Security in Virtual private network

Tripti Sharma
Computer Science and Engineering Department
P.D.M College of Engineering
Bahadurgarh, India
triptisharma33@gmail.com

Rahul Yadav(Guide)
Computer Science and Engineering Department
P.D.M College of Engineering
Bahadurgarh, India

Abstract:- Information security, sometimes shortened to Info Sec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).

Virtual private networks (VPNs) offer low-cost, secure, dynamic access to private networks. Such access would otherwise only be possible by using an expensive leased line solution or by dialling directly into the local area network (LAN).

VPNs allow remote users to access private networks securely over the internet. A remote user in one part of the UK can establish a secure network connection using a VPN to a school LAN in another part of the UK and only incur the call cost for the local internet connection.

A virtual private network gives secure access to LAN resources over a shared network infrastructure such as the internet. It can be conceptualised as creating a tunnel from one location to another, with encrypted data travelling through the tunnel before being decrypted at its destination. Remote users can connect to their organisation's LAN or any other LAN. They can access resources such as email and documents as if they were connected to the LAN as normal. By using VPN technology it is possible to connect to a school LAN from anywhere in the world via the internet, and to access it securely and privately without incurring the large communication costs associated with other solutions.

Methods and Technology Used:

i) To minimize usage of CPU and memory.

ii) Comparison between two different platform of VPN based on hardware.

Five phases for development of test bed process:

i) Planning

ii) Design

iii) Implementation

iv) Testing

v) Compare

vi) Compile

Two VPN technologies that are being used are:

i) Site-to-site VPN

ii) Remote Access VPN

INTRODUCTION

VIRTUAL PRIVATE NETWORK

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer or network-enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryptions. Major implementations of VPNs include OpenVPN and IPsec.

Virtual Private Network as a term specifies:

Virtual – means that the connection is dynamic. It can change and adapt to different circumstances using the internet's fault tolerant capabilities. When a connection is required it is established and maintained regardless of the network infrastructure between endpoints. When it is no longer required the connection is terminated, reducing costs and the amount of redundant infrastructure.

Private – means that the transmitted data is always kept confidential and can only be accessed by authorised users. This is important because the internet's original protocols –TCP/IP (transmission control protocol/internet protocol) – were not designed to provide such levels of privacy. Therefore, privacy must be provided by other means such as additional VPN hardware or software.

Network – is the entire infrastructure between the endpoints of users, sites or nodes that carries the data. It is created using the private, public, wired, wireless, internet or any other appropriate network resource available. [1]

Types of VPN

There are 2 common types of virtual private network, which are remote access VPN and site-to-site VPN.

1. Remote Access VPN

Remote access VPN is very common VPN service that you can set up in your office or home network. It can be...
implemented by setting up a VPN gateway or server and you can connect to it by using VPN client from other locations. If not, you can also subscribe to VPN service provided by a VPN provider for similar secure access too. The remote access VPN is supported by L2F, PPTP, L2TP and IPsec tunneling protocols. Sometimes if the user uses the web browser instead of VPN client to connect to VPN gateway, we call this type of VPN as SSL VPN.

2. Site-to-Site VPN
Site-to-site VPN is the VPN connection established between 2 VPN gateways that reside in 2 different networks over the Internet, so that both networks’ computers can exchange data securely. There is no VPN client needed on user computers. The VPN connection will be established between both VPN gateways. Both VPN gateways will encrypt and decrypt the communication data to ensure the security and integrity of data [2]. The site-to-site VPN can be supported by IPsec tunnel mode, PPTP, L2TP over IPsec tunneling protocols.

II. Literature Study
A. Study the best approach of Virtual Private Network
In this paper we studied about the approach to propose an architectural solution to implement Virtual Private Network (VPN) test bed in campus environment. The objective of this evaluation is to measure the quality of the audio and video streaming on client server performance over different types of VPN technology.

1. Working
There are six phases development of test bed process such as:

- Planning
- Design
- Implementation
- Testing
- Compare
- Compile
In the experiment, the analysis performance will focus on CPU and memory measurement during audio and video streaming. Network management system is used to analyze activities of streaming over VPN technology. Figure.1 shows the process and criteria selection of streaming evaluation.

