

Cryptanalysis of a User Authentication Protocol

Zuowen Tan

School of Information Technology, Jiangxi University of Finance and Economics,
Nanchang City 330013, Jiangxi Province, P.R. China
Email: tanzyw@yahoo.com.cn

Abstract—Recently, Peyravin and Jeffries proposed a password-based practical authentication scheme using one-way collision-resistant hash functions. However, Shim and Munilla independently showed that the scheme is vulnerable to off-line guessing attacks. Hölbl, Welzer and Brumenn presented an improved password-based protocols. In the paper, we showed that the improved scheme still suffers from off-line guessing attacks on user authentication protocol and Denial-of-Service attacks on password change protocol.

Index Terms—authentication; password; identity-based; impersonation attack

I. INTRODUCTION

People always are faced with many potential security threats over insecure network, such as the communication channel could be eavesdropped, the message transmitted could be modified and impersonation attacks could be mounted. User Authentication enables a legitimate user to login onto a remote server. The authentication method based on password is the most commonly used technique to provide the authentication between the server and the remote user. The identity information of users is usually considered to be public information whereas passwords are considered to be private or secret information. Lamport proposed the first password authentication scheme [1] to provide authentication between the legal users and the remote server. Since then, many password-based remote user authentication schemes have been proposed [2-7]. Over the public network, the authentication scheme should provide mutual authentication, which does not only make the server verify the user but also a user can verify identity of the remote server.

The authentication schemes based on password can be further classified into two categories: encryption-based authentication and hash-function-based authentication. Encryption-based authentication employs symmetric key cryptosystems such as DES, AES etc. or public key cryptosystems such as RSA, ElGamal, etc. [8,9].

In an encryption-based authentication scheme, encryption often is employed for protecting passwords transferred over public networks. Encryption and decryption of passwords imposes additional cost overhead on the user and remote server. In encryption-based

authentication schemes, the sender and receiver of the password messages know the operative encryption and decryption schemes. Thus, the main disadvantage of the encryption-based password authentication schemes is high computational cost.

In 2000, Peyravian and Zunic proposed authentication schemes [10] for remote user authentication, password change and session key establishment over insecure networks, which are not based on cryptosystems. Their schemes are based only on the one-way collision-resistant hash functions. These functions can map efficiently binary strings of arbitrary length to binary strings of some fixed length. Furthermore, it is computationally infeasible to find two distinct inputs which hash to a common value; given a specific hash value, it is computationally infeasible to find the input. Since a hash-function-based user authentication is simpler and efficient, more and more hash-function-based user authentication schemes are proposed [11]. Unfortunately, Hwang and Yeh [12] pointed that Peyravian and Zunic's schemes suffer from password guessing attacks, stolen-verifier attacks and denial-of-service attacks. Lee et al. and Yoon et al. proposed their improved versions [11, 13] to enhance security of the Peyravian-Zunic scheme, respectively. However, Ku et al. showed [14] that these schemes still suffers from the same weaknesses of Peyravian-Zunic scheme.

Recently, Peyravian and Jeffries [15] pointed that protocols based on collision-resistant hash function suffer from an off-line password guessing attack. Peyravian and Jeffries combined the Diffie-Hellman (DH) key agreement [16] into a collision-resistant hash function technique to overcome the above mentioned weaknesses. However, Shim [17] and Munilla et al. [18] presented an off-line dictionary attack on the Peyravian-Jeffries's scheme, respectively. Shim also presented a Denial-of-Service attack [17] on Peyravian-Jeffries's scheme. Based on Peyravian-Jeffries's scheme, Hölbl, Welzer and Brumenn employed the Diffie-Hellman (DH) key agreement scheme and collision resistant hash functions to construct an improved remote user authentication protocol and password change protocol presented in [19]. The author claimed that the improved protocol provides protection against off-line password-guessing attacks. Jorge Munilla and Alberto Peinado found a passive off-line password-guessing attack on it [20].

In this paper, we will analyze the security of Hölbl-Welzer-Brumenn's authentication protocol and password change protocol. The analysis shows that the scheme is not still immune to a different off-line password-guessing attack and Denial-of-Service attack.

Manuscript received July 18, 2009; revised August 28, 2009; accepted October 1, 2009.

Supported by the National Natural Science Foundation of China (10961013 and 10701040).

Corresponding author: Zuowen Tan

The rest of the paper is organized as follows. In Section 2, we review Hölbl-Welzer-Brumenn's scheme. In Section 3, we analyze the security flaws of the scheme during the remote user authentication and password change. Finally, conclusion will be given in Section 4.

