Date
Page

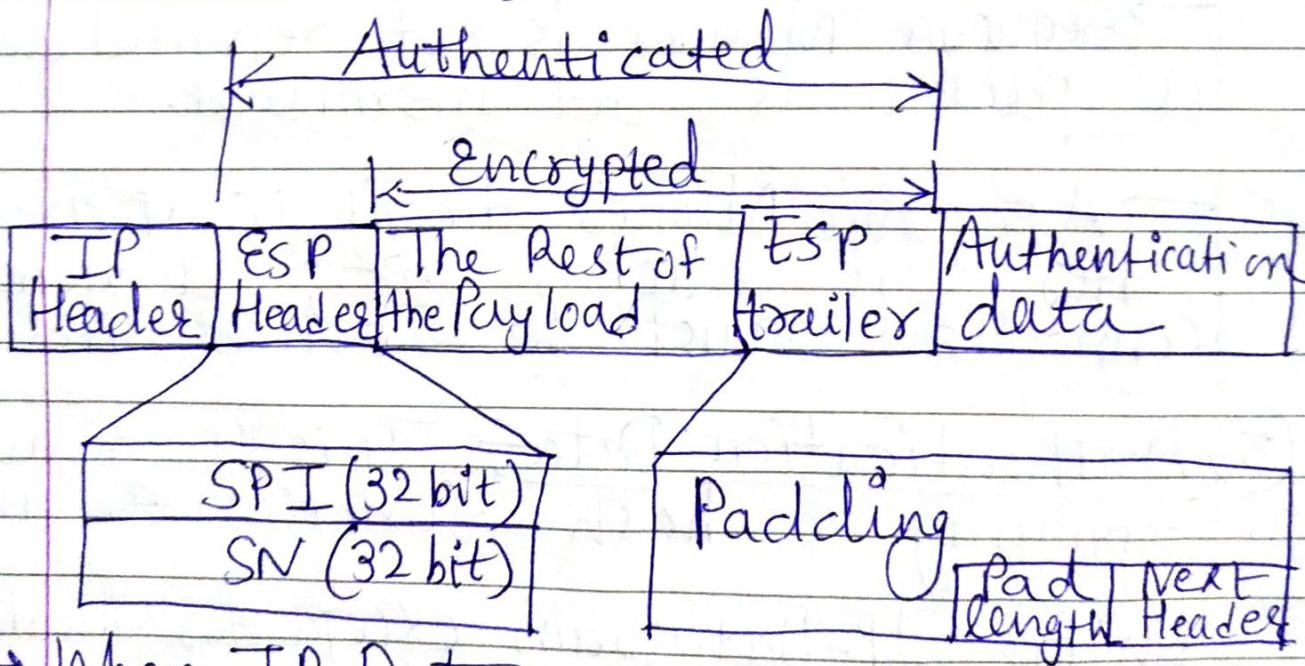
★ Encapsulating Security Payload :

→ The AH protocol doesn't provide privacy. It provides only source authentication and data Integrity.

→ ESP Provides
- → Source Authentication
- → Integrity
- → Privacy

→ ESP adds a Header and a Trailer.

→ ESP's authentication data are added at the end of the packet, which makes its calculation easier.



→ When IP Datagram carries an ESP Header and trailer, the value of the protocol field in the IP Header is 50.

→ A field inside the ESP-Trailer (Next Header) holds the original value of Protocol field.

ESP Procedure steps:

1. ESP-Trailer is added to the Payload.
2. Payload and trailer are encrypted.
3. ESP-Header is added
4. ESP-Header, Payload and ESP-Trailer are used to create authentication data.
5. Authentication data are added to the end of the ESP-Trailer.
6. IP header is added after changing the protocol value to 50.

* **Padding:** The variable length field (0 to 255 bytes) of 0's serves as padding.
* **Pad length:** The 8-bit pad length field defines the number of padding bytes. The value is between 0 and 255.
* **Authentication data:** Computed over ESP-H, Payload (Encrypted), ESP-T.

Note: In AH, part of the IP-Header is included in the calculation of the authentication data; In ESP, it is not.

→ IPSec supports both IPV4 and IPV6.

→ ESP was designed after AH.
ESP is better than AH
Then why do we need AH?

↓

We don't need. However, AH is already included in some commercial products, which means AH will remain part of the Internet until these products are phased out.

