Unit – 06: Network Security

- Internet security protocols, SSL, TLS TSP WAP security,
- SET Hashing Authentication & Signature Schemes
- E-mail security, Email architecture SSL, PGP, MIME, S/MIME
- Internet Protocol Security (IP Sec) IP Sec architecture, IP Sec verses other layers security Mobile IP Sec, VPN, Web security SSL, TLS, SET etc.

Questions to be discussed:

1. What do you mean by network security? What are the benefits of network security?
2. What are network security protocol? Discuss any two network security protocol.
3. Discuss about email security. Also explain email architecture.
4. Differentiate between PGP and S/MIME.
5. What is IP Security? Define its architecture in brief.
6. Define Virtual Private Network in brief.

What is Network Security?

- It is the process of securing data or information on the network from various attacks.
- This aims at securing the confidentiality and accessibility of the data and network.
- It protects your network and data from breaches, intrusions and other threats.
- Network security also helps you to protect proprietary information from attack.
- Ultimately it protects your reputation.

Benefits of Network Security:

- Network Security has several benefits, some of which are mentioned below:
  1. It helps in protecting clients' information and data which ensures reliable access and helps in protecting the data from cyber threats.
  2. It protects the organization from heavy losses that may have occurred from data loss or any security incident.
  3. It overall protects the reputation of the organization as it protects the data and confidential items.

What are Network Security Protocols?

- Network security protocols are network protocols that ensure the integrity and security of data transmitted across network connections.
- The specific network security protocol used depends on the type of protected data & network connection.
- Various security mechanisms exist for specialized internet services like email, electronic commerce, payment, wireless internet, etc.
- To provide security to the internet, various protocols like:
  1. SSL (Secure Socket Layer),
  2. TLS (Transport Layer Security),
  3. TSP (Tunnel Setup Protocol)
  4. WAP (Wireless Application Protocol) etc.

SSL:

- SSL stands for secure socket layer.
- It provides security to the data that is transferred between web browser and server.
- SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.
- SSL Record provides two services to SSL connection:
  1. Confidentiality
  2. Message Integrity

TLS:

- TLS stands for Transport Layer Security.
- TLS are designed to provide security at the transport layer.
- TLS was derived from a security protocol called Secure Socket Layer (SSL).
- TLS ensures that no third party may eavesdrop or tampers with any message.
- It is an IETF standard protocol that provides authentication, privacy and data integrity between two communicating computer applications.
- IETF stands for Internet Engineering Task Force.

TSP:

- TSP stands for Time Stamp Protocol.
- The TSP is a cryptographic protocol for certifying timestamps using X. 509 certificates and public key.
- The TSP is the signer's assertion that a piece of electronic data existed at or before a particular time.
- The protocol is defined in RFC 3161.

WAP Security:

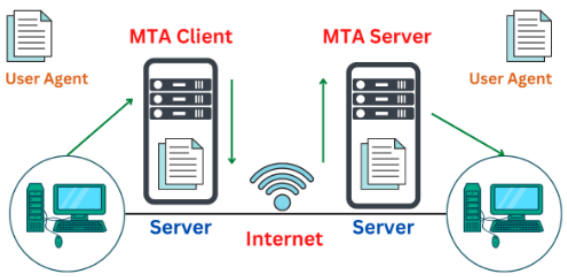
- WAP stands for Wireless Application Protocol.
- It is a protocol that is introduced in 1999.
- It offers Internet communications over wireless devices, such as mobile phones.
- It offers a way of creating web applications for mobile devices, and it is designed for micro-browsers.

Email security:

- It is the practice of protecting email accounts and communications from unauthorized access or loss.
- Email security refers to the steps where we protect the email messages and the information.
- It involves ensuring the confidentiality, integrity, and availability of email messages.
- Organizations can enhance their email security using tools to protect against malicious threats such as malware, spam, and phishing attacks.

What is email architecture?

- It is the structure and design of an email system.
- It includes the protocols, servers, and clients involved in the transmission and reception of emails.
- Email architecture consists of three components:
  - User Agent (UA)
  - Message Transfer Agent (MTA)
  - Message Access Agent (MAA)



PGP:

- PGP stands for Pretty Good Privacy.
- PGP is an open source software package that is designed for the purpose of email security.
- Phil Zimmerman developed it.
- It provides the basic or fundamental needs of cryptography.

S/MIME:

- S/MIME stands for Secure/Multipurpose Internet Mail Extension.
- S/MIME is a security-enhanced version of Multipurpose Internet Mail Extension (MIME).
- In this, public key cryptography is used for digital sign, encrypt or decrypt the email.
- User acquires a public-private key pair with a trusted authority and then makes appropriate use of those keys with email applications.

Difference between PGP and S/MIME:

PGP	S/MIME
PGP stands for Pretty Good Privacy.	Secure/Multipurpose Internet Mail Extension.
It is designed for processing the plain texts.	While it is designed to process email as well as many multimedia files.
PGP is less costly as compared to S/MIME.	While S/MIME is comparatively expensive.
PGP is good for personal as well as office use.	While it is good for industrial use.
PGP is less efficient than S/MIME.	While it is more efficient than PGP.

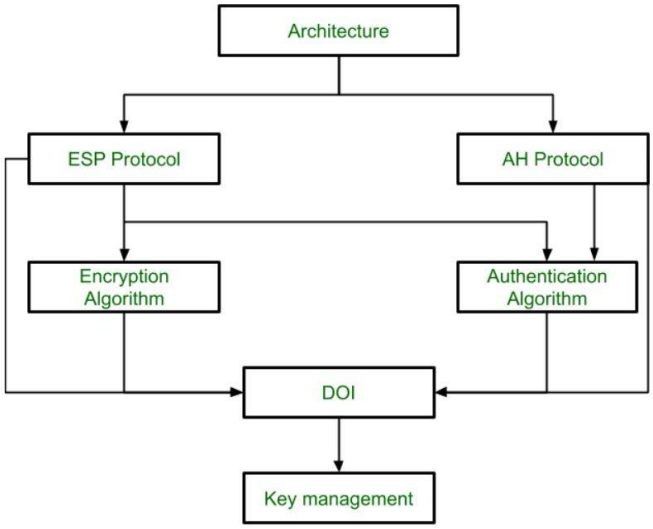
IP security (IPSec):

- IP Sec stands for Internet Protocol Security.
- It is a standard suite of protocols between two communication points across the IP network.
- It provides data authentication, integrity, and confidentiality.
- It also defines the encrypted, decrypted, and authenticated packets.
- The protocols needed for secure key exchange and key management are defined in it.

IP Security Architecture:

- IP Security architecture uses two protocols to secure the traffic or data flow.
- These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header).

- IPSec Architecture includes protocols, algorithms, DOI, and Key Management.
- All these components are very important in order to provide the three main services:
  1. Confidentiality
  2. Authenticity
  3. Integrity



Types of Network Security Protections:

- There are multiple components working together to ensure the security of data and networks.
- Based on this, there are several different types of network security:
  1. Firewalls
  2. Access control
  3. Virtual private networks (VPNs) etc.

Virtual Private Networks (VPNs)

- VPN stands for "Virtual Private Network".
- It describes the opportunity to establish a protected network connection when using public networks.
- VPNs encrypt your internet traffic and disguise your online identity.
- This makes it more difficult for third parties to track your activities online and steal data.
- The encryption takes place in real time**.**

Web Security:

- Web security refers to protecting networks and computer systems from damage to or the theft of software, hardware, or data.
- It includes protecting computer systems from misdirecting or disrupting the services they are designed to provide.