Remote Login Password Authentication Scheme using Tangent Theorem on Circle in a Multi-Server Environment

$ShipraKumari^1, HariOm^1$
Computer Science and Computer Engineering
Indian School Mines, Dhanbad
Jharkhand, 826004
Email: [1]shiprakumari18jan@gmail.com, [2]hariom4india@gmail.com

***Abstract*—In this paper we propose a remote password authentication scheme based on a circle. This scheme is simple and practically feasible in a multi-server environment. In this scheme, we use some simple tangent theorem like secant tangent theorem and a strong one way function to authenticate the user and the server. Furthermore, a legal user can freely choose and change his password using his smart card. The security of this scheme depends on the tangent points located in a plane associated with the circle and tangent line.**

Keywords: Authentication, Tangent Theorem, Chinese Remainder Theorem, Circle

I. Introduction

In this network environment, the communication among persons depends on the remote computers. Sharing or communication through remote computers however causes unauthorized access or unauthorized service. Therefore, the selection of a appropriate security scheme to prevent the data to be disclosed, altered, copied destroyed or forged becomes very important. Among the existing security schemes, the password authentication is broadly adopted authentication method in login procedure because of its user friendliness and easy implementation. Lamport [1] has discussed the first remote password authentication scheme in which the server stores a password table to check the client legitimacy. If a user wishes to enter the system, he has to login by entering his account ID and password. The system validates the submitted ID and password according to the information available in the verification table. The very problem with [1] is that in order to maintain a management system the verification table has to be kept inside the system. These schemes however suffer from the problem of server compromise attack or verification table modification attack. Several new methods have been developed that do not require a password table. These methods perform smart card-based authentication.

To date, several researchers have developed more secure authentication schemes using different techniques to communicate securely without using any password table. Many use smart card to identify a fake user and to decrease the server overhead, assuming the smart card is maintained securely [2]-[4] Some schemes are also developed using geometric like, Wu has discussed a remote login authentication scheme using geometric in the Euclidean plane along with smart card. In this scheme, no verification table is required and a user can freely choose his password [5].However, Hwang has showed that an illegal user can easily forge a valid message [6]. Later, Chien has showed that the Wus scheme is breakable and they improved it [7]. Liaw and Lei discuss an authentication scheme based on unit circle in which the radius of the circle is one unit, i.e.1 and its center is origin i.e. (0,0) in 2-Dim. [8]. Instead of on the simple Euclidean space in past schemes Wang discusses another scheme using an N-dimensional construction based on the circle. The author claimed that this scheme would be more secure than previously proposed schemes [9]. However, Shuhong et al.s show that the scheme of Wang is vulnerable to off-line password guessing and replaying attacks [10]. These schemes also have some limitations, e.g., a user cannot change his password and mutual authentication cannot be performed.

Das et al. proposed a dynamic ID-based remote user authentication scheme using smart cards[11]. They pointed out that their scheme does not maintain any verification table and can resist the guessing attacks, insider attacks, replay attack and forgery attacks. However, Wang et al. pointed out that Das et al.s scheme does not achieve mutual authentication and could not resist impersonation attack[12]. Wen and Li analyzed Wang et al.s scheme and pointed out that their scheme is susceptible to impersonation attack; only through intercepting and modifying the messages transmitted in the public networks, the third person could impersonate the legal user to login the server. Moreover, an insider user who has registered in the remote server can expose some secret information of the server and the other user and proposed an improved scheme, which can resist impersonation attack, avoiding partial information leakage and providing anonymity for the users[13]. However, recently, Juan et als pointed that Wen and Lis scheme cannot withstand insider attack and forward secrecy, and, though eavesdropping the users login request message in the public networks, the user can be traced out, and also proposed secure dynamic- ID

978-1-4799-3486-7/14/$31.00

remote user authentication scheme using ECC[14]. In 2009, Liao and Wang also presented a dynamic ID-based remote user authentication scheme using one way hash function [15]. However, Chen et al. pointed out that Liao-Wangs scheme does not provide forward secrecy[16]. Hsiang and Shih found that Liao-Wangs scheme fails to resist insider attack, impersonation attack, server spoofing attack and shows inadequacy in providing mutual authentication. To overcome these weaknesses, they also proposed an improved scheme[17]. Though, Sood et al. showed that Hsiang-Shihs improved scheme fails to provide security against replay attack, impersonation attack, stolen smart card attack and has incorrect password change phase[18].
We now discuss our proposed method which fulfill all the security requirements and easy to implement.

