ISSN 2229-5518

Enhanced Public Key Encryption Algorithm for Security of Network

Vishal Garg, Rishu

Abstract -- Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern 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. When the architecture of the internet is modified it can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. By means of firewalls and encryption mechanisms many businesses secure themselves from the internet. The businesses create an "intranet" to remain connected to the internet but secured from possible threats. 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 will make encryption harder with enhanced public key encryption protocol for security and will discuss the applications for proposed work. We will enhance the hardness in security by improving the Diffie-Hellman encryption algorithm by making changes or adding some more security codes in current algorithm.

Index Terms -- Diffie-Hellman, Private Key, Public Key, Cipher, Security.

1. Introduction

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. The background knowledge of the internet, its vulnerabilities, attack methods

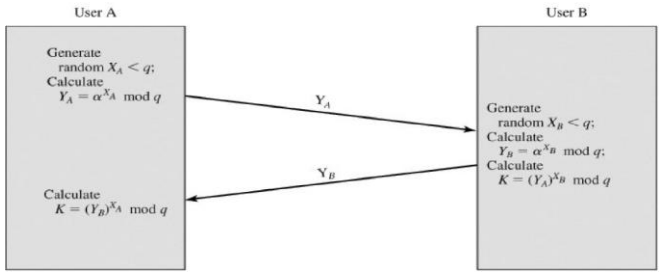

Figure 1.Diffie Hellman Algorithm

through the internet, and security technology is important and therefore they are reviewed in order to understand the research being performed today.

1.1 Diffie-Hellman Key Exchange Algorithm:

Step1: Global Public Elements: Prime number q; $\alpha < q$ and α is a primitive root of q.

Step2: User A Key Generation: User B Key Generation:

Step3: Select private X_A $X_A < q$

Select private X_B $X_B < q$

Step4: Calculate public Y_A $Y_A = \alpha^{X_A} \bmod q$

Calculate public Y_B $Y_B = \alpha^{X_B} \bmod q$

Step5: Calculation of Secret Key by User A:

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

Calculation of Secret Key by User B:

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

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

$$\boldsymbol{X_B = dlog_{a,q}(Y_B).}$$

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.

Figure 1 shows a simple protocol that makes use of the Diffie-Hellman calculation and exchange. Suppose user A wishes to set up a connection with user B and then 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 it to the 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 the 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 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. To overcome this vulnerability the use of digital signatures and public-key certificates is effective.

2. Literature Review

Farshid Farhat et al. [1] has focused on identification, authentication and key agreement protocol of UMTS networks with security mode setup has some weaknesses in the case of mutual freshness of key agreement, DoS-attack resistance, and efficient bandwidth consumption. In this paper they consider UMTS AKA and some other proposed schemes. Then they explain the known weaknesses of the previous frameworks suggested for the UMTS AKA protocol. After that they propose a new protocol called private identification, authentication, and key agreement protocol (PIAKAP), for UMTS mobile network.

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". 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). These protocols need to be discussed in brief in terms of the technical use of the DH algorithm and the status of the protocol standards established or still being defined.

3. Problem Formulation

As Encryption became a vital tool for preventing the threats to data sharing and tool to preserve the data integrity so we will focusing on security enhancing by enhancing the hardness of encryption process in different network. For required research we are working on well known encryption algorithm "Diffie-Hellman". We are proposing the Enhancement for Diffie-Hellman Algorithm after studying the issues of Diffie-Hellman. Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern 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 architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. The businesses create an "intranet" to remain connected to the internet but secured from possible threats. 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. For required research we are working on well known encryption algorithm "Diffie-Hellman". In our proposed work we will make encryption harder with enhanced public key encryption protocol for security and will discuss the applications for proposed work. We will enhance the hardness in security by improving the Diffie-Hellman encryption algorithm by making changes or adding some more security codes in current algorithm.
The encryption method we are using is simple one (like a transposition cipher). As there are lots of public key algorithm but in this encryption method, some further refinements are possible as it is not hard coded. After some more changes this algorithm become more better than other public key algorithm because after calculating private key K we can apply some mathematical method to make our private key more secure but it s not possible in RSA and DSA because they are hard coded.

