National Journal of Multidisciplinary Research and Development
ISSN: 2455-9040
Impact Factor: RJIF 5.22
www.nationaljournals.com
Volume 3; Issue 1; January 2018; Page No. 458-462

User anonymity based trusted authentication scheme for wireless environment

Sahil Khatri, Himanshu Saxena, Ravi Singh Pippal
Assistant Professor, Department of CSE, MITRC, Alwar, Rajasthan, India

Abstract
In recent years, wireless technology has gained popularity due to its cost effectiveness when compared to wired network. On the other hand, it is open to security attacks because of its transmission media. Out of various security issues related to wireless network, authentication is the primary one. To accomplish this, password based smart card authentication scheme is the most prominent scheme. However, most of these schemes are vulnerable to one or the other possible attacks. This paper presents an efficient and secure smart card authentication scheme based on difficulty in solving Elliptic Curve Discrete logarithm Problem (ECDLP). It allows users to choose and change the password without taking any assistance from the Home Agent (HA). Security analysis proves that the proposed scheme is more secure and practical.

Keywords: authentication, ECDLP, roaming, smart cards, user anonymity, wireless networks

1. Introduction

These days, wireless networks have been widely deployed and used due to their convenience, usability and flexibility. GLOBAL mobility network (GLOMONET) provides global roaming service to permit a mobile user MU to get access to the internet when roams into a network other than his/her home network i.e. foreign network. So, the foreign agent FA needs to authenticate the MU under the assistance of his/her home agent HA in the home network. In conventional wired networks, anonymity and location of mobile user are not considered as the mobile users are fixed users. But, it is very important in case of wireless networks. User anonymity is necessary to prevent unauthorized entities from tracking the mobile user's movement. Hence, a secure authentication scheme is needed to provide both the authentication and the confidentiality at the time of roaming. In the past, various fascinating user authentication schemes have been proposed for wireless communication. But the most promising among them is smart card based password authentication scheme [1-3, 6, 8-9]. In this context, Chang and Wu [10] first proposed password based smart card authentication scheme without verification table. Subsequently, authentication based on smart card has been employed continuously in several applications [11-16].

In view of the fact, all the existing schemes have their pros and cons. This paper proposes a new smart card authentication scheme for wireless communication to resist all the identified attacks and satisfies the desires of a user. Its security depends on hardness of solving the elliptic curve discrete logarithm problem (ECDLP).

Rest of the paper is organized as follows. The proposed smart card authentication scheme is described in section 2. Section 3 demonstrates security analysis of the proposed scheme. A functionality comparison of proposed scheme with the other related schemes is presented in section 4 and finally, section 5 concludes the paper.

2. Proposed Smart Card Authentication Scheme for Wireless Communication

This section describes the proposed smart card authentication scheme for wireless communication. The notations used throughout this paper are summarized as follows.

MU	Mobile user
HA	Home agent of MU
FA	Foreign agent of MU roamed
ID_i	Identity of MU
PW_i	Password chosen by MU
ID_h	Identity of HA
ID_f	Identity of FA
X_h / X_f	Public key of HA / FA
x_h / x_f	Private key of HA / FA
q	Large prime, where $q > 2^{160}$
E	Elliptic curve over a finite field F_q
P	Random point on the elliptic curve $E(F_q)$ with a prime order $n > 2^{160}$ and $n \bullet P = 0$
h(•)	Secure one way hash function
$\oplus$	Bitwise XOR operation
$E_K[\bullet]$ / $D_K[\bullet]$	Symmetric Encryption/Decryption function with key 'K'
SK	Common session key
$\Longrightarrow$	Secure channel
$\longrightarrow$	Insecure channel

The scheme consists of four phases: Initialization phase, Registration phase, Login and Authentication phase and Password Change phase.

2.1 Initialization phase

Three entities are involved in the proposed scheme: the mobile user (MU), the home agent (HA) and the foreign agent (FA). The HA selects a private key x_h and computes its public key $X_h = x_h \bullet P$. Also, the FA selects a private key x_f and computes its public key $X_f = x_f \bullet P$.

2.2 Registration phase

This phase is invoked when a new mobile user MU wants to register with its home agent HA. Fig. 1 shows the registration phase of the proposed scheme and the registration steps work as follows.

