ISSN (Online): 2456-5717

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3 Issue.9 September 2017

Enhanced Endorsement Scheme for Smart Card Using Elliptic Curve Cryptography

[1]Shakeela Joy A, [2]R. Ravi.,
Assistant Professor in Computer Science Department, Loyola Institute of Technology of Science[1]
Professor and Research Centre Head, Department of Computer Science and Engineering,
Francis Xavier Engineering College, Tirunelveli - 627003, Tamil Nadu State, India[2]

***Abstract*- Now-a-days smart card plays a major role in the world, due to its high security and privacy. But with the existing password endorsement method through an unsecure communication canal, a hacker can guess the password. Our proposed enhanced endorsement scheme with Elliptic Curve Cryptography provides better security, confidential and privacy. The scheme is susceptible to offline password guessing attack such as spidering, stolen-verifier and key stroke dynamics.**

***Keywords*- Password, Elliptic Curve Cryptography, Smart Card, attacks**

I. INTRODUCTION

Today e-Payment is broadly used as an application of smart card. Smart card is a card made by plastic with embedded Integrated Chip. It contain the information about medical, banking, academic, financial etc..Smart card is mainly used due to its security, confidential and privacy. The password is guessed by hackers, with the existing security protocols.

The rest of the paper is section as follows Section 2 describes the existing system. Sections 3 discuss the proposed system. Sections 4 discuss the conclusion and Section 5 describes the reference.

II. EXISTING SYSTEM

In [1] security based enhanced remote authentication scheme was used. In [4] the encryption of the message is not done at the client side and it sends to the server for authentication and login process. So there is a possible to modify the message. In [5] Lin-Hwang's password authentication scheme cannot withstand for stolen-verifier attack and log in by multi user attack. In [7] a dynamic ID based authentication is used to provide privacy and efficiency. In [9] Islam-Biswas's scheme is used to exclude the Lin-Hwang's scheme weakness and the security. In [11] Wang Chang scheme is used, by attaining the timestamp the hacker can login as a user.

III. PROPOSED SYSTEM

The proposed algorithm is categorized into four phases

(i) Client registration phase,
(ii) Login phase
(iii) Authentication phase

(iv) Password update phase

Before the protocol is ever executed, The Server S generate two keys m *and n* , then the Secret Key SK=h(ID | n) with the server S

(i) Client Registration Phase

In this phase, the Client C firmly chooses its Identity ID_C and Password PW_C to the Server S.

The procedure for Registration Phase

Procedure

1. The Client C choose the Identity ID_C and Password PW_C
2. Generate random number R_C
3. Evaluate $PW_{CC} = h(PW_C \oplus R_C)$
4. Client C sends ID_C and PW_C to Server S through a protected canal
5. The Server S evaluate
6. $K_C = h(ID_C \| m) \text{ X } P$
7. $A_C = PW_{CC} \oplus h(m \oplus n)$
8. $B_C = h(ID_C \| PW_{CC}\, h(m \oplus n))$
9. $W_C = h(ID_C \| PW_{CC} \|) \oplus K_C$
10. Now the smart card is loaded with { A_C , B_C , W_C ,h(.)}

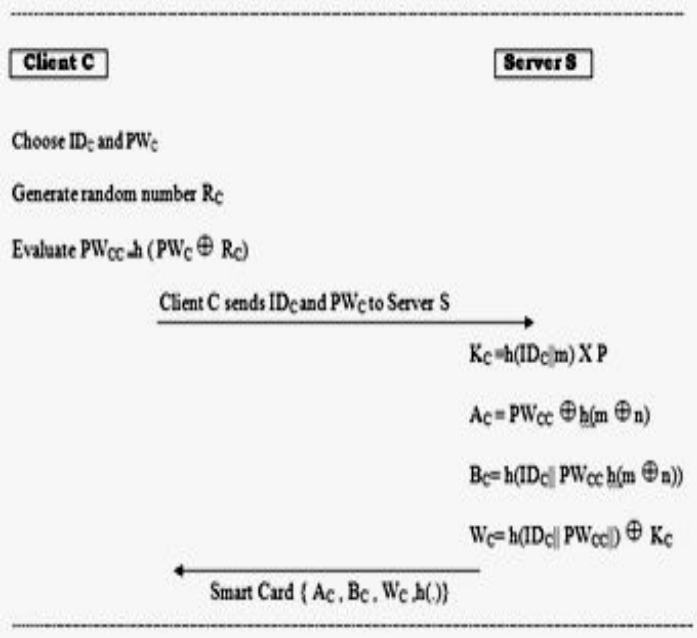

Fig. 1. Client Registration Phase

(ii) Login phase

This phase is active whenever the Client C wants to use the smart card.