→ IPSec Services :-

	AH	ESP
① Access Control	✓	✓
② Msg Authentication (Integrity)	✓	✓
③ Confidentiality	✗	✓
④ Replay protection	✓	✓
⑤ Entity Authentication	✓	✓

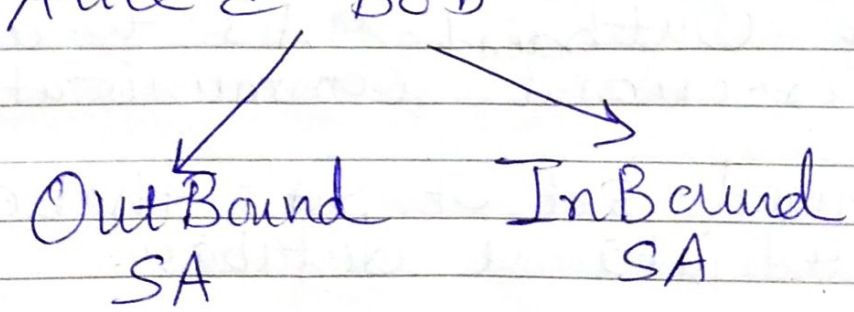
✡ Security Association :-

→ Very Imp aspect of IPsec
→ IPsec requires a logical relationship called a Security Association (SA), between two hosts.

✡ Idea of SA :-

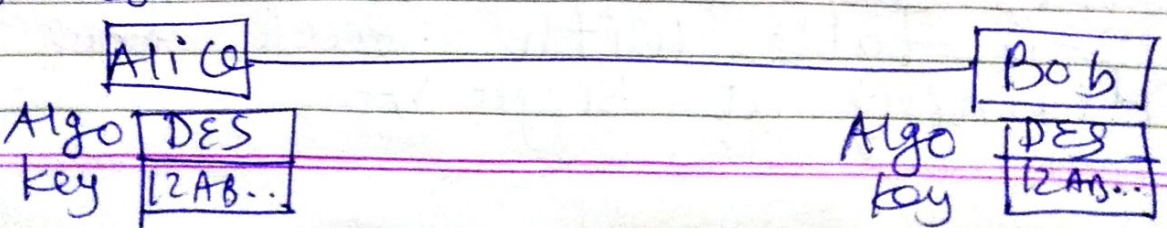
→ It is a contract between two parties;
→ It creates a Secure channel between them.
→ Let us assume that Alice needs to unidirectionally Communicate with Bob.
→ If Alice, Bob are interested in Confidentiality aspect only, they can get a shared key between themselves.

2 Security Associations between Alice & Bob



→ Each of them stores the value of the key in a variable and the name of the encryption/decryption algo in other.

Very Simple SA



→ SA's are more involved if the two parties need Message Integrity and Authentication.

→ Each association needs other data such as algo for Message Integrity, the key and other parameters.

★ SAD: (Security Association Database)

↳ Purpose: Access Control

→ SAD can be very Complex.

→ This is true if Alice wants to send messages to many people and Bob needs to receive messages from many people.

→ Each site needs to have both In-bound and Outband SA's to allow bi-directional communication.

→ We need set of SA's that can be collected into a database.

→ This database is called the SAD i.e. Security Association Database.

→ This database can be thought of as 2-D table with each row defining a single SA.

SAD:

Index	SN	OF	ARW	AH/ESP	LT	Mode	MTU
<SPI, DA, P>							
<SPI, DA, P>							
<SPI, DA, P>							

→ When a host needs to send a packet which carries IPSec Header, the host needs to find the corresponding entry in the Outbound SAD to find the information for applying Security to the packet.

→ Similarly, when a host receives a packet that carries an IPSec Header, the host needs to find the corresponding entry in the Inbound SAD to find the information for checking the Security of the packet.

→ This searching is specific in the sense that the receiving host needs to be sure that correct information is used for processing the packet.

→ Each entry in the In-Bound SA is selected using a triple

1. SPI
2. DA: Destination Address
3. P: Protocol (AH/ESP)

✱ Typical SA Parameters

① Sequence Number Counter
→ 32-bit value that is used to create Sequence Numbers for the AH/ESP header.

② Seq. Number Overflow
→ Indicates event of Seq. number overflow.

③ Anti-Replay Window
→ This detects an inbound replayed AH/ESP packet.

④ AH Info.
→ Section contains information for AH protocol.
(i) Authentication algo
(ii) Keys
(iii) Key Lifetime
(iv) Other related parameters

⑤ ESP Info.
(i) Encryption algo
(ii) Auth. algo
(iii) Keys
(iv) Key Lifetime
(v) IV
(vi) Other related parameters

⑥ SA Lifetime
⑦ IPSec Mode (Transport/Tunnel)
⑧ Path MTU