Table 1: Notation Used

Symbol	Meaning
ID,PW	Identity and Password of User U
p,g	Large prime no. and generator of p
SR_i	ith server
e_i,d_i	Public and secret key of ith server
r_i	Relatively prime no. of ith server
C,D,M,N,A,B	Points on xy plane of User
T	Current login time of user
RC_i, RS_i	Radius of circle
m_i, n_i	Slope of line
L_i, L_c, L_s	Line in different phase
*, $\|$,$\oplus$	Multiplication , concatenation, XOR

II. Proposed Scheme

A. Initialization

Let SR_i, 1$\leq$ i $\leq$m be a set of servers in a multi-server environment. There is a trusted central manager (CM) that performs the following actions: Select a Galois field GF(p) for large prime p and assuming g as a its generator Compute servers secret key d_i and a prime number r_i relatively prime for each server and calculate
e_i= $g_i^{d_i}$ mod p, 1 $\leq$ i $\leq$ m Each server SRi stores its parameters: (e_i, d_i, r_i).C_{x_i}

B. Registration

Assume that the new user is granted registration only by a set S_n of servers, where $S_n \subseteq S_m$

(i) The new user chooses and delivers his own identity ID and password f(PW) to CM securely.
(ii) For each server $SR_i \subseteq S_n$, the CM calculates the following pairs of points on the xy-plane: C=(C_{x_i}, C_{y_i}) and D = (D_{x_i}, D_{y_i}) where
C_{x_i} = ID^{e_i} mod p, C_{y_i} = ID^{d_i} mod p,
D_{x_i} = e_i^{ID} mod p , D_{y_i} = $e_i^{f(PW)}$ mod p

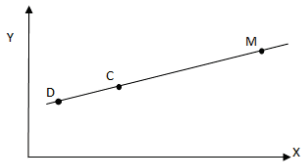

Fig. 1. Registration Phase

(iii) CM constructs a line Li passing through the points C and D.

(iv) CM randomly chooses a point M = (M_{x_i}, M_{y_i}) on line L_i

(v) Let K be a number for each server in which the user U_i is registered, where

(vi) K= f(ID $\|$ d_i) mod , for i=1,2,$\cdots$, n.

(vii) Compute this number K using the Chinese Remainder Theorem (CRT)
(viii) CM stores {ID, M[], K, e[], g, p} message in the smart card and delivers it to user U_i .

C. Login

When the user U wants to login a set of server S_n , he keys his identity ID and password PW. Then, the smart card performs the following:

(i) Obtain a current login time T from the system.
(ii) Compute the point D=(D_{x_i}, D_{y_i}) as
D_{x_i} = e_i^{ID} mod p , D_{y_i} = $e_i^{f(PW)}$ mod p
(iii) Redraw a line L_c passing the points D and M.
(iv) Compute slope (m) of line L_c as $m - i$ = (M_{y_i} D_{y_i})/(M_{x_i} D_{x_i})
(v) Compute C_{x_i} = ID^{e_i} mod p
(vi) Compute C_{y_i} by substituting C_{x_i} in the equation of line L_c
(vii) Compute RC_i = $e_i^{f((D_{y_i} \oplus f(T) \| K)}$ mod p
(viii) Draw a circle in xy-plane using the point C = (C_{x_i}, C_{y_i}) as center and RC_i as radius.
(ix) Through the point M draw a tangent on a circle which touches the circle at point N
(x) Draw a line from the center C to tangent point N. By tangent theorem, the line CN is perpendicular to the tangent line. Thus, <MNC = 90^0 (refer Fig.2).
(xi) By Pythagoras theorem $MN_i^2 = (MC_i^2 - CN_i^2)$ mod p where, CN_i^2= RC_i
(xii) Compute $\alpha_i = f(ID \oplus T \oplus MN_i^2)$
(xiii) Send the authentication message: $\{ID, \alpha_i, T\}$.

