A study on simple key exchange and password authenticated protocol

Abstract

Internet has its widespread use due to continuous progress in information technology, the information exchange model among enterprises changes accordingly. After the open key concept has been proposed, authentication process can be done even when both sides of transaction don't know each other, this is to ensure communication security and prevent the leak of transmission data.

This study try to build an improved multiple persons key exchange and password authentication protocol system based on the spirit of key agreement and password authentication protocol, this is to stop in time the attacking purpose from a faked person by using password faked method and reflection method, therefore, identity can still be proved without the release of password from the user, and the goal of zero knowledge can thus be easily achieved.

Key word：Key exchange and password authentication, congruence equation in two unknowns, discrete logarithm, reflection attack method, zero knowledge

1. Preface

Internet can reach almost anywhere , it greatly shorten the distance between two points , massive data has been exchanged nowadays through internet channels , this convenience brings lots of business opportunity ,but it also brings people's interest to spy into the transmitted data , the environment of internet it thus very insecure . In the past , Kwon and Song et al. have proposed "A Study on the Generalized Key Agreement and password Authenticated protocol "[2], its main purpose is to ensure a secure channel is used for message transmission between both communication sides , therefore , even if related data is stolen by the faked person , it's still useless to the faked person unless the discrete logarithm problem can be solved, that is, Diffie-Hellman problem can be solved[1]. Later on , many scholars proposed different versions of attacking methods [3,4] targeting at [2]. This study is based on a core spirit of [2], it improves the original communication architecture, besides, it not only prevents effectively the current attacks, but also removes the limitation on the communication of both sides set by the original version. In section 2, the Kwon-Song protocol system is going to be reviewed, the investigation on the attacking methods by Yeh et al. are going to be reviewed in section 3, the reflection attacking methods by Ku et al. are going to be reviewed in section 4 , and the group key exchange and password authentication protocol proposed by this article are going to be reviewed in section 5 , the conclusion and future studies are going to be put in the last section .

2. Review on Kwon-Song Protocol

In 2000 , Korean scholars Kwon and Song proposed a concept of generalized key agreement and password authentication protocol , the main features of this method that are different than traditional methods are , under key environment , it authenticates the open key mechanism so that the security of the key and the whole system is reached . For instance , [5,6,7] are two party authentication , [8] is three party authentication , all these belong to the traditional protocol of the traditional open key infrastructure , the Kwon-Song version is suitable for any operation of limited cyclic group , it is based on the following principles：

Symbol descriptions：

A : represents User A , here it is Alice

B : represents User B, here it is Bob

E : represents User, here it is faked person Emma

P: represents Concatenation, that is, the link

$A \to B$: represents User A transfers to User B

Alice and Bob have agreed in advanced to use a common Random Oracle and shared a weak secret S on secure channel）, both sides agree to perform communication protocols based on the same Generator G and a multiplying group Z_p^*. Alice selects arbitrarily any two random integral variables α and x, their values fall in the range of $2 \leqq \alpha$ and $x \leqq P-2$, in the mean time , the results of formula（1）and（2）are calculated .

g^{α} （1）

$g^{\alpha+h_1(s,g^{\alpha})}$ （2）

The result is then sent to Bob, $h()$ is one way hash function, and $g^{\alpha+h_1(s,g^{\alpha})} = g^{x} g^{h_1(s,g^{\alpha})}$, before getting the reply from Bob , Alice can use the idle time to calculate the value of $-xs \mod P-1$.

1. $A \rightarrow B: A \| g^{\alpha} \| g^{x+h_1(s,g^{\alpha})}$ （3）

Bob acquires the password s transferred by Alice from the secure local storage, he also selects two random integral variables l and y , their values fall in the range of $2 \leqq l$ and $y \leqq P-2$, to calculate formula（4）

$(g)^{y}(g^{\alpha})^{ls}$ （4）

Bob has set $b_0 = g$,$b_1 = g^{\alpha}$,$e_0 = y$,$e_1 = ls$ as effective architecture , he transfers the cipher text back to Alice and waits for response , formula（5）is then calculated

$(g^{x+h_1(s,g^{\alpha})})^{y}(g)^{-yh_1(s,g^{\alpha})}$ （5）

Bob has set $b_0 = g^{x+h_1(s,g^{\alpha})}$,$b_1 = g$,$e_0 = y$,$e_1 = -yh_1(s,g^{\alpha})$, he can get the secret key value of common protocol $K = h_4(g^{xy})$ through $(g^{x+h_1(s,g^{\alpha})})^{y}(g)^{-yh_1(s,g^{\alpha})} = g^{xy}$.

