ISSN 1512-1232

WEAKNESSES OF S-3 PAKE' PROTOCOL

Shirisha Tallapally

Computer Science and Engineering Department
Malla Reddy Engineering College, Secunderabad, India
shirisha27@yahoo.co.in

Abstract
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. Chung and Ku proved impersonation-of-initiator attack, an impersonation-of-responder attack, and a man-in-the-middle attack on S-3 PAKE protocol and proposed 3-S PAKE' protocol to avoid these attacks. Unlike their claims Phan et al., presented an Undetectable online dictionary attack on S-3 PAKE protocol and concluded that the same attack holds good for 3-S PAKE' protocol. In the present paper an impersonation-of-initiator attack, a man-in-the middle attack and an Unknown key share attack are demonstrated on S-3 PAKE' protocol using the Undetectable online dictionary attack and the countermeasures to avoid the attacks are discussed.

Key-Words: *- S-3 PAKE' protocol, impersonation-of-initiator attack, Unknown key share attack, man-in-the middle attack, Undetectable on-line dictionary attack.*

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 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

ISSN 1512-1232

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]. Recently, Lu and Cao [14] proposed a simple three-party key exchange (SPAKE) protocol based on the chosen-bases 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 Chung and Ku proved that S-3 PAKE protocol is vulnerable to an impersonation-of-initiator attack, an impersonation-of-responder attack and a man-in-the middle attack and suggested a countermeasure to resist these attacks. Overriding their claims, Phan et al., proved that S-3 PAKE protocol falls to undetectable online dictionary attack [15] and claimed that the same attack holds good for Chung and Ku protocol.

In this paper an impersonation-of-initiator attack, a man-in-the middle attack and an Unknown key share attack on S-3 PAKE' protocol using the Undetectable on-line dictionary attack are demonstrated.

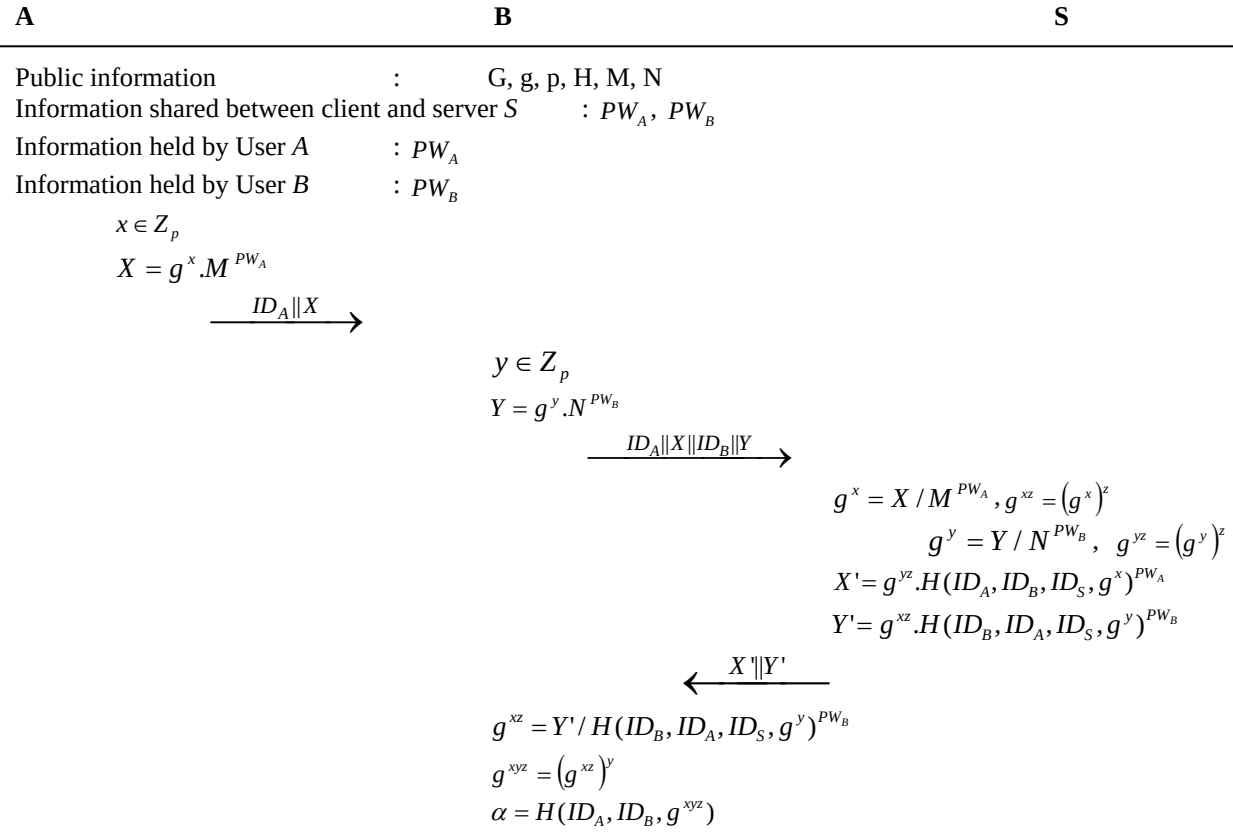
The paper is organized as follows: section 2 briefly reviews the Chung and Ku S-3 PAKE' protocol and the undetectable online dictionary attack. Section 3 describes the impersonation-of-initiator attack, a man-in-the middle attack and an Unknown Key share attack on S-3 PAKE' protocol. Section 4 gives the countermeasure and the concluding remarks.