![Diagram of Streaming Evaluation](image)

**Fig.1: Framework of VoIP over VPN Technology in Campus Environment**

B. Virtual Private Network
In this paper we studied how VPN maintains privacy of data through security procedures and tunneling protocols. In effect, data is encrypted at sender’s side and forwarded via "tunnel” which is then decrypted at receiver’s side.

There are three primary components:
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- Internet Key Exchange (IKE) protocols.

1. Authentication Header (AH)
The IP Authentication Header (AH) is used to provide
- Connectionless integrity
- Data origin authentication for IP data grams.
- Anti-replay protection, which protects against unauthorized retransmission of packets.
AH can be used in two modes:
- **Tunnel mode**- AH creates new IP header for each packet.
- **Transport mode**- no new header is created.
Integrity and authentication are provided by the placement of the AH header between the IP header and the transport (layer 4) protocol header, which is shown as:
AH may be applied alone or in combination with the IP Encapsulating Security Payload (ESP). ESP when used with AH provides same anti-replay and integrity services with add on service of data confidentiality.

2. Encapsulating Security Payload (ESP)
ESP is the second core security protocol which provides authentication, integrity, and confidentiality which protects against data tampering and most importantly, provides message content protection. ESP also provides all encryption services. Encryption translates a readable message into an unreadable format to hide the message content. The
opposite process, called decryption, translates the message content from an unreadable format to a readable message. Encryption/decryption allows only the sender and the authorized receiver to read the data. Like AH, ESP can also be used in two modes: transport and tunnel. In tunnel mode, ESP creates a new IP header for each packet. This mode encrypts and protects the integrity of both IP header and data. While in transport mode no new IP header is created so ESP can only encrypt and protect the integrity of the data.

3. **Internet Key Exchange (IKE)**

Internet Key Exchange (IKE) is the protocol used to set up a security association (SA) in the IPsec protocol suite and to exchange keys between parties transferring data. Before secured data can be exchanged, a security agreement between the two computers must be established. In this security agreement, called as security association (SA), both agree on how to exchange and protect information.

**IPsec VPN Working**

When IPsec VPN is used, a virtual “tunnel” connecting the two endpoints is created. Configure which packets are sensitive. Once configured, an IPsec peer sends the packet through the tunnel to the remote peer. The traffic within the VPN tunnel is encrypted so that other users of the public Internet can not readily view intercepted communications [3][4].

**SSL VPN**

An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser. In contrast to the traditional Internet Protocol Security (IPsec) VPN, an SSL VPN does not require the installation of specialized client software on the end user's Computer. It is used to give remote users with access to Web Applications, client/server applications and internal network connections [5].

**SSL VPN Working**

An SSL VPN consists of one or more VPN devices to which the user connects by using his Web browser. The traffic between the Web browser and the SSL VPN device is encrypted with the SSL protocol or its successor [6].

C. **Number Theory In Providing Network Security**

Number theory is crucial for encryption algorithms, as it is most important to everyone in their life, as the whole world revolves around mathematics. We need to develop various machineries (notations and techniques) for manipulating numbers before can describe algorithms in a natural fashion. For security purpose in this paper Cryptography technique was applied as secret message:

1. **Cryptography**

A Cryptosystem is comprised of a pair of related encryption and decryption processes. In cryptography parlance, message is called “Plain Text”. The process of scrambling that message is referred to as [7] “Encryption”. After encryption of the message, the scrambled version is called “Cipher Text”. From the Cipher Text, Anyone can recover the original unscrambled message via “Decryption”.

**Secret Message**

Cryptography is the science (some might say art) of concealing data. Imagine that A needs to compose confidential email to someone. Having written the email, A can send it in one of two ways. The first, and usually convenient, way is to simply press the send button and not care about how our email will be delivered. Sending an email in this manner is similar to writing a confidential message on a postcard can see our message. On the other hand, before sending the email, A can scramble the confidential message and then press the send button. Scrambling the Message is similar to enclosing the postcard inside an envelope. While not 100% secure; at least we know that anyone wanting to read A’s postcard has to open the envelope [2].

