

# Privacy and Security on Internet: Virtual Private Networks

Doina Bein<sup>\*</sup>, Wolfgang Bein<sup>\*\*</sup>, Vasu Jolly<sup>\*\*\*</sup> and Shahram Latifi<sup>\*\*\*\*</sup>

<sup>\*</sup> School of Computer Science, University of Nevada Las Vegas, Postal address, 4505 Maryland Parkway, Las Vegas, NV, 89154, USA, Phone: +1 702 895 1634, Fax: +1 702 894 2639, Email: siona@cs.unlv.edu, Web: www.cs.unlv.edu/~siona

<sup>\*\*</sup> School of Computer Science, University of Nevada Las Vegas, Postal address, 4505 Maryland Parkway, Las Vegas, NV, 89154, USA, Phone: +1 702 895 1477, Fax: +1 702 894 2639, Email: bein@cs.unlv.edu, Web: www.cs.unlv.edu/~bein

<sup>\*\*\*</sup> Department of Electrical and Computer Engineering, University of Nevada Las Vegas, Postal address, 4505 Maryland Parkway, Las Vegas, NV, 89154, USA, Phone: +1 702 895 1382, Fax: +1 702 895 0488, Email: jolly@egr.unlv.edu, Web: www.egr.unlv.edu/~jolly

<sup>\*\*\*\*</sup> Department of Electrical and Computer Engineering, University of Nevada Las Vegas, , Postal address, 4505 Maryland Parkway, Las Vegas, NV, 89154, USA, Phone: +1 702 895 4016, Fax: +1 702 895 0488, Email: latifi@ee.unlv.edu, Web: www.egr.unlv.edu/~latifi

***Abstract*** - *The need for privacy and data security within an organization's infrastructure and also among corporation's remote sites or employees has been a crucial issue for years. Such privacy and security needs have caused the development of Virtual Private Networks. A Virtual Private Network is a concealed network, which uses a public network (usually the Internet) to connect remote sites or users. Virtual Private Networks do not offer network services already offered through alternative mechanisms. Rather, a unique mix of technologies (tunneling and encryption) permits organizations to establish secure, private, end-to-end network connections over third-party networks. Thus, instead of using a dedicated, real-world connection, such as a leased line, a Virtual Private Network uses virtual connections routed through the Internet from the company's private network to the remote site thus reducing the in-house requirements for equipment and support. In this article we study current trade-offs in tunneling and encryption, the key aspects in a Virtual Private Network.*

***Keywords:*** *Encryption, P2P Networks, tunneling, Virtual Private Networks.*

## I. INTRODUCTION

Virtual Private Networks (VPNs) started out in response to a need for secure, reliable and fast communication between offices, employees, and headquarters of a company. Leased lines, ranging from ISDN (Integrated Services Digital Network, 128 Kbps) to OC3 (Optical Carrier-3, 155 Mbps) fiber, provided a way to expand the company private network beyond its immediate geographic area ([2]). But the reliability, performance and security of such a Wide Area Network (WAN) had to be traded off for high costs of leased lines to bridge distances among offices. The goal of all VPNs is to enable a geographically distributed group of hosts to interact and be

managed as a single network, independent of the physical position (*virtual* network). A *private network* supports an isolated community of authorized users, which can access resources and services only within the network. Thus, a VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users ([2]). VPNs feature the security of a private network via encryption and access control while taking advantage of the inherent management capabilities and low costs of large public networks.

Rather than using a dedicated, real-world connection such as a leased line, a VPN uses virtual connections routed through the Internet from the company's private network to the remote site or employee. Traditionally, a large organization wanting to build a WAN needed to obtain costly, dedicated lines to link its offices. The high price of such a line has been unaffordable for most companies, which preferred instead to lease the lines and pay a monthly fee for the privilege of using such lines. The high cost of implementing and managing private networks compared to inexpensive but insecure public networks has implied a compelling alternative: Internet-based Virtual Private Networks.