II. BRIEF REVIEWS OF HÖLBL -WELZER-BRUMENN'S SCHEME

In this section, we briefly review Hölbl et al's scheme. Hölbl et al's scheme is composed of a user authentication protocol and a password change protocol. Based on Diffie-Hellman key agreement and a collision-resistant hash function, their scheme makes use of additional exclusive-or operations to withstand the man-in-the-middle attack and the off-line dictionary attack. The scheme consists of the registration, login and authentication phases. Here we introduce the notations used throughout the paper.

- C, S : a client and a server, respectively.
- idi : user U_i 's identity.
- pw $_i$: user U_i 's password.
- p : a large prime number.
- g : a primitive element in GF(p).
- H : a collision-resistant one-way hash function.
- idpw_digi: $H(\text{idi}, \text{pw}_i)$.
- \oplus : exclusive or operation.

A. Review of Hölbl et al's user authentication protocol

In the Hölbl et al's scheme, the user authentication protocol consists of the following six steps.

Step 1 The user U_i submits id_i and pw_i to Client C . C then generates a random value r_c , chooses a large prime p and a primitive element $g \in GF(p)$ and a large random integer $x < p-1$. Then C computes $g^x \pmod{p}$ and masks it by computing $m_g^x = g^x \oplus H(id_i, idpw_digi)$, where $idpw_digi = H(id_i, pw_i)$ and has been stored by Server S . C sends $\{id_i, r_c, p, g, m_g^x\}$ to Server S .

Step 2 After receiving the messages, S chooses a random value r_s and a large random integer $y < p-1$ and computes $g^y \pmod{p}$. S calculates $g^x = m_g^x \oplus H(id_i, idpw_digi)$ and then $g^{xy} \pmod{p}$. Next, S generates a one-time challenge token as follows:

$$\begin{aligned} ch_1 &= r_s \oplus H(g^{xy}; idpw_digi; r_c), \\ ch_2 &= g^{xy} \oplus H(g^{xy}; idpw_digi; r_c). \end{aligned}$$

Note: S has stored $idpw_digi$ instead of the password pw_i itself. Challenge token is a one-time value which ensures freshness of the communication. Then S masks g^y as $m_g^y = g^y \oplus H(id_i, idpw_digi)$. Next, S sends $\{m_g^y, ch_1, ch_2\}$ to C .

Step 3 Upon receiving the message from S , C first uses id_i, pw_i to compute $idpw_digi = H(id_i, pw_i)$ and then $H(id_i, idpw_digi)$. Next, C derives $g^y = m_g^y \oplus H(id_i, idpw_digi)$ and computes $g^{xy} \pmod{p}$ by raising g^y to x , and $H'(g^{xy}; idpw_digi; r_c) = ch_2 \oplus g^{xy}$. C obtains r_s by computing $ch_1 \oplus H(g^{xy}; idpw_digi; r_c)$. At last, C checks

if the received $H'(g^{xy}; idpw_digi; r_c)$ is equal to its computed $H(g^{xy}; idpw_digi; r_c)$. If not, S is not genuine and C terminates the protocol; Otherwise, C responds $\{id_i, r_s\}$ to S .

Step 4 After receiving (id_i, r_s) , S verifies that the received r_s is the same as the generated r_s . If they are the same, user U_i is authenticated. Next, S generates a one-time authentication token $sat = H(g^{xy}; idpw_digi; r_c; r_s)$. Then S sends $\{sat\}$ to C .

Step 5 Upon receiving the authentication token from S , C computes $sat' = H(g^{xy}; idpw_digi; r_c; r_s)$ and checks its validity by verifying if the following formula holds: $sat = sat'$. If Server's authentication token is valid, S is authenticated.

Step 6 Both C and S may optionally establish a symmetric session key to encrypt further information exchanged in Session after the initial authentication. If this is desired, they can generate a one-time session key by applying $\{g^{xy}; idpw_digi; r_c; r_s\}$ in some different ways. For example, Session key can be computed as $session_Key_1 = H(g^{xy}; idpw_digi; r_c; r_s(1))$; where $r_s(1)$ implies r_s plus some fixed value. That is, the fixed value added to r_s makes Session key different from server's authentication token.

The authentication protocol can be depicted as follows.

