Module 5

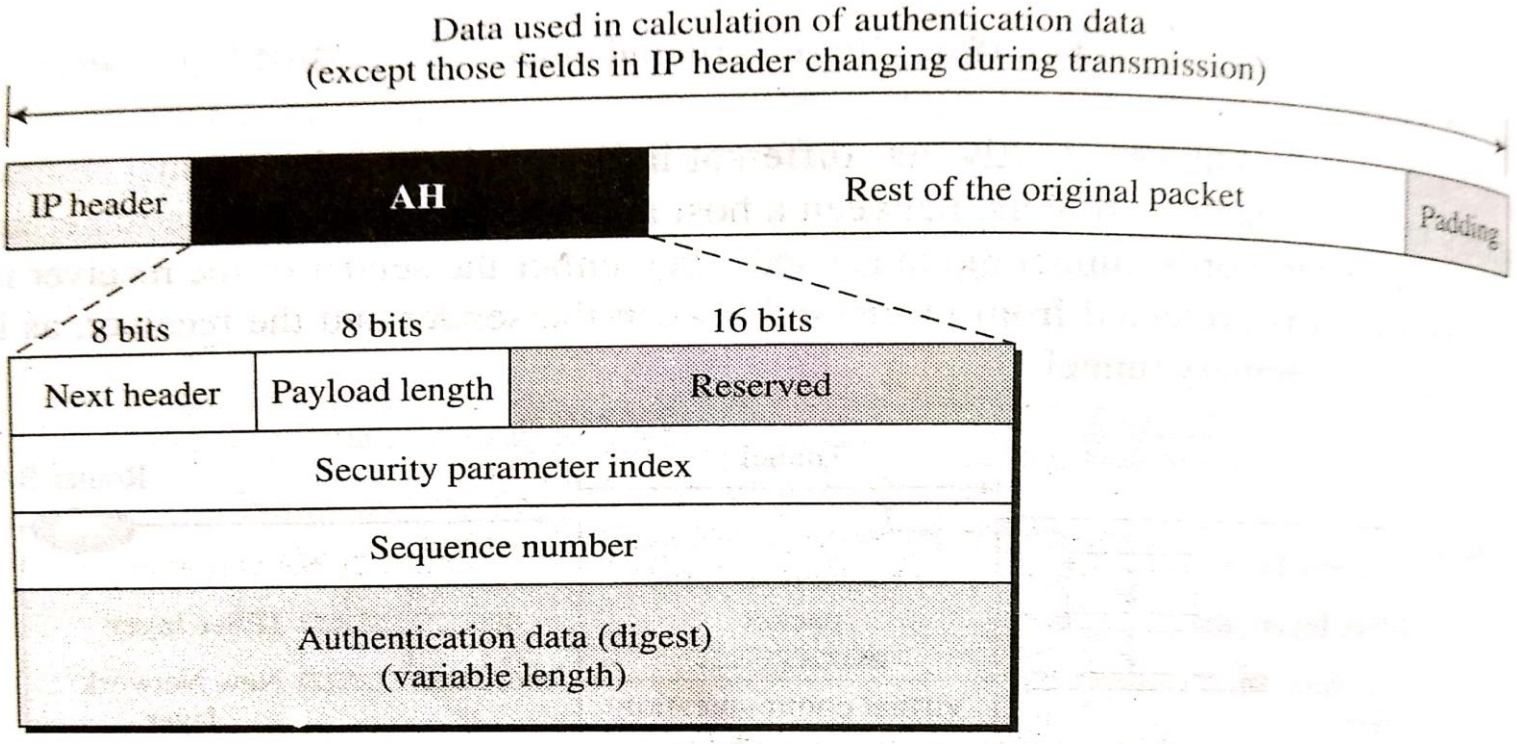
Network Security and Applications

IPSec-Authentication Header(AH)

- Purpose:
  - Authentication of source host
  - Ensuring Integrity of the payload carried in the IP packet

