International Journal of Science Engineering and Advance Technology, IJSEAT, Vol1, Issue 7, December - 2013 | ISSN 2321-6905

International Journal of Science Engineering and Advance Technology

Digital Signature and Key Agreement

[1]Krishna Kant, [2]Fahim Iqbal , [3]Md Irshad Alam

[1] Research Scholar, B. R. Ambedkar University, Muzaffarpur, India, natkhatkk@gmail.com
[2] Fahim Iqbal, Department of I T, L N Mishra College of Business Management, Muzaffarpur
[3] Md Irshad Alam, Research Scholar, MIT, Muzaffarpur, India

ABSTRACT

Diffie Hellman key exchange protocol is the most commonly used protocol. This protocol is used to exchange keys in a network. But it has bit m to exchange keys over a network but it has some drawbacks. This is the first proposed algorithm through which parties can exchange information without knowing each other. This algorithm permits exchange even over a insecure networks. Hellman algorithm was introduced by Martin Hellman and Whitfield Diffie in 1976. It is useful over a large number of authenticated protocols. Moreover, it works on transport layers too. In this research efforts are being made to declare new agreement protocol based on key confirmation and Diffie Hellman algorithm as well. This work also ensures the digital signature standard (DSS) with the help of Diffie-Hellman key exchange protocol by making use of two integers randomly. This protocol also performs on the elliptic curve cryptography in asymmetric encryption.

Keywords

Digital signature standard, Diffie exchange algorithm, Random number, Key agreement, Diffie-Hellman protocol, Public key cryptography.

.

1. INTRODUCTION

Very first time Arazi proposed a scheme for the combination of both Diffie-Hellman key exchange protocol and digital signature [1]. Few years later Harn et.al gave some modifications in the algorithm to prevent known and unknown key attacks [2]. Finally Phan modified this scheme with two major attributes i.e. forward secrecy and key freshness [3]. In this paper we have emphasized on the concept of key freshness by making use of the randomly selected number and verifying the standards of digital signature.For the establishment of the communication the parties requires the session key which can be generated by the key establishment protocol and it can also be refers as the key agreement protocol. For the key agreement the first famous protocol developed by Diffie and Hellman which was based on asymmetric encryption or public key cryptography [4]. They proposed the two versions of protocols. In the first protocol all the entities in the communication network exchange the static public keys. In this scenario there is a shortcoming that the entities A and B computes the same session key for each run of protocol, and in the second case they exchange the ephemeral public keys which is vulnerable to the man-in-middle attack. For overcoming of these situation a authenticated key agreement is proposed, which is the combination of both static and ephemeral versions of two entities A and B which meets all security attributes [5].

2. BACKGROUND

In this protocol we require to know that two publicly known numbers i.e. p and g which will be the primitive roots of p. Suppose two users A & B want to exchange a key which is unknown to each other. First time user A selects a random Integer XA <p and computes YA = g XA modulo p. Further, user B selects a random number XB <p and computes YB = g XB modulo p. Individual side keeps the value of X privately and Y will be available publicly to the another side, this is called public key for both users A & B. This process is known as the public key generation for A & B. Now user A evaluates the key as K= (YB) XA modulo. p and user B evaluates the key K= (YA) XB modulo p. Both these values should produce the same result [6].

The Diffie-Hellman [7] proposed a cryptosystem which is based upon the difficulty of finding discrete logarithm in field. For this protocol we need to know that two publicly known numbers that are p and g which will be the roots (primitive) of p. Suppose there

are two users A & B which want to exchange a key and unknown to each other. First time user A selects a random Integer XA <p and computes YA = g XA modulo p. Similarly, a random number is selected by user B XB <p and computes YB = g XB modulo p. Each one keeps the value of X privately and makes the Y value available publicly to the other side, this is known as public key for both A & B. Thus process is referred as the public key generation for A & B. Now user A computes the key as K= (YB) XA modulo p and user B computes the key K= (YA) XB modulo p. These two values should produce similar result.

