On the Security of a Novel Remote User Authentication Scheme using Smart Card based on ECDLP

Manoj Kumar
Department of Mathematics
R. K. College Shamli-Muzaffarnagar, U.P.-India - 247776
E-mail: yamu_balyan@yahoo.co.in

Abstract

In 2009, Jena et al. proposed a novel remote user authentication scheme using smart card based on ECDLP and claimed that the proposed scheme withstands to security threats. This paper shows that Jena et al.'s scheme is vulnerable to serious security threats and also does not satisfy the attributes of an ideal password authentication scheme .

Keywords*: Login, remote user and server, access system, network security, security threats.*

1 Introduction

To authenticate the legitimacy of a remote user over insecure channel, password based remote user authentication scheme is widely used. In 1981, Lamport [2] proposed the first well-known remote user authentication scheme without using encryption techniques. In this scheme, a password table is required to achieve the user authentication. However, high hash overhead and the necessity for password resetting decrease the suitability and practical use of Lamport's scheme. So far different types of password authentication schemes with smarts cards have been proposed [4], but none of them provide the ideal solution to the related problem of remote user authentication.

In 2009, Jena et al. [1] proposed a novel efficient remote user authentication scheme using smart cards based on Elliptic Curve Discrete Logarithm Problem (ECDLP) and claimed that the proposed scheme withstands to security attacks.This paper analyzes Jena et al.'s scheme [1] and found that the proposed scheme is vulnerable to serious security vulnerabilities. The rest work is organized as follows. Section 2 reviews the proposed work of Jena et al. Our observations and analysis about the error and security flaws of Jena et al.'s scheme [1] are discussed in section 3. Finally, comes to a conclusion in the section 4.

2 Review of Jena et al.'s proposed scheme

This section provides a review Jena et al.'s proposed scheme [1]. Jena et al. proposed a novel remote user authentication scheme using smart card based on ECDLP. The proposed scheme has three phases, namely registration phase, login phase and authentication phase. These three phases are described below.

2.1 Registration Phase

- Initially, the *U* and the *AS* must be agreed upon the elliptic curve domain parameters *q, FR, a,b,G, n, etc*.
- Every new user *U* submits his/her identity *ID* to the remote server for registration. The *AS* computes the password $PW = d_S \times ID$ and delivered this password *PW* to the user through a secure channel.
- The registration center issues a smart card which contains the public parameter (f, n, G, Q)

2.2 Login phase

For login, *U* attaches his smart card to the smart card reader and keys his/her identity *ID* and *PW*. The smart card will perform the following operations :

- Select *r* randomly between [1, *n* -1]
- Compute $C_1 = r \times ID$.
- Compute $t = f(T \bigoplus PW)$ mod *n*, where *T* is the current date and time of the smart card reader.
- Compute $M = t \times ID$.
- Compute $C_2 = M + r \times PW$.
- Send a message C consists of (ID, C_1, C_2, T) to *AS*.

2.3 Authentication Phase

Let *AS* receives the message *C* sent from *U* at time *T'* , where *T'* is the current date and time at *AS*. Upon receive of the message C, *AS* authenticate the login user *U* as follows :

- 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 $(T' - T) \geq T$, where *T* denotes the expected legal time interval for transmission delay, then *AS* reject the login user.
- If $C_2 - d_S \times C_1 = M$, where $M = t \times ID$, then the *AS* accept the login user,otherwise reject her/him.

3 Security Analysis of Jena et al.'s Scheme

3.1 Impersonation Attack Via Registered Identity

In Jena et al.'s proposed scheme [1], a registered user, Alice is a strong antagonist. A registered user can mount a serious attack by using his registered identity and password. He can generate a new fake identity and corresponding password without the involvement of authentication server. Alice uses her valid pair (ID_A, PW_A) to generate another valid pair (ID_B, PW_B). The related attacks are given below.

Attack-I

- Alice computes $ID_B = ID_A \times ID_A$
- Alice computes the corresponding password PW_B, as,

$$\begin{aligned} PW_B &= d_S \times ID_B \\ PW_B &= d_S \times ID_A \times ID_A \\ PW_B &= PW_A \times ID_A \end{aligned}$$

Thus, PW_B is generated by Alice with the help of previously registered identity ID_A and password PW_A and there is no involvement of the *AS* in this fake construction.

Attack-II

- Computes $ID_B = ID_A \pm ID_A$
- Computes the corresponding password PW_B, as,

$$\begin{aligned} PW_B &= d_S \times ID_B \\ &= d_S \times (ID_A \pm ID_A) \\ &= d_S \times ID_A \pm d_S \times ID_A \\ &= PW_A \pm PW_A \end{aligned}$$

In this way, Alice can generate a new fake identity ID_B and corresponding password PW_B easily without the involvement of authentication server.

3.2 Masquerading Attack Via Registered Password

An adversary, Bob can masquerade another valid user Alice to login a remote server and gain access right.The related steps are given below.

- Bob computes an identity $ID_B = k \times ID_A$, where *k* is a random number such that *gcd* (*k* , *q*) = 1.
- Bob submits this identity ID_B to *AS* for registration.
- *AS* provides a smart card and a password $PW_B = d_S \times ID_B$ to Bob.
- With the knowledge of PW_B, Bob can compute $PW_A = d_S \times ID_A$ = $PW_B \times k^{-1}$.