- The AH protocol uses a hash function and a symmetry key to create a Message Digest
- This Message Digest is inserted into the Authentication Header(AH)
- The AH is then placed in the appropriate location based on the mode (tunnel or transport mode)

IPSec-Authentication Header(AH)



AH-Protocol Fields

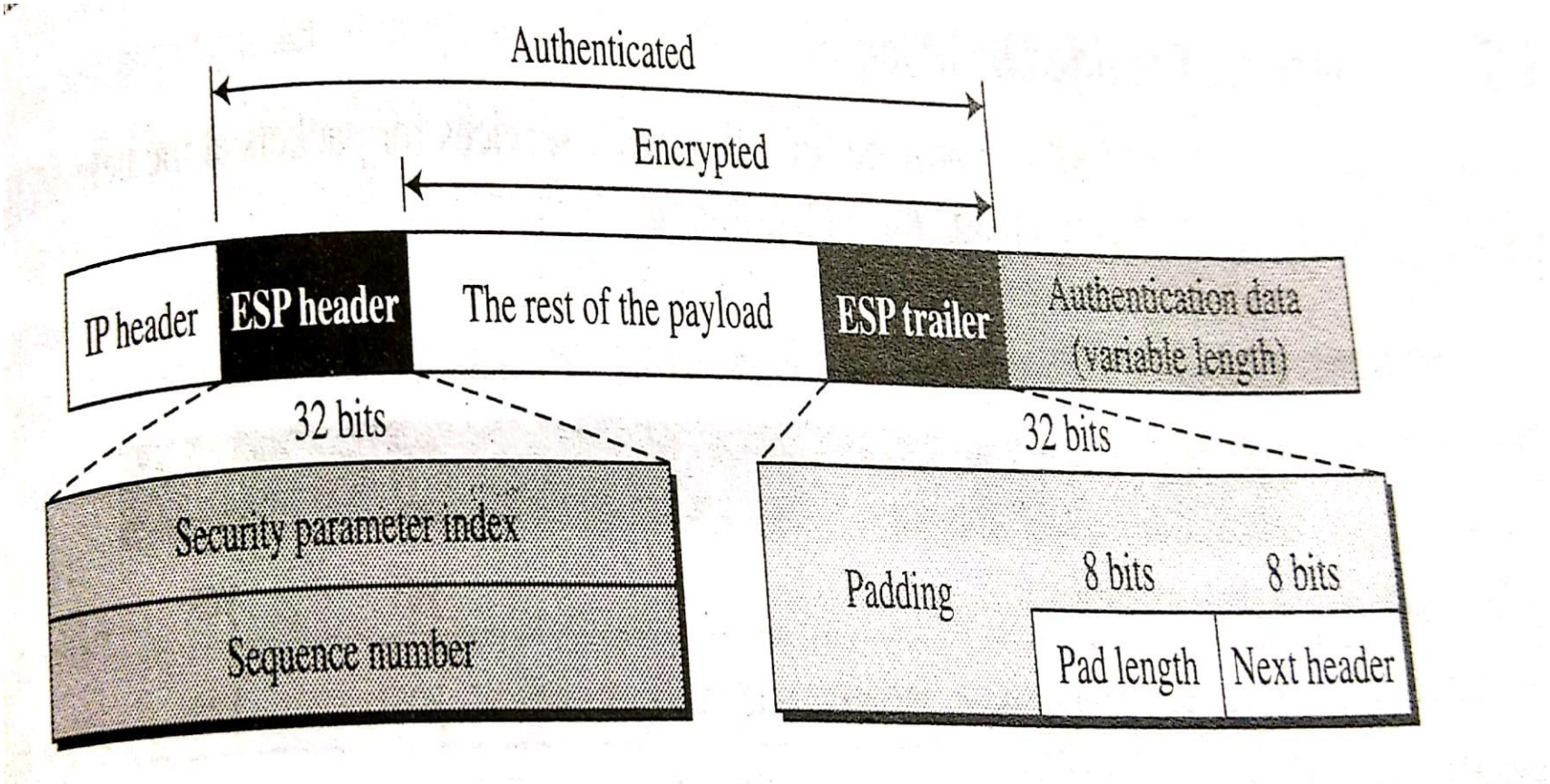
- **Next Header:** It is a 8-bit field that defines the type of payload carried by the IP datagram such as TCP,UDP,ICMP
- **Payload Length**: It is a 8-bit field that defines length of authentication header
- **Security Parameter Index(SPI):** It is a 32-bit field that plays the role of virtual circuit identifier. It is same for all packets sent during a connection.
- **Sequence Number:** It is a 32-bit field that provides ordering information for a sequence of datagrams.
- **Authentication Data:** This field is the result of applying a hash function to the entire datagram except for the fields that are changed during the transit like time to live (TTL).

