*International Journal of Engineering & Technology*, 7 (4.6) (2018) 328-331

**International Journal of Engineering & Technology**

*Website: www.sciencepubco.com/index.php/IJET*

***Research paper***

# A study of virtual private networks security issues and restrictions

**A.Saritha[1]*, B.RamaSubba Reddy[2], A. Suresh Babu[3]**

*[1] Research Scholar, JNTUCEA, Anantapuramu, India,*
*[2]Professor, Dept of CSE, SV College of Engineering Tirupati, India,*
*[3]Associate Professor, ACE, JNTUACEA, Anantapuramu, India,*
**Corresponding author E-mail:sarithaanchuri@gmail.com*

**Abstract**

VPN also called as Virtual Private Network serves as a communication network that supports secure data transmission in a public or an unsecured network using several technologies. A connection that is virtual is established among the users who are globally dispersed and are connected through the public or shared network (eg: Internet). Though virtual network is within the public network, it still gives the end-user a feeling of a private connection. This paper explains the concepts of core VPN technology. Security threats posed for VPN environment are discussed in detail and that care must be taken to handle these threats while implementing a virtual private network.

***Keywords***: *Virtual Private Network (VPN), VPN Protocols, Security, Limitations.*

## 1. Introduction

In recent days providing a secure access to the private sources has become the need of the era. The most effective and cost-efficient way to achieve this is through VPN [1].VPN can construct a logical structure in order to connect the global users through LAN into a private network. This logical private network then uses internet to establish communication [2].While considering other modes of network it is prone to hackers who cause a threat to data security and attack data directly. Whereas in case of VPN since data travels through a private traffic it is restricted to only the authenticated or authorized users to have access to information. IPSec-based VPNs are now being commonly used in Frame Relay, ATM, MPLS, and internet. Users choose to use internet since it is cheap and easy to access, but still VPN is given priority while considering the requirement of secured network. There are various types of VPN networks that were developed based on the operational requirements. The explanation on these various VPNs and ways to create them are discussed in [3]. In IPSec based VPN we have encryption method to secure the data. This is achieved by connecting private and public networks and then encrypts the packets that are transferred in the net. It also increases its resistance towards data retouch and hacker's attack [4].The sole purpose of implementing VPN is to eliminate data sniff and to manage the integrity of un-trusted networks [5].

### 1.1. Main differences with TLS/SSL, IPSec and SSH

Let's look into TCP networking model that consists of four layers: transport, application, network and finally the physical layer. When discussing on TLS/SSL, SSH and IPSec they have their own individual places to serve in the network. SSH has its position at the top of the model called as the application layer. So SSH acts as an application itself and it works in combination with other network applications like ftp, http and others. SSH can acts as a port-forwarding mode that can create tunnels for other applications. Coming to the TLS/SSL it acts as security for the transport layer. TLS/SSL is not a single application and SSH takes the responsibility to deliver security for the applications. SSL was initially proposed by Netscape2 with the purpose of serving as HTTP. TLS is nothing but an up-gradation of the SSL technology. Discussing on the functions of IPSec it acts as the security task at the IP layer. IPSec is not integrated at higher levels like the TLS/SSL. IPSec works on the network-level that gets integrated with the clients or servers. In case of routers it acts as a dedicated VPN concentrator, or as an operating system kernel, or as a firewall. There is no connection between the TLS/SSL, SSH, and IPSec as they all work in different levels when considering the TCP model. But the traffic can be routed using SSH that runs through TLS in a trusted environment using IPSec. But on practical note this process consumes heavy CPU usage since data will be encrypted and decrypted three times. So choosing one among the all is good for better outputs.

### 1.2. SSH

SSH [7] is effective when it comes to cost and is free of use in case of non-commercial purpose. There are two versions of SSH: SSH-1, SSH-2. The later one SSH-2 is much more effective and much secured than the other. But SSH-1 is still popular and is most commonly used as GPL license in most of the platforms. The drawback with SSH-1 is that it uses CRC for integrity protection which not too secure. SSH is highly available and is suitable for almost any platform. SSH-2 can support many

encryption algorithms like 3DES, IDEA, Blowfish, Two-fish and Cast. In a SSH VPN setup, SSH can tunnel service ports in the Internet within a SSH session. Though it is limited in its functions it is simple and easy to be setup and does not involve any administrative access.