VPNs provide an encrypted connection between a user site over a public network (e.g. the Internet). Such protocols effectively send data through a "tunnel" by encrypting data at the sending end and decrypting it at the receiving end. That tunnel cannot be entered by data that is not properly encrypted and is not part of the user traffic. An additional level of security can be achieved by encrypting not only the data but also the originating and receiving network addresses. Any valid remote user can connect to the corporate network, which is responsible for validating its own users. Most VPNs implement strong encryption mechanisms to prevent data to be directly viewed by sniffers. (A *sniffer* monitors network data by collecting data packets related to specific or non-specific traffic, and can be a software program or a hardware device with the appropriate software or firmware programming).

## II. FUNCTIONALITY AND TYPES OF VPN

In a VPN a company uses the bandwidth of a public packet-routed network, typically the Internet, or an ISP network to establish private, secure connections among its remote offices and employees. The company's Local Area Networks (LANs) and remote users are connected to the provider network with the same types of access methods used for Internet access: dial-up, DSL, cable, ISDN, T1, and wireless. Based on what is connected through a VPN and the type of connection, there are three types of VPNs (see Figure 1):

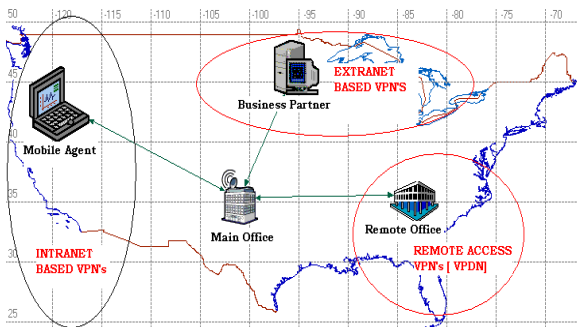


Figure 1. Types of VPNs

- Intranet VPN; it connects LAN to LAN using permanent connections to a third party network or Internet, among internal corporate departments and branch offices ([2]). Because this type of connection is fast and easy to establish, Intranet VPNs provide employees with full access to the company network, regardless of the size, number, or location of its remote operations. The primary technological requirements are strong data encryption to protect sensitive information, reliability of ensuring the prioritization of mission-critical applications, and scalable management requirements to accommodate a rapidly growing number of users, offices and applications.
- Extranet VPN; this is a special LAN to LAN temporary connection between a corporation and its strategic partners, customers, suppliers providing them with limited access to specific portions of the company network for purposes of collaboration and coordination ([3]). Access methods may include both dial-up and persistent connections, but access is subject to rigorous user identification and authorization controls. Equally important are the control of bottlenecks at network access points and a guarantee of swift delivery and rapid response time for critical data.
- Remote Access VPN, also called a virtual private dial-up network (VPDN), is a user-to-LAN connection for a company where employees need to connect from remote and changing locations. (An example is a news organization with hundreds of reporters in the field). A

company might contract out a large remote-access VPN to an enterprise service provider (ESP). The ESP sets up a network access server (NAS) and provides the remote users with desktop client software for their computers. As a result, telecommuters can dial a toll-free number to reach the NAS and use their VPN client software to access the corporate network ([2]).

## III. ENCRYPTION

Encryption ensures data privacy by allowing data to be encrypted and read by only the intended parties.

In a private-key encryption or symmetric-key encryption ([2]), each computer has a secret key (code) that it uses to encrypt a packet of information before it is sent over the network to another computer. Symmetric-key encryption requires that it is known which computers will be talking to each other such that a key can be installed on each. Symmetric-key encryption uses a secret code which each of the two computers must know in order to decode the information and where the code provides the key to decoding the message. Examples are RC4, used in Windows95, the DES Data Encryption Standard (DES) and triple DES, which are used by the IPsec suite of protocols ([4]). RC4 provides protections against all but the most professional code-breakers; used over the Internet it provides considerably more security than transmitting clear data over (supposedly) private lines. DES and triple DES are techniques used for the most sensitive commercial data.