2. Review of S-3 PAKE' protocol

This section presents a simple three-party password based key exchange protocol (S-3PAKE') and Undetectable online dictionary attack on S-3 PAKE' protocol.

Notations

(G, g, p): a finite cyclic group G generated by an element g of prime order p.
S: a trusted server
A, B: two clients.
pw_A: the password shared between A and S.
pw_B: the password shared between B and S.
H, H': two secure one-way hash functions.



ISSN 1512-1232

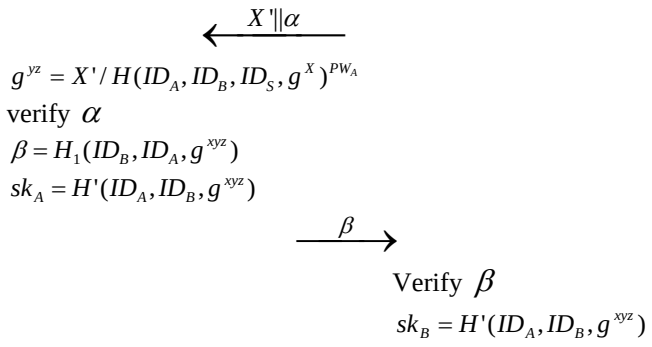


Fig 1: simple three party password authenticated key exchange' protocol

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-PAKE' protocol are described as follows:

Step1a: A chooses a random number $x \in Z_p$ and computes $X = g^x.M^{PW_A}$, then sends $ID_A \| X$ to *B*.
Step1b: upon receiving $ID_A \| X$, B also chooses a random number $y \in Z_p$ and computes $Y = g^y.N^{PW_B}$, then sends $ID_A \| X \| ID_B \| Y$ to *S*.

Step2a: Upon receiving $ID_A \| X \| ID_B \| Y$, the server *S* 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.
Step2b: Then, she chooses another random number $z \in Z_p$ and computes $g^{xz} = (g^x)^z$, $g^{yz} = (g^y)^z$.
Finally she sends $X'\|Y'$ to *B*, where $X' = g^{yz}.H(ID_A, ID_B, ID_S, g^x)^{PW_A}$ and $Y' = g^{xz}.H(ID_B, ID_A, ID_S, g^y)^{PW_B}$

Step3a: *B* computes $g^{xz} = Y'/H(ID_B, ID_A, ID_S, g^y)^{PW_B}$ and $\alpha = H(ID_A, ID_B, g^{xyz})$ and sends X', α.
Step3b: *A* computes $g^{yz} = X'/H(ID_A, ID_B, ID_S, g^X)^{PW_A}$ and verifies $H(ID_A, ID_B, g^{xyz}) = \alpha$, if the received α = computed α then *B* is authenticated by *A*.
Step3c: *A* computes the session key $sk_A = H'(ID_A, ID_B, g^{xyz})$ and $\beta = H_1(ID_B, ID_A, g^{xyz})$ and sends β to *B*.
Step3d: *B* verifies $\beta = H_1(ID_B, ID_A, g^{xyz})$ if the received β = computed β then *A* is authenticated by *B*.
The session key $sk_B = H'(ID_A, ID_B, g^{xyz})$ is determined.
Figure 1 illustrates simple three party password authenticated key exchange' protocol

2. A. Undetectable online dictionary attack on S-3 PAKE' protocol

Undetectable online dictionary attack 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[15].

Step1: Choose $x^*, y^* \in Z_p$.