**Benefits** The first benefit of using SSH is that it is useful to tunnel TCP based applications through SSH, like, email protocols, programming tools and even business applications like Oracle. In other words SSH is very much similar to Telnet. The users are not disturbed with the encryption process and thereby making security transparent to users. When it comes to system administrators SSH is a most recommended remote administration platform.

**Limitations** SSH cannot be integrated into network gateways like the firewalls or routers. It creates a VPN by creating a tunnel from PPP through SSH. SSH cannot tolerate connection with a lot of bandwidth requirements like the IPSec. IPSec and TLS/SSL are transparent to be used but not the case with SSH. To use SSH one has to be logged in to the user account in order to apply security in the transport layer. SSH is suitable for scripting applications and IPSec and TLS/SSL are merged into applications and TCP/IP stacks. ICMP and UDP is a major problem to be considered in SSH. It cannot tunnel ICMP or UDP traffic. These protocols can be used in VPNS that are used for securing the audio file that is being transported through VPN setup. Since SSH has many different implementations of the protocol, interoperability is an issue to be handled. In cases like different implementation methods can cause server crash. This occurs even when SSH is being standardized by IETF [4].

**TLS/SSL**

When protocols like TLS/SSL are used then the applications are also to be built in TLS/SSL support. Most of the web browsers at present support TLS/SSL [6]. VPN solution along with TLS/SSL is commonly used in web browser communication. TLS/SSL can also be implemented in other applications that run inside a web browser.

**Benefits** TLS/SSL is a transparent protocol for higher level. The benefits of TLS/SSL are its popularity in the web and e-commerce. It provides session oriented security and once application oriented to TLS/SSL is running the server responds immediately. Once the application is stopped the server automatically quits the session. In other words there is no such term as permanent SSL/TLS connectivity as with IPSec between two hosts.

Another benefit of using TLS/SSL is that certificates from root CA's will be added in new web browsers. Therefore users can verify a server certificate with a trusted CA. TLS/SSL also works similar to the SSH where it can port to tunnel applications with the help of TLS/SSL, like stunnel.

**Limitations** TLS/SSL does not support UDP traffic and it needs a state-full connection. There are some limitations that come along while using applications that support TLS/SSL like, e-mail applications and web browsers support TLS/SSL as standard. Another concern to be bothered with is that not all setups implement both server and client authentication. This causes a problem if the requirement is to both server and client in a connection. If TLS/SSL is used in tunnel mode then the setup expense is huge because external certification authority to sign many digital certificates is to be implemented.

**IPSec**

IPSec assures you with full transparency. All the IP packets are secured disregard to the type of packet being used. IPSec is an efficient and secured VPN solution so far. The limitations with IPsec are that using IPSec and NAT creates mess in the administration part [6]. IPSec can operate in four different modes namely: ESP Encapsulating Security Pay load) tunnel mode, ESP (transport mode, AH (Authentication Header) transport mode, and AH tunnel mode. All the above modes work with different packet securities and all modes cannot fit into all network solution.

**Benefits** IPSec delivers security on the IP network layer and almost everything is secured that lays on the IP network layer. This has been an Internet standard protocol for several years and still believed to be the most secured and trusted method of securing data.

IPSec extends its support for nested tunnels as well. In other words when a user has to pass by more than one secure gateway then the tunnels can be made double encrypted.

**Limitations** Though IPSec has a lot of advantages over SSH and TLS/SSL the complexity in setting up and implementing IPSec is high and it needs special support in routers, etc. As stated in case of SSH, IPSec also has the interoperability issues. Different IPSec implementations cannot follow the same standards and have an error-free communication.