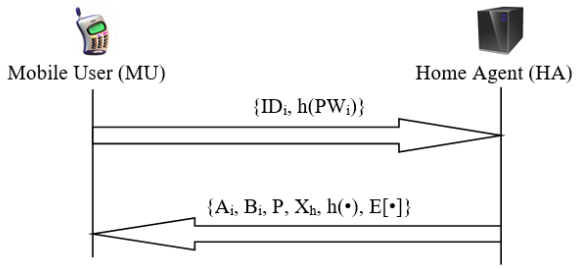

Fig 1: Registration phase

MU ⟹ **HA:** {ID_i, $h(PW_i)$}

Step 1: MU chooses an easy to remember ID_i and PW_i. MU computes $h(PW_i)$ and sends {ID_i, $h(PW_i)$} to home agent HA over a secure channel for registration.

HA ⟹ **MU:** Smart card

Step 2: After receiving the registration request {ID_i, $h(PW_i)$} from MU, HA checks whether the MU's ID_i is already in the database or not. If it holds, HA notifies MU to choose another ID_i. Otherwise, HA computes $A_i = (x_h \bullet ID_i) \bullet P$, $B_i = h(A_i, ID_i, h(PW_i))$ and issues a smart card to MU over a secure channel by storing {A_i, B_i, P, X_h, h(•), E[•]} into smart card memory.

2.3 Login and Authentication phase

MU inserts the smart card into the card reader and inputs credentials ID_i' and PW_i'. The card reader computes $B_i' = h(A_i, ID_i', h(PW_i'))$ and checks whether the computed B_i' equals the stored B_i or not. If it holds, MU is a legitimate bearer of smart card. Two Conditions arises in this scenario. Let us discuss both of these one by one.

2.3.1 When MU is in home network

Fig. 2 shows the login and authentication phase of the proposed scheme when MU is in home network and the steps work as follows.

MU ⟶ **HA:** {C_1, $TOKEN_1$}

Step 1: MU selects a random number $r_1 \in Z^*_q$ and computes $C_1 = r_1 \bullet P$, $K_1 = r_1 \bullet X_h$, anonymous identity $AID_i = K_1 \oplus ID_i$, $TOKEN_1 = E_{K1}[ID_h, AID_i, C_1, A_i]$. Then, MU sends the login request {C_1, $TOKEN_1$} to HA.

HA ⟶ **MU:** {$TOKEN_2$}

Step 2: Once the login request {C_1, $TOKEN_1$} has been received, HA computes $K_1 = x_h \bullet C_1 = x_h \bullet r_1 \bullet P = r_1 \bullet X_h$ and $D_{K1}[TOKEN_1] = (ID_h, AID_i, C_1, A_i)$. HA checks ID_h and compares both the computed C_1 and the received C_1. If it holds, HA gets anonymous identity AID_i and computes MU's identity $ID_i = AID_i \oplus K_1$. If ID_i does not exist in HA's database, the HA terminates the session. Otherwise, HA computes $A_i' = (x_h \bullet ID_i) \bullet P$ and checks whether A_i' equals A_i or not. If true, MU is a legitimate user, otherwise rejects the login request. HA generates a nonce $Nonce_i$, computes $TOKEN_2 = E_{Ai}[K_1, A_i, Nonce_i]$ and sends the response message {$TOKEN_2$} to MU.

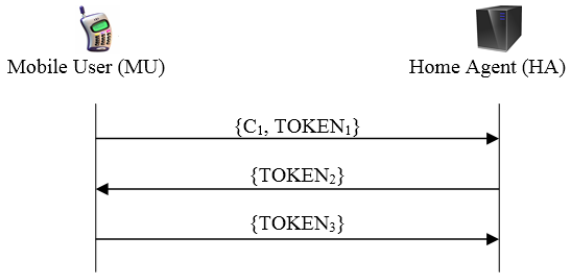

Fig 2: Login and Authentication phase when MU is in home network

MU ⟶ **HA:** {$TOKEN_3$}

Step 3: After receiving the response message {$TOKEN_2$}, MU computes $D_{Ai}[TOKEN_2] = (K_1, A_i, Nonce_i)$ and checks K_1, A_i. If it holds, HA is authentic, otherwise terminate the session. MU computes the common session key $SK = h(K_1, Nonce_i)$, $TOKEN_3 = E_{SK}[Nonce_i + 1]$ and sends {$TOKEN_3$} to HA.

