Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 3, Issue 3; April-June, 2016, pp. 138-140
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

A Survey on Mutual Authentication Secure Against Previleged-Insider Attack

Aashima Sood[1] and Shivi Sharma[2]

[1,2]L. R. College of Engineering Solan (H. P. T. U) L. R. College of Engineering Solan (H. P. T. U)
E-mail: [1]aashima018@yahoo.com, [2]shivisharma28@gmail.com

Abstract—*With increase in the number of smart devices which have the ability to connect over the internet for using the services like internet banking, online shopping, e-payment etc need of secure protocol against various attacks with low computation load is there. As a result of which active research is going on in this field. In order to check whether remote user is legal or not, remote user authentication becomes significant. Here malicious insider may harm the organization. Also, external attacker impersonates an insider by using insider credentials. In spite of this, the protocols used in a real world are inefficient. For this, key agreement protocol such as Elliptic curve cryptography plays significant role. ECC is a scheme to public key cryptography based on the algebraic structure of elliptic curves. It requires smaller keys in order to give security. ECC are used for pseudo-random generator, encryption and decryption, several integer factorization algorithms and some other tasks. ECC can be suitably used in mobile because of low-memory and efficient computation. ECC is required for safety aspect. Key generation is an significant part in ECC in which both public and private key is generated. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key. Hence, mutual authentication is used. It is also refers as two way authentication. It is an important feature for a verification service and is gaining acceptance as a tool that can minimize the risk of online fraud. [1,4-6]*

Keyword: *ECC – Elliptic Curve Cryptography*

1. INTRODUCTION

As there is increase in the number of smart devices, anyone can easily use e- services such as online shopping, internet banking etc. anytime everywhere. Thus the importance of secure communication is there. Computer security means the protection afforded to an information system so as to achieve integrity and confidentiality of resources such as software ,data ,hardware etc. Security attacks are of two types passive attacks and active attacks. Here we are dealing more with the active attacks such as modification of messages by the man in the middle attack. A security mechanism is thus a device or a kind of process that is designed to detect, prevent and recover from such attacks. Example include authentication protocol and encryption algorithm. Security is not as simple as it might first appear but the mechanism used to meet those requirement involve complex reasoning with the help of number theory. In order to check whether remote user is legal or not with any insecure channel, Remote user authentication is used. ECC can be suitably used in mobile because of low-memory and efficient computation. And this protocol should ensure the security from the privileged-insider attack. This malicious insider may harm the organization by accessing properties of the company using user's account. This protocol is very efficient and also provides more security. It is efficiently acceptable to mobile using ECC computation. Several approaches to encryption decryption using elliptic curve have been analyzed. Each user involved in communication have a pair of keys, a public key and a private key and also a set of operations known as cryptographic operations. Security of ECC depends on how difficult is the elliptic curve discrete logarithm problem. Two operations are involved in ECC – Point multiplication and point addition. Further, for accurate and efficient operations on elliptic curve two finite fields are defined – Prime field and Binary field. [1-2,4-6]

1.1 Security Threats

1. **Eavesdropping**: The process of extracting information by an unauthorized person from the communicating channel.
2. **Location privacy:** a malicious person may expose a person's location through tracing his tag.
3. **Spoofing:.** It is the process of injecting wrong information by an unauthorized person
4. **Replay attack and DOS attack**: a poor designed tag identification protocol may suffer from replay attack or deny-of-service (DOS) attack.
5. **Impersonation:** Here the attacker uses the identity of another node to gain unauthorized access to some data.

1.2 Mutual authentication

A two level hierarchy is used to provide security. In this a session key is distributed. In this authentication system, user or client authenticating themselves to a server. This server can authenticate itself to the user in such a way that both parties are assured of the others' identity. It is also refers as two-way 4 user authentication. Mutual authentication is an important feature for a verification and is widely being accepted as a tool that can reduce the risk of online fraud in e-commerce. Therefore, is very efficient. [5]

1. 3 Elliptic curve cryptography (ECC)

ECC is a scheme to public key cryptography based on the number theory. ECC makes use of elliptic curves in which the variables and coefficient are all restricted to elements of finite fields-Primary field and Secondary field. In this, elliptic curve arithmetic can be used to develop a variety of ECC schemes. Elliptic curve cryptography requires smaller keys in order to give security. ECC are used for pseudo-random generator, key exchange and encryption and decryption The advantages of ECC are given as:

1. ECC can be suitably used in mobile because of low-memory.
2. ECC to ensure the security from the privileged-insider attack which is otherwise a huge threat.
3. The principle attraction of ECC is that it offers equal security for smaller key size as compared to RSA. [2,4,6]

2. LITERATURE SURVEY

Chen, Tien-Ho, Hsiu-lien Yeh, and Wei-Kuan Shih et al. [1] proposed that an ECC dynamic id-based remote mutual authentication scheme. This paper analyzed novel approach used for mobile devices. The proposed scheme is highly secured mutual authentication. Moreover, in this paper proposed scheme has been analyzed and indicates that this scheme is more secured to authenticate users and remote servers for mobile devices.

