Virtual Private Network

Benjamin Odiyo, Mukunda Dwarkanath
{beod2131, mudw2335}@student.uu.se

Abstract:

This paper examines virtual private network (VPN) operation and how the network security concerns are implemented. We describe what VPN is, the different protocols used to address security concerns, and finally we look at point to point of protocol as used in Microsoft Windows family operating systems.

Introduction: Virtual Private Network

A virtual private network (VPN) is an extension of an organisation private network to connect remote users over shared or public network mainly the Internet. A private network is one where all data paths are secret to a certain extent, yet open to a limited group of persons, for example, to employees of a specific company [1]. VPNs extend geographic connectivity to telecommuters, mobile users, remote offices, customers and suppliers who need to connect to the main office. The following figure is an example of a VPN.

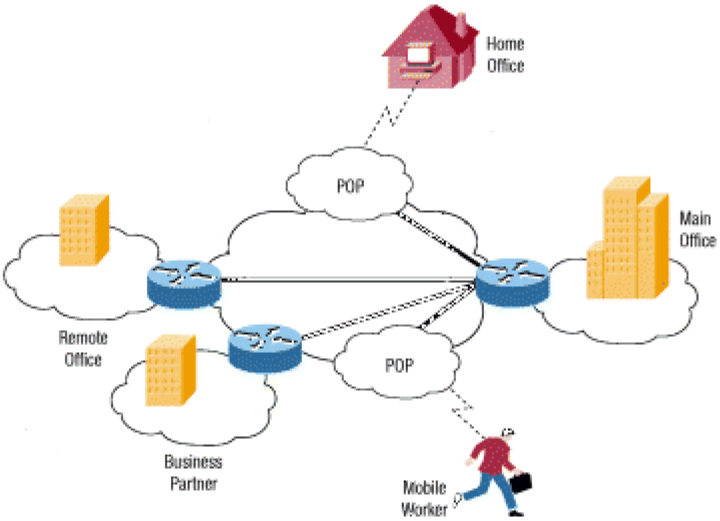

Figure 1: Example of a VPN [3]

VPNs are IP-based networks (Internet) that use encryption and tunnelling to achieve the following goals [7]:

- connect users securely their own corporate network (remote access)
- link branch offices to an enterprise network (intranet)
- Extend organizations' existing computing infrastructure to include partners, suppliers and customers (extranet).

Since security is the major concern of any VPN, the properties like confidentiality, integrity and authentication are ensured by the VPN.

Confidentiality: Protecting the privacy of the data being exchanged between the two communicating parties in done by the method of Encryption. Two primary cryptographic system used in VPN are secret key cryptography and public key cryptography.

Integrity: Information being transmitted through the Internet should not be modified during any transit. This is achieved either by one way hash function, message authentication codes (MACs) or digital signatures

Authentication ensures the identity of the communicating parties. It is achieved through password Authentication or digital certificates.

VPN Protocols

In making a connection, data it is first encapsulated and then encrypted for confidentiality. The part of the connection in which the private data is encapsulated is known as the tunnel, while the one in which the private data is encrypted is known as the virtual private network (VPN) connection

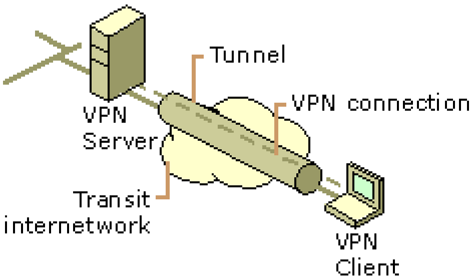

Figure 2: Virtual Private Network Connection [6]

There are different protocols used for tunnelling. Tunnelling protocol basically carry PPP datagram over a non point-to-point network. Some of the commonly used protocols are:

Point to Point Tunnelling Protocol (PPTP)

The Point-to-Point Tunnelling Protocol (PPTP), developed by Microsoft, is the most widely supported VPN method among Windows users. PPTP uses the same types of authentication as PPP (PAP, SPAP, CHAP, MS-CHAP) . PPTP establishes the tunnel, but does not provide Encryption. The encryption is done using Microsoft Point-to-Point Encryption (MPPE) protocol to create a secure VPN. PPTP has relatively low overhead, making it the fastest among the various VPN methods.

Layer 2 Tunnelling Protocol (L2TP)

The Layer 2 Tunnelling Protocol (L2TP) developed in cooperation between Cisco and Microsoft, combining features of PPTP and Layer 2 Forwarding (L2F) protocol.
One advantage of L2TP over PPTP is that it can be used on non-IP networks such as ATM, frame relay and X.25.

Internet Protocol Security (IPSec)

IPSec can itself be used as a tunnelling protocol, and is considered as the “standard” VPN solution, especially for gateway-to-gateway (site-to-site) VPNs that connect two LANs. IPSec operates at the Network layer (Layer 3)

Socks 5

This is a circuit level proxy protocol that was designed to facilitate authenticated firewall traversal. It is an excellent choice for extranet configurations since it provides a secure proxy architecture with extremely granular access control. It can be used with other VPN technologies. For example, one may combine IPSec with Socks together so that IPSec secure the underlying network protocol while SOCKS could be used to enforce user-level and application access control.

Point-to-Point Protocol Authentication

Point-to-Point Protocol (PPP) supports two kinds of authentication protocols [4]: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) as specified in RFC 1334.

PAP uses a two-way handshake for a remote node to establish its identity. After the PPP link establishment phase is complete, a username and password pair is repeatedly sent by the remote node across the link (in clear text) until authentication is acknowledged, or until the connection is terminated. It is not a secure method since password and user name is sent across the link in clear text and there is no protection from playback or trial-and-error attacks. Also the remote node is in control of the frequency and timing of the login attempts.

