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

Debasish Jena[1], Saroj Kumar Panigrahy[2], Sanjay Kumar Jena[3] and Subhendu Kumar Pani[4]
[1]Centre for IT Education Bhubaneswar, Orissa, 751 010, India
[2,3]National Institute of Technology Rourkela, Orissa, 769 008, India
[4]Regional College of Management, Bhubaneswar, Orissa, India
debasishjena@ieee.org, skp.nitrkl@gmail.com, skjena@nitrkl.ac.in, subhendu_pani@rediffmail.com

Abstract*—In this paper, a modified of Jena [1] 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. However, the scheme proposed by Jena is vulnerable to the masquerade attack. In this paper, we shall discuss the masquerade attack on their scheme. Furthermore, we shall present an enhanced scheme for preventing the above attack.

***Index Terms*—Masquerade, Password, Smartcard, ECDLP, Remote.**

I. INTRODUCTION

Remote user password based authentication scheme, proposed by Lamport [2] 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. [3–5]. 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 [6-8]. The scheme proposed by Wu which [9] paper is based on simple geometric properties on the Euclidian plane has weakness in the security [10]. 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 II, the basic concept of elliptic curve (EC) is discussed. In Section III, discussion on Elliptic Curve Cryptosystem based on variation of ElGamal scheme has been made and subsequently, the Jena scheme is explained in section IV. The crypto analysis of Jena scheme is done in section V. The proposed scheme and its security analysis are discussed in section VI. Finally, Section VII describes the concluding remarks.

II. ELLIPTIC CURVE OVER FINITE FIELD

The use of Elliptic Curve Cryptography (ECC) was initially suggested by Neal Koblitz [11] and Victor S. Miller [12] 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 [13], 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 [14].

1. *Elliptic Curve Groups over* F_q

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

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

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.

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

$$P + Q = R \qquad (2)$$

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

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

978-1-4244-4837-1/09/$25.00 ©2009 IEEE

Doubling the Point P

Provided that y_p is not 0,

$$2P = R(x_r, y_r) \tag{3}$$

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

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

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

The elliptic curve discrete logarithm problem is defined as follows [15].

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 $Q = dP$.

III. EC 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

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

IV. JENA SCHEME

In this section, we present Jena proposed remote user authentication scheme using smart cards based on ECDLP. We discuss three phases of Jena 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 throughout 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
SID	Shadow Identity
IS	identity string that includes name, unique number etc

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 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), 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).

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.

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.

V. Security Analysis

The scheme proposed by Jena is vulnerable to masquerade attack. Suppose that a user U_m wants to masquerade other legal users. She/he submits her/his ID_m to the remote server for registering to be a legal user. The remote server will responses PW_m, and a smart card for U_m, after the identity is identified. Now, U_m, wants to create a legal user U_l and corresponding a valid pair of (ID_l, PW_l). Now, she/he computes $ID_l = (ID_m + ID_m)$ and calculate PW_l as follows:

$$PW_l = d_s ID_l = d_s (ID_m + ID_m) = PW_m + PW_m .$$

Thus, U_m, can successfully login in the remote server via forged (ID_l, PW_l).

VI. Proposed Scheme and its Cryptanalysis

1. *Proposed modified scheme*

In this paper, we propose a modified scheme that can sustained the security flaw of Jena scheme. It employs the concept of hiding identity to prevent from masquerading attack. We only modify the registration phase which issues a "shadowed" identity [16-17] for every legal user. The steps of login and authentication phase are retained except that replace ID by "shadowed" identity SID, respectively. The modified registration phase is as follows.

Registration Phase: Assume that this phase is executed over a secure channel. First, U submits her/his identity string IS, to the remote server for registration, where IS, is U 's identity string that includes name, unique number etc. which are unique. The remote server computes (SID, PW) for the registering user after her/his identity IS, is identified.

$$SID = Sed(IS) \quad (4)$$

$$PW = d_s SID \quad (5)$$

where, $Sed(.)$ is a "shadowed" identity of the device which only is possessed with the remote server; SID is U's "shadowed" identity which can be disclosed. Furthermore, the remote server issues the smart card and (SID, PW) to U which f (.) is stored into the smart card.

2. *Security Analysis of the Modified*

The masquerade attack on the Jena scheme is described in Section V. The attack works because the evil user can successfully register a new ID_l using ID_m. In our modified scheme, we propose a modification of the registration phase as the (1) and to withstand the attack.

As the Section V, assume that an evil user U_m can intercepts C consists of (ID, C_1, C_2, T) from a public network. Now, U_m, submits her/his $IS_l = kIS_m$ to the remote server to register for masquerading as U_l. Upon receiving the registration message IS_l, from U_m,, the remote server will rejects the registration request because the format of IS_l, is incorrect which must includes name, unique number etc. for identifying. IS_m J, is maintained by the user U_m, and the remote server, secretly. Thus, U_m cannot masquerades as U_l to login and access the remote server.

VII. Conclusion

In this article, we have shown that the Jena scheme is vulnerable to the masquerade attack. An evil user can masquerades as another legal user to login a remote server via derive a legal user's password. For the above attacks, we presented a modified scheme to protect the flaw of Jena scheme.

Acknowledgment

This research is supported by Department of Communication and Information Technology, Government of India, under Information Security Education and Awareness Project and being carried out at department of Computer Science and Engineering, National Institute of Technology Rourkela, Orissa, India.

References

[1] Jena Debasish, Sanjay Kumar Jena, Debashisa Mohanty and Saroj Kumar Panigrahy " A Novel Remote User Authentication Scheme Using Smart Card Based on ECDLP", Proceedings of ICACC 2009,IEEE 2009, pp.246-249.

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

[3] 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.

[4] 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.

[5] 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.

[6] H. Sun, An efficient remote user authentication scheme using smart cards,. IEEE Trans Consumer Electron, vol. 46, no. 4, pp. 958-961, November 2000.
[7] 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.
[8] W. Yang and S. Shieh,.Password authentication schemes with smart cards,. Computers and Security, vol.18,no. 8, pp. 727-733, 1999.
[9] T. C. Wu, "Remote login authentication Scheme based on Geometric Approach" Computer Communications 18(12) (1995) 959-963
[10] M S Hwang, "Cryptanalysis of Remote login authentication Scheme" Computer Communications 22(8) (1990) 770-772.
[11] Koblitz N., Elliptic Curve Cryptosystems, Mathematics of Computation,48, pp.203-209, 1987.
[12] 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.
[13] Koblitz N., CM-Curves with Good Cryptographic Properties, Proceeding of Crypto'91,1992.
[14] Hankerson Darrel, Menzes Alferd, Vanstone Scott, Guide to Elliptic Curve Cryptography, Springer, 2003.
[15] Popesu C., A Secure Key Agreement Protocol Using Elliptic Curves, International Journal of Computers and Applications, Vol 27, 2005.
[16] L. Guillou and I. I. Quisquater, "Efficient digital public-key signatures with shadow," Advances in Cvptoloo, CRYPT'87, vol. LNCS 239, pp.238, 1987.
[17] L. Guillou and J. I. Quisquater, "A Pnrndoxical identitybased signature scheme resulting from zero-knowledge," Advances in Cvprology, CRYPT'88,vol. LNCS430,pp. 216-231, 1988.