DYNAMIC ID BASED ENCRYPTION USING SINGLE SIGN-ON MECHANISM

[1]H.Aneesha, [2]G.Gokula Krishnan, [3]H.Shabuddeen
[1]PG Scholar, Department of Information Technology, Jayam College of Engineering and Technology, Dharmapuri
[2]Associate Professor, Department of Information Technology, Jayam College of Engineering and Technology, Dharmapuri
[3]Assistant Professor, Department of Information Technology, Jayam College of Engineering and Technology, Dharmapuri
[1]aneeshabtech@gmail.com, [2]gokualmaths@gmail.com , [3]shabuddeen@gmail.com

Abstract: In 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 afterwards. There are few practical and secure single sign on models, even though it is of great importance to current distributed application environments. 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. However, this approach is inefficient and insecure with the exponential growth in the number of applications and services a user has to access both inside corporative environments and at the Internet. 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 distributed computer networks. Recently, Chang and Lee proposed a new SSO scheme and claimed its security by providing well organized security arguments. In this paper, however, it is shown that their scheme is actually insecure as it fails to meet security during communication, in order to provide a secure authentication digital signature with hash function is researched for future work.

1. INTRODUCTION

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. 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 environment.

In 2000, Lee and Chang proposed a user identification and key distribution scheme to maintain user anonymity in distributed computer networks. Later, Wu and Hsu pointed out that the Lee–Chang scheme is insecure against both impersonation attacks and identity disclosure attacks. Above scheme suffers from Deniable of Service (DoS) attacks and presented a new scheme.

On the other side, it is usually not practical by asking one user to maintain distinct pairs of identity and password for different service providers. Since this could increase the work load of 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.

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 use 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.

The other side, it is usually 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. That, after obtaining a credential from a trusted authority for a short period 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, enforceability, credential privacy, and soundness. Enforceability 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.By exploiting a smart card, this paper presents a robust and efficient password-authenticated key agreement scheme. This paper strengthens the security of the scheme by addressing untraceability property such that any third party over the communication channel cannot tell whether or not he has seen the same smart card twice through the authentication sessions. The proposed remedy also prevents a kind of denial of service attack found in the original scheme. High performance and other good functionalities are preserved.

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.

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. 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 In fact; this is a traditional as well as prudential way to deal with trustworthiness, since we cannot simply assume that beside the trusted authority, all service providers are also trusted. The basic reason is that assuming the existence of a trusted party is the strongest supposition in cryptography but it is usually very costly to develop and maintain.

In particular defined collusion impersonation attacks as a way to capture the scenarios in which malicious service providers.

Recover a user's credential and then impersonate the user to login to other service providers. It is easy to see that the above credential recovery attack is simply a special case of collusion impersonation attack where a single malicious service provider can recover a user's credential.

It must be emphasized that impersonation attacks without valid credentials seriously violate the security of SSO schemes as it allows attackers to be successfully authenticated without first obtaining a valid credential from the trusted authority after registration.

2. RELATED WORK ON SECURITY AND ACCESS CONTROL

We demonstrated two effective impersonation attacks on Chang and Lee's single sign-on (SSO) scheme. The first attack shows that their scheme cannot protect the privacy of a user's credential, and thus, a malicious service provider can impersonate a legal user in order to enjoy the resources and services from other service providers.

The second attack violates the soundness of authentication by giving an outside attacker without credential the chance to impersonate even a non-existent user and then freely access resources and services provided by service providers. We also discussed why their well-organized security arguments are not strong enough to guarantee the security of their SSO scheme.

In addition, we explained why Hsu and Chuang's scheme is also vulnerable to these attacks. Furthermore, by employing an efficient verifiable encryption of RSA signatures introduced by Ateniese we proposed an

improved Chang–Lee scheme to achieve soundness and credential privacy.

Anonymity (i.e., the secrecy of the identities of communicating agents) is becoming a major concern in many multiuser electronic commerce and industrial engineering applications. For example, anonymity service is one of the crucial focuses for wireless communications and requires that the identity of any mobile user should be protected from the foreign agent.

2.1 Credential Recovering Attack

In 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. 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 In fact; this is a traditional as well as prudential way to deal with trustworthiness, since we cannot simply assume that beside the trusted authority, all service providers are also trusted. The basic reason is that assuming the existence of a trusted party is the strongest supposition in cryptography but it is usually very costly to develop and maintain.

In particular defined collusion impersonation attacks as a way to capture the scenarios in which malicious service providers may recover a user's credential and then impersonate the user to login to other service providers. It is easy to see that the above credential recovery attack is simply a special case of collusion impersonation attack where a single malicious service provider can recover a user's credential.

