VPN
in the spotlight of IT- Security

Michael Seifert – michael.seifert@stud.tu-ilmenau.de

Manuel Löffelholz – manuel.loeffelholz@stud.tu-ilmenau.de

22.01.2006

Praxiswerstatt IT- Security- Tools
Prof. Dr. Grimm, WS 2005/06
Uni Koblenz / TU Ilmenau

Contents List

1. Basic description of the domain.....3
2. Threats and resulting protection targets 6
3. Explanation of the protection mechanism 7
4. System Analysis 10
5. Summary and Conclusion 12
6. Ressources .....**Fehler! Textmarke nicht definiert.**

1. Basic description of the domain

In today's world in what is known as the information age, where everyone is sending data through a computer based network like the World Wide Web and hacker attacks are trained as a sport, the ability to protect sensible data is necessary.
The World Wide Web is an open, unsecured Network. That means unencrypted data can be read along by nearly every one.
VPN means Virtual Private Network and is used to make your data transfer more secure. A virtual private network is a computer- based network to transport private data through a public network like the Internet. (cp. Wikipedia1 2006) VPN uses the tunnelling technology which provides end to end, end to side and side to side connections.
In general use you have a secured tunnel but also an unsecured tunnel is a virtual private network. (cp. Wikipedia1 2006)
At first we like to give you a short historical overview we have to start with the company BBN Technologies. The name BBN stands for the names of the three founders: Bolt, Beranek and Newman. This company built up the first secure connection to exchange data using an unsecured network. This was in 1973 when BBN developed the Private Line Interface (PLI) to encrypt messages over the ARPANET. This was a demonstration of the first secure traffic sent over a packet switch network. (cp. BBN 2006)
The first effort to develop a standard for secure networking was the IP Security Protocol (IPsec). The first version of this protocol was developed in 1995.
At the same time the Secure Socket Layer was developed by Netscape to build up a secure connection between server and client. The Secure Socket Layer is based on Layer 5/6 of the OSI- reference model which you can find below.

OSI-Schichtenmodell
(ISO 7498: Open Systems Interconnection)

	Schicht	engl. Layer	
7	Verarbeitung (Anwendung)	Application	Anwendungs-system
6	Darstellung	Presentation	
5	Kommunikations-steuerung	Session	
4	Transport	Transport	Transport-system
3	Vermittlung (Netzwerk)	Network	
2	Sicherung (Leitungssteuerung)	Data Link	
1	Bitübertragung	Physical	

(cp. Wikipedia2 2006)

Secure VPNs use cryptographic tunneling protocols to provide the necessary confidentiality (preventing snooping), sender authentication (preventing identity spoofing), and message integrity (preventing message alteration) to achieve the privacy intended. If properly chosen, implemented, and used, such techniques can provide secure communications over unsecured networks. There are different types of virtual private networks based on different protocols.

The Layer 2 VPNs, which use the point to point tunnelling protocol (PPTP) are point to point methods and establish connectivity between the two sides over a virtual connection. One advantage of layer 2 VPNs is the independence of the layer 3 traffic payload. So a layer 2 VPN can carry many different types of layer 3 traffic such as IP, IPX, AppleTalk, IP Multicast and so on.(Glaser website3 2006)

Layer 3 VPNs which are based on the IP security Protocol (IPsec) also provide a connection between the sides. The delivery header is at layer 3 of the OSI-

