VPN SECURITY

February 2008

TABLE OF CONTENTS

SUMMARY

There is an increasing demand nowadays to connect to internal networks from distant locations. Employees often need to connect to internal private networks over the Internet (which is by nature insecure) from home, hotels, airports or from other external networks. Security becomes a major consideration when staff or business partners have constant access to internal networks from insecure external locations.

VPN (Virtual Private Network) technology provides a way of protecting information being transmitted over the Internet, by allowing users to establish a virtual private "tunnel" to securely enter an internal network, accessing resources, data and communications via an insecure network such as the Internet.

This paper provides a general overview of VPN and core VPN technologies. We discuss the potential security risks as well as the security considerations that need to be taken into account when implementing a virtual private network.

I. WHAT IS VPN?

VPN (Virtual Private Network) is a generic term used to describe a communication network that uses any combination of technologies to secure a connection tunnelled through an otherwise unsecured or untrusted network[1]. Instead of using a dedicated connection, such as leased line, a "virtual" connection is made between geographically dispersed users and networks over a shared or public network, like the Internet. Data is transmitted as if it were passing through private connections.

VPN transmits data by means of tunnelling. Before a packet is transmitted, it is encapsulated (wrapped) in a new packet, with a new header. This header provides routing information so that it can traverse a shared or public network, before it reaches its tunnel endpoint. This logical path that the encapsulated packets travel through is called a tunnel. When each packet reaches the tunnel endpoint, it is “decapsulated” and forwarded to its final destination. Both tunnel endpoints need to support the same tunnelling protocol. Tunnelling protocols are operated at either the OSI (Open System Interconnection) layer two (data-link layer), or layer three (network layer). The most commonly used tunnelling protocols are IPsec, L2TP, PPTP and SSL. A packet with a private non-routable IP address can be sent inside a packet with globally unique IP address, thereby extending a private network over the Internet.

VPN SECURITY

[1] http://cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/vpn.htm

VPN uses encryption to provide data confidentiality. Once connected, the VPN makes use of the tunnelling mechanism described above to encapsulate encrypted data into a secure tunnel, with openly read headers that can cross a public network. Packets passed over a public network in this way are unreadable without proper decryption keys, thus ensuring that data is not disclosed or changed in any way during transmission.

VPN can also provide a data integrity check. This is typically performed using a message digest to ensure that the data has not been tampered with during transmission.

By default, VPN does not provide or enforce strong user authentication. Users can enter a simple username and password to gain access to an internal private network from home or via other insecure networks. Nevertheless, VPN does support add-on authentication mechanisms, such as smart cards, tokens and RADIUS.

II. BUSINESS CONSIDERATIONS

VPN DEPLOYMENT

VPN is mainly employed by organisations and enterprises in the following ways:

1. Remote access VPN: This is a user-to-network connection for the home, or from a mobile user wishing to connect to a corporate private network from a remote location. This kind of VPN permits secure, encrypted connections between a corporate private network and remote users.
2. Intranet VPN: Here, a VPN is used to make connections among fixed locations such as branch offices. This kind of LAN-to-LAN VPN connection joins multiple remote locations into a single private network.
3. Extranet VPN: This is where a VPN is used to connect business partners, such as suppliers and customers, together so as to allow various parties to work with secure data in a shared environment.
4. WAN replacement: Where VPN offers an alternative to WANs (Wide Area Networks). Maintaining a WAN can become expensive, especially when networks are geographically dispersed. VPN often requires less cost and administration overhead, and offers greater scalability than traditional private networks using leased lines. However, network reliability and performance might be a problem, in particular when data and connections are tunnelled through the Internet.

TYPES OF VPN PRODUCT

VPNs can be broadly categorised as follows[2]:

1. A firewall-based VPN is one that is equipped with both firewall and VPN capabilities. This type of VPN makes use of the security mechanisms in firewalls to restrict access to an internal network. The features it provides include address translation, user authentication, real time alarms and extensive logging.
2. A hardware-based VPN offers high network throughput, better performance and more reliability, since there is no processor overhead. However, it is also more expensive.
3. A software-based VPN provides the most flexibility in how traffic is managed. This type is suitable when VPN endpoints are not controlled by the same party, and where different firewalls and routers are used. It can be used with hardware encryption accelerators to enhance performance.
4. An SSL VPN[3] allows users to connect to VPN devices using a web browser. The SSL (Secure Sockets Layer) protocol or TLS (Transport Layer Security) protocol is used to encrypt traffic between the web browser and the SSL VPN device. One advantage of using SSL VPNs is ease of use, because all standard web browsers support the SSL protocol, therefore users do not need to do any software installation or configuration.