Encapsulation Security Payload(ESP)

- **Drawback of AH Protocol:-**
  - It does not provide privacy, it only provides data integrity and source authentication
- **Solution**:-
  - Use of ESP Protocol which provides source authentication, data integrity and privacy

- ESP adds a header and a trailer

Encapsulation Security Payload(ESP)



ESP-Header-Protocol Fields

- **Security Parameter Index(SPI):** It is a 32-bit field that plays the role of virtual circuit identifier. It is same for all packets sent during a connection.
- **Sequence Number:** It is a 32-bit field that provides ordering information for a sequence of datagrams.

ESP-Trailer-Protocol Fields

- **Padding:** It is a variable length field (0 to 255) of 0's
- **Pad Length**: It is a 8-bit pad length that defines the number of padding bytes. The value is between 0 and 255.
- **Next Header:** It is a 8-bit field that defines the type of payload carried by the IP datagram such as TCP,UDP,ICMP
- **Authentication Data:** This field is the result of applying an authentication scheme to parts of the datagram.
    - In AH protocol, part of IP Header is included in the calculation of Authentication Data
    - But in ESP protocol it is not included

How authentication and confidentiality is achieved using IPSec?

- To achieve both, encryption and authentication can be combined in order to transmit the IP packet

- ESP along with authentication needs to be applied.
    - User first applies ESP to the data to be protected
    - Then appends the authentication data field

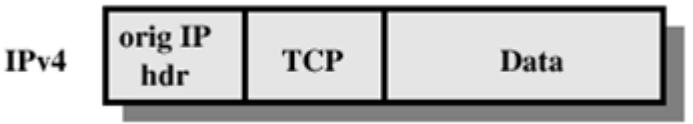
How authentication and confidentiality is achieved using IPSec?

- Two cases:
  - **Transport Mode ESP**:- Authentication and encryption are applied to the IP payload delivered to the host but in this case, the IP header is not protected
  - **Tunnel mode ESP**:- Authentication is applied to the entire IP packet delivered to the destination and also authentication is performed at that destination.

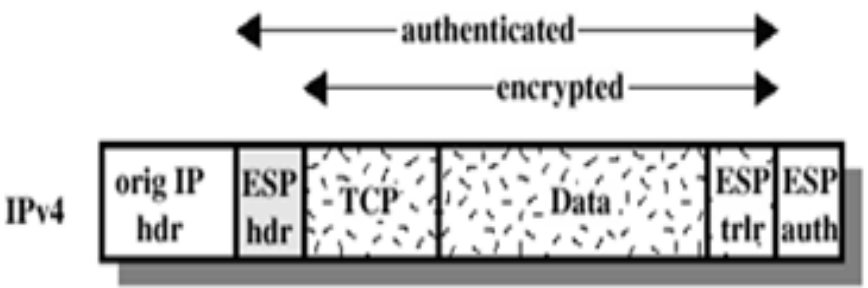
- In both cases, authentication is applied to the Cipher text not the plain text

How authentication and confidentiality is achieved using IPSec?

