SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

COURSE NAME : 19EC625 – CYBER FORENSIC AND DATA SECURITY

III YEAR / VI SEMESTER

Unit I- NETWORK LAYER SECURITY &TRANSPORT LAYER SECURITY

Topic : IPSec

What is IPSec

- IP Security (IPSec) refers to a collection of communication rules or protocols used to establish secure network connections.
- Internet Protocol (IP) is the common standard that controls how data is transmitted across the internet.
- IPSec enhances the protocol security by introducing **encryption** and **authentication**. IPSec encrypts data at the source and then decrypts it at the destination.
- It also verifies the source of the data

Importance of IPSec

•IPSec protects the data through Data Encryption.

•IPSec provides Data Integrity.

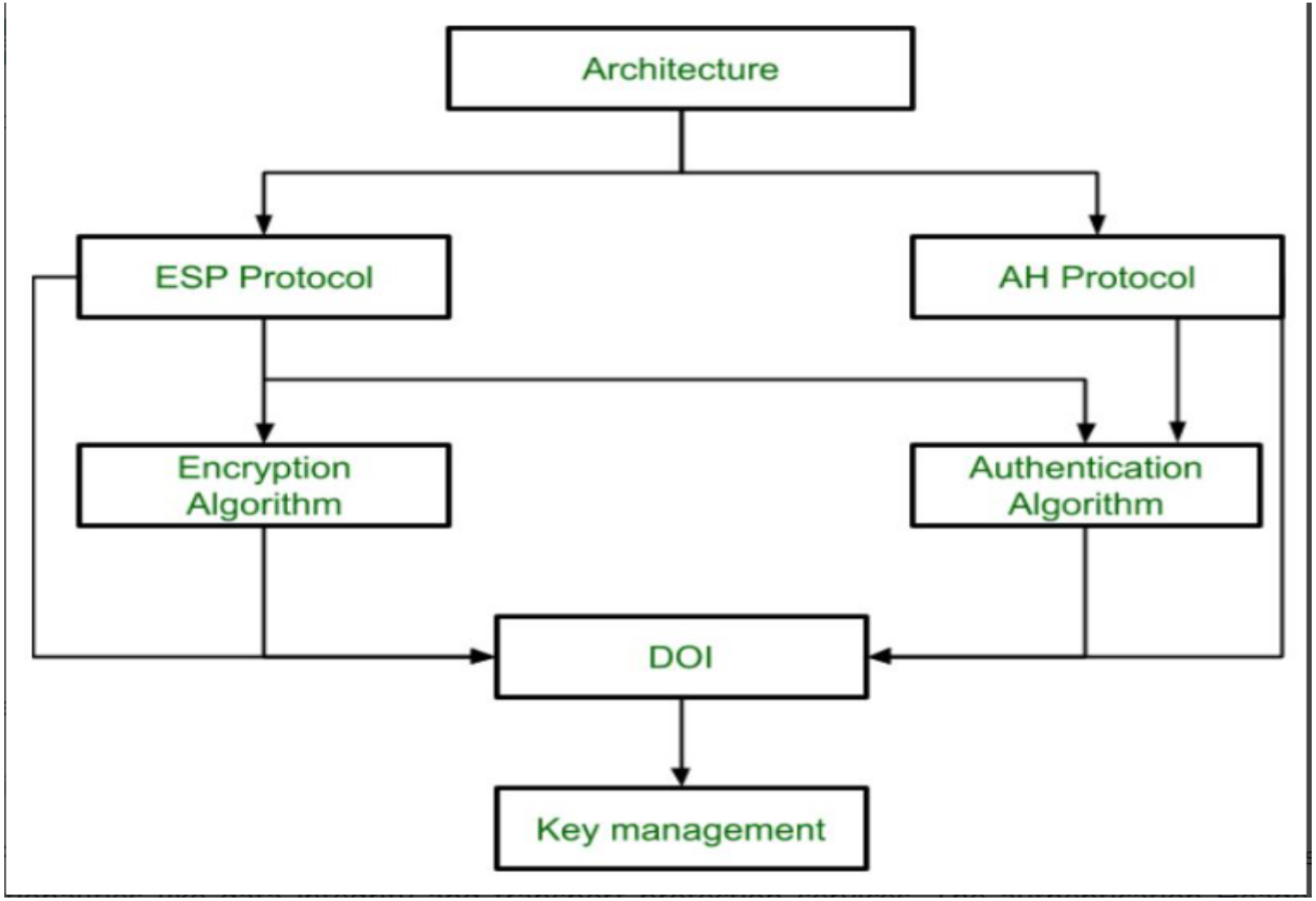
•IPSec is often used in Virtual Private Networks (VPNs) to create secure, private connections.

