ISSN : 2350-0743

www.ijramr.com

International Journal of Recent Advances in Multidisciplinary Research
Vol. 04, Issue 04, pp.2509-2511, April, 2017

RESEARCH ARTICLE

A NOVEL REMOTE USER AUTHENTICATION SCHEME USING EUCLIDEAN GEOMETRY WITH SMART CARD FOR WIRELESS NETWORKS PRESERVING USER'S ANONYMITY

***Omar M. Barukab**

Faculty of Computing and Information Systems, P.O.Box 344, Rabigh 21911, Saudi Arabia

ARTICLE INFO

Article History:
Received 24th January, 2017
Received in revised form
18th February, 2017
Accepted 05th March, 2017
Published online 30th April, 2017

Keywords:

Remoter User Authentication,
Smart Card,
Wireless Networks,
Parabola,
Euclidean Plane.

ABSTRACT

Remote user authentication is of concern in wireless communication networks. This paper proposes a novel remote user authentication scheme based on Euclidean geometry in conjunction with smart card. The proposed scheme preserves user's anonymity while withstanding the following security breaches: resistance to forgery attacks, resistance to replay attacks, resistance to password guessing attacks. In addition, a user can choose and change his password freely.

INTRODUCTION

Nowadays, wireless and mobile networks are used extensively in all aspects of our daily life. People around the globe use their hand held devices to access web services (Wen-Tsai Sung, 2016; Erik Aguirre, 2017; Ibrahim Mat, 2015; Sudip Misra and Sumit GosWami, 2017; Jianming and Jianfengm 2004). Quatative analysis of computer systems security can be found in (Rushdi and Ba-Rukab, 2005). This raises an issue of security and privacy of users while accessing such remote services. This paper proposes a novel remoter user authentication scheme based on using the properties of Euclidean geometry in conjunction with smart card for authenticating remote users in wireless network. In 1995, Wu in (Tzong-Chen Wu, 1995), proposed a remote login authentication protocol based on using geometric approach. Security breaches in this protocol were analyzed in (Min-Shiang Hwang, 1999) and (Hung-Yu Chien, Jinn-Ke Jan and Yuh-Min Tseng. 2001). Se breaches were related to both replay and off-line password guessing type of attacks. A proposed scheme was suggested in (Ming-Chen and Jeng-Farn, 2011), (Chin-Chen Chang and Iuon-Chang Lin. 2005) and (Wei-Chi Ku *et al.,* 2005). To remedy this problem. This paper presents a novel remoter user authentication scheme base on using Euclidean geometric properties in conjunction with using smart card. The proposed scheme possesses the following properties: Resistance to forgery attacks, resistance to replay attacks, resistance to off-line password guessing attacks. In addition, the scheme offers the user to choose and change his password freely. In addition, the proposed scheme maintains user ID's anonymity. The paper is organized as follows: in section 2, the proposed scheme is presented. Security analysis of the proposed scheme is the subject of section 3. Conclusion of the paper and future work is presented in section 4.

****Corresponding author: Omar M. Barukab***
Faculty of Computing and Information Systems, P.O.Box 344, Rabigh 21911, Saudi Arabia.

***Keywords*:** Symmetric encryption, Euclidean geometry, authentication, timestamp, smart card, one-way hash function, prime number.

The New Authentication Scheme

First, as a starting point, some necessary notations need to be defined. Table 1 presents the notations used in describing the proposed scheme as follows:

Before a user register in the system, CA chooses the triplet: P, $f(.)$, and two secret Cartesian points: $(x_0, y_0) and\ (x_1, y_1)$

Registration Phase

In this phase the user U_i chooses a password PW_i , then he computes $f(PW_i)$. Next, he presents it to the certificate authority CA.

Upon receiving $f(PW_i)$ by CA it will execute the following set of tasks as follows:

Step-1: CA will choose a number N.
Step-2: CA chooses identity ID_i for the intended user U_i and calculates a value n as follows:

Table 1. Notations used in this Scheme..

T_A	Timestamp generated by entity A.
P	A large prime number.
PW_i	Psssword of user U_i
$f(.)$	A one-way hash function.
$\Rightarrow$	Sending information through secure channel.
ID_i	Identity of a user U_i.
CA	Certificante authority.
$\oplus$	Logical XOR operation.
$\|\|$	Concatination operation.

$$n = f(N \,||\, ID_{CA}) \oplus f(N \,||\, ID_i) \oplus ID_{CA} \oplus ID_i \oplus x_0 \oplus y_0.$$

Step-3: Defines the three points $A = (0, f(PW_i))$, $B = (f(ID_i \,.x_0), f(ID_i \,.y_0))$, $C = (f(ID_i \,.x_1), f(ID_i \,.y_1))$.
Step-4: Constructs the parabola $y = a_i\,(x - h_i)^2 + k_i$ which passes through the three points $A.B$ and C respectively.
Step5-: Stores the following parameters $\{ID_i, f, P, a_i, h_i, k_i\}$ in the smart card for the user U_i and deliver the card securely to the intended user U_i such that:

$CA\,(sends)$: $smart\ card \leftarrow \{ID_i, f, P, a_i, h_i, k_i\} \Rightarrow U_i$
the above line means that the CA entity will load the tuple $\{ID_i, f, P, a_i, h_i, k_i\}$ in the smart card and then will send it through a secure channel to the user U_i.