CHAP on the other side; verify the identity of the remote node using three way handshake. These are the general steps performed in CHAP:

a) The authenticator sends a challenge message to the remote node.
b) The remote node responds with a value calculated through a one-way hash function.
c) The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is successful. Otherwise, the connection is terminated.

CHAP depends on a password known only to the authenticator and the remote node. The password is not sent over the link. It also supports a two-way authentication in which the remote node initiates the CHAP negotiation with a challenge.

An illustration of CHAP will clarify the process. Consider two nodes, A and B, wanting to perform a CHAP negotiation, in this case, one-way authentication where node B is the authenticator. The process is as follows:

a) Node A requests for a login challenge from node B.
b) Node B issues a challenge to node A by sending a challenge packet which has a packet type identifier, a challenge identifier (ID), random number generated and the name of the challenger. This is the challenge phase.
c) Node A, upon receipt of the challenge packet, it locates the password for the name of the challenger (node A) from it database. It then uses the password, the challenge ID, and the random number for hashing. These values are hashed using Message Digest Algorithm 5 (MD5) and a hash value is obtained. Finally it sends a response packet that contains the challenge ID, the hash value and its name (responding node name). This is the response phase.
d) Node B upon receiving the response, it retrieves the password for node A from its database, then hash it together with the challenge ID and the random number using

MD5. It compares it’s the hash value obtained with the one in the response packet. If the values match, it sends a result packet having the challenge ID and the acceptance to Node A. Otherwise the connection is terminated. This is the Result phase.

Microsoft- Challenge Handshake Authentication Protocol version 2 -(MS-CHAPv2)

This uses a two-way authentication procedure. It was mainly introduced in Windows 2000 and used also in the XP and 2003 server. Priori to its introduction, Microsoft used Challenge Handshake Authentication Protocol version 1 (MS-CHAPv1).It takes place in the following order [2]:

1) The client requests a login authenticator challenge from the server.
2) The server sends back a 16-bytes random authenticator challenge.
3) The client generates the response:
   a) The client generates 16-bytes random Peer Authenticator Challenge.
   b) The client generates an 8-byte challenge by hashing the authenticator challenge, the Peer Authenticator Challenge, and the user's login using Secure Hash Algorithm (SHA).
   c) The client generates the NT password hash from the user's password.
   d) The 16-byte NT password hash from step (c) is padded with 5 bytes of zero. From these 21 bytes three 7-byte DES keys are derived.
   e) The first 8 bytes of the hash generated in step (b) (these 8 bytes are later referred to as the challenge) are encrypted using DES with each of the three keys generated in step (d).
   f) The 24 bytes resulting from step (e), the 16-byte random peer challenge, and the user's login are sent back to the server as response.
4) The server decrypts the response with the hashed password of the client that is stored in a database.
   a) If the decrypted response matches the challenge, the server sends a positive authenticator response:
   b) The server hashes the NT password hash using MD4 to generate a password-hash-hash.
   c) The server generates a hash using SHA from the client’s response, the password-hash-hash, and the literal constant (magic server to client signing constant and is 0xD1269E value for high bits of the 64-bit RC4 [ARCFOUR] key).
   d) The server generates another hash using SHA from the 20-byte output of step (c), the 8-byte challenge, and the literal constant.
   e) The resulting 20 bytes are sent back to the client.
5) The client repeats the same procedure to generate the 20 bytes and compares them to the server’s authenticator response. If they match, both the client and the server are authenticated.

MS-CHAPv2 is complicates and it has been shown [5] that simple cryptographic libraries is sufficient to perform the equivalent authentication. Another flaw is in deriving DES key. By having the last five bytes of the third DES assigned to all zero in effect reduce the length to 16 bit. With brute force, one need 655536 different DES keys, by reducing the hash space, since hash values are usually evenly distributed, one needs only hash values from the search password space of 2^{16} factor. Finally it was susceptible to version rollback attacks.

Currently Windows XP and Windows 2003 Server version of the operating systems fully support the use of IPSec for tunnelling [6]. In Windows 2000 it was an optional feature that required third party utilities.

Conclusion

For Virtual Private Network to ensure security, data is encapsulated and encrypted before sending the packets over the Internet. The various protocols used include IPSec, L2TP, PPTP, SOCKS etc. While PPTP, developed by Microsoft and implemented heavily on it legacy operating system, it has it own flaws and require the support of an extra protocol, currently IPSec, in order to be secure. The different protocols acts at different layers of the OSI protocol stack layer model and hence can be combine to enhance security in VPN.

References

[1]. Pawel Golen, 2002 Virtual Private Networking, http://www.windowsecurity.com/articles/Virtual_Private_Networking.html

[2]. B. Schneider and Mudge, (1998), Cryptanalysis Of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)

[3]. Cisco Document ID: 14106 How Virtual Private Networks Work

[4]. Cisco Document ID: 25647 Understanding and configuring PPP CHAP Authentication

[5]. Jochen Eisinger, (2001) Exploiting Known Security Holes In Microsoft's PPTP Authentication Extensions (MS-Chapv2).

[6]. Microsoft Cooperation, (2003), Virtual Private Networking with Windows Server 2003: Interoperability, Windows Server 2003 White Paper

[7]. Christopher McDonald, Virtual Private Network Overview, http://www.intranetjournal.com/foundation/vpn-1.shtml

[8]. Gollmann, D. (2006), Computer Security. John Wiley & Sons, West Sussex, England,