- S1** $U_i \rightarrow C$: $\{id_i, pw_i\}$
 C : r_c, p, g, x
 $m_g^x = g^x \oplus H(id_i, idpw_digi)$
- $C \rightarrow S$: $\{id_i, r_c, p, g, m_g^x\}$
- S2** S : $\{r_s, y\}$
 g^y
 $g^x = m_g^x \oplus H(id_i, idpw_digi)$
 g^{xy}
 $ch_1 = r_s \oplus H(g^{xy}; idpw_digi; r_c)$
 $ch_2 = g^{xy} \oplus H(g^{xy}; idpw_digi; r_c)$
 $m_g^y = g^y \oplus H(id_i, idpw_digi)$
- $S \rightarrow C$: $\{m_g^y, ch_1, ch_2\}$
- S3** C : $idpw_digi = H(id_i, pw_i)$
 $H(id_i, idpw_digi)$
 $g^y = m_g^y \oplus H(id_i, idpw_digi)$ g^{xy}
 $H'(g^{xy}; idpw_digi; r_c) = ch_2 \oplus g^{xy}$
 $ch_1 \oplus H(g^{xy}; idpw_digi; r_c)$
Check: $H'(g^{xy}; idpw_digi; r_c) = ?$
 $H(g^{xy}; idpw_digi; r_c)$
- $C \rightarrow S$: $\{id_i, r_s\}$
- S4** S : Check: received $r_s = ?$ generated r_s
 $sat = H(g^{xy}; idpw_digi; r_c; r_s)$
 $S \rightarrow C$: $\{sat\}$
- S5** C : $sat' = H(g^{xy}; idpw_digi; r_c; r_s)$
Check: $sat = ? sat'$
- S6** $S \rightarrow C$: $\{\text{Access granted (or denied)}\}$

B Review of Hölbl et al's password change protocol

In the Hölbl et al's scheme, if the user wants to update its password pw to pw_{new} , the user and Server perform the following six steps to complete the user's password change.

Step 1 The user U_i submits id_i and pw_i to Client C . C generates a random value r_c , chooses a large prime p and a primitive element $g \in GF(p)$ and a random integer $x < p - 1$. Then C computes $g^x \pmod{p}$ and masks it by computing $m_g^x = g^x \oplus H(id_i, idpw_dig_i)$, where $idpw_dig_i = H(id_i, pw_i)$ and has been stored by Server S . C sends $\{id_i, r_c, p, g, m_g^x\}$ to Server S .

Step 2 After receiving the messages, S chooses a random value r_s and a large random integer $y < p - 1$ and computes $g^y \pmod{p}$. S calculates $g^x = m_g^x \oplus H(id_i, idpw_dig_i)$ and then $g^{xy} \pmod{p}$. Next, S generates a one-time challenge token as follows:

$$ch_1 = r_s \oplus H(g^{xy}; idpw_dig_i; r_c),$$

$$ch_2 = g^{xy} \oplus H(g^{xy}; idpw_dig_i; r_c).$$

Then S masks g^y as $m_g^y = g^y \oplus H(id_i, idpw_dig_i)$. Next, S sends $\{m_g^y, ch_1, ch_2\}$ to C .

Step 3 Upon receiving the message from S , C first uses id_i, pw_i to compute $idpw_dig_i = H(id_i, pw_i)$ and then $H(id_i, idpw_dig_i)$. Next, C derives $g^y = m_g^y \oplus H(id_i, idpw_dig_i)$ and computes $g^{xy} \pmod{p}$ by raising g^y to x , and $H'(g^{xy}; idpw_dig_i; r_c) = ch_2 \oplus g^{xy}$. C obtains r_s by computing $ch_1 \oplus H(g^{xy}; idpw_dig_i; r_c)$. At last, C checks if the received $H'(g^{xy}; idpw_dig_i; r_c)$ is equal to its computed $H(g^{xy}; idpw_dig_i; r_c)$. If not, S is not genuine and C terminates the protocol; Otherwise, C responds $\{id_i, r_s\}$ to S .

Step 4 After receiving (id_i, r_s) , S verifies that the received r_s is the same as the generated r_s . If they are the same, user U_i is authenticated. Next, S generates a one-time authentication token $sat = H(g^{xy}; idpw_dig_i; r_c; r_s)$. Then S sends $\{sat\}$ to C .

Step 5 Upon receiving the authentication token from S , C computes $sat' = H(g^{xy}; idpw_dig_i; r_c; r_s)$ and checks its validity by verifying if the following formula holds: $sat = sat'$. If Server's authentication token is valid, C generates a new password digest value $idpw_dig_new_i$ as $H(id_i, pw_new_i)$. Next, C generates one-time $mask$, mac , and $m_idpw_dig_new_i$ values as follows:

$$mask = H(g^{xy}; r_c; r_s);$$

$$mac = H(g^{xy}; idpw_dig_new_i; r_c; r_s);$$

$$m_idpw_dig_new_i = mask \oplus idpw_dig_new_i.$$

Then C sends $\{id_i, m_idpw_dig_new_i, mac\}$ to S .