The procedure for Login Phase

Procedure

1. Client C insert its smart card into the card reader and inputs its Identity ID_C and Password PW_C .
2. The smart card evaluate
   $PW_{CC} = h(PW_C \oplus R_C)$
   $B_{CC} = h(ID_C \| PW_{CC}\ h(m \oplus n))$
3. Verify if B_C is equal to B_{CC}, If equal the Client C can login.
4. Otherwise the Client C cannot login.

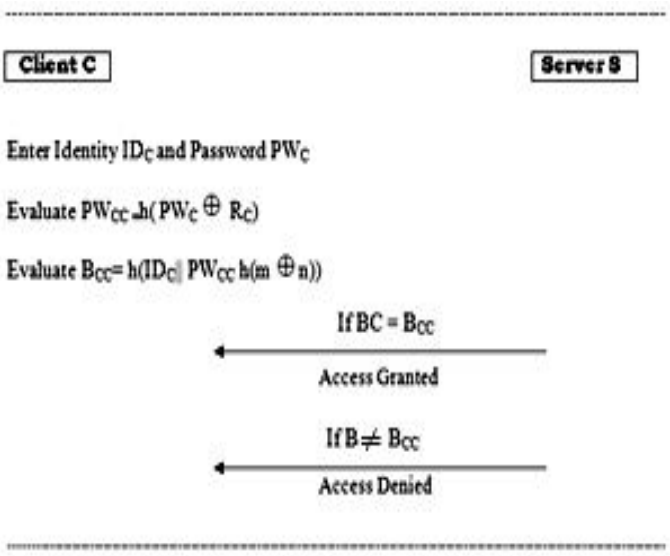

Fig. 2. Login phase

(iii) Authentication phase

The procedure for Authentication Phase

Procedure

1. Verify the format of ID_C . If the format is incorrect, the system rejects the login request.
2. Verify the validity of time interval between T_C and T_{CC}.
3. If $(T_{CC}-T_C) \geq \Delta T$, the system discards the login request

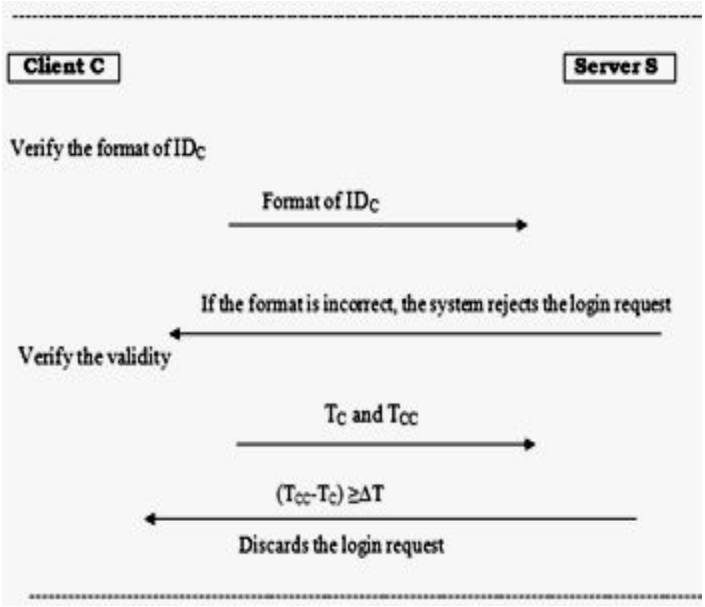

Fig. 3. Authentication phase

(iv) Password update phase

In this phase the client can update the password.

The procedures for Password update Phase

Procedure

1. Client ID_C requests the Server S to change the password.
2. Client C inserts its smart card into the card reader and enters its Identity ID_C, old Password PW_C and new Password PW'_C.
3. The smart card evaluates

   $PW_{CC} = h(PW_C \oplus R_C)$

   $h(m \oplus n) = A_C \oplus PW_{CC}$

   $B_{CC} = h(ID_C \| PW_{CC} \| h(m \oplus n))$
4. Verify if B_C is equal to B_{CC}, If not equal the Password update Phase stops.
5. Otherwise evaluate

