Institute of Advanced Engineering and Science

International Journal of Information and Network Security (IJINS)
Vol.1, No.1, April 2012, pp. 37~40
ISSN : 2089-3299

A Password attack on S-3 PAKE Protocol

SHIRISHA TALLAPALLY
Malla Reddy Engineering College
Secunderabad, Andra Pradesh, India
e-mail: shirisha27@yahoo.co.in

Abstract

Recently Chung et al proposed three party authenticated key exchange protocol. Lo et al demonstrated that Chung et al protocol is vulnerable to undetectable online dictionary attack and proposed a modified protocol. Unfortunately, this paper shows that Lo et al protocol is not secure and suffers from undetectable online password guessing attack.

Keywords: *undetectable online password gueeing attack, PAKE protocol*

1. Introduction

Password based three party authenticated key exchange protocols are extensively used in network communications due to its simplicity. In three party key exchange protocol, the two clients will depends on the server to establish a secure session key, where the server provides session key to the two clients, but the server will not be able to gain any information on the value of that session key. People choose easily remembrable passwords, hence passwords are tend to various types of attacks. 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.

In 2007, Lu cao proposed three party PAKE protocol [2]. In 2008, Chung and ku [3] pointed out impersonation of initiator attack, impersonation of responder attack and man in the middle attack on Lu Cao protocol and proposed a countermeasure. Later Lo et al [4] pointed out that Chung and ku protocol suffers from undetectable online attack and proposed an enhanced protocol. However, their enhanced protocol still suffers from undetectable online password guessing attack.

The paper is organized as follows: section 2 briefly reviews Lo et al protocol, section 3 describes undetectable online password guessing attack on Lo et al protocol and the concluding remarks are given in section 4.

2. Lo yeh Chiang protocol:

In this section, we review Lo et al S-3 PAKE protocol.

Step1: $A \to B : H^2(ID_A) \| X$

A generates a random number $x \in Z_P$, and calculates $H^2(ID_A)$ and $X = (g^x \| H(g^x, ID_A)).M^{H2(PW_1)}$. Next A sends $H^2(ID_A) \| X$ to B as a communication request.

Step 2: $B \to S : H^2(ID_A) \| X \| H^2(ID_B) \| Y$

Received March 30, 2012; Accepted April 15, 2012

Similarly B generates a random number $y \in Z_P$, and calculates $H^2(ID_B)$ and $Y = (g^y \| H(g^y, ID_B)).N^{H2(PW_2)}$.then B sends $H^2(ID_A) \| X \| H^2(ID_B) \| Y$ to the trusted server S.

Step 3: $S \to B : X' \| Y'$

S calculates $(g^x \| H(g^x, ID_A)) \leftarrow X / M^{H2(PW_1)}$ and verifies if $H(g^x, ID_A)$ holds or not. If it holds then S selects a random number $z \in Z_P$, and finds $g^{xz} \leftarrow (g^x)^z$. Similarly, S also calculates $(g^y \| H(g^y, ID_B)) \leftarrow Y / N^{H2(PW_2)}$ and verifies if $H(g^y, ID_B)$ holds or not. If it holds then S finds $g^{yz} \leftarrow (g^y)^z$, $X' \leftarrow g^{yz}.H(H^2(ID_A), H^2(ID_B), ID_s, H(PW_1), g^x)^{H(ID_A)}$ and $Y' \leftarrow g^{xz}.H(H^2(ID_B), H^2(ID_A), ID_s, H(PW_2), g^y)^{H(ID_B)}$.

Step 4: $B \to A : X' \| \alpha$

Upon receiving X' and Y', B utilizes its identity ID_B and password PW_2 to retrieve $g^{xz} \leftarrow Y' / H(H^2(ID_B), H^2(ID_A), ID_s, H(PW_2), g^y)^{H(ID_B)}$. After that, B computes $g^{xyz} \leftarrow (g^{xz})^y$ and $\alpha \leftarrow H(H^2(ID_A), H^2(ID_B), g^{xyz})$

