Efficient Verifiable Encryption of RSA signatures for Distributed Computer Networks

A.Poorna Chandra Reddy [1], Assistant Professor
Christu Jyothi Institute of Technology & Science, Jangaon
Komala G [2], Assistant Professor
Christu Jyothi Institute of Technology & Science, Jangaon

ABSTRACT:

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. Recently, Chang and Lee proposed 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 fails 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. 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. Moreover, by employing an efficient verifiable encryption of RSA signatures proposed by Ateniese, we
propose an improvement for repairing the Chang–Lee scheme. We promote the formal study of the soundness of authentication as one open problem.

1. INTRODUCTION:

Identification of user is an important access control mechanism for client–server networking architectures. The goal of a single sign on platform is to eliminate individual sign on procedures by centralizing user authentication and identity management at a central identity provider. In a single sign-on solution, the user should seamlessly authenticated to his multiple user accounts (across different systems) once he proves his identity to the identity provider. Nevertheless, in many current solutions, the user is required to repeat sign on for each service using the same set of credentials, which are validated at the identity provider by each service. User authentication [1], [2] plays a crucial role in distributed computer networks to verify the legacy of a user and then can be granted to access the services requested. To prevent bogus servers, users usually need to authenticate service providers. After mutual authentication, a session key may be negotiated to keep the confidentiality of data exchanged between a user and a provider [2], [3], [4]. In many scenarios, the anonymity of legal users should be protected as well [2], [5], [4]. These protocols offer varying degrees of efficiency. 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.

2. RELATED WORK:

In 2000, Lee and Chang [2] proposed a user identification and key distribution scheme to maintain user anonymity in distributed computer networks. Later, Wu and Hsu [6] pointed out that Lee-Chang scheme is insecure against both impersonation attack and identity disclosure attack. Meanwhile, Yang et al. [7] identified a weakness in Wu-Hsu scheme and proposed an improvement. In 2006, however, Mangipudi and Katti [8] pointed out that Yang et al."s scheme suffers from DoS (Deniable of Service) attack and presented a new scheme. In 2009, Hsu and Chuang [9] 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 [10] 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. In [11], Han et 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 Han et al.‟s generic scheme, Chang-Lee scheme 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.

3. PROBLEM STATEMENT:

3.1: EXISTING SYSTEM

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. Instinctively an SSO 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.

DISADVANTAGES:

- Actually an SSO scheme, has two weaknesses an outsider can forge a valid credential by mounting a credential forging attack since the scheme employed naïve RSA signature without using any hash function to issue a credential for any random identity.
- Their scheme is suitable for mobile devices due to its high efficiency in computation and communication.

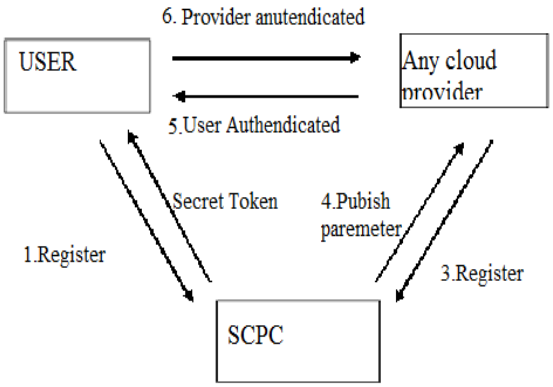
3.2: PROPOSED SYSTEM

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. This attack based on RSA Techniques. The other attack, an “impersonation attack without credentials(session attack),” demonstrates how an outside attacker may be able to freely make use of resources and services offered by service providers. The attackers can successfully impersonate a legal user without holding a valid credential and thus violate the requirement of soundness for an SSO scheme. In a real life these attacks may put both users and service providers at high risk In fact; this is a traditional as well as prudential way to deal with trustworthiness. we cannot simply assume that beside the trusted authority for all service providers are also trusted.

ADVANTAGES:

- Users need only one password for access to all applications and systems. Users have immediately have access to all necessary password-protected applications.
- Users don't need to remember multiple passwords. Users don't have to guess passwords, which potentially expose applications to unauthorized users
- The authors claimed to be able to: “prove that and are able to authenticate 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 scheme could withstand impersonation attacks.
- The authors did not give details to show how the BAN logic can be used to prove that their scheme guarantees mutual authentication.
- In other words, it means that in an SSO scheme suffering these attacks there are alternatives which enable passing through authentication without credentials.

4. SYSTEM ARCHITECTURE:



5. MODULES

Module Description:

1.User Identification Phase

To access the resources of service provider, user needs to go through the authentication protocol specified. Here, and are random integers chosen by and, respectively; and are three random nonces; and denotes a symmetric key encryption scheme which is used to protect the confidentiality of user's identity.

2. Attacks against the Chang–Lee Scheme

The Chang–Lee scheme is actually not a secure SSO scheme because there are two potential effective and concrete impersonation attacks. The first attack, the "credential recovering attack" compromises the credential privacy in the Chang–Lee scheme as a malicious service provider is able to recover the credential of a legal user. 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, 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 put both users and service providers at high risk.

3. 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 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.

4. 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.

5. 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 unforgeability of the credential is guaranteed by the unforgeability of

RSA signatures, and the security of service provider authentication is ensured by the unforgeability of the secure signature scheme chosen by each service provider.

6. FUTURE ENHANCEMENT:

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.

7. CONCLUSION:

Single sign-on (SSO) using ECC 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. The syste using ECC is more cost efficient, provide good security with smaller key sizes and faster execution. ECC is useful for battery-limited devices with limited power supply and also provide lower computational cost and lower communication cost.

8. REFERENCES:

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

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

[3]. 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.

[4]. 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.

[5]. 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.

[6]. 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.

[7]. 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.

[8]. 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.

[9]. 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.

[10]. Data Encryption Standard, NIST Std. FIPS PUB 46-2, 1988.

[11]. Advanced Encryption Standard, NIST Std. FIPS PUB 197, 2001.