Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 11, November -2016

Biometric based remote login password authentication scheme using smart card

[1]Pooja Mithoo, [2]Pranav Kumar

[1]*Department of Computer Science, Krishna Institute of Engineering &Technology Ghaziabad,India*
[2]*Department of Computer Science, IIT Dhanbad*

Abstract— *Authentication of remote user and server is a great research challenge in today's advanced wire and wireless communication. Engineers have proposed many password authentication schemes for remote login systems in past decades. In recent years, the biometrics technology has become a new issue in computer science. This new technology has allowed us to develop a novel method of user authentication using a smart card. In 2005, Ku et al. proposed an improved version of Password authentication scheme without using password table based on Geometric property of Euclidean plane. Which stands on better resistance to the offline password guessing attack and easily reparable. But unfortunately, their scheme is more difficult by user point of view and vulnerable by a wangle the legal user smart card and known password and PIN. The presented scheme of this paper is efficient in computation point of view and it is also secure from different types of cryptographic attackes.*

Keywords— *Cryptocraphy; Geometry; attack; Password authentication, Smart card.*

I. INTRODUCTION

Password authentication is one of the simplest and oldest approaches of entity authentication. In remote login password authentication system, each user has a private key, also called as password, and his identification, called public key. A user logs into the system with his password and ID and the remote server authenticates the user based on the authentication algorithm used by the system. Now-a-day, the password authentication with smart card is commonly used approach. In this approach, the users do not have to send password to the server, but he gives password to the smart card and the smart card computes message based on the information given by the user and sends that message to the server. The server authenticates the user with the help of received message from the smartcard and the further communication with it.

In a password authentication schemes, there having one common feature is that a password table, which should be securely maintained by the server and use to authenticate the remote user. In 1981, Lamport [1] proposed a remote password authentication scheme that could authenticate remote user over an insecure channel. If the password table is stolen or modified by an adversary, the total system will be damaged. So to reduce such risk, in 1990, Hwang et al. [2] proposed a non-interactive password authentication without using password table based on Shamir's ID-based signature. In 1991, Chang and Wu [3] proposed a password authentication scheme without using password table based on Chinese remainder theorem. But that scheme is vulnerable to a forgery attack as Chang and Laith [4] showed. In 1995 Wu [5] proposed an efficient "remote login authentication scheme based on a geometric property" of the Euclidean plane. However this scheme is not secure longer. In 1999, Hwang [6] proposed a Cryptanalysis to show that an illegal user can forge a valid login request from the eaves dropped login request. In 2001, Chien et al. [7] also proposed a modified remote login authentication scheme based on geometric approach with simply adding one extra hash function and bitwise xor operation instead of addition. However that scheme is also not secure further, as proposed by Chang and Lin [8] in 2005. In 2005, Ku et al. [9] proposed geometric based password authentication scheme using smart card with better resistant to the offline password guessing attack and easily reparable. Unfortunately this scheme is more difficult as because user needs to enter two information (PIN and password) for enhance the higher security. In 2004 Lin and Lai [10] proposed a 'flexible biometric remote user authentication scheme'. But Khan and Zhang [11] has shown that, this scheme is susceptible to the server spoofing attack. In 2010 Li and Hwang [12] proposed a remote user authentication scheme based on biometric verification but above scheme does not provide proper authentication and cannot resist man-in-the middle attack, as shown by Li et al. [13] in 2011.

In this paper we integrated passwords (*what the user know*), smart card (*what the user has*) and biometric(*what the user are*), and then construct a secure three factor authentication scheme that can be solved the above problems. Here we present a geometric based authentication scheme using smart card with having finger print, in this scheme the user needs to be enter only password and impression of finger print which provides better resistance in all aspect easily reparable than the improvement versions of Ku et al.[9] and it can resist man-in the middle attack. We provide solutions to these problems.

