Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 44 No. 11
November 2023

Key Agreement Protocol (KAP) to PREVENT from ATTACKS of SOCIAL NETWORK SERVICES

Dr. Sr. S. Thiraviya Regina Rajam[1], Dr. S. Arul Jothi[2]
[1]Vice Principal and Asst. prof of Computer science,
Madonna Arts and Science College for Women,
Madurai, Tamil Nadu, India.
[2]Asst. Professor, Department of Computer Science
Fatima College
Madurai, Tamil Nadu, India.

Abstract— In today's technological world information security is essential for commercial, legal trading, secrecy, truthfulness and non-reputability. The Elliptic Curve Cryptography (ECC) has become one of the latest trends in the field of Public-Key Cryptography (PKC). In this Proposed new algorithm ECC and also the Key Agreement Protocol (KAP) promises a faster, efficient and more secured method to improve the security called Enhanced Elliptic Curve Cryptography (EECC)Algorithm. It is developed for the Social Network service. The developed protocol KAP prevents the system from various network security attacks like identity theft, reply, parallel session , passive. reflection, interleaving and Man –In –The-Middle attacks. The EECC algorithm helps to assure end to end encryption for Online Social Network (OSN) users. This approach reveals a significant feature of high level security by providing KAP. The proposed protocol used in research, to prevent the system from various security attacks.

Keywords— Elliptic Curve Cryptography (ECC), Public Key Cryptography

1. INTRODUCTION

Pippal et al.[1] pointed out that impersonation attack, session attacks and reply attacks can be launched in the password attacks. The attractiveness of using elliptic curves arises from the fact that similar lever of security can be achieved with considerably shorter keys than in methods based on the difficulties of solving discrete logarithms over integers or integer factorizations.

Elliptic Curve Cryptography (ECC) employed a relatively short encryption key, and a value that must be nourished into the encryption algorithm which are used to decipher an encrypted message. Therefore the short key was faster and required a very small computing power than the other first-generation encryption public key algorithms. Elliptic curve Cryptosystem was more secure than cryptosystems based on discrete logs over finite fields or integer factorization and elliptic curve cryptosystem seemed to be the most efficient and secure public key cryptosystem. The ECC 160-bit encryption key provided the similar type of security as a 1024-bit RSA encryption key and the same was upto 15 times quicker, depending on the platform used for the purpose. Integrated cryptographic systems satisfy all the requirements. Desired properties of a secure communication system many times include any one or all of the following listed ingredients.

The reminder of this paper is as follows. Section 2, explains the definition of the problem. The methods are described in section 3. The enhanced EECC algorithm explained is explained in section4. The KAP is described in section 5. The related works is explained in section 6. The section 7 is ended with the conclusion.

2. PROBLEM DEFINITION

1. Elliptic Curve Cryptography (ECC)algorithm increases the size of Encrypted Mes¬sage and more Complex difficult implement
2. Implementation attack errors.

3. METHODOLOGY

The EECC algorithm helps to assure end to end encryption for Online Social Network (OSN) users.The proposed algorithm was designed to

assure end to end encryption for OSN users.This work introduces an enhanced as asymmetric random point Enhanced Elliptic Curve Cryptography (EECC) algorithm that differs from the standard ECC with the third random point. The data are then encrypted through a secured novel algorithm called EECC for storing user data onto the database promises a faster and more secure method of encryption compared to any other standard public-key cryptosystem with the possibilities of making the algorithm more efficient and secure through EECC algorithm. Elliptic curves E are a specific class of mathematical algebraic curves over prime finite fields (Fq). Figure 1 shows the EECC algorithm. The proposed protocols KAP prevent the system from various network security attacks like identity theft, reply, parallel session , passive. reflection, interleaving and Man – In –The-Middle attacks.

4. ENHANCED ECC ALGORITHM

The data are encrypted through a secured novel algorithm called Enhanced Elliptic Curve Cryptography (EECC) for storing user data onto the database. The proposed Security Framework for Social Network Service enables a faster and more secure method of encryption compared to any other standard public-key cryptosystem. There are possibilities of making the algorithm more efficient and secure through EECC algorithm. There are two basic operations in EECC namely point addition and point doubling. The EECC multiplication is the operation of successively adding a point along the elliptic curve.

A. Point Addition

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E with $P_1, P_2 \neq \infty$.

