World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:6, No:8, 2012

Cryptanalysis of Chang-Chang's EC-PAKA protocol for wireless mobile networks

Hae-Soon Ahn, *Member, IEEE,* and Eun-Jun Yoon, *Member, IEEE*

Abstract—With the rapid development of wireless mobile communication, applications for mobile devices must focus on network security. In 2008, Chang-Chang proposed security improvements on the Lu et al.'s elliptic curve authentication key agreement protocol for wireless mobile networks. However, this paper shows that Chang-Chang's improved protocol is still vulnerable to off-line password guessing attacks unlike their claims.

Keywords—Authentication, key agreement, wireless mobile networks, elliptic curve, password guessing attacks.

I. Introduction

WITH, the rapid development of wireless mobile communication, an authenticated key agreement protocol for mobile devices is an important issue in secure communication. Due to limitations in power consumption, bandwidth and computation, an efficient authenticated key agreement protocol can be used in the wireless mobile networks.

In 2005, Sui et al. [1] proposed an elliptic curve based password authenticated key agreement (EC-PAKA) protocol. Elliptic curve cryptography [2], [3], is more efficient in terms of computation than other authentication key agreement protocols. But, Sui et al.'s EC-PAKA protocol cannot resist the off-line password guessing attack. Therefore, Lu et al. [4] present an enhanced EC-PAKA protocol to against this attack. In 2008, Chang-Chang [5] pointed out that Lu et al.'s enhanced EC-PAKA protocol cannot withstand the parallel guessing attack and then proposed security improvements on the Lu et al.'s EC-PAKA protocol for wireless mobile networks. Chang-Chang claimed that their proposed EC-PAKA protocol can overcome the weaknesses of Lu et al.'s protocol. However, this paper shows that Chang-Chang's improved EC-PAKA protocol is still vulnerable to off-line password guessing attacks unlike their claims in which an attacker exhaustively enumerates all possible passwords in an off-line manner to determine the correct one [6], [7], [8].

The rest of this article is organized as follows. Sections 2 briefly reviews Chang-Chang's EC-PAKA protocol. Then, Section 3 points out the off-line password guessing attack exists in Chang-Chang's EC-PAKA protocol. Finally, conclusions are presented in Section 4.

II. Review of Chang-Chang's EC-PAKA protocol

This section briefly reviews Chang-Chang's EC-PAKA protocol [5]. The following notations are used throughout this paper.

- Alice(A), Bob(B): two communication users;
- E: an elliptic curve defined over a finite field A with large group order;
- n: a secure large prime;
- P; a point in E with large order n;
- D: a uniformly distributed dictionary of size $|D|$;
- S: a low-entropy password shared between Alice and Bob, which is randomly chosen from D;
- t: the value t is derived from the password S in a predetermined way, which is uniformly distributed in Z_n^*;
- $H(\cdot)$: a secure one-way hash function;
- $||$: concatenation of messages;

Fig. 1 depicts the Chang-Chang's EC-PAKA protocol, which works as follows.

Step 1. $A \rightarrow B$: $\{Q_{A1}, Q_{A2}\}$
A first chooses a random number $d_A \in [1, n-1]$, and then computes the followings:

$$Q_{A1} = (d_A + t)P \tag{1}$$

$$Q_{A2} = d_A^2 P \tag{2}$$

Finally, A sends the message $\{Q_{A1}, Q_{A2}\}$ to B.

Step 2. $B \rightarrow A$: $\{H_B, Q_{B1}\}$
Upon receiving the message $\{Q_{A1}, Q_{A2}\}$, B also chooses two random numbers $d_{B1}, d_{B2} \in [1, n-1]$, and then computes the followings:

$$Y = Q_{A1} - tP = d_A P \tag{3}$$

$$Q_{B1} = d_{B1}P + d_{B2}Y \tag{4}$$

$$Q_{B2} = d_{B1}Y + d_{B2}Q_{A2} \tag{5}$$

$$H_B = H(A||B||Q_{A1}||Q_{B1}||Y) \tag{6}$$

Finally, B sends $\{H_B, Q_{B1}\}$ and to A.