II. PROPOSED SCHEME

In proposed scheme there having five different phases namely User Enrolment Phase, Login Phase, Remote User Authentication Phase, Remote server Authentication Phase and Password change Phase. There are three kinds of participants the login user, Remote server (RS) and a Central authority(CA), where CA is assumed to be trusted. Initially, CA chose a large prime number P, a one way function **f** and pair **(x_0 , y_0)** is generated by CA and securely stored with CA and Server. The one way function f defined as follows:

Given x, it is easy to compute y=f(x)
Given y, it is infissible to compute $x=f^{-1}(y)$.

A. User Enrollment Phase:

Suppose a new user U_i , wants to register with the systems. U_i first choose password (PW_i) and identification id (ID_i). After that user obtains her/his fingerprint image via a sensor and then extracts the minutiae from the finger print image to form a template of the fingerprint and present f($PW_i \| B_i$) to CA, where B_i is the unique extracted template from imprint finger print on the input device. CA performs the following jobs:

Step1. Computes the point r_{iw} and r_{io} as (0, f($PW_i \| B_i$)) and (f ($ID_i \| x_0$), f($ID_i \| y_0$)) respectively.

Step2. CA also computes $V_i = f (f (PW_i \| B_i))$.

Step3. Construct a line L_i passing through point r_{iw} and r_{io} .

Step4. Compute a random point A_i in the ratio of m:n where (m > n) in the line L_i so A_i can be expressed as

$$A_i = (m * r_{io} + n*r_{iw}) / (m+n)$$

Store the parameters { ID_i, f, P, V_i , A_i , G, H } into the smart card of the user U_i, where $G= (m + n) \oplus f(PW_i \| B_i)$, $H=(m * n) \oplus f(PW_i \| B_i)$ and secretly deliver this card to U_i.

B. Login phase

When logging in, the registered user U_i first insert own smart card into the card reader and imprints the finger print. Then he/she needs only to enter their password PW_i and enter a onetime random number r_u into the system. If U_i passes the finger print verification then the smart card performs the following tasks:

Step1. Get the time stamp T from the system.

Step2. U_i smart card computes $r_{iw} =(0,f (PW_i \| B_i))$ and construct the line L_i passing r_{iw} and A_i.

Step3. Again it will computes the another arbitrary point C_i, in the ratio of m:n in between the point r_{iw} and A_i.where m:n can be retrieves by computing $m+n= G \oplus f(PW_i \| B_i)$ and $m * n= H \oplus f(PW_i \| B_i)$.

Step4. Now we can compute m and n by computing the following:

$$(m-n) = \sqrt{(m+n)^2 - 4(m * n)}$$
$$m1= (m *A_i + n*r_{iw}) / (m+n)$$
$$n1 = (m * n)/2$$

if(m1 >n1) then m=m1 and n=n1 otherwise m=n1 and n=m1 (as m>n)

Step5. Find $r_{iT} = (0, f (f (PW_i \| B_i) \oplus f (T)))$

Step6.Construct a line L_{wT} passing through the point r_{iT} and C_i.

Step7. U_i smart card randomly select a point R_i which is differ from r_{iT} and C_i ,on the line $L_{wT.}$ User's (U_i) smart card also computes $E_i= r_u \oplus f(PW_i \| B_i)$ and $K_i =f(PW_i \| B_i)$.

Step8. Construct an authentication message {ID_i ,A_i , R_i ,T, E_i, K_i, G,H} and transmit to the system for authentication.

C. Remote User Authentication phase

After receiving the message {ID_i ,A_i , R_i ,T, E_i, K_i} the system performs the following task to authenticate user's (U_i) login request.

Step1. Check the validation of identity ID_i . If it is invalid then login request will be rejected.

Step2. If (T – T') ≥ ΔT, where T' denotes the current time and ΔT denotes the expected valid time interval for transmission delay, then the system will rejected the login request.

Step3. Calculate r_{io} = (f (IDi || x_0), f(IDi || y_0)).

Step4. Then reconstruct the line Li passing through the point r_{io} and A_i.