As a result, Bob can masquerade Alice (a valid user) to login a remote server and gain access privilege on behalf of Alice.

3.3 Collusion Attack

Jena et al.'s proposed scheme [1] is also vulnerable to the collusion attack. Alice with (ID_A, PW_A) and Bob with (ID_B, PW_B) can collude and then they will be able to generate a new pair valid pair (ID_C, PW_C) without the involvement of authentication server. The related steps are given below.

- Computes $ID_C = ID_A \pm ID_B$
- Computes the corresponding password PW_C, as,

$$\begin{aligned} PW_C &= d_S \times ID_C \\ &= d_S \times (ID_A \pm ID_B) \\ &= d_S \times ID_A \pm d_S \times ID_B \\ &= PW_A \pm PW_B \end{aligned}$$

In same way, a group of eavesdroppers may collude to generate a valid pair of identity (ID_G, PW_G). The related steps are given below.

- Computes $ID_G = \sum ID_{A_j}$.
- Computes the corresponding password

$$PW_G = \sum PW_{A_j}.$$

3.4 Attributes of Jena et al.'s Scheme

Jena et al.'s scheme [1] does not satisfy the attributes of an ideal password authentication scheme [4] . In Jena et al.'s scheme,

1. The passwords or verification tables are not stored in the system.

2. The passwords can not be changed freely by the users.

3. The password is computed by the insider at the server.

4. Some information are transmitted in plain text over the insecure network, which are responsible for security vulnerabilities.

5. The length of a password is nor specified, while the length of the password must be appropriate for memorization.

6. The efficiency and practical abilities are not described.

7. There is no unauthorized login detection, when a user inputs a wrong password, a user can enter his password multiple times. It means there is a possibility of online password guessing attack.

8. No session key is established during the password authentication process to provide confidentiality of communication.

9. The server and the the user do not authenticate each others.

10. The login *ID* is not dynamically changed for each login session to avoid partial information leakage about the users login message.

11. The server is not forward protected. The proposed scheme is insecure if the secret key of the server is leaked out or stolen.

4 Conclusion

This paper analysis Jena et al.'s scheme and found that the proposed scheme vulnerable to impersonation attack, masquerading attack, collusion attack. On the other side, the proposed scheme also does not satisfy the essential security attributed to be an ideal remote user authentication scheme.

References

[1] Jena, D., Jena, S. K., Mohanty, D., and Panigrahy, S. K. 2009. A Novel Remote User Authentication Scheme Using Smart Card Based on ECDLP. In Proceedings of the 2009 *international Conference on Advanced Computer Control* (January 22 - 24, 2009). *IEEE Computer Society*, Washington, DC, pp. 246-249.

[2] Lamport L., 1981. Password Authentication with Insecure Communication. *Communication of the ACM*, 24, 11: pp. 770-772.

[3] Manoj K., 2009. On the Security Vulnerabilities of a Hash Based Strong Password Authentication Scheme, Cryptology ePrint Archive: a publication of The International Association for Cryptologic Research (IACR), Santa Rosa Administrative Center, University of California, Santa Barbara, CA, 93106-6120, USA, Report, http://www.eprint.iacr.org/2009/560,2009

[4] Tsai C. S., Lee C. C.and Hwang M. S., 2006. Password Authentication Schemes: Current Status and Key Issues. *International Journal of Network Security*, Vol.3, No.2, pp. 101 115.

Manoj Kumar received the B.Sc. degree in mathematics from Meerut University Meerut, in 1993; the M. Sc. in Mathematics (Gold medalist) from C.C.S.University Meerut, in 1995; the M. Phil. (Gold medalist) in Cryptography(Applied Algebra), from Dr. B. R. A. University Agra, in 1996; the Ph.D. in Cryptography, in 2003. He also qualified the National Eligibility Test (NET), conducted by Council of Scientific and Industrial Research (CSIR), New Delhi- India, in 2000. He also taught applied Mathematics at D. A. V. College, Muzaffarnagar, India from Sep 1999 to Feb 2001; at S.D. College of Engineering & Technology, Muzaffarnagar- U.P. - INDIA from March 2001 to Oct 2001; at Hindustan College of Science & Technology, Farah, Mathura- U.P. - INDIA, from Nov 2001 to March 2005. In 2005, the Higher Education Commission of U.P. has selected him. Presently, he is working in Department of Mathematics, R. K. College Shamli- Muzaffarnagar- U.P. - INDIA-247776. He is a member of Indian Mathematical Society, Indian Society of Mathematics and Mathematical Science, Ramanujan Mathematical society, and Cryptography Research Society of India. He is working as a reviewer for some International peer review Journals: Journal of System and Software, Journal of Computer Security, International Journal of Network Security, The computer networks, computer and security, The Computer Journal. He is also working as a Technical Editor for some International peer review Journals- Asian Journal of Mathematics & Statistics, Asian Journal of Algebra, Trends in Applied Sciences Research, Journal of Applied Sciences. He has published his research works at national and international level. His current research interests include Cryptography and Applied Mathematics.