Scientific Research Publishing

Journal of Computer and Communications, 2021, 9, 102-109
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

A Two-Party Password-Authenticated Key Exchange Protocol with Verifier

Shunbo Xiang, Bing Xu, Ke Chen

School of Computer, Guangdong University of Petrochemical Technology, Maoming, China
Email: qingcheng33@163.com

How to cite this paper: Xiang, S.B., Xu, B. and Chen, K. (2021) A Two-Party Password-Authenticated Key Exchange Protocol with Verifier. *Journal of Computer and Communications*, **9**, 102-109.
https://doi.org/10.4236/jcc.2021.94007

Received: March 18, 2021
Accepted: April 26, 2021
Published: April 29, 2021

Abstract

To tackle with the security lack in the password-authenticated key exchange protocol, this paper proposes a two-party password-authenticated key exchange protocol based on a verifier. In the proposed protocol, a user stores his password in plaintext, and the server stores a verifier for the user's password, using DL difficult problem and DH difficult problem, through the session between user and server to establish a session key. The security discussion result shows that the proposed protocol provides forward secrecy, and can effectively defend against server compromising fake attacks, dictionary attacks and middleman attacks. Protocol efficiency comparisons reveal our protocol is more reasonable.

Keywords

Verifier, Password-Authenticated, Key Exchange, Fake Attack, Dictionary Attack, Session Key

1. Introduction

The two-party password-authenticated key exchange protocol with verifier refers to the user and the server participating in one session protocol to establish a session key with user's password verifier stored in server's storage in order to achieve secure data communication over the insecure channel. User's password is user's long-term key and it can be used as an effective way to verify the real identity of user unless the password is leaking. Password-authenticated key exchange protocol with verifier is developed on the basis of password-authenticated key exchange protocol, which is aimed at the attacks caused by leaks or theft of user's plaintext password and it is not safe for server to store user's password directly, thus changing to store the computation value of user's password, which is called password verifier. There are many research papers about password-authenticated key exchange protocol until now.

1.1. Relate Work

In 1992, one paper [1] first proposed two-party password-authenticated key exchange protocol and that protocol is based on Diffie-Helman (DH) protocol and can resist online password dictionary attack. Other papers [2]-[16] researched two-party password-authenticated key exchange protocol with verifier protocol. The paper [3] proposed a two-party password-authenticated key exchange protocol with verifier protocol. Paper [4] proposed a revised protocol in paper [3], but the revised protocol is more complicated. One paper [5] proposed a two-party password-authenticated key exchange protocol with verifier and proved the safety of this protocol in standard model. One paper [6] pointed the errors in the process of proving the protocol proposed in paper [5]. As the existing two-party password-based key exchange protocols have shortages when using public key infrastructure and suffer dictionary attack, a two-party password-based key agreement protocol resistant to the dictionary attacks by adding password-authentication services was proposed [7], its security was proved under both the ideal-cipher model and the random-oracle model. In [8], to resist dictionary attacks, a two-party password-based key exchange Protocol was proposed based on DH key exchange and hash function. To overcome the undetectable online dictionary attacks by a malicious gateway, a gateway-oriented password-based authenticated key exchange (GPAKE) was proposed based on chameleon hash function in [9]. In two-party password authenticated key agreement protocols, servers maintain a password or verification table can incur dictionary attack, impersonation attack and the stolen-verifier attack, a protocol for session initiation protocol associated with Voice over Internet Protocol was achieved in [10] without these disadvantages, the proposed protocol had the properties of session key agreement, mutual authentication and password updating function. In 2013, one paper [11]analyzed that two-party password-based key exchange protocol had two families: implicit and explicit key authentications, the paper also indicated the protocol in [7] was an implicit one, as an improvement of [7], the paper proposed an explicit two-party password-based key exchange protocol. For some two-party password authenticated key exchange protocols fail to provide mutual authentication and key confirmation, the authors [12] proposed two improved protocols, one of which can accomplish mutual authentication and key confirmation. In [13], the authors showed that the protocol in [11] can't resist off-line password guess assault and demonstrated the protocol existed impersonation attack, they also indicated the two-party password authenticated key exchange protocol in [11] lack of forward secrecy, to deal with these security shortages, paper [13] proposed an improved two-party password authenticated key exchange protocol based on the protocol in [11]. Paper [14] explained that most of the two-party password-based key exchange protocols could not provide personalized demand, the authors in paper [14] designed a personalized key exchange protocol, in which users selected the code of mutual session keys under the demand of their own. There are few papers published about explicit authentication in two-party password-based key exchange protocols, paper [15] indicated the explicit authenticated protocol in [11] can lead to disguise attack, paper [15] also indicated the security definition in [11] exist some faults, then paper [15] redefined the security contents in two-party explicit authenticated key exchange protocols and ameliorated the protocol structure in [11]. Paper [16] also proposed an improved protocol based on the protocol in [13].