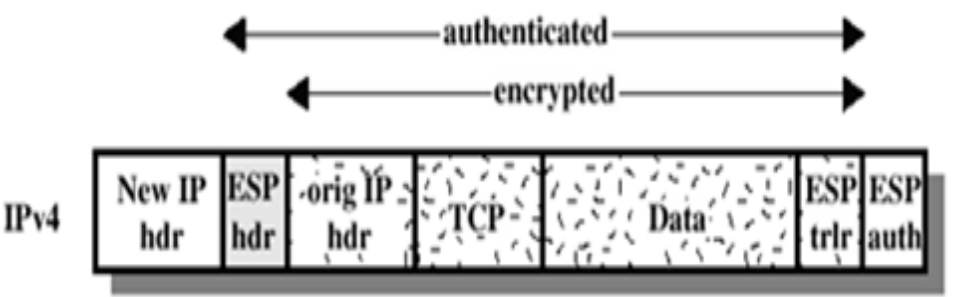
Before applying ESP



After applying ESP



Transport Mode

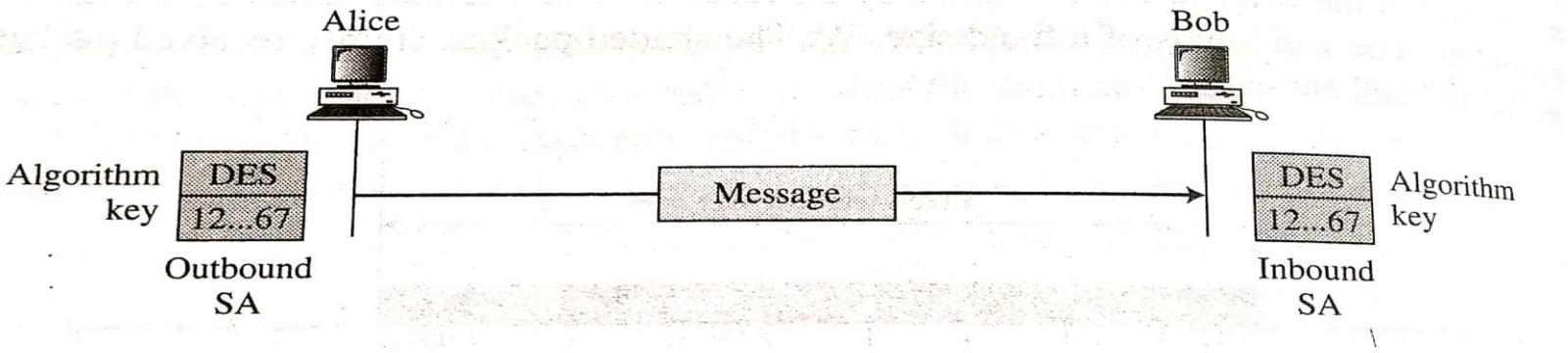


Tunnel Mode

Security Association(SA)

- A security association(SA) is a contract between two parties
- It creates a secure channel between them
- Example:- If Alice wants to send information to Bob then there are two SA's between them
    - Outbound SA
    - Inbound SA

  Each of them stores the value of the key in a variable and the name of encryption/decryption algorithm in another variable



Security Association Database(SAD)

- If Alice want to send message to many people and Bob wants to receive messages from many people then each of them need to have both SA's to allow bi-directional communication
- A database is required to collect all those set of SA's
- That database is known as Security Association Database (SAD)
- For inbound SA one separate SAD is maintained and for outbound SA another SAD is maintained
- SAD is a two dimensional table where each row defines a single SA
- Each entry in the SAD is selected using a triple index: <SPI, DA, P>
    - Security Parameter Index (SPI)
    - Destination Address (DA)
    - Protocol (P)

Security Association Database(SAD)

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

Security Association Database

Legend:

SPI: Security Parameter Index

DA: Destination Address

AH/ESP: Information for either one

P: Protocol

Mode: IPSec Mode Flag

SN: Sequence Number

OF: Overflow Flag

ARW: Anti-Replay Window

LT: Lifetime

MTU: Path MTU (Maximum Transfer Unit)

