UNIT – 3

IP Security and Architecture

Page No : 5 | Mar | 2020

IP Security :-

IP Security is a capability which provides security mechanisms that include secure datagram authentication and encryption mechanisms within IP. It can be added to current versions of Internet Protocol (IPv4 or IPv6) by means of additional headers. IP security encompasses three functional areas –
Authentication, confidentiality and key management.

The principle feature of IP security that enables it to support these varied application is that it can encrypt or authenticate all traffic at the IP level. When IP security is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.

IP Sec is a set of protocols to support "secure exchange of packets at IP layer."

- Applications of IP Security :-

It provides the capability to secure communications across a LAN, across private and public WAN and across the internet. Some important applications are as follows –

(a) Secure branch office connectivity over the internet :- A company can build a secure virtual private network over a public WAN.

(b) Secure remote access over the internet – An end user whose system is equipped with IP security protocols can make a local call to an internet service provider (ISP)

) Establishing extranet and intranet connectivity with partners

IP security can be used to secure communication with other organisations, ensuring authentication and confidentiality and providing key exchange mechanism.

(d) Enhancing electronic-commerce security — Even though some web and e-commerce applications have built-in security protocols. The use of IP security enhances that security.

★ IP Security Architecture :- IP sec architecture uses 2 protocols - ESP, AH to secure the traffic or data flow.
The IP security specification consist of numerous documents. The most important of these issued in November of 1998 are RFCs 2401, 2402, 2408. The documents are divided into seven groups -

1. Architecture
2. Encapsulating security payload (ESP)
3. Header (Authentication header) (AH)
4. Encryption algorithm
5. Authentication algorithm
6. Key management
7. Domain of interpretation

1- Architecture — It covers the general concepts, security requirements, definitions and mechanisms defining IP security technology.

2- Encapsulating security payload (ESP) — It covers the packet format & general issues related to the use of the the encapsulating security payload for packet encryption and optionally authentication.

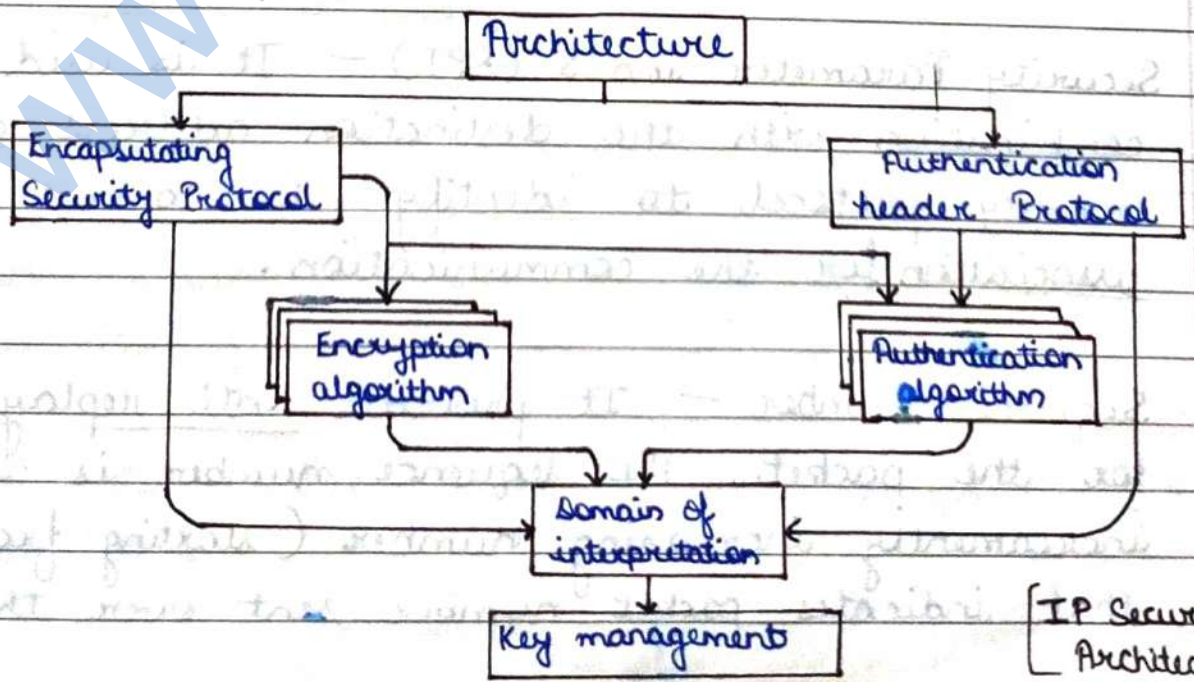
3- Authentication header (AH) — It covers the packet format of general issues related to the use of authenticcdi-on header(AH) for packet authentication and integrity.

4- Encryption algorithm — A set of documents that describes how various encryption algorithms are used for encapsulating security payload(ESP).

5- Authentication algorithm — A set of documents that describes how various authentication algorithms are used for authentication header(AH) and for the authentica-tion option of encapsulating security payload.

6- Key management — Key management contains the Documents that describe key management schemes and describes how the keys are exchanged between sender and receiver.

7- Domain of interpretation — It contains value needed for the other documents to relate to each other. These include identifiers for approved encryption and authentication algorithms as well as operational parameters such as key lifetime. DOI is the identifier which supports both ESP and AH protocols.



