CISC 611 – Network Operating Systems

Virtual Private Networks for Network Layer Security

Bhavneet Soni

Virtual Private Networks for Network Layer Security

When we are communicating over the internet any one who has access to the physical medium i.e the cables, routers, switches, bridges etc can tap into our communications and temper or steal the data. When one user communicates with another user, the data is transported from Application layer to Transport Layer to Network layer to Physcial layer. Some of the possible security issues for the open communicaiton are

- Source spoofing
- Replay packets
- Data integrity
- Data confidentioanlity

Many of these protocols were designed keeping in mind that they physcial devices or the networks were trustworthy and did not take into account any malfecience in mind. So all these protocols IP, TCP, UDP, HTTP, SMTP etc were buit with no inherent security mechanisms. Figure 1 below shows a typical technology stack and how the information flows from point A to point B. Comminication can be venurable to hacking on any of the dfferent interfaces in the system.

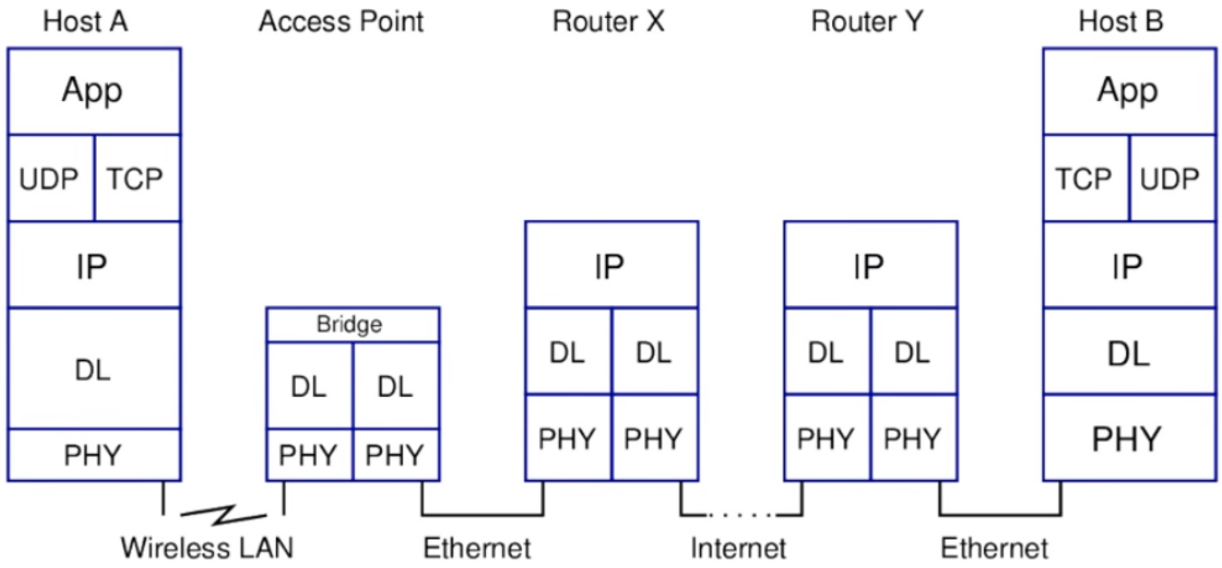

Figure 1 Typical Network Stack (Gordon, 2014)

As the networks size grew and the tansfer of sensitive data over the internet gained notority various extensions were developed to add security to the existing protocols. These extensions were developed for different layers consisting of different components that are responsible to maintian the integrity and flow of the data thru that layer. Communicaitons can be secured on

1. Application Level Security – Security is implemented at the application level i.e the security mechanism is built into the application. These are end to end securty system where by the data is encrpted at the starting point and decrypted at the end point. Data is protected all the way. However to have an application level security the developer has to design the security (encryption and decryption) mecahnism and will have to take into account the various computer archietectures (client, server, mobile etc) and computer operating systems into account. It makes it very difficult from developers point of view.

2. Transport Level Security (TLS /Secure Socket Layer SSL) system is also a type of end to end encryption but instead of the application level its host to host. When implementing a TLS security the application developer do not need to provide their own encryption mechanism but will tapinto an security API provided by the Operating system, and the OS will send the data across the network. Application tells the OS to send the data out and the OS will implement the requested security on it. TLS is widely suppored by OS but oinly will work with TCP and does not support UDP. TLS for UDP are very rare and not available for all OS. Some of the examples of TLS is HTTPS, IMAPS, FTPS, SMTPS, trailing (S) stands for secured.
3. Network Level Security - IPSec is implemented at the IP layer. The data passed from the application on to the OS and when the data is prepared into IP datagram, IPSec will encrypt the data and will send it onwards, receiving host IPSec layer will read the encrypted data and serve up the decrypted data to its TCP → Application layer. it is yet a type of end to end encryption. This type of encryption works for all and any application or transport protocols. OS governs this type of security being implemented. This is not widely used as it requires tedious IPSec configurations and not usual for day to day users. This is the best security system for implementing tunneling, which is the basis for the VPN. Tunneling is putting IP data packet within another IP data packet.