1.2. Motivations

Nevertheless, we believe that two-party password-authenticated key exchange protocol with verifier is worthy to be studied, from both the practical perspective and the cryptographic design perspective, under this background, this paper also proposed a two-party password-authenticated key exchange protocol and proved its safety. The proposed protocol is suitable in electrical transaction under mobile environment.

2. Basic Content

Definition 1:

DL difficult problem: Given G is a cyclic group whose order is prime number p, g is generator of G, given a tuple $\left(g, g^{a}\right)$, where $a \in Z_{p}^{*}$, then the process of computing a is difficult.

Definition 2:

DH difficult problem: Given G is a looping group whose order is prime number p, g is generator of G, given a triad tuple $\left(g, g^{a}, g^{b}\right)$, where $a, b \in Z_{p}^{*}$, then computation g^{ab} is difficult.

3. New Two-Party Password-Authenticated Key Exchange Protocol with Verifier

Our paper proposes a new two-party password-authenticated key exchange protocol with verifier, which has two participants called user and server. The user initiates a session with the server actively. Our new proposed two-party password-authenticated key exchange protocol with verifier is abbreviated as VBTP, so during the subsequent content, VBTP is used to represent our protocol. The session process of VBTP is as follows:

Let G notate a group whose order is prime number p, g is a generator of G, protocol participants are the User U and the Server S, Identity information is ID_{U} and ID_{S}. User registered at server and pw is the password plaintext of U, anti-collision one-way hash function $H_{0}:\{0,1\}^{*} \rightarrow Z_{p}^{*}$ and $H_{1}:\{0,1\}^{*} \times\{0,1\}^{*} \times G \rightarrow\{0,1\}^{*}$. In order to resist server leak attack, S store the verifier of password plaintext U. U computes password authentication value $V=g^{H_{0}\left(ID_{U} \| ID_{S} \| pw\right)}$ and store V in S through secure channel. Protocol execution process is as **Figure 1**, specific computation steps are as following:

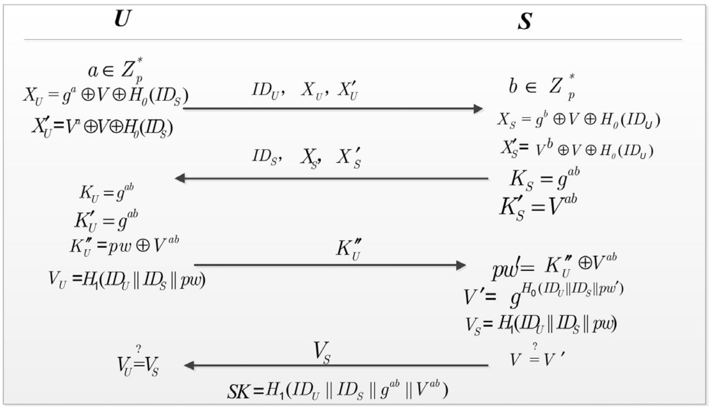
U
S
$a \in Z_p^*$
$X_U = g^a \oplus V \oplus H_0(ID_S)$
$X_U' = V^a \oplus V \oplus H_0(ID_S)$
ID_U, X_U, X_U'
$b \in Z_p^*$
$X_S = g^b \oplus V \oplus H_0(ID_U)$
$X_S' = V^b \oplus V \oplus H_0(ID_U)$
ID_S, X_S, X_S'
$K_S = g^{ab}$
$K_S' = V^{ab}$
$K_U = g^{ab}$
$K_U' = g^{ab}$
$K_U'' = pw \oplus V^{ab}$
K_U''
$V_U = H_1(ID_U \| ID_S \| pw)$
$pw' = K_U'' \oplus V^{ab}$
$V' = g^{H_0(ID_U \| ID_S \| pw')}$
$V_S = H_1(ID_U \| ID_S \| pw)$
$V_U \overset{?}{=} V_S$
V_S
$V \overset{?}{=} V'$
$SK = H_1(ID_U \| ID_S \| g^{ab} \| V^{ab})$

Figure 1. VBTP Execution process.

