World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:7, No:10, 2013

Cryptanalysis of Yang-Li-Liao's Simple Three-Party Key Exchange (S-3PAKE) Protocol

Hae-Soon Ahn, Eun-Jun Yoon

Abstract—Three-party password authenticated key exchange (3PAKE) protocols are widely deployed on lots of remote user authentication system due to its simplicity and convenience of maintaining a human-memorable password at client side to achieve secure communication within a hostile network. Recently, an improvement of 3PAKE protocol by processing a built-in data attached to other party for identity authentication to individual data was proposed by some researchers. However, this paper points out that the improved 3PAKE protocol is still vulnerable to undetectable on-line dictionary attack and off-line dictionary attack.

Keywords—Three-party key exchange, 3PAKE, Password-authenticated key exchange, Network security, Dictionary attack

I. Introduction

Three-party password-based authenticated key exchange (3PAKE) protocols allow users to communicate securely over public networks simply by using easy-to-remember passwords for the client-client-server architecture [1], [2], [3], [4], [5], [6]. In the 3PAKE protocols,, each client shares his/her password with a trusted server and resorts to the server to authenticate the peer for establishing a secure session key [7].

However, password-based 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 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 dictionary attacks on the password-based protocols should be considered a real possibility [8].

In general, the dictionary attacks can be divided into three classes [7], [8], [9] as follows:

- *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.
- *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.
- *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.

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).

TABLE I
Notations used in Yang et al.'s S-3PAKE protocol

G, q, g	A cyclic group G of prime order q generated by an element g.
M, N	The elements in a represent group G.
S	A trusted server.
A, B	Two communication parties.
x, y, z	Random exponents selected by A, B and S.
pw_A	The shared password between A and S.
pw_B	The shared password between B and S.
$H_1(\cdot), H_2(\cdot), H_3(\cdot)$	Three secure one-way hash functions.
$A \rightarrow B : M$	A sends message M to B.

In 2007, Lu and Cao [10] proposed a simple 3PAKE protocol (in short, S-3PAKE) built upon the earlier two-party PAKE protocol due to Abdalla and Pointcheval [11]. However, it is founded out that S-3PAKE is vulnerable to various attacks according to recent works in [8], [9], [12], [13], [14], [15].

In 2008, Guo et al. [13] proposed a new S-3PAKE protocol which users execute the 2-PAKE protocol with a sever to generate a message authentication code (MAC) in advance before the server can authenticate the real identity of both communication parties.

In 2009, Yang et al. [16], however, proposed an improved solution based on the Gue et al.'s protocol without executing the 2-PAKE protocol in advance. They claimed that the improved S-3PAKE protocol can secure to various attacks like on-line dictionary attacks, off-line dictionary attack, man-in-the-middle attack, unknown key-share attack, and so on.

However, this paper points out that Yang et al.'s S-3PAKE protocol is still vulnerable to undetectable on-line dictionary attack and off-line dictionary attack unlike their claim in which an attacker exhaustively enumerates all possible passwords in an on-line or off-line manner to determine the correct one.

The remainder of this paper is organized as follows. We subsequently review Yang et al.'s S-3PAKE protocol in Section 2. The undetectable on-line dictionary attack and off-line dictionary attack on the Yang et al.'s S-3PAKE protocol are presented in Section 3. Finally, we draw some conclusions in Section 4.

II. Review of Yang et al.'s S-3PAKE Protocol

This section reviews the Yang et al.'s S-3PAKE protocol [16]. Throughout the paper, notations are employed in Table

