A New Remote Authentication Scheme for Anonymous Users Using ECC

Dianli Guo
School of Mathematical Sciences
University of Jinan
Jinan 250022, China
e-mail: guodianli@163.com

Fengtong Wen
School of Mathematical Sciences
University of Jinan
Jinan 250022, China
e-mail: wftwq@163.com

***Abstract*—In 2011, Khan et al. identified that Wang et al. scheme could not achieve user anonymity and had many practical pitfalls, In addition, Khan et al. presented an enhanced scheme to eliminate the aforementioned defects. In this article, we point out that Khan et al.'s scheme is incapable to provide user anonymity and suffers from forgery attack, off-line password guessing attack. Besides, a new authentication scheme for anonymous users using elliptic curves cryptosystem is presented, which could withstand various types of network attacks and is more suitable for mobile application scenarios where resources constrained and security concerned.**

Keywords- anonymity; authentication; ID-based; ECC

I. INTRODUCTION

It is necessary for service providing servers to authenticate remote users when users access resources through public network; remote authentication is an essential mechanism for them to authenticate each other conveniently. However, a majority of the solutions are susceptible to a range of potential security attacks.

Recently, dozens of anonymous authentication schemes [3, 4, 5, 6, 7, 8] which emphasized the security problems were proposed. However, a majority of them were demonstrated to be insecure for the augmented reality applications.

In 2011, Khan et al. [9] proposed a remote user authentication scheme which was claimed to preserve user anonymity. However, we investigate that it is insecure. Further, user anonymity is neglected by authors. In order to conquer the aforementioned flaws, a new scheme preserving user privacy is presented.

This paper is organized as follows. In section II and section III, we presented the brief review of Khan et al.'s scheme and describe the weaknesses of their scheme, respectively. In section IV, we propose an authentication scheme. The analysis of our proposal and the comparisons with other related schemes are presented in section V. At last, section VI concludes this paper.

II. OVERVIEW OF KHAN ET AL.'S SCHEME

We will present the brief review the scheme of [9] in this section.

A. Registration phase

Step1. U_i chooses ID_i , PW_i and a nonce r . Then U_i computes $RPW = H(r \| PW_i)$ and sends ID_i , RPW to S for registration.

Step2. S checks the registration credential. If the received ID_i is already stored in the database, U_i has to choose another identity. More over, S checks the registration record for U_i . Assume that U_i is a new user, S will set the value $N = 0$; otherwise, S will set $N = 1$ and store ID_i with N in the database.

Step3. S computes $IDU = (ID_i \| N)$, $J = H(x \| IDU)$ and $L = J \oplus RPW$. Then S sends the smart card to U_i containing $\{L, y\}$ where y is the shared secret key.

Step4. U_i stores r into the received smart card.

B. Login phase

Step1. U_i inputs ID_i , PW_i . Then the smart card computes $RPW = H(r \| PW_i)$, $J = L \oplus RPW$, $C_1 = H(T_i \| J)$ and $AID_i = ID_i \oplus H(y \| T_i \| d)$ where d is a nonce and T_i is the fresh timestamp.

Step2. $\{AID_i, T_i, d, C_1\}$ is transmitted to S .

C. Authentication phase

Step1. Upon receiving the login request at T_i' , S checks the time interval by verifying $T_i' - T_i \le \Delta T$. If the verification fails, S terminates this procedure.

Step2. S computes $ID_i = AID_i \oplus H(y \| T_i \| d)$ and verifies its validity. If ID_i is valid, executes step 3; otherwise, S rejects this request.

Step3. S retrieves N from the database with ID_i and computes $IDU = (ID_i \| N)$, $J = H(x \| IDU)$. Then

S checks whether $C_1? = H(T_i \| J)$. If the equality holds, S will accept the login request and U_i is authentic.

Step4. S computes $C_2 = H(C_1 \oplus J \oplus T_s)$, where T_s is the fresh timestamp and then transmits the reply message $\{C_2, T_s\}$ to U_i.

Step5. On receiving the reply message at T_s', U_i verifies the freshness of T_s. If $T_s' - T_s \geq \Delta T$, U_i terminates this operation. Then U_i checks $H(C_1 \oplus J \oplus T_s) \ ? = C_2$. If fails, this session is terminated.

Step6. At the end, U_i and S compute and share the session key $SK = H(C_2 \oplus J)$ for the further communication.

D. Password-change phase

Step1. U_i enters ID_i and PW_i to the smart card and computes $RPW^* = h(r \| PW_i)$ and $J^* = L \ \oplus RPW^*$. If $J^* = J$, U_i inputs a new password PW_i^{new}; otherwise, this procedure is terminated.

Step2: Computes $L^{new} = L \oplus RPW \oplus H(r \| PW_i^{new})$ and stores L^{new} into its memory to replace L.

