Trends in Engineering and Technology (NCTET-2K17)
International Journal of Advanced Engineering Research and Science (IJAERS) *Special Issue-3*
https://dx.doi.org/10.22161/ijaers/nctet.2017.20 *ISSN: 2349-6495(P) | 2456-1908(O)*

SECURE DATA TRANSMISSION USING VIRTUAL PRIVATE NETWORKS

B.Ramasubba Reddy[1], A.Saritha[2] , B.BalaKonda Reddy[3]

[1]Professor, Dept of CSE, SV College of Engineering Tirupati, India,
Email:rsreddyphd@gmail.com
[2]Asst Professor, Dept of CSE, SV Engineering College for Women Tirupati, India,
Email:sarithaanchuri@gmail.com
[3]Asst Professor, Dept of CSE, SV College of Engineering Tirupati, India,
Email:balakondareddyb@gmail.com

Abstract:

A Virtual Private Network (VPN) is a general network mechanism to offer a secure end-to-end network connection. The design is to first negotiate and setup a network tunnel among the two communication nodes. Generally a VPN server also connects to a RADIUS server to permit only authorized users have the privilege to establish such tunnels. The data will then be encrypted before it is transmitted over the network and will then be decrypted on the receiver side. Compared to dedicated private leased lines, VPNs are much cheaper and are ideal to many companies.

VPN is the network which offers security to the sensitive traffic while traversing networks like Internet. A VPN is a communications environment in which access is controlled to permit peer connections only within a defined community of interest, and is constructed through some form of partitioning of a common underlying communications medium, where this underlying communication medium provides services to the network on a non-exclusive basis.

The main objective of VPN is to prevent outsiders (hackers) from interfering with messages sent among hosts in the network, and to protect the privacy and integrity of messages going through untrusted networks. From the user's perspective, a VPN connection is a point-to-point connection between the user's computer and the company's server. The nature of the intermediate inter network is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.VPN has been adopted by many organizations looking to expand their networking capabilities while reducing their costs. The key feature of a VPN is its ability to use public networks like the Internet rather than private leased lines in order to allow remote users to access the corporate network.

Introduction:

Confidentiality and data integrity plays an important role in the security of innovative Internet based applications. Confidentiality and data integrity is essential in all data communication networks like Virtual private networks. And can achieve more security with several kinds of symmetric and asymmetric key cryptosystem algorithms. A major part of the proposed work is about confidentiality and data integrity and we present a subset of the latest research.

Current research on VPNs to achieve secure data transmission through public network is presented along the lines of TCP-IPsec based, TCP-AES based, mTCP-IPsec based, SCTP single path-multihoming-based, WiMP-SCTP based, CMP SCTP-CMT based, SCTP-CMT based, mobile VPN, wireless VPN, TCP/IP based VPN, VPN shield, and hybrid encryption protocol based VPN.

If you are going to connect to a remote host computer using public-key authentication, you will have to generate your key pair before connecting. Public-key authentication is based on the use of digital signatures. Each user creates a pair of 'key' files. One of these key files is the user's public key, and the other is the user's private key. The server knows the user's public key, and only the user has the private key. When the user tries to authenticate, the server checks for matching public keys and sends a challenge to the user end. The user is authenticated by signing the challenge using her private key.

Remember that your private key file is used to authenticate you. Never expose your private keys. If anyone else can access your private key file, they can attempt to login to the remote host computer as you, and claim to be you. Therefore it is extremely important that you keep your private key file in a secure place and make sure that no one else has access to it.

Do not use public-key authentication on a computer that is shared with other users. Generate keys only on your personal computer that no one else can access!

https://dx.doi.org/10.22161/ijaers/nctet.2017.20 *ISSN: 2349-6495(P) | 2456-1908(O)*

Also note that if you are using the Windows roaming profiles functionality, your personal settings will be replicated with the roaming profile server. If you store your private keys in the default location (under the profile folder of your Windows user account) your private keys may be suspected to a malicious user listening to the network traffic. Therefore the User Settings folder should not be a directory that will be used in profile roaming.

In order to use public-key authentication, you must first generate your own key pair. You can generate your own key files with the help of a built-in key generation wizard. On the Key Generation - Generation page the computer will generate your key files. This can take several minutes, depending on the chosen key length and the processor speed of the computer.

Key Length:

Select the length of the key to be generated. Available options are 768, 1024, 2048 or 3072 bits. Larger keys are more secure, but also slower to use. The recommended key length for most occasions is 2048 bits.

Proposed Work:

With the advent of Internet and Virtual Private Network (VPN) technologies, data transmission has become a challenging task. In every organization, the flow of different kind of information is increasing from one organization to other as well as to its clients roaming in different areas.

Ensuring security in VPN is a major task since it is subject to several attacks along with the security criteria such as authentication, access control, confidentiality and data integrity. While several different key protocols and methods to ensure security subsist, these existing systems have their limitations. In this, a framework is proposed for secure data transmission in VPNs using XOR-DUAL-RSA algorithm. VPN itself provides security using symmetric encryption algorithm, AES.

Before data transmission takes place sender and receiver must know the secret key, for this after generating key using AES algorithm, key has to be transmitted to the other party with whom we want to communicate to. If we transmit key directly, it may be seen or accessed by the unauthorized users, and the data which we transmit using the same channel may be accessed by the unauthorized users. In order to secure the data key must be sent only to the authorized user.

We can do this with the help of RSA algorithm, which is public encryption technique. In RSA algorithm we have a pair of keys, one is private key which is to be kept secret and the other is public key, which is known to everyone. This key pair is generated in such a way that if we encrypt using public key of user it can be decrypted only with private key of the same user.