3.2 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 nonce's; and denotes a symmetric key encryption scheme which is used to protect the confidentiality of user's identity.

3.3 Attacks against Chang-Lee Scheme

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.

3.4 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.

3.5 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 no 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.

3.6 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 provide.

3.7 Dynamic Id Based Encryption and Hashing Algorithm

Steps for Data Authentication

Step1: sender encrypts message using receiver public key.

Step2: when receiver receives message from sender, receiver request a private key from key server.

Step3: the key server sends an investigating message to sender, for receiver authentication.

Step4: after getting the verification message from sender, the key generator provides a private key to receiver for decryption any time.

Steps for Node Authentication

Step 1: User u generates hash id using H(n) = PUB_KEY/ IDENTITY

Step 2: Neighbors node also generates hash id in the same way

Step 3:

If

{

If (hash_id (user) = hash_id (provider))

Then node is authenticated

}

Else

{

Node is malicious node

}

4. CONCLUSION

In This proposed System demonstrated two effective impersonation attacks on Chang and Lee's single sign-on (SSO) scheme. The first attack shows that their scheme cannot protect the privacy of a user's credential, and thus, a malicious service provider can impersonate a legal user in order to enjoy the resources and services from other service providers. The second attack violates the soundness of authentication by giving an outside attacker without credential the chance to impersonate even a non-existent user and then freely access resources and services provided by service providers. I also discussed why their well-organized security arguments are not strong enough to guarantee the security of their SSO scheme. In addition, I explained why Hsu and Chuang's scheme is also vulnerable to these attacks.

Furthermore, by employing an efficient verifiable encryption of RSA signatures introduced by Ateniese, I proposed an improved Chang–Lee scheme to achieve soundness and credential privacy. As future work, it is interesting to formally define authentication soundness and construct efficient and provably secure single sign-on schemes. Based on the draft of this work a preliminary formal model addressing the soundness of SSO has been proposed in. Further research is necessary to investigate the maturity of this model and study how the security of the improved SSO scheme proposed in this paper can be formally proven.

REFERENCES

[1] Barolli .L, Oct. 2010, ―JXTA-OVERLAY: A P2P platform for distributed, collaborative and ubiquitous computing,‖ IEEE Trans. Ind. Electron., vol. 58, no. 6, pp. 2163–2172.

[2] Cheminod .M, Feb. 2011 , ―Formal vulnerability analysis of a security system for remote field bus access,‖ IEEE Trans. Ind. Inf., vol. 7, no. 1, pp. 30–40.

[3] Chuang , 2009, ―A novel user identification scheme with key distribution preserving user anonymity for distributed computer networks,‖ Inf. Sci., vol. 179, no. 4, pp. 422–429.

[4] Fabian .B, Aug. 2012 ―SHARDIS: A privacy-enhanced discovery service for RFID-based product information,‖ IEEE Trans. Ind. Inf., vol.

8, no. 3, pp. 707– 718.

[5] Hsu .C.-L, 2004, ―Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks,‖ Comput. Security, vol. 23, no. 2, pp. 120–125.

[6] Juang .W , Jun. 2008, ―Robust and efficient password authenticated key agreement using smart cards,‖ IEEE Trans. Ind. Electron., vol. 15, no. 6, pp. 2551–2556.

[7] Lamport.L, Nov.1981,―Password authentication with insecure communication,‖ Commun. ACM, vol. 24, no. 11, pp. 770–772.

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

[9] Ma .M ,Aug. 2012. ―A server independent authentication scheme for RFID systems,‖ IEEE Trans. Ind. Inf., vol. 8, no. 3, pp. 689–696.

[10] Mangipudi K.V, 2006. ―A secure identification and key agreement protocol with user anonymity (SIKA),‖ Comput. Security, vol. 25, no. 6, pp. 420–425.

[11] Sun H.M, Apr. 2012,―oPass: A user authentication protocol resistant to password stealing and password reuse attacks,‖ IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 651–663.

[12] Valenzano .A,2012,―Review of security issues in industrial networks,‖ IEEE Trans. Ind. Inf., vol. PP, no. 99, DOI 10.1109/TII/2012.2198666.

[13] Wang .S, 2004. ―New efficient user identification and key distribution scheme providing enhanced security,‖ Comput. Security, vol. 23, no. 8, pp. 697–704.

[14] Weaver A.C, Jun. 2003, ―Distributing internet services to the network's edge,‖ IEEE Trans. Ind. Electron., vol. 50, no. 3, pp. 404–411.

[15] Zheng .D,Feb. 2010, ―Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards,‖ IEEE Trans. Ind. Electron., vol. 57, no. 2, pp. 793–800.