www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 7 July, 2014 Page No. 7346-7349

A Study On Diffie-Hellman Algorithm in Network Security

Vinothini[1], Saranya[2], Vasumathi[3]

[1] Research Scholar, Department of Computer Science,
PGP College of Arts and Science, Nammakkal, Tamilnadu
vinothinijo@gmail.com

[2] Research Scholar, Department of Computer Science,
PGP College of Arts and Science, Nammakkal, Tamilnadu
vsaranyamani@gmail.com

[3] Assistant Professor, Department of Computer Science,
PGP College of Arts and Science, Nammakkal, Tamilnadu
vasumathibaskar@gmail.com

Abstract: ***Communication is the important part in any type of network for making it possible to transfer data from one node to another. Communication needs quality and security for better performance and for acceptance of users and client companies. Quality is dependent on size and some other factors of network but security is very concern parameter in network as it is independent of network size and complexity. Security has become more important to personal computer users, organizations, and the military. Security became a major concern with the advent of internet and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The modified architecture of the internet can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. Data integrity is quite a issue in security and to maintain that integrity we tends to improve as to provides the better encryption processes for security. In our proposed work we provide harder encryption with enhanced public key encryption protocol for security and proposed work can be implemented into any network to provide better security. We have enhanced the hardness in security by improving the Diffie-Hellman encryption algorithm by adding some more security codes in current algorithm.***

Keywords: Diffie-Hellman, Private Key, Public Key, Cipher.

1. INTORDUCTION

The entire field of network security is vast and in an evolutionary stage. The range of study encompasses a brief history dating back to internet's beginnings and the current development in network security. In order to understand the research being performed today, background knowledge of the internet, its vulnerabilities, attack methods through the internet,and security technology is important and therefore they are reviewe

Secure Sockets Layer (SSL) is a cryptographic protocol developed by Netscape in 1995. SSL V3.0 has since become the predominant method and de-facto standard for securing information flow between web users and web servers. This is most commonly done for business/financial traffic, e.g. credit card transactions. Specifically, "securing information" in this context, means to ensure confidentiality (prevent eavesdropping), authenticity (the sender is really who he says he is), and integrity (the message has not been changed en route). Users may not know they are using SSL, but they probably will notice the padlock.

Diffie-Hellman in SSH

Secure Shell (SSH) is a both a protocol and a program used to encrypt traffic between two computers. This is most commonly done as a secure replacement for tools like telnet, ftp and the Berkeley "r" commands (rlogin, rsh, etc.). These older tools do not encrypt any of their traffic, including the authentication process, so account names and passwords are transmitted in plaintext. This is a bad thing! SSH was authored by Tatu Ylonen in 1995 and has since spread quickly throughout the UNIX world, and has become available for other platforms. There are both commercial [8] and free implementations available [9], and a SSH Working Group [17] sponsored by the IETF that is working to formalize and standardize the protocol. Besides providing a secure interactive shell, SSH also includes other functionality, for example, tunneling X11connections over an established SSH session.

2. LITERATURE SURVEY

From different papers studied Encryption:

Eun-Jun Yoon et al. [1] proposed an efficient Diffie-Hellman-MAC key exchange scheme providing same securities as proposed by Jeong et al. who proposed a strong Diffie-Hellman- DSA key exchange scheme providing security against session state reveal attacks as well as forward secrecy and key independence. The proposed scheme is based on the keyed MAC hash function to provide efficiency. Then, they proposed a strong Diffie-Hellman-DSA key exchange scheme

providing security against session state reveal attacks as well as forward secrecy and key independence.

Emmanuel Bresson et al. [2] has investigated the Group Diffie-Hellman protocols for authenticated key exchange (AKE) are designed to provide a pool of players with a shared secret key which may later be used, for example, to achieve multicast message integrity. Over the years, several schemes have been offered.

F. Lynn Mcnulty [7] has drawn attention to the national and societal view of the role of encryption will be one of the defining issues for our culture in the twenty-first century. Encryption is cited by Michael Baum, chairman of the Information Security Committee of the American Bar Association, as "an enabling technology that provides companies, their business partners, customers and end users with the capabilities to fetch the information required and service what they need as much faster rate and more securely and safely."1 Ubiquitous digital communications will result in either a secure environment to conduct personal affairs and electronic commerce or a Kafkaesque world laid bare by digital fingerprints indicating our every transaction and thoughts.