Related Work:

The internet protocol suite glues together a large number of computer systems and networks. The IP protocol can support many different transport layer protocols, with TCP being the most widely used protocol. Recently, the Stream Control Transmission Protocol(SCTP) has been standardized by the IETF as a reliable transport layer protocol for carrying Public Switched Telephone Network(PSTN) signaling messages over IP networks. However its advanced congestion control and fault tolerant features also make it suitable for carrying data in computer networks, for which it has already been proposed as an alternative to TCP.

SCTP is essentially a reliable, message-oriented data transport protocol that supports multiple streams within an association, and hosts with multiple network addresses. SCTP is particularly valuable to applications where monitoring and detection of loss of session is required. For such applications the SCTP path/session failure detection mechanisms, will actively monitor connectivity of the session.

The following services are also provided to its users:

1. Acknowledged error-free non-duplicated transfer of user data.

2. Data fragmentation to conform to discovered path Maximum Transmission Unit size.

3. Sequenced delivery of user messages within multiple streams, with an option for order-of-arrival delivery of individual user messages.

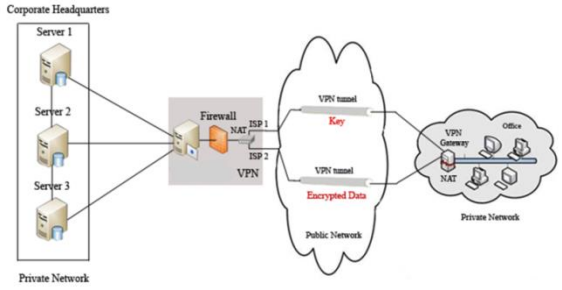
4. Optional bundling of multiple user messages into a single SCTP packet.

5. Network-Level fault tolerance through support of multihoming at either or both ends of an association.

6. Resistance to flooding and masquerade attacks.

Architecture of Proposed Work:

https://dx.doi.org/10.22161/ijaers/nctet.2017.20 *ISSN: 2349-6495(P) | 2456-1908(O)*



Conclusion and future scope:

In this paper we propose an extension of TCP that is SCTP and how to send data securely over public networks with the help of virtual private networks. It is designed to solve several problems as practical implementation, short response time, efficient computation and strength of cryptosystems. First , XOR-DUAL RSA is used since it is more robust and cannot be easily attacked. Second it makes use of SCTP which gives better performance over TCP.

The present work can be extended to improve performance metrics with packet drop due to handover and association resume of VPN. Completely developed VPN protocol analyzers may be used in performance analysis. The experimental work could be extended to the development of full-fledged VPN architecture analyzers that simulate network uncertainties attack scenarios.

References:

1. El. A, T. Saadawi, and M. Lee (2004), "LS-SCTP: a Bandwidth Aggregation Technique for Stream Control Transmission Protocol," *Computer Communications*, vol. 27, pp. 1012–1024, 2004.

2. Abd El Al, T. N. Saadawi, and M. J. Lee (2004), "LS-SCTP: A bandwidth aggregation technique for stream control transmission protocol," *Comput. Commun.* vol. 27, no. 10, pp. 1012–1024, Jun. 2004.

3. Alamgir, R., AT iquzzaman, M. and Ivancic, W. (2002). *Effect of Congestion Control on the Performance of TCP and SCTP over Satellite Networks*: proceedings of the NASA Earth Science Technology Conference, Pasadena.

4. Alwin Thomas and George Kelley (2002), "Cost-Effective VPN-Based Remote Network Connectivity Over the Internet", 2002

5. Arjen Lenstra (2001), "AES in security protocols", available at http://people.epfl.ch/arjen.lebstra , 2001

6. Arno Wagner, Thomas Dubendorfer, Roman Hiestand, Christoph Goldi and Bernhard Plattner (2006), "A Fast Worm Scan Detection Tool for VPN Congestion Avoidance", DIMVA, 2006.

7. Atkinson.R, (1998a).IP authentication header. RFC 2402. Available at http://www.ietf.org/rfc/rfc2402.txt.

8.Atkinson.R, (1998b).IP authentication header. RFC 2406. Available at http://www.ietf.org/rfc/rfc2406.txt.

9.D. Boneh, G. Durfee, "**Cryptanalysis of RSA with private key d less than N",** IEEE Trans. Inf. Theory, 46 (4) (2000), pp. 1339–1349

10. W. Burr, "Selecting the advanced encryption standard", IEEE Secur. Priv., 1 (2) (2003), pp. 43–52

11. M.J. Dubal, T.R. Mahesh, P.A. Ghosh, "Design of a new security protocol using hybrid cryptography architecture", Proceedings of 3rd International Conference on Electronics Computer Technology (ICECT), vol. 5, India (2011)

12. M. Frunza, Gh. Asachi, "Improved RSA encryption algorithm for increased security of wireless networks", ISSCS International Symposium, vol. 2 (2007)

13. Md.A. Hossain, Md.K. Islam, S.K. Das, Md.A. Nashiry, "Cryptanalyzing of message digest algorithms MD4 and MD5"

14. Int. J. Cryptogr. Inf. Secur. (IJCIS), 2 (1) (2012), "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security", Int. J. Comput. Appl., 67 (19) (2013), pp. 33–38,

15. S. Subasree, N.K. Sakthivel, "Design of a new security protocol using hybrid cryptography algorithms", IJRRAS, 2 (2) (2010), pp. 95–103.