Development of an Efficient Password-Typed Key Agreement Scheme

Dr.Sattar J. Aboud
Iraqi Council of Representative

Dr. Haidar S. Jabbar
Mansour University College

Abstract :

In this paper, we will study [*Lee, Kim and Yoo, a verifier password typed key agreement]* scheme and demonstrate that the scheme is not secure. Then, the authors will propose an enhanced verifier typed key agreement scheme relied on [*Lee, Kim and Yoo]* scheme and demonstrate that the propose scheme resists against password guessing attack and stolen verifier attack. [*The authors are]* claimed that the proposed scheme is more secure and efficient compare with [*Lee, Kim and Yoo]* which is still existed protocol.

1. Introduction

The key agreement scheme means that let two or more entities to exchange a shared secret between them through an insecure channel. The shared secret can subsequently is utilized to reach certain security requirements, for example privacy or data integrity. The first two-party key agreement is the Diffi and Hellman scheme in 1976 [1]. However, the first Diffie and Hellman scheme is defenseless to man-in-middle attack because the entities engaged with the scheme and have no channel to authenticate every other.

Key agreement protocol is one of the vital cryptography techniques like encryption and digital signature scheme. Such scheme allow two or more participants to exchange information between them through an insecure channel and agree on a shared session key, which can employed for later secure communication between the participants. Therefore, secure key agreement scheme serve as basic building block for constructing higher level and secure scheme. Key establishment is generally divided to key agreement and key transport protocols.

Secret communications with secret keys requires only trusted participants that have copies of the secret key. While secret keys can guarantee confidentiality, authentication of users, and message integrity, in network we should be capable to securely distribute keys at a distance in a timely way [2].

When security is maintained, key distribution should be as hard as the cryptography scheme and should be able to ensure that only trusted participants have copies of the keys [3]. Apparently, key distribution is the main problem. However, key establishment scheme involving authentication usually needs a set-up period whereby authentic and possibly secret first keying information is distributed. Most schemes have an aim to construct create keys on every scheme execution. In certain cases, the first keying information pre-defines static key which will result each time the scheme is implemented by a given pair or group of participants. Schemes involving such fixed keys are insecure under known-key attacks.

Key pre-distribution is a key establishment scheme whereby the resulting established key is entirely fixed a priori by first keying information. On the other hand, dynamic key establishment protocol is the key established by a fixed pair or group of participants differs on following executions. Dynamic key establishment is also denoted as session key establishment. In this situation the session key is dynamic, and it is generally intended that the scheme is invulnerable to known-key attacks. Various key establishment schemes includes a centralized or trusted authority, for either or both initial scheme setup and on-line actions that is involving real-time participation. This participant is denoted as a variety of names depending on the role played, including: trusted authority, authentication server, trusted server,

key translation center, key distribution center, and certification authority [4]. It is usually preferred that every participant in a key establishment scheme is capable to find out the correct identity of the others which may gain access to the resulting key, implying deterrence of any illegal additional participants from inferring the same key. In this situation, the method is informally to give secure key establishment. This needs both identification of those participants with access to it and secrecy of the key [5].

In a secure scheme, passwords can be simply guessed when user selected his own password in document [6]. Storing message version of password on server is unsecure. This weakness is existed in all widely used schemes. The suggested scheme is secure against dictionary attacks as long as we use only one time keys with server. This scheme is also secure against malicious insider attacks, where a host abuses the information in one scheme run to another. The suggested scheme also offers great forward secrecy that is even when one key is revealed future session keys will not be revealed. As we do not employ any public key infrastructure, great computational exponentiation is not needed. As this is a trusted authority key agreement scheme each server need not share secret information with other server.

2. Related Work

Password schemes have in the last decade received high attention, because it plays an important role to employ an authenticated key agreement schemes. As the innovative method that withstands the password guessing attacks which was presented in 1989 by Lomas, Gong, Saltzer and Needham [7], there have been a several password-typed authenticated key agreement schemes were introduced for example by Jablon in 1996 [8] were security relied on heuristic arguments. Following it, a several schemes for password-typed key exchange have been suggested.