E. Revocation phase

Smart cards may be lost or stolen, S should allow the cardholder U_i to execute the revocation. S firstly verifies the validity of U_i 's credential as mentioned in the registration phase. After that, S changes N to be $N+1$. Finally, S performs the same steps in the registration phase with another N.

III. CRYPTANALYSIS OF KHAN ET AL.'S SCHEME

We analyze the security of Khan et al.'s scheme and show their scheme is incapable to resist attacks. More over, the feature of user anonymity is not preserved in their scheme.

A. No provision of users anonymity

The user' specific and secret information (e.g., the login history and the current location) may be obtained by a malicious adversary due to the leakage of user's static identity. However, Khan et al.'s scheme [9] cannot achieve user anonymity.

Step1. Any legal but anonymous user U_k can obtain the secret value y from his/her smart card.

Step2. When U_i logins to S, U_k can intercept his/her login request $\{AID_i, T_i, d, C_1\}$. Then U_k can compute $ID_i = AID_i \oplus H(y \| T_i \| d)$.

B. Off-line password guessing attack

Suppose that the smart card of a legal remote user U_i is stolen or picked up by U_k, and the data $\{L, y, r\}$ in the smart card [1,2]. Then U_k can perform the following procedures to get U_i's password PW_i:

Step1. Choose a password PW_i^*.

Step2. Computes $C_1^* = H(T_i \| (L \oplus H(r \| PW_i^*))$ and checks $C_1^* ? = C_1$ to confirm the correctness of PW_i^*.

Step3. Repeats the step 1 and 2 by replacing another guessed password until the correct password is found.

C. Forgery attack

As explained above, with the extracted values $\{L, y, r\}$ [1,2], U_k can get PW_i and ID_i corresponding to U_i. And he/she can further impersonate U_i to deceive S by performing the following steps.

Step1. Computes $RPW = H(r \| PW_i)$, $J = L \ \oplus RPW$, $C_1' = H(T_k \| J)$, $AID_i' = ID_i \oplus H(y \| T_k \| d')$, where T_k is the fresh current time stamp and d' is a nonce generated by U_k, then, sends the forged login request message $\{AID_i', T_k, d', C_1'\}$ to S.

Obviously, S can accept the login request of the adversary, since these parameters of the forged login request message are in the correct format. Thus, the adversary can successfully impersonate as U_i to communicate with S.

IV. OUR PROPOSED SCHEME

We propose an anonymous authentication scheme in this section.

A. Registration phase

Initially, S chooses two distinct large primes p and q with $p = 2q + 1$. $E_p(a,b)$ is an elliptic curve in the finite field Z_p. P is a generator of order q on the elliptic curve $E_p(a,b)$. S computes $Q = x \cdot P \ mod \ p$ where x is the master secret key of S. $\{P, p, Q, E_p(a,b)\}$ are the public parameters.

Step1. U_i selects his/her identity ID_i and password PW_i, then sends them to S over a secure channel.

Step2. Upon receiving the message $\{ID_i, PW_i\}$, S computes $A_i = H(ID_i \| PW_i)$ and $B_i = H(ID_i \cdot y \cdot Q) \oplus H(ID_i \oplus PW_i)$, where y is a nonce chosen by S for every user.

Step3. S issues the smart card stored $\{A_i, B_i, p, E_p(a,b), P, Q, H(\cdot)\}$ to U_i.

B. Login phase

Step1. U_i keys ID_i^*, PW_i^*. The smart card computes $A_i^* = H(ID_i^* \| P_i^*)$ and verifies $A_i^* ?= A_i$. If yes, it means U_i is the cardholder; otherwise, login request is terminated.

Step2. The smart card generates a random nonce d and computes $H(ID_i \cdot y \cdot Q) = B_i \oplus H(ID_i \oplus PW_i)$, $C_i = ID_i \cdot P + d \cdot Q$, $D_i = d \cdot P$, $E_i = H(ID_i \cdot y \cdot Q) \cdot P + d \cdot T_i \cdot Q$, where T_i is the fresh current time stamp.

Step3. After that, U_i sends $\{C_i, D_i, E_i, T_i\}$ to S.

C. Authentication phase

Step1. Upon receiving $\{C_i, D_i, E_i, T_i\}$ at T_i', S verifies the freshness of T_i, if $T_i' - T_i \le \Delta T$ holds, S continues the next step.

Step2. Afterwards, S calculates $ID_i \cdot P = C_i - x \cdot D_i$ and $E_i^* = H(x \cdot y \cdot ID_i \cdot P) \cdot P + x \cdot T_i \cdot D_i$. If the digest value of E_i^* equals to received E_i, proceeds to step 3; else, this session will be terminated.

Step3. S computes $F_i = ID_i \cdot P + r \cdot P$, $G_i = r \cdot ID_i \cdot P + T_s \cdot x \cdot D_i$. Then, S transmits the replied message $\{F_i, G_i, T_s\}$ to U_i.