Step5. Find the intersection point of the y-axis and line L_i denote P_i. Let r_{io} = (0, P_i) and then compute r_{iT} = (0, f (P_i ⊕ f(T)).

Step6.Reconstruct the line L_{wT} passing through the point r_{iT} and R_i , and then computes the intercept point D_i of L_i and L_{wt} .

Step7. If the $D_i = (m*A_i + n*ri_w) / (m+n)$ is the identical, then Correspondence holds and remote user is authenticated and proceed further for server authentication, where m and n is computed as step 4 in Login phase .

Step8. Now RS retrieves r_u by computing (E_i ⊕ K_i)
Step9. RS chose a one time useable random value r_s and send the message { (r_s ⊕ K_i), f(r_s,r_u)} to the remote user smart card.

D. Remote Server Authentication Phase

After received the message { r_s ⊕ K_i , f(r_s,r_u)} from the server, the smart card performs the following task to check the authentication of server.

Step1. Smart card retrieves r_s by computing (r_s ⊕ Ki ⊕ f(PWi || Bi))

Step2. Computes f(r_s,r_u).

Step3. Compares the calculated and received value of f(r_s,r_u), if not equal then the connection is terminated, otherwise the Remote Server RS is authenticated.

Step4. Access to the RS is granted.

E. Password change phase

Whenever user wants to change current password PW_i to the new password PW_i^* ,needs to imprint finger print and insert U_i smart card into the smart card reader and then enter the current password.

Step1.User's (U_i) smart card uses PW_i and finger print template B_i to compute Q_i= f (PW_i || B_i) and f(Q_i).After User's (U_i) passes finger print verification with the stored value of V_i, needs to input the old password PW_i and new password PW_i^*. User's (U_i) smart card set the point r_{iw}= (0, Q_i). Otherwise request will be rejected.

Step2. User's (U_i) smart card computes $r_{io} = ((m + n) A_i – m.ri_w) /n$
Where m and n is computed as step 4 in Login phase .

Step3. $r_{iw}^{(new)}$ = (0, f(PW_i^* || B_i))
Now, User's (U_i) smart card computes $V_i^{(new)} = (m.r_{io} + n.r_{iw}^{(new)}) / (m+n)$

Step4. User's (U_i) smart card replaces the stored A_i and V_i with $A_i^{(new)}$ and $V_i^{(new)}$, where $V_i^{(new)}$ = f (f (PW_i^* || B_i))

III. CRYPTANALYSIS

In this section, we demonstrate the capability of our proposed scheme to defy the attacks which can take place in password authentication system.

Resistance of stolen smart card and known password, PIN attack:

In ku et al. scheme [9], suppose an user smart card is stolen and he knows the user password and PIN then adversary can easily authenticate as a legal user. But in our scheme, in case the adversary can achieve the legal user's smart card and password, he/she has not theft the fingerprint template in any phase. On checking the adversary's fingerprint minutiae with/by the minutiae template registered on the smart card, the illegal access will be discarded.

A. Resistance man-in-the middle attack:

MITM is a common attack, relevant on many cryptographic approaches. This attack ignores the internal structure of system [14].An attacker requires pairs of plaintexts and corresponding cipher texts for control to encryption and decryption. In Li and Hwang's [6] approach, server selects a random number R_s for any login credential message (ID_i,M_2), the attacker E eavesdrops the message (ID_i,M_2) and stars a session with server using the same message (ID_i,M_{E2})=(ID_i,M_2). By changing the corresponding authentication messages, attacker can execute the man-in-the middle attack. But in our scheme the shared line L_i constructed in the initial registration phase, so that even if the attacker E eavesdropped the login credentials {ID_i, A_i, R_i,T, E_i, K_i, G,H}, however the L_i is only known to the system (constructed from points r_{i0} and A_i) and the registered user U_i (constructed from points r_{iw} and A_i) .Thus, the correct line L_i can't be reconstruct by the attacker E without perceptive r_{i0} or r_{iw}. So man-in-the middle attack can't be performed by the attacker.

