ISSN (ONLINE) : 2395-695X
ISSN (PRINT) : 2395-695X
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 6, September 2015

DEFENSE AGAINST PASSWORD GUESSING ATTACK IN SMART CARD

A. Shakeela Joy.,
Assistant Professor in Computer Science Department
Loyola Institute of Technology of Science

Dr. R. Ravi.,
Professor & Research Centre Head,
Department of Computer Science and Engineering
Francis Xavier Engineering College,
Tirunelveli - 627003, Tamil Nadu State, India.
fxhodcse@gmail.com

Abstract

Password authentication in the smart card plays an important role in insecure networks. Security slanting protocols used for authentication between user and remote server include a brawny covert password. But the existing security slanting protocols are very costly. Also the users desire to use easily memorize password (ie., feeble password). So the hackers can easily guess the password leading to password guessing attack. The two password guessing attacks are online attack and offline attack. In this paper we proposed PGAE scheme for encryption and PGAD scheme for decryption. The PGAE and PGAD based on Elliptic Curve Cryptography provide better security, privacy and user friendly.

Keywords: attacks, password, smart card, Elliptic Curve Cryptography, Least Significant Bit algorithm, unique key algorithm

1 INTRODUCTION

Smart card is a chip card with embedded Integrated Circuit. It is made up of polyvinyl chloride. In the Smart card the data can be stored and transacts. The data may be either value or information. It is transacted through a card reader Nowadays Smart cards are used in applications such as healthcare, banking, entertainment and transportation.

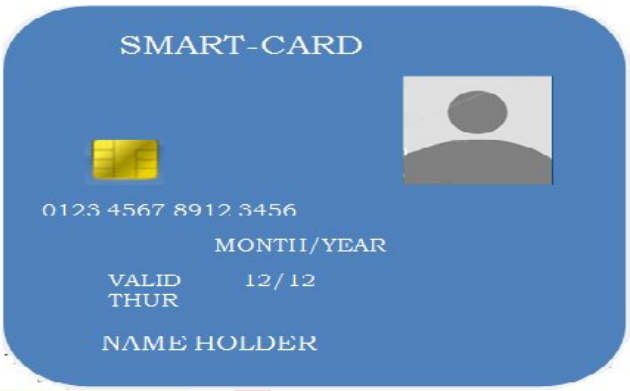


Fig.1. Smart card

Smart cards are mainly preferred by the users due to its security while transaction. It provides tamper-proof storage and description identity. In recent years the password in the Smart card is stolen by the hackers either in online or offline computation. Therefore security slanting protocols are used for authentication.

The remaining section of this paper is structured as follows. Section 2 discuss about the types of password guessing attack, Section 3 discuss the existing system, Section4 describe the proposed scheme, Section 5 deals with the architecture of proposed scheme, Section 6 describe the implementation algorithm, and finally the conclusion in Section 7.

2 TYPES OF PASSWORD GUESSING ATTACK

There are two types **of** password guessing attacks. They are

1) Online password guessing attack
2) Offline password guessing attack

1) Online password guessing attack:

ISSN (ONLINE) : 2395-695X
ISSN (PRINT) : 2395-695X
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 6, September 2015

It is widely spread on every user login and peer to peer system. Eg: brute force attack and dictionary attacks

Brute force attack:

In this attack the hackers choose the words by using all possible combination of numbers and alphabets.

Dictionary attacks:

In this attack the hackers choose the dictionary words

Masquerade attack:

It use forged identity to access the system.

Forgery attack:

It is the method of adopting or imitating objects, figures or credentials with the target device.

Denial of Service attack (DoS):

It makes computer resources unavailable to its anticipated users.

2) Offline password guessing attack: In this attack the hackers will not interact with the victim host.

Eg: Eavesdropping and recording the conversation on the communication channel.

Man-in-the middle attack:

This attack is a form of eavesdropping. In this the hackers makes an autonomous channel with the victims, the user, the server and the relays messages between them, making them believe that they are talking directly to each other.