Step4. The smart card verifies the freshness of T_s. Subsequently, computes $r \cdot P = F_i - ID_i \cdot P$ and checks whether G_i equals to the computed $ID_i \cdot r \cdot P + T_s \cdot d \cdot Q$. If yes, S is authentic and the authentication is completed successfully.

After that, U_i and S agree on the session key $SK = d \cdot r \cdot P$.

C. Password changing phase

Step1. The smart card performs step 1 of the login phase.

Step2. If U_i is the cardholder, U_i inputs a new password PW_i^{new}; on the contrary, the smart card terminates the request of updating the password.

Step3. The smart card calculates $A_i^{new} = H(ID_i \| PW_i^{new})$, $B_i^{new} = B_i \oplus H(ID_i \oplus PW_i) \oplus H(ID_i \oplus PW_i^{new})$ and stores A_i^{new}, B_i^{new} into the smart card to replace A_i, B_i.

V. Security Analysis of Our Scheme

A. Preserving user anonymity

If U_k has intercepted all of U_i's authentication messages $\{C_i, D_i, E_i, F_i, G_i, T_i, T_s\}$. There is no any static value in these parameters based on the randomness of d and r. Accordingly, U_k cannot retrieve $ID_i \cdot P$ from C_i without knowing the random numbers of d and r since the difficulty of the Computation Diffie-Hellman problem.

B. Off-line password guessing attack

Suppose that U_k has gotten smart card of another legitimate user U_i and the value A_i can be revealed from the smart card. After that U_k may try to guess both ID_i and PW_i by computing $A_i = H(ID_i \| PW_i)$, because we have demonstrated that user anonymity confidentiality is achieved in the proposed scheme. It is impossible for the adversary to guess identity and password correctly simultaneously in polynomial time.

C. Forgery attack

U_k should attempts to forge a valid login request $\{C_i, D_i, E_i, T_i\}$. However, U_k cannot compute the C_i and E_i without knowing ID_i and the secret number y generated by S, even if U_k has extracted the secret values $\{A_i, B_i, p, E_p(a,b), P, Q, H(\cdot)\}$ stored in U_i's smart card. Hence, U_k cannot launch the forgery attack to fool the server.

D. Server impersonating attack

In order lunch the server spoofing attack to fool U_i, U_k may attempt to forge a legal reply message $\{F_i, G_i, T_s\}$ after receiving U_i's login request message. However, U_k cannot compute the forged reply message without knowing the master secret key x of the server, even if U_k has extracted the secret data from U_i's smart card. Hence, U_k

cannot masquerade as S to fool U_i and the server spoofing attack is meaningless in the proposed scheme.

E. Comparison

In this section, the security features comparison of Ma et al.'s [8] and Khan et al.'s [9] schemes is presented to evaluating our scheme. We summarize the detailed comparisons in the Table II. As you can see in Table II, our proposal is relatively more secure than the other two schemes.

TABLE I. TABLE TYPE STYLES

	Khan et al.[9]	***Ma et al.*** [8]	***Ours***
User anonymity	No	No	Yes
Prevention of forgery attack	No	No	Yes
Prevention of off-line dictionary attack	No	No	Yes
Prevention of server spoofing attack	Yes	No	Yes
Freely change password	Yes	Yes	Yes
Mutual authentication	Yes	Yes	Yes

VI. CONCLUSION

In this paper, we find out that Khan et al.'s scheme is insecure and incapable to provide user privacy. Also, we proposed a robust anonymous authentication scheme using elliptic curves cryptosystem to conquer the aforementioned weaknesses. Security analysis show that our proposal is relatively more secure than the related schemes in terms of the security.

REFERENCES

[1] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," 19th Annual international cryptology conference, 1999, p. 388-97.

[2] T. S. Messerges, E. A. Dabbish and R. H. Sloan, "Examining smart - card security under the threat of power analysis attacks," IEEE Trans Comput, 2002, 5(51):541-552.

[3] M. L. Das, A. Saxena and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," IEEE Trans on Consumer Electronics, 2004, 50(2):665-667.

[4] Y. F. Chang and P. Y. Chang, "An improved user authentication and key agreement scheme providing user anonymity," Journal of Electronic Science and Technology, 2011, 4(9):352-358.

[5] 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 Communications, 2009, 4(32):583-585.

[6] F. T. Wen and X. L. Li, "An improved dynamic ID-based remote user authentication with key agreement scheme," Computers and Electrical Engineering, 2011, 38(2):381-387.

[7] R. C. Wang, W. S. Juang and C. L. Lei, "Robust authentication and key agreement scheme preserving the privacy of secret key," Computer Communications, 2011, 3(34):274-280.

[8] Y. Ma, G. W. Li and L. M. Zhang, "A Novel Remote Authentication Scheme Based-On Password for Anonymous Users," Information and Business Intelligence, 2012, 187-194.

[9] M. K. Khan, S. K. Kim and K. Alghathbar, "Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme," Computer Communications, 2011, 34(3):305-309.