

# International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: [www.ijarcsms.com](http://www.ijarcsms.com)

## *Password-Based Key Agreement System*

**Dr. Sattar J. Aboud**

Department of Computer Science and Technology

University of Bedfordshire

Luton, United Kingdom

*Abstract: In this paper, we will consider some system, a verifier password-based key agreement system and claim that the system is insecure. Then, the author present an enhanced verifier-based key agreement system relied on Lee, et al. system and show that the propose system resists against password guessing attack and stolen verifier attack. The author is claimed that the proposed system is more secure and efficient compare with Lee, et al.*

*Keywords: key agreement system, verifier-based, password guessing attack, stolen verifier attack.*

### I. INTRODUCTION

Password-based authenticated key agreement has received high attention since it plays an important role to utilize authenticated key agreement systems. In general, classical password systems require a human memorable shared between the users. The password-based key agreement systems are prone to password guessing attack, since a user picks a password so it can be easily memorized. The key agreement system is one of the important methods in public key cryptography systems. Such system allow two or more users to exchange messages over insecure channel and agree on the shared session key, which can used later for secure communication between the users. Thus, secure key agreement system work as basic building block for building a high level of security. Secure communication requires only trusted users that have a copy of private key, while private key can promise privacy, user authentication, and message integrity. In network we can be able to securely distribute keys over a distance at a timely way. It seems that, key distribution is the main problem and should be as hard as the cryptography system and should be able to ensure that only trusted users have the copy of the private key. Most systems have an objective is to construct key on every system execution. In this case, the keying information define static key which will result each time the system is implemented by a given pair of users. Systems involving such fixed keys are insecure under known-key attacks. Alternatively, dynamic key protocol is established by a group of users differ on each execution. Dynamic key is also denoted as session key establishment. In this case the session key is dynamic, and it is generally intended that the system is invulnerable to known-key attacks [1, 2]. It is preferable that each user in a key establishment system is able to find the correct id user of others which may gain access to the key, including prevention of any illegal user from deducing the same key. This needs identifications of both users and the private key. But, the first two-party key agreement is the Diffie-Hellman system [3]. But, in fact Diffie-Hellman system is defenseless to man-in-middle attack because users engaged with a system and have no channel to authenticate each other.

The password-based system is vulnerable to dictionary attack since many users tend to pick memorable passwords of relatively low entropy [4]. In password-based key agreement system the data depicted from the password is entirely common between the users. In this case the hacker can get access to private messages, and then can pretend any user. To a key agreement system running in centralized approach, it is vulnerable to stolen-verifier attack, and the hacker who gets the verifier from a server will attempt to impersonate any user by agree on a session key with the server. Storing message version of password on server is insecure. This weakness is existed in all widely used systems.

However, the presented system is secure against dictionary attacks if we use only one time keys with server. The proposed system also offers great secrecy if one key is revealed, the following session keys will not be revealed. Since we do not use any public key infrastructure, great computational exponentiation is not needed.

## II. RELATED WORKS

Since the innovative method that withstands the password guessing attacks was presented in 1989 by Lomas, *et al* [5], there have been a several password-based authenticated key agreement systems were introduced. In 1996, Jablon [6] proposed a system where security relied on heuristic arguments. Also, in 1999 Halevi-Krawczyk [7] introduced another system, the system considered as inflexible for security of password-based authenticated system. However, Boyarsky in 1999 [8] improved this system by making it secure in multi-user environment, but, this system is inappropriate for situation where communication has to be established between users those sharing a common limited-entropy password. In 2000 [9], another password-based key exchange system has been proposed by Boyko, *et al*. This system is relied on two-party password-based system. An improvement for this system was made to multi-party setting by Bresson, *et al* [10]. The security of Bresson, *et al* system is based on the random oracle model.

In 2004, Lee, *et al* [11] suggested a verifiable-based key agreement system. In this system, the user uses a document of the password, while the server keeps as a verifier for the password. Thus the system cannot let a hacker who able to exchange information with the server to impersonate any user without running the dictionary attack in the password file. But, the system is not protected against stolen-verifier attack as Kwon in 2004 [12] has claimed. Also, Yoon-Kin 2005 [13] proposed a two-party key agreement system relied on Diffie-Hellman system. In 2006, Strangio [14] presented another two-party key agreement protocol relied also on Diffie-Hellman system. Both systems are not appropriate for large networks since they cannot assume each party shares a secret password with other user.