In 1999 Halevi and Krawczyk [9]) introduced their scheme. The scheme considered as an inflexible treatment of the security system for password-typed authenticated scheme and given a protocol officially proven to be secure with standard on user environment. But in 1999 Boyarsky[10] improved this scheme to make it secure in the multi-user environment. The Halevi and Krawczyk protocol considered to be asymmetric hybrid approach in which entity B the server can keep a high-class key and the other participant entity A can have the password. This scheme is inappropriate to settings in which communication has to be established between entities sharing a common limited-entropy password. Two other schemes for password -typed key exchange have been suggested, the first scheme by Bellare, Pointcheval and Rogaway in 2000[11] and the second scheme by Boyko, MacKenzie and Patel in 2000 [12].

They relied on the two-party password-typed scheme. An enhancement of this scheme was made to multi-party setting by Bresson, Chevassut and Pointcheval [13]. Bresson, Chevassut and Pointcheval study the security of two-party AuthA password-authenticated key exchange scheme standardized by IEEE P1363. The security of these protocols in the arbitrary oracle approach and in the ideal cipher approach is as follows. In the ideal cipher approach, a keyed cipher is examined as a family of arbitrary permutations that are queried by oracle to encrypt and decrypt. Ideal cipher approach does not give the same security assures as those in the arbitrary oracle approach and the typical schemes, but it is surely better to those offered by ad-hoc scheme designs. Reducing ideal cipher approach assumption is an interesting area of research.

Though, traditional password-typed scheme is vulnerable to dictionary attack, for instance Kim, Hub, Hwang and Lee, in 2004[14] proposed their scheme, as many entities tend to select memorable passwords of relatively low entropy. In certain password-typed key agreement scheme, the data depicted from the password is entirely common among the entities. Therefore, in the case of certain entity compromise, the hacker will get the whole secret message. After that, the hacker can pretend any entity wants. To a key agreement scheme running in centralized approach, it is also susceptible to stolen-verifier attack in case of server compromise. In stolen-verifier attack, the hacker, who gets the verifier from the server, attempts to impersonate a wanted entity and to agree on a session key with the server. In order to handle the risk of server compromise, Lee, Kim, Kim and Yoo in 2004 [15] suggested a verifiable-typed key agreement scheme. In this scheme, the entity employs a document of the password, while the server keeps a verifier for the password. Thus the scheme cannot let an opponent who negotiates the server to impersonate an entity without really running a dictionary attack on the password file. But, the scheme is not protected against stolen-verifier attack as Kwon, in 2004[16] have claimed.

Also, Yoon and Yoo Kin 2005 [17] is a two-party key agreement scheme relied on Diffie and Hellman scheme. In 2006, Strangio [18] presented a two-party key agreement protocol relied on Diffie and Hellman scheme in 1976. This scheme is not appropriate for large networks since we cannot assume that each party shares a secret password with each other participant. However, the initial work to cope with off-line dictionary attacks is introduced in 2007 by Bellovin and Merritt [19]. They presented a family of encrypted key exchange protocols to resist dictionary attack. This protocol is very important and become the foundation for future work in this area.
In 2008, Shakir Hussain and Hussein Al-Bahadili [20] proposed simple authenticated key agreement protocol which is also a two party key agreement protocol which is relied on password typed authentication and Diffie and Hellman key agreement. Unfortunately, this protocol is inefficient for practical use and does not allow concurrent executions. Also, this scheme is simple and cost effective.

In 2009, SeongHan Shin, Kazukuni Kobara and Hideki Imai [21] introduced a scheme relied on threshold anonymous scheme and show its security in the standard security system. This scheme is complicated and costly. The only considerable work in this field is the Bresson, Chevassut and Pointcheval [13] scheme. As we previously mentioned, this protocol is secure in both random oracle approach and in ideal cipher approach.

In this paper, we will briefly evaluate Lee, Kim, Kim and Yoo 2004 [15] password-typed key agreement scheme and show its weaknesses to stolen-verifier attack. Then, we introduce an enhanced scheme to verifier-typed key agreement scheme. Thus, we suggest a new scheme that resists against password guessing attack and stolen-verifier attack.