Table 1. Public Key Generation

$K = (Y_B)^{X_A} \bmod p$

$= (g^{X_B} \bmod p)^{X_A} \bmod p$

$= (g^{X_B})^{X_A} \bmod p$ (By the rule of modular arithmetic)

$= g^{X_B X_A} \bmod p$

$= (g^{X_A})^{X_B} \bmod p$

$= (g^{X_A} \bmod p)^{X_B} \bmod p$

$= (Y_A)^{X_B} \bmod p$

Above result indicates that the two sides can change the secret value and these values are alike with each other.

3. RELATED WORK

The Diffie-Hellman key algorithm is the first proposed public key algorithm by which two parties can communicate with each other without having any prior knowledge of each other over an insecure communication channel proposed by Harn.et.al. Diffie-Hellman key exchange algorithm is quite popular algorithm to exchange keys over a network but it has few shortcomings [8].

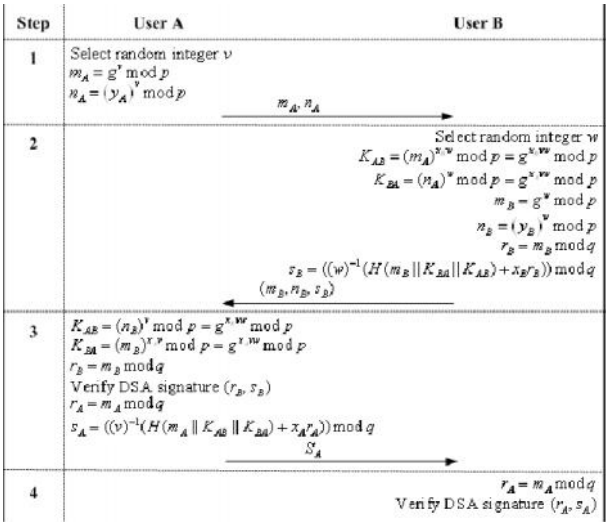
To establish the communication the parties need the session keys that are produced by the key establishment protocol and referred to as key agreement protocol. Diffie and Hellman made the very first popular key agreement protocol. This agreement protocols is based on public key cryptography or asymmetric encryption [9].

They made the two versions of protocols. First protocol shows that exchange of static keys takes place in the communication network. But in this situation there is a problem that both the entities A & B compute similar session key on execution of protocol. In another case they exchange the ephemeral public keys. These keys are vulnerable to the man-in-middle attacks.

3.1 Phan's Digital Signature Algorithm

Phan [4] combined these computations used in Diffie-Hellman key exchange protocol into the Digital Signature algorithm as follows:

Table 2. Digital Signature Algorithm



4. PROPOSED WORK

For authenticated key distribution, aforementioned integration was performed by Phan. We made effort only to reevaluate and investigate the piece of work done by Phan. We have also tried to show the accuracy of digital signature standard algorithm along with Diffie-Hellman key exchange protocol [10]. Digital signature standard approach with Diffie Hellman protocol is as follows.

The input in the form of hash code along with random number is given to signature function. Here K is generated for signature [11]. Moreover this signature function depends upon both the sender A's private key X_A and integer g selected globally.

If digital signature produces the result that contains two parts s and r then the generated output of the

verification function will be equal to the considered value in sighing function 'r' if signature is true [12].

If there are three public key parameters p, q, g. Where p denotes a prime number selected with a length bit 512 & 1024 bit. i.e. $512 \leq L \leq 1024$ and L is multiply of 64, q divides (p-1) and bit length 160 bits (160 prime number) and g is the $h^{(p-1)/q}$ mod p (h is any integer).

Here now user selects a private random integer number as in the case of Diffie-Hellman protocol $\mathbf{X_A < p.}$ By this we can produce the user's public key $\mathbf{Y_A = g^{X_A} \bmod p}$. In digital signature standard approach user can select a secret number k per message selected randomly. This can be done by any algorithm of random number in the range of $0 < k < q$.