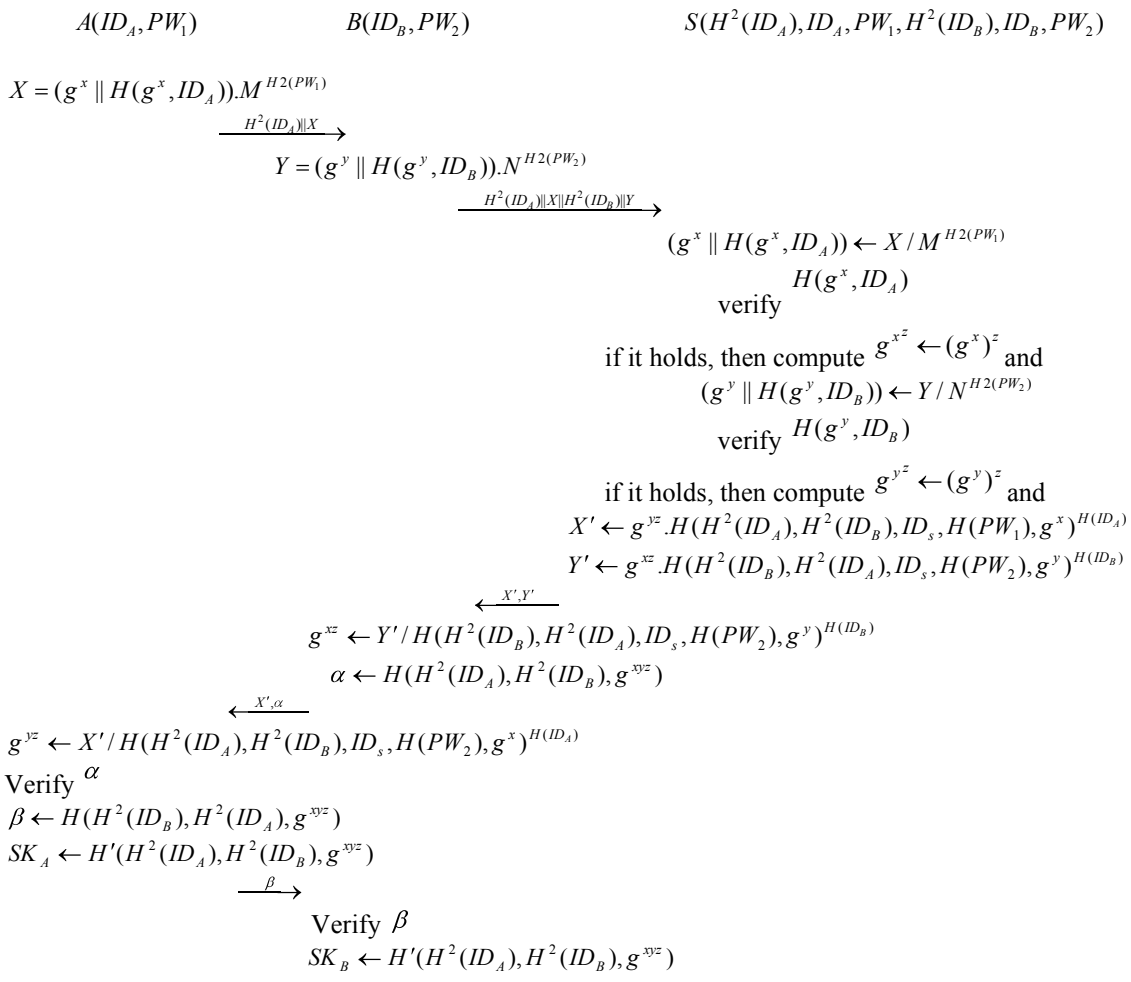

Fig 1. Lo Yeh Chiang protocol

Step 5: $A \rightarrow B : \beta$

Upon receiving $X' \| \alpha$, A utilizes its identity ID_A and password PW_1 to retrieve $g^{yz} \leftarrow X' / H(H^2(ID_A), H^2(ID_B), ID_s, H(PW_1), g^x)^{H(ID_A)}$. After that, A computes $g^{xyz} \leftarrow (g^{yz})^x$ and verifies $\alpha \leftarrow H(H^2(ID_A), H^2(ID_B), g^{xyz})$, if the received α is equal to computed α then B is authenticated by A. Now, A calculates $\beta \leftarrow H(H^2(ID_B), H^2(ID_A), g^{xyz})$ and sends β to B.

Now B calculates $\beta \leftarrow H(H^2(ID_B), H^2(ID_A), g^{xyz})$, if the received β is equal to calculated β, then A is authenticated by B. Finally A and B finds the key $SK_A = SK_B = H'(H^2(ID_A), H^2(ID_B), g^{xyz})$

Fig 1 shows Lo et al protocol.

3. Undetectable online attack on Lo et al protocol

In this section, we demonstrate undetectable online attack on Lo et al protocol

If ID_A is exposed (since identities of clients are not generally secret), B can mount undetectable online password guessing attack on Lo et al protocol

Step1: $A \rightarrow B : H^2(ID_A) \| X$

A generates a random number $x \in Z_P$, and calculates $H^2(ID_A)$ and $X = (g^x \| H(g^x, ID_A)).M^{H2(PW_1)}$. Next A sends $H^2(ID_A) \| X$ to B as a communication request.