Step2: For all guesses of PW_A and PW_B
Step2a: Compute $X* = g^{x*}.M^{PW*_A}$ and $Y* = g^{y*}.N^{PW*_B}$
Step2b: Send $ID_A, X*, ID_B, Y*$ to *S*.
Step2c: Server Computes $X'* = X*/M^{PW_A} = g^{x*}.M^{PW*_A}/M^{PW_A}$ and $Y'* = Y*/N^{PW*_B} = g^{y*}.N^{PW*_B}/N^{PW_B}$.
Step2d: *S* selects $z \in Z_p$ and computes $X''* = (Y'*)^z.H_1(ID_A, ID_B, ID_S, X'*)^{PW_A}$ and
$Y''* = (X'*)^z.H_1(ID_B, ID_A, ID_S, Y'*)^{PW_B}$

ISSN 1512-1232

Step2e: S returns X''^*, Y''^*

Step2f: Compute $X'''^* = X''^*.H_1(ID_A, ID_B, ID_S, g^*)^{PW_A^*} =$
$(Y'^*)^z.H_1(ID_A, ID_B, ID_S, X'^*)^{PW_A} / H_1(ID_A, ID_B, ID_S, g^{x^*})^{PW_A^*} = (g^{y^*}.N^{PW^*_B} / N^{PW_B}).H_1(ID_A, ID_B, ID_S, X'^*)^{PW_A} /$
$H_1(ID_A, ID_B, ID_S, g^{x^*})^{PW_A^*}$ and
$Y'''^* = Y''^*.H_1(ID_B, ID_A, ID_S, Y'^*)^{PW_B^*} = (X'^*)^z.H_1(ID_B, ID_A, ID_S, Y'^*)^{PW_B} / H_1(ID_B, ID_A, ID_S, Y'^*)^{PW_B^*} =$
$(g^{x^*}.M^{PW^*_A} / M^{PW_A}).H_1(ID_B, ID_A, ID_S, Y'^*)^{PW_B} /$
$H_1(ID_B, ID_A, ID_S, Y'^*)^{PW_B^*}$

C **S**

$x^*, y^* \in Z_p$
Guess PW^*_A and PW^*_B
$X^* = g^{x^*}.M^{PW^*_A}$
$Y^* = g^{y^*}.N^{PW^*_B}$

$ID_A, X^* ID_B, Y^*$ →

$X'^* = X^* / M^{PW_A} = g^{x^*}.M^{PW^*_A} / M^{PW_A}$
$Y'^* = Y^* / N^{PW^*_B} = g^{y^*}.N^{PW^*_B} / N^{PW_B}$
$z \in Z_p$
$X''^* = (Y'^*)^z.H_1(ID_A, ID_B, ID_S, X'^*)^{PW_A}$
$Y''^* = (X'^*)^z.H_1(ID_B, ID_A, ID_S, Y'^*)^{PW_B}$

← X''^*, Y''^*

$X'''^* = X''^*.H_1(ID_A, ID_B, ID_S, g^*)^{PW_A^*}$
$= (Y'^*)^z.H_1(ID_A, ID_B, ID_S, X'^*)^{PW_A} / H_1(ID_A, ID_B, ID_S, g^{x^*})^{PW_A^*}$
$= (g^{y^*}.N^{PW^*_B} / N^{PW_B}).H_1(ID_A, ID_B, ID_S, X'^*)^{PW_A} / H_1(ID_A, ID_B, ID_S, g^{x^*})^{PW_A^*}$

$Y'''^* = Y''^*.H_1(ID_B, ID_A, ID_S, Y'^*)^{PW_B^*}$
$= (X'^*)^z.H_1(ID_B, ID_A, ID_S, Y'^*)^{PW_B} / H_1(ID_B, ID_A, ID_S, Y'^*)^{PW_B^*}$
$= (g^{x^*}.M^{PW^*_A} / M^{PW_A}).H_1(ID_B, ID_A, ID_S, Y'^*)^{PW_B} / H_1(ID_B, ID_A, ID_S, Y'^*)^{PW_B^*}$

Fig.2: Undetectable on-line dictionary attack on simple three party password authenticated key exchange' protocol

Step2g: Check $[X''']^{(y^*)^{-1}} = [Y''']^{(x^*)^{-1}}$. Clearly, if the password guesses PW_A^* and PW_B^* are correct, this equality would be satisfied.

3. Attacks on S-3PAKE' protocol

This section describes impersonation of initiator attack, man in the middle attack and unknown key share attacks on S-3PAKE' protocol.