## 2. Related Work

Ram raj [8] composed an encryption protocol designed for VPN along with a management key. The author assumes that the VPN server is a trusted one. When a request proposal from the customer is sent to VPN server then a key value for the customer is sent. Customer can encrypt data with the help of this key and AES. The customer can send data using the public key. With the help of private key implemented in a VPN server the customer can understand the value of main key and with the help of RSA encryption algorithm the decoding can be done thus ensuring high security.

**Limitations**

- ✓ Very complex mathematical description
- ✓ Short time of research in cryptanalysis(breaking cipher)
- ✓ Loss of private key is irreparable
- ✓ Widespread security threat is possible

M.C. Nicalescu [9] proposed IP mobile security for VPNs. At first ESP, AH examined the proposed protocols in case of IKE and in IPSec-IETF architecture. Later it was extended to protect against sniff and the other dangers and viruses. This paper also deals with the scopes around "Internet". Secure tunneling and its applications were also discussed and tested for its protective mechanism.

**Limitations**

Though IPSec has a lot of advantages over SSH and TLS/SSL the complexity in setting up and implementing IPSec is high and it needs special support in routers, etc. In case of SSH, IPSec also has the interoperability issues. Different IPSec implementations cannot adhere to the standards and deliver a error-free communication system.

Elkeelany et al. [10] details about implementing Data Encryption Standard (DES) (to provide confidentiality) Message Digest (MD5) and Secure Hash Algorithm 1 (SHA-1) (to provide authentication security) in combination with IPSec. [10] Advanced Encryption Standard (AES) is also being discussed here since it is an advanced version of DES and 3DES.

**Limitations**

An encryption system falls in two categories namely: public and private or secret key. In a system, where same key used for both decryption and encryption, gets it difficult to secure the key. In case of public key prototype two keys are being used. The private key is hidden and is used to decrypt data whereas the public key is for encrypting data. Since the tasks here are handled with

different keys information is more secured in this setup. Public key encryption is suitable for situations where the key has to be kept safe like over the Internet.

Miltchev et al. [11] writes about the benchmark-based investigation about IPSec that is used in Open BSD system. The same setup is also being tested for its benefits around implementing hardware accelerators in order to fasten the cryptographic process.

**Limitations:** Though IPSec has a lot of advantages over SSH and TLS/SSL the complexity in setting up and implementing IPSec is high and it needs special support in routers, etc. As stated earlier in case of SSH, IPSec also has the interoperability issues. Different IPSec implementations cannot adhere to the standards and have error-free communication.

Amirgaliyev Yedilkhan at al [12] composed this article in order to analyze information security when the transmission happens between virtual subnets that are considered in encryption algorithms of EZ-cryptosystem and the secret key that safeguards the information from obstacles. Also in case where the data has to be inter segmental transfer coded output from one network and decoded at the other input network. Data encryption algorithm is being used to safeguard the circulation between the endpoints. Data manipulations are kept transparent to the user.

**Limitation**

- ✓ The public-key cryptography aimed at encryption does not have a great speed in the system. Several other popular secret-key encryption methods are available in the markets that are significantly faster.
- ✓ It is not capable of providing digital signatures that cannot be repudiated.

Alexander V. Uskov [13] discusses on the effectiveness of mobile VPN (MVPN). The author quotes that various factors decide on the efficiency of the system such as: selected architectural model, MVPN's scheme model, and levels of OSI model structure, topology model, authentication algorithms, key management protocols, cipher operation modes, encryption algorithms (ciphers), modes of operation, connection modes and several parameters of security protocols.

**Limitations**

- ✓ Even a legitimate user will find difficulty in decoding the digitally signed information. It is easy to be hacked or cracked and become non-functional by an intruder.
- ✓ High availability and the basic aspects of information security, it cannot be secured only through cryptography. Additional methods are required to protect it against the threats like denial of service and complete shutdown of information system.

Marcin Niemiec et al [14] propose a very strong and efficient secure authentication system that cannot be achieved using any of the currently-available techniques. Secure authentication is the vital key for an efficient virtual private network (VPN). The authors implemented a simulation with quantum-based distribution of a shared secret for a VPN connection. With the help of this dedicated simulator the author captured all individual steps that are involved in the quantum key distribution process. With the help of the captured details a secure IPSec tunnel was proposed in a Strong Swan environment between VSB (Czech Republic) and AGH (Poland). Communications between the end-users were set with high security levels in a VPN environment.