Step 6 Upon receiving the messages, S computes $mask = H(g^{xy}; r_c; r_s)$ and retrieves

$$idpw_dig_new_i = mask \oplus m_idpw_dig_new_i.$$

Next, S computes $mac' = H(g^{xy}; idpw_dig_new_i; r_c; r_s)$,

and checks the validity of the received mac by the equation $mac' = mac$. If it is valid, S sends a message to C accepting the password change. Also, S replaces $idpw_digi$ with the new password hash value $idpw_dig_new_i$. Otherwise, it sends a message rejecting the password change. The password accept or reject message sent from S to C contains a protected response called $code = H(g^{xy}; idpw_dig_i; flag; r_c; r_s)$, where $flag$ is set to either 'accept' or 'reject' depending upon whether the password change is accepted or rejected.

III. CRYPTANALYSIS OF HÖLBL ET AL'S SCHEME

As the authors [19] stated that Peyravian-Jeffries scheme is vulnerable to off-line password-guessing attack. Hölbl et al's scheme employs exclusive or operations to mask g^x and g^y during transfer and additional checking in order to prevent man-in-middle attacks and off-line dictionary attacks. However, some security flaws still exist in the scheme. We will show that in Hölbl et al's scheme, the user authentication protocol cannot resist off-line password-guessing attack and the password change protocol suffers from denial-of-service attacks.

● *Off-line password guessing attacks on Hölbl et al's user authentication protocol*

In the password-based authentication scheme, the user can choose his password. In general, the user tends to choose easy-to-remember passwords which will potentially lead to password guessing attack. If an adversary tries to guess passwords and could verify their correctness, password-guessing attack is called successful. The adversary first intercepts some message transferred through the channel between the user and Server. Then the adversary mounts an off-line password guessing attack on the authentication scheme.

Although the authors claim that the proposed scheme is secure against password guessing attack, we demonstrate that their user authentication protocol is subject to password guessing attack.

Suppose that an adversary intercepts the transferred message between the user (the client) and the server. Then it is easily known from the authentication protocol in Section 2.1 that the adversary can obtain $\{id_i, r_c\}$ from the communication channel during Step 1, $\{ch_1, ch_2\}$ during Step 2, and $\{r_s\}$ during Step 3. Moreover the adversary can judge if the authentication succeeds by monitoring subsequent steps. If the user has succeeded in login onto the remote server this time, then the following equations hold:

$$ch_1 = r_s \oplus H(g^{xy}; idpw_dig_i; r_c),$$

$$ch_2 = g^{xy} \oplus H(g^{xy}; idpw_dig_i; r_c),$$

$$sat = H(g^{xy}; idpw_dig_i; r_c; r_s).$$

Thus, the adversary can compute

$$g^{xy} = ch_2 \oplus ch_1 \oplus r_s.$$

Therefore, the following two formulae hold:

$$ch_1 = r_s \oplus H(ch_2 \oplus ch_1 \oplus r_s; idpw_dig_i; r_c),$$

$$sat = H(ch_2 \oplus ch_1 \oplus r_s; idpw_dig_i; r_c; r_s).$$

Note that $idpw_dig_i = H(id_i, pw_i)$. Since for the above

equations, ch_1 , ch_2 , r_s , r_c and id_i are all known to the adversary and $H()$ is a public hash function, the adversary can guess the password value pw_i and verify these guesses by the equations. So the password guessing attack can work.

● *Denial-of-Service attacks on Hölbl et al's password change protocol*

Now, we show an attack on password change protocol in Hölbl et al's scheme. Assume that an adversary wiretaps the communication channel and intercepts $\{id_i, r_c, ch_1, ch_2, r_s\}$ from the channel during Step 1, Step 2, and Step 3 of password change protocol in Hölbl et al's scheme. Then, the adversary can obtain $g^{xy} = ch_2 \oplus ch_1 \oplus r_s$.

When the password change protocol goes to Step 5, the adversary masquerades the user to communicate with the server by performing the following steps:

Step I Compute $sat'=H(g^{xy}; idpw_dig_i; r_c; r_s)$ and check its validity by the equation $sat= sat'$. If Server's authentication token is valid, the adversary generates a new password and the digest value $idpw_dig_new_i=H(id_i, pw_new_i)$.

Step II Compute the following values:

$$mask = H(g^{xy}; r_c; r_s);$$

$$mac = H(g^{xy}; idpw_dig_new_i; r_c; r_s);$$

$$m_idpw_dig_new_i = mask \oplus idpw_dig_new_i.$$

Step III Send $\{id_i, m_idpw_dig_new_i, mac\}$ to S .