---

[2] http://www.processor.com/editorial/article.asp?article=articles%2Fp2634%2F31p34%2F31p34.asp

[3] http://csrc.nist.gov/publications/drafts/SP800-113/Draft-SP800-113.pdf

III. COMMON VPN TUNNELING TECHNOLOGIES

The following tunnelling technologies are commonly used in VPN:

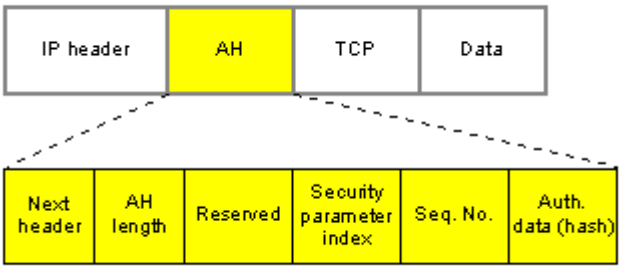
IPSEC (INTERNET PROTOCOL SECURITY)

IPsec was developed by IETF (the Internet Engineering Task Force) for secure transfer of information at the OSI layer three across a public unprotected IP network, such as the Internet. IPsec enables a system to select and negotiate the required security protocols, algorithm(s) and secret keys to be used for the services requested. IPsec provides basic authentication, data integrity and encryption services to protect unauthorised viewing and modification of data. It makes use of two security protocols, AH (Authentication header) and ESP (Encapsulated Security Payload), for required services. However, IPsec is limited to only sending IP packets.

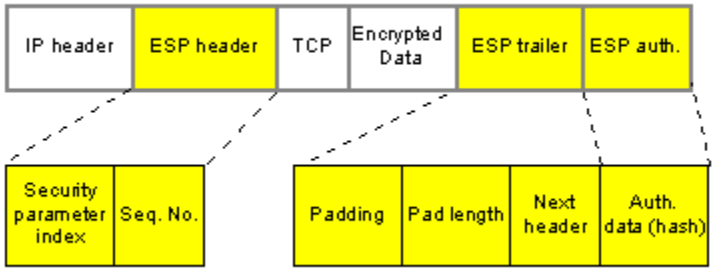
Security Protocols for Traffic Security

IPsec makes use of the AH and ESP protocols to provide security services:

1. AH (Authentication Header) protocol provides source authentication, and integrity of IP packets, but it does not have encryption. An AH header added to the IP packet contains a hash of the data, a sequence number etc., and information that can be used to verify the sender, ensure data integrity and prevent replay attacks.



2. ESP (Encapsulated Security Payload) protocol provides data confidentiality, in addition to source authentication and integrity. ESP uses symmetric encryption algorithms, such as 3DES, to provide data privacy. The algorithm needs to be the same on both communicating peers. ESP can also support encryption-only or authentication-only configurations. However, research in 2007 showed that any RFC-compliant implementations of IPsec that make use of encryption-only ESP can be broken[4].



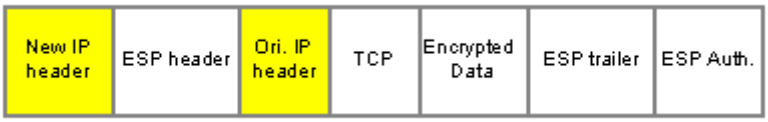
Modes of Operation

Each security protocol supports two modes of operation: a tunnel mode and a transport mode. Tunnel mode encrypts and/or authenticates the header and the data of each packet while transport mode only encrypts and/or authenticates the data itself.

[4] http://eprint.iacr.org/2007/125

1. Tunnel mode (end-to-end)

   Here the entire packet is protected. The original IP packet, with original destination address, is inserted into a new IP packet and the AH and ESP are applied to the new packet. The new IP header points to the end point of the tunnel. Upon receipt of the packet, the tunnel end point will decrypt the content and the original packet is further routed to its final destination in the target network.



2. Transport mode (host-to-host)

   Here the AH and ESP headers are applied to the data of the original IP packet. The mode encrypts and / or authenticates the data but not the IP header. The overhead added is less than that required in tunnel mode. However, the final destination and source addresses could be sniffed. Attackers can perform traffic analysis based on header information in this type of header. It is generally only used for host-to-host connections.

