Two undetectable on-line dictionary attacks on Debiao et al.’s S-3PAKE protocol
Sung-Bae Choi, Member, IEEE, Sang-Yoon Yoon, Member, IEEE, and Eun-Jun Yoon, Member, IEEE

Abstract—In 2011, Debiao et al. pointed out that S-3PAKE protocol proposed by Lu and Cao for password-authenticated key exchange in the three-party setting is vulnerable to an off-line dictionary attack. Then, they proposed some countermeasures to eliminate the security vulnerability of the S-3PAKE. Nevertheless, this paper points out their enhanced S-3PAKE protocol is still vulnerable to undetectable on-line dictionary attacks unlike their claim.

Keywords—Authentication, 3PAKE, password, three-party key exchange, network security, dictionary attacks.

I. INTRODUCTION

RECENTLY, three-party password-based authenticated key exchange (3PAKE) protocols are extremely important security technologies to secure communications and are now extensively adopted in various network communications. These 3PAKE protocols allow users to communicate securely over public networks simply by using easy-to-remember passwords. In the 3PAKE protocols, each user can exchange session keys with other users securely via the remote server. The remote server authenticates users by encrypting sending messages with personal passwords; only valid users can decrypt the received messages with their own passwords and derive the correct common session keys for their subsequent communications.

In 2007, Lu and Cao [1] proposed a simple 3PAKE protocol (short, S-3PAKE) built upon the earlier two-party PAKE protocol due to Abdalla and Pointcheval [2]. However, it is found out that S-3PAKE is vulnerable to various attacks according to recent works in [3], [4], [5], [6]. Quite recently, Debiao et al. [7] also pointed out that S-3PAKE protocol is vulnerable to an off-line dictionary attack [8], [9]. Furthermore, they proposed some countermeasures to eliminate the security vulnerability of the S-3PAKE. They claimed that the enhanced S-3PAKE protocol (in short Debiao-S-3PAKE) is secure to the off-line dictionary attack. Nevertheless, this paper points out their Debiao-S-3PAKE protocol is still vulnerable to undetectable on-line dictionary attacks unlike their claim in which an attacker exhaustively enumerates all possible passwords in an on-line manner to determine the correct one [10].

The remainder of this paper is organized as follows. We subsequently review Debiao-S-3PAKE protocol in Section 2. The undetectable on-line dictionary attacks on Debiao-S-3PAKE protocol are presented in Section 3. Finally, we draw conclusions in Section 4.

II. REVIEW OF DEBIAO-S-3PAKE PROTOCOL

This section reviews the Debiao-S-3PAKE Protocol [7]. Throughout the paper, notations are employed in Table I. Fig. 1 depicts the Debiao-S-3PAKE protocol, which works as follows.

1) \( A \rightarrow B: A||X^* \)

\( A \) chooses a random number \( x \in Z_p \), computes \( X = g^x \) and \( X^* = X \cdot M^{pw_A} \), and sends \( A||X^* \) to \( B \).

2) \( B \rightarrow S: A||X^*||B||Y^* \)

\( B \) selects a random number \( y \in Z_p \), computes \( Y = g^y \) and \( Y^* = Y \cdot N^{pw_B} \), and sends \( A||X^*||B||Y^* \) to \( S \).

3) \( S \rightarrow B: \bar{X}||\bar{Y} \)

Upon receiving \( A||X^*||B||Y^* \), \( S \) first recovers \( X \) and \( Y \) by computing \( X = X^* \cdot M^{pw_A} \) and \( Y = Y^* \cdot N^{pw_B} \). Then \( S \) checks \( X = 1, -1 \) and \( Y = 1, -1 \) hold or not. If one of above equations holds, then \( S \) stops the protocol. Otherwise, \( S \) selects a random number \( z \in Z_p \) and computes \( \bar{X} = X^z \) and \( \bar{Y} = Y^z \). Then \( S \) computes \( pw_A' = H(A)||S||X)^{pw_A} \), \( pw_B' = H(B)||S||Y)^{pw_B} \), and sends \( \bar{X}||\bar{Y} \) to \( B \).

4) \( B \rightarrow A: Y^*||\alpha \)

After having received \( \bar{X}||\bar{Y} \), \( B \) computes \( pw_B'' = H(B)||S||Y)^{pw_B} \), \( K = (\bar{X} / pw_B'')^y = g^{\alpha y} \), \( \alpha = H(A)||B||K \), and sends \( Y^*||\alpha \) to \( A \).