**Limitation**

- ✓ The mathematical cryptography is strong in our public-key and symmetric algorithm. Though they do not have rigorous mathematical theory they are strong enough to survive the attacks. The real problems actually lie in the network security, computer security, and user interface.
- ✓ Security is solely dependent on the privacy and strength of the password.
- ✓ It does not have a strong identity check (authentication is done only using password).

**Yu-Liang Liu et al [15]** discusses on way to increase the bandwidth efficiency in a single *hose-mode* VPN. Though this paper did not reveal any satisfactory *rejection ratio* in cases like: (1) the residual bandwidth present on network backbone is finite (2) several VPN setup requests should be handled on-line. This paper composes a new *hose-model* VPN algorithm called as *MTRA* as a solution to this issue. The proposed *MTRA* system can execute multiple VPN setup requirements in no time and also minimizes the *rejection ratio*. The hypothetical upper bounds of *rejection ratios* results are also being achieved in this paper.

**Limitation**

- ✓ Optimal VPN tree with link capacity constraints: it is the same as with the bandwidth infinite case, except that the bandwidth reserved on vpn tree link must not be more than their residual bandwidth.

In paper [16], the selected algorithms namely: AES, 3DES, DES and Blowfish are being implemented and the corresponding results are compared in this paper. With the implementation of these algorithms the performance of decryption and encryption process of text files are computed with the help of throughput parameter. Encryption time is computed based on the total plaintext in bytes encrypted divided by the encryption time. Whereas decryption time is computed with the he total plaintext in bytes decrypted divided by the decryption time. The results derived from this paper demonstrate that [14] Blowfish algorithm has better performance result than the others. The least efficient is the3DES.

**Limitation**

- ✓ The 3DES algorithm is sluggish in terms of its software.
- ✓ Since DES was initially designed for hardware implementation, its application on software does not work well.
- ✓ 3DES is complex in its computation and hence makes it slow.

IPSec [17] is a forth coming way of delivering security at network layer of the Internet. It gives authentication of the communicating entities and also enables them to set up secure IP channels to perform data exchange. It also enables a prototype to support different cryptographic algorithms based on the level of security demanded by applications and the users.

**Limitations**

Though IPSec has a lot of advantages over SSH and TLS/SSL the complexity in setting up and implementing IPSec is high and it needs special support in routers, etc. As stated earlier SSH, IPSec also has the interoperability issues. Different IPSec implementations cannot adhere to the standards and supports communicate problem-free between each other.

**Table.1.**Shows Advantage and limitation of various Algorithm

| Ref.No | Author | Technique | Advantage | Limitation |
|---|---|---|---|---|
| [7] | Ole Martin Dahl | SSH | Advantage of SSH is that it is capable to tunnel TCP based applications through SSH, e.g. programming tools, email protocols and some business applications like Oracle. | SSH cannot be considered as a complete VPN solution since it was not designed for network gateways like routers or firewalls. It is converted into a VPN by patching PPP through SSH, but this needs much overhead and it cannot handle huge bandwidth requirements like IPSec. |
| [6] | Stephen Northcutt et al | TLS/SSL | In case of TLS/SSL, the certificates from root CA's are added in new web browsers and hence users can verify a server certificate with a trusted CA. Similar to SSH it is capable to tunnel applications with TLS/SSL like with tunnel. | When TLS/SSL is used in tunnel mode, the setup cost is high and it needs external certification authority in order to sign many digital certificates. |
| [6] | Stephen Northcutt | IPSec | IPSec is capable of providing security directly on the IP network layer and it can secure everything that is present on top of the IP network layer. | Though IPSec has added features than SSH and TLS/SSL it gets difficult to implement IPSec and it needs special support in routers etc. |
| [8] | Ram raj et al | RSA | ✓ It is fast and follows easy encryption process<br>Easy to implement<br>✓ Easy to understand | In case of loss of private key is irreparable<br>✓ Security compromise is possible in RSA. |
| [10] | Elkeelany et al. | Data Encryption Standard | It has strong encryption confusion and diffusion<br>✓ It is suitable for voice and video | An encryption system falls in two categories. Private Key or secret key. Same key is used for both encryption and decryption. Therefore keys must be kept hidden and secured from unauthorized users. . |
| [12] | Amirgaliyev Yedilkhan at al | EZ-cryptosystem | It is possible for individuals to post their public key on their websites | It cannot afford digital signatures that cannot be repudiated |

