A Novel Remote User Authentication Scheme using Smart Card based on ECDLP

Debasish Jena[1], Sanjay Kumar Jena[2], Debashisa Mohanty[1], Saroj Kumar Panigrahy[2]
[1]*Centre for IT Education, Biju Patnaik University of Technology, Orissa 751010, India*
[2]*Department of Computer Science & Engineering*
National Institute of Technology Rourkela, Orissa-769 008, India
debasishjena@ieee.org, skjena@nitrkl.ac.in, debashisamohanty@yahoo.com

Abstract

In this paper, a novel efficient remote user authentication scheme using smart cards based on Elliptic Curve Discrete Logarithm Problem (ECDLP) has been proposed. A remote user authentication scheme is a two-party protocol whereby an authentication server confirms the identity of a remote individual logging on to the server over an untrusted, unsecured network. The password based authentication schemes are commonly used for authenticating remote users. Many passwords based schemes both with and without smart card have been proposed; each scheme has its merits and demerits. Our proposed scheme does not require verifier table and allows the user to choose their passwords. The proposed scheme also withstands message replying attack.

Keywords: Password, Smartcard, ECDLP, Remote.

1. Introduction

Remote user password based authentication scheme, proposed by Lamport [1] in 1981, is a way to authenticate the remote user over an insecure and untrusted network. His scheme can withstand replaying attacks, but requires a verification table to check the validity of the login request made by the user. After that, may scheme based on password table has been proposed. [2-4]. However, this approach introduces the risk and cost of managing and protecting the password table. To overcome this problem, several password authentication scheme with smart cards have been proposed [5-7]. The scheme proposed by Wu which [8] paper is based on simple geometric properties on the Euclidian plane has weakness in the security [9]. Elliptic curve cryptosystems gives more security with less bit size key and more computational fast than the other cryptosystems, because of this we proposed a a novel efficient remote user authentication scheme using smart cards based on Elliptic Curve Discrete Logarithm Problem (ECDLP)

The organization of this paper is as follows. In the Section 2, the basic concept of elliptic curve (EC) is discussed. In Section 3, discussion on Elliptic Curve Cryptosystem based on variation of ElGamal scheme has been made and subsequently, the proposed scheme is explained in section 4. The security analysis has been made in section 5. Finally, Section 6 describes the concluding remarks.

2. Elliptic curve over finite field

The use of Elliptic Curve Cryptography (ECC) was initially suggested by Neal Koblitz [10] and Victor S. Miller [11] and after that many researchers have suggested different application of Elliptic Curve Cryptosystems. Elliptic curve cryptosystems over finite fields have some advantages. One is the much smaller key size as compared to other cryptosystems like RSA or Diffie-Hellman, since: (a) only exponential-time attack is known so far if the curve is carefully chosen [12], and (b) elliptic curve discrete logarithms might be still intractable even if factoring and multiplicative group discrete logarithms are broken. ECC is also more computationally efficient than the first-generation public key systems such as RSA or Diffie-Hellman [13].

2.1. Elliptic curve groups over F_q

A non-super singular Elliptic curve E over F_q can be written as:

$$E: \quad y^2 \bmod q = (x^3 + ax + b) \bmod q \quad \ldots (1)$$

where $(4a^3 + 27b) \bmod q \neq 0$.

978-0-7695-3516-6/08 $25.00 © 2008 IEEE
DOI 10.1109/ICACC.2009.110

The points $P=(x,y)$ where $x,y\in F_q$. $P(x,y)$ that satisfy the Eqn. 4 together with a "point of infinity" denoted by O form an abelian group $(E,+,O)$ whose identity element is O.

2.1.1. Adding Distinct Points P and Q : The negative of the point $P=(x_1,y_1)$ is the point $-P=(x_1,-y_1)$. If $P(x_p,y_p)$ and $Q(x_q,y_q)$ are two distinct points such that P is not $-Q$, then

$$P+Q=R \quad \ldots (2)$$

where $R=(x_r,y_r)$.

$\therefore s=(y_p-y_q)/(x_p-x_q) \bmod q$ where $s.$ is the slope of the line passing through P and Q.

$x_r=(s^2-x_p-x_q) \bmod q$ and

$y_r=(-y_p+s(x_p-x_r)) \bmod q$

2.1.2. Doubling the Point P

Provided that y_p is not 0,

$$2P=R(x_r,y_r) \quad \ldots (3)$$

$\therefore s=((3x_p^2+a)/(2y_p)) \bmod q$

$x_r=(s^2-2x_p) \bmod q$ and

$y_r=(-y_p+s(x_p-x_r)) \bmod q$

The elliptic curve discrete logarithm problem is defined as follows [14].

Definition 1: Let E be an elliptic curve over a finite field F_q and let $P\in E(F_q)$ be a point of order n. Given $Q\in E(F_q)$, the elliptic curve discrete logarithm problem is to find the integer $d\in[0,n-1]$, such that $Q=dP$.

3. Elliptic curve crypto system based on Elgamal

Suppose Alice wishes to send a message M to Bob. First, she imbeds the value M onto the elliptic curve E , i.e. she represents the plaintext M as a point $P_m\in E$. Now she must encrypt P_m . Let d_B denote Bob's secret key. Alice first chooses a random integer k and sends Bob a pair of points on E:

$$(C_1,C_2)=(kG,P_m+k(d_BG))$$

To decrypt the cipher text, Bob computes

$$C_2-d_B(C_1)=P_m+k(d_BG)-d_B(kG)=P_m$$

4. Proposed scheme

In this section, we present our proposed remote user authentication scheme using smart cards based on ECDLP. We discuss three phases of our proposed scheme, namely registration phase, login phase and authentication phase. When a legal user wants to login the computer system, he/she has to insert his/her smart card into the login device and keys in his/her identity and password.