Key Exchange and Management

IPsec supports two types of key management over the Internet: automated and manual.

1. Automated Key Management

   IKE (Internet Key Exchange) is the default protocol used in IPsec to determine and negotiate protocols, algorithms and keys, and to authenticate

the two parties. It is useful for widespread, scalable deployments and implementations of VPN.

The IKEv2 protocol was released in 2005. It preserves most of the functionalities of IKEv1 protocol, but also supports the Network Address Translation (NAT) traversal and provides more flexibility.

IKE also supports the use of digital certificates. Users authenticate by first signing the data with their digital signature key. The other endpoint will then verify the signature. IKE creates an authenticated, secure tunnel between two entities, then negotiates a security association (SA) between the two entities, and exchanges key(s). SA is a set of parameters used by negotiating peers to define the services and mechanisms for protecting traffic. These parameters include algorithm identifiers, modes, keys, and so on. IKE also keeps track of the keys and updates them between communicating peers. IKE uses protocols like ISAKMP (The Internet Security Association and Key Management Protocol) and Oakley to define procedures for key generation, creation and management of SA and authentication.

There are several authentication methods that an IPsec VPN gateway works with IKE for remote user authentication[5], including hybrid authentication, eXtended authentication (Xauth), challenge/response authentication for cryptographic keys (CRACK), and digital certificates. This allows additional third-party authentication services to be used to strengthen the access control process.

2. Manual key management

   Secret keys and security associations are manually configured in both VPN communicating peers before a connection starts. Only the sender and recipient know the secret key for the security services at hand. If the authentication data is valid, the recipient knows that the communication

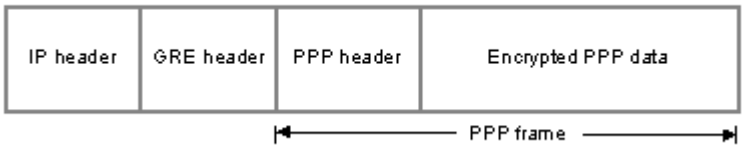
[5] http://www.networkworld.com/community/node/23073

came from the sender and it was not modified. This approach is easy to use in small, static environments, but it does not scale well. All keys should be distributed to communicating peers securely beforehand. If the keys are compromised, another person could pose as the user and make a connection into the VPN.

PPTP (POINT-TO-POINT TUNNELING PROTOCOL)

PPTP (Point-to-Point Tunnelling Protocol) is an OSI layer two protocols built on top of the PPP (Point-to-point protocol). PPP is a multi-protocol, dial-up protocol used to connect to the Internet. Remote users can access a private network via PPTP by first dialling into their local ISP. PPTP connects to the target network by creating a virtual network for each remote client. PPTP allows a PPP session, with non-TCP/IP protocols (e.g. IP, IPX or NetBEUI), to be tunnelled through an IP network. PPTP is documented in RFC 2637 as an informational draft.

The same authentication mechanism used for PPP connections is supported in a PPTP-based VPN connection. These include EAP (Extensible Authentication Protocol, MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol), CHAP, SPAP (Shiva Password Authentication Protocol), and PAP (Password Authentication Protocol). For encryption, PPP data can be optionally encrypted using MPPE (Microsoft Point-to-Point Encryption) which is based on the RSA RC4 (40/56/128 bit) standard for link encryption.



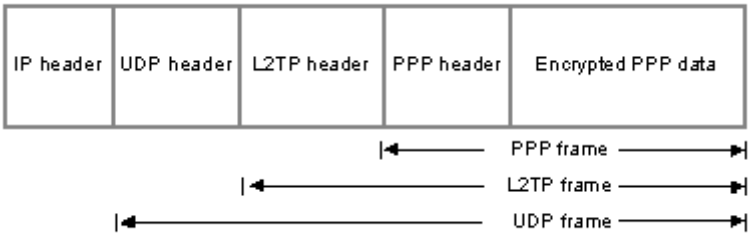
PPTP data tunnelling is accomplished through multiple levels of encapsulation. PPTP encapsulates PPP frames as tunnelled data for transmission over an IP network, such as

the Internet or a private intranet, using a modified version of GRE (Generic Routing Encapsulation). GRE provides a flow and congestion controlled encapsulated service for carrying PPP packets. The data in the encapsulated PPP frames can be encrypted (and/or compressed). The resulting GRE-and-PPP-encapsulated data is then encapsulated with an IP header containing the appropriate source and destination IP addresses for the PPTP client and PPTP server. Upon receipt of the PPTP tunnelled data, the PPTP server processes and removes the IP, GRE and PPP headers, then decrypts (and/or decompresses) the PPP data.