HA

Step 4: Once received, HA computes session key $SK = h(K_1, Nonce_i)$, $D_{SK}[TOKEN_3] = (Nonce_i + 1)$ and checks it. If the decrypted value equals $Nonce_i + 1$, the request is a fresh request and not a replayed message. Now, both MU and HA agreed upon the session key $SK = h(K_1, Nonce_i)$.

2.3.2 When MU is in foreign network

This phase is invoked when MU moves to foreign network. Fig. 3 shows the login and authentication phase of the proposed scheme when MU moves to foreign network and the steps work as follows.

MU ⟶ **FA:** {ID_h, C_1, $TOKEN_1$}

Step 1: MU selects a random number $r_1 \in Z^*_q$ and computes $C_1 = r_1 \bullet P$, $K_1 = r_1 \bullet X_h$, anonymous identity $AID_i = K_1 \oplus ID_i$, $TOKEN_1 = E_{K1}[ID_f, ID_h, AID_i, C_1, A_i]$. Then, MU sends the login request {ID_h, C_1, $TOKEN_1$} to FA.

FA ⟶ **HA:** {ID_f, C_2, $TOKEN_2$}

Step 2: After receiving, FA selects a random number $r_2 \in Z^*_q$, computes $C_2 = ID_f \bullet r_2 \bullet P$, $K_2 = ID_f \bullet r_2 \bullet X_h$, $TOKEN_2 = E_{K2}[ID_h, C_1, TOKEN_1, ID_f, C_2]$ and sends the login request {ID_f, C_2, $TOKEN_2$} to HA.

HA ⟶ **FA:** {C_3, $TOKEN_4$}

Step 3: Upon receiving the message {ID_f, C_2, $TOKEN_2$}, HA computes $K_2 = ID_f \bullet x_h \bullet C_2 = ID_f \bullet x_h \bullet r_2 \bullet P = ID_f \bullet r_2 \bullet X_h$, $D_{K2}[TOKEN_2] = (ID_h, C_1, TOKEN_1, ID_f, C_2)$ and checks whether the decrypted value contains (ID_h, ID_f, C_2) or not. If it holds, HA computes $K_1 = x_h \bullet C_1 = x_h \bullet r_1 \bullet P = r_1 \bullet X_h$, $D_{K1}[TOKEN_1] = (ID_f, ID_h, AID_i, C_1, A_i)$, $ID_i = AID_i \oplus K_1$. If ID_i does not exist in HA's database, the HA notifies FA that MU is not a legal user. Otherwise, HA computes $A_i' = (x_h \bullet ID_i) \bullet P$ and checks whether the computed A_i' equals the

decrypted A_i or not. If true, HA confirms that MU is a legitimate user. HA selects a random number $r_3 \in Z^*_q$, computes $C_3 = r_3 \bullet P$, $K_3 = r_3 \bullet X_f$, $TOKEN_3 = E_{Ai}[K_1, K_2, K_3]$, $TOKEN_4 = E_{K3}[ID_i, K_1, K_2, K_3, TOKEN_3]$ and sends the response message $\{C_3, TOKEN_4\}$ to FA.

FA ⟶ MU: $\{TOKEN_3, TOKEN_5\}$

Step 4: Once the response message $\{C_3, TOKEN_4\}$ has been received from HA, FA computes $K_3 = x_f \bullet C_3 = x_f \bullet r_3 \bullet P = r_3 \bullet X_f$, $D_{K3}[TOKEN_4] = (ID_i, K_1, K_2, K_3, TOKEN_3)$ and checks whether the decrypted value contains K_2, K_3 or not. If true, FA generates a nonce $Nonce_i$, computes $TOKEN_5 = E_{K1}[Nonce_i, K_1]$ and sends the response message $\{TOKEN_3, TOKEN_5\}$ to MU.