VPN is utilized to provide secured data links over the internet but sill securing a connection between two nodes, these nodes could be

a) Client to Firewall – Connecting to your office network from your home or while traveling. It is a type of remote VPN where a vpn client on the user machine connects with a server on the secured network.

b) Router to Router – site to site VPN

c) Firewall to Firewall – Connections between two remote offices also known as site to site

Network level security (IPSec) each data packet is encrypted and tranported. IPsec provide benefits of confidnetiality because of the encryption algorithms, it also provides data integrity assurance by the means of providing checksum or hash value of the data. Data modificaiton can be detected by signature verificaiton. IPsec also provides for Authethication by the means of Signatures and cerificates. Mostly preshared keys or digital certificates are used for autheticaiton process. Data signed by the sender and signature is verified by the reciever. IPSec provides for all this while maintaining the ability to route through existing IP networks.

IPSec also provies for Anti-replay protection such as a man in the middle attack, an entity which can listen to all the data packets for communication and can capture some packets and send after modifiying the data packet. To check against such attacks IPsec is very helpful. Its done by checking the sequence number. SSL-based VPN is remote access only and IPsec-is point to point based VPN.

It mainly follows two modes Figure 2 gives a brief overview of the key differences between them

1. Transport Mode – In this mode only the message with in the datapaket is encrypted. Mostly used for remote-access VPNs. Only IPsec header is inerted into the IP packet and no new packet is created so no not much overhead is involved.

2. Tunneling Mode - In tunneling mode the whole datapaket is encrypted. Tunneling is most widely used for encryption and setting up VPN networks. IPSec can be established between two hosts, or from one host to another internal network router or even between two routers. Advantage of doing so is that you do not need to establish it on each host and hence its very effective way to secure the entry points to the otherwise sterile netwok setup. It can be achieved at multiple levels, tunneling at Application layers like SSH at Network layer such as IP-in-IP or IP-in-IPsec and at Data Link lyaer such as PPTP and L2TP.