However, the first work that copes with offline dictionary attacks is introduced in 2007 by Bellare-Meritt [15]. They presented a family of encrypted key exchange to resist dictionary attack. This protocol is very important and become the foundation for future work in this area. Also, this system is simple and cost effective. In 2009, Shin, *et al* [16] introduced a system relied on threshold anonymous system. However, the system is complicated and costly. Other proposed password systems based on authenticated key exchange are Groce-Katz in 2010 [17], Aboud in 2011, [18] and Pointcheval in 2012 [19].

In this paper, we will briefly evaluate Lee, *et al* key agreement system and show its weaknesses to stolen-verifier attack. Then, we introduce a new system that verifier-based key agreement system. The new system resists password guessing attack and stolen-verifier attack.

## III. LEE ET AL, SYSTEM

In 2004 Lee, *et al* [12] introduced a verifier-based key agreement system. They claimed that the proposed system was secure in the case of server compromise. It indicates that when the hacker attacks the server, he cannot obtain sufficient information to pose as a user without execution a dictionary attack on the password file. Now, we briefly describe their system which is as follows:

### A. Notation Used

*The notations used in this paper are as follows:*

*A : User communicate with user B the sever*

*B : Server user*

*v : Verifier computed by user A*

*P : The password*

$q$  : Secure large prime number

$g$  : Generator in  $Z_q^*$  of order  $q-1$ .

$id_A$  : Identification of user  $A$

$id_B$  : Identification of user  $B$

$x, y$  : Two integer randomly selected numbers of order  $Z_q^*$ .

$h$  : Secure one-way hash function.

$\oplus$  : The XOR function

### B. The System Description

Suppose there is a secure hash function  $h : \{0,1\}^* \rightarrow Z_q^*$ . The steps of the system are as follows:

#### Step 1: User $A$

- 1.1. Select a password  $P$
- 1.2. Find  $v = g^{h(id_A, id_B, P)}$
- 1.3. Pass  $v$  to the server user  $B$  as the Verifier.
- 1.4. Select an arbitrary number  $x \in Z_q^*$
- 1.5. Find  $T_A = g^x \oplus v$
- 1.6. Pass  $(id_A, T_A)$  to server user  $B$

#### Step 2: User $B$

- 2.1. Select an arbitrary number  $y \in Z_q^*$
- 2.2. Find  $T_B = v^y \oplus v$
- 2.3. Find  $r_B = (T_A \oplus v)^y = g^{x*y}$
- 2.4. Compute  $d'_A = h(id_A, T_B, r_B)$
- 2.5. Find  $d_B = h(id_B, T_A, r_A)$
- 2.6. Pass  $T_B$  and  $d_B$  to user  $A$

#### Step 3: User $A$

- 1.1. Find  $r_A = (T_B \oplus v)^{x*h(id_A, id_B, P^{-1})} = g^{x*y}$
- 1.2. Compute  $d_A = h(id_A, T_B, r_A)$
- 1.3. Compute  $d_B = h(id_B, T_A, r_A)$
- 1.4. pass  $d_A$  to user  $B$

Step 4: User  $B$

- 4.1. Verify if  $d_A = d'_A$  if yes, user  $B$  authenticates user  $A$
- 4.2. Find the common session key  $r = h(r_A) = h(g^{x*y})$ .

Step 5: User  $A$

- 5.1. Verify  $d_B = d'_B$  if yes, user  $A$  authenticates user  $B$
- 5.2. Find the common session key  $r = h(r_B) = h(g^{x*y})$ .

### C. Vulnerabilities

Lee, et al claimed that the system was secure in the case of server compromise. But, in 2005 Shim-Seo [20] stated that the system was weak against stolen verifier attack. Alternatively, given the verifier, the hacker can impersonate an authorized user  $A$  to negotiate a session key with the server user  $B$ . The weakness of the system is that user  $B$  has not an efficient way to verify the message claimed to be sent by user  $A$ . So, we develop the system of Lee, et al by introducing a new verifier-based authenticated protocol, which resists against stolen verifier attack.