2. $A \leftarrow B: l \| g^{y}(g^{\alpha})^{ls}$ （6）

Alice can use her own private key values（ x and the $-xs$ value obtained by calculation in advance）based on the messages transferred by Bob（as formula 6）to analyzed and solve formula（7）

$(g^{y+\alpha ls})^{x}(g^{x})^{-xls}$ （7）

Alice has set $b_0 = g^{y+\alpha ls}$,$b_1 = g^{\alpha}$,$e_1 = x$,$e_1 = -xls$, and thus $(g^{y+\alpha ls})^{x}(g^{x})^{-xls} = g^{xy}$, she can also obtain the secret key value of common protocol $K = h_4(g^{xy})$, she then passes the value by calculating $h_2(g^{\alpha}, K)$ to Bob.

3. $A \rightarrow B: h_2(g^{\alpha}, K)$ （8）

Bob receives the value h_2 transferred by Alice, it is then compared to a self-generated value h_2' , if $h_2 = h_2'$, then Alice is authenticated, and $h_3(l, K+1)$ is replied Alice.

4. $A \leftarrow B: h_3(l, K+1)$ （9）

At this moment , Alice also receives the message h_3 （as formula 9）transferred from Bob, she also compares self-generated h_3' to h_3 , if $h_3 = h_3'$, the authenticate Bob, from now on , both sides agree the protocol key value is K , the trust mechanism for future mutual communication is then built .

The complete communication protocol is summarized and briefly described as follows：

$$\left.\begin{array}{l} 1. A \rightarrow B: A \| g^{\alpha} \| g^{x+h_1(s,g^{\alpha})} \\ 2. A \leftarrow B: l \| g^{y}(g^{\alpha})^{ls} \\ 3. A \rightarrow B: h_2(g^{\alpha}, K) \\ 4. A \leftarrow B: h_3(l, K+1) \end{array}\right\} \quad (10)$$

However , Kwon-Song think the original version, that is, formula 10 ,can be simplified from four steps into three steps , meanwhile , the Generator G based on originally mutual common protocol can be additionally added with a new Generator η , it forces another communication side（takes Bob as an example）to select η , and makes it to have the same cyclic group as that of Generator G, then $g^{\alpha} \equiv \eta (\mathrm{mod}\, P)$ has $G.C.D(a, P-1) = 1$ effect on Z_p^* multiplying group, or has $G.C.D(a, P-1) = 1$ effect on subgroup of g

order. Based on these , the simplified communication protocol can be summarized as three steps as in the followings：

$$\left.\begin{array}{l} 1.A \to B:\eta^{\alpha} \mathrm{P} g^{x+h_1(s,g^{\alpha})} \\ 2.A \leftarrow B:l \mathrm{P} g^{y}\eta^{\alpha ls} \mathrm{P} h_2(\eta^{\alpha},K) \\ 3.A \to B:h_3(l,K+1) \end{array}\right\} \quad (11)$$

For easy distinguishing purpose, formula 10 is called original version, and formula 11 is called enhanced version.

3. A study on the attacking method version proposed by Yeh et al.

In 2001, Yeh et al. proposed security analysis on Kwon-Song version [3], Chu et al. think if off-line password is used to guess attacks, enhanced version then exists relative high insecure issue. Yeh et al. further pointed out , the attackers can store locally in advance the released information（or known related parameters and authentication information）,therefore , while still off-line , try to find password S（weak secret password）which satisfies authentication formula. Since it is off-line , the server can not predict off-line guessing attacks . Faked person Emma first selects guessed password s' and two random integers α and x to calculate $\eta^{\alpha} \mathrm{P} g^{x+h_1(s',g^{\alpha})}$, then the calculated result is sent to Bob, at this moment, Emma can pretend to be Alice to cheat Bob.