3. A. Impersonation-of- initiator attack

The attack sequence after mounting Undetectable on-line dictionary attack on simple three party password authenticated key exchange' (S-3PAKE') leads to impersonating initiator attack.

ISSN 1512-1232

C can impersonate *A* and make *B* believe that it is communicating with *A*, but it is actually communicating with *C*.

Any legitimate client, say *C*, who has shared pw_c with *S*, can impersonate *A* to initiate an instance of the protocol with *B* (after mounting Undetectable on-line password guessing attack as shown in fig.2) as in the following:

Step1a: C chooses a random number $w \in Z_p$ to compute $W \leftarrow g^w.M^{pw_C}$, and then impersonates *A* to send $ID_A \| W$ to B.

Step1b: Upon receiving $ID_A \| W$, *B* chooses a random number $y \in Z_p$ to compute $Y \leftarrow g^y.N^{pw_B}$, and then sends $ID_A \| W \| ID_B \| Y$ to *S*. In the meanwhile, *C* intercepts the message sent from *B*, and replaces the identifier *A* in this message with *C*. Next, *C* sends $ID_C \| W \| ID_B \| Y$ to *S*.

Step2a: Upon receiving $ID_C \| W \| ID_B \| Y$, *S* uses pw_c and pw_b to compute $g^w \leftarrow W / M^{pw_C}$ and $g^y \leftarrow Y / N^{pw_B}$, respectively, according to the identifiers contained in the received message.

Step2b: In addition, *S* chooses a random number $z \in Z_p$ and then computes $g^{wz} \leftarrow (g^w)^z$ and $g^{yz} \leftarrow (g^y)^z$. Next, *S* computes $W' \leftarrow g^{yz}.H(ID_C, ID_B, ID_S, g^w)^{pw_C}$ and $Y' \leftarrow g^{wz}.H(ID_B, ID_C, ID_S, g^y)^{pw_B}$ and then sends $W' \| Y'$ to *B*.

Step3a: *C* intercepts $W' \| Y'$ and modifies Y' as follows:

(i) *C* computes $g^{wz} \leftarrow Y'.H(ID_B, ID_C, ID_S, g^y)^{pw_B}$ where $g^y \leftarrow Y / N^{pw_B}$ (Y-received in step 1b, PW_B is determined by mounting undetectable on-line password guessing attack as shown in fig. 2, N is an element of G).

(ii) $Y'^* = g^{wz}.H(ID_B, ID_A, ID_S, g^y)^{pw_B}$ (To make *B* believe that it is communicating with *A*).

(iii) Now *C* sends $W' \| Y'^*$ to *B*.

Step3b: Upon receiving $W' \| Y'^*$, *B* uses PW_B to compute $g^{wz} \leftarrow Y'^*.H(ID_B, ID_A, ID_S, g^y)^{pw_B}$, and then uses y to compute $g^{wyz} = (g^{wz})^y$. Next, *B* computes $\alpha \leftarrow H(ID_A, ID_B, g^{wzy})$ and then forwards $W' \| \alpha$ to *A*. In the meanwhile *C* intercepts the message sent from *B*.

Step3c: *C* computes $g^{yz} \leftarrow W' / H(ID_C, ID_B, ID_S, g^w)^{pw_C}$, $g^{yzw} = (g^{yz})^w$. and $\beta \leftarrow H(ID_B, ID_A, g^{yzw})$ and then impersonates *A* to send β to *B*. In addition, *C* computes $SK_A \leftarrow H'(ID_A, ID_B, g^{yzw})$ as the session key for securing subsequent communications with B.

Step3d: Upon receiving β, *B* computes $H(ID_B, ID_A, g^{yzw})$. Since the computed $H(ID_B, ID_A, g^{yzw})$ is equal to the received β, *B* is convinced that g^{wzy} is valid. In addition, *B* computes $SK_B \leftarrow H'(ID_A, ID_B, g^{yzw})$ as the session key for securing subsequent communications. Clearly, *B* is believing that *C* is *A*, $SK_A = SK_B$, *C* can successfully impersonate *A* to communicate with *B*. Thus, the S-3 PAKE' protocol cannot resist the impersonation –of-initiator attack.

Figure 3 illustrates impersonation-of-initiator attack.

