A SURVEY REPORT ON VPN SECURITY & ITS TECHNOLOGIES

JAYANTHI GOKULAKRISHNAN
Research Scholar, Department of CSE, Sathyabama University,
Chennai, Tamil Nadu, India.
jayagokul2003@yahoo.co.in

DR. V. THULASI BAI
Vice-Principal & Dean (R&D), Prathyusha Institute of Technology & Management,
Chennai, Tamil Nadu, India.
thulasi_bai@yahoo.com

Abstract

Virtual Private Network (VPN) is a communication network which provides secure data transmission in an unsecured or public network by using any combination of technologies. A virtual connection is made across the users who are geographically dispersed and networks over a shared or public network, like the Internet. Even though the data is transmitted in a public network, VPN provides an impression as if the data is transmitted through private connection. This paper provides a survey report on VPN security and its technologies.

Keywords: Tunneling; Protocols; Authentication; Encryption; Internet Key Exchange.

1. Introduction

A virtual private network (VPN) is the collection of private and public network such as Internet, and performs secure data transmission. A virtual private network can establish secured virtual links among different organizations, such as branch offices [6]. It will not provide any other external service between them and it will not allow any other organization to interrupt them [4]. A VPN sends data between two systems across a public network in such a way that the transmitted data is transparent to the other systems connected in the network. This transparency in data transmission is possible because VPN emulates point to point link between the two systems. Point to point link is provided by encapsulation of data. Data encapsulation is done by wrapping the data with a header, which provides routing information. This process is called as tunneling. To provide confidentiality to the encapsulated data, the data is secured by encryption. When data reaches a tunnel end point, the encapsulated data is decrypted and forwarded to its final destination point. A diagrammatic representation of Virtual Private Network is given in Fig.1.

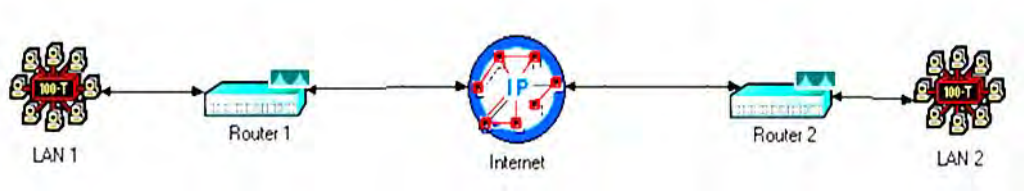

Fig.1. Virtual Private Network

VPN allows organizations to connect to their branch offices or to other companies over a public network while maintaining secure communications. The VPN connection across the Internet logically operates as a wide area network (WAN) link between the sites. The secure connection across the internet appears to the user as a private network communication—despite the fact that this communication occurs over a public internetwork—hence the name virtual private network. The paper is organized as follows: Section 1 gives an introduction to VPN. Section 2 contains an overview of VPN. Vulnerabilities and risks of VPN are described in Section 3. Section 4 contains various security protocols used in VPN. Conclusion is given in section 5.

2. VPN Security – An Overview

Security is the most important and critical factor for companies worldwide. Organizations need a secure and reliable infrastructure for their systems to mitigate the risk of malicious activity from both external and internal sources. Organizations worldwide have major security concerns namely

- Data access from the remote site
- Infection by viruses
- Intrusion by hackers

- Disruption in the storage network

To overcome the above mentioned threats and vulnerabilities in the network, VPN provides various security measures. The measures are outlined below:

- VPN provides authentication and encryption to data traffic in the network.
- Secure VPNs have more than one tunnels and each tunnel has two ends points, sender and the receiver. The sender and the receiver accept and agree upon the security properties of the tunnel.
- No external third party can change, modify or alter the security properties of the VPN.
- VPN creates a trusted path between the two end points, namely sender and receiver. This trusted path of transmission cannot be modified or altered by the third party who is not privy to VPN. The VPN provider only can make changes in the trusted path.
- Outsider cannot change, add or delete data on a path in VPN.
- The routing information and addressing used in a VPN are established before the creation of VPN.

The address boundaries of the VPN are made clear, so that data transmission between two addresses is done in a secured and trusted manner.

3. Vulnerabilities and Risks in VPN

A client node in a VPN can become a target machine for attack from within the network or from outside the network. An attacker can try to exploit the vulnerabilities in the client and try to attack the machine. Some of the attacks are:

- VPN Hijacking
- Man-in-the-middle attacks

VPN Hijacking: An attacker takes control over a VPN connection and impersonates a client machine in the network is called as VPN hijacking.