The cheating steps are as in the followings：

$$Eve \to B:\eta^{\alpha} \mathrm{P} g^{x+h_1(s',g^{\alpha})} \quad (12)$$

After Bob receives the message from Emma, he follows the normal procedures to retrieve the parameter s locally, in the mean time , two integers l and y are randomly selected to calculate $K=h_4((g^{x+h_1(s',g^{\alpha})})^{y} g^{-yh_1(s,g^{\alpha})})$, then $g^{y}\eta^{\alpha ls}$ is calculated and the message（formula 13）is sent back to Emma.

$$Eve \leftarrow B:l \mathrm{P} g^{y}\eta^{\alpha ls} \mathrm{P} h_2(\eta^{\alpha},K) \quad (13)$$

At this moment ,Emma receives the result sent from Bob, and sends the message（formula 13）to be stored locally, then according to the off-line password attacking method , Emma will select another password s'' to calculate $R=g^{y}\eta^{\alpha ls}\eta^{-\alpha ls''}$, since α is selected by Emma and l is Plaintext data, Emma can then get $K'=h_4((R)^{x+h_1(s',g^{\alpha})-h_1(s'',g^{\alpha})}$, and compare if $h_2(\eta^{\alpha},K)$ and $h_2(\eta^{\alpha},K')$ is the same , if they are the same , Emma then have a right guess on the password , contrarily , another password will be selected until the target is hit .

4. An analysis on the attacking method version proposed by Ku et al.

In 2004, Ku et al. proposed a security analysis on Kwon-Song original version [4], the major difference from that proposed by Yeh et al. is that it adopts reflection attacks, this is a Replay Attack, after the message is intercepted, it can still send back the intercepted message to the sender.

Its operation principles are described as in the followings:

Alice communicates with Bob starting from S1, and the faked person Emma communicates with Alice starting from S2.

$$
\left.\begin{array}{ll}
\text{S1/Step 1.} & A \to B(E): A \| g^{\alpha} \| g^{x+h_1(s,g^{\alpha})} \\
\text{S2/Step 1.} & B(E) \to A: B \| g^{\alpha} \| g^{x+h_1(s,g^{\alpha})} \\
\text{S2/Step 2.} & B(E) \leftarrow A: l \| g^{y} g^{\alpha ls} \\
\text{S1/Step 2.} & A \leftarrow B(E): l \| g^{y} g^{\alpha ls} \\
\text{S1/Step 3.} & A \to B(E): h_2(g^{\alpha}, K) \\
\text{S2/Step 3.} & B(E) \to A: h_2(g^{\alpha}, K) \\
\text{S2/Step 4.} & B(E) \leftarrow A: h_3(l, K+1) \\
\text{S1/Step 4.} & A \leftarrow B(E): h_3(l, K+1)
\end{array}\right\} \qquad (14)
$$

'$A \to B(E): message$' represents Emma has intercepted the message sent from Alice to Bob, and prevented Bob from receiving it. '$B(E) \to A: message$' represents that Emma pretends to be Bob and sends message to Alice. After S2/Step 3, Alice believes she is communicating with Bob, but actually, Emma has pretended to be Bob and performed the first authentication procedure to her; however, in S1/Step 4, Emma again pretends to be Bob and performs the second authentication to her.

We can clearly see that in the protocol of Kwon-Song original version, although the protocol key is not known by faked person Emma, smart attacker can still attack through the potential weak point leaked by the system . Ku et al. think, under certain enforced environment, the communication protocol design in original version does not use the protocol key K value to protect the attached message after an exchange agreement has been built between Alice and Bob.

For example, one identification mechanism architecture is used in the original protocol, the message followed is then not yet got protected by Message Authentication Code, MAC, or by protocol key K value .Therefore, Emma can easily pretends to be Bob to cheat Alice, Ku et al. suggest that the Step3 part can be modified from direction-independent to indirection-independent, this can thus prevent Reflection Attack. The steps are described as in the followings:

$$
\text{Step3}' \quad A \to B: h_2(g^{\alpha}, K, B) \qquad (15)
$$

Emma intercepts and sends message from S1/step 3 and S2/Step 3, since $h_2(g^{\alpha}, K, B)$ is not equal to $h_2(g^{\alpha}, K, A)$, therefore, Alice can reject the message decisively, and S2 step will then stop immediately. Based on the above, Emma will be unable to pretend to be Bob and reply to Alice in S1/Step 4, the whole communication will become failed due to failure on the authentication.