C	**B**	**C**	**S**
Public information : G, g, p, H, M, N			
Information shared between client and server *S* : PW_B, PW_C			
Information held by User *C* : PW_C			
Information held by User *B* : PW_B			
$w \in Z_p$			
$W \leftarrow g^w.M^{pw_C}$			
	$\xrightarrow{ID_A \| W}$	$y \in Z_p$	

ISSN 1512-1232

$Y = g^{y}.N^{PW_B}$

$\xrightarrow{ID_A||W||ID_B||Y}$

C intercept this message
and sends $ID_C \,||\, W \,||\, ID_B \,||\, Y$ to S

$g^{w} \leftarrow W / M^{pw_C}, g^{wz} \leftarrow (g^{w})^{z}$

$g^{yz} \leftarrow (g^{y})^{z}$

$W' \leftarrow g^{yz}.H(ID_C, ID_B, ID_S, g^{w})^{pw_C}$

$Y' \leftarrow g^{wz}.H(ID_B, ID_C, ID_S, g^{y})^{pw_B}$

$\xleftarrow{W'||Y'}$

Since C knows the password of B

$g^{y} \leftarrow Y / N^{pw_B}$

(Y-received, PW_B -determined by mounting
undetectable on-line password guessing attack, N-an element of G).

$g^{wz} \leftarrow Y'^{*}.H(ID_B, ID_A, ID_S, g^{y})^{pw_B}$

Y' will be modified

i.e. $Y'^{*} = g^{wz}.H(ID_B, ID_A, ID_S, g^{y})^{pw_B}$

$\xleftarrow{W'||Y'^{*}}$

$g^{wz} \leftarrow Y'^{*}.H(ID_B, ID_A, ID_S, g^{y})^{pw_B}$

$\alpha \leftarrow H(ID_A, ID_B, g^{wzy})$

$\xleftarrow{W'||\alpha}$ $g^{wyz} = (g^{wz})^{y}$

$g^{yz} \leftarrow W' / H(ID_C, ID_B, ID_S, g^{w})^{pw_C}$

verify α

$\beta \leftarrow H(ID_B, ID_A, g^{yzw})$

$SK_A \leftarrow H'(ID_A, ID_B, g^{yzw})$

$\xrightarrow{\beta}$ verify β

$SK_B \leftarrow H'(ID_A, ID_B, g^{yzw})$

Fig 3: Impersonation of Initiator attack on simple three party password authenticated key exchange' protocol.

3. B. Man-in-the middle attack

Step1a: A chooses a random number $x \in Z_p$ to compute $X \leftarrow g^{x}.M^{pw_A}$, and then $ID_A \,||\, X$ to B. In the meanwhile, *C* intercepts the message sent from *A*, and then chooses 2 random numbers $v \in Z_p$ and $w \in Z_p$ to compute $V \leftarrow g^{v}.N^{pw_C}$ and $W \leftarrow g^{w}.M^{pw_C}$, respectively. Next, *C* sends $ID_A \,||\, W$ to *B*.

Step1b: *B* chooses a random number $y \in Z_p$ to compute $Y \leftarrow g^{y}.N^{pw_B}$, and then sends ID_A, *W*, ID_B, *Y*, to *S*. In the meanwhile, *C* intercepts the message sent from *B*, and then sends ID_A, *W*, ID_C, *V*, and ID_C, *W*, ID_B, *Y*, to *S* to establish two concurrent sessions session$_1$ and session$_2$. The message ID_A, *X*, ID_C, *V* is used for the session$_1$ in which *C* impersonates *B* to respond to the request sent from *A*, and the message ID_C, *W*, ID_B, *Y* is used for the session$_2$ in which *C* impersonates *A* to initiate the instance of the protocol with *B*.

ISSN 1512-1232

Step2a: Upon receiving ID_A, X, ID_C, V in session1, S uses PW_A and PW_C to compute $g^x \leftarrow X / M^{pw_A}$ and $g^v \leftarrow V / N^{pw_C}$ respectively, according to the identifiers contained in the received message in addition, S chooses a random number $z_1 \in Z_p$ to compute $g^{xz_1} \leftarrow (g^x)^{z_1}$ and $g^{vz_1} \leftarrow (g^v)^{z_1}$. Next, S computes $X' = g^{vz_1}.H(ID_A, ID_C, ID_S, g^x)^{pw_A}$ and $V' = g^{xz_1}.H(ID_C, ID_A, ID_S, g^v)^{pw_C}$ and then sends $X' \| V'$ to C.

Step2b: Simultaneously, upon receiving $ID_C \| W \| ID_B \| Y$ in session2, S uses PW_C and PW_B to compute $g^w \leftarrow W / M^{pw_C}$ and $g^y \leftarrow Y / N^{pw_B}$ respectively, according to the identifiers contained in the received message in addition, S chooses a random number $z_2 \in Z_p$ to compute $g^{wz_2} \leftarrow (g^w)^{z_2}$ and $g^{yz_2} \leftarrow (g^y)^{z_2}$. Next, S computes $W' = g^{yz_2}.H(ID_C, ID_B, ID_S, g^w)^{pw_C}$ and $Y' = g^{wz_2}.H(ID_B, ID_C, ID_S, g^y)^{pw_B}$ and then sends $W' \| Y'$ to B.