Man-in-the-middle attacks: An unauthorized machine starts intercepting the communication between the nodes in the network and changes the contents of the data that is transmitted between them. The type of changes includes addition, deletion and modification of data.

3.1 Authentication of Valid Users

User authentication is not strong in VPN. Since VPN connection is established by authorized users, it is assumed that the users in the VPN are authenticated users. Because of this vulnerability, there will be unauthorized access into the network and there can be data theft, missing of data etc.

3.2 Risks at the Client Side

Client users may have two connections, namely, a internet connection and a VPN connection to a private network. This will pose risk and threat to the private network, since the users expose the private network to the public network, which is internet. A client system may also be connected with a compromised system in terms of security in the network.

3.3 Interoperability

The two connecting systems in the network should agree upon the security protocols used for the data transmission. The protocols implemented by different vendors on the two sides of transmission may not always be synchronized. This may enhance the risks in the network.

3.4 Infections due to Virus or Malware

If a client system is infected by virus or malware, the whole network is compromised for an immediate attack. The attacker may be able to steal the VPN connection password. The virus or malware present in one client system may systemically spreads to other systems in the network thus making the network vulnerable and risk prone. Therefore, an effective anti-virus system should be incorporated into the network.

4. VPN Security Protocols

A VPN provides connectivity to end hosts or subnets identified as members of VPN [5]. VPN addresses the following requirements to be an effective network.

- Authentication: VPN validates the sender by providing provides data authentication
- Data Integrity: The data is not modified or changed in transit during transmission.
- Confidentiality: The data is encrypted so that the data becomes transparent to the other users in the network. The data can be seen only the sender and receiver.
- Replay Protection: VPN ensures that the attackers cannot intercept the data and play it back at some other time.

- Interoperability: Interoperability with other VPN network is possible because of the standard-based technologies used in VPN.

VPN uses various security protocols for tunneling. They are:

- Internet Protocol Security (IPSec)
- Layer 2 Tunneling Protocol (L2TP)
- Point-to-Point Tunneling Protocol (PPTP)

4.1 Internet Protocol Security (IPSec)

IPSec is one of the most complete, secure, and accessible standards based on developed protocols for data transportation [2]. It operates in the network layer. IPSec contains protocols which help in establishing mutual authentication between the two communicating parties at the beginning of the session and negotiation of cryptographic keys to be used during the session [1]. IPSec is a collection of security protocols that allows the system to choose the appropriate security protocols during data transmission. IPSec can be used to protect data transmission between two hosts or between a pair of security gateways (e.g. firewalls or routers) [7]. IPSec provides authentication of users, encryption of data and data integrity during the transmission of data between senders and receivers. It uses three primary protocols namely, Authentication header, Encapsulated Security Payload and Internet Key Exchange for establishing connection and transmitting data in a secure manner.

4.1.1 Authentication Header (AH):

Authentication Header protocol provides authentication of source nodes, data integrity. It does not provide encryption of data. All IP packets contain AH in their packed format. AH contains hashed data, sequence number, security parameter index etc. The diagrammatic representation of AH is given below in Fig. 2.

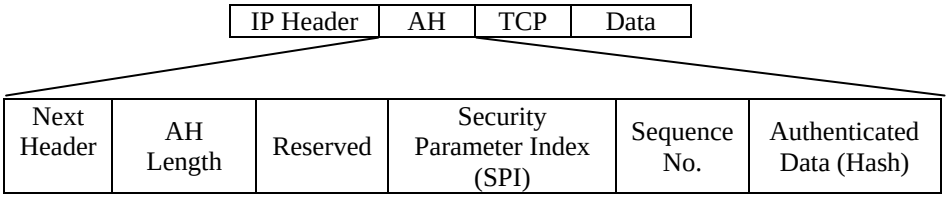

Fig. 2 Authentication Header

4.1.2 Encapsulated Security Payload (ESP):

Encapsulated Security protocol provides three major services namely, confidentiality of data, data integrity and authentication of source. It uses symmetric encryption algorithms for providing privacy and security of data. The sender and the receiver have to use the same encryption algorithm. The diagrammatic representation of ESP header and trailer in the data packet is given in Fig.3.