3 EXISTING SYSTEM

In [1] Elliptic Curve Cryptography Scheme is used. It provides password authentication, login client exact identity and mutual authentication. It requires low computation cost. The drawback is unprotected to masquerade attack and forgery attack. In [2] Li-Lee's scheme assumes that smart card is tamper resistant. But such assumption is difficult in practice. The server has to maintain a security –sensitive verification table. This scheme is not free from smart card loss attack. The drawback is, it cannot endure offline password guessing attack with the uncorrupt resistance guess and fails to provide user privacy. In [3] PGRP protocol can be used to prevent online or offline attack. In PGRP when a user login from a new machine, for the first time it will not answer ATT test. (ie protocol need less ATT test). Whenever the ATT test answered the user can login otherwise the user cannot login. In [5] robust authentication scheme based on secure one way hash function is used. It provide forward secrecy, user can change the password locally and preserve privacy. The drawback is additional cost are needed to provide the feature of forward secrecy and to achieve user privacy. In [7] Elliptic Curve Cryptography scheme is used. It authorizes login clients and remote server with a secure and privacy preserving authentication. The drawback is unprotected to offline password guessing attack, stolen-verifier and insider attack. In [14] one-time pad and strong one-way hash function technique is used in protecting week secrets from guessing attack. It is more efficient in terms of number of random values and cryptographic operations. The drawback is replacing attack is expensive. In [15] Pinkas and Sander (PS) protocol reply the ATT test first before entering the $\{ID_A, PW_A\}$ pair. If the user fails to response the ATT properly the user cannot proceeds further. The PS is effective for online dictionary attacks. The drawback is the login server should generate an ATT test for each user login.

4 PROPOSED SCHEME: (PGAE and PGAD)

In 1985 Victor Miller and Neil discovered Elliptic Curve Cryptography (ECC). It is substitute method for implementing public key cryptography. The elliptic curve equation is

$$y^2=x^3+ax+b$$

The proposed scheme PGAE for encryption and PGAD for decryption is based on Elliptic Curve Cryptography to provide confidentiality to the user.

The proposed scheme consists of four phases. They are

1) Registration phase
2) Login phase
3) Password change phase
4) Authentication phase

The symbols and notation used in the phase are shown in Table 1

Notations

Symbol	Notations
U_A	User A
ID_A	User A's Identity
PW_A	User A's Password

ISSN (ONLINE) : 2395-695X
ISSN (PRINT) : 2395-695X
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 6, September 2015

S	Public key
r	Private key
P	Point on the curve
q	randomly number (1-(n-1)
M	Point on the curve

Table: 1

1) Registration Phase

In this phase whenever the user U_A wants to become a new authorized user, U_A has to register to the server S with his/her identity ID_A and password PW_A. The following steps are required to complete this phase:

Step 1: U_A chooses his/her $IDA_,$ PW_A password and select a random number 'r' within the range of (1 to n-1).

$$U_A \rightarrow \{ID_A, PW_A\}$$

Generate the public key using the following equation:

$$S=r*P.$$

Where r is the random number selected within the range (1 to n-1). P is the point on the curve.
'S' is the public key and 'r' is the private key.

Step 2: Let the password 'm' has the point 'M' on the curve 'E'. Select a random number 'q' within the range of (1- (n-1).
Generate two cipher texts T1 and T2.

$$T1= q*P$$
$$T2=M+q*S$$

Step 3: Encrypted password is embedded in to the image by using LSB algorithm.
Step 4: Encrypt the image using unique key algorithm.

2) Login Phase:

If the user U_A wants to access the server S, the user U_A should insert the Smart card (S) in to the card reader and enter his/her ID_A and PW_A . Then the Smart card performs the following operation.
Step 1: Decrypt the image using unique key algorithm.
Step 2: Extract the encrypted password from the image.
Step 3: Decrypt the password by calculating

$$M=T2-r*T1$$

3) Password change phase

In this phase when the user U_A wants to change his/her password PW_A to a new password PW_A',the user U_A inform the server to update the password $U_A \rightarrow \{ID_A, PW_A\}$ to a new password $U_A' \rightarrow \{IDA_, PW_A'\}$

Step 1: User U_A requests the Server S to change the password.

Step 2: User U_A sends the new password PW_A' to the server S along with the old password.