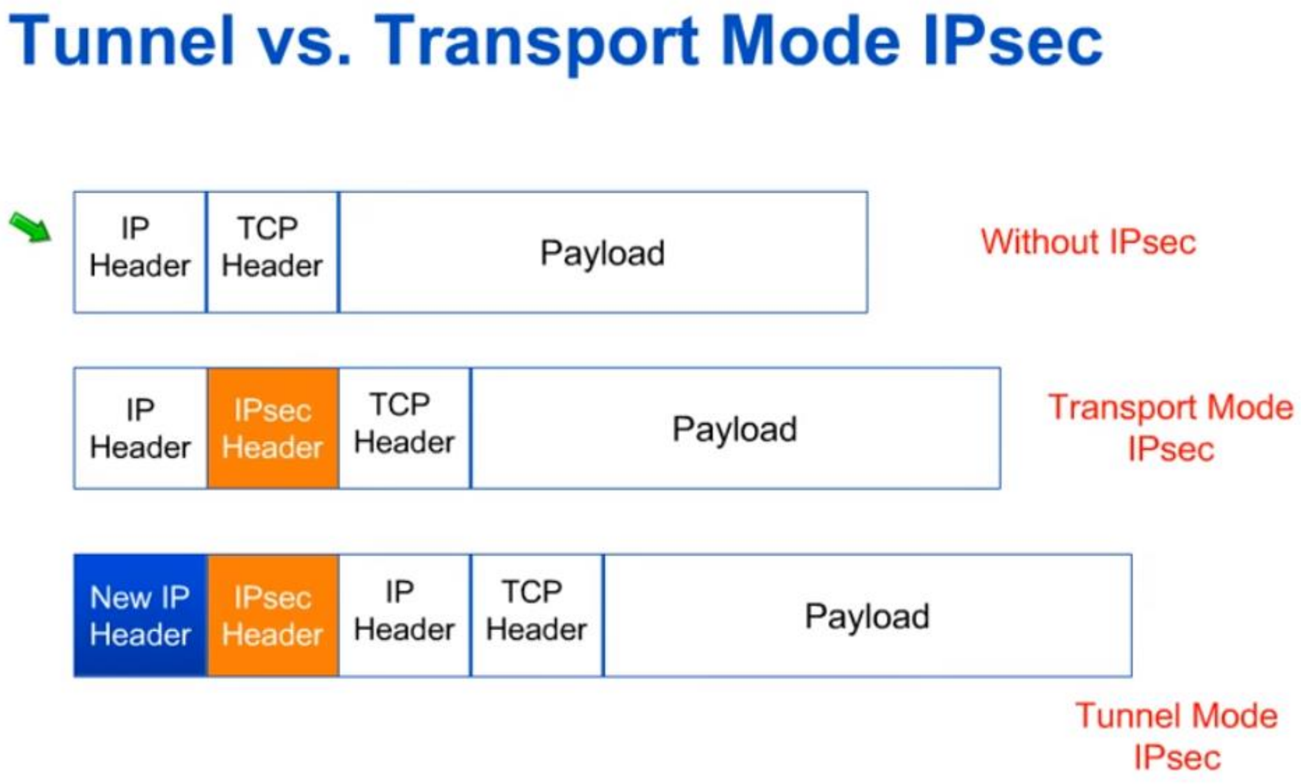

Figure 2 Transport vs Tunnel Mode

VPN protocol use a tunneling protocol and security protocol, we will discuss how the tunneling works. VPN Tunneling consists of two main steps

1. Encapsulation – The data is packed into a packet that will have destination information for the VPN server, all the data is routed to the VPN server and then VPN routes it to the end point.
2. Encryption – The data sent over the network is encrypted so that it can not be read by un authorized entity. Security association (SA) are created between the two end points to secure the session. SA are a collection of parameters required to manage security, these are uniquely identified by Security Parameter Index (SPI), IP destination address and Security Protocol being used Autheticaiton headers (AH) or ESP