Diffie-Hellman key exchange, also called exponential key exchange, is a method of digital encryption that uses numbers raised to specific powers to produce decryption keys on the basis of components that are never directly transmitted, making the task of a would-be code breaker mathematically overwhelming. To implement Diffie-Hellman, the two end users Alice and Bob, while communicating over a channel they know to be private, mutually agree on positive whole numbers p and q, such that p is a prime number and q is a generator of p. The generator q is a number that, when raised to positive whole-number powers less than p, never produces the same result for any two such whole numbers. The value of p may be large but the value of q is usually small.

Once Alice and Bob have agreed on p and q in private, they choose positive whole-number personal keys a and b, both less than the prime-number modulus p. Neither user divulges their personal key to anyone; ideally they memorize these numbers and do not write them down or store them anywhere. Next, Alice and Bob compute public keys a* and b* based on their personal keys according to the formulas.

4. Proposed Methodology

To achieve the set objectives, we will do the research in following steps

Step 1: Deep study of the security flaws in network will be done and encryption prospective will be taken in account.

Step 2: Study of Diffie-Hellman Algorithm to sense the security in key exchange process will be done.

Step 3: Study and proposed Algorithm with enhancement will comes into shape in form of algorithm.

Step 4: After shaping up of proposed algorithm, implementation of proposed algorithm will be tested on C compiler with c language.

Step 5: Encryption will be shown with Demonstration in form of encrypted data and Decrypted Data.

5. Proposed Algorithm

a) Sender end

Step 1: $X_a < q$ (user can select any random number less than q)
Step 2: $Y_a = a^{X_a} \bmod q$ (Y_a is a public key of sender)
Step 3: $K = Y_b^{X_a} \bmod q$ (where Y_b is a public key of receiver and K is a private key)
Step 4: $pow = 2^K$
Step 5: pow = pow + q
Step 6: Encrypt every letter of plain text using pow

b) Receiver end

Step 1: $X_b < q$ (user can select any random number less than q)
Step 2: $Y_b = a^{X_b} \bmod q$ (Y_b is a public key of receiver)
Step 3: $K = Y_a^{X_b} \bmod q$ (where Y_a is a public key of sender and K is a private key)
Step 4: $pow = 2^K$
Step 5: pow = pow + q
Step 6: Decrypt every letter of cipher text using pow

where ,
1) q is a prime number.
2) a is a root of prime number q.

6. 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. 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. Our 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. But to cover up those types of issues, we develop our algorithm in such a way so that it can provide security to vendors even if they do hacked.

7. References

[1] Farshid Farhat, Somayeh Salimi,Ahmad Salahi, "Private Identification, Authentication and Key Agreement Protocol with Security Mode Setup", Iran Telecommunication Research Centre

[2] Emmanuel Bresson, Olivier Chevassut, David Pointcheva, Jean-Jacques Quisquater, "Authenticated Group Diffie-Hellman Key Exchange", Computer and Communication 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] Tony Chung and Utz Roedig," Poster Abstract: DHB-KEY - A Diffie-Hellman Key Distribution Protocol for Wireless Sensor Networks", Infolab21, Lancaster University, UK.

[9] A. Chandrasekar, V.R. Rajasekar, V. Vasudevan," Improved Authentication and Key Agreement Protocol Using Elliptic Curve Cryptography" in 2006.

[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_exchange.

- *Vishal Garg is currently working as assistant professor at JMIT, Radaur, Haryana.*
  E-mail:vishalgarg.9@gmail.com
- *Rishu is currently pursuing MTech in CSE from JMIT, Radaur, Haryana.*
  E-mail:rishubk1987@gmail.com