In Cryptography parlance, A’s message is called “Plaintext”. The process of scrambling the message is referred to as “Encryption”. After encryption of the message, the scrambled version is called “Cipher Text”. “From the Cipher text, and can recover the original unscrambled message via “Decryption”. [8]

**Cryptography used Hill Cipher as an encryption technique**

**Classical Encryption Technique: HILL CIPHER**

This is a type of encryption technique. In this method the encryption function is defined by C=KP mod 26.

Where C and P are column vectors of length is 3x3 matrices represents the encryption key. Operations are performed mod 26. In this method also we “Mod “function in encryption process this is number theory tool. So the Number theory functions are so important in providing security while transmitting messages.

Some of the functions are so important in number theory while providing security in transmitting messages in network and in internet [7].

D. **Voice Security in Virtual Private Network**

Secured voice communication plays a very important role in our day to day lives. Any voice communication is threatened by two biggest risks. One is, when
someone is listening to our conversation behind our shoulder. The other main dangerous risk is, someone listening to it over the wire at the time when it is getting transmitted. Hence there is emerging need to digitize voice data packets over SIP protocol using ZRTP as the encryption mechanism [9]. The commercial deployment of VoIP leads to the employment of security mechanisms that can assure availability, reliability, confidentiality and integrity. The Session Initiation Protocol (SIP) is considered as the dominant signaling protocol for calls over the Internet. SIP, like other Internet protocols, is vulnerable to known Internet attacks [10].

1. VoIP

VoIP (voice over internet protocol)

A number of individuals in research environments, both in educational and corporate institutions, took a serious interest in carrying voice and video over IP networks, especially corporate intranets and the Internet. This technology is commonly referred to today as VoIP and is, in simple terms, the process of breaking up audio or video into small chunks, transmitting those chunks over an IP network, and reassembling those chunks at the far end so that two people can communicate using audio and video.

Importance

One of the most important things to point out is that VoIP is not limited to voice communication. In fact, a number of efforts have been made to change this popular marketing term to better reflect the fact that VoIP means voice, video, and data conferencing. All such attempts have failed up to this point, but do understand that video telephony and real-time text communication (VoIP), for example, is definitely within the scope of the VoIP [10].

2. SIP

SIP (Session Initiation Protocol) is a signaling protocol used to create, manage and terminate session in an IP based network. A session could be a simple two-way telephone call or it could be a collaborative multi-media conference session. This makes possible to implement services like voice-enriched e-commerce, web page click-to-dial or Instant Messaging with buddy lists in an IP based environment. SIP has been the choice for services related to Voice over IP (VoIP) in the recent past.

SIP is still growing and being modified to take into account all relevant features as the technology expands and evolves. But it should be noted that the job of SIP is limited to only the setup and control of sessions.

SIP serves four major purposes:

- SIP allows for the establishment of user location (i.e. translating from a user’s name to their current network address).
- SIP provides for feature negotiation so that all of the participants in a session can agree on the features to be supported among them.
- SIP is a mechanism for call management - for example adding, dropping, or transferring participants.
- SIP allows for changing features of a session while it is in progress.

3. ZRTP

ZRTP

It is described in the Internet Draft as a “key agreement protocol which performs Diffie-Hellman key exchange during call setup in-band in the Real-time Transport Protocol (RTP) media stream which has been established using some other signaling protocol such as Session Initiation Protocol (SIP).

ZRTP can be used with any signaling protocol, including SIP, H.323, Jingle, and distributed hash table systems. ZRTP is independent of the signaling layer, because all its key negotiations occur via the RTP media stream. ZRTP/S, a ZRTP protocol extension, can run on any kind of legacy telephony networks including GSM, UMTS, ISDN, PSTN, SATCOM, UHF/VHF radio, because it is a narrow-band bit stream-oriented protocol and performs all key negotiations inside the bit stream between two endpoints [11].

This protocol does not require prior shared secrets or rely on a Public key infrastructure (PKI) or on certification authorities, in fact ephemeral Diffie-Hellman keys are generated on each session establishment: this allows the complexity of creating and maintaining a trusted third-party to be bypassed. These keys contribute to the generation of the session secret, from which the session key and parameters for SRTP sessions are derived, along with previously shared secrets.