3. Lee, Kim and Yoo Scheme

In 2004 Lee, Kim and Yoo [15] introduced a verifier based key agreement scheme. They claimed that the proposed scheme was secure in the case of server compromise. It means that when the hacker attacks the server, he cannot obtain sufficient dada to impersonate a participant without running a dictionary attack on the password file. Now, we briefly describe their scheme which is as follows:

3.1 The Scheme Description

Suppose that there is an initialization in which an entity A selects a password. Also, suppose there is a robust one way hash function $h:\{0,1\}^* \to Z_q^*$. The description of the scheme is as follows:

1. **Entity A finds the verifier $k = c^{h(ID_A, ID_S, password)}$ and then passes k to the server entity B**
2. **Entity A selects an arbitrary number $x \in Z_q^*$**
3. **Finds $z_A = c^x \oplus k$ and then passes (ID_A, z_A) to entity B.**
4. **Entity B selects an arbitrary number $y \in Z_q^*$**
5. **Entity B finds $S_s = k^y \oplus k, r_s = (z_A \oplus k)^y = c^{x*y}, k_A^{'} = h(A, S_s, r_s)$**
6. **Entity B finds $k_s = h(ID_s, S_A, r_A)$ then passes S_s and r_s to entity A.**
7. **Entity A finds $r_A = (S_s \oplus k)^{x*h(ID_A, ID_B, password^{-1})} = c^{x*y}, k_A = h(ID_A, S_s, r_A)$ and passes k_A to entity B.**
8. **Entity B verifies if $k_A = k_A^{'}$ if yes, entity B authenticates entity A**
9. **Entity B finds the common session key $r = h(r_A) = h(c^{x*y})$.**
10. **Entity A verifies $k_s = B_s^{'}$ if yes, entity A authenticates entity B and finds the common session key $r = h(r_s) = h(c^{x*y})$.**

3.2 Vulnerabilities

Lee, Kim and Yoo [15] claimed that their scheme was secure in the situation of server compromise. But, in 2005 Shim and Seo [22] reported that the scheme was weak against stolen verifier attack. On the other hand, given the verifier the hacker can impersonate an authorized user to negotiate a session key with the entity B. The weak of the scheme is that entity B has not an efficient way to verify the message claimed to be sent by entity A. Motivated by Lee, Kim and Yoo scheme, we introduce a verifier-typed authenticated two-party protocol, which resists against stolen verifier attack.

4. The Proposed Password Scheme

Suppose that there is an initialization in which the entity A selects a password, finds $k = c^{h(ID_A, ID_s, password)}$ and then passes k to the entity B as the verifier. The suggested scheme includes the following steps:

1. **Entity A selects an arbitrary number $x \in Z_q^*$**
2. **Entity A finds $S_{A1} = c^x$ and then passes it to entity B the server.**
3. **Entity B selects an arbitrary number $y \in Z_q^*$**
4. **Entity B finds $S_{s1} = k^y$ and then passes it to entity A**
5. **Entity A finds $x = (S_{s1})^{x*h(ID_A, ID_s, password)^{-1}}$**
6. **Entity A finds $S_{A2} = h(x)$ and then passes S_{A2} to entity B**
7. **Entity B finds $k_A = h(S_{A1})^y$**
8. **Entity B verifies if $k_A = S_{A2}$. If it is yes, entity B authenticates entity A**
9. **Entity B finds $S_{s2} = k^{y^2}$ and then passes it to entity A.**
10. **Therefore, entity B finds the session key $r = h(ID_A, ID_s, S_{A1}^y)$**
11. **Entity A verifies whether: $e(S_{s2}, c) = e(S_{s1}, S_{s1}^{h(ID_A, ID_s, password)^{-1}})$ if it is yes, entity A authenticates entity B**
12. **Entity A finds the shared session key $r = (h(ID_A, ID_s, S_{s1}^{x*h(ID_A, ID_s, password)^{-1}})$**

Upon successfully implementing above scheme the two entities, will agree on a shared session key $r = h(ID_A, ID_s, c^{x*y})$.