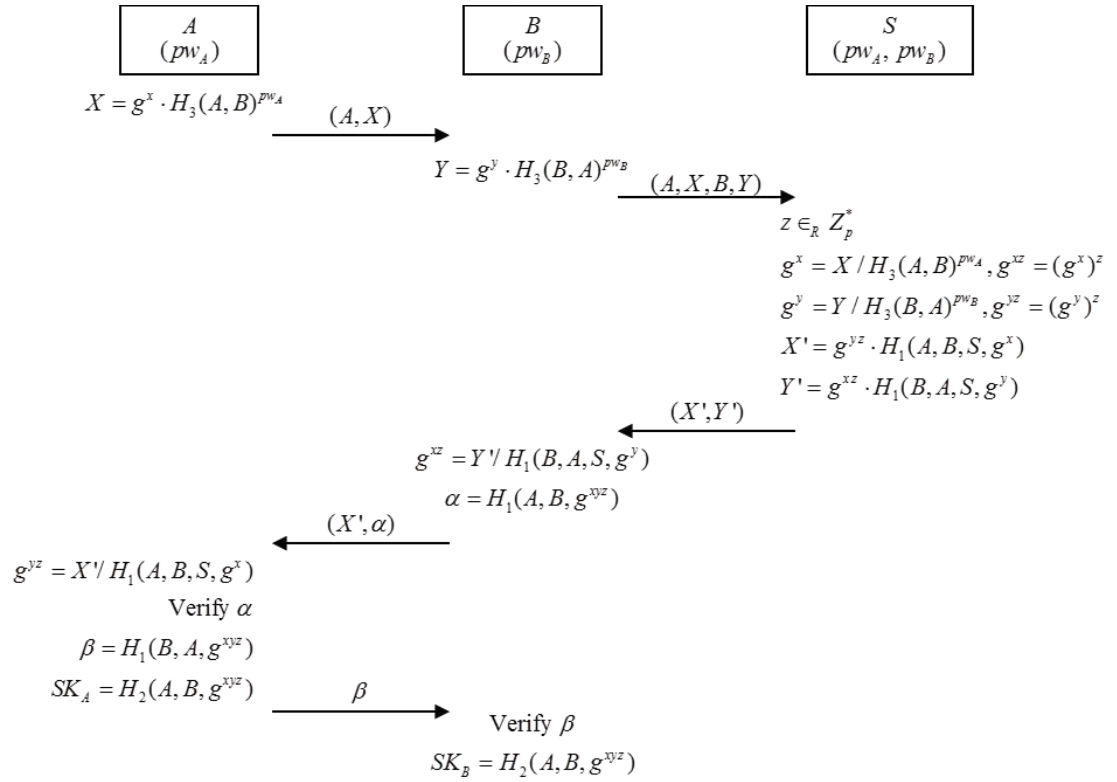

Fig. 1. Yang et al.'s simple three-party key exchange protocol(S-3PAKE) protocol.

I. Fig. 1 depicts the Yang et al.'s S-3PAKE protocol, which works as follows.

1) $A \to B$: (A, X)
   A selects a random number $x \in Z_p^*$ and computes
   $$X = g^x \cdot H_3(A,B)^{pw_A} \quad (1)$$
   and then sends (A, X) to B.
2) $B \to S$: (A, X, B, Y)
   B selects a random number $y \in Z_p^*$ and computes
   $$Y = g^y \cdot H_3(B,A)^{pw_B} \quad (2)$$
   and then sends (A, X, B, Y) to S.
3) $S \to B$: (X', Y')
   Upon receiving (A, X, B, Y), the server S first uses the passwords pw_A and pw_B to compute
   $$g^x = X / H_3(A,B)^{pw_A} \quad (3)$$
   and
   $$g^y = Y / H_3(B,A)^{pw_B} \quad (4)$$
   respectively.
   Next, S selects a random number $z \in Z_p^*$ and computes $g^{xz} = (g^x)^z$ and $g^{yz} = (g^y)^z$. S then computes
   $$X' = g^{yz} \cdot H_1(A,B,S,g^x) \quad (5)$$
   and
   $$Y' = g^{xz} \cdot H_1(B,A,S,g^y) \quad (6)$$
   and sends (X', Y') to B.
4) $B \to A$: (X', α)
   Upon receiving $(X'||Y')$, B computes
   $$g^{xz} = Y' / H_1(B,A,S,g^y) \quad (7)$$
   and
   $$\alpha = H_1(A,B,g^{xyz}) \quad (8)$$
   and then sends (X', α) to A.
5) $A \to B$: β
   Upon receiving $(X'||\alpha)$, A computes
   $$g^{yz} = X' / H_1(A,B,S,g^x) \quad (9)$$
   and checks whether
   $$H_1(A,B,g^{xyz}) ? = \alpha \quad (10)$$
   holds or not. If it does not hold, A stops executing the protocol. Otherwise, A believes that client B is valid and computes the session key
   $$SK_A = H_2(A,B,g^{xyz}) \quad (11)$$
   Then, A sends
   $$\beta = H_1(B,A,g^{xyz}) \quad (12)$$
   to B.
6) Upon receiving β, B checks whether
   $$H_1(B,A,g^{xyz}) ? = \beta \quad (13)$$
   hold or not. If it does hold, B believes that client A is valid and computes the session computes
   $$SK_B = H_2(A,B,g^{xyz}) \quad (14)$$