1) U chooses $a \in Z_p^*$ randomly, then computes $X_U = g^a \oplus V \oplus H_0(ID_S)$ and $X_U' = V^a \oplus V \oplus H_0(ID_S)$, finally sends ID_U, X_U and X_U' to S;

2) After receiving the message from U, S randomly chooses $b \in Z_p^*$, gets verifier V from password file, computes $X_S = g^b \oplus V \oplus H_0(ID_U)$ and $X_S' = V^b \oplus V \oplus H_0(ID_U)$, the sends ID_S, X_S and X_S' to U, finally S computes $K_S = \left(X_U \oplus V \oplus H_0(ID_S)\right)^b = g^{ab}$, $K_S' = \left(X_U' \oplus V \oplus H_0(ID_S)\right)^b = V^{ab}$;

3) After receiving S's message, U compute $K_U = \left(X_S \oplus V \oplus H_0(ID_U)\right)^b = g^{ab}$, $K_U' = \left(K_S' \oplus V \oplus H_0(ID_U)\right)^a = V^{ab}$, then computes $K_U'' = pw \oplus V^{ab}$, $V_U = H_1(ID_U \| ID_S \| pw)$, sends K_U'' to S;

4) After receiving K_U'', S computes U's password plaintext $pw' = K_U'' \oplus V^{ab}$, then computes $V' = g^{H_0(ID_U \| ID_S \| pw')}$ and $V_S = H_1(ID_U \| ID_S \| pw)$, verifies if $V \overset{?}{=} V'$ or not, if yes, S trusts identity verification of user U, then sends V_S to U, obviously $K_U'' \oplus V^{ab} = pw \oplus V^{ab} \oplus V^{ab} = pw$;

5) After receiving V_S, U verifies if $V_U \overset{?}{=} V_S$ or not, if yes, U trusts identity verification of server S;

6) Finally, U and S compute the same session key

$$SK = H_1\left(ID_U \| ID_S \| K_U \| V^{ab}\right) = H_1\left(ID_U \| ID_S \| K_S \| V^{ab}\right), \text{ then}$$

$$SK = H_1\left(ID_U \| ID_S \| g^{ab} \| V^{ab}\right).$$

4. Security Analysis

A two-party password-authenticated key exchange protocol with verifier has many security requirements, which can be proved by through different methods, our VBTP also needs to be had security analysis. By means of forward security in two-party password-authenticated key exchange, resistance to server's leakage fake attack, dictionary attack resistance, resistance to man-in-the-middle attack and other security requirements , the security of the our VBTP was proved.

Theorem 1. VBTP has forward security.

Proof: forward security of two-party password-authenticated key exchange protocol with verifier is that during the process of one protocol session, even if the user's password plaintext leaks to the adversary, the adversary can not explicitly work out the past session key based on the user's password plaintext before this session, which means there is independence between session key and password plaintext. In our VBTP, if the user's password plaintext pw had been leaked to an adversary A during a mutual session, the adversary A obtained the message $g^a \oplus V$, $g^b \oplus V$ and $pw \oplus V^{ab}$ of another session before this session via wiretapping, A computed V by pw, then figured out g^a, g^b and V^{ab} through calculation, but he couldn't calculate g^{ab}, according to our Definition 1, gaining g^{ab} is DL difficult problem or DH difficult problem, but the adversary A couldn't resolve DL difficult problem or DH difficult problem, so VBTP has forward security.

Theorem 2. VBTP can resist to server's leakage fake attack.

Proof: server's leakage fake attack to a two-party password-authenticated key exchange protocol with verifier is that an adversary A gets the user's password verifier V stored in the server by attack, theft and other attack means, then the adversary Aim personates the user to initiate a protocol session with the server. A two-party password-authenticated key exchange protocol with verifier can resist server's leakage fake attack is that the server can recognize the identity of fakers, thereby terminate the session. In our VBTP, supposing that an adversary A obtains the user's password verifier V, in each session, the adversary A knows the value K''_U, but he cannot obtain the user's password plaintext pw, he can choose $V = g^{H_0(ID_U \| ID_S \| pw)}$ or $pw \oplus V^{ab}$ to figure out pw, if he selects $V = g^{H_0(ID_U \| ID_S \| pw)}$ to compute pw, he must compute $H_0(ID_U \| ID_S \| pw)$ firstly, so he confronts the DL difficult problem as our Definition 1 says. If the adversary A selects $pw \oplus V^{ab}$ to obtain pw, he should computer V^{ab} before $pw \oplus V^{ab} \oplus V^{ab} = pw$, he can compute V^a through $V^a \oplus V \oplus H_0(ID_S)$ and compute V^b by $V^b \oplus V \oplus H_0(ID_U)$, the computation process is
$V^a \oplus V \oplus H_0(ID_S) \oplus H_0(ID_S) \oplus V = V^a$,
$V^b \oplus V \oplus H_0(ID_U) \oplus H_0(ID_U) \oplus V = V^b$, finally, the adversary A cannot calculate V^{ab}, because our Definition 2 has described that computing V^{ab} is a DH difficult problem. The adversary does not know pw, so the message he sends to the server does not contain pw, the server can be able to accurately verify the fake identity, thereby preventing fake attack, so that our VBTP can resist server's leakage fake attacks.