MU ⟶ FA: $\{TOKEN_6\}$

Step 5: After receiving the response message $\{TOKEN_3, TOKEN_5\}$, MU computes $D_{Ai}[TOKEN_3] = (K_1, K_2, K_3)$ and checks whether the decrypted value contains K_1 or not. If it holds, computes the common session key $SK = h(K_1, K_2, K_3)$, $TOKEN_6 = E_{SK}[Nonce_i + 1]$ and sends $\{TOKEN_6\}$ to FA.

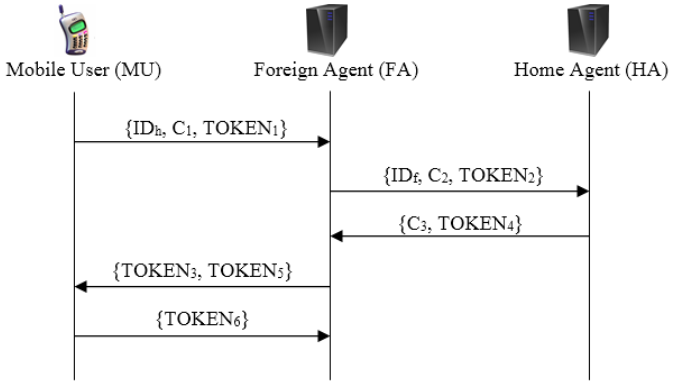

Fig 3: Login and Authentication phase when MU is in foreign network

FA

Step 6: Once received, FA computes session key $SK = h(K_1, K_2, K_3)$, $D_{SK}[TOKEN_6] = (Nonce_i + 1)$ and checks whether the decrypted value equals $Nonce_i + 1$ or not. If it is true, the request is a fresh request and not a replayed message. Now, both MU and FA agreed upon the session key $SK = h(K_1, K_2, K_3) = (r_1 \bullet X_h, ID_f \bullet r_2 \bullet X_h, r_3 \bullet X_f)$.

2.4 Password Change phase

Step 1: This phase is invoked whenever MU requests to change the password.In case of password lost or forgotten, MU inserts the smart card into the card reader and inputs his or her credentials ID_i' and PW_i'. The card reader computes $B_i' = h(A_i, ID_i', h(PW_i'))$ and checks whether the computed B_i' equals the stored B_i or not. If it holds, MU is a legitimate bearer of smart card.

Step 2: Now, MU is requested to input a new password. MU inputs new password PW_{inew}, computes $B_{inew} = h(A_i, ID_i, h(PW_{inew}))$ and replaces B_i with B_{inew} in smart card memory.

3. Security Analysis

This section provides an in-depth analysis of the proposed scheme in terms of security and functionality properties. The security terms needed to conduct an analysis of the proposed scheme are as follows:

Definition 1: The Elliptic Curve Discrete Logarithm Problem (ECDLP) is defined as follows: Let E be an elliptic curve over a finite field F_q and let $P \in E(F_q)$ be a point of order n. Given a public key point $Q = \alpha \bullet P$, it is hard to compute secret key α.

Definition 2: A secure one-way hash function $y = h(x)$ is one where given x to compute y is easy and given y to compute x is difficult.

Definition 3: A secure encryption / decryption function $E_K[\bullet]$ /$D_K[\bullet]$ is one where it is computationally infeasible to break it without the knowledge of secret key 'K'.

Considering the above mentioned definitions, the following propositions are used to analyze the proposed scheme.

Proposition 1: The proposed scheme is able to provide user anonymity.

Proof 1: In the login and authentication phase, MU sends encrypted anonymous identity AID_i by using K_1 as the encryption key. This anonymous identity differs among sessions as $AID_i = K_1 \oplus ID_i$ and $K_1 = r_1 \bullet X_h$. As per the definition 3, it is hard to derive ID_i without knowing K_1 or r_1.

Proposition 2: The proposed scheme is secure against impersonation attack.

Proof 2: This scheme makes it impossible for an attacker to masquerade as a legal mobile user MU. To successfully perform an impersonation attack, the attacker requires A_i which is securely stored in smart card memory. Moreover, there is no way to get A_i from intercepted $TOKEN_1$ without any knowledge of K_1 (as per definition 3). Consider the scenario where an attacker selects a random number r_a, computes $C_a = r_a \bullet P$, $K_a = r_a \bullet X_h$, anonymous identity $AID_a = K_a \oplus ID_i$, $TOKEN_a = E_{Ka}[ID_f, ID_h, AID_a, C_a, A_a]$ and sends the forged login request $\{ID_h, C_1, TOKEN_a\}$ to FA. After receiving, HA can easily identify that the requested MU is not a legitimate user by comparing computed A_i with the decrypted value of A_a. Therefore, the proposed scheme resists impersonation attack.