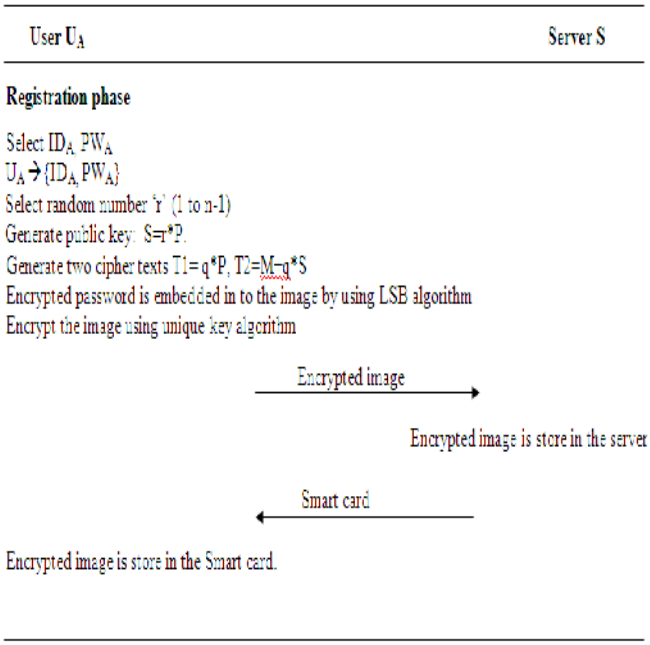
$U_A \rightarrow \{ID_A, PW_A\}$ change to $U_A' \rightarrow \{IDA_, PW_A'\}$

Step 3: Password changed accepted or rejected.

4) Authentication Phase:

Step 1: Check the format of ID_A. If the format is wrong, the system discards the login request.
Step 2: Check the validity of time interval between T and T'. If $(T'-T) \geq \Delta T$, the system discards the login request. (ΔT is the expected valid time interval)

$(T'-T) \geq \Delta T \rightarrow$ discard the login request



ISSN (ONLINE) : 2395-695X
ISSN (PRINT) : 2395-695X
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 6, September 2015