When S receives the messages, S can compute

$$mask = H(g^{xy}; r_c; r_s),$$

$$idpw_dig_new_i = mask \oplus m_idpw_dig_new_i,$$

$$mac' = H(g^{xy}; idpw_dig_new_i; r_c; r_s).$$

It is easy to know that the equation $mac' = mac$ holds. Thus, S believes the validity of the received mac . S will replace $idpw_dig_i$ with the new password hash value $idpw_dig_new_i$. And S sends a message to C accepting the password change.

Thus, the adversary succeeds changing the password of the user with the identity ID. Thus, while the legal user with the identity ID logs the server with the password pw_i as in Section 2.1, the server will refuse the user. Because the server has stored a new password hash value $idpw_dig_new_i$.

V. CONCLUSION

In this paper, we have shown that Hölbl et al's authentication protocol is vulnerable to password guessing attack and their password change protocol suffers from Denial-of-Service attack.

REFERENCES

- [1] L. Lamport, "Password authentication with insecure communication," *Communication of ACM* 24, 1981, pp.28-30.
- [2] H. Guo, Z. Li, Y. Mu, X. Zhang, "Cryptanalysis of simple three-party key exchange protocol," *Computers & Security*, Vol. 27, No. 1-2, 2008, pp. 16-21.
- [3] T. Xiang, K. Wong, X. Liao, "Cryptanalysis of a password authentication scheme over insecure networks," *Computer and System Sciences*, Vol. 74, No. 5, 2008, pp. 657-661.
- [4] H. B. Chen, T. H. Chen, W. B. Lee, C. C. Chang, "Security enhancement for a three-party encrypted key exchange protocol against undetectable on-line password guessing attacks," *Computer Standards & Interfaces*, Vol. 30, No. 1-2, January 2008, pp. 95-99.
- [5] M. Hölbl, T. Welzer, B. Brumen, "Improvement of the Peyravian-Jeffries's user authentication protocol and password change protocol," *Computer Communications*, Vol. 31, No. 10, June 2008, pp. 1945-1951.
- [6] M. Peyravian, C. Jeffries, "Secure remote user access over insecure networks," *Computer Communications*, Vol. 29, No. 5, March 2006, pp. 660-667.
- [7] M.K. Khan, J. Zhang, "Improving Security of a flexible biometrics remote user authentication scheme," *Computer Standards & Interfaces* 29 (1), 2007, pp.82-85.
- [8] D.P. Jablon, "Strong password only authenticated key exchange," *Computer Communication Review* 26 (5) , 1996, pp. 5-26.
- [9] C.C. Chang, W.Y. Liao, "A remote password authentication scheme based upon ElGamal's signature scheme," *Computer Security*, 13(2),1994, pp. 137-144.
- [10] M. Peyravian, N. Zunic, "Methods for protecting password transmission," *Computers and Security* 19 (5), 2000, pp.466-469.
- [11] Lee CC, Li LH, Hwang MS. "A remote user authentication scheme using hash functions," *ACM SIGOPS Oper Syst Rev* 2002;36(4), pp.23-29.
- [12] Hwang JJ, Yeh TC, "Improvement on Peyravian - Zunic's password authentication schemes," *IEICE Trans Commun.*2002; E85-B(4), pp.823-825.
- [13] Yoon EJ, Ryu EK, Yoo KY, "A secure user authentication scheme using hash functions," *ACM SIGOPS Oper Syst Rev* 2004;38(2), pp.62-68.
- [14] Ku WC, Chen CM, Lee HL, "Weaknesses of Lee-Li-Hwang's hash-based password authentication scheme," *ACM SIGOPS Oper Syst Rev* 2003;37(4):19-25.
- [15] M. Peyravian, C. Jeffries, "Secure remote user access over insecure networks," *Computer Communications* 29 (5-6), 2006, pp.660-667.
- [16] W. Diffie, M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory* 22(6),1976, pp. 644-654.
- [17] J. Munilla, A. Peinado, "Off-line password-guessing attack to Peyravian-Jeffries's remote user authentication protocol," *Computer Communications* 30 (1), 2006, pp. 52-54.
- [18] K.A. Shim, "Security flaws of remote user access over insecure networks," *Computer Communications* 30 (1), 2006, pp.117-121.
- [19] M. Hölbl, T. Welzer, B. Brumen, "Improvement of the Peyravian-Jeffries's user authentication protocol and password change protocol," *Computer Communications* 31, 2008, pp. 1945-1951.
- [20] Jorge Munilla and Alberto Peinado, "Security flaw of Hölbl et al.'s protocol," *Computer Communications*, Volume 32, Issue 4, 4 March 2009, pp.736-739.