Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme

Hakhyun Kim, Woongryul Jeon, Yunho Lee and Dongho Won*

***Abstract*—In 2010, Yoon *et al.* proposed a robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. In this letter, however, we show that Yoon *et al.*'s scheme is vulnerable to off-line password guessing attack and propose an improved scheme to prevent the attack.**

***Index Terms*—Authentication, biometrics, cryptanalysis, key agreement.**

I. Introduction

After Lamport proposed a password authentication scheme in 1981 [1], many password-based multi-server authentication schemes have been proposed so far. Among those schemes, Yoon *et al*. proposed a robust multi-server authentication with key agreement scheme for smart cards using biometrics and elliptic curve cryptosystem [2].

In this letter, we briefly review the scheme, show its vulnerability to off-line password guessing attack and improve the scheme to prevent the attack.

II. Review of Yoon et al.'s scheme

This section reviews Yoon *et al*.'s multi-server authentication with key agreement scheme briefly. The scheme is composed of four phases; the server registration phase, the user registration phase, the authenticated key agreement phase, and the password and biometrics update phase. Notations used in this scheme are defined as follows.

- U, S_j : the user and the jth server, respectively.
- RC : the registration center.
- ID, PW, B: U's identity, password and biometric template, respectively.
- SID_j: S_j's identity.
- x: U's secret key maintained by the registration center.
- y: S_j's secret key maintained by the registration center.
- p: large prime number.
- F_p: finite prime field.
- E: non-super singular Elliptic curve over a finite field F_p, where $E : y^2 = (x^3 + ax + b) \bmod p$ with $\alpha, \beta \in F_p$ satisfying $(4a^3 + 27b) \bmod p \neq 0$.
- $E(F_p)$: additive group of points on E over a finite field F_p, where $E(F_p) = \{(x,y) : x, y \in F_p \text{ satisfy } y^2 = x^3 + ax + b\} \cup \{O\}$.
- P: generating element (point) of $E(F_p)$ under consideration F_p.
- α, β: session-independent random integer numbers $\in [1, p\text{-}1]$ chosen by U and S_j, respectively.
- SK: shared fresh session key computed by U and S_j.
- $d(\cdot)$: symmetric parametric function.
- τ: predetermined threshold for biometric verification.
- $h(\cdot)$: secure one-way hash function.
- $\oplus$: bit-wise exclusive-or(XOR) operation.
- $||$: concatenation operation.
- $A \rightarrow B: M$: A sends a message M to B.

A. Server registration phase

The following steps are performed during the server registration phase.

Step 1: $S_j \rightarrow RC: SID_j$

S_j chooses its identity SID_j and transmits it to RC via a secure channel.

Step 2: $RC \rightarrow S_j: h(SID_j||y)$

RC computes $h(SID_j||y)$, where y is the S_j's secret key maintained by RC, and transmits it to S_j via a secure channel.

B. User registration phase

The following steps are performed during the user registration phase.

Step 1: $U \rightarrow RC: \{ID, h(PW||B), B\}$

U selects ID and PW, and imprints her biometric information B at the sensor. Then U submits $\{ID, h(PW||B), B\}$ to RC. These private data must be sent

Manuscript received October 9, 2001. (Write the date on which you submitted your paper for review.) This work was supported in part by the U.S. Department of Commerce under Grant BS123456 (sponsor and financial support acknowledgment goes here). Paper titles should be written in uppercase and lowercase letters, not all uppercase. Avoid writing long formulas with subscripts in the title; short formulas that identify the elements are fine (e.g., "Nd–Fe–B"). Do not write "(Invited)" in the title. Full names of authors are preferred in the author field, but are not required. Put a space between authors' initials.

H. Kim, W. Jeon, Y. Lee, D. Won, are with the Information Security Group, Sungkyunkwan University, Gyeonggi-do 440-746, Korea (e-mail: {hhkim, wrjeon, leeyh, dhwon}@security.re.kr).

* : corresponding author

in a secure channel.

Step 2: $RC \rightarrow U$: {Smart card containing (Z, B, $h(\cdot)$, $d(\cdot)$, τ)}

RC computes the user authentication key R and Z as follows:

- $R = h(ID||x)$
- $Z = R \oplus h(PW||B)$

Then, RC stores $\{Z, B, h(\cdot), d(\cdot), \tau\}$ in a smart card and issues it to U via a secure channel.