Theorem 3. VBTP can resist all kinds of dictionary attack.

Proof: dictionary attacks to a two-party password-authenticated key exchange protocol with verifier divide into two types: online and offline dictionary attacks.

1) In our VBTP, online dictionary attack against the can be detected by the server. The so-called dictionary attack is that the adversary A randomly selects a password from a record which has a variety of passwords in plaintext to constantly test the user's real password. It is supposed that the adversary A randomly selects $pw' \neq pw$ to log in to the server S to test the match of the user's password pw in plaintext, the adversary A calculates V' through pw', then calculates $X_U = g^a \oplus V'$, $(V')^a$ and K'_U, the adversary A sends X_U, $(V')^a$

and K'_U to the server, the server calculates pw to verify V, then he will find that he cannot verify the user's identity, concludes that user's fake identity, so that the server will ask the adversary A to re-login to the server with a new password, after finite logins fails, the server will terminate any session with the adversary A, then the server ascertains that this is an online dictionary attack; 2) Offline dictionary attack to the user. Offline dictionary attack is that the adversary A tries to calculate the user's password plaintext from the intercepted conversation information, the adversary A could not calculate the user's password plaintext, this attack is same as Theorem 2, because the adversary to face DL difficult problem or DH difficult problem, so the adversary's attack is invalid. Above all, VBTP can resist all kinds of dictionary attack.

Theorem 4. VBTP for man-in-the-middle attack is safe.

Proof: Man-in-the-middle attack in our VBTP refers to that there is an adversary A between the user and the server, for the server, the user is counterfeit, while for the user, the server is faked. In fact, the man-in-the-middle attack for a two-party password-authenticated key exchange protocol with verifier is invalid, because in such circumstance, the password verifier is used to prevent the man-in-the-middle attack. In our VBTP, if the adversary does not know the user's password plaintext, then he cannot impersonate a user to log into the server, similar to attacks with Theorem 2 or 3, the adversary fake action can easily be detected by the server, so the attack cannot succeed. Similarly, if the adversary counterfeits the server to interact with the user, unless the adversary knows the user's password plaintext, otherwise the attack cannot be successful, in fact, the adversary cannot figure out the user's password plaintext, so the man-in-the-middle attack fails in our VBTP.

5. Efficiency Comparisons and Discussions

Efficiency of a two-party password-authenticated key exchange protocol with verifier can perform in terms of communication load and computation load. Table 1 is the protocol operational efficiency of the our VBTP compared to protocols of paper [3] and paper [4] which are write as paper [3] and paper [4] respectively. In Table 1, the unit of communication round is step, the unit of random number is individual and others are time. It is showed in Table 1, exponentiations of VBTP is smaller one time than the protocol of paper [3], hash

Table 1. Protocol operational efficiency comparison.

Protocol	paper [3]	paper [4]	VBTP
communication round	4	3	4
random number	2	2	2
exponentiation	7	9	6
hash function	6	10	6
XOR computation	4	4	8

functions of VBTP is same as the protocol of paper [3]. Compared to the protocol of paper [4], communication round of VBTP is one more time and others are not high. The discussion shows that the protocol operational efficiency of our VBTP is high.

6. Conclusion

A two-party password-authenticated key exchange protocol with verifier has various kinds of security attacks, especially the server's leakage fake attack and dictionary attack, aiming at such attack, a two-party password-authenticated key exchange protocol with verifier abbreviated as VBTP was proposed. Security analysis shows that our VBTP has forward security, resistance to server's leakage fake attack, offline dictionary attack, online dictionary attack and man-in-the-middle attack. VBTP can be applied to a client/server communications, especially mobile e-commerce environment, the mobile terminal uses a password to login to the server, using a password and password verifier the server can verify the true identity of the user. At the end, efficiency discussion explains our protocol VBTP is low cost.

Acknowledgements

This work is supported by Guangdong Natural Science Foundation of China (No.2017A030307027, 2018A030307032) and Key Platform and Scientific Research Projects of Guangdong Education Department, China (No.2020ZDZX3038).