Login Phase

The user U_i starts by keying his password PW_i into the terminal. Next, the smart card will execute the following steps as follows:

Step-1: Get the current timestamp T_1.
Step-2: Computes $A = (0, f(PW_i))$.
Step-3: Constructs a straight line L_i joining point A and the focus of the parabola which is $F = (h_i, k_i + \frac{1}{4a_i})$.
Step-4: Computes the point D of the intersection of the line L_i and the parabola.
Step-5: Computes a new point $A_1 = \big(0, f(PW_i) + f(T_1)\big)$ on the $y - axis$.
Step-6: Constructs the line L_1 between the two points A_1 and D.
Step-7: Gets a new point E as a result of the intersection of the parabola and the line L_1.
Step-8: Finally, the smart card presents the following login request message to the system as follows:

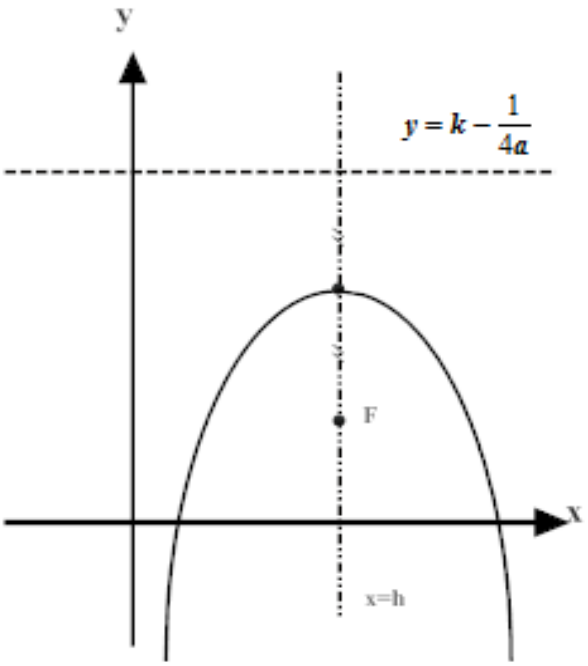
$$m = f(n||ID_i) \oplus f(E) \oplus T_1.$$

Authentication Phase

Upon receiving the login request from the smart card, CA will execute the following steps as follows:

Step-1: Validates both the user ID_i and the received time stamp T_1. If the time stamp is within a valid time frame, the system will accept the login request, otherwise it will reject it.
Step-2: Get the value of E by computing the following: $= m \oplus f(n||ID_i) \oplus T_1)$, then it will Constructs a new parabola using the vertex $V = (h_i, k_i)$ and passing through the newly obtained point E in this step.
Step-3: Computes the intersection point $A_{new} = (0, g)$ of the new constructed parabola with the $y - axis$.
Step-4: Checks g is equals $f(PW_i)$. If so, it will proceed and assume that the user U_i is a bona fide one, otherwise it will reject the authentication request and report a failure.

Figure 1 below shows a schematic for the proposed scheme, while Fig. 2 shows the detailed steps followed in this scheme including: registration, login and authentication phases.



$Parabola: Standard Form$
$vertical: y = a(x-h)^2 + k,$
$Axis\ of\ Symmetry: x = h,$
$Focus: F \equiv (h, k + \frac{1}{4a}),$
$directrix: y = k - \frac{1}{4a},$
$vertix: v \equiv (h, k).$