B. Resistance to Insider attack:

An insider attack is a type of malicious attack. Insiders that perform attacks have a distinct advantage over external attackers because they as insider have authorized system access and also recognizable with network system architecture, so it have a distinct advantage over external intruder.

As we have seen in this proposed scheme the user U_i register with CA by submitting $f(PW_i \| B_i)$ instead of PW_i or $f(PW_i)$ to CA. Any challenger may discover no useful knowledge for learning a user password from the public parameter by applying the secure one way function f. So this scheme is withstand the insider attack.

C. Resistance off-line password guess attack:

In this proposed scheme, let that the adversary has intercepted the login massages { ID_i, A_i, R_{i1}, T_1 } and { ID_i, A_i, R_{i2}, T_2 } transmitted in step 8, at time T_1 and T_a respectively in login phase. Next he can guess the candidate password $PWi^{"}$ and then attempt to confirm his guess by using intercepted credentials. If the adversary can compute $r^{*}_{iT1} = (0, f(f(PW_i^{"} \| B_i) \oplus f(T_1)))$, he can determine $L^{"}_{WT1}$ passing through the $r^{"}_{iT1}$ and R_{i1}. Similarly if the adversary can compute $r_{iT2,}$ can find out $L^{"}_{WT2}$ passing through the $r^{"}_{iT2}$ and $R_{i2.}$. Then the adversary can compute the intersection point $D^{"}_{i}$ of $L^{"}_{WT1}$ and $L^{"}_{WT2.}$ On the other hand, if the adversary can compute $r^{"}_{iw}$, he can easily obtain the middle point $D^{""}_{i}$ of $r^{"}_{iw}$ and A_i. Once the equation $D^{"}_{i} = D^{""}_{i}$ holds, the adversary has correctly guessed $PW_i^{"}$. However, since the adversary guessed password successfully he can not authenticate until he will not change the stored B_i with his own finger print template B_{i1} and respective parameter, from smart card. Therefore this scheme is resist off-line password guessing attack.

D. *Resistance of reply attack:*

In replay attack[15] information is stored without any authorization and then retransmitted through unauthorized operations such as fake credentials or authentication or a replica/duplicate transaction. In our propsed scheme, suppose the adversary intercepted the login message {ID_i ,A_i , R_i, T, E_i, K_i, G,H} then adversary can attempt to impersonate U_i to login through server by directly replying intercept message to server. Clearly server will rejected the login request because step 2. In Remote User authentication phase will be invalid. In other way if the adversary change the intercepted message with {ID_i ,A_i, R_i,T_1 , E_i, K_i, G,H},with the current timestamp T_1, then also the login request will be rejected by the server, as because T_1 is inconsistent with R_i and as a result, the computed H_i can not be identical with A_i . So our presented scheme resists reply attack successfully.

E. Reparability:

If adversary has learned password PW_i then also he cannot impersonate U_i to login server as because he cannot generate B_i. But however if any how he passed the fingerprint verification then he can impersonate U_i to login server. In this case, if U_i finds or suspect that someone impersonate, then he can change his password by changing only his old PW_i with new password PW_i^* as mentioned in password change phase. Hence this scheme is easily reparable than Ku et al. proposed scheme, because in this scheme, it needs to change only the password not anything else.

F. *The Brute Force attack:*

In this type of attack, all possible combinations of password apply to break the password.[16] Using brute force attack was a difficult task in the past but it is easier today using computer. Brute-force attacks are straightforward to recognize. It is also called exhaustive key search attack. Encrypted file is stolen by attacker. They know that encrypted file contains message which they (attacker) wants, and the can unlock the message through encryption. Attacker tries by every single key to decrypt the message so he can success to create the original message.
In the proposed scheme there is one hash function F() is used. It works on the output of some logical computation based on both password and figure print template. So it is very difficult and time consuming to apply brute force technique to crack F() , because it will not give the actual password or figure print template.

