International Journal of Information Technology and Knowledge Management
July-December 2011, Volume 4, No. 2, pp. 649-651

A NOVEL REMOTE USER AUTHENTICATION SCHEME USING SMART CARD WITH BIOMETRIC BASED ON ECDLP

K K Goyal[1] & M S Chahar[2]

In this paper, a novel efficient remote user authentication scheme using smart card with biometric based on Elliptic Curve Discrete Logarithm Problem (ECDLP) has been proposed. A remote user authentication scheme is a client server based protocol whereby an authentication server identifies the identity of a remote user when he/she individually logging on to the server using public, untrusted, unsecured network. Password authentication is one of the simplest and the most convenient authentication mechanisms to deal with secret data over insecure networks. It is more frequently required in areas such as computer networks, wireless networks, remote login systems, operation systems, and database management systems. Number of password based authentication scheme both with and without smart card have been proposed; each scheme has its merits and demerits. Our proposed scheme withstands password guessing attack if the smart card is lost.

Keywords: Password, Smartcard, ECDLP, Remote, Biometric Information.

1. Introduction

The authentication scheme is commonly used for verifying a user's identity. Only the authenticated users can access the remote systems. The scatter of remote systems in different places allows more efficient and convenient access for geographically dispersed users. Remote access is one of the applications which ascertain whether the user is legal and whether it can access. In 1981, one of the password based authentication scheme was proposed by Lamport [1] 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, many schemes based on password table have 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 schemes with smart cards have been proposed [5-7]. The scheme proposed by Wu [8] is based on simple geometric properties on the Euclidian plane has weakness in the security [9]. Lal et al [16] proposed their scheme based on bilinear pairing. Elliptic curve cryptosystems gives more security with less bit size key and more computational fast than the other cryptosystems. In 2008, Jena et al's [15] proposed a novel efficient remote user authentication scheme using smart cards based on Elliptic Curve Discrete Logarithm Problem (ECDLP). If the smart card is lost and password is revealed then any one can impersonate to sever as authorized user, because of this we proposed A Novel Remote User Authentication Scheme using Smart Card with Biometric based on ECDLP.

[1,2]Faculty of Management & Computer Application, R.B.S.College, Khandari, Agra-282002 (U.P), India.
E-Mail: [1]kkgoyal@gmail.com, [2]meetendra26@gmail.com

The organization of this paper is as follows. In the Section 2, we show the notations used through out in this paper. In Section 3, we discuss the basic concept of elliptic curve (EC). Elliptic Curve Cryptosystem based on variation of ElGamal scheme is shown in section 4, the proposed scheme is explained in section 5. The security analysis has been made in section 6. Finally, Section 7 describes the concluding remarks.

2. Notation

The notations used through out in this paper are 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
- q order of the field
- FR is the field representation for F_q
- G generator of group
- n large prime number
- h division of N (the order of E (F_q) to n)
- d_s secrete key of authentication server
- Q Public key of the authentication server
- B Personal biometric

3. 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 firstgeneration public key systems such as RSA or Diffie-Hellman [13].

3.1 Elliptic Curve Groups Over

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

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

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

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.

3.1.1. 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

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

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.

$$x_r = (s^2 – x_p – x_p) \bmod q \text{ and}$$

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

3.1.2. Doubling the Point P

Provided that y_p is not 0,

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

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

$$x_r = (s^2 – 2x_p) \bmod q \text{ and}$$

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

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.

4. 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:

$$(C_1, C_2) = (kG, P_m + k(d_B G))$$

To decrypt the cipher text, Bob computes

$$C_2 – d_B (C_1) = P_m + k(d_B G) – d_B(kG) = P_m$$

5. Proposed Scheme

In this section, we describe our proposed remote user authentication scheme using smart cards with biometric based on ECDLP. We have mainly divided our proposed scheme in three phases, 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 card reader and submits ID, PW and personal biometric B to server.

5.1 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 $Q = d_s G$.

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

$$PW = d_s ID$$

The registration centre issues a smart card which contains the public parameter (f, n, G, Q, B_i), where f is a one way function and $B_i = f(B)$. 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) but only differ in the personal biometric.

5.2 Login Phase

Upon login, U attaches his smart card to the card reader and inputs his personal biometric B on the specific device to check if f(B) is equal to B_i stored in the smart card. 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 ⊕ PW) mod 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.

5.3 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 rejects the login user. Test the time interval between T and T′. If (T′ – T) ≥ ΔT, 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.

6. 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_sID. 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′) ≥ ΔT. Once T is changed, the step 3 in the authentication phase is failure unless either t or C_2 has been changed accordingly. If the smart card is lost and password is revealed then it is very difficult to the attacker to produce the same biometric information as stored into the smart card. Therefore, the proposed scheme is secure to withstand the replying attack as well as password guessing attack if the smart card is lost.

7. CONCLUSION

In this paper we have discussed the basic concept of elliptic curve (EC) and cryptosystem based on Elliptic Curve with ElGamal scheme. Then we have proposed the scheme which 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, the proposed scheme is secure to withstand the replying attack as well as password guessing attack if the smart card is lost and also has low computation requirements.

ACKNOWLEDGEMENT

The authors thank Prof. Sunder Lal [V.C., VBS Purvanchal University, Jaunpur, Uttar Pradesh] for his kind supervision of the work.

REFERENCES

[1] L. Lamport, "Password Authentication with Insecure Communication", Communication of the ACM, 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, 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, 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, 12, no. 6, pp. 1498-1504, 2001.

[5] H. Sun, "An Efficient Remote User Authentication Scheme Using Smart Cards", IEEE Trans Consumer Electron, 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, 46, no. 1, pp. 28-30, February 2000.

[7] W. Yang and S. Shieh, "Password Authentication Schemes with Smart Cards",Computers and Security, 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, 27, 2005.

[15] D. Jena, S. K. Jena, D. Mohanty and S. K. Panigrahy, "A Novel Remote User Authentication Scheme Using Smart Card based on ECDLP", IEEE Proceeding of International Conference on Advanced Computer Control, 2008.

[16] Lal Sunder and K.K.Goyal, "An Improved Remote User Authentication Scheme Using Bilinear Pairing", http://eprint.iacr.org/2007/440.pdf.