www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 10 Oct 2015, Page No. 14609-14612

Security Mechanism for Authentication

Mr. Kurhe B. S. Prof., Deokate Gajanan S
Second Year Master of Engineering
Department of Computer Engineering
Sharadchandra Pawar College of Engineering, Dumbarwadi, Otur, Pune, India,
Email- b.kurhe@gmail.com

Assistant Professor
Department of Computer Engineering,
Sharadchandra Pawar College of Engineering, Dumbarwadi, Otur, Pune, India
Email- deokate.gd@gmail.com

***Abstract*— This mechanisms allow users to sign on only once and have their identities automatically verified by each application or service they want to access afterwards. There are many practical and secure single sign-on models even though it is of great importance to current distributed application. Many application architectures required the user to memorized and utilize a different set of credentials (eg, username/password or tokens) for each application he/she wants permission. In this approach is not practical and not secure with the exponential growth in the number of applications and services a user has to access both inside corporative environments. This 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. In this paper we proposed a new single sign-on scheme and claimed its security by providing well-organized security arguments. In this paper shows the Chang & Lee scheme and it aims to enhance security using RSA encryption and decryption. The programming part is done using socket programming in Java. Identification of user is an important access control mechanism for client–server networking architectures. The goal of this platform is to eliminate individual sign on procedures by centralizing user authentication and identity management at a central identity provider. In this paper a SSO the user should seamlessly authenticate to his multiple user accounts (across different systems) once he proves his identity to the identity provider.**

***Keywords*- Single Sign On (SSO), Zero Knowledge (ZK), Public Key Infrastructure (PKI)**

I. INTRODUCTION

With the widespread use of distributed pc networks, it has become common to permit users to access numerous network services offered by distributed service providers. Consequently, user authentication (also called user identification) plays an important role to verify if a user is legal in distributed computer networks and can so be granted access to the services requested. To avoid phony servers, users sometimes ought to attest service providers. Once mutual authentication, a session key is also 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 secured as well. On the other side, it is usually unpractical by asking one user to maintain distinct pairs of identity and password for different providers, since this could increase the load of both users and service providers as well as the communication overhead of networks. To avoid 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, each user's authentication person can use this single credential to complete authentication on behalf of the user and then access multiple service providers. An SSO scheme should meet at least three basic security requirements, i.e., enforceability, privacy.

II. LITERATURE SURVEY

In the literature survey we will go to discuss various existing methods which allow user to access the services from multiple service providers in network. Below discussing some of them.

Chang and Lee proposed scheme. But in that two attacks are found as the First attack allows a malicious/bogus service details and then it act as a genuine service provider for user to access resources. In another attack, an unregistered without any credential details able to access services offered by service provider. This leads to attack . L. Harn and J. Ren proposed a similar concept like SSO known as generalized digital certificate (GDC), in this system authentication is done by digital certificate [5]. It is used in wireless network system will get the digital signature GDC which is provided by a trusted authority, after that user can authenticate self with the help of GCD signature. Every user will get unique GCD Signature. Hsu–Chuang user identification scheme is also based on SSO mechanism. There are two drawback found in this scheme

a) an outside user can able to create a valid authentication details without registered to any trusted authority and with that details also able to access services [1].

b) This requires clock synchronization as it is based on time stamp.

Han proposed a generic SSO structure. This is based on broadcast encryption in Addition with zero Knowledge (ZK) proof [1]. In this scheme user knows the equivalent private key of a given public key. With this each user is considered to have been issued a public key in a public key infrastructure (PKI). By making use of RSA cryptosystem ZK proof is very inefficient and unproductive due to the complexity of interactive communications between the a user and the verifier (a service provider) [9]. A. C. Weaver and M. W. Condtry propose an alternative- a client server architecture that can

assign some multifaceted data processing and device interface tasks to a network device, the Net Edge [2]