## 3. Conclusion

Virtual Private Network provides privacy and security to data in public network. This technology is extensively used by multi-national corporations and organizations to perform their business activities. It is cost efficient and provides an efficient and effective transmission of data among the network. This paper discusses the various risks and vulnerabilities that are involved in VPN and provides an insight to various VPN security protocols used. This paper focused on the demand for information security in a VPN environment considering its existing issues and limitations.

## References


[1].A.Thomas and G.Kelley," Cost-Effective VPN-Based Remote Network Connectivity over the Internet", Department of Computer Science, University of Massachusetts,100 Morrissey Boulevard, Boston, MA 02125-3393,2002.

[2] W. BouDiab, S. Tohme and Carole Bassil "Critical VPN Security Analysis and New Approach for Securing VoIP Communications over VPN Networks", WMuNeP"07, pp 92-96.

[3] IP Encapsulating Security Payload, Network Working Group, Request for Comments: 2406, Obsoletes: 1827, Category: Standards Track, @Home Network November 1998

[4]S.Kadry and W.Hassan, "Design and implementation of system and network security for an enterprise with worldwide branches", Journal of Theoretical and Applied Information Technology, School of Engineering, LIU, Beirut, Lebanon ,2008

[5] "Security & Savings with Virtual Private Networks", available:http://tools.netgear.com/media/whitepapers/VPN_Security.pdf. Last Available 19,04,2014.

[6] Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent Frederick, and Ronald W. Ritchey. Inside Network Perimeter Security. New Riders, 2003.

[7] SSH. Ssh main homepage. http://www.ssh.com, Visited 2004.

[8]Net gear, Virtual Private networking, 24,santacalara, 4500 Great America Parkway Santa Clara, CA 95054 USA, Available: http://documentation.netgear.com/reference/nld/vpn/pdfs/FullManual.pdf. Last Available: 19.04.2014.

[9] G. Bastian, E.Carter and C.Degu, "CCSP Cisco Secure PIX Firewall Advanced Exam Certification Guide", Cisco Press, 808, Indianpolis, IN 46240 USA, 2005.

[10] O. Elkeelany et al., "Performance analysis of IPSec protocol: encryption and authentication", IEEE Communications Conference (ICC 2002), 2002, pp. 1164–1168.

[11] S. Miltchev, S. Ioannidis and A. Keromytis, "A study of the relative costs of network security protocols", USENIX 2002 Annual Technical Conference, Monterey, CA, June 2002.

[12] Amirgaliyev Yedilkhan, Amanzholova Saule, Kalizhanova Aliya, ZamanovaSaule, Kozbakova Ainur" Using the ez-Cryptosystem for Data Transmission in Virtual Private Networks (Vpn)"

[13] Alexander V. Uskov" Information Security of IPSec-Based Mobile VPN: Authentication and Encryption Algorithms Performance" 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, DOI 10.1109/TrustCom.2012.187

[14] MarcinNiemiec & PetrMachnik" Authentication in virtual private networks based on quantum key distribution methods" DOI 10.1007/s11042-014-2299-1

[15] Yu-Liang Liu · Yeali S. Sun · Meng Chang Chen" MTRA: An on-line hose-model VPN provisioning algorithm" Telecommunication System (2006) 31:379–398 DOI 10.1007/s11235-006-6724-2.

[16] "Performance Analysis of AES and BLOWFISH Algorithms ", National Conference on Computer Communication & Informatics", School of computer science, RVS college of arts and science, March 07, 2012.

[17] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.