Impersonating the Server on Simple three Party Key Exchange Protocol

R. Padmavathy
National Institute of Technology Waranal, Andra Pradesh, India
E-mail: r_padma3@rediffmail.com

Abstract: The Password-authenticated key exchange (PAKE) protocols allow parties to share secret keys in an authentic manner based on an easily memorizable password. On the other hand, the protocol should resist all types of password guessing attacks, since the password is of low entropy. Recently Lu Cao proposed a simple three-party password based authenticated key exchange (S-3 PAKE) protocol and claimed that it can resist various attacks. Unlike their claims Phan et al., presented an Undetectable online dictionary attack on the above protocol. In the present paper, impersonation of the server is demonstrated on S-3PAKE protocol using the Undetectable online dictionary attack proposed by Phan et al.

Key words: S-3PAKE protocol, Undetectable online dictionary attack, Impersonating server, password.

1. INTRODUCTION

In the secure communication areas, key exchange protocol is one of the most important cryptographic mechanisms, by which a pair of users that communicate over a public unreliable channel can generate a secure session key. As the password based authenticated key exchange protocols require users only to remember a human-memorable (low-entropy) password, it is rather simple and efficient. In a three-party PAKE protocol, each client first shares a human-memorable password with a trusted server, and then when two clients wants to agree a session key, they resort to the trusted server for authenticating each other. Password-based authenticated key exchange protocols, however, are vulnerable to password guessing attacks [1] since users usually choose easy-to-remember passwords. The goal of the attacker is to obtain a legitimate communication party’s password. In general the password guessing attacks can be divided into three classes and they are listed below [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.

- **Undetectable on-line password guessing attacks**: Similar to Detectable on-line password guessing attack, an attacker tries to verify a password guess in an on-line transaction. However, a failed guess cannot be detected and logged by server, as server is not able to distinguish an honest request from a malicious one.

- **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.

The first practical key exchange protocol is proposed by Diffie-Hellman [2]. Subsequently, many other two-party PAKE protocols have been proposed [3, 4, 5, 6, 7]. The first PAKE protocol, known as Encrypted key Exchange (EKE), was proposed by Bellovin and Merritt [8]. Two party PAKE protocols are only suitable for the client-server architecture, many researchers have recently begun to study the three-party PAKE protocols [9, 10, 11, 12, 13, 14, 15]. Recently, Lu and Cao [15] proposed a simple three-party key exchange (SPAKE) protocol based on the chosen-basis computational Diffie-Hellman (CCDH) assumption. They claimed that their protocol can resist various attacks and is superior to similar protocols with respect to efficiency. Overriding their claims, Phan et al., proved that S-3PAKE protocol falls to undetectable online dictionary attack [16].
In this paper impersonating server on S-3PAKE protocol using the Undetectable on-line dictionary attack proposed by Phan et al., is demonstrated. The attacker can impersonate the server, where the server is not at all involved with two party’s password is known, which is guessed in some other session. If a malicious party able to guess the password of other clients, then the same party will act as a server during the session between two parties and will provide the required information to the clients through which they will get the key but the server is not at all involved in the session at all. undetectable online dictionary attack. Section 3 describes the impersonation of the server by the attacker on S-3PAKE protocol and the concluding remarks are made in section 4.

\[(G, g, p): \text{a finite cyclic group } G \text{ generated by an element } g \text{ of prime order } p.\]
\[M, N: \text{two elements in } G.\]
\[S: \text{a trusted server.} \]
\[A, B: \text{two clients.} \]
\[PW_A: \text{the password shared between } A \text{ and } S.\]
\[PW_B: \text{the password shared between } B \text{ and } S.\]
\[H_1, H_2: \text{two secure one-way hash functions.} \]

Let us assume two clients, such as A and B, wish to agree upon a common session key. However, as they do not hold any shared information in advance, they cannot directly authenticate each other and have to resort to the trusted server S for a session key agreement.

The detailed steps of the S-3PAKE protocol are described as follows:

**Step 1:**
1A: A chooses a random number \( x \in Z_p \) and computes \( X = g^x \cdot M^{PW_A} \) then sends ID\(_A\), X to B.
1B: B also chooses a random number \( y \in Z_p \) and computes \( Y = Y \cdot N^{PW_B} \), then sends ID\(_B\), Y, ID\(_A\), X to S.