Proposition 3: The proposed scheme is secure against replay attack.

Proof 3: In this scheme, the replay attack will fail because the freshness of the communicated messages is provided by the random numbers r_1, r_2, r_3. Suppose, an attacker replays the login request $\{ID_h, C_1, TOKEN_1\}$ to FA. Attacker cannot decrypt the response message $\{TOKEN_3, TOKEN_5\}$ coming from FA used to compute the session key $SK = h(K_1, K_2, K_3)$. FA can easily detect this attack by decrypting $TOKEN_6$. Similarly, if attacker replays the message $\{ID_f, C_2, TOKEN_2\}$ to HA, he /she fails to decrypt the response message $\{C_3, TOKEN_4\}$ coming from HA to further prepare the message $\{TOKEN_3, TOKEN_5\}$. Hence, the proposed scheme is free from replay attack.

Proposition 4: The proposed scheme provides perfect forward and backward secrecy.
Proof 4: The proposed scheme generates shared session key $SK = h(K_1, K_2, K_3) = (r_1 \bullet X_h, ID_f \bullet r_2 \bullet X_h, r_3 \bullet X_f)$ which is different for every session. As per the definition 2, it is hard to get (K_1, K_2, K_3) from a revealed SK. Moreover, the values (K_1, K_2, K_3) are protected by ECDLP (Definition 1). Since, there is no relation between past, present or future session keys, the proposed scheme is able to provide both perfect forward and backward secrecy.

Proposition 5: The proposed scheme is secure against online and offline password guessing attacks.

Proof 5: In the proposed scheme, the password of MU (PW_i) is not used in calculation of any of the communicated message parameters. Therefore, the scheme is secure against both of these guessing attacks.

Proposition 6: The proposed scheme provides early wrong password detection.
Proof 6: In most of the existing schemes, attacker can create invalid login request by entering wrong password which will be detected only at the HA. It leads to Denial-of-Service attack. Therefore, it is necessary to verify the legitimacy of the card bearer by checking the correctness of its credentials. This scheme provides the facility to check wrong password at the MU side by comparing B_i' with the stored B_i.

Proposition 7: The proposed scheme is secure against insider attack.
Proof 7: Secure transmission of password is desirable at the time of registration. During the registration phase, MU sends $h(PW_i)$ instead of PW_i to HA. As per the definition (2), any insider of HA cannot directly obtain PW_i and use it to impersonate MU to access any FA. Hence, the proposed scheme resists insider attack.

Proposition 8: The proposed scheme solves time synchronization problem.
Proof 8: In timestamp based authentication schemes, the clock of home agents and foreign agents need to be synchronized. However, it is hard to synchronize the clock when each entity is located in different time zones. To overcome this problem, the proposed scheme uses random numbers r_1, r_2, r_3 and $Nonce_i$. Therefore, the scheme is free from time synchronization problem.

Proposition 9: The proposed scheme provides freedom to choose and change the password securely.
Proof 9: A mobile user finds difficulty to remember the password if it is issued by the HA. Hence, scheme need to allow the users to choose their password freely at any time. In addition, if, due to an accident, the password is revealed then user has the facility to change password securely without any interaction with HA. The proposed scheme is user friendly as it offers both of these services so that there is no need to remember system generated password.

4. Functionality Comparison of Proposed Scheme with other schemes

In this section, the functionality of the proposed scheme is compared with the other related schemes [3, 8, 9] as shown in Table 1. Keeping all the previous advantages, the proposed scheme uses nonce instead of timestamp to avoid replay attack. Offline card holder verification is very essential to avoid unnecessary burden on the server. The scheme verifies the legitimacy of card holder at the time of login. As far as efficiency is concerned, the given scheme uses ECC instead of other intense computational public key cryptosystems which makes it efficient. It can be clearly seen from Table 1 that the proposed scheme achieves all the security and functionality requirements. It is clear that these existing schemes fail to satisfy the needs of a user and need not to consider for practical purposes.