C. Authenticated key agreement phase

The following steps are performed during the authenticated key agreement phase.

Step 1: $U \rightarrow S_j$: $\{ID, \alpha P, C_1\}$

U inserts her smart card into a card reader, executes the login application software, and imprints biometric B^* at the sensor. Then a biometric verification process of U's smart card compares the imprinted B^* with the stored B. If $d(B^*,B) < \tau$, then it outputs *accept* message. If $d(B^*,B) \geq \tau$, then it outputs *reject* message which means U does not pass the biometric verification thus the authentication process is terminated. On the contrary, if it outputs *accept*, U enters her password PW, and then the reader extracts R by computing $Z \oplus h(PW||B)$, generates a random number $\alpha \in [1, q\text{-}1]$, and computes $C_1 = h(R||\alpha P) = h(h(ID||x)||\alpha P)$. Then U transmits ID, αP and C_1 to S_j.

Step 2: $S_j \rightarrow RC$: $\{ID, \alpha P, C_1, SID_j, \beta P, C_2\}$

S_j generates a random number $\beta \in [1, q\text{-}1]$ and computes $C_2 = h(h(SID_j||y)||\beta P)$. Then S_j transmits ID, αP, C_1, SID_j, βP and C_2 to RC.

Step 3: $RC \rightarrow S_j$: $\{C_3, C_4\}$

RC computes $C'_1 = h(h(ID||x)||\alpha P)$ and $C'_2 = h(h(SID_j||y)||\beta P)$ and then RC checks whether $C_1 \stackrel{?}{=} C'_1$ and $C_2 \stackrel{?}{=} C'_2$, respectively. If both equations hold, RC computes the follows:

- $V = h(h(SID_j||y)||\beta P||\alpha P)$,
- $W = h(h(ID||x)||SID_j||\alpha P||\beta P)$,
- $C_3 = V \oplus W$, and
- $C_4 = h(V||W)$,

where W is used to the ephemeral secret key between U and S_j. Finally, RC transmits C_3 and C_4 to S_j.

Step 4: $S_j \rightarrow U$: $\{\beta P, C_5\}$

S_j computes $V' = h(h(SID_j||y)||\beta P||\alpha P)$, and extracts the ephemeral secret key W by computing $C_3 \oplus V' = V \oplus W \oplus V' = W$. Then S_j computes $C'_4 = h(V'||W)$ and checks whether $C_4 \stackrel{?}{=} C'_4$. If it holds, S_j computes the shared session key $SK = \beta(\alpha P) = \alpha\beta P$, and $C_5 = h(ID||SID_j||W||SK)$. Finally, S_j transmits βP and C_5 to U.

Step 5: $U \rightarrow S_j$: $\{C_6\}$

U computes the ephemeral secret key W, the shared session key SK and C'_5 as follows:

- $W = h(h(R||SID_j||y)||\alpha P||\beta P)$
- $SK = \beta(\alpha P) = \alpha\beta P$
- $C'_5 = h(ID||SID_j||W||SK)$.

And U checks whether $C_5 \stackrel{?}{=} C'_5$. If it holds, U computes $C_6 = h(W||SK||\beta P)$ and transmits C_6 to S_j.

Step 6: S_j computes $C'_6 = h(W||SK||\beta P)$ and checks whether $C_6 \stackrel{?}{=} C'_6$. If it holds, S_j confirms the validity of U.

D. Password and biometrics update phase

In this phase, U can liberally and securely change the old password PW to a new password PW^{new} and the old biometrics B to a new biometrics B^{new}, respectively, with own ability.

Step 1: $U \rightarrow U$'s smart card: $\{B^*\}$

U inserts smart card into a card reader, executes the password update application software, and imprints biometric B^{new} at the sensor.

Step 2: U's smart card $\rightarrow U$: {Password input request}

U's smart card compares the imprinted B^{new} with the stored B. If $d(B^{new}, B) \geq \tau$, it means U does not pass the biometric verification, thus the password and biometrics update phase is terminated. On the contrary, if $d(B^{new}, B) < \tau$, it means U passes the biometrics verification and then U's smart card sends a password input request message to the user U.