## IV. THE PROPOSED PASSWORD SYSTEM

The description of the system is as follows:

### A. Algorithm of the Proposed System

The steps of the algorithm are as follows:

Step 1: User  $A$

- 1.1. Select a password  $P$
- 1.2. Find  $v = g^{h(id_A, id_B, P)}$
- 1.3. Pass  $v$  to the server user  $B$  as the Verifier.
- 1.4. Select an arbitrary number  $x \in Z_q^*$
- 1.5. Find  $T_A = g^x \text{ mod } q$
- 1.6. Pass  $T_A$  to server user  $B$

Step 2: User  $B$

- 2.1. Select an arbitrary number  $y \in Z_q^*$
- 2.2. Find  $T_B = v^y \text{ mod } q$
- 2.3. Pass  $T_B$  and to user  $A$

Step 3: User  $A$

- 3.1. Find  $r = (T_B)^{x * h(id_A, id_B, P)^{-1}} \text{ mod } q$
- 3.2. Compute  $d_A = h(r) \text{ mod } q$

3.3. Pass  $d_A$  to user  $B$

Step 4: User  $B$

4.1. Find  $F_A = h(T_A)^y \bmod q$

4.2. Verify if  $F_A = d_A$  if yes, user  $B$  authenticates user  $A$

4.3. Compute  $E_B = v^{y^2} \bmod q$

4.4. Find the common session key  $r = (h(id_A, id_B, T_A^y) \bmod q)$

Step 5: User  $A$

5.1. Verify  $e(E_B, g) = e(T_B, T_B^{x \cdot h(id_A, id_B, P)^{-1}}) \bmod q$  if yes, user  $A$  authenticates user  $B$

5.2. Find the common session key  $r = h(id_A, id_B, T_B^{x \cdot h(id_A, id_B, P)^{-1}}) \bmod q$ .

Upon successfully implementing above system the two users, will agree on a shared session key  $r = h(id_A, id_B, g^{x \cdot y})$ .

### Example

Suppose that the prime  $q = 13, g = 6, id_A = 9, id_B = 12, P = 10$

Step 1: User  $A$

$$v = (g = 6^{h(id_A=9, id_B=12, P=10)}) \bmod 13$$

$$= 6^{(9+12+10)} \bmod 13 = 7, \text{ then pass this result to user } B$$

Suppose  $x = 3$

$$\therefore T_A = 6^{x=3} \bmod 13 = 8, \text{ send this value to user } B$$

Step 2: User  $B$

Suppose  $y = 4$

$$\therefore T_B = 7^{y=4} \bmod 13 = 9, \text{ and send this value to user } A$$

Step 3: User  $A$

$$\text{Find } r = (9)^{3 \cdot h(9, 12, 10)^{-1}} \bmod q$$

$$= 9^{3(31)^{-1}} \bmod 13 = 9^{3(8)} \bmod 13 = 9^{24} \bmod 13 = 1$$

Compute  $d_A = h(1) \bmod q = 1$ , send this value to user  $B$

Step 4: User  $B$

$$4.1. \text{ Find } F_A = h(8)^4 \bmod q = 1$$

4.2. Verify if  $F_A = d_A$  if yes, user  $B$  authenticates user  $A$

$$4.3. \text{ Compute } E_B = v^{y^2} \bmod q = 7^{4^2} \bmod 13 = 9$$

4.4. Find the common session key  $r = (h(id_A, id_B, T_A^y) \bmod q = (9, 12, 8^4) = 4117 \bmod 13 = 9$

### B. Security Discussion

We will show that the proposed password-based key agreement protocol is secure against both password guessing attack and stolen verifier attack.

- 1. Resist Man-in-Middle Attack:** The pre-shared password and verifier are employed to stop the man-in-middle attack is easy because a hacker does not have the verifier or password; it means that the hacker cannot impersonate user  $A$  to exchange information with user  $B$ .
- 2. Resist Dictionary Attack:** To the on-line password guessing attack, the users can overcome the hacker by selecting suitable trail intervals. In an off-line guessing attack, the hacker must repeatedly guess the password and check its accuracy by the message collected in an off-line approach. In the proposed system, the hacker is allowed to gather any message exchanged through the channel. It means that the hacker can get  $g^x, g^{y*x}, h(g^{x*y}), g^{y^2*x}$  since  $x, y \in Z_q^*$  are arbitrary numbers uniformly distributed in  $Z_q^*$  the off-line dictionary attack is beaten. In addition, known  $g^{y*x}$  and  $g^{x^2*x}$  a hacker cannot obtain  $g^y$  by the proposed scenario. As a result, we can mention that the suggested system is secure against dictionary attack.
- 3. Resist Stolen Verifier Attack:** Suppose that a hacker, user has imposed user  $B$  and obtained the verifier. A hacker goal is to impersonate user  $A$  to negotiate a session key with user  $B$ . We have the following theorem.