$P_1 + P_2 = P_3 = (x_3, y_3)$ defines as follows

If $x_1 \neq x_2$ then

$$x_3 = m^2 - x_1 - x_2, \quad (1)$$

$$y_3 = m(x_1 - x_3) - y_1 \quad (2)$$

$$m = y_2 - y_1 \quad (3)$$

If $x_1 = x2$ but $y_1 \neq y2$ then $P_1 + P_2 = \infty$

B. Point Doubling

If $P_1 = P_2$ and $y_1 \neq 0$ then

$$x_3 = m^2 - 2x_1 \quad (4)$$

$$y3 = m(x1 - x3) - y1 \quad (5)$$

The ECC encryption uses key agreement establishment protocol, which consists of a set of rules and regulations that governs the security of communication in a network. It is based on elliptic curve cryptography with Discrete Diffie-Hellman (DDH) method. This protocol is designed to ensure firm identity privacy of the user. In the proposed system, key agreement protocol of the elliptic curve ($y2=x3+Ax+B$) is taken. The elliptic curve (E) is defined by equation (6) over F(q) with a large group F of points on the curve, order q and a base point P.

$$y^2 = x^3 + Ax + B \quad (6)$$

It is assumed that A and B share the parameters of the elliptic curve E , group G and the base point P. The protocol has three stages: setup stage, key exchange stage and execution stage.

C. Setup Stage

Setup can also be called prerequisite stage which takes care of the prerequisite arrangements that are necessary for the secured establishment of communication. This phase generates a group of curve points P, derived from the elliptical curve equation over the prime q. The points on E form an additive abelian group with infinity (∞) as the identity element and elliptic curve addition as the group operator. When the data are to be exchanged, this phase generates, a random base point P to be agreed between the users.

D. Key Exchange Stage

In this phase, every user involved in the communication chooses a random private key k (1 to q-1) to be multiplied with base point P. To agree on a shared key, the users (sender and receiver) individually generate key pairs (k_i*P) and (k_j*P) respectively. Then they exchange the public keys k_i*P and k_j*P, such that each can compute the points Sk = (k_i kj*P) = ($k_j k_i$*P) using their respective private keys.

E. Execution Stage

The shared secret key (Sk) is derived by substituting the K co-ordinates in the elliptic curve equation (6) by a key derivation function for encryption. The inverse function for SK is

executed at the receiver machine for decryption. Figure 1 shows the flow diagram of Enhanced ECC.

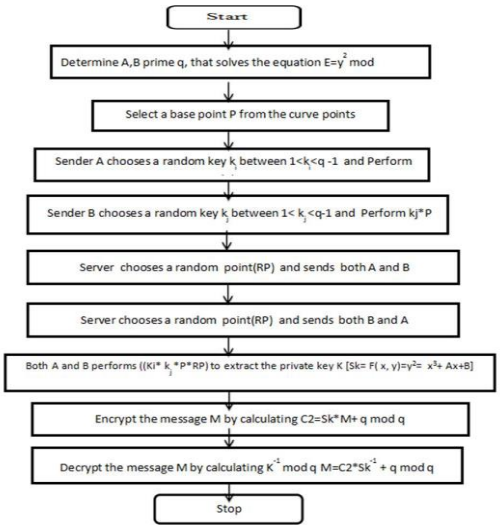

Fig. 1. Flow diagram of Enhanced ECC

5. The KAP

A. Key Agreement Protocol (KAP) for Security Attacks

The KAP helps to prevent the system from various network security attacks such as the identity theft, replay, parallel session, passive, reflection, interleaving, and Man-In-The-Middle attacks.

B. Identity Protection

The proposed system does not give any loops to the attackers to guess the identification of the user. Since the community users' credentials are transferred through post method, where the data are explicitly hidden via insecure channel. Figure 2 depicts the identity protection through two-factor password protection from theft.

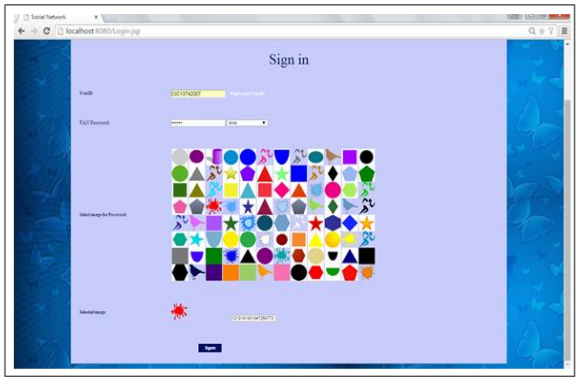

Fig. 2. Screenshot of Shap Code password

C. Replay attack

The replay attack is when an attacker tries to imitate the user to log into the server by resending the messages transmitted between the user and the server. In the proposed work, the data are transmitted only in encrypted formthrough the communication channel. Even if the attacker underplays the reply from the server user cannot recover original message, unless, the attackers know the private key to decrypt the message. Figure 3 shows prevention from replay attack.

```
UserId=cic102
5c2a5c487c14
fullname=Raj
3b4179
Email=raj@gmail.com
6241794e0f60412a11615c7b60
Mno=9876543210
3165164a7e2f6314487c
Dob=10/May/1991
487c2d39417f2d48313148
FontCode=1210
4814487c
Pass=muthukumar
60497d5e494549604162
Dob=0510
7c7e487c
```

Prevention from replay attack.