Step3a: Upon receiving $X' \| V'$ in session$_1$, C computes $g^{xz_1} = V' / H(ID_C, ID_A, ID_S, g^v)^{pw_C}$ and $g^{xvz_1} = (g^{xz_1})^v$. Next, C computes $\lambda \leftarrow H(ID_A, ID_B, g^{xvz_1})$. Now, C will modify X' as follows:

(i) C calculates $g^{vz_1} = X' / H(ID_A, ID_C, ID_S, g^x)^{pw_A}$ [$g^x = X / M^{pw_A}$ where X is received in step 1a, M is an element in G, PW_A already obtained as shown in fig.2].

(ii) $X'^* = g^{vz_1}.H(ID_A, ID_B, ID_S, g^x)^{pw_A}$ [To make A believe that it is communicating with B].

(iii) Now C forwards $X'^* \| \lambda$ to A.

(iv) C computes $SK'_B = H'(ID_A, ID_B, g^{xvz_1})$ as the session key for securing subsequent communications with A in session$_1$.

Step3b: The message $W' \| Y'$ is sent from server to B. This is intercepted by C. C will modify Y' as follows:

(i) C computes $g^{wz_2} = Y' / H(ID_B, ID_C, ID_S, g^y)^{pw_B}$ [where $g^y \leftarrow Y / N^{pw_B}$, Y is received in step 1b from B, N is an element in G and PW_B is obtained by mounting Undetectable on-line dictionary attack as shown in fig.2].

(ii) Now $Y'^* = g^{wz_2}.H(ID_B, ID_A, ID_S, g^y)^{pw_B}$ [To make B believe that it is communicating with A].

(iii) Now C forwards $W' \| Y'^*$ to B.

Step3c: Simultaneously, upon receiving $W' \| Y'^*$ in session$_2$, B uses PW_B to compute $g^{wz_2} = Y^* / H(ID_B, ID_A, ID_S, g^y)^{pw_B}$, and then uses y to compute $g^{wz_2 y} = (g^{wz_2})^y$. Next, B computes $\gamma = H(ID_A, ID_B, g^{wyz_2})$, and then forwards $W' \| \gamma$ to A. In the meanwhile, C intercepts the message sent from B.

Step3d: Upon receiving $X'^* \| \lambda$ in session$_1$, A computes $g^{vz_1} = X'^* / H(ID_A, ID_B, ID_S, g^x)^{pw_A}$ and $g^{xvz_1} = (g^{vz_1})^x$, and then computes $H(ID_A, ID_B, g^{xvz_1})$. Since the computed $H(ID_A, ID_B, g^{xvz_1})$ is equal to the received hash value. A is convinced that g^{xvz_1} is valid. Next, A computes $\sigma = H(ID_A, ID_B, g^{xvz_1})$ and returns σ to B. In addition, A computes $SK_A = H'(ID_A, ID_B, g^{xvz_1})$ as the session key for securing subsequent communications in session$_1$. Simultaneously, in session$_2$, C computes $g^{yz_2} = W' / H(ID_C, ID_S, g^w)^{pw_C}$, $g^{wyz_2} = (g^{yz_2})^w$ and $\delta = H(ID_B, ID_A, g^{wyz_2})$ as the session key for securing subsequent communications with B in session$_2$.

Step3e: C intercepts σ sent by A to B in session$_1$. Simultaneously, upon receiving δ, B is convinced that g^{wyz_2} is valid. In addition, B computes $SK_B = H'(ID_A, ID_B, g^{wyz_2})$ as the session key for securing subsequent communications in session$_2$.

ISSN 1512-1232

Consequently, *A* believes *C* as *B* and B believes C as *A*. Since $SK_B' = SK_A$ and $SK_A' = SK_B$, *C* can decrypt all the ciphertexts transmitted between *A* and *B*. Thus, the S-3PAKE' protocol cannot resist man-in-the-middle attack.

3. C. Unknown Key Share attack on S-3 PAKE' protocol

Now let *A* and *B* want to establish a session. Then *C* acts as attacker (after mounting Undetectable on-line password guessing attack). Server believes that *A* and *C* wants to establish a session key. A believes that it is communicating with *B*. But *A* is actually communicating with *C* .