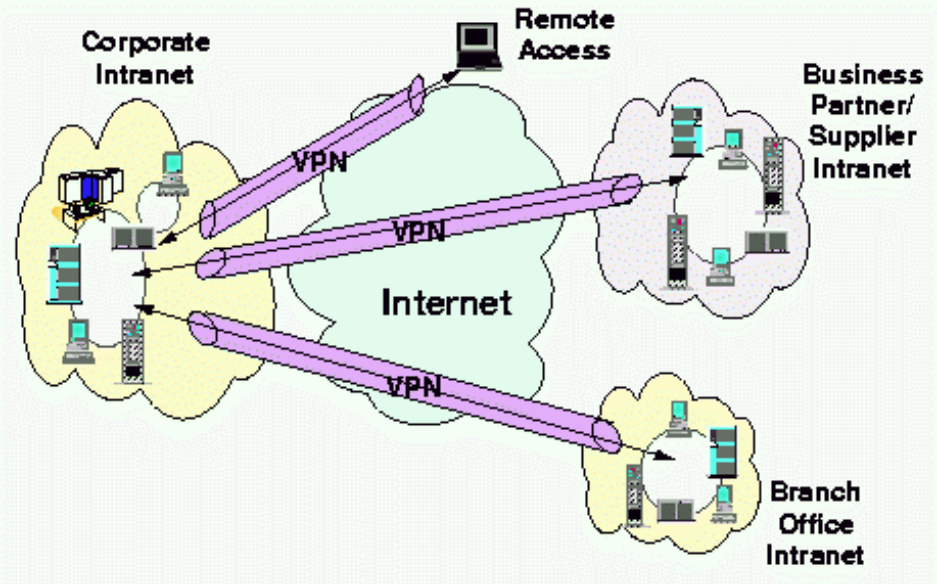
Reference model. Till nowadays IPsec provides only the encryption of IP packets, and does not provide multicasts. (Glaser website3 2006)

Layer 5/6 VPNs (SSL VPN) use the application- Layer 5/6. SSL was developed to authenticate the server and exchange sensible data over an encrypted channel, for example in the use of home- banking.
Today SSL / TSL are used to build up a VPN- tunnel.
Here you have to differentiate between two application areas:

- Web based application → the end of the tunnel is the Web server
- Java / ActiveX based application → applet emulates the VPN Client

(Glaser website2 2006)

VPNs are in use by many companies to reduce costs by communicating over a public network. The following graphic shows some applications in practise.

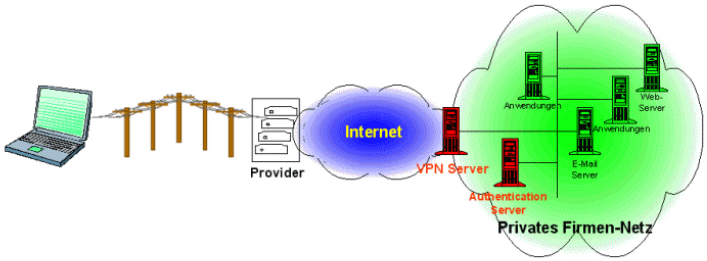


(Boros 2006)

VPN is used to build up a connection between a remote computer and a company intranet. Also Business Partners and other Intranets can get access over a VPN to the corporate intranet. This graphic shows that you can connect single computers with entire networks.

In the next animated GIF- File you can see in general how a single computer is building up a connection to a single computer in the company's intranet.

Click on the graphic to follow the link and see the animated gif.



(Glaser website1 2006)

2. *Threats and resulting protection targets*

Basic threats of unsecured networks and the protection targets which can be achieved by a virtual private network are following in this task.

The first threat by sending data through the World Wide Web is that some unauthorised people can read or copy that information. Therefore means the target is to protect information from being read or copied by anyone who hasn't been authorised by the owner. The protection target which is described here is called **confidentially.** A virtual private network can achieve this target with encryption of the connection and the encryption of the data.

Another threat is the erasure or alteration of information. The protection of data being deleted or altered in any way without the permission of the owner is identified as **data integrity.** If you permit access to a network or a folder on your machine the data integrity is highly in danger. When the usage of a virtual private network is given, the data integrity can be protected because of the constricted access which is allowed for the authorised clients only.

A very hazardous point is when someone pretends to be somebody else. If you want to prevent this, you have to realise authorisation by authentication. **Authentication** is the process of proving that a subject is what the subject assures to be. A VPN provides server and client authentication so that the server and clients can trust each other.

Another thing is that an unknown, unauthorised user has access to your network or system. A restriction for that ability is named in the target **access control**. This means that only authorised users can get access to the data.
By the use of authentication the VPN- server has the ability to accept or to deny the client.

3. Explanation of the protection mechanism

Why is a secure connection between A and B through the internet needed? A survey of 250 large corporations has shown that there is a great danger of losing information. And this information is worth much money.
48% of these corporations have suffered computer break-ins over the last 12 months.
24% reported break-in attempts via the Internet.
66% lost more than $50,000 worth of information
18% lost more than $1,000,000 worth of information
So the today's economy has to handle this challenge. One possibility to prevent unauthorised access on critical information is to use a VPN.