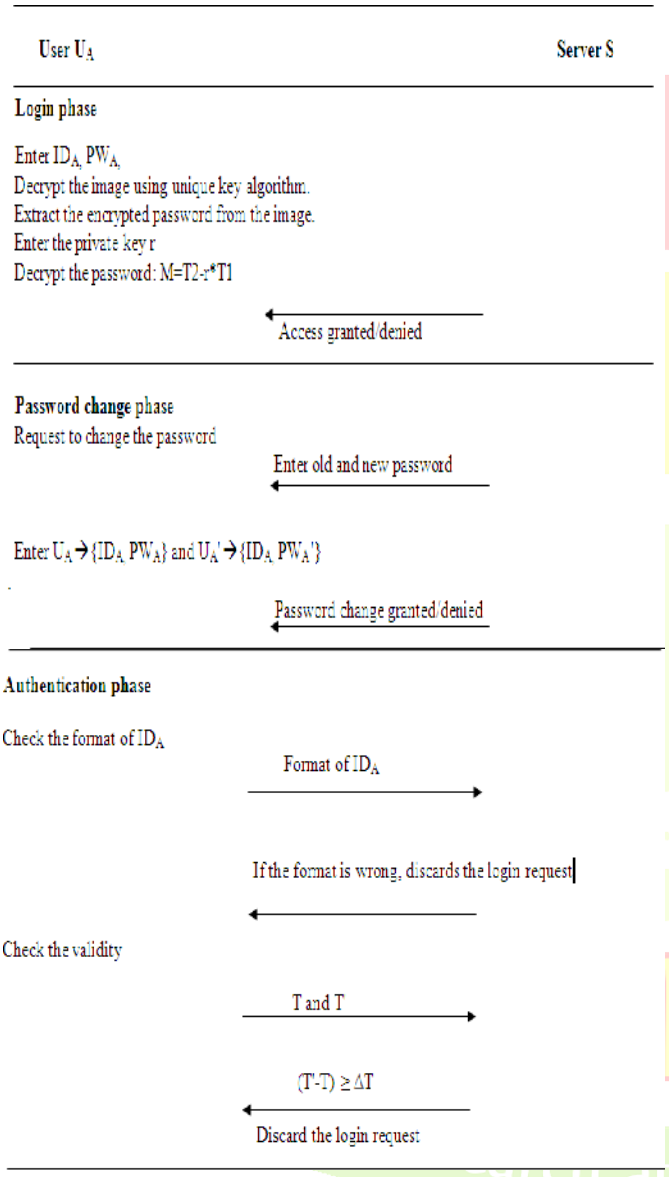


Fig. 2 Phases of the proposed scheme

5 ARCHITECTURE OF PROPOSED SCHEME

In this section the architecture of PGAE scheme and PGAD scheme is shown in Fig.3 and Fig. 4

ARCHITECTURE- PGAE SCHEME

In PGAE scheme the password is encrypted by using Elliptic Curve Cryptography. The encrypted password is embedded in to the image by using LSB (Least Significant Bit algorithm) algorithm. The image is encrypted by using unique key algorithm.

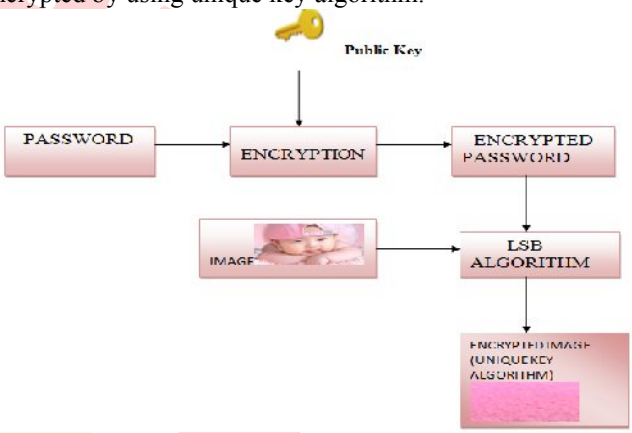


Fig. 3 PGAE scheme

ARCHITECTURE- PGAD SCHEME

In PGAD scheme decrypt the image using unique key algorithm. Extract the encrypted password from the image. Decrypt the password by using Elliptic Curve Cryptography

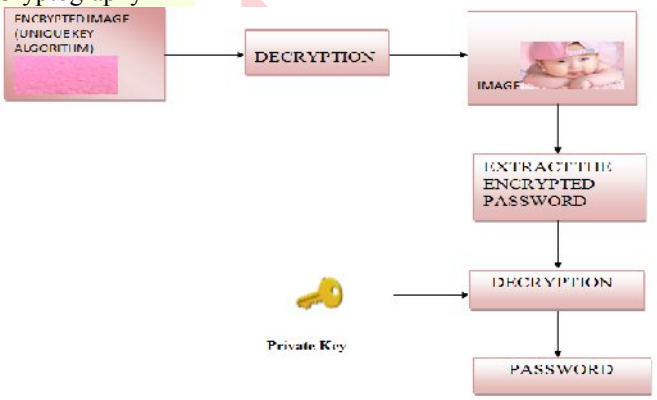


Fig. 4 PGAD scheme

6 IMPLEMENTATION ALGORITHMS

In the registration phase the user U_A register to the server S with his/her identity ID_A and password PW_A. By using Elliptic Curve Cryptography the password is encrypted. The encrypted password is embedded in to the image by using LSB (Least Significant Bit algorithm) algorithm. In this algorithm the least significant bit of the encrypted password is arranged with the bits of the

ISSN (ONLINE) : 2395-695X
ISSN (PRINT) : 2395-695X
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 6, September 2015

carrier file such as .jpeg or .bmp image. The bits in the encrypted password will merge with the bits of a carrier file. Encrypt the image using unique key algorithm.