Step1a: A chooses a random number $x \in Z_p$ and compute $X \leftarrow g^x.M^{pw_A}$, and then sends $ID_A \| X$ to B.

A	**C**	**S**

Public information : G, g, p, H, M, N

Information shared between client and server *S* : PW_A, PW_C

Information held by User *C* : PW_A

Information held by User *B* : PW_C

$x \in Z_p$

$X \leftarrow g^x.M^{pw_A}$

$\xrightarrow{ID_A \| X}$

$w \in Z_p$

$W = g^w.N^{PW_C}$

$\xrightarrow{ID_A \| X \| ID_C \| W}$

$g^x \leftarrow X / M^{pw_A}$

$g^{xz} = (g^x)^z$

$g^w \leftarrow W / N^{pw_C}$

$g^{wz} = (g^w)^z$.

$X' = g^{wz}.H(ID_A, ID_C, ID_S, g^x)^{pw_A}$

$W' = g^{xz}.H(ID_C, ID_A, ID_S, g^w)^{pw_C}$

$\xleftarrow{X' \| W'}$

$g^{xz} \leftarrow W' / H(ID_C, ID_A, ID_S, g^w)^{pw_C}$

$\alpha \leftarrow H(ID_A, ID_B, g^{xzw})$

$g^{xzw} \leftarrow (g^{xz})^w$

Now, $g^x = X / M^{PW_A}$

(*X*-received from *A*, M-an element in G

PW_A-obtained by Undetectable on-line password guessing attack)

Find $g^{wz} \leftarrow X' / H(ID_A, ID_C, ID_S, g^x)^{pw_A}$

Compute $X'^* = g^{wz}.H(ID_A, ID_B, ID_S, g^x)^{PW_A}$

(i.e. X' is modified to make *A* believe that it is communicating with *B*)

$\xleftarrow{X'^* \| \alpha}$

$g^{wz} \leftarrow X'^* / H(ID_A, ID_C, ID_S, g^x)^{pw_A}$

verify α

$\beta = H(ID_B, ID_A, g^{xwz})$

ISSN 1512-1232

$SK_A \leftarrow H'(ID_A, ID_B, g^{xwz})$

$\xrightarrow{\beta}$ verify β

$SK_B \leftarrow H'(ID_A, ID_B, g^{xwz})$

Fig 4: Unknown Key share attack on simple three party password authenticated key exchange' protocol.

Step1b: *C* intercepts the message i.e. $ID_A \| X$. Upon receiving $ID_A \| X$, *C* also chooses a random number $w \in Z_p$ and computes $W \leftarrow g^w.N^{pw_C}$, then sends $ID_A \| X \| ID_C \| W$ to *S*.

Step2a: Upon receiving $ID_A \| X \| ID_C \| W$, the server *S* first uses the passwords PW_A and PW_C to compute $g^x \leftarrow X / M^{pw_A}$ and $g^w \leftarrow W / N^{pw_C}$ respectively.
Step2b: Then, she chooses another random number $z \in Z_p$ and computes $g^{xz} = (g^x)^z$, $g^{wz} = (g^w)^z$. Finally, she sends $X' \| W'$ to *B*, where $X' = g^{wz}.H(ID_A, ID_C, ID_S, g^x)^{pw_A}$ and $W' = g^{xz}.H(ID_C, ID_A, ID_S, g^w)^{pw_C}$

Step3a: Upon receiving $X' \| W'$, *C* computes $g^{xz} \leftarrow W' / H(ID_C, ID_A, ID_S, g^w)^{pw_C}$, $\alpha \leftarrow H(ID_A, ID_B, g^{xzw})$ and $g^{xzw} \leftarrow (g^{xz})^w$.
Step3b: X' is modified as follows to make *A* believe that it is communicating with *B*.
(i) C will find $g^{wz} \leftarrow X' / H(ID_A, ID_C, ID_S, g^x)^{pw_A}$
(ii) *C* computes $g^x = X / M^{PW_A}$ (*X* is received from *A* in step 1a, M is an element in G, PW_A is obtained by mounting Undetectable on-line dictionary attack as shown in fig.2).
(iii) *C* computes $X'^* = g^{wz}.H(ID_A, ID_B, ID_S, g^x)^{PW_A}$ and forwards $X'^* \| \alpha$.
Step3c: *A* computes $g^{wz} \leftarrow X'^* / H(ID_A, ID_C, ID_S, g^x)^{pw_A}$, $g^{wzx} \leftarrow (g^{wz})^x$ and verifies $H(ID_A, ID_B, g^{xwz})$ if the received α = computed α then *B* is authenticated by *A*.
Step3d: *A* computes the session key $SK_A \leftarrow H'(ID_A, ID_B, g^{xwz})$ and $\beta = H(ID_B, ID_A, g^{xwz})$ sends β to *B*.
Step3e: *B* verifies $\beta = H(ID_B, ID_A, g^{xwz})$ if the received β = computed β then *A* is authenticated by *B*. The session key $SK_B \leftarrow H'(ID_A, ID_B, g^{xwz})$ is determined.
Figure 4 illustrates impersonation-of-the responder attack.