SANS Institute Info Sec Reading Room [10] has investigated the overview of the Diffie-Hellman Key Exchange algorithm and review several common cryptographic techniques in use on the Internet today that incorporate diffie-Hellman. The privacy requirements for users normally described in the traditional paper document world are increasingly expected in Internet transactions today. Secure and safe digital communications are very much necessary part for web-based e-commerce, mandated privacy for medical information, etc. In simple scenario, secure and safe connections between different parties which are communicating over the Internet are now a requirement. Whitfield Diffie and Martin Hellman founded the protocol which can provide secure
connection which gain popularity as "Diffie-Hellman (DH)" algorithm in 1976. It is an amazing and ubiquitous algorithm found in many secure connectivity protocols on the Internet. In an era when the lifetime of "old" technology can sometimes be measured in months, this algorithm is now celebrating its 25th anniversary while it is still playing an active

role in important Internet protocols. DH is a method for securely exchanging a shared secret between two parties, in real-time, over an untrusted network. A shared secret is important between two parties who may not have ever communicated previously, so that they can encrypt their communications. As such, it is used by several protocols for security purposes mainly, including Secure Sockets Layer (SSL), Secure Shell (SSH), and Internet Protocol Security (IPSec).

Michel Abdalla [18] discussed a Diffie-Hellman based encryption scheme, DHIES (formerly named DHES and DHAES), which is now in several (draft) standards. The scheme is as efficient as ElGamal encryption, but has stronger security properties. Furthermore, these security properties are proven to hold under appropriate assumptions on the underlying primitive. DHIES is a Diffie-Hellman based scheme that combines a symmetric encryption method, a message authentication code, and a hash function, in addition to number-theoretic operations, in a way which is intended to provide security against chosen cipher text attacks. The proofs of security are based on the assumption that the underlying symmetric primitives are secure and on appropriate assumptions about the Diffie-Hellman problem. The latter are interesting variants of the customary assumptions on the Diffie-Hellman problem, and we investigate relationships among them, and provide security lower bounds. Their proofs are in the standard model; no random-oracle assumption is required.

3. The Diffie-Hellman Key Exchange Algorithm:

1. Global Public Elements: Prime number q; $\alpha < q$ and

α is a primitive root of q.

2. User A Key Generation: User B Key Generation:

3. Select private X_A $X_A < q$
Select private X_B $X_B < q$

4. Calculate public Y_A $Y_A = \alpha^{XA} \bmod q$
Calculate public Y_B $Y_B = \alpha^{XB} \bmod q$

5. Calculation of Secret Key by User A:

$K = (Y_B)^{XA} \bmod q$

Calculation of Secret Key by User B:

$K = (Y_A)^{XB} \bmod q$

The result is that the two sides have exchanged a secret value. Furthermore, because X_A and X_B are private, an adversary only has the following ingredients to work with: q, a, Y_A, and Y_B. Thus, the adversary is forced to take a discrete logarithm to determine the key. For example, to determine the private key of user B, an adversary must compute $X_B = dlog_{a,\ q}(Y_B)$. The adversary can then calculate the key K in the same manner as user B calculates it. The security of the Diffie-Hellman key exchange lies in the fact that, while it is relatively easy to calculate exponentials modulo q prime, it is very difficult to calculate discrete logarithms. For large primes, the latter task is considered infeasible.

Our Research proceeds with following algorithm

Sender Side

1. $X_a < q$ (user can select any random number less than q)
2. $Y_a = a^{Xa} \bmod q$ (Y_a is a public key of sender)
3. $K = Y_b^{Xa} \bmod q$ (where Y_b is a public key of receiver and K is a private key)
4. $pow = 2^K$
5. pow = pow + q

Encrypt every letter of plain text using pow.

Numerical Analysis for Diffie-Hellman Algorithm:

Sender:

1. $X_a = 6$ ($X_a < q$; $6 < 23$)
2. $Y_a = a^{Xa} \bmod q$ (Y_a is tha public key for sender)
   $= 5^6 \bmod 23$
   $Y_a = 8$
3. $K = Y_b^{Xa} \bmod q$ (K is the private key)
   $= 19^6 \bmod 23$
   $K = 2$
4. $Pow = 2^2 = 4$
5. Pow = pow+q
   = 4 + 23=27
   Pow = 27

Reciver Side

1. $X_b < q$ (user can select any random number less than q)
2. $Y_b = a^{Xb} \bmod q$ (Y_b is a public key of receiver)
3. $K = Y_a^{Xb} \bmod q$ (where Y_a is a public key of sender and K is a private key)
4. $pow = 2^K$
5. pow = pow + q

Decrypt every letter of Cipher text using pow.

Numerical Analysis for Diffie-Hellman Algorithm:

Receiver:

1. $X_b = 15$ ($X_b < q$; $15 < 23$)
2. $Y_b = a^{Xb} \bmod q$ (Y_b is the public key for receiver)
   $= 5^{15} \bmod 23$
   $Y_b = 19$
3. $K = Y_a^{Xb} \bmod q$
   $= 8^{15} \bmod 23$
   $K = 2$
4. $Pow = 2^2 = 4$
5. Pow = pow +q
   =4+23=27
   Pow = 27

Figure 1 shows a simple protocol that makes use of the Diffie-Hellman calculation and exchange. Suppose that user A wishes to set up a connection with user B and use a secret key to encrypt messages on that connection. User A can generate a one-time private key X_A, calculate Y_A, and send that to user B. User B responds by generating a private value X_B calculating
Y_B, and sending Y_B to user A. Both users can now calculate these key.

