)$	A symmetric encryption of plaintext M using a key K
$D_K(C)$	A symmetric decryption of ciphertext C using a key K
$h(\cdot)$	The one-way hash function
$\|$	The concatenation operator

Table 1: Notations used in the algorithm

III.PROPOSED SYSTEM

AES has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits, whereas Rijndael can be specified with key and block sizes in any multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits. AES operates on a 4×4 array of bytes, termed the state. For encryption, each round of AES (except the last round) consists of four stages. a) SubBytes - a non-linear substitution step where each byte is replaced with another according to a lookup table (known as S Box). b) ShiftRows - a transposition step where each row of the state is shifted cyclically a certain number of steps. c) MixColumns - a mixing operation which operates on the columns of the state, combining the four bytes in each column using a linear transformation. d) AddRoundKey - each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

AES algorithm comprises of various rounds depending on the key size and block size,(Fig No.1).Out of all the rounds the Pre- round comprises only AddRoundKey whereas the final round omits the MixColumns stage.

Number of rounds (Nr)	128-bit Data	192-bit Data	256-bit Data
128-bit Key	10	12	14
192-bit Key	12	12	14
256-bit Key	14	14	14

Fig.1. Hardware I/O Specifications

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 (e, g, n, N).

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 i = (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:

Ui submit the request with a random nonce n1, m1 to Pj. On receiving m1, Pj chooses a random number k and then generates a random nonce n2. Pj calculates Z = g k mod n, u = h (Z||ID j ||n1), and the signature v = (u||h (u)) d j mod Nj .Next, Pj sends the message m2 = {Z, v, n2} back to Ui . After receiving m2 from Pj, Ui computes u =h (Z||ID j ||n1) and performs the next step. Ui verifies the signature v by checking the equivalency of v e j mod N? = (u||h (u)) mod Nj. Otherwise, Ui informs Pj that someone has tampered with Z and aborts the protocol. Otherwise, Ui choose a random number t to be his short-term private key and computes w = g t mod n. Ui calculates the parameter k ij as kij = Z t mod n. U i generates a random nonce n3 and calculates three parameters K ij , x and y in accordance with the following equations: K ij = h(ID j ||kij), the session key, x= Si h(Kij ||w||n2) mod N, y = E Kij (IDi||n3||n2), where E(·) is a symmetric crypto system such as DES or AES. Ui sends m3= {w, x, y} to Pj After receiving m3, P j computes k ij as k ij = w k mod n. P j can obtain the session key K ij by computing K ij=h (ID j || kij). Pj uses K ij to decrypt cipher text y and retrieves IDi, n3, and n2. If n2 is valid, Pj computes SIDi = (IDi||h (IDi)). Pj verifies the validity of the identity IDi by checking SID ih (Kij ||w||n2) mod N? = x e mod N. If the equation holds, Pj trusts that Ui is a legal user. Pj computes V = h (n3) and sends m4 = {V} to Ui. After receiving m4 from Pj, Ui computes V ||= h (n3) and confirms that V? = V „. When both the equations are same, Ui trusts that Pj is an authorized service provider

and P j has really calculated the common session key K ij.

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.

PERFORMANE COMPARISON

Number of objects	**AES**	**RSA**	**RSA**
Key length (bits)	128	512	1024
100	2314	3021	3925
200	3080	6030	7096
300	4405	18171	17168

Table 2: Comparing AES algorithm with RSA algorithm in terms of performance

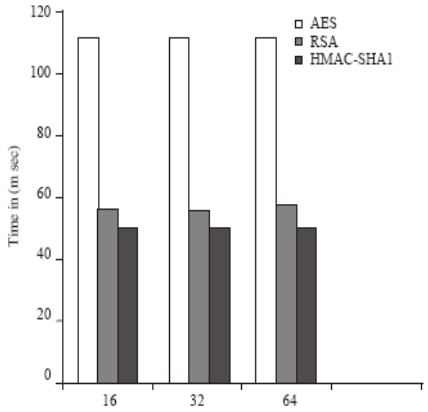

Fig.2.Comparison of the cryptographic algorithm with the time taken vs different key sizes

IV. METHODOLOGY

In the existing system, different security schemes are proposed by many researchers. In the proposed system, various .Client-Server programs are written to implement the project using socket programming in Java. This work uses the multithreading features of Java to run in parallel for different providers. Chang-Lee algorithm is used for user identification phase. But, it is using a less secure DES algorithm. This paper user a more secure AES algorithm to enhance the security features. So, this scheme is more secure than Chang-Lee scheme.

V. CONCLUSION

This paper proposes a secure single sign-on mechanism based on one-way hash functions and random nonce's to solve the weaknesses described above and to decrease the overhead of the system. Encryption and Decryption of data sent between user and provider can improve security of communication. Encryption and Decryption process can be done using a more secure algorithm, i.e., AES Encryption. AES is strong enough to be certified for use by the US govt. for top secret information. AES is federal information processing standard and there are currently no known non-brute-force attacks against AES. Thus AES is given priority than other standards when security is taken into consideration. By using this SSO scheme, users need only one password for secure access to all applications and systems and would lock out the hackers entering into the system. But there are some vulnerability problems and there should be a good password, one that is very hard to crack.

VI. FUTURE WORK

This paper 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.

VII. REFERENCES

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

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

[3]. Chin-Chen Chang, "A secure single mechanism for distributed computer networks," IEEE Trans. On Industrial Electronics, vol.59, no. 1, Jan 2012.

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

[7]. 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.

[8]. 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.

[9]. 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.

[10]. 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.