•IPSec protects from Cyber Attacks .

Features of IPSec

- **Authentication:** IPSec provides authentication of IP packets using digital signatures or shared secrets. This helps ensure that the packets are not tampered with or forged.
- **Confidentiality:** IPSec provides confidentiality by encrypting IP packets, preventing eavesdropping on the network traffic.
- **Integrity:** IPSec provides integrity by ensuring that IP packets have not been modified or corrupted during transmission.
- **Key management:** IPSec provides key management services, including key exchange and key revocation, to ensure that cryptographic keys are securely managed.
- **Tunneling:** IPSec supports tunneling, allowing IP packets to be encapsulated within another protocol, such as GRE (Generic Routing Encapsulation) or L2TP (Layer 2 Tunneling Protocol).
- **Flexibility:** IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.
- **Interoperability:** IPSec is an open standard protocol, which means that it is supported by a wide range of vendors and can be used in heterogeneous environments.

IPSec Architecture



IPSec Connection Establishment Process

The process of establishing an IPSec connection involves two main phases:

Phase 1: Establishing the IKE (Internet Key Exchange) Tunnel

In phase 1, the main aim is to establish the secure channel the IKE tunnel, which is used to further negotiations. Phase 1 can operate in one of two modes:

- **Main Mode:** Main Mode is a six-message exchange procedure that is more secure than Basic Mode, although at the cost of a longer session, since identity information is transmitted during negotiations.
- **Aggressive Mode:** Aggressive Mode takes lesser time with the exchange of three messages and is less secure since more information like identity is disclosed during the course of negotiation.

Phase 2: Establishing the IPSec Tunnel

Phase 2 is called Quick Mode and its aim is to negotiate the IPSec Security Associations after the construction of a secure IKE tunnel has been made. There are two modes in Phase 2.

- **Tunnel Mode:** This mode encapsulates the whole of the original IP packet including the header and data. It is mostly deployed in the site to site VPNs.
- **Transport Mode:** By this mode, only the actual data to be transmitted is encrypted and the header part of the IP packets remain unaltered. It is mainly employed in end to end communication between hosts.

Protocols Used in IPSec

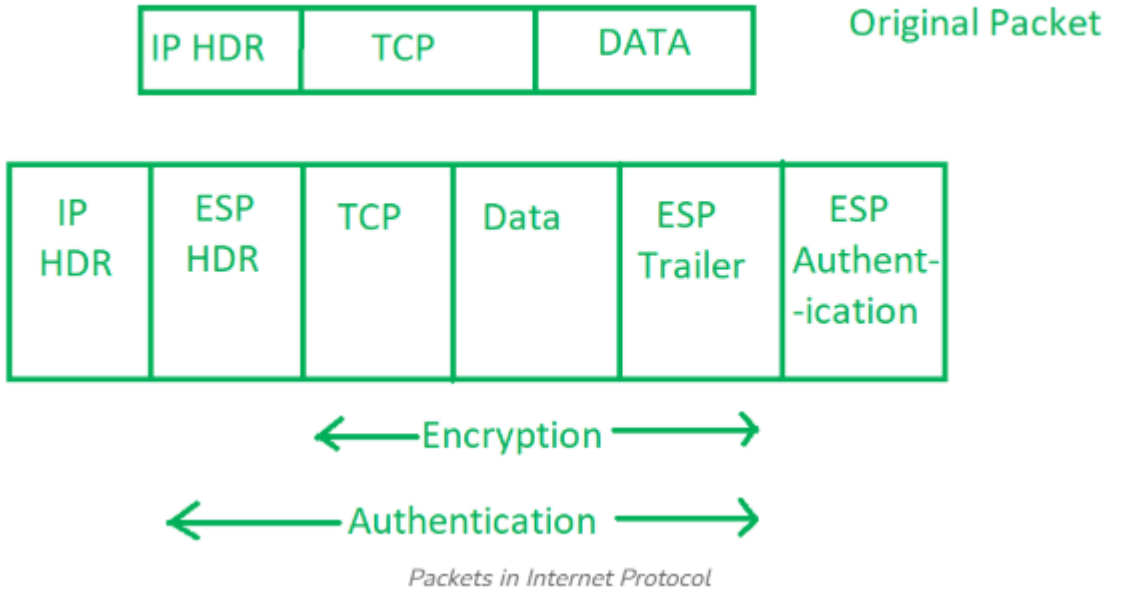
1. Encapsulating Security Payload (ESP)
2. Authentication Header (AH)
3. Internet Key Exchange (IKE)

1. Encapsulating Security Payload (ESP): It provides data integrity, encryption, authentication, and anti-replay. It also provides authentication for payload.

