A Publication of TRANS Asian Research Journals

AJMR
Asian Journal of Multidimensional Research
Vol.1 Issue 3, August 2012, ISSN 2278-4853

ALGORITHM FOR ROBUSTNESS DATA SECURITY IN VIRTUAL PRIVATE NETWORK

ANUBHA GAUR*; DR. ASHOK SINGH SHEKHAWAT**

*Research Scholar,
Suresh Gyan Vihar University,
Jaipur, India.
**Associate Professor,
Suresh Gyan Vihar University,
Jaipur, India.

ABSTRACT

VPN (Virtual Private Network) is a network which describes a communication network, uses any combination of technologies to secure a connection and supports authorization to access data with security. In previous paper we have discussed about the tunneling process and cryptography and all its terminology with the algorithm. In this paper various algorithm of encryption are discussed.

A VPN enables a user to send data between two computers with in a network. This paper involves various issues of data security on which security algorithm depends upon .Also underline the various services provided by the VPN nework. This paper also proposed an encryption algorithm for the data security.

KEYWORDS: *VPN, ATM, FR, PKI, QOS, DEC, PAP.*

INTRODUCTION

A VPN is a group of interconnected networks in various different locations, called sites. These sites are connected through ATM or Frame Relay (FR) leased lines supplied by a service provider. These leased lines to provide, a variety of protocols including ATM and Frame Relay for data communication via network. For transferring data, data security should be maintained and it should be maintain by various encryption techniques. Symmetric-key block ciphers are very important for today's point of view that it secures the infrastructure. Their main is application information hiding and security, besides it also used in block ciphers which are also used in the implementation of pseudo-random number generators, message Authentication protocols, stream ciphers, and hash functions [2]. A cipher should have the main two properties:

(a) Correctness of Functions that decryption should invert encryption;

(b) Security, that the cipher text should be unbreakable from unauthorized users.[3]

AJMR
Asian Journal of Multidimensional Research
Vol.1 Issue 3, August 2012, ISSN 2278-4853

ENCRYPTION

Encryption method is used to protect the data and it prevent unauthorized user to read that massage which has been send to the second user. Both the ends are called source and destination respectively. When the data is being transferred in between source and destination. Both the Source and destination endpoints must have to know the rules, these rules are called cipher. The cipher transforms the original data into a coded form [5]. It is important that both the

Source and the destination endpoints knows the cipher, when encrypted data is being sent from source end, the destination end can decode the data into the original data and this can be possible by two ways encryption:

SHARED KEY ENCRYPTION

Shared key encryption system, means that both the source end, also called the encryptor and the destination end also called the decryptor shared the same cryptographic key, called the shared key.

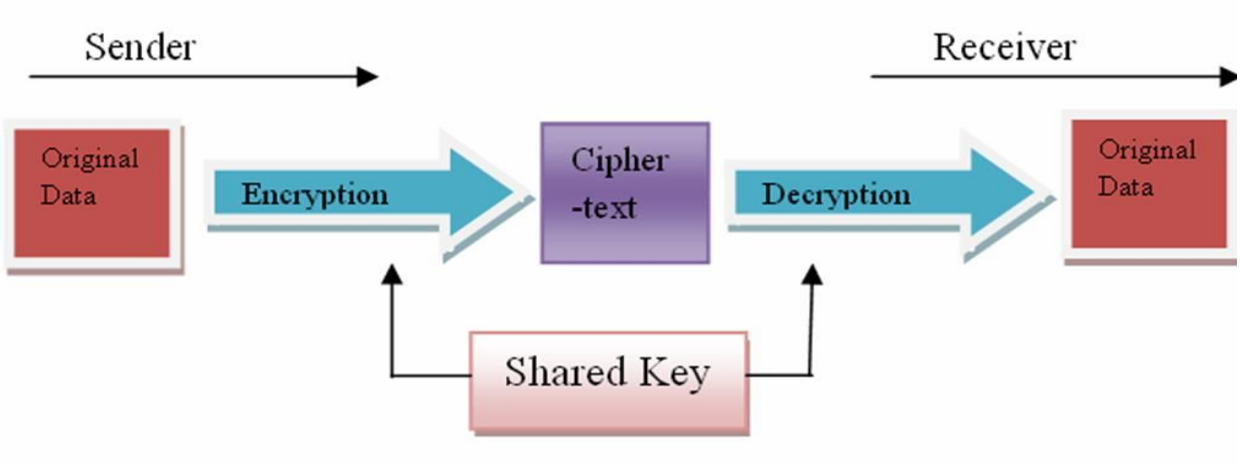

FIG-1 SHARED KEY ENCRYPTION

On the other hand that the shared key is secret for both the sender and the receiver which secure the data, the shared key cryptographic method maintains the confidentiality, authentication and security. It means that the formation of the shared key is the very importance as the encryption and decryption is important.