Table 1: Functionality comparison between proposed scheme and other related schemes.

Functionality Offered	Proposed Scheme	Li & Lee's Scheme [9]	He *et al.*'s Scheme [8]	Wu *et al.*'s Scheme [3]
No use of password table	✓	✓	✓	✓
Freedom to choose password	✓	✓	✓	✗
Secure change of password	✓	✗	✓	✗
Provide user anonymity	✓	✓	✗	✗
Prevent replay attack	✓	✓	✓	✗
Prevent impersonation attack	✓	✓	✓	✗
Prevent insider attack	✓	✓	✓	✗
Provide early wrong password detection	✓	✗	✓	✗
Avoid time synchronization problem	✓	✗	✗	✗
Secure session key establishment	✓	✓	✗	✗
Fairness in key agreement	✓	✓	✗	✗

5. Conclusion

In this paper, an ECDLP based smart card authentication scheme for wireless communication is proposed and it is proved that the scheme withstands impersonation attack, online and offline password guessing attacks, replay attack, insider attack and solves time synchronization problem. Further, the proposed scheme allows users to choose and change the password freely, provides mutual authentication, early wrong password detection, perfect forward secrecy and perfect backward secrecy. It is shown that the given authentication scheme not only solves all of the earlier security pitfalls but also increases the efficiency by using ECDLP.

6. References

1. Zhu J, Ma J. A new authentication scheme with anonymity for wireless environments, IEEE Transactions on Consumer Electronics. 2004; 50(1):231-235.
2. Lee CC, Hwang MS, Liao IE. Security enhancement on a new authentication scheme with anonymity for wireless environments, IEEE Transactions on Consumer Electronics. 2006; 53(5):1683-1687.
3. Wu CC, Lee WB, Tsaur WJ. A secure authentication scheme with anonymity for wireless communications, IEEE Communications Letters. 2008; 12(10):722-723.
4. Zeng P, Cao Z, Choo KKR, Wang S. On the anonymity of some authentication schemes for wireless communications, IEEE Communications Letters. 2009; 13(3):170-171.
5. Lee JS, Chang JH, Lee DH. Security flaw of authentication scheme with anonymity for wireless communications, IEEE Communications Letters. 2009; 13(5):292-293.
6. Chang CC, Lee CY, Chiu YC. Enhanced authentication scheme with anonymity for roaming service in global mobility networks, Computer Communications. 2009; 32(4):611-618.
7. Youn TY, Park YH, Lim J. Weaknesses in an anonymous authentication scheme for roaming service in global mobility networks, IEEE Communications Letters. 2009; 13(7):471-473.
8. He D, Ma M, Zhang Y, Chen C, Bu J. A strong user authentication scheme with smart cards for wireless communications, Computer Communications. 2011; 34(3):367-374.
9. Li CT, Lee CC. A novel user authentication and privacy preserving scheme with smart cards for wireless communications, Mathematical and Computer Modelling. 2012; 55(1-2):35-44.
10. Chang CC, Wu TC. Remote password authentication with smart cards. IEE Proceedings E: Computers and Digital Techniques. 1991; 138, pp. 165-168.
11. Pippal RS, Jaidhar CD, Tapaswi S. Enhanced time-bound ticket-based mutual authentication scheme for cloud computing. Informatica. 2013; 37(2):149-156.
12. Hu J, Chen HH. Hou TW. A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. Computer Standards and Interfaces. 2010; 32(5-6):274-280.
13. Pippal RS, Jaidhar CD, Tapaswi S. Secure key exchange scheme for IPTV broadcasting. Informatica. 2012; 36(1):47-52.
14. He D, Ma M, Zhang Y, Chen C, Bu J. A strong user authentication scheme with smart cards for wireless communications. Computer Communications. 2011; 34(3):367-374.
15. Pippal RS, Jaidhar CD, Tapaswi S. Robust smart card authentication scheme for multi-server architecture. Wireless Personal Communications (Springer). 2013; 72(1):729-745.
16. Fan R, He DJ, Pan XZ, Ping LD. An efficient and DoS-resistant user authentication scheme for two-tiered wireless sensor networks. Journal of Zhejiang University-Science C (Computers and Electronics). 2011; 12(7):550-560.