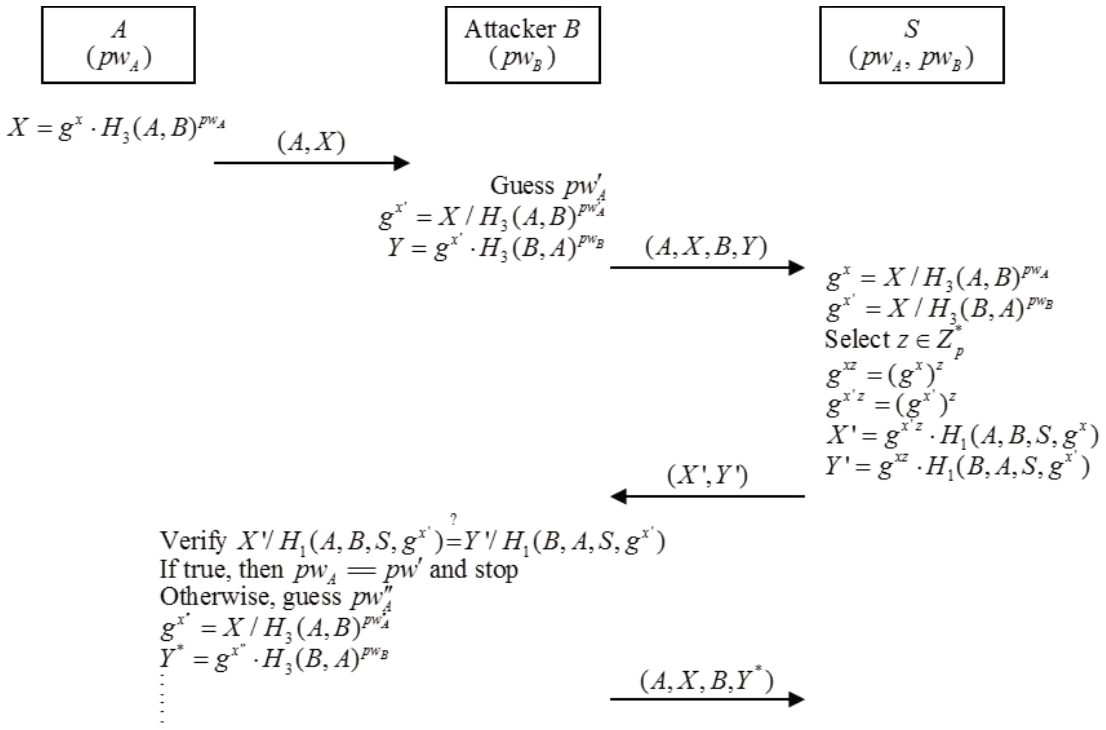

Fig. 2. Undetectable on-line dictionary attack scenario on Yang et al.'s S-3PAKE protocol.

Otherwise, B aborts the protocol.

Finally, both A and B share a common session key $SK_A = SK_B = H_2(A, B, g^{xyz})$.

III. Cryptanalysis of Yang et al.'s S-3PAKE Protocol

This section proofs that Yang et al.'s S-3PAKE protocol [16] is not secure to undetectable on-line dictionary attacks by any other user and off-line dictionary attacks. First, we define the security term needed for security problem analysis of the Yang et al.'s S-3PAKE protocol as follows:

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

A. Undetectable on-line dictionary attack

The *undetectable on-line dictionary attack* scenario is outlined in Fig. 2. A malicious user B with helping a legal user A can perform the following "undetectable on-line dictionary attack".

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 Yang et al.'s S-3PAKE protocol in Fig. 1. B guesses a password pw'_A, and establishes an authenticated and private channel with S. B first computes

$$g^{x'} = X/H_3(A,B)^{pw'_A} \tag{15}$$

for an unknown element $x' \in Z_p^*$. Then, B computes

$$Y = g^{x'} \cdot H_3(B,A)^{pw_B} \tag{16}$$

and sends (A, X, B, Y) to S.

3) $S \rightarrow B$: (X', Y')
   Upon receiving (A, X, B, Y), the server S first will recover g^x and $g^{x'}$ by computing

$$g^x = X/H_3(A,B)^{pw_A} \tag{17}$$

$$g^{x'} = Y/H_3(B,A)^{pw_B} \tag{18}$$

Next, S will select a random number $z \in Z_p^*$ and compute

$$g^{xz} = (g^x)^z \tag{19}$$

$$g^{x'z} = (g^{x'})^z \tag{20}$$

S then will compute

$$X' = g^{x'z} \cdot H_1(A,B,S,g^x) \tag{21}$$

and

$$Y' = g^{xz} \cdot H_1(B,A,S,g^{x'}) \tag{22}$$

and will send (X', Y') to B.

