International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 2, Issue 1, No 3, 2014. ISSN: 2348-6600
Reference ID: IJCS-045. PAGE NO: 256-259.

PRIVACY ENHANCED NEW MECHANISM FOR DCN USING DYNAMIC ID BASED ENCRYPTION AND HASHING ALGORITHM

THANGAPONNU.V

M.E COMPUTER SCIENCE AND ENGINEERING

BHARATHIYAR INSTITUTE OF ENGINEERING FOR WOMEN

DEVIYAKURICHI

thangaponnuvarutharaj@gmail.com

Abstract— The Single sign-on (SSO) is an authentication mechanism that enables a legal user with a single credential to be authenticated by multiple service providers in a distributed computer network. The Chang and Lee proposed a new SSO scheme and claimed its security by providing well-organized security arguments. Their scheme is actually insecure as it fails to meet credential privacy and soundness of authentication. Specifically, it present two impersonation attacks. The first attack allows malicious service provider has successfully communicated with a user twice, to recover the credential of a user and then to impersonate the user to access resources and services offered by other service providers. The another attack is that an outsider without any credential may be able to enjoy network services freely by impersonating any legal user .The formal study of the soundness of authentication as one open problem.

. ***Index Terms*—Single sign-on, authentication, distributed computer networks ,security analysis.**

I. 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 Denial 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 Workload of both users and service providers as well as the communication overhead of networks. 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.

.

II. EXISTING SYSTEM

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. 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. So 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.

A. Disadvantages of Existing System

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 2, Issue 1, No 3, 2014. ISSN: 2348-6600
Reference ID: IJCS-045. PAGE NO: 256-259.

- 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.

- It is suitable for mobile devices due to its high efficiency in computation and communication.

.

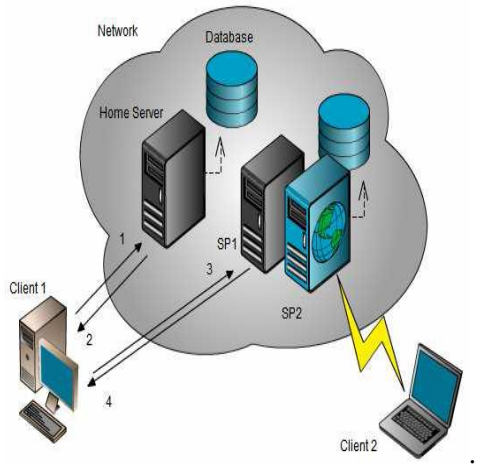
III. PROPOSED SYSTEM

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. 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.

A. Advantages of Proposed System

- Users need only one password for access to all applications and systems. Users have immediately have access to all necessary password-protected applications.
- The authors claimed to be able to: "prove that and are able to authenticate each other using the authentication protocol" .

B. System Architecture



C. Module Description

The user authentication phase provides all the details of authentication part. The second module gives the description for attacks against chang-lee scheme.

1) User Identification Phase: To access the resources of service provider Pj, user Ui needs to go through the authentication protocol .Here ,k and t are random integers chosen by Pj and Ui , respectively;n1,n2 and n3 are three random nonces; and E(.)denotes a symmetric key encryption scheme which is used to protect the confidentiality of user 's identity . We highlight this phase as follows.

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 (hash_id (user) = hash_id(provider))
            Then node is authenticated
         }
      Else
        {
            Node is malicious node

        }
```

2) Attacks Against 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

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 2, Issue 1, No 3, 2014. ISSN: 2348-6600
Reference ID: IJCS-045. PAGE NO: 256-259.

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 ciphertext to get 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. Credential privacy or credential irrecoverableness requires that there be a negligible probability of an attacker recovering a valid credential from the interactions with a user. Signature hiding means that an attacker cannot extract a signature from VES without help from the user who encrypted the signature or the trusted authority who can decrypt a VES. So ,if this improved SSO scheme fails to meet credential privacy, it implies that Ateniese's RSA-VES fails to satisfy signature hiding.

D .CONCLUSIONS

There are 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. It also discussed why their well-organized security arguments are not strong enough to guarantee the security of their SSO scheme. In addition 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 , 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 can be formally proven.

REFERENCES

[1] Lamport L. (1981) 'Password authentication with insecure communication' Commun. ACM, vol. 24, no. 11, pp. 770–772.
[2] Lee W.B. and Chang C.C (2000) 'User identification and key distribution maintaining anonymity for distributed computer networks' Comput. Syst. Sci. Eng., vol. 15, no. 4, pp. 113–116.
[3] Weaver A.C. and Condtry M.W. (2003) 'Distributing internet services to the network's edge' IEEE Trans. Ind. Electron., vol. 50, no. 3, pp. 404–411.
[4] Wu T.S. and 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.

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 2, Issue 1, No 3, 2014. ISSN: 2348-6600
Reference ID: IJCS-045. PAGE NO: 256-259.

[5] Juang W. Chen S. and Liaw H.(2008) 'Robust and efficient password authenticated key agreement using smart cards' IEEE Trans. Ind. Electron., vol. 15, no. 6, pp. 2551–2556.
[6] Barolli L. and Xhafa F. (2010) 'JXTA-OVERLAY: A P2P platform for distributed, collaborative and ubiquitous computing' IEEE Trans. Ind. Electron., vol. 58, no. 6, pp. 2163–2172.
[7] Cheminod M., Pironti A., and Sisto R. (2011) 'Formal vulnerability analysis of a security system for remote fieldbus access' IEEE Trans. Ind. Inf., vol. 7, no. 1, pp.
[8] Valenzano A., Durante L., and Cheminod M. (2012) 'Review of security issues in industrial networks' IEEE Trans. Ind. Inf., vol. PP, no. 99.
[9] M. Bellare and P. Rogaway, "Entity authentication and key distribution," in *Proc. of CRYPTO'*, 1993, pp. 232–249
.
[10] 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.*, vol. 57, no. 2, pp. 793–800,Feb. 2010.
[11] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A practical and provably secure coalition-resistant group signature scheme," in *Proc.CRYPTO*, 2000, pp. 255–270.
[12] 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.
[13] B.Wang and M. Ma, "A server independent authentication for RFID systems," *IEEE Trans. Ind. Inf.*, vol. 8, no. 3, pp. 689–696.

Published by SK Research Group of Companies (SKRGC).