Step 2: B guesses a password PW_1^* and finds $M^{H2(PW_1^*)}$

Step 3: Now, B calculates $X / M^{H2(PW_1^*)} \approx g^{x^*}$ [X is sent by A to B]

Step 4: Calculate $H(g^{x^*}, ID_A)$

Step 5: Let $g^{x^*} = g^y$, now B finds $Y = (g^y \| H(g^y, ID_B)).N^{H2(PW_2)}$

Step 6: B sends $H^2(ID_A) \| X \| H^2(ID_B) \| Y$ to S

Step 7: S calculates $(g^x \| H(g^x, ID_A)) \leftarrow X / M^{H2(PW_1)}$ and verifies if $H(g^x, ID_A)$ holds or not. If it holds then S selects a random number $z \in Z_P$, and finds $g^{xz} \leftarrow (g^x)^z$. Similarly, S also calculates $(g^y \| H(g^y, ID_B)) \leftarrow Y / N^{H2(PW_2)}$ and verifies if $H(g^y, ID_B)$ holds or not. If it holds then S finds $g^{yz} \leftarrow (g^y)^z$, $X' \leftarrow g^{yz}.H(H^2(ID_A), H^2(ID_B), ID_s, H(PW_1), g^x)^{H(ID_A)}$ and $Y' \leftarrow g^{xz}.H(H^2(ID_B), H^2(ID_A), ID_s, H(PW_2), g^y)^{H(ID_B)}$ and sends X', Y' to B.

Step 8: B finds $g^{xz} \leftarrow Y' / H(H^2(ID_B), H^2(ID_A), ID_s, H(PW_2), g^y)^{H(ID_B)}$ and $g^{yz} \leftarrow X' / H(H^2(ID_A), H^2(ID_B), ID_s, H(PW^*_1), g^{x^*})^{H(ID_A)}$. If $g^{xz} = g^{yz}$, the the guesses password PW_1^* is correct.

Else, guess one more password and repeat step 2-step 6 and step 8.

Figure 2 shows undetectable online password guessing attack on Lo et al protocol.

$A(ID_A, PW_1)$ $B(ID_B, PW_2)$ $S(H^2(ID_A), ID_A, PW_1, H^2(ID_B), ID_B, PW_2)$

$X = (g^x \| H(g^x, ID_A)).M^{H2(PW_1)}$

$\xrightarrow{H^2(ID_A)\|X}$

guess password PW_1^*

find $M^{H2(PW_1^*)}$

Now find $X / M^{H2(PW^*{}_1)} \approx g^{x*}$ |

Calculate $H(g^{x^*}, ID_A)$

let $g^{x^*} = g^y$

$Y = (g^y \| H(g^y, ID_B)).N^{H2(PW_2)}$

$\xrightarrow{H^2(ID_A)\|X\|H^2(ID_B)\|Y}$

$(g^x \| H(g^x, ID_A)) \leftarrow X / M^{H2(PW_1)}$

$H(g^x, ID_A)$

verify

if it holds, then compute $g^{xz} \leftarrow (g^x)^z$ and

$X' \leftarrow g^{yz}.H(H^2(ID_A), H^2(ID_B), ID_s, H(PW_1), g^x)^{H(ID_A)}$

$(g^y \| H(g^y, ID_B)) \leftarrow Y / N^{H2(PW_2)}$

$H(g^x, ID_A)$

verify

if it holds, then compute $g^{yz} \leftarrow (g^y)^z$ and

$Y' \leftarrow g^{xz}.H(H^2(ID_B), H^2(ID_A), ID_s, H(PW_2), g^y)^{H(ID_B)}$

$\xleftarrow{X', Y'}$

$g^{xz} \leftarrow Y' / H(H^2(ID_B), H^2(ID_A), ID_s, H(PW_2), g^y)^{H(ID_B)}$

$g^{yz} \leftarrow X' / H(H^2(ID_A), H^2(ID_B), ID_s, H(PW^*{}_1), g^{x^*})^{H(ID_A)}$

If $g^{xz} = g^{yz}$ then the guessed password is correct

Fig 2. Undetectable online password guessing attack on Lo Yeh Chiang protocol

4. Conclusion

Lo et al proposed security enhanced S-3 PAKE protocol. However, this paper had shown that their protocol suffers from undetectable online password guessing attack.

References:

[1] Ding Y, Horster P., "Undetectable on-line password guessing attacks" *ACM Operat Syst Rev*, vol. 29, no. 4, pp. 77– 86, 1995.

[2] R. Lu, Z. Cao, "Simple three-party key exchange protocol", *Computers and Security*, vol. 26, pp. 94-97, 2007.

[3] H.Chung, W. Ku, "Three Weaknesses in a simple three-party key exchange protocol", Information Sciences, vol. 178, pp. 220-229, 2008.

[4] N.W. Lo, Kuo-Hui Yeh and Meng-Chih Chiang, "Cryptanalysis of a Simple Three-Party Key Exchange Protocol", Joint Workshop on Information Security, http://jwis2009.nsysu.edu.tw/location/paper/Cryptanalysis%20of%20a%20Simple%20Three-party%20Key%20Exchange%20Protocol.pdf, 2009