The system proposed performs as follows. Notations being used in the protocol are given in the Table 3.

Table 3. Notations

A,B	Entities
IDA, IDB	Identity parameter of A,B
G	Generator Point
E k (x)	Encryption of x using the key k
D k (x)	Decryption of x using the key k
KRA	Static private key of A
KUA	Static public key of A which is elliptic curve point i.e. KRA.G
rA	A's ephemeral key (Random no.)
K	Session key between entities
A→B: M	Sending of message M From A to B
SgnA	Signature using private key of A
SK	Session key between A and B

Similarly for B KRB, KUB, and rB

The protocol works on the parameter of elliptic curve that are common to both entities. The parameter cover an elliptic curve E that is defined upon a field Fq and generates a point G. G belongs to E (Fq). Here n is in the order of G, E (Fq), whereas h is cofactor of n.

$r = (g^k \bmod p.) \bmod q$

$s = [K^{-1} H(M) + X_A r] \bmod q$

Signature will be (r, s)

$w = (s')^{-1} \bmod q$

$v_1 = [H(M') w] \bmod q$

$v_2 = (r') w \bmod q$

$r' = [(g^{v1} Y_A^{v2}) \bmod p] \bmod q$

Where M = Message to be signed

H (M) = Hash of using SHA-1

M' r's' = Received version of M, r, s.

5. RESULT

Verification and proof of correctness is shown below (r = r') so that its correctness can be prove as the same message received by the receiver send by the sender. In the verifying step.

$r' = [(g^{v1} Y_A^{v2}) \bmod p] \bmod q$

$= (g^{H(M) w \bmod q} Y_A^{r w \bmod q} \bmod p) \bmod q$

$= (g^{H(M) w \bmod q} g^{X_A r w \bmod q} \bmod p) \bmod q)$

$= (g^{H(M) w + X_A r w \bmod q} \bmod p) \bmod q$

$= (g^{(H(M) + X_A) w \bmod q} \bmod p) \bmod q$

$= (g^{(((H(M) + X_A r) k H(M) + X_A r)^{-1} \bmod q} \bmod p) \bmod q$

$= (g^k \bmod p.) \bmod q$

$= r$

This correctness provides the authentication to the sender and receiver that a message which is signed is intended for the appropriate users.

For the establishment of any session the entities need a session key and for sharing of a session key they should know the public key of each other this process can be done by the certificate authority [13] which provides CAA i.e. A's certificate congaing the public key and the

signature of A. the proposed protocol will work as follows.

The communicating entities will take the public keys of each other with the help of certificate authority. Now A will have KUB and B will have KUA.

The session key K will be generated by using the KRA and KUB as K = KRA.KUB = KRA.KRB.G

In the next step a select a random number rA as its ephemeral key and computes a point on elliptic curve MA = rA KUB. After encryption of signed message with K the result is like.

A→B: IDB,EK(MA,SgnA (IDB,KUA,KUB))

With the same process like A,B will also find the value of K, and decrypts the message received from A, recovers MA and verify the signature sent by A.B will select again a random number rB as its ephemeral key and calculate the session key SK = h(rB KUA + MA).If SK = 0 then B can terminate the protocol. Otherwise B will send a message to A as A did in previous step.i.e.

B→A: EK (MB), ESK (SgnB (IDA, MA, MB))

After receiving the message from B, A decrypts with K to recover MB. The session key will be computed again with the help of KUB and MB if SK = 0 then A will terminate the protocol otherwise a message will be sent to B.

A→B: ESK (SgnA (IDA, MA, MB)

In the last step B will decrypt the received message using SK and verify the signature created by A. if the signature verified then B will store the session key SK. The multiplication by h in SK will ensure that the session key SK is a point in the subgroup of order n in E (Fq) to protect against small subgroup attack [14].

Table 4. Proof of Correctnes

For A

SK = h (rA.KUB + MB)
= h (rA.KUB + rB.KUA)
= h (rA.KRB.G + rB.KUA.G)
= h (rA.KRB + rB .KRA).G
= h (rB.KRA + RA.KRB).G
= Which is the SK of B.