Yoon, Eun-Jun, and Kee-Young Yooet al. [2] in this paper new authentication scheme has been presented which is based on a one-way hash function and Diffie-Hellman key exchange. This proposed scheme is suitable for mobile communication and it required less computational costs. Diffie-Hellman key exchange could help to isolate various issues and it provide mutual authentication between the user and the remote system.

Kim, Hyun-Sung, Sung-Woon Lee, and Kee-Young Yoo et al. [3] this paper proposes two ID-based password authentication schemes, which does not require a dictionary of passwords or verification tables, with smart card and fingerprint. In these schemes, users can change their passwords freely. For a network without synchronization clocks, the proposed nonce-based authentication scheme can withstand message replay attacks. The proposed two schemes require a system to authenticate each user by each user's knowledge, possession, and biometrics, and this feature makes our schemes more reliable

Liao, Yi-Pin, and Shuenn-Shyang Wang et al. [4] presented a authentication scheme which is secured and used for multi-server environment. The entire requirement can satisfy with this novel approach. These schemes achieve user's anonymity and also help to manage the secret key table which is associated with users. This approach uses hashing functions in order to implement mutual verification and session key agreement. This scheme is well suited to the smart card's applications.

Chen, Yalin, Jue-Sam Chou et al. [5] proposed a Jules's scheme which is vulnerable to known-plaintext and replay attacks. As, several other secure schemes have been proposed for RFID systems but only few of them can attain TID anonymity, individual location privacy and forward. Furthermore, mutual authentication RFID approach has been presented based on quadratic residues. This proposed scheme is very efficient in terms of security.

Liao, I-En, Cheng-Chi Lee et al. [6] in this paper, slight modification has been to their scheme to improve their weaknesses. In this paper, it is pointed out that the Das-Saxena Gulati scheme is not strong enough against some security weaknesses. There fore,a slight modification of their scheme has been proposed. The proposed scheme does not only achieve their advantages but also enhances their security by withstanding the weaknesses. The efficiency of the proposed scheme is even higher than that of their scheme. In addition, the proposed scheme does not add many computational costs additionally. Compare with their scheme, our scheme is also efficient.

Arshad, Hamed et al. [7] proposed a secure authentication and key agreement approach for session initiation protocol. This approach is based on the elliptical cryptograph curve. Its security analyses indicate that proposed approach is secure against attacks of different types.

Jin, Chunhua, et al [8] proposed an RFID mutual authentication scheme. This is based on elliptic curve cryptography In order to increase the patient medication safety. This approach can attain security requirement and provides better performance with low computational cost.

Farash, Mohammad Sabzinejad et al. [9] proposed a improved password-based authenticated key agreement protocol in order to overcome security problem. This proposed protocol is analyzed in random oracle model. The result indicates that its gives low computational cost, better efficiency and performance as compared with other protocol.

Mishra, Dheerendra et al. [10] presented a secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using smart card. This scheme is used to overcome the weakness and is simulated for the formal security using Automated Validation of Internet Security Protocols and Applications.

3. CONCLUSION

In this review paper, we have discussed various techniques for improving authentication between the two parties depending on the different types of attacks. Some has used ID based authentication and others have used ECC. As new authentication techniques are coming up day in and out so it is making network more secure. So, ECC is the newer and promising topic in this regard. Here if the study including ECC is proceeded further so it will drive a more meaningful result. Also these schemes which are based on id based are somewhat based on timestamp which makes them more authentic and further helps in verification. This scheme can withstand message replay attack.

4. ACKNOWLEDGEMENT

First of all I would like to thank my worthy supervisor Ms Shivi Sharma (Asst. Professor), in the department of Computer Science and Engineering at L. R. Institute Solan. She is helping me further by providing all possible guidance and support. Also all my teachers, classmates, lab incharges with all the help that I am getting. I hope with such good support I will be able to complete my research in the coming month.

REFERENCES

[1] Arshad, Hamed, and MortezaNikooghadam. "An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC. " *Multimedia Tools and Applications* 75, no. 1 (2016): 181-197.

[2] Chen, Tien-Ho, Hsiu-lien Yeh, and Wei-Kuan Shih. "*An advanced ecc dynamic id-based remote mutual authentication scheme for cloud computing. "* Multimedia and Ubiquitous Engineering (MUE), 2011 5th FTRA International Conference on. IEEE, 2011.

[3] Chen, Yalin, Jue-Sam Chou, and Hung-Min Sun. "A novel mutual authentication scheme based on quadratic residues for RFID systems. " Computer Networks 52. 12 (2008): 2373-2380.

[4] Dong Hoon Lee, Hyoseung Kim and Song Yi kim "An efficient Id-based secure in computer network"

[5] Dr. Sanjay Sharma, Author –"Principles of Computer Networks"

[6] William Stallings, Author-"Cryptography and Network Security"