Fig. 1. Characteristics of the parabola

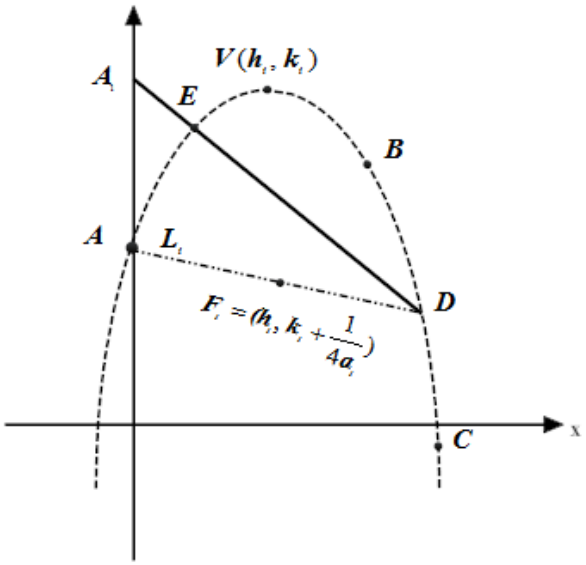


Fig. 2. Schematic of the proposed authentication scheme

Security analysis of the proposed scheme and future work

To address the security analysis of the proposed scheme, we begin with the fact that the proposed new scheme is characterized by the fact that it preserves the user's identity anonymous. This is due to the fact that the user's identity is embedded in the calculations of the *n* value at the second step of the registration phase. In addition, the user's identity cannot be captures or inferred even during the transit of data in the login phase. If the request message *m* is eavesdropped somehow at the eighth step of the login phase, it will not be possible to reveal any useful information to the adversary even by tracking a history of some *m* messages. Moreover, the *m* message keeps changing due to the new value of the time stamp *T*. The new authentication scheme allows the user to change his password at any the login phase any time when he need to do that. This scheme is resistance to replay attack even when the intruder managed to intercept the login message request and tracing its signature in the past. There is a high value of entropy for the attacker not gaining anything useful from such message on transient. The scheme is also resistant to forgery attack due to the fact that the attacker will not be able to reconstruct the parabola and any of the necessary lines that interest with it to obtain the password in any way. Finally, the scheme is resistant to password guessing attack. This is due to the fact that the attacker cannot gain any useful information during any phase of the authentication phases of the proposed scheme. Even in case the attacker in possession of the message *m* while in transient, he cannot gain any useful information from it even by keeping track of this message during a specific duration of time intervals. Future work will incorporate the usage of fault-tree analysis technique [Rushdi, 2005] and Petri nets [Simon Admeit, 2010] due to its concurrency to analyze such wireless authentication schemes.

Conclusion and future work: In this paper, a novel remote user authentication scheme is proposed. It uses the smart card. It is based on using Euclidean plane to reconstruct the user password. It preserves user's identity anonymous. The user can freely choose his password during the registration phase of the protocol. The scheme is resistance to replay attack, forgery attack and password guessing attack.

Acknowledgment

This work was supported by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah Saudi Arabia. The author, therefore, gratefully acknowledge the DSR technical and financial support.

REFERENCES

Chin-Chen Chang and Iuon-Chang Lin. 2005. "Cryptanalysis of The Modified Remote Login Authentication Scheme Based on a Geometric Approach". Informatica. 16(1), pp. 37-44.

Erik Aguirre et al. 2017. Design and Implementation of Context Aware Applications With Wireless Sensor Network Support in Urban Train Transportation Environments. IEEE Sensors Journal. 17(1), pp. 169-178.

Hung-Yu Chien, Jinn-Ke Jan and Yuh-Min Tseng. 2001.A modified remote login authentication scheme based on geometric approach. *Journal of Systems and Software*. 55(3), pp. 287-290.

Ibrahim Mat et al. 2015. Precision agriculture applications using wireless moisture sensor network. IEEE 12th Malaysia International Conference on Communications (MICC), pp. 18-23.

Jianming, Z. and Jianfeng M. 2004. A New Authentication Scheme with Anonymity for Wireless Environments. IEEE Trans. Consum. Electron. 50(1): 231-235. Ming-Chen, C. and Jeng-Farn, L. 2011. An Anonymous Remote User Authentication Scheme Based on a Geometric Approach for Wireless Network.

Min-Shiang Hwang. 1999. Cryptanalysis of a Remote Login Authentication Scheme. Computer Communications. 22(8), 742-744.

Rushdi, A. M., Ba-Rukab, O. M. 2005. Fault-tree modeling of computer system security. International Journal of Computer Mathematics, 82(7), 805-819.

Sudip Misra and Sumit GosWami. 2017. Network Routing: Fundamentals, Applications, and Emerging Technologies. Wiley.

Tzong-Chen Wu. 1995. Remote login authentication scheme based on a geometric approach. Computer Communications. 18(12), pp. 959-963.

Wei-Chi Ku et al. 2005. Weakness and Simple Improvement of a Password Authentication Scheme Based on Geometric Approach", *IEEE Conference on Local Computer Networks (LCN)*. pp. 472-473, 2005.

Wen-Tsai Sung et al. 2016. Application of wireless sensor network for monitoring system based on IOT. IEEE International Conference on Systems, Man, and Cybernetics (SMC). Pp. 613-617.

****