IP Security Architecture

★ Authentication header :-

It provides authentication, integrity and anti-replay protection for the entire packet (Both the IP header and the data payload carried in the packet).

It doesn't provide confidentiality, which means that it doesn't encrypt the data. The data is readable but protected from modification.

It contains following fields -

1. Next header
2. Length
3. Sequence number
4. Authentication data
5. Security parameter index (SPI)

★ ~~Encapsulation Security Payload~~

1. Next header - It identifies the IP payload by using the IP protocol ID.

2. Length - It indicates length of AH header.

3. Security Parameter index (SPI) - It is used in combination with the destination address and the security protocol to identify the correct security association for the communication.

4. Sequence number - It provides anti-replay protection for the packet. The sequence number is a 32-bit, incrementally increasing number (starting from 1) that indicates packet number sent over the security

association for the communication.

5- Authentication data — It contains the integrity check value (ICV), also known as the message authentication code, which is used to verify both message authentication and integrity. The receiver calculates the ICV values and checks it against this value (which is calculated by the sender) to verify integrity.

★ Encapsulating Security Payload (ESP) :-
ESP provides confidentiality services, including confidentiality of message contents and limited traffic flow confidentiality.

ESP can also provide an authentication service. ESP contains following feilds —

1. Security parameter index (32-bits)
2. Sequence number (32-bit)
3. Payload data (variable)
4. Padding (0-255 bytes)
5. Pad length (8-bit)
6. Next header (8-bit)
7. Authentication data

1- Security parameter index (32-bit) — It identifies a security association for the communication when used in combination with the destination address and the security protocol.

2- Sequence number (32-bit) — It provides anti-replay function.

3- Payload data — This is a transport level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.

4- Padding (0–255 bytes) — The purpose of this field is to make message of fixed length.

5- Pad length — It indicates the number of pad bytes immediately preceding this field.

6- Next header — It identifies the type of data contained in the payload data field by identifying the first header in that payload.

7- Authentication data — It is a variable length field that contains ICV value (Integrity Check Value) computed over the encapsulating security payload (ESP) packet (—) the authentication data field.

★ Security association —

It is a key concept that appears in both the authentication and confidentiality mechanisms for IP. An association is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it.

A security association is uniquely identified by three parameters -

(a) Security parameter index
(b) IP destination address
(c) Security protocol identifier

Following are the parameters for defining security associations -

1- Sequence number counter — It is a 32-bit value to generate the sequence number field in authentication header(AH) or encapsulating security payload(ESP) header.

2- Sequence counter flow — It is a flag indicating overflow of the sequence counter.

3- Anti-replay window — It is used to determine replay attack.

4- Authentication header information — It includes authentication algorithms, keys or key lifetimes.

5- Encapsulating security payload information — It contains encryption and authentication algorithm, keys, initial values, key lifetimes and other related parameters.

6- Duration — It contains lifetime of security association.

7- IP security protocol mode — It is also called tunnel mode

8- Path — Any observed path maximum transmission unit (MTU).

* Security association bundle :-
It refers to a sequence of security associations through which traffic must be processed to provide a desired set of IP security services.

- Combined Security Associations :-

Security associations may be combined into bundles in two ways -

1. Transport adjacency
2. Iterated tunneling

1. Transport adjacency — It refers to applying more than one security protocol to the same IP packet, without invoking tunneling. This approach to combining authentication header (AH) and ESP allows for only one level of combination.

2. Iterated tunneling — It refers to the application of multiple layer of security protocols affected through IP tunneling. This approach allows for multiple level of nesting, since each tunnel can originate or terminate at a different IP security site along the path.

Imp. Key-

★ Management :-

The key management portion of IP Security involves the determination and distribution of secret keys.

A typical requirement is four keys for communication between two applications — transmit and receive pairs for AH and ESP.

IP security architecture document mandates support for two types of key management -

1. Manual
2. Automated

1. Manual – A system administrator manualy configure each system with its own keys and with the keys of other communication systems. This is practical for small and static environment.

2. Automated – An automated system enables the on demand creation of keys and facilitates the use of keys in a large distribution system with an involving configuration.

The default automated key management protocol for IP security is refered to as ISAKMP/Oakley.

- Features of Oakley –

1- It employs a mechanism known as cookies to transfer/thwart clogging attacks.
2- It enables the two parties to negotiate a group, this in essence, specifies the global parameters of the diffie Hellman key exchange.
3- It uses nonces to ensure against replay attacks.
4- It enables the exchange of Diffie Hellman public key values.
5- It authenticates the Diffie Hellman exchange to thwart man-in-middle attack.

- ISAKMP – (Internet Security Association and Key Management Protocol)

An ISAKMP message has a fixed header format. This format has following fields –

1. **Initiater cookie (64-bit)** – It is a cookie of entity that initiated security association establishment, security association notification or security association deletion

2- Responder cookie (64-bit) — It is a cookie of responding entity, null in first message from initiater.

3- Next Payload (8 bit) — It indicates the type of first payload in the message.

4- Major version (4 bit) — It indicates major version of internet security association and key management protocol (ISAKMP).

5- Exchange type (8 bit) — It indicates type of exchange

6- Flag (8 bit) — It refers to bit of information.

7- Message Id (32 bit) —