ISSN:0975-9646

Pratibha Lanka et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (6) , 2015, 5595-5598

A Novel Cryptographic Approach for Preventing Attacks in a Network

Pratibha Lanka[#1], Ch. Sita Kameswari[*2],

[#]*Student of M.Tech[CST], Department of Computer Science Engineering, BABA Institute of Technology and Sciences, Visakhapatnam, India.*

[*]*Professor, Department of Computer Science Engineering, BABA Institute of Technology and Sciences, Visakhapatnam, India.*

***Abstract*--"A Novel Cryptographic Approach for Preventing Attacks in a Network" mainly aims at handling a key agreement technique among the communicating users in a dedicated network. The proposed novel approach utilized the MQV key agreement protocol to ensure authentication among the users from intruders. An enhancement is done in MQV in terms of a "Hash Variant", and is termed as HMQV which generates a hash value for the identity of the other user. The output of this hash value is taken as f=|q|/2 where q is a prime order number. The ephemeral keys are obtained from users public/private key pairs ensuring the same secret session key generated among the communicating users.**

***Keywords*—MQV, Hash Variant, Ephemeral Keys, Secret Session Key.**

I. INTRODUCTION

The encryption and decryption of data between the users is termed as Cryptography. When transmitting the perceptive data or information over an insecure media cryptography enables the intruders cannot read the data or information except the authorized user. A secret key was established in between the communicating users agreeing upon a key exchange protocol which allows both the users to share data without any intruders influence or any other type of attacks [1].

The algorithms for key exchange protocol in cryptography plays a vital role in both the theory of cryptographic research and network security [2]. A public, private key pairs, secret session key, signature etc. were established to authenticate both the communicating users.

The main root of public-key cryptography in key exchange protocols is a Diffie-Hellman Key-exchange protocol [3]. It is the first key agreement protocol that shares a key over an insecure media. In this protocol both the communicating users agree on a key so that the eavesdropper cannot obtain the key. But there is no authentication support between the two users with the man-in-middle attack.

Due to this drawback, Menezes, Qu, Solinas and Vanstone developed a protocol popularly called MQV protocol which eliminates man-in-middle attack [4]. In MQV protocol a shared secret key is established between the two trusted users of their public keys generating dynamic public and private keys. An implicit signature is generated by using their own public key where a shared secret key is implemented. If any of the user's public key is not employed then an implicit signature will not be generated unless linked to the trusted public key. But MQV protocol is invalidate to different type of attacks and security goals such as Impersonation attacks, UKS attacks, KCI attacks etc .

A. Types of Attacks for which MQV Fails

1) Impersonation Attacks: Impersonation attack [5] is an attack where the user's identities will compromises in a malicious manner due to the lack of authentication in a communication media.

2) Unknown Key Share Attack: In an Unknown Key Share (UKS) attack [6] both the users believe that they are sharing the key in a secure communication media authenticating the key confirmation. But the fact is that the authentication key agreement is communicated in an insecure media by both the users which lead to authentication failure [7].

3) Key Compromise Impersonation Attack (KCI): In Key Compromise Impersonation (KCI) attack, where the eavesdroppers takes the advantage of having knowledge on the user's private key in a communication media [8].

So MQV protocol fails to different types of security attacks invalidating the authentication of the user's identity over a communication media. To overcome from these attacks, a "hash variant" protocol was proposed termed as HMQV that which maintains the same functionality, performance and fulfilment of the key protocol.

II. METHODOLOGY

A. Description of HMQV Approach

The HashMQV (HMQV) [9] is a very transparent and straightforward protocol variant of MQV. MQV generates a session key i.e., for both encryption and decryption same session key is generated among the users to ensure that they are communicating over a secure media.

For encryption and decryption a key is generated randomly called Session Key [10] which ensures the security over communication between the users. It is derived from a hash value. The key is transmitted along with the information and encrypted with user's public key throughout the each session.

The session keys that are generated by HMQV computation, key values contain hash value for the identity of the other user. The output of this hash value is taken as f=|q|/2 where q is a prime order number. In addition to that in HMQV, the length f of the desired session key considered as f-bit keys that which requisites the hashing values $\sigma\,\bar{A}$ must be equal to that of $\sigma\,\bar{B}$. So the hashing function of 'f ' bits outputs as $\bar{H}$ with f bit of H [11].

