ISSN 2349-6193
Impact Factor: 2.805

IJESMR

International Journal OF Engineering Sciences &Management Research

SECURE SINGLE SIGN-ON (SSO) MECHANISM FOR ELLIPTIC CURVE CRYPTOGRAPHY (ECC) ON DISTRIBUTED COMPUTER NETWORKS

V.Suresh[*1], **B.Venkatesh**[2] **& A.Anajaneyulu**[3]
[*1,2&3]Department of ECM (Electronics and Computer Engineering), Vignan's Institute of Information Technology, Duvvada, Visakhapatnam -530049,A.P., India

Keywords: *Single Sign-On (SSO), Authentication, credential privacy, Soundness, Unforgeability, Distributed Computer Networks*

ABSTRACT

This paper introduces a Single sign on (SSO) mechanism that uses Elliptic Curve Cryptography (ECC) to avoid the communication overheads as well as the workload of both the users and the service providers in the network. Single sign on mechanism allow users to sign on using single credential and to enjoy the services provided by the multiple service providers in a distributed computer network. This mechanism includes, after obtaining a credential from a trusted authority, each legal user's authentication agent can use that credential to complete authentication on behalf of the user and can then access multiple service providers. A detailed up-to-date discussion and various techniques on Single Sign-On mechanism in distributed computer networks have been done. ECC is an alternative mechanism for implementing public-key cryptography. Public-key algorithms create a mechanism for sharing keys among large numbers of participants in a complex information system. Since ECC helps to establish equivalent security with smaller key size, lower computing power and battery resource usage, it can also be widely used for mobile applications. Unlike other popular algorithms such as RSA, ECC is based on discrete logarithms that are much more difficult to challenge.

INTRODUCTION

There is an increased chance for forgery, authentication of user is very important in every application of this modern world. It is an important access control mechanism in which, after mutual authentication between the users and the service providers, a session key may be negotiated to keep the confidentiality of the data exchanged between them. The internet is growing every day, and the performance of computers and networks is appreciably increased, enabling the improvement of complex large-scale applications. It is difficult to remember the identity/password required to access each service provider in the network. User authentication which plays a crucial role in this Single Sign On mechanism scheme, identifies whether a user is legal or not. Hence, a Single Sign On mechanism is proposed in which, a user with single credential can be authenticated by multiple service providers in a distributed network.

There are three basic security requirements in a SSO scheme i.e., unforgeability, credential privacy and soundness of authentication. Unforgeability demands that, except the trusted authority, none can 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 act as that user to login to other service providers. Soundness of authentication says an unregistered user without any credential should not be able to access the services offered by the service providers. This paper aims to provide a more secure authentication mechanism.

RELATED WORKS

The SSO scheme for various studies which includes the following: 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 Lee-Chang scheme is insecure against both impersonation attack and identity disclosure attack. Meanwhile, Yang et al. identified a weakness in Wu-Hsu scheme and proposed an improvement. In 2006, however, Mangipudi and Katti pointed out that Yang et al. scheme suffers from DoS (Deniable of Service) attack and presented a new scheme. In 2009, Hsu and Chuang 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.

Hence, a single sign-on (SSO) mechanism has been introduced so that, after obtaining a credential from a trusted authority, 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. It is usually impractical to ask one user to maintain distinct pairs of identity and passwords to access different service providers within a distributed network.. A similar concept, called the generalized digital certificate (GDC), was proposed to provide user authentication and key agreement in wireless networks [10]. In this concept, a user holds a digital signature of his/her GDC issued by an authority, can authenticate him/herself to a verifier by proving the knowledge of the signature without revealing it.

Compared to other previous schemes Chang-Lee scheme is more efficient in terms of computation as well as communication. It has got several attracting features also: less underlying primitives without using broadcast encryption, high efficiency without resort to ZK proof, and no requirement of PKI for users. The Chang–Lee scheme is actually insecure by presenting two impersonation attacks:

- Credential recovering attack.
- 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.

To avoid the above attacks, an improved SSO scheme was proposed to enhance the user authentication phase of the Chang-Lee scheme. For this, the efficient RSA-based Verifiable Encryption of Signatures (VES) proposed by Ateniese was employed to verifiably and securely encrypt a user's credential. With the involvement of RSA VES (Verifiable Encryption of Signatures), soundness and signature hiding are the two core security properties to guarantee the fairness of digital signature exchange. 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. But there are several limitations also for this scheme. It includes the key generation, which is comparatively very slower. Various other limitations include:

- Time taken for encryption/decryption is very high.
- Large amount of memory storage.
- More CPU consumption.
- Less security.

PROPOSED SCHEME

The proposed scheme includes the Elliptic Curve Cryptography (ECC), which is an alternative mechanism for implementing public-key cryptography. Public-key algorithms create a mechanism for sharing keys among large numbers of participants in a complex information system. Unlike other popular algorithms such as RSA, ECC is based on discrete logarithms that are much more difficult to challenge.