With the help of VPN a smaller net is build up in a bigger net (e.g. the internet). Only the persons who know the right addresses and code words are able to communicate through this secure channel.
Using IPsec is one possibility to establish a VPN. Furthermore there are some others, but IPsec is widely used, because it features many advantages.
IPsec stands for Internet Protocol Security. It was build by the IETF (Internet Engineering Task Force), which is an open organisation recruited by volunteers. These people make proposals for the standardisation of the internet.
IPsec features the security aims **confidentiality**, **authenticity** and **integrity**.
IPsec is a complex modification to the IP stack itself.
IPsec examines packets coming out of an IP interface, determines if a security association exist with the destination, and then tries to automatically encrypt packets at one end and decrypt them at the other.
Authenticity is provided by the user and packet authentication. The sender and its messages are authenticated by the Authentication header (AH).
Integrity is guaranteed by the data encryption via ESP (Encapsulation Security Payload). So the protection of the data is given by the encoding process.
Confidentiality is being given by the management of keys, the Internet Key Exchange (IKE)

Procedure of an IPsec- connection

Before two stations can exchange data via IPsec, several steps have to be executed. At first the security service has to be defined. The two stations have to agree, if encryption, authentication and integrity, or all three of them will be used. After this, the stations have to set the exact algorithm, for example DES (Data Encryption Standard) for encryption or MD5 (Message Digest Algorithm 5) to prove the integrity.
In the next step the keys for the session have to be exchanged. For secure communication IPsec uses the Security Association (SA). A SA describes the relationship between 2 or more stations and how these stations use security services to communicate. The Security Associations are clearly labelled by the Security Parameter Index (SPI). The SPI consists of a random number and the target address. That is why between two stations are 2 SPIs, one for the

communication from A to B and one for the communication in the other direction.
If a station wants to transfer data securely, it checks the Security Association which was arranged with the other. Then it uses the specified procedure on the data package. After this, the sender station writes the Security Parameter Index into the packet- header and dispatches it to the destination address.

Key- management in IPsec

IPsec uses existing Security Associations, but does not feature mechanisms to create them. For this task IPsec refer to the IKE (Internet Key Exchange). To create the Security Association both stations have authenticate themselves. The Internet Key Exchange uses mainly these methods for the communication between the stations.

Pre-shared keys: A key is installed on both machines. IKE builds a hash- value based on the key and sends it to the destination station. If both can build up the same hash they obviously have the same keys. As a result they are authenticated.

Public keys: Each side creates a random number and encrypt it with the public key, which everybody can see, of the other side. If the other side is able to decrypt it with its own private key and sends it back, it is also authenticated.

Digital signature: With this method every side is signing a date package and sends it to the destination station. Today RSA and Digital Signature Standard (DSS) are supported.
To secure this data exchange, both sides have to agree on a common key for the session. This session key is generated by the Diffie Hellmann protocol.

For encryption IPsec uses the ESP (Encapsulation Security Payload) and supports nearly all encryption algorithms.
IPsec can use 2 operation modes, the transport mode or the tunnel mode.

In the transport mode only the data part, the payload, of the IP package is encrypted. All the other parts of the message (IP header) are not changed. Only the ESP header is prefixed before the data. The transport mode is used for the assignment of critical information, like passwords.
In the tunnel mode the complete IP package, with the original data and the IP-header, is encrypted before the transmission. A new IP header, with the information of the destination gateway, is prefixed. In this case a transparent connection between two business- networks via the internet can be established. Alternatively a single machine (e.g. a notebook) could build up a secure connection over a public network to its business network. Both ways establish a Virtual Private Network. As a result the new data package look like this:
[IP-header *(new)*] - [ESP-header] - [IP header *(original)*] - [data] - [ESP-trailer]
The IP header (original) and the data are encrypted via ESP. The new IP header contains the information about the destination gateway.

4. System Analysis

If you want to establish a VPN connection between two machines with Windows as operating system, the server need to have Win NT / 2000 / XP as operating system. The other machine, the client, could have Windows 9x / ME or another Windows based operating system. The VPN server should have a static IP. Certainly both machines should have a connection to the internet or should be aligned over a LAN to build up a VPN connection between them. Because of the encryption of the data packets the delay of the package is even longer.