Security Policy (SP)

- Security Policy (SP) defines the type of security applied to the packet when it is to be sent or when it has arrived
- SP is used before using SAD
- Each host needs to have a Security Policy Database (SPD)

Security Policy Database(SAD)

- There is a separate Inbound SPD and a separate Outbound SPD
- Each entry in SPD is accessed using a six tuple index:
  <SA, DA, Name, P, Sport, DPort>

Index	Policy
< SA, DA, Name, P, SPort, DPort >	
< SA, DA, Name, P, SPort, DPort >	
< SA, DA, Name, P, SPort, DPort >	
< SA, DA, Name, P, SPort, DPort >	

Legend:

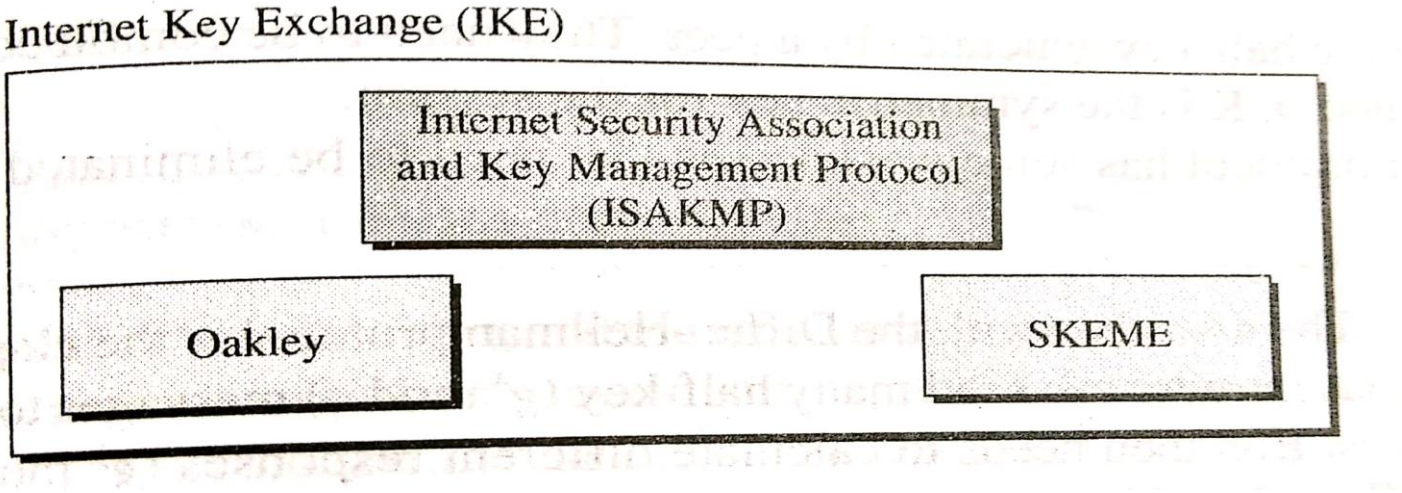
SA: Source Address
DA: Destination Address
P: Protocol
SPort: Source Port
DPort: Destination Port

Internet Key Exchange (IKE)

- The Internet Key Exchange (IKE) protocol is used to create both inbound and outbound SA
- When a host wants to send a IP packet, it consults the SPD to see if there is an SA for that type of traffic.
- If there is no SA, IKE is called to establish one.
- So, purpose of IKE is to create SAs for IPSec
- It is a complex protocol which is based on three protocols:
    - Oakley
    - SKEME
    - ISAKMP