Step 3. $A \rightarrow B$: $\{H_A\}$
Upon receiving the message $\{H_B, Q_{B1}\}$, A checks whether the equality

$$H(A||B||Q_{A1}||Q_{B1}||Y) \stackrel{?}{=} H_B \tag{7}$$

holds or not. If it holds, A computes and sends

$$H_A = H(B||A||Q_{B1}||Q_{A1}||d_A P) \tag{8}$$

to B. Then, A computes

$$X = d_A Q_{B1} = d_{B1} d_A P + d_{B2} d_A^2 P \tag{9}$$

and sets the session key as

$$K_A = X \tag{10}$$

H.-S. Ahn is with the Faculty of Liberal Education, Daegu University, 201 Naeri-Ri, Jillyang-Ub, Kyungsan-Si, Kyungsangpuk-Do 712-830, Republic of Korea e-mail: ahs221@hanmail.net.

E.-J. Yoon is with the Department of Cyber Security, Kyungil University, 33 Buho-Ri, Hayang-Ub, Kyungsan-Si, Kyungsangpuk-Do 712-701, Republic of Korea e-mail: ejyoon@kiu.ac.kr. (Corresponding author.)

Manuscript received July 1, 2012; revised July 1, 2012.

Step 4. Upon receiving the message $\{H_A\}$, B checks whether the equality

$$H(B||A||Q_{B1}||Q_{A1}||Y) \stackrel{?}{=} H_A \quad (11)$$

holds or not. If it holds, B sets the session key as

$$K_B = Q_{B2} \quad (12)$$

III. Cryptanalysis of Chang-Chang's EC-PAKA protocol

This section shows that Chang-Chang's EC-PAKA protocol is still vulnerable to off-line password guessing attacks unlike their claims. Password-based AKA protocols can be vulnerable to password guessing attacks because users usually choose easy-to-remember passwords. Unlike typical private keys, the password has limited entropy, and is constrained by the memory of the user. For example, one alphanumerical character has 6 bits of entropy, and thus the goal of the attacker, which is to obtain a legitimate communication party's password, can be achieved within a reasonable time. Therefore, the password guessing attacks on the password-based AKA protocols should be considered a real possibility. In general, the password guessing attacks can be divided into three classes as follow[6], [7], [8]:

1) *Detectable on-line password guessing attacks*: an attacker attempts to use a guessed password in an on-line transaction. He/she verifies the correctness of his/her guess using the response from server. A failed guess can be detected and logged by the server.
2) *Undetectable on-line password guessing attacks*: similar to above, an attacker tries to verify a password guess in an online transaction. However, a failed guess cannot be detected and logged by the server, as the server cannot distinguish between an honest request and an attacker's request.
3) *Off-line password guessing attacks*: an attacker guesses a password and verifies his/her guess off-line. No participation of server is required, so the server does not notice the attack as a malicious one.

Based on the above definitions of password guessing attacks, we define the security term needed for security problem analysis of the Chang-Chang's EC-PAKA protocol as follows:

Definition 1: A weak secret (password S) is a value of low entropy Weak(k), which can be guessed in polynomial time.

An adversary Eve can perform the following off-line password guessing attack. Let us assume that an adversary Eve has intercepted one of the A and B's past communication messages, i.e., $\{Q_{A1}, Q_{A2}, H_B, Q_{B1}, H_A\}$. Then Eve can perform an off-line password guessing attack to obtain the password S as follows:

1) Eve generates a candidate password S^* from password dictionary which called D.
2) Eve derives the value $t^*(\in Z_n^*)$ from the guessed password S^*.
3) Eve obtains $d_A P^*$ by computing

$$d_A P^* = Q_{A1} - t^* P \quad (13)$$

where $Q_{A1} = d_A P + tP$.