4. Dialer

In this component, once the SIP account is registered, the user will be able to dial the number of another Android SIP user through a custom-made touch-pad. In order to develop the custom touch-pad, we have created different images of the numbers in the application and have used them as resources.

Then we worked on the Android event listeners in order to display the numbers on the screen when the user accesses those resources. We have also built a delete key through which the user will be able to delete the numbers if any incorrect numbers have been typed. After the user has typed the correct the numbers, the Android APIs will initiate a call to the SIP recipient.
registered on the server [12]. If the call is made to an invalid recipient, it will be handled by the IVR of call centric server. Else, once the call is connected, the human voice shall be digitized by the Android APIs and the VoIP packets will travel over the SIP layer.

E. Network design for OSPF routing

Internet protocol (IP) traffic follows rules established by routing protocols, such as Open Shortest Path First (OSPF). Each router computes shortest paths using weights assigned by the network operator, and creates destination tables used to direct each IP packet to the next router on the path to its final destination. The Internet is made up of many routing domains, called autonomous systems (AS). Internet protocol (IP) traffic flows follows rules established by routing protocols. Shortest path first protocols, such as Open Shortest Path First (OSPF), are the most commonly used Interior Gateway Protocols (IGPs). These routing protocols direct traffic based on link weights assigned by the network operator. If a router has multiple outgoing links on shortest path to a given destination, it splits traffic evenly over these links. To satisfy requirements for Quality of Service (QoS) in IP routing, it is desirable to design a network to easily handle a single link or router failure without causing overload. One possible solution is to maintain part of the link bandwidth free in the eventuality of failures. This extended abstract addresses the issue of designing an OSPF-routed network with minimum total link capacity needed to route the required demand and handle any single (link or router) failure. We assume the topology is given but link capacities must be determined. [13]

F. Security Research of VPN Technology Based on MPLS

The VPN technology based on MPLS is the current mainstream VPN technology that uses isolations of routing and address or other information technologies to resist attacking and marking spoofing.

The VPN technology Based on MPLS is the current mainstream VPN technology that uses isolations of routing and address or other information technologies to resist attacking and marking spoofing, in which the security of data transmission is guaranteed to a certain extent. But as an IP-based network technology, it is not solving illegal access of a protected network element and the error configuration as well as internal attacks and other security issues which widespread in the management of shared network [14].

Multi-Protocol Label Switching (MPLS) is a new network technology of booting high speed data transmission and exchange by utilizing fixed-length label in open communication network[14]. It is powerful to overcome packet forwarding technology limitations of the traditional IP for the performance characteristics of a perfect combination of flexible routing functionality in the network layer (Layer 3) and the high-speed switching data in link layer (Layer 2). The key of MPLS technology is Label concept which is short and easy-to-handle and only has local significance of information content.

. It consists of several different sites collection in VPN which a site can belong to different VPN and sites can be controlled for visits and isolation. MPLS VPN architecture is mainly divided into data and control plane. Data plane defines the VPN forwarding process; the control plane defines the establishment of the Label Switched Path (LSP) and routing information distribution process of the VPN. Network framework of MPLS VPN is shown in the figure 2.6.

![Network Framework of MPLS VPN](image)

**Figure.2:** Network Framework of MPLS VPN

**Architecture:** The architecture of MPLS VPN consists of three components: CE, PE and P.

- **Customer Edge (CE):** the user interface. There are edge devices directly with the service provider network. CE can be either a router or a switch or a host. Typically, CE “perception” does not exist to VPN, also not need to support MPLS.

- **Provide Edge (PE):** the service provider of edge router, which is directly connected with the user’s CE. All managements of the VPN occur on PE, which the VPN routing information are maintained that is directly connected to, while all other VPN routing do not need to.

- **Provide (P):** the backbone routers of service provider in the network not directly connected with CE, which have MPLS forwarding capabilities

1. **The security threats of the control plane**

VPN routing information are exchanged through P/PE routers providing VPN services in the control plane, in which security attacks are against the two classes of devices. On the one hand, attacks are used on a routing protocol and illegal exchanging information of routers,
on the other hand, there is an attack on a routing device which allows P/PE router does not work regularly.