D. Authentication

Upon receiving a login request at time T, the server SRi performs the following:

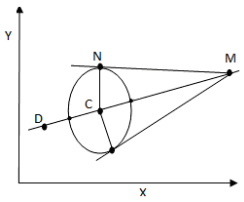

Fig. 2. Login Phase

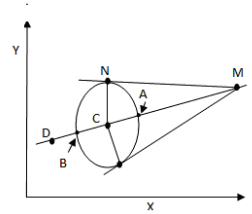

Fig. 3. Authentication Phase

(i) Check whether the format of ID is correct. If not, login request is rejected.
(ii) Check whether the transmission time $(T^1 - T)$ is within the legal tolerant interval $\triangle$T. If $(T^1 - T) > \triangle T$, then the login request is rejected.
(iii) Compute K_c = K mod $r_i, for 1 \leq i \leq n$
(iv) Compute K_s = f(ID $\|d_i$) mod $r_i, for 1 \leq i \leq n$
(v) If $K_s \neq K_c$, then login is terminated.
(vi) Compute:
= C_{x_i} = ID^{e_i} mod p, C_{y_i} = ID^{d_i} mod p,
(vii) Using the points C and M, draw a line L_s.
(viii) Compute slope n_i of line L_s
n_i = (M_{y_i} - C_{y_i})/(M_{x_i} - C_{x_i})
(ix) Compute RS_i = $e_i^{f((D_{y_i} \oplus f(T) \| K)}$ mod p
(x) Server sends f($n_i \oplus RS_i$) to the user .
(xi) User compare f($n_i \oplus RS_i$) and f($m_i \oplus RC_i$), if equal then Server SR_i is authenticated then, proceed. Otherwise, terminate the session.
(xii) Draw a circle in xy-plane using the point C as center and RS_i as radius
(xiii) Equation of the circle is
$(x - C_{x_i})^2 + (y - C_{y_i})^2 = RS_i^2$ ———(1)
(xiv) Equation of the line Ls is
$y - C_{y_i} = n_i(x - C_{x_i})$ ————(2)
(xv) Let line Ls cut the circle at two points.
(xvi) From (1) and (2), we get two points: A and B
(xvii) Draw a tangent on the circle from the point M
(xviii) If N is a tangent point on the circle, then by Secant Tangent theorem $MN_i^2 = MA * MB$, where AB is secant of circle that passes through the center C. Thus, AB is the diameter of circle (refer Fig.3). Now,
$MN_i^2 = MA_i * MB_i = MA_i * (MA_i + MB_i)$
$= (MC_i - CA_i) * ((MC_i - CA_i) + 2 * CA_i)$
$= (MC_i - CA_i) * (MC_i + CA_i)$
$= MC_i^2 - CA_i^2 = MC_i^2 - CN_i^2$
$where, CN_i = CA_i = RS_i$
(xix) Compute $\beta_i = f(ID \oplus T \oplus MN_i^2)$
(xx) If $\alpha_i = \beta_i$, then user is authenticated; otherwise the login request is rejected.

E. Password Change Phase

To change the password, the user U first enters his smart card and then his Identity ID and password PW.

(i) Compute the point D =(D_{x_i}, D_{y_i}) as
$D_{x_i} = e_i^{ID}$ mod p and $D_{y_i} = e_i^{f(IPW)} mod p$
(ii) Redraw a line L_c passing the points D and M.
(iii) Compute $C_{x_i} = ID^{e_i}$ mod p
(iv) Compute C_{y_i} by substituting C_{x_i} in the equation of line L_c
(v) If user U and servers SR_i are authenticated, then
(vi) Enter new password PW_{new}
(vii) Compute $(D_{y_i})_{new}$ as
$(D_{y_i})_{new}$ = $e_i^{f(PW_{new})}$mod p
(viii) Redraw a line $(L_c)_{new}$ passing the points $(D)_{new}$ and C.
(ix) Take an arbitrary point $(M)_{new}((M_x)_{new}, (M_y)_{new})$ on the line $(L_c)_{new}$.
(x) Replace the M by $(M)_{new}$. Password is changed successfully.