   $K_C = W_C \oplus h(ID_C \| PW_{CC})$

   $PW'_{CC} = h(PW'_C \oplus R_C)$

   $A'_C = PW'_{CC} \oplus h(m \oplus n)$

   $B_{CC} = h(ID_C \| PW'_{CC}\ h(m \oplus n))$

   $W'_C = h(ID_C \| PW_{CC} \|) \oplus K_C$

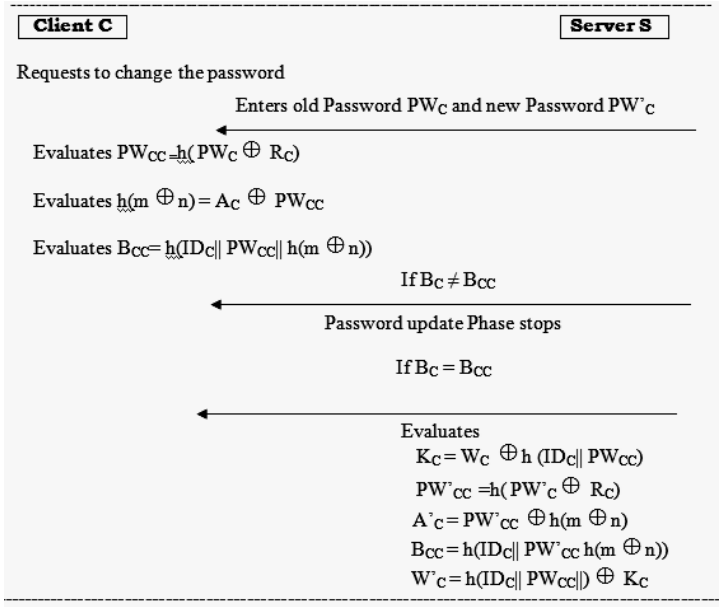

Fig. 4. Password update phase

IV. CONCLUSIONS

Smart Card is mainly used due to its security. In this paper we proposed enhanced endorsement scheme with Elliptic Curve Cryptography provides better security, confidential and privacy. The scheme is susceptible to offline password guessing attack such as spidering, stolen-verifier and key stroke dynamics. The proposed algorithm is categorized into four phases (i) Client registration phase, (ii) Login phase (iii) Authentication phase and (iv) Password update phase

In Client registration phase, the Client C firmly chooses its Identity ID_C and Password PW_C to the Server S. The Login phase is active whenever the Client C wants to use the smart card. The Authentication phase is to verify the validity. In Password update phase the client can update the password.

REFERENCES

[1] Zhuo Hao and Nenghai Yu, A security Enhanced Remote Password Authentication Scheme using Smart Card, Second International Symposium on Data, Privacy and E-Commerce(2010) 56-60.
[2] J.J Shen, C.W.Lin, M.S. Hwang, A modified remote user authentication scheme using smart cards, IEEE Transaction on Consumer Electronics 49(2) (2003) 414-416.
[3] Li, C.T., Lee,C.C, Wang, L.J., Liu, C.J.: 'A secure billing service with two-factor user authentication in wireless sensor networks', Int. J. Innov. Computing.. Inf. Conrol, 2011,7, (8), pp.4821-4831.
[4] C.Li Secure Smart card based password authentication scheme with user anonity, Information Technology and control, Vol 40, No.2, pp.157-162,2011.
[5] Lin, C.L., Hwang, T.: 'A password authentication scheme with secure password updating ', Comput. Secur. 2003,22,(1),pp.68-72.
[6] Sood Sk, Sarje AK, Singh K (2010) An improvement of Xu etal.'s authentication scheme using smart cards. In: Proceedings of the third annual ACM Banglore conference.
[7] K.H. Yeh, C. Su, N.W. Lo, Y. Li, and Y.X. Hung, "Two robust remote user authentication protocols using smart cards," *J. Syst. Softw.*, vol. 83, no. 12, pp. 2556–2565. 2010.

[8] M.S. Hwang, S.K. Chong, and T.Y. Chen, "DoS-resistant ID-based password authentication scheme using smart cards."Journal of Systems and Software, Vol.83, No. 1.pp. 163-172, 2010.
[9] Islam, S.H., Biswas, G.P.: 'Design of improved password authentication and update scheme based on elliptic curve cryptography', Math.Comput.Model., 2012, in press.
[10] Chen, TH; Shih, WK. A Robust Mutual Authentication Protocol for Wireless Sensor Networks. ETRIJ 2010, 32, 704-712.
[11] Eun-Jun Yoon and Kee-Young Yoo, 'Breaking a Smart Card based Secure Password Authentication Scheme", International Conference on Information Security and Assurance, pp.83-86, 2008.
[12] C.C. Chang and T.C. Wu, "Remote password authentication with smart cards," IEE Proceedings-E, vol. 138, no.3.pp. 165-168,1993.
[13] C.C. Chang, H.D.Le.C.Y.Lee, and C.H. Chang, "A robust and efficient smart card oriented remote user authentication protocol," Proc. 7th Int. Conf. Intekkigent Information Hiding and multimedia signal Processing, pp. 252-255. Dalina, China, 2011.
[14] Q.Xie, J.L. Wang, D.R. Chen, and X.Y. Yu," A novel user authentication scheme using smart crds" In: Proceedings of the 2008 International Conferences on Computer Science and Software Engineering, pp.834-836, 2008.