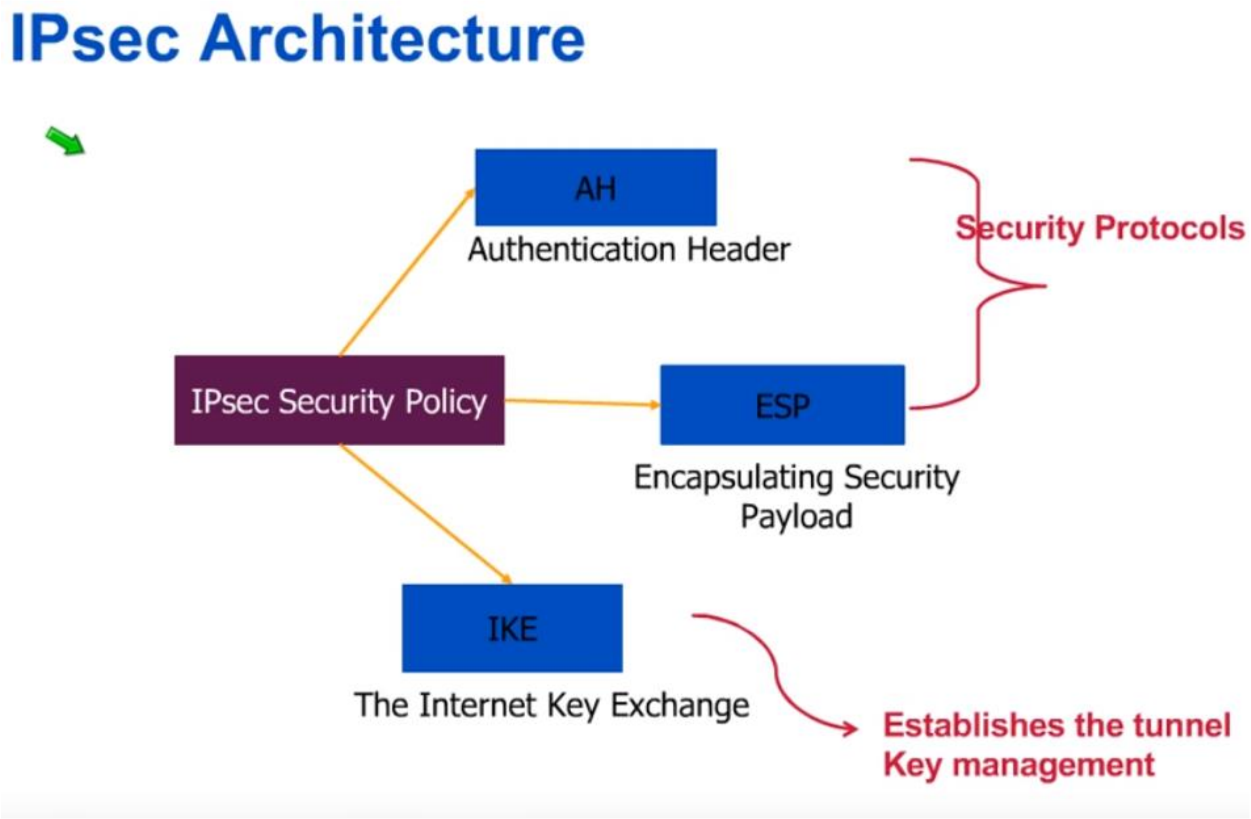

Figure 3 IPsec Architecture

Authentical headers provides source authetication and data integrity but do not provide data confedentiality. Where as ESP provides us with all the desired aspects for a secured communication.

There are various VPN Tunneling protocols that are available and are discuss below

1. PPTP – Point to Point Tunneling Protocol - its one of the oldest protocol it encapsulates PPP frames in to IP datagrams and these datagrams are wrapped with Microsft Point to Point Encryption (MPPE). It was first introduced in Windows 95 and is quite old and outdate for any meaning modern day info security. It uses TCP Port 1723 and GRE Protocol 47. It does not provide data integrity i.e proof that the data was not tempered with over the transit, also this system lacks the data origin authetication i.e proof that the only the authorized user is sending the data. Most modern day OS like iOS have stopped supporting this type of tunneling. It is venurable to disctionary and bit flipping attacks.
2. L2TP – Layer 2 Tunneling Protocol – There is double encapsulation in this type of tunneling hence the 2 layers. PPP frame is wrapped in IP datagram then this is again wrapped with the IPsec Encapsulated security payload (ESP). Data in encrypted using IPsec encryption algorithms. It uses UDP Port 500 and 4500 with ESP protcol 50, UDP 500 port is used for initial key exchange, UDP 1701 for iniital configuration setup and UDP 4500 for NAT traversal. It can support older clients and can use certificates or preshared key for IPsec. L2TP can support 3DES and AES encryption algorithms , its considered more secure when using AES but not as much when using a preshared key. Layer two tunneling (L2TP) for IOS is very

secured but bit slower due to 256 bit encrypotion. It implements fixed ports and protocols which makes it inflexible for use.

3. IKEv2 – Interenet key Exchange version 2 – It is one of the most recent type of tunneling mechanism available. Developed jointly by CISCO and Microsft. It utilises the IPsec and ESP for encapsulation of data packets and IPsec encryption algorithm for encrypting and securing the data. Since there is only one leve of encapsulation its much faster then L2TP. As L2TP it also works on UDP Port 500 and 4500 with ESP protocol 50. All the newer VPN clients support this type of tunneling protocols, however it faces some challenges when connecting to hosts behind a NAT. If there is disruption of connectivity or switching of networks, it will automatically reconnect and handles is with ease. For this reason its best suited for mobile devices.
4. SSTP – Secure Socket Tunneling Protocol – It was first introduced in windows vista, SSTP encapsulates PPP frames in IP datagrams going over port 443. It uses the SSL channel of the HTTPS protocol to encrypt and secure the data. Due to its utilization of port 443 its always available even behind firewalls, however its not supported by OS other then Microsoft as it was developed and owned by Microsoft. It works well with NAT.

L2TP and IKEv2 tunneling can cause issues with NAT because of the ESP protcols as its designed to work behind a firewall. These use UDP port 4500 for NAT traversal. These protocols are easily blocked by firewalls so they have to employ port forwarding to bypass firewalls. It becomes important for the VPN client to manage it properly.

However ESP protected links are susseptible to IP sniffing attack as the IP headers are not coverd by the ESP and are open to attack.

What are replay attacks and how is sliding widows Describe the mechanisms employed by the sliding window to defeat replay attacks. Session tokens are deployed to thwart these attacks

IKE SA is a bidirectional process i.e key is exhanged so the both ends agree where as IPsec has two SA (Security Association) certificates one   by specifying their purposes and the method of computation.

References

(n.d.). Retrieved from Coursera.org: https://www.coursera.org/learn/network-protocols-architecture/

(n.d.). Retrieved from www.techopedia.com: https://www.techopedia.com/definition/6006/application-layer

Coulouris, G., Dollimore, J., Kindberg, T., & Blair, G. (n.d.). *DISTRIBUTED SYSTEMS Concepts and Design.* Addison Wesley.

Gordon, S. (2014, Feburary 27). Lecture 25 of ITS335 IT Security. Bangkadi, Pathumthani, Thailand .