4) Eve computes H_B^* as follows:

$$H_B^* = H(A||B||Q_{A1}||Q_{B1}||d_A P^*) \quad (14)$$

5) Eve compares H_B^* with the intercepted H_B.
6) If H_B^* is equal to H_B, then Eve has guessed the correct password S^*, otherwise, Eve performs steps 1-5 repeatedly until $H_B^* \equiv H_B$ by choosing another password S^{**}.

The algorithm of the off-line password guessing attacks for getting the password S is as follows:

Off-line Password Guessing Attacks(Q_{A1}, H_B, D)
{
  for $i := 0$ to $|D|$
  {
    $S^* \leftarrow D$;
    $t^*(\in Z_n^*) \leftarrow S^*$;
    $d_A P^* = Q_{A1} - t^* P$;
    $H_B^* = H(A||B||Q_{A1}||Q_{B1}||d_A P^*)$;
    if $H_B^* \stackrel{?}{=} H_B$ **then**
      return S^*
  }
}

After the adversary Eve has obtained the user A's password S^* using the above off-line password guessing attack method, the adversary Eve can impersonate A by forging A's sending message $\{Q_{A1}^* = (d_{Eve} + t)P, Q_{A2} = d_{Eve}^2 P\}$, where d_{Eve} is a random number $\in [1, n-1]$. Therefore, Chang-Chang's EC-PAKA protocol is vulnerable to off-line password guessing attacks.

Real applications for the proposed off-line password guessing attacks are as follows: Passwords are the most common methods of user authentication and key agreement on the Internet or mobile environments. For practical security applications, PAKA protocols are required when making use of Internet or mobile network services like E-learning, on-line polls, on-line ticket-order systems, roll call systems, on-line games, etc. In real security applications, users offer the same password as above to access several application servers for their convenience [8]. Thus, an adversary Eve may try to use the guessed password S to impersonate the legal user A to login to other systems that the user A has registered with outside this Chang-Chang's EC-PAKA protocol-based server. If the targeted outside server adopts the normal authentication and key agreement protocol, it is possible that the adversary Eve can successfully impersonate the user A to login to it by using the guessed password S. Therefore, the password breach cannot be revealed by the adversary's actions.

IV. Conclusions

The EC-PAKA technology has been widely deployed in various kinds of applications. This paper demonstrated that Chang-Chang's EC-PAKA protocol is still insecure to off-line password guessing attacks. For this reason, Chang-Chang's