**Theorem:** Assume that we have the key agreement protocol is secure against stolen verifier attack.

**Proof:** In this scenario, hacker is allowed to select an arbitrary number  $x \in Z_q^*$  and finds  $T_A = g^x$ . We assume that the hacker has aptitude to impersonate user  $A$ . Alternatively, hacker must produce two results  $T_A$  and  $d_A$  which satisfy  $r_A = d_A$

As  $h$  is a robust one way hash function, obtained  $g^x$  and  $g$ , hacker must calculate  $g^y$  and then utilize the result to calculate  $d_A$  hence verifier  $r$  is indicated by  $g^x$ . Clearly, it is different from the complexity scenario illustrated previously. There is an alternative technique for hacker to impersonate user  $A$ . Hacker can gather messages  $g^x, g^{y*x}$  and  $g^{y^2*x}$  to obtained result. But, the scenario described previously is intractable. From depicted above we can summarize that a hacker cannot impersonate user  $A$  even if he gets the verifier kept in server and attempts to make stolen verifier attack.

### C. Efficiency

Efficiency of the proposed system is related to the costs of communication and computation. Communication cost involves counting total number of rounds and total messages transmitted through the network during a protocol execution. Number of rounds is a critical concern in practical environments where number of group members is large. Compares the proposed protocol with Lee et al. password based key agreement protocol.

Concerning cost communications, the presented system requires only two rounds while Kim-Yoo requires  $n$  rounds; where every user sends one message in every round. Regarding the maximum bit length of messages sent per user during the execution of the proposed system is  $2|e|$  with  $|e|$  is the maximum size of an encrypted message compare with  $n|e|$  in Lee, et al password based key agreement protocol. Concerning the maximum number of point-to-point communication per user, the proposed protocol require  $n+1$  while Lee, et al password based key agreement protocol require  $2n-2$ . To understand this case considers the users  $U_1, \dots, U_n$  participating in the protocol are on a ring and  $U_{i-1}, U_{i+1}$  are respectively the left and right neighbours of  $U_i$  for  $1 \leq i \leq n$  with  $U_0 = U_n, U_{n+1} = U_1$ . User  $U_i$  where  $1 \leq i \leq n-1$ , sends a message in round 1 only to the users  $U_{i-1}, U_{i+1}$  and a

message in round 2 to the rest of the  $n - 1$  users whilst the last user  $U_n$  sends one message in each round to all the  $n - 1$  users.

These will make the proposed system efficient from communication viewpoint.

Regarding cost computation, in the proposed system every group member executes at most 3 modular exponentiations compared with  $2n$  in Lee, et al system. Also, the proposed system requires 4 one-way hash function evaluations, 2 encryptions and  $n + 1$  decryption operations. The operations dependent on the number of group members are the asymmetric key decryption operation, compared with 1 encryption and 2 decryptions in Lee, et al system. The total cost of computation is highly reduced compared to Lee; et al system password based key agreement protocol. We use asymmetric key encryption and decryption. Hence the proposed system attains efficiency in both communication and computation costs. The constant round protocol can be implemented for a large group of participants as compared to Lee, et al system password-based system which becomes not practical if  $n > 100$ .

## V. CONCLUSION

In this paper, we have shown that Lee, *et al* password-based key agreement protocol is vulnerable to the password guessing attack and stolen verifier attack. To avoid these attacks, we presented a modified verifier-based key agreement system relied on Lee, *et al* system and demonstrate that the propose system resists against password guessing attack and stolen verifier attack. According to the security analysis, it is obvious that the modified protocol is secure enough to withstand all possible mentioned attacks. Constructing password systems using authenticated key agreement has received high attention in the last decade. In practice, password-based systems are appropriate for implementation in many situations, especially where no device is able of securely storing high-entropy long-term secret key. As we are mentioned, password has low entropy and is vulnerable to dictionary attack and man-in-middle attack, researchers must be cautious in construction password-based system.