PUBLIC KEY ENCRYPTION

Public key encryption is very important the basis of security, which is based on the concept of two different on the both end points, the source and destination but these keys is related keys. The two related keys are called the public key and the private key. By the public key the data is

encrypted at the user end and on the other hand the data is decrypted by the private key. An advantage with public key encryption is that the public key is public, available to anyone. By this the user avoids the distribution of the key, the main problem with private key encryption.[5]

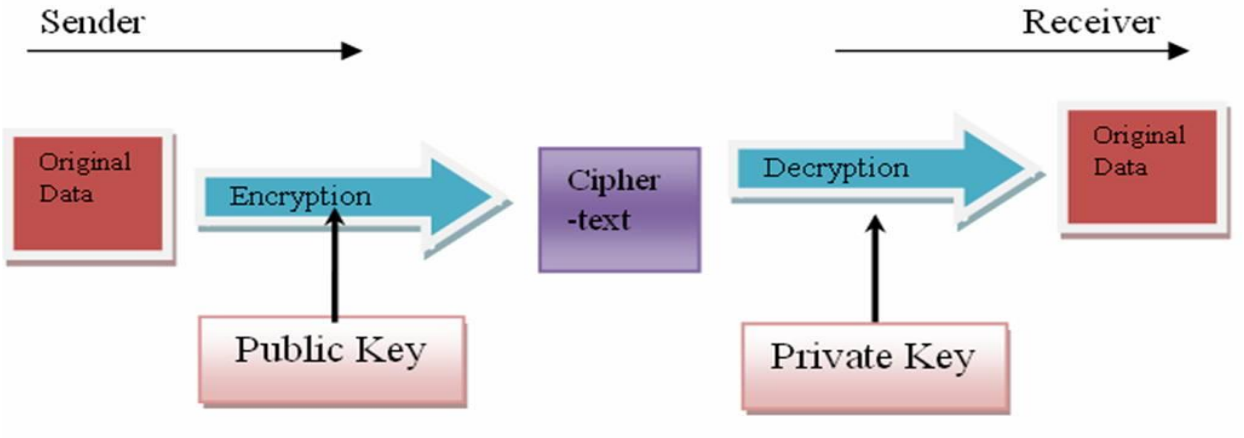

FIGURE 2: PUBLIC KEY ENCRYPTION

SECURITY IN WIRELESS LAN-VIRTUAL PRIVATE NETWORK

VPN makes a secure communication over various open or unsecured networks. The data in VPN which transit over the network is more protected but mostly networks have no strong authentication and security for the data, included so an extra component like a onetime password generator might be needed [6].Various companies provides the a lots of certificates like (Public Key Infrastructure) and the choice is made from the security demands the companies should have.

In mostly cases the companies don't have the security criteria and measurement for availabity of data. There are many criteria for it which are as follows:

SERVICES PROVIDED BY THE VPN

The VPN decide the services which one is suitable and required the type of service by the VPN user. Different VPN solutions offer either layer 2 or layer 3 connectivity between various VPN sites, the choice of services will depend on the type of traffic that will be sent between customer sites, as well as the layer 2 and layer 3 protocols in use at each individual site.

QUALITY OF SERVICE

The VPN user may require a certain quality of service (QoS) for the connections between VPN sites. For the quality of service QoS-constrained tunnels are required, the VPN solution must be able to make use of these tunnels [7].

AJMR
Asian Journal of Multidimensional Research
Vol.1 Issue 3, August 2012, ISSN 2278-4853

SECURITY OF DATA

If the data is being sent across the various between VPN sites, then it maintains encryption, authentication and integrity by checking the data in the VPN tunnels. The VPN user may require a solution which is not costly and easily available, existing hardware. It should not have the expensive service provider. if possible, this will be fully interworked able with the VPN user's existing switches and routers.

MANAGEMENT AND AVAILABILITY OF DATA

The VPN user wants a easy solution for the data management and availability of data, which minimizes the cost. The configuration of the VPN should not be so complex. There should be less risk for the architectural and interoperability issues.VPN Solution must be latest and easy to use for the users

OBJECTIVES OF THE STUDY

1. To study the security issues related to vpn.

2. To identify the encrption and decryption techniques of data security.

3. To analyze the security technique in encryption.

4. To study about the various encryption algorithm.

5. To know whether these techniques are secure or not.

REVIEW OF LITERATURE

Today various encryption algorithms are popular and used for security purpose.There are many algorithms such as DES, 3DES, AES, Blowfish.