6. RELATED WORKS

M.Aydos et.al [2] has presented an implementation of ECC over the field GF(p) on an 80 MHz, 32 bit RAM microprocessor along with the results. Kristin Lauter has provided an overview of ECC for wireless security [3]. It focuses on the performance advantages in the wireless environment by using ECC instead of the traditional RSA cryptosystem. Ray C., [4] in his work has explained the design of a generator, which automatically produces a customized ECC hardware that meets user-defined requirements. C. J. McIvor et.al [5] introduces a novel hardware architecture for ECC over GF(p). The work presented by Gang Chen presents a high performance ECC cryptographic process for general curves over GF(p) [6]. Rajeswari et al. [7] proposed a simple and efficient authentication protocol based on ECC for Mobile networks. They implemented a protocol which establishes the secure communication between base station and nodes in mobile networks. The protocol proposed by them, was new one for verification scheme, having simplicity and efficiency. The

protocol was designed by employing a most acquainted public-key cryptographic scheme, ECC and then it was keen to mobile networks for verification of base station. The server base station was meant to receive the information and the client node was meant to transmit the information to a valid server base station. The application of this protocol in mobile networks allowed only the official base station to access the node and hence it was denying the information to eavesdroppers when they tried to hack or misuse the node. Barman et al. suggested an idea on E-Governance Security using public key cryptography[8]. An approach using biometric signatures, based on the ECC was implied in E-Governance. The use of ECC in biometric signature creation improved the electronic banking security and in this technique the public and private keys were created without transmitting and storing any private information.

7. Conclusion

The security EECC algorithms provide strong authentication and avoid the security threat of attacks by tampering. The proposed algorithms are developed using Public Key Infrastructure, which ensures the security needs of community user transactions in an integrated manner. It provides a cost-effective means to manage security administration, activity and operations for community applications like social network applications. Thus, the system supports effectively community requirements of the organization. The user interface encrypts the data with standard asymmetric key cryptography. The EECC algorithm supports end-to-end communication between community groups.The User ID and Passwords are stored by Ardamax KeyLogger software (information received from the key pad). It is visible to the user. Suppose biometric information is received, it is very hard to temper and store the information. Nowadays use of biometric information is not practical and so the proposed KAP mechanism is introduced and it highly secured from the attacks.

REFERENCES

1. R.S Pippal, C.D Jaidhar and S. Tapasw,i “Security issues in password authentication Scheme”, *International Journal of Computing Theory engineering*, vol.4 pp. 206-211, 2012.
2. M.Aydos, T.Yanik and C.K.Kog, "High-speed implementation of an ECC based wireless authentication protocol on an ARM microprocessor", *lEEE Proc. Communication system*.,Vol. 148, No.5, pp. 273-279, October 2001.
3. Kristin Lauter, "The Advantages of Elliptic Cryptography for Wireless Security", *IEEE Wireless Communications*, pp. 62- 67, Feb. 2006.
4. Ray C. C. Cheng, Nicolas Jean-baptiste, Wayne Luk, and Peter Y. K Cheung, "Customizable Elliptic Curve Cryptosystems", *IEEE Trans. On VLSISystems*, vol. 13, no. 9, pp. 1048-1059, Sep. 2005.
5. C. I. McIvor, M. McLoone, and I. V. McCanny, "Hardware elliptic curvecryptographic processor over GF(p)," *IEEE Trans. Circuits Syst.l Reg. Papers*, vol. 53, no. 9, pp. 1946-1957, Sep. 2006.
6. Gang Chen, Guoqiang Bai, and Hongyi Chen, "A High-Performance Elliptic Curve Cryptographic Processor for General Curves Over GF(p) Based on a Systolic Arithmetic Unit" , *IEEE Trans. Circuits Syst. - 11: Express Briefs*, vol. 54, no. 5, pp. 412- 416, May. 2007.
7. MPG Rajeswari and K Thilagavathi, “An Efficient Authentication Protocol Based on Elliptic Curve Cryptography for Mobile Networks”, *International Journal of Computer Science and Network Security*, Vol 2, pp.76–85,2009.
8. P Barman and B Saha, “E-Governance Security using Public Key Cryptography with special focus on ECC”, *Proceedings on Computer Engineering Science Invention*, vol .8, pp.10–16. 2013.