Various phases included in this scheme include:

1. System Initialization
2. Registration Phase
3. Authentication Phase
4. Session Maintaining Phase

1. System Initialization

Smart Card Producing Center (SCPC), the trusted authority, chooses the two prime numbers, and key pairs. Then SCPC publishes system initialization, keeps some value as secret, and erases the prime numbers immediately once this phase has been completed.

RSA cryptosystems are used to initialize the trusted authority, called SCPC (smart card producing center), and service providers. Each user applies a credential from the trusted producing center), and service providers. Each user applies a credential from the trusted authority SCPC, who signs the RSA signature for user's hashed identity. After that, the user uses a kind of knowledge proof to show that he/she is in possession of the valid credential without revealing his/her identity to eavesdroppers.

2. Registration Phase

The users and the providers have to register in order to enjoy the services. They chooses one unique identity ID, gets converted into fixed bit-length, concatenates with the hash of that ID and gets stored in SCPC system for further authentication. At the same time, each service provider with identity should maintain its own RSA public parameters and private key as done by SCPC.

Upon receiving a register request, SCPC gives fixed-length unique identity and issues a credential, which is calculated as SCPC's RSA signature. Each service provider with an identity should maintain a pair of signing/verifying keys for a secure signature scheme. The signature on the message is signed using the signing key. Verifying of signature and public key is done and the outputs “1” or “0” indicate whether the signature is valid or invalid.

3. Authentication Phase

To access the resources of service provider, user needs to go through the authentication. Here, two random integers are chosen by both the provider and the user respectively. Upon receiving a service request message from the user, the service provider generates and returns user message which is made up primarily by its ECC signature on. Once this signature is validated, it means that the user has authenticated the service provider successfully.

4. Session Maintaining Phase

After authentication is completed between the user and the providers, one session ID is provided for mutual communication between them. This will be maintained securely for the entire session in order to avoid the attacks.

The figure below shows the work flow of the entire scheme in which the SCPC is initialized as the trusted authority. Then the users and the providers along with its services will register at SCPC and obtains a valid credential. The users can login using this credential and can select the required service from the list of services displayed after the successful mutual authentication. A session ID provided for mutual communication will be maintained securely for the entire session in order to avoid the attacks.

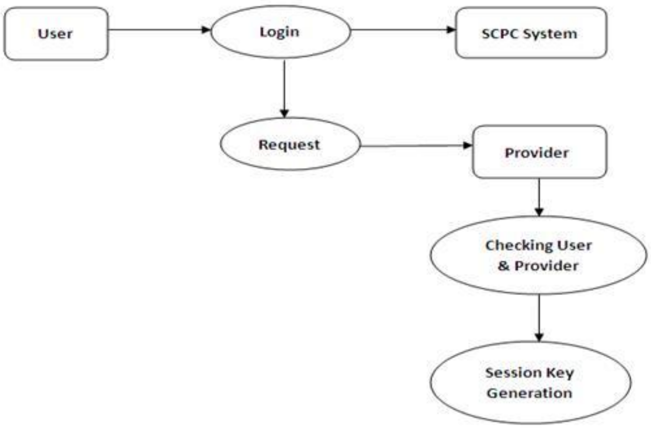

Fig.1. Workflow diagram

CONCLUSION

Using SSO mechanism, after obtaining a credential from a trusted authority, each legal user's authentication agent can use the single credential to complete authentication on behalf of the user and then access multiple service providers. A SSO mechanism that uses Elliptic Curve Cryptography (ECC) algorithm which is an alternative mechanism for implementing public-key cryptography is presented. Public-key algorithms create a mechanism for sharing keys among large numbers of participants in a complex information system. Unlike other popular algorithms such as RSA, ECC is based on discrete logarithms that are much more difficult to challenge. Since ECC is widely used for mobile applications , it helps to establish equivalent security with smaller key size, lower computing power and battery resource usage.

REFERENCES

1. *Chin-Chen Chang, "A secure single mechanism for distributed computer networks," IEEE Trans. On Industrial Electronics, vol. 59, no. 1, Jan 2012.*
2. *Guilin Wang, Jiangshan Yu and Qi Xie,"Security Analysis of a Single Sign-On Mechanism for Distributed Computer Networks", IEEE Trans. on Industrial Informatics, vol.9 no.1, Feb 2013.*
3. *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.*
4. *L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications," IEEE Trans. Wireless Commun., vol. 10, no. 7, pp. 2372–2379, Jul. 2011.*
5. *L.Lamport, "Password authentication with insecure communication", Commun. ACM, 24(11): 770-772, Nov. 1981.*
6. *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.*
7. *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.*
8. *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.*
9. *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.*
10. *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*