**Step 2**
2A: upon receiving ID\(_A\), X, ID\(_B\), Y, the server S first uses the passwords pw\(_A\) and pw\(_B\) to compute \( X' = \frac{X}{M^{PW_A}} \) and \( Y' = \frac{Y}{N^{PW_B}} \), respectively.
2B: Then, she chooses another random number \( z \in Z_p \) and computes \( \gamma = g^z \cdot H_1(ID_A, ID_B, X') \).

**Step 3**
3A: B computes \( \gamma = \frac{Y'}{H_1(ID_B, ID_S, Y^{PW_B})} \) and sends \( X' = \gamma \cdot H_1(ID_A, ID_B, X') \).

\[\text{Figure 1: S-3PAKE Protocol}\]
Impersonating the Server on Simple Three Party Key Exchange Protocol

3B: A computes \( X^\alpha = X^*/H_1(ID_A, ID_B, g^{X^*}) = g^{\alpha} \) and verifies \( H_1(ID_A, ID_B, X^*) = \alpha \), if the received \( \alpha = \) computed \( \alpha \) then B is authenticated by A.

3C: A computes the session key \( sk_A = H_2(ID_A, ID_B, X^*) = H_2(ID_A, ID_B, g^{X^*}) \) and \( \beta = H_1(ID_B, ID_A, X^*) = H_1(ID_B, ID_A, g^{X^*}) \) and sends \( \beta \) to B.

3D: B verifies \( \beta = H_1(ID_B, ID_A, Y^*) \) if the received \( \beta = \) computed \( \beta \) then A is authenticated by B.

Figure 1 illustrates simple three party password authenticated key exchange protocol.

2a. Undetectable Online Dictionary Attack on S-3PAKE Protocol

Undetectable online dictionary attack [16] on S-3PAKE can be mounted by any adversary, such as C as shown in figure 2. The following steps explains the attack in detail.

Step 1: Choose \( x, y \in Z_p \)

Step 2: For all guesses of \( PW_A \) and \( PW_B \):

\[
\begin{align*}
& X^* = g^x \cdot M^{PW_A}, \\
& Y^* = g^y \cdot N^{PW_B}
\end{align*}
\]

Step 3: C (attacker) intercepts the message sent by B. Upon receiving \( ID_A, X, ID_B, Y \) the C first uses the passwords \( PW_A \) and \( PW_B \) to compute \( g^{X^*} = X / M^{PW_A} \) and \( g^{Y^*} = Y / N^{PW_B} \), respectively.

Step 4: Then, C chooses another random number \( z \in Z_p \) and computes \( g^{Z^*} = (g^x)^z \cdot g^{Z^*} = (g^y)^z \).

Finally, she sends \( X', Y' \) to B, where
Step 5: B computes $g^{z_c} = Y'/H_1(ID_B, ID_D, g^{x'})^{PWS}$ and $\alpha = H_1(ID_A, ID_B, (g^{z_c})^y)$ and sends $X', Y'$ to B.

Step 6: A computes $g^{z_c} = X'/H_1(ID_A, ID_D, g^{x'})^{PWS}$ and verifies $H_1(ID_A, ID_B, (g^{z_c})^y) = \alpha$, if the received $\alpha = $ computed $\alpha$ then B is authenticated by A.

Step 7: A computes the session key $sk_A = H_2(ID_A, ID_B, g^{xyz})$ and $\beta = H_1(ID_B, ID_A, g^{xyz})$ and sends $\beta$ to B.

Step 8: B verifies $\beta = H_1(ID_B, ID_A, g^{xyz})$ if the received $\beta = $ computed $\beta$ then A is authenticated by B. The session key $sk_B = H_2(ID_A, ID_B, (g^{z_c})^y)$ is determined.

Now, A and B has obtained the Key where the server is not involved at all. Figure 3 illustrates the impersonation of server by the attacker on simple three party password authenticated key exchange protocol.

Figure 3: The Attacker Impersonating the Server
4. CONCLUSIONS

The above results show that if passwords are exposed then, the attacker can act as server and impersonate the server, where the server is not involved in the session at all. Hence the protocol should be designed such that it should resist all types of password guessing attacks. It can be avoided by satisfying mutual authentication between the client and the server. The attack is achieved due to two elements $M, N \in \mathbb{Z}_q$ used in the protocol. The attack can be avoided by sharing $M$ and $N$ between server, $A$ and server, $B$ respectively. This leads to avoid the impersonation of the server attack.

REFERENCES