5. Group key exchange and password authentication protocol

5.1 Linear congruence equation

This section is based on congruence equation in two unknowns (congruence) as its architecture to enhance the endurance capability of the system to take attacks such as Dictionary Attack or Guessing Attack from the attackers. It forces both sides in the communication process to honestly use and activate password, the authentication can still be finished while a protocol key value K is generated between both sides, this can prevent the threat of Middle in Man Attack , the communication process can be stopped immediately on the dishonest authentication or faked side during the message exchange process . The details are described as in the followings：

Secret key value： a, b, c, d

Private key value： u, v

Original root： g

$$
ax + b \equiv u \pmod{P} \qquad (16)
$$

$$
cx + d \equiv v \pmod{P} \qquad (17)
$$

$$
\Delta \equiv (ad - bc) \pmod{P} \qquad (18)
$$

$$
\Delta g \Delta^{-1} \equiv 1 \pmod{P} \qquad (19)
$$

$$x \equiv \Delta^{-1}(bv - du) (\text{mod } P) \quad (20)$$

$$(\Delta, P) = 1 \quad (21)$$

First, Alice want to have a common protocol with Bob , Alice randomly picks two positive integers a and b ,its value is limited to the range $2<a \le P-2$ and $2<b \le P-2$, and the system will randomly generate an integer x ($2 < x \le P-2$) to calculate $ax+b \equiv u \pmod{P}$, the calculated result (formula 22, 23) will then be transferred to Bob.

$$g^{u+x} \quad (22)$$

$$g^{x} \quad (23)$$

Bob will also pick randomly two integers c and d ,their values will be limited to the range $2<c \le P-2$ and $2<d \le P-2$ to calculate $cx+d \equiv v \pmod{P}$ $A \rightarrow B: A, g^{u}, g^{u+x}$ (24)

Bob receives the message from Alice (formula 24) , and set $b_0 = g^{u+x}$,$b_1 = g^{v}$,$e_0 = v$,$e_1 = -x$ to calculate $(g^{u+x})^{v} (g^{v})^{-x} = g^{uv}$, Bob will then get common protocol key $K = g^{uv}$.

$$A \leftarrow B: B, g^{v}, g^{v+x} \quad (25)$$

Alice will then activate u and set $b_0 = g^{v+x}$,$b_1 = g^{u}$,$e = u$,$e_0 = -x$ according to the message transferred from Bob (formula 25)in order to obtain common protocol key $K = (g^{v+x})^{u} (g^{x})^{-u} = g^{uv}$.

$$A \rightarrow B: A, g^{a}, g^{b}, (A, K) \quad (26)$$

Alice then transfer g^{a} and g^{b} to Bob and calculate $(g^{v})^{-b}$ in advance.

After Bob receives g^{a} and g^{b} from Alice , he can obtain $\Delta = (g^{a})^{d} (g^{b})^{-c} \equiv g^{(ad-bc)}$ through secret key c and d , then use Δ value to calculate its multiplying reverse element $\Delta^{-1} \Delta \equiv 1 \pmod{P}$ .The $(g^{b})^{-v}$ value will be calculated first and verify $\Delta x = \Delta^{-1} (g^{u})^{d} (g^{b})^{-v} \equiv x \pmod{P}$, if they are equal , then authenticate Alice , and send back g^{a} and g^{c} to Alice.

$$A \leftarrow B: B, g^{d}, g^{c}, (B, K) \quad (27)$$

When Alice receives g^{d} and g^{c} sent from Bob , she can calculate to obtain $\Delta = (g^{d})^{a} (g^{c})^{-b} \equiv g^{(da-cb)}$ through secret keys a and b , then use Δ to get its reverse element , in the mean time , $\Delta x = \Delta^{-1} (g^{d})^{u} (g^{v})^{-b} \equiv x \pmod{P}$ can be verified , if it is equal ,then the authentication to Bob is approved . From now on , Alice and Bob has a common protocol key K .

5.2 Coding and security analysis

5.2.1 Coding

$$A \equiv g^{u} (\text{mod } P) \quad (28)$$

$$B \equiv g^{v} (\text{mod } P) \quad (29)$$

If Alice wants to transfers (A, z) to Bob, she can let $z \equiv B^{u} m (\text{mod } P)$ .After Bob receives (A, z) , he then sets $t = P-1-v$ to calculate $m \equiv A^{t} z (\text{mod } P) \equiv K^{-1} z (\text{mod } P)$ in order to recover plaintext m .

Proof：

$$\left.\begin{aligned} & m \equiv A^{t} z (\text{mod } P) \\ & A^{t} z \equiv (g^{u})^{P-1-v} (g^{v})^{u} m (\text{mod } P) \\ & \equiv g^{uP} g^{-u} g^{-uv} g^{uv} m (\text{mod } P) \\ & \equiv (g^{P-1})^{u} m (\text{mod } P) \\ & \equiv 1 m (\text{mod } P) \qquad \text{Q 費馬小定理 } g^{P-1} \equiv 1 (\text{mod } P) \end{aligned}\right\} \quad (30)$$

End of proof.