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Bellovin, S.M. and Merritt, M. (1992) Encrypted Key Exchange: Password-Based Protocols Secure against Dictionary Attacks. *IEEE Computer Society Symposium on Research in Security and Privacy*, Oakland, 4-6 May 1992, 72-84.

[2] Jablon, D.P. (1997) Extended Password Key Exchange Protocols Immune to Dictionary Attack. *Proceedings of the 6th IEEE Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, Cambridge, 18-20 June 1997, 248-255.

[3] Lee, S.W., Kim, W.H., Kim, H.S., *et al.* (2004) Efficient Password-Based Authenticated Key Agreement Protocol. In: *ICCSA*'04, Springer-Verlag, Perugia, 617-626. https://doi.org/10.1007/978-3-540-24768-5_66

[4] Tan, S.-C., Zhang, N. and Wang, Y.-M. (2008) A New Password-Based Authenticated Key Agreement Protocol. *Journal of University of Electronic Science and Technology of China*, **37**, 17-19.

[5] Shu, J. and Xu, C.-X. (2009) Efficient Password-Based Authenticated Key Exchange Protocol under Standard Model. *Journal of Electronics and Information*, **31**, 2717-2719.

[6] Hu, X.-X., Liu, W.-F. and Zhang, Z.-F. (2010) Cryptanalysis of Two Password Authenticated Key Exchange Protocols. *Computer Engineering and Applications*, **46**,

18-19.

[7] Zhou, H., Wang, T. and Zheng, M. (2011) Provably Secure Two-Party Password-Based Key Agreement Protocol. In: *Proceedings of the International Conference on Human-Centric Computing* 2011 *and Embedded and Multimedia Computing* 2011, Springer, Berlin, 213-221. https://doi.org/10.1007/978-94-007-2105-0_21

[8] Wang, L.-B., Pan, J.-X. and Ma, C.-S. (2011) Simple and Efficient Password-Based Authenticated Key Exchange Protocol. *Journal of Shanghai Jiaotong University*, **16**, 459-465. https://doi.org/10.1007/s12204-011-1174-8

[9] Gao, F., Wei, F. and Ma, C. (2012) Gateway-Oriented Password-Authenticated Key Exchange Based on Chameleon Hash Function. 2012 8*th International Conference on Wireless Communications*, *Networking and Mobile Computing* (*WiCOM*), Shanghai, 21-23 September 2012, 1-4. https://doi.org/10.1109/WiCOM.2012.6478530

[10] Zhang, L., Tang, S. and Cai, Z. (2013) Efficient and Flexible Password Authenticated Key Agreement for Voice over Internet Protocol Session Initiation Protocol Using Smart Card. *International Journal of Communication Systems*, **27**, 2691-2702. https://doi.org/10.1002/dac.2499

[11] Zheng, M., Zhou, H. and Chen, J. (2013) An Efficient Protocol for Two-Party Explicit Authenticated Key Agreement. *Concurrency & Computation Practice & Experience*, **27**, 2954-2963. https://doi.org/10.1002/cpe.3198

[12] Saeed, M., Shahhoseini, H.S., Mackvandi, A., *et al.* (2014) A Secure Two-Party Password-Authenticated Key Exchange Protocol. 2014 *IEEE* 15*th International Conference on Information Reuse and Integration* (*IRI*), Redwood City, 13-15 August 2014, 466-474. https://doi.org/10.1109/IRI.2014.7051926

[13] Farash, M.S., Islam, S.H. and Obaidat, M.S. (2015) A Provably Secure and Efficient Two-Party Password-Based Explicit Authenticated Key Exchange Protocol Resistance to Password Guessing Attacks. *Concurrency & Computation Practice & Experience*, **27**, 4897-4913. https://doi.org/10.1002/cpe.3477

[14] Yi, T., Shi, M. and Shang, W. (2015) Personalized Two Party Key Exchange Protocol. 2015 *IEEE*/*ACIS* 14*th International Conference on Computer and Information Science* (*ICIS*), Las Vegas, 28 June-1 July 2015, 575-579. https://doi.org/10.1109/ICIS.2015.7166659

[15] Ou, R., Kumar, N., He, D., *et al.* (2015) Efficient Provably Secure Password-Based Explicit Authenticated Key Agreement. *Pervasive & Mobile Computing*, **24**, 50-60. https://doi.org/10.1016/j.pmcj.2015.06.008

[16] Aboud, S.J. (2015) Password-Based Key Agreement System. *Ijarcsms*, **3**, 9-16.