(a) Advanced Encryption Standard: is also called AES Algorithm and is the new encryption standard recommended by NIST which replace Data Encryption Standard. It was also known as Password Authentication Protocol (PAP) Rijndael (pronounced Rain Doll). It was selected in 1997 after a competition to select the best encryption standard.[7].In this algorithm it has variable key length of 128, 192, or 256 bits; default 256. AES encryption is fast and flexible; This algorithm can be implemented on various platforms especially in small devices

(b) Data Encryption Standard, also known as DES was the first encryption standard to be recommended by National Institute of Standards and Technology. It is based on the IBM proposed algorithm called Lucifer. DES became a Standard in 1974[8]. This standard algorithm is not much secure for the data encryption.

(c) 3DES: It is also called Triple DES which is improved version of DES. This is very much similar with the standard DES but because this is Triple DES, That is why it applied 3 times to

AJMR
Asian Journal of Multidimensional Research
Vol.1 Issue 3, August 2012, ISSN 2278-4853

increase the encryption level. But it is a known fact that 3DES is slower than other block cipher methods.

(D)BLOWFISH

It is one of the most common public domain encryption algorithms provided by Bruce Schneider .It takes a variable length key (32 bits to 448bits; default 128 bits.).Blowfish is the most popular algorithm for the users and is available free for all users.

RESEARCH METHODOLOGY

On the study of above algorithms now a new much secure algorithm is required and the proposed framework identifies the trusted users those are sending message to the destination and look at on activities of users to prevent masquerading, denial of service and unauthorized access from them. To establish initial trust level and prove its authenticity, each and every user is assumed to get registered at the user end and a authenticate registration number is assigned to them. Only after that a user is able to access the services. This work proposes a Algorithm for data security in VPN. After analyzing the problems of related algorithm. Every incoming request at the destination end point, the data will go through the process of this algorithm and decryption key, this will secure the message.

User name:

Encrypt

{

Allotted key

Inputs from calling process:

USER AUTHENTICATION

msg_Aun[n] n*16 bits, n > 1

Inputs from internal stored data:

AUN_KEY[0-8] 16 bits

Outputs to calling process:

msg_Out[n] n*16 bits

Outputs to internal stored data:

Decrypted Msg

Secured msg

None.

This algorithm encrypts and decrypts messages that are of length n*16

Bits, where n > 1. Decryption is performed in the same manner as

Encryption.

CONCLUSION AND FUTURE SCOPE

On the basis of above algorithm we can conclude that all the data which is transferred at the destination end is secured. But still it requires more updation for the security of data and encryption techniques. In future we will discuss about the security of VPN,we have not covered this topic in this paper.

REFERENCES

1. R. Boutaba, W. Ng., A. Leon-Garcia, Web-based Customer Management of VPNs, Journal of Network and Systems Management.
2. Davey, B. et al. IETF RFC3246: An Expedited Forwarding PHB. March 2002
3. Heinanen, J. et al. IETF RFC2597: Assured Forwarding PHB Group. June 1999
4. http://dmoz.org/Science/Math/Applications/Communication_Theory/

   Cryptography/Historical
5. D. Harkins and D. Carrel. The Internet Key Exchange (IKE),RFC 2409 (Proposed Standard), Nov. 1998.
6. S. Kent and R. Atkinson. IP authentication header. RFC,2402 (Proposed Standard), Nov. 1998.
7. S. Kent and R. Atkinson. IP encapsulating security payload. RFC 2406 (Proposed Standard), Nov. 1998.
8. 8. S. Kent and R. Atkinson. Security architecture for the internet
9. Protocol. RFC 2401 (Proposed Standard), Nov. 1998.
10. http://cnscenter.future.co.kr/resource/security/vpn/virtual private networks.pdf, June 2003.
11. [2] V. G. Cerf and E. Cain. The DOD internet architecture model. Computer Networks, pages 307–318, 1983.
12. [3] IETF. Ip security protocol. http://www.ietf.org/html.charters/ipseccharter. Html, Visited 2004.
13. [4] IETF. Secure shell. http://www.ietf.org/html.charters/secsh-charter.html, Visited 2004.
14. [5] IETF. Transport layer security. http://www.ietf.org/html.charters/tlscharter.Html, Visited 2004.