4) When B receives (X', Y'), B checks if the following equation holds or not

$$X'/H_1(A,B,S,g^{x'}) \stackrel{?}{=} Y'/H_1(B,A,S,g^{x'}) \tag{23}$$

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

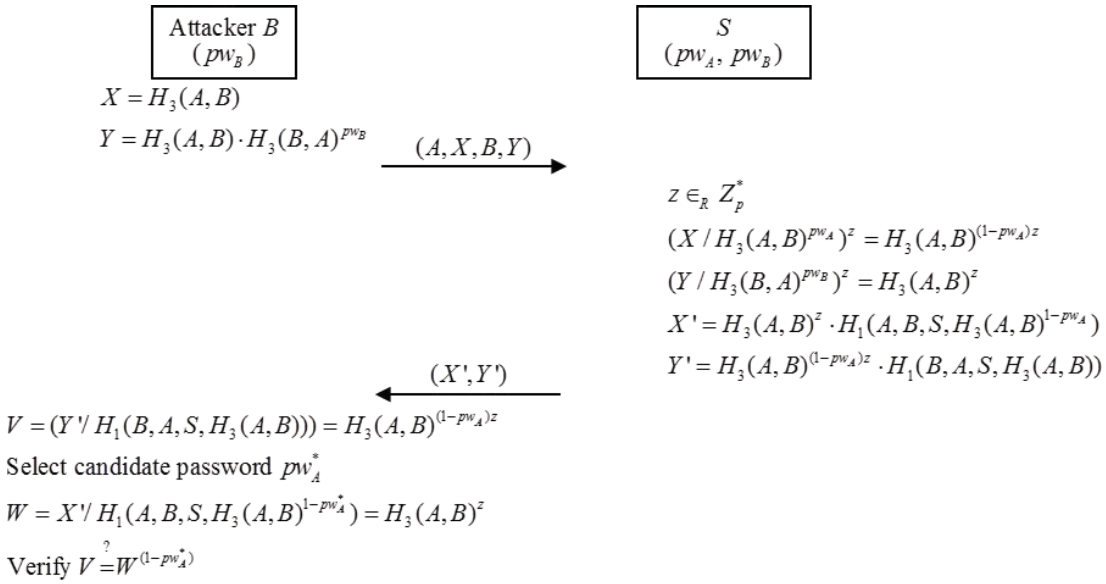

Fig. 3. Off-line dictionary attack scenario on Yang et al.'s S-3PAKE protocol.

5) Otherwise, B repeatedly performs the steps (2)-(4) without being noticed by S. For example, B guesses another password pw_A'', and computes

$$g^{x''} = X/H_3(A,B)^{pw_A''} \quad (24)$$

and

$$Y^* = g^{x''} \cdot H_3(B,A)^{pw_B} \quad (25)$$

Then, B sends (A,X,B,Y^*) to S.

It is clear that if $pw_A' = pw_A$, then $g^{x'z} = g^{xz}$. Therefore, $g^{x'} = g^x$.

B. Off-line dictionary attack

The *off-line dictionary attack* scenario is outlined in Fig. 3. A malicious user B without helping a legal user A can perform the following "off-line dictionary attack".

1) $B \to S$: (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

$$X = H_3(A,B) \quad (26)$$

$$Y = H_3(A,B) \cdot H_3(B,A)^{pw_B} \quad (27)$$

Finally, B sends (A,X,B,Y) to S.

2) $S \to B$: (X',Y')
Upon receiving (A,X,B,Y), S will select a random number $z \in Z_p^*$ and then compute

$$(X/H_3(A,B)^{pw_A})^z = H_3(A,B)^{(1-pw_A)z} \quad (28)$$

and

$$(Y/H_3(B,A)^{pw_B})^z = H_3(A,B)^z \quad (29)$$

S then will compute

$$X' = H_3(A,B)^z \cdot H_1(A,B,S,H_3(A,B)^{1-pw_A}) \quad (30)$$

$$Y' = H_3(A,B)^{(1-pw_A)z} \cdot H_1(B,A,S,H_3(A,B)) \quad (31)$$

Finally, S will send (X',Y') to B.