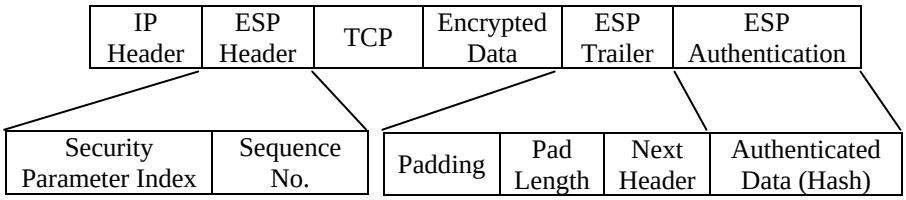

Fig.3 ESP Header and Trailer

All the security protocols run in two modes of operations. They are:

- Tunnel Mode
- Transport Mode

Tunnel mode operation is also called as end-to-end mode of operation. A tunnel connects two points of a VPN across the shared network infrastructure. In the tunnel mode, the end-points of the tunnel are common nodes of the VPN and the shared network infrastructure [8]. Tunnel mode provides data security. The data packet contains new IP header in addition to ESP header and trailer, original IP header, encrypted data and ESP authentication. The new IP header contains address of the end point of the tunnel. When the encrypted data packet reaches the end point of the tunnel, it is decrypted by the tunnel end point to find the destination address. Upon finding the destination address, the tunnel point routes the original data packet in the network to its destination. The diagrammatic representation of the tunnel mode packet format is given in Fig.4.

New IP Header	ESP Header	Original IP Header	Encrypted Data	ESP Trailer	ESP Authentication

Fig.4. Tunnel Mode Packet format

The other name for transport mode is host-to-host mode of operation. The data packet contains ESP header and trailer, ESP authentication, IP header etc. The IP header is not encrypted. Hence there is a possibility of sniffing the address by the attackers. It is also possible for the attackers to analyze the data traffic since header information is easily available to them. Fig.5 shows the transport mode packet format.

Original IP Header	ESP Header	TCP	Encrypted Data	ESP Trailer	ESP Authentication

Fig. 5. Transport Mode Packet format

4.1.3 Key Exchange and Management

IPSec provides two types of key management for virtual private network over the public network. They are:

- Manual Key Management
- Automated Key Management

In manual key management, secret keys are exchanged between the sender and receiver before connection is established between them. The values of secret keys and the security associations are known only to the sender and the receiver. This type of key management can be used in a small and static network environment. The secret keys between the communicating nodes are exchanged and known to each other before the actual data transmission takes place. Hence, the network cannot be dynamic and scaled. The major disadvantage of this method is, if the secret keys are captured by the third party who can be an attacker, there is every possibility that the security of the network is compromised.

Automated key management otherwise popularly known as Internet Key Exchange (IKE) is the default protocol used in IPSec for generating and managing the secret keys between the communicating nodes in the network. Unlike manual key management, the network which uses this type of key management can be dynamic and scaled. IKE performs the following tasks.

- Authentication of Users
- Session Negotiation between the communicating parties
- Key Exchange for data transmission
- IPSec tunnel negotiation and configuration

Authentication is the most important task performed by IKE. It uses any of the methods given below to authenticate the communicating nodes to each other.

- Shared key – Hashing technique is used by IKE and ensures that the nodes which possess the same can send the data packets.
- Digital Signature Standard - IKE uses public key digital signature cryptography to verify the valid nodes involved in the data transmission.
- Encryption - IKE uses encryption algorithms and makes sure that the negotiation between the two nodes can occur only if the node contains the correct private key.

During session negotiation, IKE allows the communicating nodes to negotiate the authentication method, the type of exchange algorithm and the encryption algorithm to be used. This is done before the actual data transmission that takes place between the nodes.

IKE uses the negotiated key-exchange method so that secure transaction takes place between sender and the receiver. Every session of the data transaction is protected with a new secret key.

After IKE has finished negotiating a secure method for exchanging information, IKE starts negotiating for an IPSec tunnel. IKE creates new secret key for the IPSec tunnel to use. The encryption and authentication algorithms for this tunnel are also negotiated. IPSec tunnels are configured using the VPN Group section for VPN Client tunnels and the Tunnel Partner section for LAN-to-LAN tunnels.