L2TP (LAYER 2 TUNNELING PROTOCOL)

L2TP (Layer 2 Tunnelling Protocol) is a combination of Microsoft PPTP (Point-to-Point Tunnelling Protocol) and Cisco L2F (Layer 2 Forwarding). L2TP can be used as a tunnelling protocol to encapsulate PPP (Point-to-Point Protocol) frames to be sent over IP, X.25, Frame Relay or ATM networks. Multiple connections are allowed through one tunnel. Like PPTP and L2F, L2TP operates on OSI layer two. Layer two VPN protocols encapsulate data in PPP frames and are capable of transmitting non-IP protocols over an IP network. L2TP is documented in RFC 3931 as standards track.

L2TP connections use the same authentication mechanisms as PPP connections, such as EAP, CHAP, MS-CHAP, PAP and SPAP. L2TP tunnelling is accomplished through multiple levels of encapsulation. The PPP data is encapsulated within a PPP header and an L2TP header. The L2TP encapsulated packet is further wrapped in a UDP header with the source and destination ports set to 1701. The final packet is encapsulated with an IP header containing the source and destination IP addresses of the VPN client and VPN server.



Due to the lack of confidentiality provided by L2TP, it is often used in conjunction with IPsec and referred to 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.

SSL / TLS[6]

SSL / TLS is a transport-layer protocol that use TCP port 443. SSL protocol is defined by the IETF and there are no versions of SSL beyond version 3.1. TLS 1.0 and TLS 1.1 are two standardised versions of TLS, and TLS 1.0 is the same as SSL 3.1.

There are a number of cryptographic features provided by SSL / TLS and these include confidentiality, integrity, and digital signatures. Unlike IPsec, in which the two communicating parties agree to cryptographic functions, SSL / TLS uses cipher suites to define the set of cryptographic functions for a client and server to use when communicating.

[6] http://csrc.nist.gov/publications/drafts/SP800-113/Draft-SP800-113.pdf

An SSL VPN gateway can authenticate itself to the Web user using a SSL server certificate signed by a trusted CA (Certification Authority), in order that the user can verify that he / she is talking to a trusted server via their browser. In practice, some SSL VPNs may use a self-signed digital certificate that is not normally trusted in most web browsers. In this case, the user might need to add the SSL VPN's server certificate to the user's own list of trusted certificates, or accept ‘yes’ to trust the certificate.

IV. RISKS & LIMITATIONS OF VPN

HACKING ATTACKS

A client machine may become a target of attack, or a staging point for an attack, from within the connecting network. An intruder could exploit bugs or mis-configuration in a client machine, or use other types of hacking tools to launch an attack. These can include VPN hijacking or man-in-the-middle attacks:

1. VPN hijacking is the unauthorised take-over of an established VPN connection from a remote client, and impersonating that client on the connecting network.
2. Man-in-the-middle attacks affect traffic being sent between communicating parties, and can include interception, insertion, deletion, and modification of messages, reflecting messages back at the sender, replaying old messages and redirecting messages.

USER AUTHENTICATION

By default VPN does not provide / enforce strong user authentication. A VPN connection should only be established by an authenticated user. If the authentication is not strong enough to restrict unauthorised access, an unauthorised party could access the connected network and its resources. Most VPN implementations provide limited authentication methods. For example, PAP, used in PPTP, transports both user name and password in

clear text. A third party could capture this information and use it to gain subsequent access to the network.

CLIENT SIDE RISKS

The VPN client machines of, say, home users may be connected to the Internet via a standard broadband connection while at the same time holding a VPN connection to a private network, using split tunnelling. This may pose a risk to the private network being connected to.

A client machine may also be shared with other parties who are not fully aware of the security implications. In addition, a laptop used by a mobile user may be connected to the Internet, a wireless LAN at a hotel, airport or on other foreign networks. However, the security protection in most of these public connection points is inadequate for VPN access. If the VPN client machine is compromised, either before or during the connection, this poses a risk to the connecting network.