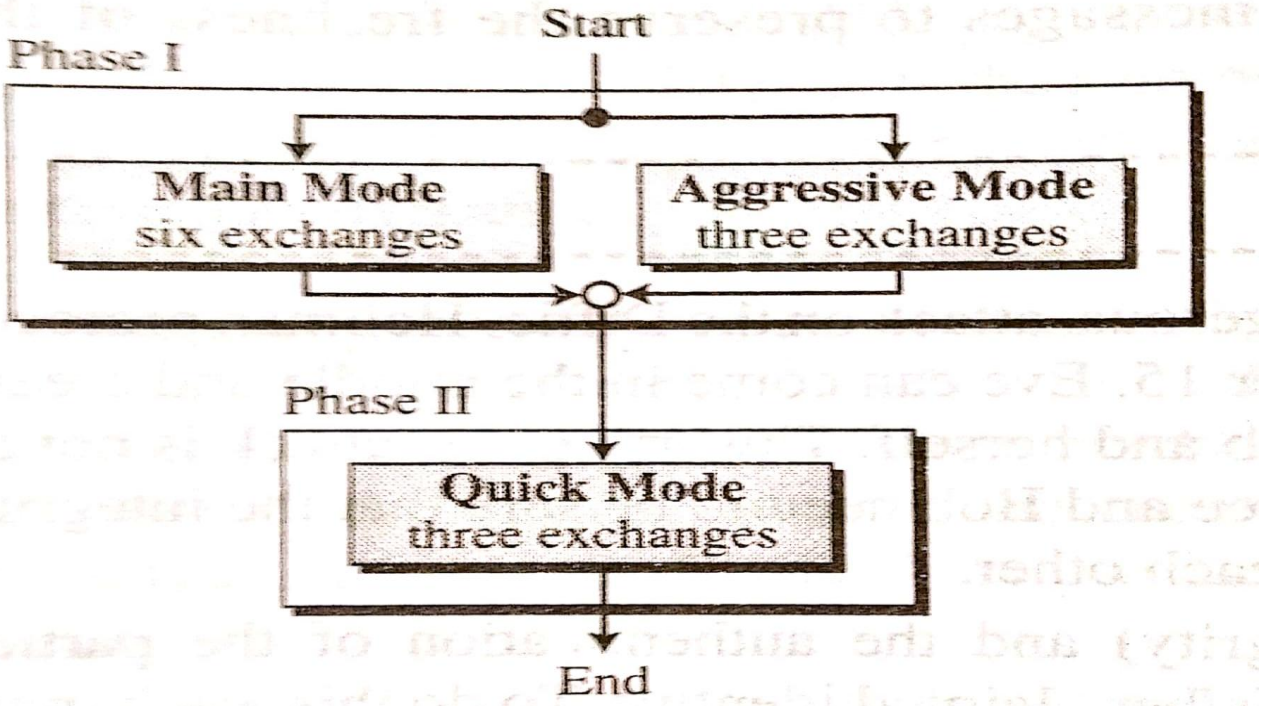
Internet Key Exchange (IKE)

- Oakley: It is a key creation protocol based on Diffie Hellman key exchange method
- SKEME: It uses public key encryption for entity authentication
- ISAKMP: It defines several packets, protocols and parameters that allow the IKE exchanges to take place in standardized formatted messages to create SAs



Internet Key Exchange (IKE)- Two phases

- Phase I :- It creates SAs for phase II
- Phase II :- It creates SAs for data exchange protocol



Services Provided by IPSec

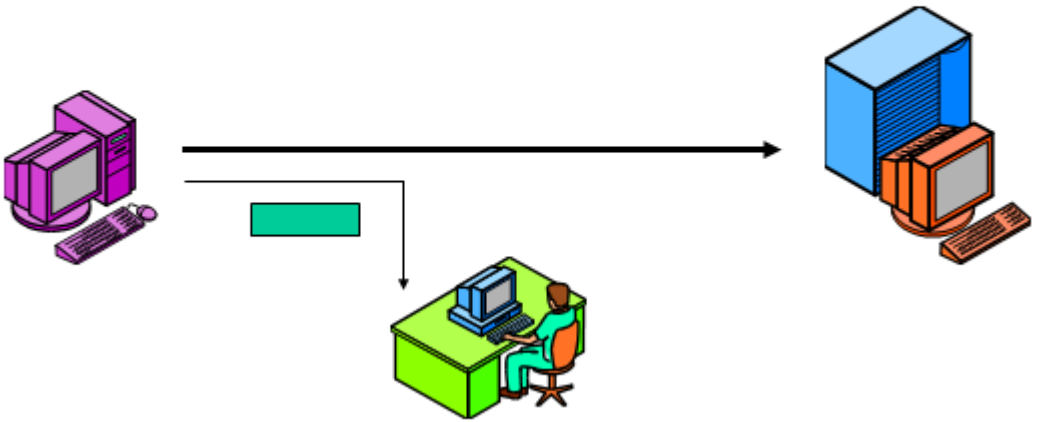
Services	AH	ESP
Access control	yes	yes
Message authentication (message integrity)	yes	yes
Entity authentication (data source authentication)	yes	yes
Confidentiality	no	yes
Replay attack protection	yes	yes