5. Security [Analyses

We will show that the proposed password typed key agreement protocol is secure in the model as described in section 4. The security of the suggested protocol is achieved in both random oracle approach and the ideal cipher approach and demonstrate that the propose scheme resists against password guessing attack and stolen verifier attack. The description is as follows:-

1. **Resist Man-in-Middle Attack: The pre-shared password and verifier 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 entity A to exchange information with entity B.**

2. **Resist Stolen Verifier Attack: Suppose that a hacker, entity H has imposed entity B and obtained the verifier. Entity H goal is to impersonate entity A to negotiate a session key with entity B. We have the following theorem.**

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

<u>Proof</u>: In this scenario, entity H is allowed to select an arbitrary number $x \in Z_n^*$ and finds $S_{A1} = c^x$. We assume that the hacker entity H has aptitude to impersonate entity A. On the other hand, entity H must produce two results S_{A1} and S_{A2} which satisfy $k_A = S_{A2}$

As h is a robust one way hash function, obtained c^d and c, entity H must calculate c^y and then utilize this result to calculate S_{A2} hence verifier k is indicated by c^d. Clearly, it is different from the complexity scenario illustrated previously. There is an alternative technique for entity H to impersonate entity A. Entity H can gather messages c^d, c^{y*d} and c^{y^2*d} then attempt with the obtained result. But, the scenario described previously is intractable. From depicted above we can summarize that the hacker cannot impersonate entity A even if he gets the verifier kept in Server and attempts to make stolen verifier attack.

3. **Resist Dictionary Attack: To the on-line password guessing attack, the entities 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 scheme, the hacker is allowed to gather any message exchanged through the channel. It means that the hacker can get $c^x, c^{y*d}, h(c^{x*y})$, c^{y^2*d} since $x, y \in Z_n^*$ are arbitrary numbers uniformly distributed in Z_n^* the off-line dictionary attack is beaten. In addition, known c^{y*d} and c^{d^2*d} a hacker cannot obtain c^y by the proposed scenario. As a result, we can mention that the suggested scheme is secure against dictionary attack.**

6. Efficiency

Efficiency of the proposed protocol 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, Kim and Yoo password typed key agreement protocol [15].

Concerning cost communications, the suggested protocol requires only two rounds while Kim and Yoo require 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 protocol is $2|e|$ such that |e| is the maximum size of an encrypted message compare with $n|e|$ in Lee, Kim and Yoo password typed key agreement protocol. Concerning the maximum number of point-to-point communication per user, the proposed protocol require $n+1$ while Lee, Kim and Yoo password typed key agreement protocol require $2n-2$. To understand this case consider the users $U_1,...,U_n$ participating in the protocol are on a ring and U_{i-1},U_{i+1} are respectively the left and right neighbors of U_i for $1 \le i \le n$ such that $U_0 = U_n, u_{n+1} = U_1$. User U_i where $1 \le i \le n-1$, 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 protocol efficient from communication viewpoint.

Regarding cost computation, in the proposed protocol every group member executes at most 3 modular exponentiations compared with $2n$ in Lee, Kim and Yoo protocol. Also, the proposed protocol require 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, Kim and Yoo protocol. The total cost of computation is highly reduced compared to Lee, Kim and Yoo protocol password typed key agreement protocol [15]. We use asymmetric key encryption and decryption. Hence the proposed protocol 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, Kim and Yoo protocol password typed protocol which becomes not practical if $n > 100$.

7. Conclusions

[In this paper, we have shown that Lee, Kim and Yoo password-typed key agreement *protocol [15] is vulnerable to the password guessing attack and stolen verifier attack. To avoid these attacks, we presented a modified verifier-typed key agreement scheme relied on Lee, Kim and Yoo protocol and demonstrate that the propose scheme 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 schemes using authenticated key agreement has received high attention in the last decade. In practice, password-typed protocols 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-typed scheme.

[Different channel characteristic and different environment need to be studied to determine further useful relations. Since multiple channels might increase overheads, studies might be done to consider the best environment combinations to reach high security at the least cost. Work also remains to be done to formalize these schemes.]

