IPSec

Principles of Information Security and Privacy (CSE607)

M.Tech. I, Semester I

Department of Computer Science and Technology
S.V.National Institute of Technology-Surat

September 16, 2022

Overview

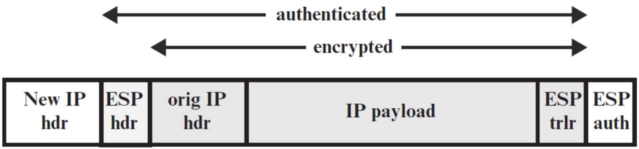
IPSec

- IP-level security encompasses three functional areas:
  - **Authentication** mechanism assures that a received packet was, in fact, transmitted by the party identified as the source in the packet header.
  - **Confidentiality** facility enables communicating nodes to encrypt messages to prevent eavesdropping by third parties
  - **Key management** facility is concerned with the secure exchange of keys.

Applications of IPSec

- Secure branch office connectivity over the Internet
  - A company can build a secure virtual private network over the Internet or over a public WAN.
  - enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.
- 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) and gain secure access to a company network.
  - reduces the cost of toll charges for traveling employees and telecommuters.
- Establishing extranet and intranet connectivity with partners
- Enhancing electronic commerce security
  - use of IPsec enhances the security.
  - IPsec guarantees that all traffic designated by the network administrator is both encrypted and authenticated
  - adding an additional layer of security to whatever is provided at the application layer.

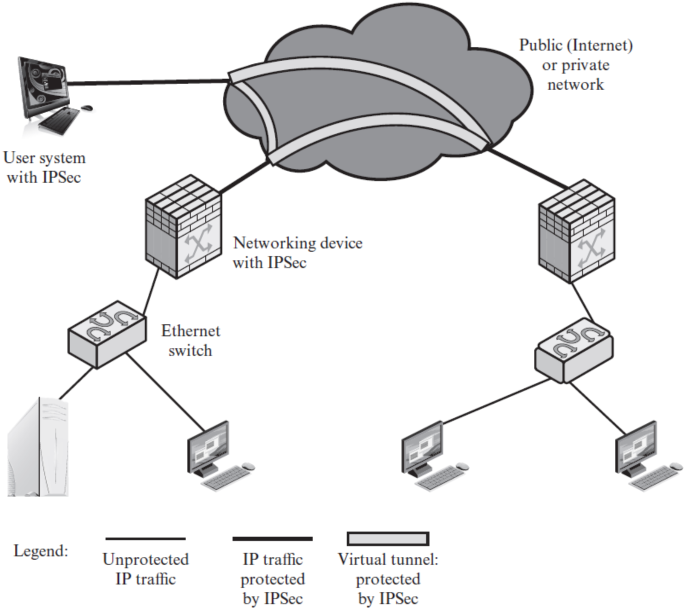
Tunnel Mode



(a) Tunnel-mode format

- Tunnel mode makes use of an IPsec function, a combined authentication/encryption function called Encapsulating Security Payload (ESP), and a key exchange function. For VPNs,
- both authentication and encryption are generally desired, because it is important both to
  - assure that unauthorized users do not penetrate the VPN, and
  - assure that eavesdroppers on the Internet cannot read messages sent over the VPN.

Tunnel Mode


User system
with IPSec
Public (Internet)
or private
network
Networking device
with IPSec
Ethernet
switch
Legend:
Unprotected
IP traffic
IP traffic
protected
by IPSec
Virtual tunnel:
protected
by IPSec

Benefits of IPSec

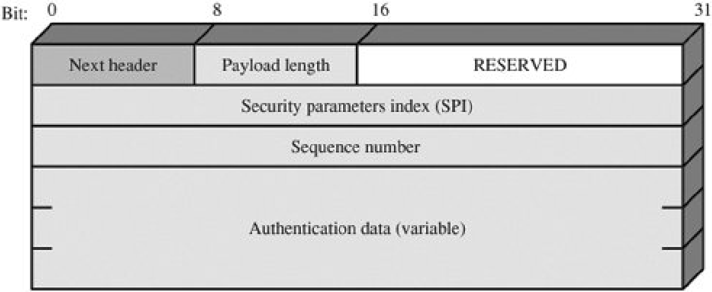
- When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.
- IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.
- IPsec is below the transport layer (TCP, UDP) and so is transparent to applications. There is no need to change software on a user or server system when IPsec is implemented in the firewall or router. Even if IPsec is implemented in end systems, upper-layer software, including applications, is not affected.
- IPsec can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.'
- IPsec can provide security for individual users if needed. This is useful for offsite workers and for setting up a secure virtual subnetwork

IPSec Services

- Two protocols are used to provide security: an authentication protocol designated by the header of the protocol, Authentication Header (AH); and a combined encryption/authentication protocol designated by the format of the packet for that protocol, Encapsulating Security Payload (ESP).
  - Access control
  - Connectionless integrity
  - Data origin authentication
  - Rejection of replayed packets (a form of partial sequence integrity)
  - Confidentiality (encryption)
  - Limited traffic flow confidentiality

Anti-reply services

- A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits to the intended destination.



Bit: 0	8	16	31
Next header	Payload length	RESERVED	
Security parameters index (SPI)			
Sequence number			
Authentication data (variable)			

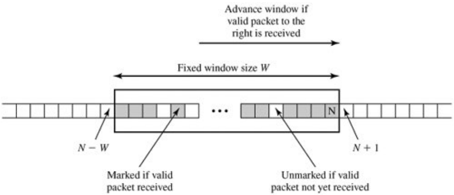
Anti-reply services

- When a new SA is established, the sender initializes a sequence number counter to 0.
- Each time that a packet is sent on this SA, the sender increments the counter and places the value in the Sequence Number field. Thus, the first value to be used is 1.
- If anti-replay is enabled (the default), the sender must not allow the sequence number to cycle past 2^{32} back to zero.
- If the limit of 2^{32} is reached, the sender should terminate this SA and negotiate a new SA with a new key.