III. ILLUSTRATION

We illustrate our algorithm using numerical example.
Initialization

(i) Let CM chooses p=31, g=11.
(ii) Let SR_1, SR_2, SR_3, SR_4 are set of servers.
(iii) CM Chooses servers secret key d_i and a relatively prime number r_i for each server.
(iv) Let secret key and a prime number of SR_1, SR_2, SR_3, SR_4 are(10,19), (11,37), (66,73), (18,11)relatively.
(v) Compute: e_1 = 5, e_2 = 24, e_3 = 4, e_4 = 2, where. e_i= $g_i^{d_i}$ mod p

(vi) Each server stores (e_i, d_i, r_i).
SR_1 stores (5,10,19)
SR_2 stores (24, 11,37)
SR_3 stores (4, 66,73)
SR_4 stores (2, 18,11)

Registration:

(i) User chooses his identity ID=2679 and password PW=1408 and Send ID and f(PW)=19 to CM
(ii) Let user U registered with Server SR_1 and SR_2
(iii) CM calculates: ID= 2679 mod 31=13
(iv) For server SR_1 : $C_1 = (6, 5), D_1 = (5, 5)$

(v) Compute equation of line L_1 through points: C_1 and D_1
Y - 5 = 0
(vi) CM chooses an arbitrary point on line L_1. let M_1 = (20,5)

(vii) For server SR2 :$C_2 = (2, 8), D_2 = (12, 17)$

(viii) Compute equation of line L_2 through points: C_2 and D_2
9X - 10Y + 78 = 0

(ix) CM chooses an arbitrary point on line L_2. let M_2 = (10,9)

(x) Let K be a number for each server SR_1, SR_2 in which the user U is registered such that,
K =$f(13 \oplus 10)$ mod 7
K =$f(13 \oplus 11)$ mod 3

(xi) Using Chinese remainder theorem CM computes K=128

(xii) Store $\{2679, \{(20, 5), (10, 9)\}, 128, \{5, 24\}, 31\}$ in the smart card and deliver it to the user.

Login:
User first inserts his smart card and then his ID and PW.
Get current time from the system, let T = 15

(i) Smart card computes:

(ii) For Server SR_1:C_{x_1} =6, D_1=(5,5)
Using points: M and D, draw a line L_c
slope of the $L_{c_1} = m_1 = 0$
Substituting C_{x_1} = 6 in equation of line L_c , we get C_{y_1} = 5
Compute $RC_i = 5^{f((5 \oplus 26) \| 128)}$ mod 31=25
Draw a tangent on circle through a point M. Draw a line from center C of the circle to the tangent point N. By tangent theorem, CN is perpendicular to MN.
$MN_i^2 = 14^2 - 25^2 = 5$
Compute α_1 = 2

(iii) For Server SR_2:C_{x_2} =2, D_2=(12, 17)
Using points: M and D, draw a line L_c
Slope of the line L_{c_2} : m_2 = 4
Substituting C_{x_2} = 2 in equation of line L_c , we get C_{y_2} = 8
Compute $RC_2 = 24^{f((17 \oplus 26) \| 128)}$ mod 31 = 15
Draw a tangent on circle through a point M. Draw a line from center C of the circle to the tangent point N. By tangent theorem, CN is perpendicular to MN.
$MN_2^2 = 20$
Compute α_2 = 16

(iv) Send the authentication message = $\{2679, \{2, 16\}, 15\}$

Authentication Phase
Upon receiving a login request at time T_1, the server SR_i performs the following:

(i) Check the format of ID and legal tolerant interval of transmission.

(ii) For Server SR1:
Compute K_c = 128 mod 7 = 2 and K_s = 16 mod 7 = 2
Here, K_s = K_c = 2, then login is continued
Compute: C_{x_1} = 13^5 mod 31 = 6, C_{y_1} = 13^{10} mod 31 = 5
Using the points C_1 and M_1, draw a line L_{s_1}.
Compute RS_1 = 25
Compute slope of line L_{s_1} as n_1 = 0
Server sends f($n_1 \oplus RS_1$) =25 to the user .
User equate f($n_1 \oplus RS_1$) = f($m_1 \oplus RC_1$)=25, then Server SR_1 is authenticated.