1) Confrontation to Impersonation Attack: Not knowing the private key of a user $\bar{A}$ which is a minimum requirement for communicating over a secure key exchange protocol the attacker will not be able to impersonate$\bar{A}$. MQV fails in handling this requirement. HMQV hold this security by generating the keys as d= $\bar{H}$(X, $\bar{B}$) and e= $\bar{H}$(Y, $\bar{A}$) which are fixed constants.

2) Confrontation to UKS Attacks: Comparing MQV with HashMQV(HMQV) the values of a session are termed as $\bar{A}$,$\bar{B}$, X, Y where X and Y are the sending and the receiving values over a communication media between the users. Both the users are communicating over a secure session if ($\bar{A}$, $\bar{B}$, X , Y) matches to that of ($\bar{B}$, $\bar{A}$, Y , X).

3) Confrontation to KCI attacks: In case of KCI attacks, the session key is computed with the ephemeral values [12]that means generating a key during execution of a key establishment process which are the designing principles of HMQV. The proposed designed principle of HMQV is that which contains the hashing of session key k where H ($\sigma\,\bar{A}$) must be same as H ($\sigma\,\bar{B}$).

So from the above comparisons HMQV protocol ensures all of the mentioned security attacks such as impersonation attacks, UKS attacks and KCI attacks.

An elaborated description about the extended key compromise impersonation (KCI) attack is presented by Qiang et.al,[8]. According to the authors the attacks like KCI may cause session's hazards to both the authenticated keys. Also the authors presented an approach for how to prevent such attacks.

The importance of reutilization of ephemeral keys is proposed by Alfred Menezes et.al,[13] in their publication. They mentioned that the use of ephemeral keys in key agreement protocol reduces the computational complexity of the protocol. Also they pointed out on how to launch the small subgroups attacks successfully on DH protocols.

B. The Algorithmic Computation of HMQV Key-Agreement Protocol

1: Domain Parameters are q (prime number), g (integer).
2: $\bar{A}$ and $\bar{B}$ are public key identities of both communicating users.
3:a and b are the private keys of $\bar{A}$ and $\bar{B}$ where a,bϵ[1,q-1].
4: A and B are public keys of $\bar{A}$ and $\bar{B}$.
5: x and y are the ephemeral private keys of $\bar{A}$ and $\bar{B}$ where x, y ϵ [1, q-1].
6: X and Y are the ephemeral public keys of $\bar{A}$ and $\bar{B}$.
7: H is a Hash function.
8: $\bar{H}$ is an f-bit hash function where f=|q|/2.
9: K is a session key.

Both communicating users compute same session key i.e K = H($\sigma\,\bar{A}$) = H($\sigma\,\bar{B}$).

C. The Key Agreement Technique of HMQV

INPUT: Domain parameters (q, g) , pre-established key pairs User1(private key, public key) = (a, A=g^a).
User2 (private key, public key) = (b, B=g^b).

OUTPUT: Shared session key K = H($\sigma\,\bar{A}$) = H($\sigma\,\bar{B}$).

step1: User1 choose a random number x and sends X=g^x to User2.
step2: User2 choose a random number y and sends Y=g^y to User1.
step3: User1 choose a random number a and compute key $\bar{A}$ as A = g^a and send to User2.
step4: User2 choose a random number b and compute key $\bar{B}$ as B = g^b and send to User1.
U1:
Step5: User1 checks that Y!=0 and compute the shared secret key $\sigma\,\bar{A}$.
Step6: compute $\sigma\,\bar{A}$ = $(YB^e)^{x+da}$.
U2:
Step5: User2 checks that X!=0 and compute the shared secret key $\sigma\,\bar{B}$.
Step6: compute $\sigma\,\bar{B}$= $(XA^d)^{y+eb}$.
Where d = $\bar{H}$ (X, $\bar{B}$) i.e. d = 2f+Xmod2f and
e = $\bar{H}$ (Y, $\bar{A}$) i.e. e = 2f+Ymod2f.
Both users User1 and User2 compute the same session key K i.e. K= H($\sigma\,\bar{A}$) = H($\sigma\,\bar{B}$).

D. Comparison between MQV and Proposed HMQV

The step-wise comparison of both MQV and HMQV protocols are described in Table [1] and Table[2]. The domain parameters of MQV key agreement technique are p,q and g. Where p and g are generated integers and q is a prime number. Similarly the domain parameters described in the proposed approach are q and g. Where q is a prime number and g is a generated integer.