Anti-reply services

- Because IP is a connectionless, unreliable service, the protocol does not guarantee that packets will be delivered in order and does not guarantee that all packets will be delivered.
- The receiver should implement a window of size W, with a default of $W = 64$. The right edge of the window represents the highest sequence number, N, so far received for a valid packet.
- For any packet with a sequence number in the range from N $W + 1$ to N that has been correctly received (i.e., properly authenticated), the corresponding slot in the window is marked

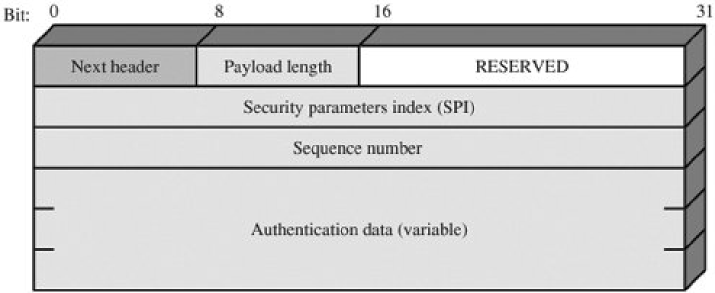
Anti-reply services


Advance window if valid packet to the right is received
Fixed window size W
N
$N - W$
$N + 1$
Marked if valid packet received
Unmarked if valid packet not yet received

- If the received packet falls within the window and is new, the MAC is checked. If the packet is authenticated, the corresponding slot in the window is marked.
- If the received packet is to the right of the window and is new, the MAC is checked. If the packet is authenticated, the window is advanced so that this sequence number is the right edge of the window, and the corresponding slot in the window is marked.
- If the received packet is to the left of the window, or if authentication fails, the packet is discarded; this is an auditable event.

Integrity Check Value

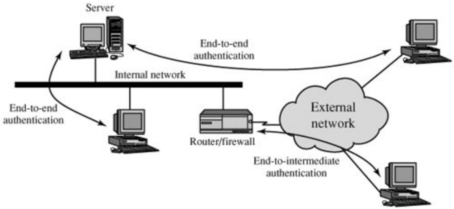
- The Authentication Data field holds a value referred to as the Integrity Check Value. The ICV is a message authentication code or a truncated version of a code produced by a MAC algorithm.


Bit:
0
8
16
31
Next header
Payload length
RESERVED
Security parameters index (SPI)
Sequence number
Authentication data (variable)

Integrity Check Value

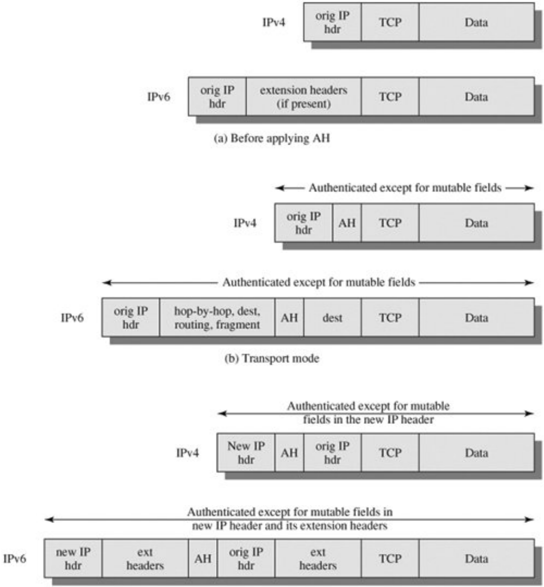
- The current specification dictates that a compliant implementation must support
  - HMAC-MD5-96
  - HMAC-SHA-1-96
- The MAC is calculated over
  - IP header fields that either do not change in transit (immutable) or that are predictable in value upon arrival at the endpoint for the AH SA.
  - Fields that may change in transit and whose value on arrival are unpredictable are set to zero for purposes of calculation at both source and destination.
  - The AH header other than the Authentication Data field.
  - The Authentication Data field is set to zero for purposes of calculation at both source and destination.
  - he entire upper-level protocol data, which is assumed to be immutable in transit (e.g., a TCP segment or an inner IP packet in tunnel mode).

Transport and Tunnel Mode



- Transport mode SA: authentication is provided directly between a server and client workstations; the workstation can be either on the same network as the server or on an external network. As long as the workstation and the server share a protected secret key, the authentication process is secure.
- Tunnel mode SA : A remote workstation authenticates itself to the corporate firewall, either for access to the entire internal network or because the requested server does not support the authentication feature.

Transport and Tunnel Mode


IPv4
orig IP hdr
TCP
Data
IPv6
orig IP hdr
extension headers (if present)
TCP
Data

(a) Before applying AH

Authenticated except for mutable fields
IPv4
orig IP hdr
AH
TCP
Data
Authenticated except for mutable fields
IPv6
orig IP hdr
hop-by-hop, dest, routing, fragment
AH
dest
TCP
Data

(b) Transport mode

Authenticated except for mutable fields in the new IP header
IPv4
New IP hdr
AH
orig IP hdr
TCP
Data
Authenticated except for mutable fields in new IP header and its extension headers
IPv6
new IP hdr
ext headers
AH
orig IP hdr
ext headers
TCP
Data

(c) Tunnel mode