A VPN have to protect against passive and active attacks. A passive attack happens if someone tries to read the content of the packages you are sending. In this case the data is not changed. First you do not get any disadvantages. The passive attacker only knows what you have bandied over the VPN. But if you have exchanged sensitive data, the damage could be very fatal, because this

information may be worth much money. To defeat these passive attackers a VPN can encrypt the data packets. This encryption provides the security of the content of a package.
The more challenging threat of data exchange is an active attacker. Such an attacker has the ability to intrude into the communication channel. So the packets between both parties could be modified, deleted or replaced. In this case the whole data stream is corrupted and the destination gateway is getting wrong information.
VPN security is not all about encryption, the larger and more difficult problem to solve is the problem of authentication, to disable active attacks.
Authentication in the VPN context involves “signing” every packet with a secure hash, so that the recipient can prove that it is originated from a legitimate source. If an active attacker was able to modify a data package the recipient can identify a corrupted package and refuse the receiving. Both, openVPN and IPsec use the HMAC construction to authenticate packets.
HMAC is based on a cryptographic Hash- value. If an attacker wants to modify packages, such Hash- values have to be broken to crack the HMAC.
Other risks are replay attacks. The solution of problem is to embed a unique ID or timestamp in every packet before it is signed. The receiver needs to keep track of this timestamp, and make sure that it never accepts a packet with the same timestamp twice. Both openVPN and IPsec implement replay protection using the Sliding Window Algorithm.
To secure the data exchange against all possible threats all protection mechanisms have to be combined. Encryption must be combined with authentication (HMAC) and replay protection, to protect against all kinds of attacks.

There are some circumstances when VPN is not the best alternative. These are mission critical situation when you need to have a guaranteed bandwidth all day long. This can not be achieved presently by an IP connection but can be achieved using leased lines. As you can see a VPN does not solve all your communication problems but is a step in the right direction. The alternatives for a VPN solution consists of a frame relay, ATM (Asynchronous Transfer Mode) or a leased line. In many instances, these options fall short for an

offering to the corporation. The transport of data across a frame relay or ATM line will be required traverse public networks without any security. This is usually not an option. However, to minimize the danger of data being observed by the public, a company would have to lease a line from a data carrier. In many cases, the cost of a leased line is prohibitive. By utilizing VPNs, companies can have access to the public network benefits of frame relay and ATM and can also have some degree of security similar to that of a private line. As expected, this option which falls in between the two extremes in functionality also falls between them in price.

5. Summary and Conclusion

At last we have to say that the use of a VPN is sensitive, if you have an appliance field which has to execute the targets of confidentiality, data integrity, user authentication and user access control. It takes a lot of time and "know how" to install and maintenance a virtual private network.
Overall a VPN reaches the aimed protection targets and shows that location-independent work is no longer a future dream.
There are manifold applications of a VPN, to connect field managers with the company's network, the connection of two PCs or networks. There are various uses for VPNs.
With the help of a VPN the data exchange could be secured. You are saving a large amount of money if you want to connect machines, or networks which are placed far away from each other. All in all it is relatively cheap and easy to establish a Virtual Private Network.

6. Resources

BBN website: in the internet at: http://www.bbn.com//About_BBN/Timeline/Timeline_1970s.html (21.01.06)

Wikipedia1 in the internet at: http://de.wikipedia.org/wiki/VPN (21.01.06)

Wikipedia2 in the internet at: http://de.wikipedia.org/wiki/OSI-Modell (21.01.06)

Wikipedia3 in the internet at: http://de.wikipedia.org/wiki/IETF (21.01.06)

Wikipedia4 in the internet at: http://de.wikipedia.org/wiki/HMAC (21.01.06)

Glaser, Gerhard Markus website1 in the internet at: http://www.tcp-ip-info.de/tcp_ip_und_internet/vpn.htm (22.01.06)

Glaser, Gerhard Markus website2 in the internet at: http://www.tcp-ip-info.de/security/ssl.htm (22.01.06)

Glaser, Gerhard Markus website3 in the internet at: http://www.tcp-ip-info.de/tcp_ip_und_internet/tunneling_protokolle.htm (22.01.06)

Boros, Dragos; Crowe, Art; Habinc, Rok; Meeker, Sherwin: VPN article: in the internet at: http://www.emory.edu/BUSINESS/et/P98/vpn/ (22.01.06)