TABLE I

MQV KEY AGREEMENT PROTOCOL

MQV	
USER 1	USER 2
1. Short term keys Public key = x Private key $X = g^x \bmod p$ 2. Long term keys Public key = a Private key $A = g^a \bmod p$ 3. Common key execution $\bar{X} = X \bmod 2^l + 2^l$ 4. Implicit Signature $S_A = (x + \bar{X} a) \bmod q$ 5. Public key $t_A = Y B^{\bar{Y}} \bmod p$ 6. Shared secret key $Z_A = (t_A)^{S_A} \bmod p$	1. Short term keys Public key = y Private key $Y = g^y \bmod p$ 2. Long term keys Public key = b Private key $B = g^b \bmod p$ 3. Common key execution $\bar{Y} = Y \bmod 2^l + 2^l$ 4. Implicit Signature $S_B = (y + \bar{Y} b) \bmod q$ 5. Public key $t_B = X A^{\bar{X}} \bmod p$ 6. Shared secret key $Z_B = (t_B)^{S_B} \bmod p$

TABLE II

HMQV KEY AGREEMENT PROTOCOL

HMQV	
USER 1	**USER 2**
1. Short term keys Ephemeral private key = x Ephemeral public key $X = g^x$ 2. Long term keys Private key = a Public key $A = g^a$ 3. Compute f-bit hash function $e = \bar{H} (Y, \bar{A}) = 2f+Y \bmod 2f$ 4. Compute Shared Session key $K = H(\sigma \bar{A})$ where $\sigma \bar{A} = (YB^e)^{x+da}$	1. Short term keys Ephemeral private key = y Ephemeral public key $Y = g^y$ 2. Long term keys Private key = b Public key $B = g^b$ 3. Compute f-bit hash function $d = \bar{H} (X, \bar{B}) = 2f+X \bmod 2f$ 4. Compute Shared Session Key $K = H (\sigma \bar{B})$. where $\sigma \bar{B} = (XA^d)^{y+eb}$.

E. Numerical Illustration for the Verification of Proposed Algorithm

Consider the domain parameters: q =2 and g=2.

	User1	User2
1:	x = 1	y = 2
2:	$X = g^x$ $= 2^1$ X = 2	$Y = g^y$ $= 2^2$ Y = 4
3:	a = 2	b = 1
4:	$A = g^a$ $= 2^2$ A = 4	$B = g^b$ $= 2^1$ B = 2

5: compute $\sigma \bar{A} = (YB^e)^{x+da}$ and $\sigma \bar{B} = (XA^d)^{y+eb}$.

6: $d = \bar{H} (X, \bar{B})$ i.e. $d = 2f+X \bmod 2f$ and
$e = \bar{H} (Y, \bar{A})$ i.e. $e = 2f+Y \bmod 2f$.

$d = 2f+X \bmod 2f$ and	$e = 2f+Y \bmod 2f$.
$= 2x1+2 \bmod 2x1$	$= 2x1+4 \bmod 2x1$
$= 2+2 \bmod 2$	$= 2+4 \bmod 2$
$=2+0$	$= 2+0$
$=2$	$= 2$

7: $\sigma \bar{A} = (YB^e)^{x+da}$ and	$\sigma \bar{B} = (XA^d)^{y+eb}$
$= (4x2^2)^{1+2x2}$	$= (2x4^2)^{2+2x1}$
$= (4x4)^{1+4}$	$= (2x16)^{2+2}$
$= (16)^5$	$= (32)^4$
$= 1048576$	$= 1048576$

III. CONCLUSIONS

The results in the proposed method reveal that the HMQV is predominantly better than the MQV in terms of Impersonate attacks, UKS attacks and KCI attacks. Due to introduction of hash variant in key establishment process the computational weight of the proposed algorithm has been reduced while comparing with existing MQV approach. Hence in this work an improved Diffie-Hellman key exchange technique is introduced by incorporating the existing protocols in public key cryptography with much secure and safe while exchanging the keys between the two users. The proposed algorithm has been verified successfully with numerical values.

REFERENCES

[1] Paul Krzyzanowski, "Lecture Notes on Cryprography", Rutgers University, CS-417, pp 1-4, 2006.

[2] William Stallings, Cryptography and Network Security: Principles and Practice, 5th edition.