Replay Attacks

- **Replay Attack**: When an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination
- The receipt of a duplicate authenticated IP packet may disrupt the service in some way or may have some other undesired consequence.
- The information from one session can be replayed in a future session by a malicious intruder.

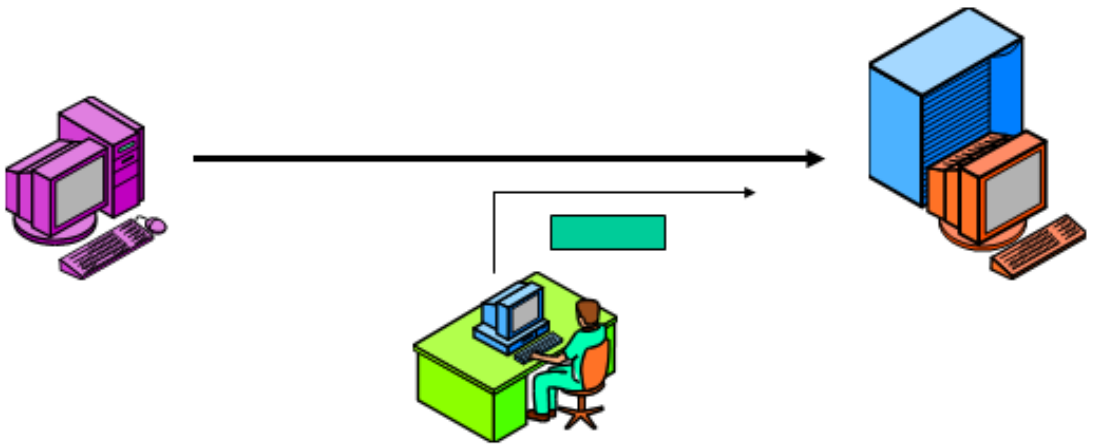
Replay Attacks

- First, attacker intercepts a message



Replay Attacks

- Later, attacker retransmits (*replays*) the message to the original destination host



Replay Attacks Example

- When login and password information is sent over the network, attacker can capture it and replay it later
- Attack occurs for security certificates-Attacker can resubmit the certificate, hoping that it will be validated by the authentication system
- Session key reuse: Eve(attacker) replays message from Alice to Bob, so Bob re-uses session key to communicate with Eve thinking him to be Alice