4.2 Point to Point Tunnel Protocol (PPTP)

Point to Point Tunneling Protocol is an OSI layer two protocol built on top of the Point to Point Protocol (PPP). PPTP connects to the target network by creating a virtual network for each remote client. The PPTP control connection carries the PPTP call control and management message that is used to maintain the PPTP tunnel [3]. PPTP allows a PPP session, with non-TCP/IP protocols, to be tunneled through an IP network. The authentication protocols used by PPTP are: Extensible Authentication Protocol (EAP), Microsoft Challenge-Handshake Authentication Protocol (MCHAP), Shiva Password Authentication Protocol (SPAP), and Password Authentication Protocol (PAP). Fig.6 represents the PPTP packet format.

IP Header	GRE Header	PPP Header	Encrypted PPP Data

Fig.6. PPTP Packet Format

Multiple levels of encapsulation of the data packet take place in PPTP tunneling. PPTP uses Generic Routing Encapsulation (GRE) for encapsulating the PPP data frames and transmits the encapsulated data in the public network such as Internet. GRE also provides congestion control and flow control mechanisms in addition to encapsulation of data. The encapsulated PPP data frames are encrypted. The resultant encapsulated and encrypted data frame is again encapsulated with an IP header. The IP header contains the source and destination IP addresses. When the PPTP data packet reaches the PPTP server, it removes the IP header, GRE header and PPP header from the data packet and decrypts the PPP data.

4.3 Layer 2 Tunneling Protocol (L2TP)

Asynchronous Transfer Mode, Frame Relay and X.25 networks use L2TP as tunneling protocol for data transmission between the communicating nodes. L2TP is also operated at the layer 2 of OSI architecture. One tunnel can allow multiple connections. Layer two tunneling protocol encapsulates data in PPP frames and is capable of transmitting non-IP protocols over an IP network. L2TP connections use the same authentication mechanisms as PPP connections, such as EAP, CHAP, and MSCHAP. L2TP tunneling is accomplished through multiple levels of encapsulation. The PPP data is encapsulated within a PPP header and an L2TP header. The encapsulated L2TP packet is further encapsulated in a UDP header. The final packet is encapsulated with an IP header containing the source and destination IP addresses of the VPN client and VPN server. L2TP packet format is given in Fig.7.

IP Header	UDP Header	L2TP Header	PPP Header	Encrypted PPP Data

Fig. 7 L2TP Packet Format

L2TP does not provide data confidentially. Hence it is used in conjunction with IPSec and is called as L2TP/IPSec. When L2TP is running over IPSec, security services are provided by IPSec, AH and ESP. All L2TP controls and data appear as homogeneous IP data packets to the IPSec system.

5. Conclusion

Virtual Private Network provides security and privacy to data in a public network. This technology is extensively used by organizations and multi-national corporations for their business activities. This technology is cost effective and provides an effective and efficient transmission of data among the network. This paper explains the various risk and vulnerabilities present in VPN and provides an insight to various VPN security protocols used. This paper focused majorly on three security protocols and their functionalities.

References

[1] Dhall H, Dhall D, Batra S and Rani P (2012), Implementation of IPSec Protocol, Second International Conference on Advanced computing & CommunicationTechnologies.978-0-7695-4640-7/1.2

[2] Gharehchopogh F S, Aliverdiloo R and Banayi V 2013), A New Communication Platform for data transmission in Virtual Private Network, International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol. 3, No.2,DOI : 10.5121/ijmnct.2013320101.

[3] Hussein S N and Hadi A (2013), The Impact Of Using Security Protocols In Dedicated Private Network And Virtual Private Network, International Journal of Scientific & Technology Research, Volume 2, Issue 11, ISSN 2277-8616, pp. 170-175.

[4] Kumar N M and Kumar K S (2013), Proposed Architecture for Implementing Privacy In Cloud Computing Using Grids And Virtual Private Network. International Journal of Technology Enhancements and emerging Engineering Research, Volume 1, Issue 3, ISSN 2347-4289.

[5] Lim L K, Gao J, Ng T S E, Chandra P, Steenkiste P and Zhang H (2001), Customizable Virtual Private Network Service with QoS, Computer Networks, Elsevier, pp.137-151.

[6] Malik A, Verma H K and Pal R. (2012), Impact of Firewall and VPN for securing WLANI, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 5, May 2012, pp.407-410.

[7] Parmer M S and Meniya A D (2013), Imperatives and Issues of IPSEC Based VPN, International Journal of Science and Modern Engineering (IJISME), ISSN: 2319-6386, Volume-1, Issue-2,pp. 38-41.

[8] Venkateswaran R (2001), Various Services and Implementation Scenarios: Virtual Private Networks". Institute of Electrical and Electronics Engineers (IEEE) Potentials, 11-15.