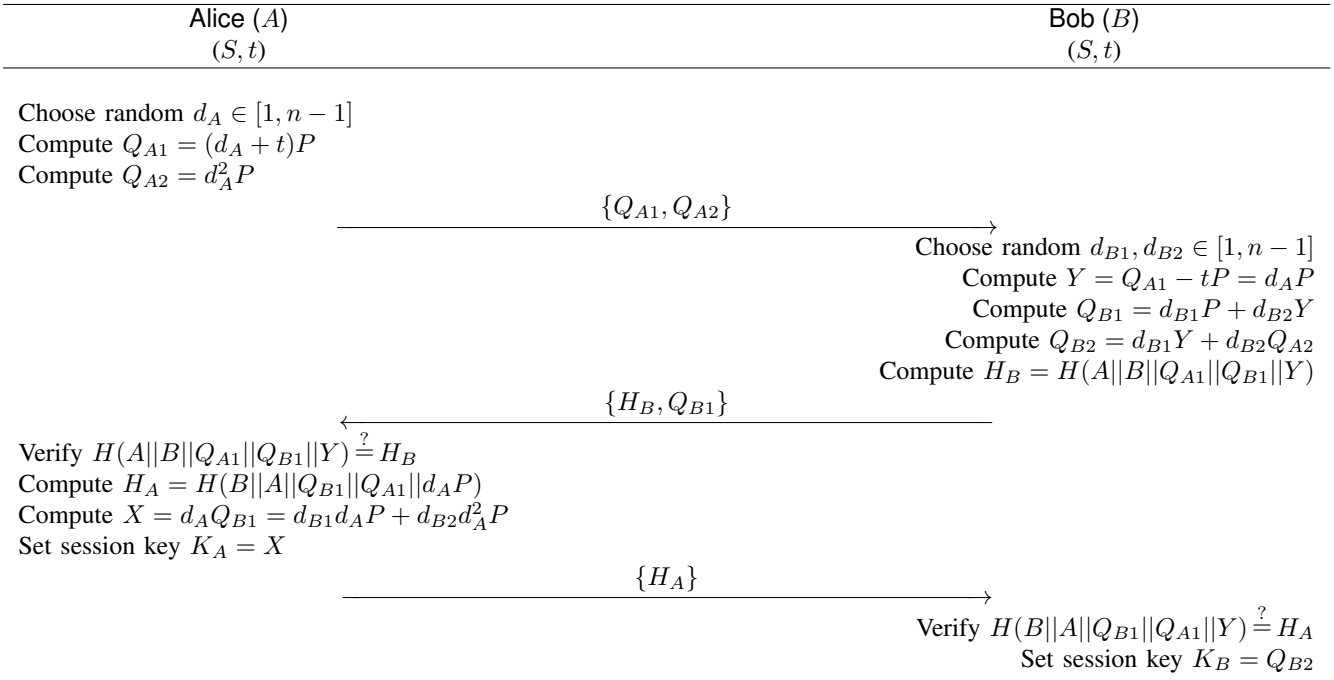

Fig. 1. Chang-Chang's EC-PAKA protocol for wireless mobile networks

EC-PAKA protocol cannot use for practical application, especially in the resource-limited environments and real-time systems. Further works will be focused on improving the Chang-Chang's EC-PAKA protocol which can be able to provide greater security and to be more efficient than the existing EC-PAKA protocols by an accurate performance analysis.

ACKNOWLEDGEMENTS

We would like to thank the anonymous reviewers for their helpful comments in improving our manuscript.

REFERENCES

[1] A. Sui, L. Hui, S. Yiu, K. Chow, W. Tsang, C. Chong, K. Pun, and H. Chan, An improved authenticated key agreement protocol with perfect forward secrecy for wireless mobile communication, *IEEE Wireless Communications and Networking Conference (WCNC 2005)*, LA USA, pp. 2088-2093, 2005.

[2] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation*, vol. 48, pp. 203-209, 1987.

[3] V. S. Miller, Use of elliptic curves in cryptography, *Proceedings of Advances in Cryptology Crypto'85*, Lecture Notes in Computer Science, Springer, Berlin, vol. 128, pp. 417-426, 1985.

[4] R. Lu, Z. Cao, and H. Zhu, An enhance authentication key agreement protocol for wireless mobile communication, *Computer Standards and Interfaces*, vol. 29, pp. 647-652, 2007.

[5] C. C. Chang and S. C. Chang, An improved authentication key agreement protocol based on elliptic curve for wireless mobile networks, *International Conference on IEEE Intelligent Information Hiding and Multimedia Signal Processing*, vol. 1, pp. 1375-1378, 2008.

[6] H. S Kim and J. Y. Choi, Enhanced password-based simple three-party key exchange protocol, *Computers & Electrical Engineering*, vol. 35, pp. 107-114, 2009.

[7] Y. Ding and P. Horster, Undetectable on-line password guessing attacks, *ACM Operating Systems Review*, vol. 29, no. 4, pp. 77-86, 1995.

[8] H. J. Kim and E. J. Yoon, Cryptanalysis of an enhanced simple three-party key exchange protocol, *Communications in Computer and Information Science*, vol. 259, pp. 167-176, 2011.