Step 3: $U \rightarrow U$'s smart card: $\{PW, PW^{new}\}$

U enters her old password PW and inputs the new password PW^{new}.

Step 4: U's token computes new $Z^{new} = Z \oplus h(PW||B) \oplus h(PW^{new}, B^{new})$, and then replaces the old Z and B with Z^{new} and B^{new}, respectively, on the smart card.

III. Cryptanalysis of Yoon et al.'s scheme

We have two assumptions about adversary A as follows:

1. Adversary A has ability to intercept any message between U and S_j during the communication, and
2. Adversary A may steal U's smart card and extracts information stored on it.

A. Off-line Password Guessing Attack

Suppose that an adversary A steal U's smart card. In the beginning of authenticated key exchange phase, Adversary A intercepts a message $<ID, \alpha P, C_1>$ sent to S_j by U.

Now A can perform off-line password guessing attack by performing the following steps.

Step 1: A extracts Z, B from smart card.

Step 2: A guesses a random password PW'

Step 3: Using biometric information B, A computes $E = Z \oplus h(PW'||B)$.

Step 4: Using E and intercepted αP, A computes $C' = h(E||\alpha P)$.

Step 5: If $C_1 = C'$, A finds the PW successfully. Otherwise, A starts over with another password.

IV. Improved scheme

An adversary A can launch off-line password guessing attack

because the *U*'s biometric data *B* is stored to the smart card without concealment and can be obtained by *A*. A simple way to prevent this attack is to protect *B* by storing $h(B)$ instead of *B*. However, due to the nature of hash function, it outputs completely different hash values even if the input biometrics are very close to each other. Therefore, we need more sophisticated method to store $h(B)$ instead of *B*, such as [3]. For the improved scheme, *B* should be obtained as follows: Firstly, extract feature vector FV of a user's biometric data. Secondly, apply the one-way transformation(e.g., various Gaussian functions) and quantization to FV. Lastly, concatenate values obtained after quantization yielding *B* (For more details, see [3]). For simplicity, we define a function $h'(\cdot)$ as the combination of the one-way transformation and the secure hash functions.

The improved scheme is described as follows. We will show only the modified steps of User registration and Authenticated key agreement phases, because of its lengthy description.

1. In Step 2 of User registration phase, *RC* computes the user authentication key $R = h(ID||x)$ and $Z = R \oplus h(PW||B)$. Then, *RC* stores the secure information $\{Z, h'(B), h'(\cdot), h(\cdot), d(\cdot), \tau\}$ to the memory of *U*'s smart card and issues it to *U* via a secure channel.
2. In Step 1 of Authenticated key agreement phase, *U* inserts the smart card into a card reader, executes the login application software, and imprints biometric B^* at the sensor. Then smart card compares $h'(B)$ with $h'(B^*)$. If $h'(B) = h'(B^*)$, then it outputs *accept* message. If $h'(B) \neq h'(B^*)$, then it outputs *reject* message. If it outputs *reject*, it means *U* does not pass the biometric verification thus the authentication process is terminated. On the contrary, if it outputs *accept*, *U* enters own password *PW*, and then the reader extracts *R* by computing $Z \oplus h(PW||B^*)$, generates a random integer number $\alpha \in [1, q\text{-}1]$, and computes $C_1 = h(R||\alpha P) = h(h(ID||x)||\alpha P)$. Then *U* sends *ID*, αP and C_1 to S_j.

V. Conclusion

In this letter, we showed that Yoon *et al.*'s scheme is insecure against off-line password guessing attack. We also presented an improved scheme that can withstand such attack.

References

[1] L. Lamport, "Password authentication with insecure communication," Communication of ACM, vol. 24, pp.28-30, 1981.

[2] E.J. Yoon and K.Y. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," Journal of supercomputing, DOI: 10.1007/s11227-010-0512-1, 2010.

[3] Y. Sutcu, T. Sencar, and N. Memon, "A secure biometric authentication scheme based on robust hashing," ACM MMSEC Workshop, pp.111-116, 2005.