5) \( A \rightarrow B: \beta \)

After having received \( Y^*||\alpha \), \( A \) computes \( pw_A'' = H(A)||S||X)^{pw_A} \), \( K = (\bar{Y} / pw_A'')^x = g^{\alpha x} \), and verifies...
that $\alpha$ is equal to $H(A||B||K)$. If the verification fails, then $A$ aborts the protocol. Otherwise, $A$ computes the session key $SK_A = H'(A||B||K)$ and sends $\beta = H(B||A||K)$ to $B$.

6) $B$ verifies the correctness of $\beta$ by checking that $\beta$ is equal to $H(B||A||K)$. If it holds, then $B$ computes the session key $SK_B = H'(A||B||K)$. Otherwise, $B$ aborts the protocol.

III. CRYPTOANALYSIS OF DEBIAO-S-3PAKE PROTOCOL

This section shows that Debiao-S-3PAKE protocol [7] is not secure to undetectable on-line dictionary attacks by any other registered user. Password-based authentication protocols can be vulnerable to dictionary attacks because users usually choose easy-to-remember passwords. Unlike typical private keys, the password has limited entropy, and is constrained by 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, dictionary attacks on the password-based protocols should be considered a real possibility. In general, the dictionary attacks can be divided into three classes as follow[8], [9]:

1) Detectable on-line dictionary 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 dictionary 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 dictionary 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 dictionary attacks, we define the security term needed for security problem analysis of the Debiao-S-3PAKE protocol as follows:

Definition 1: A weak secret (password $pw_i$) is a value of low entropy $\text{Weak}(k)$, which can be guessed in polynomial time.

1) Real applications for the proposed dictionary attacks [10]: In the modern life which the Internet has strong influence to people, passwords are the most common means of user authentication on the Internet. For practical applications, password-based authentication protocols are required when making use of Internet network services like E-learning, online polls, on-line ticket-order systems, roll call systems, online games, etc. In real applications, users offer the same password as above to access several application servers for their convenience. Thus, an attacker may try to use the guessed password $pw_A$ to impersonate the user $A$ to login to other systems that the user $A$ has registered with outside this Debiao-S-3PAKE protocol-based server. If the targeted outside server adopts the normal authentication protocol, it is possible that the attacker can successfully impersonate the user $A$ to login to it by using the guessed password $pw_A$. Therefore, the password breach cannot be revealed by the attacker’s actions.

A. Undetectable on-line dictionary attack with helping $A$

A malicious user $B$ with helping a legal user $A$ can perform the following “undetectable on-line dictionary attack $1^*$”.

1) $A \rightarrow B: A||X^*$

$A$ operates as specified in the protocol in the first step.

2) $B \rightarrow S: A||X^*||B||Y^*$

Let $B$ be a malicious user mediating between $S$ and $A$. Upon intercepting $A||X^*$ form the user $A$ in flow (1) of the Debiao-S-3PAKE protocol. $B$ guesses a password $pw'_A$, and establishes an authenticated and private channel with $S$. $B$ first computes $g^x = X^*/M_{pwA}$ for an unknown element $x \in Z_q$. Then, $B$ computes $Y^* = g^{x^*} \cdot N_{pwA}$ and sends $A||X^*||B||Y^*$ to $S$.

3) $S \rightarrow B: \overline{X}^*, \overline{Y}^*$

Upon receiving $A||X^*||B||Y^*$, $S$ first will recover $X$ and $Y$ by computing $X = X^*/M_{pwA} = g^x$ and $Y = Y^*/N_{pwA} = g^{x^*}$. $S$ then will check $X = 1$ and $Y = 1$, and $1$ hold or not. Because the above equations always not hold, $S$ will not stop this session. Next, $S$ will select a random number $z \in Z_q$ and compute $\overline{X} = X^* \cdot g^{xz}$ and $\overline{Y} = Y^* = g^{y^*}$. $S$ then will compute the followings:

$$pw'_A = H(A||S||X)^{pwA} = H(A||S||g^{x})^{pwA}$$  \[1\]

$$pw_B = H(B||S||Y)^{pwA} = H(B||S||g^{x^*})^{pwA}$$  \[2\]

$$\overline{X} = \overline{X} \cdot pw'_B = g^{xz} \cdot pw_B$$  \[3\]

$$\overline{Y} = \overline{Y} \cdot pw_A = g^{y^*} \cdot pw_A$$  \[4\]

and will send $\overline{X}^*||\overline{Y}^*$ to $B$.