VIRUS / MALWARE INFECTIONS

A connecting network can be compromised if the client side is infected with a virus. If a virus or spyware infects a client machine, there is chance that the password for the VPN connection might be leaked to an attacker. In the case of an intranet or extranet VPN connection, if one network is infected by a virus or worm, that virus / worm can be spread quickly to other networks if anti-virus protection systems are ineffective.

INCORRECT NETWORK ACCESS RIGHTS

Some client and/or connecting networks may have been granted more access rights than is actually needed.

INTEROPERABILITY

Interoperability is also a concern. For example, IPsec compliant software from two different vendors may not always be able to work together.

V. SECURITY CONSIDERATIONS

GENERAL VPN SECURITY CONSIDERATIONS

The following is general security advice for VPN deployment:

1. VPN connections can be strengthened by the use of firewalls.
2. An IDS / IPS (Intrusion Detection / Prevention System) is recommended in order to monitor attacks more effectively.
3. Anti-virus software should be installed on remote clients and network servers to prevent the spread of any virus / worm if either end is infected.
4. Unsecured or unmanaged systems with simple or no authentication should not be allowed to make VPN connections to the internal network.
5. Logging and auditing functions should be provided to record network connections, especially any unauthorised attempts at access. The log should be reviewed regularly.
6. Training should be given to network/security administrators and supporting staff, as well as to remote users, to ensure that they follow security best practices and policies during the implementation and ongoing use of the VPN.
7. Security policies and guidelines on the appropriate use of VPN and network support should be distributed to responsible parties to control and govern their use of the VPN.
8. Placing the VPN entry point in a Demilitarised Zone (DMZ) is recommended in order to protect the internal network.
9. It is advisable not to use split tunnelling to access the Internet or any other insecure network simultaneously during a VPN connection. If split tunnelling is

used, a firewall and IDS should be used to detect and prevent any potential attack coming from insecure networks.

10. Unnecessary access to internal networks should be restricted and controlled.

EXTRANET VPN SECURITY CONSIDERATIONS

The following are additional security considerations for extranet VPN deployment:

1. Strong user authentication mechanisms should be enforced.
2. The VPN entry point should be placed inside a DMZ to prevent partners from accessing the internal network.
3. Access rights should be granted on an as-needed basis. Only necessary resources should be available to external partners. Owners of these resources should review access permissions regularly.

CLIENT SIDE VPN SECURITY CONSIDERATIONS

The following are general security considerations for VPN users:

1. Strong authentication is required when users are connecting dynamically from disparate, untrusted networks, for example:
    a) By means of certificates and/or smart cards, or tokens:

    A smart card is used to store a user profile, encryption keys and algorithms. A PIN number is usually required to invoke the smart card. A token card provides a one-time password. When the user authenticates correctly on the token by entering the correct PIN number,

the card will display a one-time passcode that will allow access to the network.

b) By means of add-on authentication system, like TACACS+, RADIUS.

This kind of central authentication system contains a profile of all VPN users, controlling the access to the private network.

2. Personal firewalls should be installed and configured properly on client VPN machines to block unauthorised access to the client, ensuring it is safe from attack. Many of the more recent remote access VPN clients include personal firewalls. Some may also include other configuration checks, such as the client not being able to connect to the network if anti-virus software is not running, or if virus signatures are out of date.
3. The client machine should have anti-virus software installed, with up-to-date signatures, to detect and prevent virus infections.
4. The user should remain aware of the physical security of the machine, in particular when authentication information is stored on the machine.
5. All users should be educated on good Internet security practices. Access from home should be considered an insecure channel, as traffic is routed over the Internet.

COMMON SECURITY FEATURES IN VPN PRODUCTS

The following are security features to look for when choosing a VPN product:

1. Support for strong authentication, e.g. TACACS+, RADIUS, smart cards / tokens.
2. Industry-proven strong encryption algorithms, with long key strength support to protect data confidentiality during transmission.

3. Support for anti-virus software, and intrusion detection / prevention features.
4. Strong default security for all administration / maintenance ports.
5. Digital certificate support, such as using certificates for site to site authentication
6. Address management support, such as the capability to assign a client address on the private network and ensuring all addresses are kept private.

VI. CONCLUSION

VPN provides a means of accessing a secure, private, internal network over insecure public networks such as the Internet. A number of VPN technologies have been outlined, among which IPsec and SSL VPN are the most common. Although a secure communication channel can be opened and tunneled through an insecure network via VPN, client side security should not be overlooked.