5.2.2 Security analysis

If the faked person Emma randomly pick two integers a_e and b_1 to calculate $a_e x + b_e \equiv u_e \pmod{P}$, $\Delta_e \equiv (a_e d - b_e c) \pmod{P}$ can then be obtained, and through $\Delta_e g \Delta_e^{-1} \equiv 1 \pmod{P}$.

$$A_e \equiv g^{u_e} \pmod{P} \quad (31)$$

$$K_e \equiv (g^{u_e + x})^v (g^v)^{-x} \equiv g^{u_e v} \pmod{P} \quad (32)$$

$$a_e x + b_e \equiv u_e \pmod{P} \quad (33)$$

$$\Delta_e \equiv (a_e d - b_e c) \pmod{P} \quad (34)$$

$$\Delta_e g \Delta_e^{-1} \equiv 1 \pmod{P} \quad (35)$$

$$\Delta x_e \equiv \Delta_e^{-1} (d u_e - b_e v) \pmod{P} \quad (36)$$

For congruence equation in two unknowns, there is a single and only solution ,that is , $\Delta \equiv (ad - bc) \pmod{P}$ and $x \equiv \Delta^{-1} (bv - du) \pmod{P}$, if formula (35) is correct , then formula (36) is also correct, and formula (35) is always equal to formula (19), and formula (36) is always equal to (30).

From the above, we know that congruence equation in two unknowns has more than two sets of solutions, this is obviously contradictory to the result. Therefore , $\Delta \neq \Delta_e$ and $\Delta^{-1} \neq \Delta_e^{-1}$, formula (34) is not equal to formula(18), formula(35)to(36)generated by formula (34) must be contradictory to each other. Unless correct secret keys a and b are owned to calculate corresponding reflection u value ,then through cross computation(formula 26 to 27)to obtain Δ, and use Δ to deduce its multiplying reverse element Δ^{-1}, Δ^{-1} can not be calculated correctly if Δ can not be known .

For communication system of more than three persons , the modification is as follows：

$$\begin{cases} a_1 x + b_1 \equiv c_1 \pmod{P} \\ a_2 x + b_2 \equiv c_2 \pmod{P} \\ a_3 x + b_3 \equiv c_3 \pmod{P} \end{cases} \quad (37)$$

Proof: neglected.

6. Conclusions

The concept of key exchange has widespread use in the business for a long time, for instance, SSL and PKCS all have their origins from such spirit, such algorithm is based on the difficulty to solve the discrete logarithm. There is still the possibility to leak the information if both sides are communicate under insecure channels, this article performs mutual parameter exchange based on linear congruence equation combined with the complexity to solve discrete logarithm, this is to ensure the authentication procedures to be completed without releasing the parameters from both communication sides, therefore, any possible leak of information can be minimized, and the zero knowledge requirement can be achieved.

7. References

1. W. Diffie and M. E. Hellman, New direction in cryptography, IEEE transaction on Information Theory, Vol. IT-11, pp. 644-654, Nov. 1976.
2. T. Kwon and J. Song, A study on the generalized key agreement and password authentication protocol, IEICE transaction on Communication, Vol. E83-B, No.9, pp.2044-2050, Sep. 2000.
3. Her-Tyan Yeh, hung-Min Sun and Tzonelih Hwang, Security Analysis of the Generalized Key Agreement and Password Authentication Protocol, IEEE Communication Letter, Vol. 5, No.11, pp.462-463, Nov. 2001.
4. Wei-chi Ku, Hui-Lung Lee and Chien-Ming Chen, Reflection Attack on a Generalized Key Agreement and Password Authentication Protocol, IEICE transaction on Communication, Vol. E87-B, No.5, pp.1386-1388, May. 2004.
5. Alain Mayer and Moti Yung, Secure protocol transformation via “expansion”: from two-party to groups,

Proceedings of the 6th ACM conference on Computer and communications security, Nov. 1999.
6. Philip MacKenzie, Alina Oprea and Michael K. Reiter, Cryptographic protocols/ network security: Automatic generation of two-party computations, Proceedings of the 10th ACM conference on Computer and communication security, October 2003.
7. Yehuda Lindell, Bounded-concurrent secure two-party computation without setup assumptions, Proceedings of the thirty-fifth annual ACM symposium on Theory of computing, June 2003.
8. Chun-Li Lin, Hung-Min Sun and Tzonelih Hwang, Three-party encrypted key exchange: attacks and a solution, ACM SIGOPS Operating Systems Review, Vo. 34, Issue 4, Oct. 2000.