4) When $B$ receives $\overline{X}^*, \overline{Y}^*$, $B$ uses his/her password $pw'_B$, the guessed password $pw'_A$, and $g^{x^*}$ to obtain the followings:

$$pw'_A = H(A||S||g^{x^*})^{pwA}$$  \[5\]

$$pw_B = H(B||S||g^{x^*})^{pwA}$$  \[6\]

$B$ checks if the following equation holds or not:

$$\overline{Y}^*/pw'_A = \overline{X}^*/pw_B$$  \[7\]

If the check passes, then $B$ confirms that the guessed password $pw'_A$ is the correct one.

5) Otherwise, $B$ repeatedly performs the steps 2-4 without being noticed by $S$. For example, $B$ guesses another password $pw''_A$, and computes $g^{x''} = X^*/M_{pw''A}$ and $Y^{**} = g^{x''} \cdot N_{pw''A}$. Then, $B$ sends $A||X^*||B||Y^{**}$ to $S$.

It is clear that if $pw'_A = pw_A$, then $\overline{Y}^*/pw'_A = g^{y^*} = \overline{X}^*/pw_B = g^{xz}$. Therefore, $g^x = g^{x^*}$. 

International Scholarly and Scientific Research & Innovation 6(8) 2012 932

ISNI:0000000091950263
B. Undetectable on-line dictionary attack without helping A

A malicious user B without helping a legal user A can perform the following “undetectable on-line dictionary attack” 2.

1) \( B \rightarrow S: A||X^*||B||Y^* \)

Let B be a malicious user mediating between S and A. Without any contribution from A, B guesses a password \( pw_A' \), and establishes an authenticated and private channel with S. B computes \( X^* = g \cdot M^{pw_A} \) and \( Y^* = g \cdot N^{pw_B} \). Finally, B sends \( A||X^*||B||Y^* \) to S.

2) \( S \rightarrow B: \text{X}^, \text{Y}^\)

Upon receiving \( A||X^*||B||Y^* \), S first will recover \( X \) and \( Y \) by computing \( X = X^*/M^{pw_A} \) and \( Y = Y^*/N^{pw_B} = g \cdot S \) then will check \( X = 1 \) and \( Y = 1 \). Because the above equations always not hold, S will not stop this session. Next, S will select a random number \( z \in Z_p \) and compute \( \text{X} = X^z \) and \( \text{Y} = Y^z = g^z \). Then, S will compute the followings:

\[
\begin{align*}
    pw_A'^z &= H(A||X^z)\cdot|M|^{pw_A} \quad \text{(8)} \\
    pw_B'^z &= H(B||Y^z)\cdot|N|^{pw_B} = H(B||S||g)^{pw_B} \quad \text{(9)} \\
    X^r &= X \cdot pw_B'^z = X^z \cdot pw_B' \quad \text{(10)} \\
    Y^r &= Y \cdot pw_A'^z = g^z \cdot pw_A' \quad \text{(11)}
\end{align*}
\]

and will send \( X^r||Y^r \) to B.

3) When B receives \( X^r, Y^r \), B uses the guessed password \( pw_A' \) to check if the following equation holds or not:

\[
Y^r / pw_A' = H(A||S||X^r)\cdot|M|^{pw_A} \quad \text{(12)}
\]

If the check passes, then B confirms that the guessed password \( pw_A' \) is the correct one.

4) Otherwise, B repeatedly performs the steps 1-3 without being noticed by S. For example, B guesses another password \( pw_B'' \), and computes \( X'' = H(pw_A') \) and \( Y'' = H(pw_B) \). Then, B sends \( A||X''||B||Y'' \) to S.

It is clear that if \( pw_A' = pw_A' \), then \( Y'' = H(A||B||S||1)^{pw_A} = pw_A' \). Therefore, \( X'' = H(pw_A') \).

IV. Conclusions

The 3PAKE technology has been widely deployed in various kinds of applications. This paper demonstrated that Debiao-S-3PAKE protocol still insecure to undetectable on-line dictionary attacks. For this reason, Debiao-S-3PAKE protocol cannot use for practical application. It is important that security engineers should be made aware of this, if they are responsible for the design and development of 3PAKE systems. Further works will be focused on improving the Debiao-S-3PAKE protocol which can be able to provide greater security and provides computation efficiency.
ACKNOWLEDGEMENTS
We would like to thank the anonymous reviewers for their helpful comments.

REFERENCES