Cryptanalysis of an Authenticated Key Agreement Protocol for Wireless Mobile Communications

Debiao He

With the rapid progress of wireless mobile communications, the authenticated key agreement (AKA) protocol has attracted an increasing amount of attention. However, due to the limitations of bandwidth and storage of the mobile devices, most of the existing AKA protocols are not suitable for wireless mobile communications. Recently, Lo and others presented an efficient AKA protocol based on elliptic curve cryptography and included their protocol in 3GPP2 specifications. However, in this letter, we point out that Lo and others' protocol is vulnerable to an offline password guessing attack. To resist the attack, we also propose an efficient countermeasure.

Keywords: Authenticated key agreement, offline password guessing attack, wireless mobile communication, 3GPP2.

I. Introduction

In 2005, Sui and others proposed an improved authenticated key agreement (AKA) protocol [1] for wireless mobile communications. Their scheme provided perfect forward secrecy but was vulnerable to an offline password attack [2]. To enhance the security, Lu and others proposed an enhanced AKA protocol for wireless mobile communications in 2007 [2]. Later, Chang and others [3] pointed out that the Lu and others' scheme cannot resist the parallel guessing attack. Chang and others [3] proposed an improved protocol. However, Lo and others [4] demonstrated that Chang and others' protocol does not offer the mutual authentication property. Lo and others also proposed an improved scheme using elliptic curve cryptography (ECC), included their protocol in 3GPP2 specifications, and claimed their scheme could withstand various attacks. However, in this letter, we will propose an offline password guessing attack against Lo and others' protocol. To withstand the attack, we also propose an efficient countermeasure.

Manuscript received July 31, 2011; revised Nov. 8, 2011; accepted Nov. 30, 2011.

This research was supported by the Fundamental Research Funds for the Central Universities and the Specialized Research Fund for the Doctoral Program of Higher Education of China (No. 20110141120003).

Debiao He (phone: +86 153 0718 4927, hedebiao@whu.edu.cn) is with the School of Mathematics and Statistics, Wuhan University, Wuhan, China

http://dx.doi.org/10.4218/etrij.12.0211.0340

II. Review of Lo and Others' Scheme

For convenience, the abbreviations and notations used in this letter are shown in Table 1.

The detailed steps of Lo and others' protocol are described as follows.

Step 1. Alice (A) picks a random number $d_A \in [1, n-1]$ and computes $Q_A = (d_A + t)P$, where t is an integer that is predetermined by the corresponding password and P is a point in the elliptic curve. Then, A sends its identity A and Q_A to Bob

Table 1. Notations.

A, B	Abbreviation/identity of the participators Alice (client) and Bob (server), individually
E	Elliptic curve defined over a finite field F_q with large group order
n	Secure large prime
P, Q	Two points on E with large order n
D	Uniformly distributed dictionary of size $\mid D \mid$
S	Low-entropy password shared between Alice and Bob, which is randomly chosen from D
t	Integer derived from the password S in a predetermined way
H	Secure one-way hash function

(B).

Step 2. B also chooses a random number $d_B \in [1, n-1]$ and then computes $Q_B = (d_B - t)P$, $Y = Q_A - tP$, $K_B = d_B Y$, and $H_B = H(K_B \| Y)$. Then, B sends the Q_B and H_B to A.

Step 3. A computes $X = Q_B + tP$ and then computes $K_A = d_A X$. Next, A verifies the equality of $H(K_A \| d_A P)$ and H_B. If it does not hold, the protocol is terminated. Otherwise, A sends $H_A = H(K_A \| X)$ to B and sets the session key to K_A.

Step 4. When B receives the message, it checks the equality of $H(K_B \| d_B P)$ and H_A. Only if the equality holds, B agrees on the session key K_B. Otherwise, B terminates the protocol.

III. Weakness in Lo and Others' Protocol

An offline password guessing attack succeeds when there is information in communications that can be used to verify the correctness of the guessed passwords. Lo and others claimed that their protocol can resist offline password guessing attacks. However, in this section, we will show that the offline password guessing attack, contrary to their claim, is still effective in Lo and others' protocol. Our attack consists of two phases.

First phase.

1) The adversary $\mathscr{A}$ generates a random number $d_A \in [1, n-1]$, computes $Q_A = d_A P$, and sends A and Q_A to B.

2) Upon receiving A and Q_A, B also chooses a random number $d_B \in [1, n-1]$ and then computes $Q_B = (d_B - t)P$, $Y = Q_A - tP = (d_A - t)P$, $K_B = d_B Y = d_B(d_A - t)P = d_A d_B P - t d_B P$, and $H_B = H(K_B \| Y)$. Next, B sends the Q_B and H_B to A.

Upon receiving Q_B and H_B, the adversary $\mathscr{A}$ carries out the second phase as follows.

Second phase.

1) The adversary $\mathscr{A}$ guesses a password S' from D and derives the corresponding t'.