## ACKNOWLEDGEMENT

The author wishes to extend his thanks to the University of Bedfordshire, Computer Science Department and Technology for their helpful suggestions and supports.

## References

1. Sattar J. Aboud, "Cryptanalysis of a Known Key Exchange Password Scheme", International Journal of Advanced Research, 01/2013, 1(7): 400-403, 2013.
2. Sattar J. Aboud, "Cryptanalysis of password scheme", International Conference on 01/2012, Information Society, London IEEE, (i-Society), 2012.
3. Diffie W and Hellman M, "New Directions in Cryptography", IEEE Transactions on Information Theory IT-11, pp. 644-654, November 1976
4. Wen F, Guo D., "An Improved anonymous scheme for telecare medical information system", Journal of Medicine System, 38(2) 26, E-publication, May 2014
5. Lomas T, Gong L, Saltzer J and Needham, "Reducing Risks from poorly chosen Keys", ACM SIGOPS Operat, System Review, 23: 14-18, 1989
6. Jablon D, "Strong password-only authenticated key exchange", SIGCOMM Computer Communication Review, volume 26, Number 5, pp. 5-26, 1996.
7. Halevi S and Krawczyk H, "Public key cryptography and password protocols", ACM Transactions on Information and System Security, pp. 524-543, 1999.
8. Boyarsky M, "Public-key cryptography and pass-word protocols: The multi-user case", ACM Security (CCS'99), pp. 63-72, 1999.
9. Boyko V, MacKenzie P and Patel S, "Provably secure password-authenticated key exchange using Diffie-Hellman", Euro-crypt 2000, LNCS 1807, pp. 156-171, Springer-Verlag, May 2000
10. Bresson E, Chevassut O and Pointcheval D, "New security results on encrypted key exchange," in PKC 2004, LNCS 2947, pp. 145-158, Springer, March 2004.
11. Lee S, Kim W, Kim H and Yoo K, "Efficient Password-based Authenticated Key Agreement Protocol", In ICCSA, LNCS, 3046: 617-626, 2004
12. Kwon T, "Practical Authentication Key Agreement Using Passwords", ISC 2004, LNCS, 3255:1-12, 2004
13. Yoon E and Yoo K, "New Efficient Simple Authenticated Key Agreement Protocol", COCOON 2005, LNCS, 3595: 945-954, 2005
14. Strangio M., "An Optimal Round Two-Party Password-Authenticated Key Agreement Protocol", the First International Conference on Availability, Reliability and Security, p. 8, April 2006
15. Bellare S and Merritt M, "Augmented encrypted key exchange: A password-based protocol secure against dictionary attacks and password file", International Journal of Network Security, Vol.3, No.1, PP.23-34, July 2007

16. SeongHan Shin, Kazukuni Kobara and Hideki Imai, "A Secure Threshold Anonymous Password Authenticated Key Exchange Protocol", Crypto 2009, LNCS, Springer-Verlag, 2009
17. Adam Groce and Jonathan Katz, "A new framework for efficient password-based authenticated key exchange", 17th Conference on Computer and Communications Security, pp. 516–525, ACM Press, October 2010
18. Sattar J. Aboud, "Password without Trusted Server", International Conference on Information Society (i-society), London IEEE, 06/2011.
19. David Pointcheval, "Password-based Authenticated Key Exchange", 15th International Conference on Practice and Theory of Public-Key Cryptography, LNCS 7293, pp. 390–397, Springer, may 2012.
20. Shim, K and Seo S, "Security Analysis of Password Authenticated Key Agreement Protocols", CANS, LNCS, 3810: 49-58, 2005.

#### **AUTHOR(S) PROFILE**



**Dr. Sattar J. Aboud**, received his Master degree in 1982 and a PhD in 1988 in the area of computing system. The two degrees were awarded from U.K. In 1990, he joined the Institute of Technical Foundation in Iraq as an assistant professor. In 1995 he joined the Philadelphia University in Jordan as a chairman of computer science department. Then, he moved as a professor at the Middle East University for Graduate Studies, Amman-Jordan. Currently, he is a visiting professor at University of Bedfordshire in UK. His research interests include areas such as public key cryptography, digital signatures, identification and authentication, networks security and cyber security. He has supervised numerous PhDs and Masters Degrees thesis. He has published more than 100 research papers in a multitude of international journals and conferences.