G. The Deriving the Secret key of the System:

In this type of attack intruder tries to derive the secrete key of the system. Let n=p*q then intruder tries to find p and q to break the system. In the proposed scheme the secret key (p) selection is not based on any calculation It is a very large prime number which is selected by system from a large collection of prime numbers. So it is very difficult to find n from a large collection of prime numbers whose number is increasing day by day.

H. The Dictionary Attack:

Dictionary Attack is relatively faster than brute force attack. The attacker doesn't check for all possible value of password of given length but, he tries to match with some well known format of passwords. The proposed scheme is not only depends on the password which can be guessed but also depends on the parameters stored in the smart card and the figure print template. So dictionary attack is very difficult to implement for this scheme.

I. Rainbow table attacks:

By using the hash as the key it is possible to target a time space trade-off by pre-computing dictionary words from a hash list. But Attack execute faster as it require considerable less amount of preparation time. Due to the low cost of disk storage the storage requirements for the pre-computer tables were the major cost. It is less of an issue now-a-days. Pre-computed dictionary attacks are particularly effective when a large number of passwords are to be hacked. To find the corresponding password we can refer password hashes instantly any time.

The proposed scheme is not only depends on the password which can be guessed but also depends on the parameters stored in the smart card and the figure print template. So dictionary attack is very difficult to implement for this scheme.

K. The Shoulder Surfing Attack:

The attacker spies the user's movements to get password. He observes the user to know, how he enters the password i.e. what keys of keyboard the user has pressed. In the proposed scheme smart card and figure print template are used. So the possibility of Shoulder Surfing Attack is very low.

L. The Stolen-Verifier Attack:

In this attack intruder Steals the verification password table and try to break the system and guess the password. In the proposed scheme no verification table is needed .So, it is not possible for an attacker to apply the stolen verifier attack on it.

M. Denial of service attack:

System may slow or totally damage/interrupt the services by the DOS. Many strategies use by the attacker to achieve this. It is designed to bring the whole network system damaged with useless traffic. For all known DoS attacks, there is software so that user can install to limit the damage caused by the attacks.

In our scheme smart card is used and at first the verification of login id takes place then after further computation completed. If a message arrived to server having wrong login id then that message will be discarded by server without performing the computation on that message. The bandwidth usage of our scheme is very low so, it can survive with extra network traffic.
From the result of cryptanalysis we observed that our scheme is not at risk to different types of attacks. It means as compare to other existing schemes our scheme is more secure.

IV. PERFORMANCE ANALYSIS

After performing the cryptanalysis on our scheme we tried to find the overhead of our scheme. For doing it we take three parameters these are as follows:

A. No of operation performed

In our scheme we are using smart card. The computational capacity of smart card is limited. So, the measure operation is performed at server. Now a day calculation of hash function is very time and power consuming. In our scheme we are used only one hash function. Smart card performs the execution only one time of this only hash function. Rest of operation are simpler arithmetic operations.

B. Network Usage

In our scheme we performed the all operation on galious field GF_n , Where n is a prime number. So any intermediate value cannot be more than n. In the login phase smart card sends a message to server for authentication but the length of this message is very small and its depend on chosen n.
The maximum size of transmitted message= $8 * \log_2^n$
So, the transmitted message will take less bandwidth to travel from smart card to authentication server.

C. Size of data base used

In our scheme central authority only store the value of n and the ratio of interception. The size of these parameters is very small. So there is no need to maintain a large database. Some time if the size of data base became very large then it takes even more time to access the value of secure parameters. So, the performance of our scheme is better.

V. CONCLUSION

A Biometrical authentication scheme based on geometric approach using smart card. The problem of user of ku et al. and 2010 Li and Hwang scheme. ku et al scheme is vulnerable in stolen smart card and known password and PIN. Li and Hwang proposed a remote user authentication scheme based on biometric verification but above scheme does not provide proper authentication and cannot resist man-in-the middle attack.