2) $\mathscr{A}$ computes $Y' = Q_A - t'P$, $d'_B P = Q_B + t'P$, $d_A d'_B P = d_A(d'_B P)$, $t' d'_B P = t'(d'_B P)$, and $K'_B = d_A d'_B P - t'(d'_B P)$.

3) $\mathscr{A}$ verifies the equality of $H(K'_B \| Y')$ and H_B. If it does hold, the adversary gets the correct password. Otherwise, $\mathscr{A}$ repeats 1), 2), and 3) until finding the correct password.

From the above description, we know the adversary can get the correct password. Therefore, Lo and others' scheme is vulnerable to the offline password guessing attack.

IV. Countermeasure

In Lo and others' scheme, the session key is simply a linear combination of $d_A P$, $d_B P$, and tP. The adversary can deduce the session key upon identifying two out of the three values correlating to d_A, d_B, and t. Then, having guessed what the password might be, the adversary can verify whether or not the guess is correct. To withstand such an attack, we introduce another point, Q on E, to introduce complexity to the relationships in the session key.

First, the system selects a random point Q on E. However, Q is an important parameter and should be chosen carefully to ensure that it is computationally difficult for an adversary to find the discrete logarithm of Q with P as the base. Otherwise, the protocol will be insecure.

Step 1. A picks a random number $d_A \in [1, n-1]$ and computes $Q_A = d_A P + tQ$. Then A sends out its identity A and Q_A to B.

Step 2. B also chooses a random number $d_B \in [1, n-1]$ and then computes $Q_B = d_B P - tQ$, $Y = Q_A - tQ$, $K_B = d_B Y$, and $H_B = H(K_B \| Y)$. Next, B sends the Q_B and H_B to A.

Step 3. A computes $X = Q_B + tQ$ and then computes $K_A = d_A X$. Next, A verifies the equality of $H(K_A \| d_A P)$ and H_B. If it does not hold, the protocol is terminated. Otherwise, A sends $H_A = H(K_A \| X)$ to B and sets the session key to K_A.

Step 4. When B receives the message, it checks the equality of $H(K_B \| d_B P)$ and H_A. Only if the equality holds, B agrees on the session key K_B. Otherwise, B terminates the protocol.

With this modification, the improved protocol can withstand the offline password guessing attack described in section III. The reason is described as follows.

The adversary $\mathscr{A}$ generates a random number $d_A \in [1, n-1]$, computes $Q_A = d_A P$, and sends A and Q_A to B. Upon receiving A and Q_A, B also chooses a random number $d_B \in [1, n-1]$ and then computes $Q_B = d_B P - tQ$, $Y = Q_A - tQ = d_A P - tQ$, $K_B = d_B Y = d_B(d_A P - tQ) = d_A d_B P - t d_B Q$, and $H_B = H(K_B \| Y)$. Next, B sends the Q_B and H_B to A.

Upon receiving Q_B and H, the adversary $\mathscr{A}$ chooses a password S' from D and derives the corresponding t'. $\mathscr{A}$ could compute $d_A d'_B P = d_A(Q_B + t'Q)$ but not $d'_B Q$ since $\mathscr{A}$ would face an elliptic curve discrete logarithm problem. Therefore, $\mathscr{A}$ cannot compute K'_B since $K'_B = d_A d'_B P - t' d'_B Q$. Thus, $\mathscr{A}$ is not able to verify the correctness of S'. The modified protocol can resist the offline password guessing attacks described in section III.

V. Conclusion

In this letter, we reviewed Lo and others' protocol [4] and showed that their protocol cannot resist an offline password guessing attack. We then demonstrated how to fix the protocol to ensure that it is robust against attacks.

Acknowledgements

The author thanks Dr. Kyu-Seok Lee, Ms. Julie Turner, and the anonymous reviewers for their valuable comments.

References

[1] A.-F. Sui et al., "An Improved Authenticated Key Agreement Protocol with Perfect Forward Secrecy for Wireless Mobile Communication," *IEEE Wireless Commun. Netw. Conf.*, vol. 4, 2005, pp. 2088-2093.

[2] R. Lu, Z. Cao, and H. Zhu, "An Enhanced Authenticated Key Agreement Protocol for Wireless Mobile Communication," *Comput. Stds. Interfaces*, vol. 29, 2007, pp. 647-652.

[3] C.-C. Chang and S.-C. Chang, "An Improved Authentication Key Agreement Protocol Based on Elliptic Curve For Wireless Mobile Networks," *Int. Conf. Intell. Info. Hiding Multimedia Signal Process.*, 2008, pp. 1375-1378.

[4] J.-W. Lo, C.-C. Lee, and M.-S. Hwang, "A Secure and Efficient ECC-based AKA Protocol for Wireless Mobile Communications," *Int. J. Innovative Comput., Info. Control*, vol. 6, no. 11, 2010, pp. 5249-5258.