References

[1] Diffie W and Hellman M, "New Directions in Cryptography", IEEE Transactions on Information Theory IT-11, pp. 644-654, November 1976

[2] Menezes A.,Oorschot P. van and Vanstone S, "Handbook of Applied Cryptography", CRC Press, 1996

[3] Schneier Bruce, "Applied Cryptography: Protocols and Algorithms", John Wiley and Sons, 1994

[4] Mel H, Baker Doris M and Burnett Steve, "Cryptography Decrypted", Addison-Wesley, 2004

[5] Bellare Mihir and Rogaway Phillip, "Provably Secure Session Key Distribution-The Three Party Cases", Proceedings of the 27th annual ACM symposium on Theory of computing STOC '95, ACM Press, May 1995

[6] Gong L, Lomas M, Needham R and Saltzer J, "Protecting Poorly Chose Secrets from Guessing Attacks", Selected areas of communications, vol. 11, no. 5, pp. 648-656, June 1993

[7] Lomas T, Gong L, Saltzer J and Needham, "Reducing Risks from poorly chosen Keys", ACM SIGOPS Operat, System Review, 23: 14-18, 1989

[8] Jablon D, "Strong password-only authenticated key exchange", SIGCOMM Computer Communication Review, vol. 26, no. 5, pp. 5-26, 1996.

[9] Halevi S and Krawczyk H, "Public key cryptography and password protocols", ACM Transactions on Information and System Security, pp. 524-543, 1999.

[10] Boyarsky M, "Public-key cryptography and pass-word protocols: The multi-user case", ACM Security (CCS'99), pp. 63-72, 1999.

[11] Bellare M, Pointcheval Dand and Rogaway P, "Authenticated key exchange secure against dictionary attacks", Eurocrypt 2000, LNCS 1807, pp. 139-155, Springer-Verlag, 2000

[12] Boyko V, MacKenzie P and Patel S, "Provably secure password-authenticated key exchange using Diffie-Hellman", Eurocrypt 2000, LNCS 1807, pp. 156-171, Springer-Verlag, May 2000

[13] Bresson E, Chevassut O and Pointcheval D, "New security results on encrypted key exchange," in PKC 2004, LNCS 2947, pp. 145-158, Springer-Verlag, Mar. 2004.

[14] Kim Y, Hub B, Hwang J and Lee B, "An Efficient Key Agreement Protocol for Secure Authentication", ICCSA 2004, LNCS, 3043: 746-754, 2004

[15] Lee S, Kim W, Kim H and Yoo K, "Efficient Password-based Authenticated Key Agreement Protocol", In ICCSA, LNCS, 3046: 617-626, 2004

[16] Kwon T, "Practical Authentication Key Agreement Using Passwords", ISC 2004, LNCS, 3255:1-12, 2004

[17] Yoon E and Yoo K, "New Efficient Simple Authenticated Key Agreement Protocol", COCOON 2005, LNCS, 3595: 945-954, 2005

[18] 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

[19] Bellovin 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

[20] YShakir M. Hussain and Hussein Al-Bahadili, "A non-exchanged password scheme for password-based authentication in client-server systems", American Journal of Applied Sciences, 2008

[21] SeongHan Shin, Kazukuni Kobara and Hideki Imai, "A Secure Threshold Anonymous Password Authenticated Key Exchange Protocol", Crypto 2009, LNCS, Springer-Verlag, 2009

[22] Shim, K and Seo S, "Security Analysis of Password Authenticated Key Agreement Protocols", CANS, LNCS, 3810: 49-58, 2005.

تطوير نظام كلمات مرور سرية كفوء اعتمادا على برتوكول اتفاق المفتاح

د. ستار جبار عبد
مستشار تكنولوجيا المعلومات في البرلمان العراقي

د. حيدر ستار جبار
كلية المنصور الجامعة

المستخلص :

في هذه الورقة سنقوم بدراسة نظام كلمات المرور السرية المطورة من قبل لي, كيم و يو ونثبت ان هذا النظام غير امن. ثم سنقوم بأقتراح نظام محسن اعتمادا على نظام لي, كيم و يو المعتمد على نظام اتفاق المفتاح ونثبت من ان النظام المقترح يقاوم هجوم تخمين الكلمات السرية وكذلك يقاوم هجوم المدقق السارق. يدعي كاتبوا الورقة من ان النظام المقترح هو اكثر امنا مقارنه بنظام لي, كيم و يو الذي لا يزال موجود ومطبق ليومنا هذا.