The notations used through out in this paper is as follows:

U	Remote user
ID	the identity of the remote user
PW	the password corresponding to the registered identity
AS	the authentication server
f (.)	a cryptographic one way hash function

4.1 Registration Phase:

Initially the curve domain parameters (q,FR,a,b,G,n,h) must be agreed upon by both the U and the AS , where q is the field order, FR is the field representation for F_q , G is the generator group, n is a large prime, and h is the division of N , the order of $E(F_q)$ to n . Here AS must have a key pair suitable for elliptic curve cryptography, consisting of a private key d_s (a randomly selected integer in the interval $[1,n-1]$) and a public key Q where $Q=d_sG$.

Initially the new user U submits his/her identity ID to the system for registration. The AS calculates the password PW as follows.

$$PW=d_sID$$

The registration centre issues a smart card which contains the public parameter (f, n, G, Q), where f is a one way function. The registration centre is also delivered PW to the user through a secure channel. The smart cards possessed by all users will contain the same data and functions i.e. (f, n, G, Q).

4.2 Login phase

Upon login, U attaches is smart card to his/her input device. Then he/she convert his/her identity into a point on EC i.e.. ID. Then he keys his ID and PW to the device. The smart card will perform the following operations :

- Select r randomly between $[1, n-1]$
- Compute $C_1 = rID$
- Compute $t = f(T \oplus PW) \bmod n$ where T is the current date and time of the input device.
- Compute $M = tID$
- Compute $C_2 = M + rPW$

Send a message C consists of (ID, C_1, C_2, T) to the authentication server.

4.3 Authentication Phase

Upon receive of message C, AS authenticate the login user as follows :

Let AS receive the message C sent from U at T', where T' is the current date and time of the system

Test the validity of ID. If the format of the ID is incorrect, then the AS reject the login user.

Test the time interval between T and T'. If $(T' - T) \geq \Delta T$, where ΔT denotes the expected legal time interval for transmission delay, then AS reject the login user.

If $(C_2 - d_s C_1) = M$ where $M = tID$, then the AS accept otherwise reject the login user.

5. Security analysis

As the proposed scheme is based on ECDLP, so it not possible for attacker to find the secret key d_s of AS from PW where $PW = d_s ID$. It is also difficult for the attacker to find the randomly selected r from $C_1 = rID$ in the login phase. For the attacker to pass through the step 2 of the authentication phase he must change T' into new T'' such that $(T'' - T') \geq \Delta T$. Once T is changed, the step 3 in the authentication phase is failure unless either t or C_2 has been changed accordingly. Therefore, the proposed scheme is secure to withstand the replying attack.

As the scheme is based on ECDLP, it achieves the same security with fewer bits key as compared to RSA, which is more suitable in the application where the smart card is being used. In addition, it has low-computation requirements

5. References

[1] L. Lamport, "Password authentication with insecure communication," communication of the ACM, vol. 24, no. 11, pp. 770-772, 1981.M. S.

[2] J. J. Shen, C. W. Lin and M. S. Hwang, "A modified remote user authentication scheme using smart cards," IEEE Trans. Consumer Electronic, vol. 49, no. 2, pp. 414-416, May 2003.

[3] K. C. Leung, L. M. Cheng, A. S. Fong and C. K. Chen, "Cryptanalysis of a remote user authentication scheme using smart cards", IEEE Trans. Consumer Electronic, vol. 49, no. 3, pp. 1243-1245, Nov 2003.

[4] L. H. Li, I. C. Lin and M. S. Hwang, "A remote password authentication scheme for multi-server architecture using neural networks," IEEE Trans. Neural Networks, vol. 12, no. 6, pp. 1498-1504, 2001.

[5] H. Sun, .An efficient remote user authentication scheme using smart cards,. IEEE Trans Consumer Electron, vol. 46, no. 4, pp. 958-961, November 2000.

[6] M. Hwang and L. Li, .A new remote user authentication scheme using smart cards,. IEEE Trans Consumer Electron, vol. 46, no. 1, pp. 28-30, February 2000.

[7] W. Yang and S. Shieh, .Password authentication schemes with smart cards,. Computers and Security, vol.18,no. 8, pp. 727-733, 1999.

[8] T. C. Wu, "Remote login authentication Scheme based on Geometric Approach" Computer Communications 18(12) (1995) 959-963

[9] M S Hwang, "Cryptanalysis of Remote login authentication Scheme" Computer Communications 22(8) (1990) 770-772.

[10] Koblitz N., Elliptic Curve Cryptosystems, Mathematics of Computation ,48, pp.203-209, 1987.

[11] Miller V., Uses of Elliptic Curve in Cryptography, Advances in Cryptography, Proceedings of Crypto'85, Lectures notes on Computer Sciences,218, Springer– Verlag, 1986, pp.417-426.

[12] Koblitz N., CM-Curves with Good Cryptographic Properties, Proceeding of Crypto'91,1992.

[13] Hankerson Darrel, Menzes Alferd, Vanstone Scott, Guide to Elliptic Curve Cryptography, Springer, 2003.

[14] Popesu C., A Secure Key Agreement Protocol Using Elliptic Curves, International Journal of Computers and Applications, Vol 27, 2005.