4. CONCLUSION

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. Chung and Ku proved impersonation-of-initiator attack, an impersonation-of-responder attack, and a man-in-the-middle attack on S-3 PAKE protocol and proposed S-3 PAKE' protocol to avoid these attacks. Unlike their claims Phan et al., presented an Undetectable online dictionary attack on the above protocol. In the present paper, an impersonation-of-initiator attack, a man-in-the middle attack and an Unknown key share attack are demonstrated on

ISSN 1512-1232

S-3PAKE' protocol using the Undetectable online dictionary attack proposed by Phan et al. Hence S-3PAKE' protocols should be designed such that they resist all types of password guessing attacks.

References:

1. Ding. Y and Horster. P, "Undetectable on-line password guessing attacks", ACM Operat Syst Rev, Vol 29(4), pp.77– 86, 1995.
2. Diffie. W and Hellman. M, "New Directions in cryptography", IEEE Transactions on Information theory, Vol 22(6), pp. 644-654, 1976.
3. Abdalla . M, Chevassut . O, and Pointcheval. O, "One-time verifier-based encrypted key exchange", Proc. of PKC '05, Springer-Verlag, LNCS 3386, pp. 47–64. 2005.
4. Abdalla. M and Pointcheval. D, "Simple Password-Based Encrypted Key Exchange Protocols", Proc. of Topics in Cryptology - CT-RSA, Springer-Verlag, LNCS 3376, pp. 191-208, 2005.
5. Bellare. M, Pointcheval. D and Rogaway. P, "Authenticated key exchange secure against dictionary attacks", Proceedings of the 2000 Advances in Cryptology (EUROCRYPT'2000). Berlin, Germany: Springer-Verlag, pp. 139-155, 2000.
6. Bresson. E, Chevassut. O, and Pointcheval. D, « New security results on encrypted key exchange", Proc. PKC, Springer-Verlag,, LNCS 2947, pp. 145-158, Mar. 2004.
7. Kobara. K and Imai. H, "Pretty-simple password-authenticated key exchange under standard assumptions", IEICE Transactions, E85-A (10):pp.2229-2237, Oct. 2002.
8. Bellovin. S. M and Merritt. M, "Encrypted key exchange: Password-based protocols secure against dictionary attacks", Proc. 1992 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, pp. 72-84, May 1992.
9. Abdalla. M, Fouque. P. A and Pointcheval. D, "Password-based authenticated key exchange in the three-party setting", Proceedings of the 8th International Workshop on Theory and Practice in Public Key Cryptography (PKC'2005). Berlin, Germany: Springer-Verlag, pp.65-84, (2005). Full version appeared in IEE Information Security, Volume 153, Issue 1, pp. 27–39, March 2006.
10. Kim and Choi, "Enhanced Password-based simple three-party Key exchange protocol", Computers and Electrical Engineering, Vol 35(1), pp107-114, 2009.
11. Lee. S. W, Kim. H. S and Yoo. K. Y, "Efficient verifier-based key agreement for three-parties without server's public key", Applied Mathematics and Computation, 167(2), pp. 996-1003, 2005.
12. Lin. C. L, Sun. H. M and Hwang. T, "Three-party encrypted key exchange attacks and a solution", ACM Operating Systems Review, 34(4), pp.12-20, 2000.
13. Lin. C. L, Sun. H. M, Steiner. M and Hwang. T, "Three-party encrypted key exchange without server's public keys", IEEE Communications Letters, Vol 5(12), pp. 497-499, 2001.
14. Lu. R and Cao. Z, " Simple three-party key exchange protocol", Computers and Security, 26:pp.94-97, 2007.
15. Phan Raphael. C. W, Yau. W. C and Bok-Min. G, "Cryptanalysis of simple three- party key exchange protocol (S-3PAKE)", Information Science, Vol. 178, pp. 2849-2856, 2008.

Article received: 2011-12-10