The combination of passwords (what the user know), smart card (what the user has) and biometric (what the user are), and then construct a secure three factor authentication scheme that can be solved the above problems. In this scheme the user is need not to remember two passwords (password & PIN) to enhance the higher security. This scheme also can resist offline password guessing attack, reply attack, insider attack, man in the middle attack and easily reparable. We performed the cryptanalysis on proposed scheme and found that our scheme is non vulnerable to different types of attacks like password guessing attack, reply attack, Brute Force attack, Dictionary Attack, Phishing Attacks, side channel attacks and so on.

VI. REFERENCE

[1] L. Lamport, "Password authentication with insecure communication," Communication of the ACM , vol. 24(11) , November 1981, pp. 720-722.

[2] T. Hwang, Y. Chan, C.S. Laih, "Non-interactive password authentication without password tables," IEEE Region 10 Conferrence on Computer and Communication systems, IEEE Computer Society, 1990 (September), pp. 429-431.

[3] C. C. Chang ,T. C. Wu, "Remote password authentication with smart card," IEE Proc. –E, vol. 138, no.3, pp. 165-168.

[4] C. C. Chang, C. S. Laith, "Correspondence: Remote password authentication with smart cards," IEE Proc.-E,vol.139, no.4,1992, pp. 372.

[5] T. C. Wu, "Remote login authentication scheme based on a geometric approach," Computer Communication, vol.18, no.12, December 1995, pp. 959-963.

[6] M. S. Hwang, "Cryptanalysis of remote login authentication scheme," Computer communication, vol.22, no.8, 1999, pp. 742-744.

[7] H. Y. Chien, J. K. Jan, Y. M. Tseng, " A modified remote login authentication scheme based on geometric approach," J. System Software, vol.55, no.3, January 2001, pp.287-299.

[8] C. C. Chang, I. C. Lin, "Cryptanalysis of the modified remote login authentication scheme based on geometric approach," Informatica, vol.16, no.1, 2005, pp. 37-44.

[9] W. C. Ku, H. H. Chen, S. T. chang and C. H. Hwang, "An improved geomatric based password authentication scheme using smart card," Proceeding of the workshop on Consumer Electronics and signal processing, 2005.

[10] C. H. Lin and Yi-Yi Lai, " A flexible biometrices remote user authentication scheme," Computer Standard and Interfaces, vol.27, 2004, pp. 19-23.

[11] M. K. Khan and J. Zhang, Improving the security of " a flexible biometrices remote user authentication scheme," Computer Standard and interfaces vol. 29, no.1, 2007, pp.82-85.

[12] T. C. Lie and M. S. Hwang, " An efficient biometrices based remote user authentication scheme using smart card." Jurnel of Network and Computer Applications, vol.33, 2010, pp. 1-5.

[13] X. Lie, J. W. Nieu, J. Ma, " Cryptanalysis and improvement of a biometrices based remote user authentication scheme using smart card," vol.34, 2011, pp. 73-79.

[14] Shish Ahmad, Mohd. Rizwan, Beg Jameel Ahmad and Nabarun Barua, "Meet In The Middle Attack: A Cryptanalysis Approach", International Journal of Computer Applications, Vol. 1, No. 25, 2010, pp. 1-5.

[15] Syverson, P. et al., "A taxonomy of replay attacks" Proceedings of Computer Security Foundations Workshop Vol. 7, 1994, pp. 187-191.

[16] Fujita, K. and Y. Hirakawa, "A study of password authentication method against observing attacks", International Symposium on Intelligent Systems and Informatics, Vol. 6, SISY 2008.

[17] Thomas S. Messerges, Ezzat A. Dabbish and Robert H. Sloan, "Examining smart-card security under the threat of power analysis attack", IEEE Trans. on computers, Vol. 51, No. 4, 2002.

[18] Paul C. Kocher, "Timing Attacks on implementations of Die-Hellman, RSA, DSS, and Other Systems," International Journal of Advances in Engineering & Technology, Vol. 4, No. 2 , 2012, pp. 150-155.