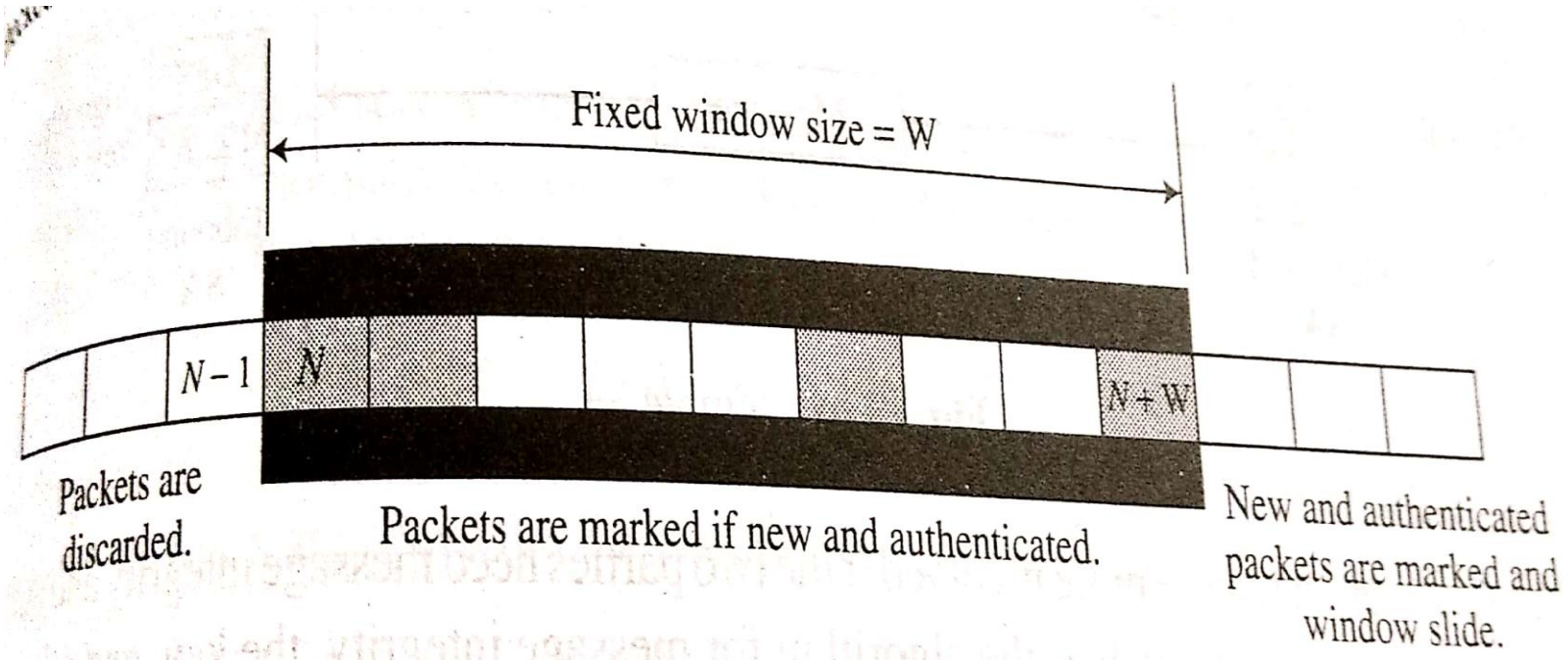
Replay Attacks Protection

- Since IP is a connectionless, unreliable service, there is no guarantee that
  a) packets will be delivered in order and
  b) all packets will be delivered
- So, it becomes easy for an attacker to launch a replay attack
- The **Sequence Number** field is designed in both AH and ESP protocols of IPSec to prevent such attacks
- When a SA is established, the sequence number is initialised to 0 and it increases until it reaches 2^{32}-1
- When this number reaches maximum, it is reset to 0, and old SA is deleted and a new one is established

Replay Attacks Protection

- To prevent processing of duplicate packets, the receiver should implement a fixed size window
- The default size of window, W=64
- The highest sequence number received so far for a valid packet is denoted by N

Replay Attack Protection



Replay Attacks Protection

- When a packet is received the following processing happens:

1. If the sequence number is < N :-
   - The packet is put on the left side of window. The packet is discarded because it is either duplicate or its arrival time has expired.

2. If the sequence number is between N and N+W-1:-
   - The packet is put inside the window.
     - If the packet is new and authenticated then the sequence number is marked and packet is accepted
     - Else packet is discarded

Replay Attacks Protection

3. If the sequence number is > N +W-1:-
   - The packet is put on the right side of window.
     - If the packet is new and authenticated then the sequence number is marked, window slides to the right to cover the newly marked sequence number and packet is accepted
     - Else packet is discarded