Public key encryption or asymmetric-key encryption ([2]) uses a combination of a private key and a public key. The public key is published with a certificate (or public key certificate) which is a data structure that is digitally signed by a certification authority (CA) using a private key. To decode an encrypted message, a computer must use the public key provided by the originating computer and its own private key ([4]). A very popular public-key encryption utility is Pretty Good Privacy (PGP).

## IV. TUNNELING

Most VPNs rely on tunneling to create a private network that reaches across the Internet. Essentially, *tunneling* is the process of placing an entire packet within another packet and sending it over a network. Tunneling requires three different protocols ([2]):

- Carrier protocol - the protocol used by the network that the data utilizes,
- Encapsulating protocol - the protocol wrapped around the original data (GRE, IPsec, L2F, PPTP, L2TP, SOCKS),
- Passenger protocol - the original data (IPX, NetBeui, IP) carried.

These protocols work at different layers of the OSI model (see Figure 2). In the OSI model, data communication starts with the top layer at the sender side, travels down to the bottom layer, then crosses the network connection to the bottom layer on the receiver side, and then goes back up.

The upper layers of the OSI model represent software that implements network services like encryption and connection management. The lower layers of the OSI model implement more primitive, hardware-oriented functions like routing, addressing, and flow control.

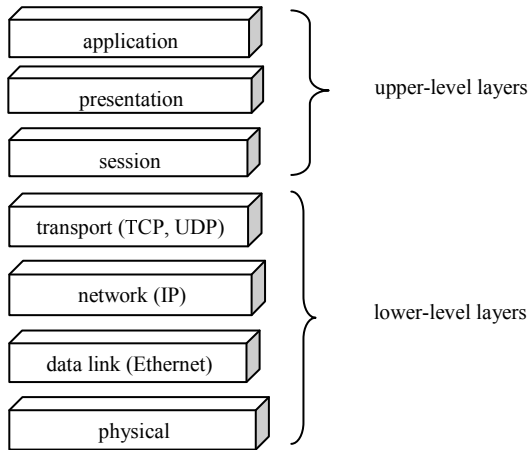


Figure 2. The OSI model

As part of the TCP/IP stack, PPP (Point-to-Point Protocol) is the carrier for other IP protocols when communicating over the network between the host computer and a remote system. In a remote-access VPN, tunneling normally uses PPP. Each of the protocols listed below were built using the basic structure of PPP. Internet Protocol Security (IPSec) works at the third layer of the OSI model, and encrypts and encapsulates the payload into IP packets ([5]). Only systems that are IPSec-compliant can take advantage of this protocol. Also, all devices must use a common key and the firewall of each network must have similar security policies.

Internet Protocol Security extends standard IP for the purpose of supporting more secure Internet-based services (including, but not limited to, VPNs). Internet Protocol Security specifically protects against "Man in the Middle Attacks" by hiding IP addresses that would otherwise appear on the wire. Internet Protocol Security has two encryption modes: Tunnel and Transport. The mode "Tunnel" encrypts the header and the payload of each packet while "Transport" only encrypts the payload. IPSec works well on both remote-access and site-to-site VPNs. We note that IPSec must be supported at both tunnel interfaces.

Generic Routing Encapsulation (GRE) is usually the encapsulating protocol that provides the framework in a LAN-to-LAN VPN. It specifies how to package the passenger protocol for transport over the carrier protocol (typically IP-based ([2]).) This includes information on

what type of packet is encapsulated and about the connection between the client and server. Instead of GRE, IPSec (in Tunnel mode) is sometimes used as the encapsulating protocol.

The Network Security Protocol (SOCKS) functions at the session layer (layer five) in OSI unlike all of the other VPN protocols that work at layer two or three. Such an implementation has both advantages and disadvantages when compared with other protocol choices. Operating at this higher level, SOCKS allows administrators to limit VPN traffic to certain applications. To use SOCKS, however, administrators must configure SOCKS proxy servers within the client environments as well as SOCKS software on the clients themselves.