III. Existing System

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 avoid this problem, single sign-on (SSO) mechanism is introduced so that after obtaining a login from a trusted authority each legal user can use this single credential to authenticate itself and then access multiple service providers. This scheme should meet at least two basic Security requirements ex: soundness and credential privacy. In Soundness means that an unregistered user without a credential should not be able to access the services offered by service providers and 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.Actually AN SSO theme, has 2 weaknesses outsider will forget a sound written document by mounting a written document formation attack since the theme utilized naïve RSA signature while not mistreatment any hash operate to issue a written document for any random identity.Their theme is appropriate for mobile devices because of its high potency in computation and communication.This paper aims to reinforce security mistreatment RSA cryptography and decipherment.We denote the safety flaw of Hsu and Chuang's theme as follows.Hsu–Chuang's theme really uses the RSA cryptosystem to generate a secure token Si for every user [1].
In other words, Si is thought to be the signature of the identity.
As know, a signature supported RSA is existentially forgeable.
Common a tendency to demonstrate this doable attack as follows. Assume that AN assaulter UA needs to Masquerade as legal user Ui to grant permission to the Service supplier Pj.
Assume that AN assaulter UA needs to Masquerade as legal user to grant permission to the Service supplier Pj.It is first determined whether or not a Mathematical algorithmic program is recited directly or indirectly within the claim.If so, it's next determined whether or not the claimed invention as a full is not any quite the algorithmic program itself; that's, whether or not the claim is directed to a mathematical algorithmic program that's not applied to or restricted by physical components or method steps.Such claims are non-statutory However, once the mathematical algorithmic program is applied in one or additional steps of AN otherwise statutory method claim, or one or additional components of AN otherwise statutory equipment claim, the wants of section a hundred and one are met[12].

IV. Proposed Work

SSO is a session/user authentication process that permits a user to enter one name and password in order to access multiple applications. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session. SSO is the ability for a user to enter the same id and password to logon to multiple applications within an enterprise. As passwords are the least secure authentication mechanism, single sign on has now become known as reduced sign on (RSA) since more than one type of authentication mechanism is used according to enterprise risk models. Ability to enforce uniform enterprise authentication and/or authorization policies across the enterprise. End to end user audit sessions to improve security reporting and auditing. Removes application developers from having to understand and implement identity security in their applications usually results in significant password help desk cost savings [12], [3].

Fig 1: Single Sign on System

In this paper present a new protocol that allows two players to exchange digital signatures over the Internet in a fair way, so that either each player gets the other's signature or neither player does. The obvious application is where the signatures represent items of value, for example, an electronic check or airline ticket. The protocol can also be adapted to exchange encrypted data. It relies on a trusted third party, but is "optimistic," in that the third party is only needed in cases where one player crashes or attempts to cheat. A key feature of our protocol is that a player can always force a timely and fair termination, without the cooperation of the other player, even in a completely asynchronous network. A specialization of our protocol can be used for contract signing; this specialization is not only more efficient, but also has the important property that the third party can be held accountable for its actions: if it ever cheats, this can be detected and proven. AS MORE business is conducted over the Internet, the fair exchange problem assumes increasing importance. For example, suppose player is willing to give an electronic check to player in exchange for an electronic airline ticket. The Problem is this: how can and exchange these items so that either each player gets the other's item, or neither player does. Both electronic checks and electronic airline tickets are implemented as digital signatures. Presumably, many other items to be exchanged over the Internet will be so implemented. Therefore, it seems fruitful to focus our attention on the fair exchange of digital signatures[5].

A. User Identification Phase

Fig 2: User Identification Phase

This method check RSA signature using DH key .To access the resources of service provider, user needs to go through the authentication protocol. A symmetric key encryption scheme which is used to protect the confidentiality of user's identity. Suppose a service request message from user, service provider generates and return user message which is made up by RSA on Signature Once this signature is validated, it means that user has authenticated service provider successfully. If he receives any message service provider can confirm validity by checking .After that the user generates the key temporarily. Once u close the process the same key does not work automatically your

session are stopped [7].

V. RECOVERING ATTACK

The malicious and then mount the above attack. On the one hand, the Chang–Lee SSO scheme specifies that is the trusted party. So, this implies that service providers are not trusted parties and that they could be malicious. By agreeing with, when they said that "the Wu–Hsu's modified version cold not protect the user's token against a malicious service provider, the work also implicitly agrees that there is the potential for attacks from

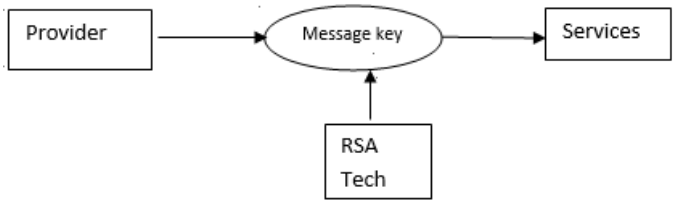

Fig 3: SSO with RSA

Malicious service providers against SSO schemes. Moreover, if all service providers are assumed to be trusted, to identify him/her user can simply encrypt his/her credential under the RSA public key of service provider. Then, can easily decrypt this cipher text to get 's credential and verify its validity by checking if it is a correct signature issued by . In fact, such a straightforward scheme with strong assumption is much simpler, more efficient and has better security, at least against this type of attack [6], [7].

VI. NON-INTERACTIVE ZERO KNOWLEDGE (NZK)

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 non-interactive zero-knowledge (NZK) proof to convince Bob that she has signed the message and the trusted 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 [1], [4].