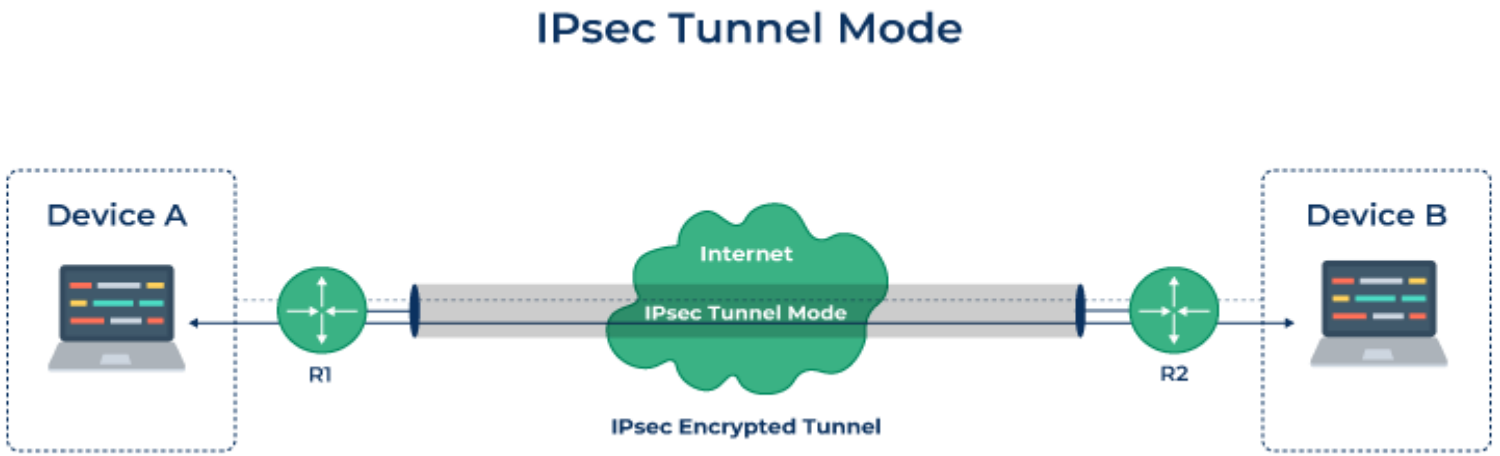
2. Authentication Header (AH): It also provides data integrity, authentication, and anti-replay and it does not provide encryption. The anti-replay protection protects against the unauthorized transmission of packets. It does not protect data confidentiality.

Protocols Used in IPSec cont..

Internet Key Exchange (IKE): It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices.



How Does IPSec Work



How Does IPSec Work

IPSec (Internet Protocol Security) is used to secure data when it travels over the Internet.

IPSec works by creating secure connections between devices, making sure that the information exchanged is kept safe from unauthorized access.

IPSec majorly operates in two ways

Transport Mode and

Tunnel Mode.

IPSec uses two main protocols:

AH (Authentication Header) and

ESP (Encapsulating Security Payload)

When two devices communicate using IPSec, the devices first initiate the connection by sending a request to each other. After that, they mutually decide on protection of data using **passwords** or **digital certificates**. Now, they establish the secure tunnel for communication. Once the tunnel is set up, data can be transmitted safely, as IPSec is encrypting the data and also checking the integrity of the data to ensure that data has not been altered. After the communication is finished, the devices can close the secure connection. In this way, the IPSec works.

Difference Between IPSec Tunnel Mode and IPSec Transport Mode

•**Tunnel:** The IPSec tunnel mode is appropriate for sending data over public networks because it improves data security against unauthorised parties. The computer encrypts all data, including the payload and header, and adds a new header to it.

•**Transport:** IPSec transport mode encrypts only the data packet's payload while leaving the IP header unchanged. The unencrypted packet header enables routers to determine the destination address of each data packet. As a result, IPSec transport is utilized in a closed and trusted network, such as to secure a direct link between two computers.

Advantages & Disadvantages

Advantages of IPsec:

1.IPsec provides network-layer security as it works on the network layer and provides transparency to applications.
2.It provides confidentiality during any kind of data exchange.
3.As it is implemented on the network layer, IPsec has zero dependability on applications.

Disadvantages of IPsec:

IPsec has a wide access range, In IPsec networks giving access to a single device can give access privilege to other devices too.
In many of the cases, it brings a couple of incompatibility issues with different software.
In many cases, IPsec leads to high CPU usage.

Any Query????

Thank you……