The Point-to-Point Tunneling Protocol (PPTP) supports non-IP protocols. It was created by the PPTP Forum, a consortium, which includes US Robotics, Microsoft, 3COM, Ascend and ECI Telematics ([2]). PPTP is generally associated with Microsoft because nearly all flavors of Windows include built-in support for the protocol ([1]). The primary drawback of PPTP is its inability to choose a single standard for encryption and authentication. Two products which both fully comply with the PPTP specification may be entirely incompatible with each other; they might encrypt data differently, for example. PPTP supports 40-bit and 128-bit encryption and can use any authentication scheme supported by PPP.

L2F (Layer 2 Forwarding) was implemented primarily in Cisco products that use any authentication scheme supported by PPP ([2]).

L2TP (Layer 2 Tunneling Protocol) works at layer two of the OSI model. It encapsulates PPP frames to be sent over IP, X.25, frame relay, SONET or ATM (asynchronous transfer mode) networks ([5]). Combining features of both PPTP and L2F, L2TP also fully supports IPSec ([1]). L2TP carries the PPP through networks that are not point-to-point and simulates a point-to-point connection by encapsulating PPP data grams for transportation through routed networks or inter-networks. Upon arrival at their intended destination, the encapsulation is removed, and the PPP datagrams are restored to their original formats.

## V. CONCLUSION

Internet based VPNs have become a feasible and economically interesting solution for deploying wide area corporate networks. They accomplish that objective in a very secure and efficient manner. Indeed, an important aspect is the potential for businesses to reduce cost. Should the cost of long-distance calling and leased lines continue to drop, fewer companies may feel the need to switch to VPNs for remote access. However, if VPN standards solidify and vendor products become compatible, the appeal of VPNs will inevitably still increase. The success of VPNs also depends on the ability of Intranets and Extranets to deliver on their promises. Companies have had difficulty measuring the cost savings of their private networks, but if it can be demonstrated that these provide significant value, the use of VPN technology internally may also increase.

VPN technology is still in its infancy. With some of the hype that has surrounded VPNs historically, the potential pitfalls or weak spots in the VPN model are sometimes missed. These four concerns with VPN solutions are often raised ([1]):

- VPNs may be more susceptible to "Man in the Middle" Attacks. In addition, some private data may not be encrypted by the VPN before it is transmitted on the public wire. IP headers, for example, will contain the IP addresses of both the client and the server. Hackers may capture these addresses and choose to target these devices for future attacks.
- VPNs require an in-depth understanding of public network security issues and proper deployment of precautions.
- The availability and performance of an organization's wide-area VPN (over the Internet in particular) depends on factors largely outside of their control.
- VPN technologies from different vendors may not work well together due to immature standards.

But the general belief is that in a few years VPNs will demonstrate most of the advantages promised. VPN will then indeed be a global technology linking geographic regions around the world.

## ACKNOWLEDGEMENTS

This paper was supported by the Graduate & Professional Student Association Summer 2004 grant.

## REFERENCES

- [1] Bradley Mitchel, Introduction to VPN, About Inc., <http://compnetworking.about.com/library/weekly/aa010701c.htm>
- [2] Jeff Tyson, "How Virtual Private Networks work?" <http://computer.howstuffworks.com/vpn.htm>
- [3] Jerry Ryan "Managing the costs and complexities of VPN deployment", Techguide2001, [http://www.lucent.com/livelink/09009403800048e8\\_White\\_paper.pdf](http://www.lucent.com/livelink/09009403800048e8_White_paper.pdf)
- [4] Microsoft Corporation, White paper on "Virtual Private Networking in Windows 2000: An Overview", September 2001, <http://www.microsoft.com/windows2000/docs/VPNoverview.doc>
- [5] Roger Younglove "Virtual private networks-how they work", Computing and control engineering journal, December 2000