VII. SECURITY ANALYSIS

The security of the improved SSO scheme by focusing on the security of the user authentication part, especially soundness and credential privacy due to two reasons. On the one hand, the enforceability of the credential is guaranteed by the enforceability of RSA signatures, and the security of service provider authentication is ensured by the enforceability of the secure signature scheme chosen by each service provider [10].

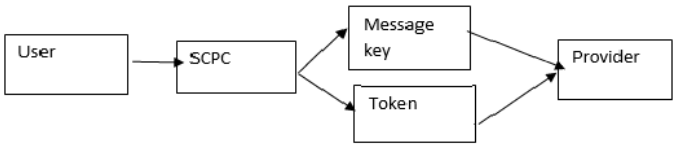

Fig 4: Security Analysis

Algorithm: RSA-VES

Definition

A public-key encryption technology developed by RSA Data Security, Inc. The acronym stands for Rivest, Shamir, and Adelman, the inventors of the technique. The RSA algorithm is based on the fact that there is no efficient way to factor very large numbers. Deducing an RSA key [8], therefore, requires an extraordinary amount of computer processing power and time. The RSA algorithm has become the de facto standard for industrial-strength encryption, especially for data sent over the Internet. It is built into many software products, including Netscape Navigator and Explorer. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. It's also part of Lotus Notes, Intuit's Quicken, and many other products. The encryption system is owned by RSA Security. The company licenses the algorithm technologies and also sells development kits. The technologies are part of existing or proposed Web, Internet, and computing standards [1].

Example

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < &phi(n) and e and n are coprime. Let e = 7
- Compute a value for d such that (d * e) % &phi (n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$
- The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$
- Select random prime numbers p and q, and check that p != q
- Compute modulus n = pq
- Compute phi,= (p - 1)(q - 1)
- Select public exponent e, 1 < e <such that gcd(e,) = 1
- Compute private exponent d = e

VIII. CONCLUSION

This paper adresses the limitations of Chang and Lee's single sign-on (SSO) scheme against two types of attacks and proposees an improved Chang–Lee scheme to achieve soundness and credential privacy. This propose scheme will improve the security single sign on mechanism.As future work, it is interesting to formally define authentication soundness and construct efficient and provably secure single sign-on schemes.

REFERENCES

[1] Guilin Wang, Jiangshan Yu, and Qi Xie "Security Analysis of a Single Sign On Mechanism for Distributed Computer

Networks", *IEEE ON INDUSTRIAL INFORMATICS*, VOL 9 PAGE NO 1 FEBRUARY 2013

[2] A. C. Weaver and M. W. Condtry, "Distributing internet services to the network edge" *IEEE Transaction Ind. Electron*, volume 50 no. 402 to 413, June 2003.

[3] L. Barolli and F. Xhafa, "JXTA-OVERLAY A P2P platform for distributed, collaborative and ubiquitous computing system" *IEEE Transaction Ind. Electron*. Volume 58 no. 6 pp. 2160 to 2174 October 2010.

[4] L. Lamport, "Password authentication with insecure communication" Communication *ACM volume* 24 no 11 pp 770 to 774, November 1981.

[5] Lein Harn and Jian Ren," Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications", *IEEE TRANSACTIONS* JULY 2011.

[6] Manuel Cheminod, Alfredo Pironti, and Riccardo Sisto,"Formal Vulnerability Analysis of a Security System for Remote Fieldbus Access", *IEEE TRANSACTIONS* FEBRUARY 2011.

[7] Jason Bau and John C. Mitchell," Security Modeling and Analysis", *IEEE* MAY/JUNE 2011.

[8] Xiaohu Li, Timothy Paul Parker, and Shouhuai Xu," A Stochastic Model for Quantitative Security Analyses of Networked Systems", *IEEE TRANSACTIONS* JANUARY FEBRUARY
2011.

[9] Xiangxue Li,et.al.," Anonymity Enhancement on Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards",*IEEE TRANSACTIONS* FEBRUARY 2010.

[10] Vittorio Giovannetti, Seth Lloyd and Lorenzo Maccone," Quantum Private Queries: Security Analysis", *IEEE TRANSACTIONS* JULY 2010.

[11] W. B. Lee and C. C. Chang, "User identification and key distribution maintaining anonymity for distributed computer networks," Comput.Syst.Sci.Eng., vol. 15, no. 4, pp. 113–116, 2000.

[12] C.-L. Hsu and Y.-H. Chuang, "A novel user identification scheme with key distribution preserving user anonymity for distributed computer networks,"*Inf. Sci*., vol. 179, no. 4, pp. 422–429, 2009.