3) When B receives (X',Y'), B first compute

$$V = Y'/H_1(B,A,S,H_3(A,B)) = H_3(A,B)^{(1-pw_A)z} \quad (32)$$

Then, B selects a candidate password pw_A' and then computes

$$W = X'/H_1(A,B,S,H_3(A,B)^{1-pw_A'}) = H_3(A,B)^z \quad (33)$$

S checks if the following equation holds or not

$$V \stackrel{?}{=} W^{(1-pw_A')} \quad (34)$$

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

4) If it is not correct, B chooses another password pw_A'' and repeatedly performs above step (3) until

$$V \stackrel{?}{=} W^{(1-pw_A'')} \quad (35)$$

It is clear that if $pw_A' = pw_A$, then

$$W^{(1-pw_A')} = H_3(A,B)^{z(1-pw_A')} = V \quad (36)$$

IV. Conclusions

This paper pointed out that Yang et al.'s S-3PAKE protocol is still vulnerable to undetectable on-line dictionary attack and off-line dictionary attack unlike their claim in which an attacker exhaustively enumerates all possible passwords in an on-line or off-line manner to determine the correct one. For this reason, Yang et al.'s S-3PAKE protocol is insecure for practical application. Further works will be focused on improving the Yang et al.'s S-3PAKE protocol which can be able to provide greater security and to be more efficient than the existing S-3PAKE protocols by an accurate performance analysis.

ACKNOWLEDGEMENTS

This work was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(No. 2010-0010106) and partially supported by the MSIP(Ministry of Science, ICT & Future Planning) support program (NIPA-2013- H0301-13-2004) supervised by the NIPA(National IT Industry Promotion Agency).

REFERENCES

[1] S.-M. Bellovin, and M. Merrit, "Encrypted key exchange: password based protocols secure against dictionary attacks," In: Proceedings of IEEE symposium on research in security and privacy. IEEE Computer Society Press, pp. 72-84, May 1992

[2] C.-L. Lin, H.-M. Sun, and T. Hwang, "Three party-encrypted key exchanges: attacks and a solution," ACM Operating Systems Review, vol. 34, no. 4, pp. 12-20, 2000.

[3] C.-L. Lin, H.-M. Sun, M. Steiner, and T. Hwang, "Three-party encrypted key exchange without server public-keys," IEEE Communication Letters, vol. 5, no. 12, pp. 497-499, 2001.

[4] L. Law, A. Menezes, M. Qu, J. Solinas and S.Vanstone, "An efficient protocol for authenticated key agreement," Designs, Codes and Cryptography, vol. 28, no. 2, pp. 119-134, March 2003.

[5] C.-C. Chang, and Y.-F. Chang, "A novel three-party encrypted key exchange protocol," Computer Standards and Interfaces, vol. 26, no. 5, pp. 471-476, 2004.

[6] T.-F. Lee, T. Hwang, and C.-L. Lin, "Enhanced three-party encrypted key exchange without server public keys, Computers & Security, vol. 23, no. 7, pp. 57-577, 2004

[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.

[9] 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.

[10] R. Lu and Z. Cao, "Simple three-party key exchange protocol," *Computers & Security*, vol. 26, no. 1, pp. 94-97, 2007.

[11] M. Abdalla and D. Pointcheval, "Simple password-based encrypted key exchange protocols," in P*roc. CT-RSA'05*, LNCS vol. 3376, pp. 191-208, 2005.

[12] H.-R. Chung and W.-C. Ku, "Three weaknesses in a simple three-party key exchange protocol," *Inform. Sciences*, vol. 178, no. 1, pp. 220.229, 2008.

[13] H. Guo, Z. Li, Y. Mu, and X. Zhang, "Cryptanalysis of simple threeparty key exchange protocol," *Computers & Security*, vol. 27, no. 1, pp. 16-21, 2008.

[14] R. C.-W. Phan, W.-C. Yau, and B.-M. Goi, "Cryptanalysis of simple three-party key exchange protocol (S-3PAKE)," *Inform. Sciences*, vol. 178, no. 13, pp. 2849-2856, 2008.

[15] J. Nam, J. Paik, H.-K. Kang, U.-M. Kim, and D. Won, "An off-line dictionary attack on a simple three-party key exchange protocol," *IEEE Commun. Lett.*, vol. 13, no. 3, pp. 205-207, 2009.

[16] F.-Y. Yang, W.-H. Li, and C.-M. Liao, "An enhanced of simple three-party key exchange protocol," *International Journal of Advanced Information Technologies (IJAIT)*, vol. 3, no. 2, pp. 121-134, 2009.