Unique Key algorithm for encryption of image

1) The .jpeg or.bmp image is given as input.
2) Allocate a key value of 256
3) Read image volume as matrix
4) Create matrix of random numbers.
5) Ceil the random values
6) Perform XOR operation of ceil values
7) Display the encrypted image

In the login phase If the user U_A wants to access the server S, the user U_A should insert the Smart card (S) in to the card reader and enter his/her ID_A and PW_A . Decrypt the image using unique key algorithm

Unique Key algorithm for decryption of image

1) Encrypted image is given as input
2) Allocate the mixture of same key of 256
3) Read the encrypted image size
4) Create random numbers
5) Ceil the random values
6) Perform XOR operation of ceil values
7) Display the original image

By using Least Significant Bit algorithm the embedded encrypted password in the image is extracted (original image). Decrypt the password by using Elliptic Curve Cryptography. In password change phase the user U_A can change his/her password PW_A to a new password PW_A'. In the authentication phase check the format of ID_A and the validity time.

7 CONCLUSIONS

Today there are many protocols and techniques for password guessing attack, in online or offline. In this paper we proposed PGAE scheme for encryption and PGAD scheme for decryption. The proposed scheme consists of four phases. They are 1) Registration phase, 2) Login phase 3) Password change phase and 4) Authentication phase.

In the registration phase the user U_A register to the server S with his/her identity ID_A and password PW_A. By using Elliptic Curve Cryptography the password is encrypted. The encrypted password is embedded in to the image by using LSB (Least Significant Bit algorithm) algorithm. Encrypt the image using unique key algorithm. In the login phase If the user U_A wants to access the server S, the user U_A should insert the Smart card (S) in to the card reader and enter his/her ID_A and PW_A . Decrypt the image using unique key algorithm. In password change phase the user U_A can change his/her password PW_A to a new password PW_A'. In the authentication phase check the format of ID_A and the validity time. The PGAE and PGAD based on Elliptic Curve Cryptography provide better security, privacy and user friendly when compared with the existing methods.

REFERENCES:

[1] A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card IET Information Security Chun-Ta Li Department of Information Management, Tainan University of Technology, 529 Zhongzheng Road, Tainan City 71002

[2] C.T. Li and C.C. Lee, "A Robust Remote User Authentication Scheme using Smart Card," Information Technology and Control, vol. 40, no. 3, pp. 231–238, 2011.

[3] "Defence to curb online password guessing attacks", R. Kirushnaamoni PG Scholar, Dept. of Computer Science and Engineering, IEEE.

[4] C.C. Chang and T.C. Wu, "Remote password authentication with smart cards," *IEE Proceedings-E*, vol. 138, no. 3, pp. 165–168, 1993.

[5] Secure password based remote user authentication scheme against smart card security Breach Ding Wang, Chun-Guang-Guang Ma,Qi-Ming Zhang, Sendong Zhao.Journal of networks, Vol 8, No 1,Jan 2013

[6] 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. Comput., Inf. Control, 2011, 7, (8), pp. 4821–4831.

[7]Islam, S.H., Biswas, G.P.: 'Design of improved password authentication and update scheme based on elliptic curve cryptography', Math. Comput. Model., 2012,

[8] Li, C.T., Lee, C.C.: 'A novel user authentication and privacy preserving scheme with smart cards for wireless

ISSN (ONLINE) : 2395-695X
ISSN (PRINT) : 2395-695X
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 6, September 2015

communications', Math. Comput. Model., 2012, 55, (1–2), pp. 35–44.

[9] Wang, R.C., Juang, W.S., Lei, C.L.: 'Robust authentication and key agreement scheme preserving the privacy of secret key', Computer Communication., 2011, 34, (3), pp. 274–280.

[10] Song, R.: 'Advanced smart card based password authentication', Comput. Stand. Interfaces, 2010, 32, (5–6), pp. 321–325.

[11] E.J. Yoon, E.K. Ryu, K.Y. Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 612–614, 2004..

[12] J. Xu, W.T. Zhu, and D.G. Feng, "An improved smart card based password authentication scheme with provable security," *Computer Standards & Interfaces*, vol. 31, no. 4, pp. 723–728, 2009.

[13] D.Florence, C Herley, and B Coskun, "Do Strong Web passwords Accomplish Anything?" Proc USENIX Workshop Hot Topics in Security (HotSec'07) 2007

[14] Security and efficiency in authentication protocols resistant to password guessing attacks. Taekyoung Kwon; Dept of Compuer Science., Yonsei Univ., Seoul, South Korea; JooSeok Song