For B

SK = h (rB.KUA + MA)
= h (rB.KUA + rA.KUB)
= h (rB.KRA.G + rA.KUB.G)
= h (rB.KRA + rA.KRB).G
= h (rA.KRB + r.KRA).G
= Which is the SK of A.

In this paper we provide some further cryptography and analysis on the Phan's integration of DSA and DIffie-Hellman Key exchange protocol. We present an improvement on protocol with the help of two randomly selected integers which makes the protocol more secure. Also these random numbers can provide two basic attribute for key exchange protocol i.e. 1) The forward secrecy as we have chosen the different random number each and every time as X_A and X_B which are private to both of users.2) Key Freshness as the public key of both user does not depend on each other it depends on the randomly selected value by users so key freshness can be maintained i.e. with the help of these random numbers we can generate a new key for every communication.

Security issue of proposed protocol works on the Diffie-Hellman problem in ECC.The proposed protocol provides known-key security because each run of the protocol between A and B should produce a unique session key which depends on rA and rB. The proposed protocol also provide the prevention against the meet-in- middle attack [5] in which an attacker fools both the communication parties in a legitimate conversation by creating two private, public key pairs. In the proposed protocol an attacker cannot forge the private keys of entities to create the signature. If it is possible then the signature will not be verified because of certificates provided by certificate authority.

6. EFERENCES

[1] A. Arazi, “Integrating a key cryptosystem into the digital signature standard," Electronic Letters, vol.29, pp. 966-967, Nov. 1993.

[2] L. Harn, Ma. Mehta, and W. J. Hsin, “Integrating Diffie-Hellman Key Exchange into the Digital Signature Algorithm (DSA)," IEEE Communication Letters, vol. 8, no. 3, Mar. 2004.

[3] W. Diffie and M. Hellman, “New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. IT-l 22, No.6, November,1976, PP.644-654.

[4] R. C. W. Phan, “Fixing the integrated diffie-Hellman - DSA key exchange protocol," IEEE Communication Letters, vol. 9, no. 6, Jun. 2005.

[5] Charanjit S. Jutla and Anindya C. Patthak. Is SHA-1 conceptually sound? Cryptology ePrint Archive, Report 2005/350, 2005.

http://eprint.iacr.org/.

[6] M. Matsumoto and T. Nishimura, "Weight Discrepancy Tests on M-sequences", Bulltin of Yamagata University (Natural Science), Vol. 16, No.3, 2007, 105--112.

[7] “Cryptography and Network Security” by William Stalling Fourth Edition.

[8] Rescorla, E., Diffie-Hellman Key Agreement Method, RFC 2631, IETF Network Working Group, http://www.ietf.org/rfc/rfc2631.txt

[9] Curry, Ian, Entrust Technologies, “Getting Acquainted With Entrust/Solo and Public-key Cryptography”, version 1.0, July 1997

[10] N. Howgrave-Graham and N. Smart, \Lattice attacks on digital signa- ture schemes", Designs, Codes and Cryptography, 23 (2001), 283-290.

[11] Bon Wook Koo, Hwan Seok Jang and Jung Hwan Song, Constructing and Crypt-analysis of a 16 £ 16 Binary Matrix as a Di®usion Layer. In K. Chae and M. Yung (Eds.): WISA 2003, LNCS 2908, pp.489-503, Springer-Verlag 2004.

[12] A. Lenstra and E. Verheul, "Selecting Cryptographic Key Sizes", Journal to Cryptology 14(2001) pp. 255 – 293, http:/www.cryptosavvy.com/

[13] Improved Authentication and Key Agreement Protocol UsingElliptic Curve Cryptography A. Chandrasekar, V.R. Rajasekar

NIST, "Special Publication 800-57: Recommendation for Key Management. Part 1: GeneralGuideline", Draft Jan.2003.