[3] W.Diffie and M.Hellman, " New directions in Cryptography " IEEE Transaction on Information Theory, 22 (1976), 644-654.

[4] Law, Lauri, AAlfred Menezes, Minghua Qu, jerry Solinas and Scott Vanstone (1998), "An Efficient protocol for Authenticated Key Agreement, Technical report CORR 98-05,University of Waterloo, Canada March 1998.

[5] Law, Lauri, AAlfred Menezes, Minghua Qu, jerry Solinas and Scott Vanstone (1998), "An Efficient protocol for Authenticated Key Agreement, Designs, Codes and Cryptography 28(2):119-134, 2003.

[6] Jr.B.S.Kaliski, "An unknown key-share attack on the MQV key agreement protocol. ACM Transactions on Information and System Security", 4(3):275–288, 2001.

[7] Liqun Chen, Qiang Tang, "Bilateral Unknown Key-Share Attacks in Key Agreement Protocols" July 1 2007.
[8] Qiang Tang, Liqun Chen, "Extended KCI attack against two key establishment protocol", Elsevier, Vol111, Issue 15, 15 Aug 2011.
[9] Hugo Krawczyk, HMQV: A High-Performance Secure Diffie-Hellman Protocol, July 2005.
[10] K R Chandrasekhara Pillai, M P Sebastian, "Elliptic Curve based Authenticated Session Key Establishment Protocol for High Security Applications in Constrained Network Environment", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010.
[11] Alfred Menezes, "Another Look at HMQV", Nov 2 2005.
[12] Alfred Menezes and Berkant Ustaoglu, "On the Importance of Public-Key Validation in the MQV and HMQV Key Agreement Protocols" R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 133–147, 2006. c Springer-Verlag Berlin Heidelberg 2006.
[13] Alfred Menezes and Berkant Ustaoglu, "On reusing ephemeral keys in Diffie-hellman key agreement protocols", International Journal of Applied Cryptography, Vol 2, Issue 2, pp 154-158, 2010.

Prof.Ch. Sita Kameswari M.C.A., M.Tech.
M.B.A (Ph.D.)
I/C Principal & Co-ordinator for PG Courses.
DEPT. OF COMPUTER SCIENCE & ENGINEERING
BITS VIZAG.

She is M.Tech (co-ordinator) BABA INSTITUTE OF TECHNOLOGY & SCIENCES, A lady of true vision towards modern professional education and deep routed values. Mrs. Ch.Sita Kameswari has come in association with BITS in the capacity of Professor, Dept. of CSE and PG Co-ordinator. She pursued her MCA in the year 1997 and M.Tech (CSE) with specialization in Artificial Intelligence and Robotics from Andhra University in the year 2008. Her quest for knowledge led her to attain the MBA degree from IGNOU. Currently she is at the verge of submission of her thesis with GITAM University for the award of Ph.D. She has a reckonable and meritorious experience of 15 years in the teaching field since 1997. During this period she served for various professional colleges like J.A.Karia college, Jamnagar, Gujarat; Boston college for professional studies, Gwalior, ANITS, Visakhapatnam etc. in the capacity of Asst. Professor, Associate Professor and also discharged the additional responsibilities as HOD of MCA and CSE. She was ratified for the post of Associate Professor by AU, Visakhapatnam and RGPV, Bhopal.

She has organized a joint International Conference on Swarm, Evolutionary and Memetic Computing (SEMCCO) and Fuzzy and Neural Computing Conference (FANCCO) at ANITS, Visakhapatnam successfully in the position of organizing secretary in the month of Dec 2011. She organized I CSI AP Student convention at ANITS in coordination with CSI successfully as co-convener She organized various national level student fests such as TECHNOCOM 2k6, AADYOTA-08, AADYOTA-09 in the institutions she worked with and earned the appreciation of one and all.

She had published her research papers in 2 international journals, 2 proceedings of international conferences and 2 national conferences. She also presented papers in international and national conferences. A few more papers of her are under processing for publication. She actively participated in about 20 workshops organized by Indian Science Congress and other professional bodies at various organizations. Her areas of interest are Artificial Intelligence, Computer Graphics, Object Oriented Software Engineering, Operating Systems, System Programming Machine Learning, and Neural Networks.

Mrs LANKA PRATIBHA
M.Tech [CST],
BITS Visakhapatnam.
Affiliated to JNTUK-Kakinada