The necessary public values q and α would need to be known ahead of time. Alternatively, user A could pick values for q and α and include those in the first message. The protocol depicted in Figure 1

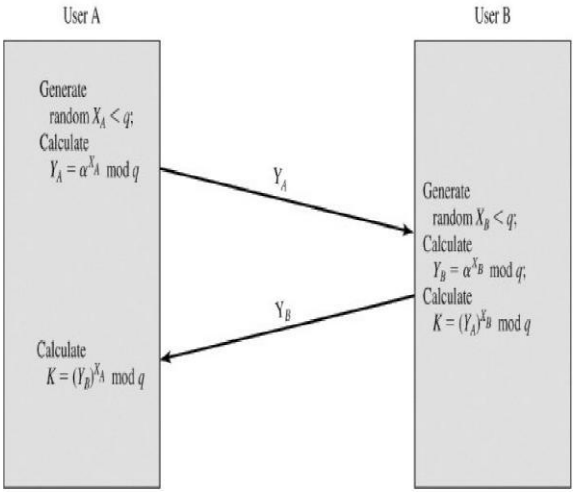

Figure 1.Diffie Hellman Algorithm

is insecure against a man-in-the-middle attack. The key exchange protocol is vulnerable to such an attack because it does not authenticate the participants. This vulnerability can be overcome with the use of digital signatures and public-key certificates.

4.CONCLUSION

The purpose of this Research is to provide some solution to better encryption algorithms and try to provide better security to email services and to other web services etc. The Encryption and Decryption
software available all time. This utility is helpful for sending secure email or any kind of message on internet. Our research could provides great solutions for web services like email transmission as we have enhance the encryption process and if any case someone broke into those email services, will only have a better hard encrypted copy of file which containing data which is very difficult to decrypt without information or implementation of our new research algorithm. Diffie Hellman algorithm could prove to be the vision for both online and offline email security services. However our research lacks little in providing solutions to attacks like man in middle attack.

5. REFERENCE

[1] Eun-Jun Yoon and Kee-Young Yoo, "An Efficient Diffie- Hellman-MAC Key Exchange Scheme", 2009 Fourth International Conference on Innovative Computing, Information and Control.

[2] Emmanuel Bresson, Olivier Chevassut, David Pointcheva, Jean-Jacques Quisquater, "Authenticated Group Diffie-Hellman Key

Exchange", Computer and Communicatio n Security- proc of ACM CSS'01, Philadelphia, Pennsylvania, USA, Pages 255-264, ACM Press, November 5-8, 2001.

[3] Mario Cagaljm, Srdjan Capkun and Jean-Pierre Hubaux," Key agreement in peer-to-peer wireless networks", Ecole Polytechnique F´ed´erale de Lausanne (EPFL), CH-1015 Lausanne.

[4] Michel Abdalla, Mihir Bellare, Phillip Rogaway," DHIES: An encryption scheme based on the Diffie-Hellman Problem", September 18, 2001.

[5] Jean-Fran¸cois Raymond, Anton Stiglic," Security Issues in the Diffie-Hellman Key Agreement Protocol".

[6] Whitfield Diffie and Martin E. Hellman," New Directions in Cryptography", invited paper.

[7] F. Lynn Mcnulty," Encryption's importance to economic and infrastructure security" in 2002.

[8] SSH Communications Security Home Page, http://www.ssh.com/.

[9] OpenSSH Home Page, http://www.openssh.com/.

[10] SANS Institute Info Sec Reading Room," A Review of the Diffie-Hellman Algorithm and its use in Secure Internet Protocols".

[11] Paul C. Kocher, "Timing Attacks on Implementations of Diffie- Hellman, RSA, DSS, and Other Systems", Cryptography Research, Inc. 607 Market Street, 5th Floor, San Francisco, CA 94105, USA.

[12] Brita Vesterås," Analysis of Key Agreement Protocols", Mtech Thesis, Department of Computer Science and Media Technology, Gjovik University College, 2006

13] (2006) The YouTube website [online]. Available: http://www.youtube.com/watch?v=40i9ujVJ040

[14] (2008) The YouTube website [online]. Available: http://www.youtube.com/watch?v=3QnD2c4Xovk.

[15] (2011) The Wikipedia website [online]. Available: http://en.wikipedia.org/wiki/Key-agreement_protocol.

[16] (2009) The Wikipedia website [online]. Available: http://en. wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exch ange.

[17] Secure Shell IETF Working Group Home Page, http://www.ietf.org/html.charters/secsh-charter.html.

[18] Michel Abdalla, Mihir Bellare, and Phillip Rogaway, " DHIES: An encryption scheme based on the Diffie-Hellman Problem", In Proc.of ACM CCS '01, ACM Press September18,2001.