(iii) To authenticate user U by server SR_1 : Using point C_1 as center and RS_1 as radius draw a circle in xy-plane.
Equation of the circle:
$(x - 6)^2 + (y - 5)^2$ = 252
Let line Ls cuts the circle at points A_1 and B_1
Equation of the line L_s through point C_1 and slope n:
y = 5
Draw a tangent on circle from point M. If N is tangent point on a circle, where AB is secant of circle but it passes through the center C. Thus, AB is diameter of circle
By Secant tangent theorem
MN_1^2 = MA_1 * MB_1 = 5
Let β_1 = 2
Here, α_1 = β_1 = 2, So, user U is authenticated by server SR_1.

(iv) For Server SR_2: Compute K_c = 128 mod 37 = 17 and K_s = 17 mod 37 = 17
Here, K_s = K_c = 17, then login is continued
Compute: C_{x_2} = 2, C_{y_2} = 8
Using the points C_2 and M_2, draw a line L_{s_2}.
Compute RS_2 = 15
Compute slope of line L_{s_2} as n_2 =4
Server sends f($n_2 \oplus RS_2$) =11 to the user .
User equate f($n_1 \oplus RS_1$) = f($m_1 \oplus RC_1$)=11, then Server SR_2 is authenticated.

(v) To authenticate user U by server SR_2 : Using point C_2 as center and RS_2 as radius draw a circle in xy-plane.
Equation of the circle:
$(x - 2)^2 + (y - 8)^2$ = 252
Let line Ls cuts the circle at points A_2 and B_2
Equation of the line L_s through point C_2 and slope 4:
y - 2 = 4(x - 8)
Draw a tangent on circle from point M. If N is tangent point on a circle, where AB is secant of circle but it passes through the center C. Thus, AB is diameter of circle
By Secant tangent theorem
MN_2^2 = MA_2 * MB_2 = 20
Let β_1 = 16
Here, α_1 = β_1 = 16, So, user U is authenticated by server SR_2.

Hence, User U authenticated by servers SR_1 and SR_2 and also both servers are authenticated.

IV. Security Analysis

1) Replay attack: The replay attack cannot work on our proposed scheme because of the renewal of α_i, β_i ,

f($n_i \oplus RS_i$), $f(m_i \oplus RC_i)$ at different timestamps T for every login session. So, there is no possibility of replay attacks.

2) Stolen verifier: Since the server neither saves any verification table nor stores any entry in its database, no question arises for an attacker to make a way inside the scheme.

3) Privileged insider attack: Our scheme could withstand privileged insider attack. In the registration phase of our scheme, the user sends f(PW) to the Central Authority. So, privileged insider cannot get the users password PW as it is protected by a secure hash function.

4) Server masquerading attack: Our scheme could withstand server masquerading attack. To impersonate the server to the user, the adversary cannot calculate K_s without the value of d_i and r_i. Thus, $K_c \neq K_s$ and hence our scheme could withstand the server masquerading attack.

5) Mutual authentication: Our scheme can work on the multi-server environment and every server and users are mutually authenticated. All users and servers compute $(\alpha_i, f(m_i \oplus RC_i))(\beta_i, f(n_i \oplus RS_i))$ using their own secret keys. Therefore, the server and user authenticate each other by checking the legality of $(\alpha_i = \beta_i)$, (f$(n_i \oplus RS_i) = f(m_i \oplus RC_i)$) and

6) Impersonation attack: Our scheme could withstand user impersonation attack The adversary cannot C_y as he does not know the servers secret key d_i. $C_y = ID^{d_i}$ mod p

7) password guessing attack: If the adversary extracts the secured data in smart card though physically monitoring its power consumption. He can also get the authentication message. Let the adversary guess the password PW. He cannot verify the correctness of PW without servers secret key d_i .

V. Comparision

This section describes comparison among various multiserver authentication schemes with our proposed scheme on the basis of security features as well as possible attacks. Table 2 shows this comparison.

Table 2. Comparison among our proposed scheme with various multi-server authentication schemes.