2. The security threats of the data plane
   - The security threats of internet
     In the case of VPN users are connect with internet, attacks are launched with IP source address spoofing, TCP session hijacking and planting Trojans, in which the user data streams are viewed, modified and deleted non-authorized.
   - The security threats of the shared device
     In the MPLS VPN network, it is shared of network resources by normal VPN users, such as CE and PE equipment. In this case, although the VPN tunnel system can guarantee the security of information delivery to a certain extent, all security measures only will increase security threshold, the possibility of an attacker illegal capture, forgery and replay the possibility of MPLS label package cannot rule out.

3. The security threats of the management plane
   - The attacking to network devices through the administrative interface: An attacker accesses network management system remotely through the network access control management interface illegal gained by means of guessing. Configuration management information of the device is viewed, extracted and changed.
   - Impact or damage management information delivery through clogging resource: If deliveries of resources are not through a specialized transport channel or the use of a "band" way of delivery, the management information does not pass normally for network resources are excessive extending by an attacker.
   - The disclosure of internal information.

The Improvements of MPLS VPN Security
Although the MPLS VPN has the same level of security as ATM, FR virtual circuit for packets are sent in the MPLS domain in the form of label forwarding, it is not secure enough by MPLS technology itself[6]. Therefore, the use of appropriate security measures to protect the MPLS VPN network security is very necessary for the threats of MPLS VPN in three levels. The design of MPLS VPN should be sure of routing information of the control plane are accurate, reliable and guaranteed, data delivery of the data plane are privacy, accuracy and integrity, configuration information of the management is secure [15].

1. Control plane safety
   The safe measures of control plane are mainly guaranteeing the deliverable security of the routing information and isolation of routing.

The routing protocol neighbor certifications are most widely deployed. Neighbor certification allows receiving routing to use key to authenticate routing update source that only it and neighbor router know. The key of authentication between routers does not need transport with using MD5 authentication. The key and message are created into message digests as MD5 hash value to prevent the router receiving unauthorized updates from routing peers. This mechanism are also used to verify tag distribution peers receive updates.

2. Data plane safety
   CE-PE data encryption the transmission path between CE and PE is relatively safe for multiple CE devices are connected into the PE via Ethernet switches with Virtual Local Area Network (VLAN) which the transmission path is determined by the network administrator.

3. PE-PE data encryption
   In order to guarantee the security of data transmission, Internet Protocol Security (IPsec) is deployment to authenticate or encrypt the data flow between ingress to export. The transmission of information between the PE is not encryption in general. The reasons are that it has a degree of security for the technology of MPLS VPN tunnels are used to transmit information; it is very complex of the implementation of encryption between PE and expensive of information delivery that heavy burdens of processing are bring to P/PE devices.

4. CE-CE data encryption
   IPsec tunnel is deployed to provide user data security in mutual communication between sites. This technology is deployed in the CE or between hosts requiring data protection in site.

5. Management plane safety
   The attack of hacker to network management system is primarily implemented through network management interfaces. In order to prevent the information of management thieving and malicious tampering, access authentication should be deployed at the administrative interface.
   The delivery channel of network management information In order to prevent information of resource network management abnormal delivering for resource squeezed, management terminal should be used with out-of-band access management interface. The use of the link is isolated physically or logically with other infrastructure in VPN. If manage terminal is in-band access management interface, a filter or firewall must use to limit access to non-authorized users.
The correctness of device configuration Network administrators should guarantee the correctness of the VPN device configuration to prevent leakages of user data, which require improving the skillful level of administrator and increasing the moral quality of education at the same time.

REFERENCES
[12] Lucas, etc. [author], Xielin, etc. [translate]. Firewall policy and VPN configuration [M].Chongqing: China Waterpower Press, 2008 “Network design for OSPF routing” – Luciana S. Buriliu1, Paulo M.França,1Mauricio G.C. Resende 2, and Mikkel Thorup2 Faculdade de EngenhariaEletrica de Computac a’o, UNICAMP, SP, Brazil.Internet and Network Systems Research, AT&T Labs Research, Florham Park, NJ, USA.