Features	[15]	[17]	[18]	Proposed Scheme
R_1	Y	Y	N	Y
R_2	Y	Y	Y	Y
R_3	Y	Y	Y	Y
R_4	Y	Y	Y	Y
R_5	N	N	Y	Y
R_6	N	N	Y	Y
R_7	Y	N	Y	Y
R_8	Y	N	Y	Y

Where,Y= Yes, N= No
R_1=Free from maintaining verification table
R_2=User is allowed to choose the password
R_3= User is allowed to change the password
R_4 = Provides mutual authentication
R_5 = Resists user impersonation attack
R_6 = Resists server impersonation attack
R_7= Resists replay attack
R_8= Provides mutual authentication without the support of Central Manager

VI. Conclusion

In this paper, we have discussed a new remote user authentication scheme based on the tangent theorem of circle. Instead of unit circle, we have used different center of circle on a XY-plane (i.e, center of a circle is not fixed to (0,0) with different size (i.e, radius of circle) for every user in different login session. This scheme provides freedom to choose and change password to a user and achieves mutual authentication between a user and remote servers.

References

[1] L. Lamport, "Password authentication with in secure communication," Communications of the ACM, Vol. 24(11), pp. 770-772, 1981.

[2] Chang, C.C., Wu, T.C.: Remote password authentication with smart cards. IEE Proceedings-E 138(3), 165168 (1993)

[3] Ku, W.C., Chen, S.M.: Weaknesses and improvements of an efficient password based remote user authentication cheme using smart cards. IEEE Transactions on Consumer Electronics 50(1), 204207 (2004)

[4] A. K. Awasthi and S. Lal, A remote user authentication scheme using smart cards with forward security," IEEE Transactions on Consumer Electronics,vol. 49(4), pp. 1246-1248, 2003.

[5] Wu, T.C., Remote login authentication scheme based on a geometric approach, Computer communication, Vol. 18(12), pp.1995.

[6] M. S.Hwang , Cryptanalysis of a remote login authentication scheme, Computer communication, Vol. 22(), pp. 742-744, 1999.

[7] H. Y.Chein, A modified login authentication scheme based on a geometric approach, Journal of system and software vol. 55(3) pp. 287-290

[8] H.T. Liaw and C.L. Lei, An efficient password authentication scheme based on a unit circle , Cryptologia, Vol.19(2) pp.198-208,1995.

[9] Shiuh-Jeng Wang Yet Another Log-in Authentication Using N-dimensional Construction Based on Circle Property, IEEE Transactions on Consumer Electronics, Vol. 49(2), pp. 337-341, 2003.

[10] Shuhong Wang, Feng Bao and Jie Wang Comments on Yet Another Log-in Authentication Using N-dimensional Construction, IEEE Transactions on Consumer Electronics, Vol. 50(2), MAY 2004.

[11] M.L. Das, A Saxena, V.P. Gulati, A dynamic ID based remote user authentication scheme. IEEE trans. On computer electronics, vol. 50(2), pp. 629-631, 2004.

[12] Y.Y Wang,J.Y Liu, F.X.Xiao, and J.Dan., A more efficient and secure dynamic ID based remote user authentication scheme. Computer communication, Vol. 32(), pp. 583-585, 2009.

[13] F.Wen., X. Li, An improved dynamic ID-based remote user authentication with key agreement scheme, Computers and Electrical Engineering, vol. 38, no. 2, pp. 381387, 2012.

[14] Juan Qu , Li-min Zou, An Improved Dynamic ID-Based Remote User Authentication with Key Agreement Scheme, Journal of Electrical and Computer Engineering Volume 2013 (2013), Article ID 786587, 2013.

[15] Y. P. Liao, S. S. Wang , A secure dynamic ID based remote user authentication scheme for multi-server environment. Computer Standards and Interfaces Vol.31, pp. 24-29, 2009.

[16] T. Y. Chen, M. S. Hwang, C. C. Lee, and, J. K. Jan. Cryptanalysis of a secure dynamic ID based remote user authentication scheme for multi-server environment. In Proceedings of the 4th International Conference on Innovative Computing, Information and Control. 2009.

[17] C. Hsiang, W. K. Shih Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment. Computer Standards and Interfaces Vol., pp. 1118-1123. 2009.

[18] S. K. Sood, , A. K. Sarje, K. Singh, A secure dynamic identity based authentication protocol for multi-server architecture. Journal of Network and Computer Applications Vol.34, pp. 609-618, 2011.