CSCI-GA.3205 Applied Cryptography & Network Security

Department of Computer Science
New York University

PRESENTED BY DR. MAZDAK ZAMANI
mazdak.zamani@NYU.edu

Wireless Network Security

WEP, WPA2, 802.1X

IPsec

11

NYU

CompTIA Security+ Guide to Network Security Fundamentals, Fifth Edition

Chapter 9
Wireless Network Security

Wireless Attacks

- Several attacks can be directed against wireless data system:
  - Bluetooth attacks
  - Near Field Communication (NFC) attacks
  - Wireless local area network attacks

Bluetooth

- Wireless technology that uses short-range radio frequency (RF) transmissions
  - Personal Area Network (PAN) technology
- Bluejacking - an attack that sends unsolicited messages to Bluetooth-enabled devices
  - Bluejacking is considered more annoying than harmful (No data is stolen)
- Bluesnarfing
  - An attack that accesses unauthorized information from a wireless device through a Bluetooth connection
  - Often between cell phones and laptops
  - Attacker copies e-mails, contacts, or other data by connecting to the Bluetooth device without owner's knowledge

Near Field Communication (NFC)

- A set of standards primarily for smartphones and smart cards that can be used to establish communication between devices in close proximity
  - NFC devices are used in contactless payment systems

Vulnerability	Explanation	Defense
Eavesdropping	The NFC communication between device and terminal can be intercepted and viewed.	Because an attacker must be extremely close to pick up the signal, users should be aware of this. Also, some NFC applications can perform encryption.
Data manipulation	Attackers can jam an NFC signal so transmission cannot occur.	Some NFC devices can monitor for data manipulation attacks.
Man-in-the-middle attack	An attacker can intercept the NFC communications between devices and forge a fictitious response.	Devices can be configured in *active-passive* pairing so one device only sends while the other can only receive.
Device theft	The theft or loss of a smartphone could allow an attacker to use that phone for purchases.	Smartphones should be protected with passwords or PINs.

Table 9-2 NFC risks and defenses

Wireless Local Area Network (WLAN) Attacks

- A WLAN is designed to replace or supplement a wired LAN
- Institute of Electrical and Electronics Engineers (IEEE) WLANS
  - Most influential organization for computer networking and wireless communications
  - Dates back to 1884
  - Began developing network architecture standards in the 1980s
- 1997: release of IEEE 802.11
  - Standard for wireless local area networks (WLANs)
  - Higher speeds added in 1999: IEEE 802.11b
- IEEE 802.11a
  - Specifies maximum rated speed of 54Mbps using the 5GHz spectrum
- IEEE 802.11g
  - Preserves stable and widely accepted features of 802.11b and increases data transfer rates similar to 802.11a
- IEEE 802.11n
  - Ratified in 2009
  - Improvements: speed, coverage area, resistance to interference, and strong security

Wireless Local Area Network (WLAN) Attacks

- IEEE 802.11ac
  - Ratified in early 2014 and has data rates over 7 Gbps

	802.11	802.11b	802.11a	802.11g	802.11n	802.11ac
Frequency	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz	2.4 & 5 GHz	5 GHz
Nonoverlapping channels	3	3	23	3	21	21
Maximum data rate	2 Mbps	11 Mbps	54 Mbps	54 Mbps	600 Mbps	7.2 Gbps
Indoor range (feet/meters)	65/20	125/38	115/35	115/35	230/70	115/35
Outdoor range (feet/meters)	328/100	460/140	393/120	460/140	820/250	460/140
Ratification date	1997	1999	1999	2003	2009	2014

Table 9-3 IEEE WLAN standards

NYU

Wireless Local Area Network (WLAN) Attacks

- WLAN Hardware
  - Wireless client network interface card adapter
    - Performs same functions as wired adapter
    - Antenna sends and receives signals
  - Access point (AP) major parts
    - Antenna and radio transmitter/receiver send and receive wireless signals
    - Bridging software to interface wireless devices to other devices
    - Wired network interface allows it to connect by cable to standard wired network
  - Wireless broadband routers
    - Single hardware device containing AP, firewall, router, and DHCP server
    - Also known as *residential WLAN gateways*

Wireless Local Area Network (WLAN) Attacks

- Types of wireless attacks
  - Rogue access points
  - Evil twins
  - Intercepting wireless data
  - Wireless replay attacks and denial of service attacks

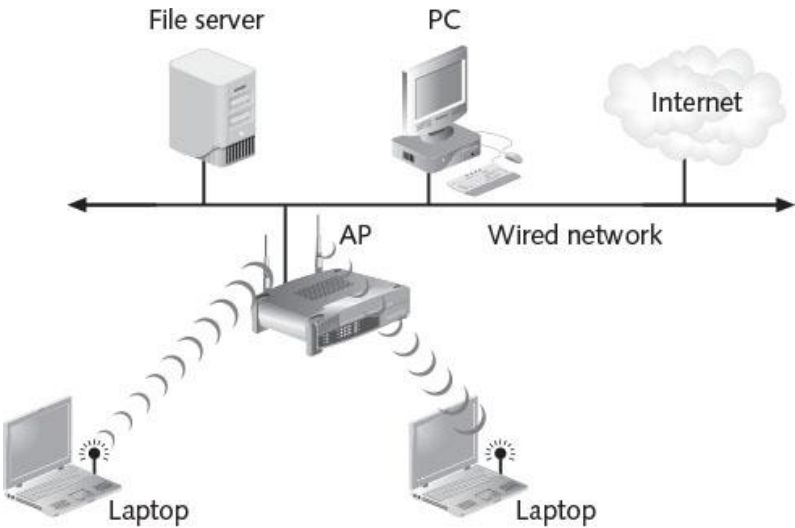


Figure 9-4 Access point (AP) in WLAN

Wireless Local Area Network (WLAN) Attacks

- Rogue access point
  - An unauthorized access point that allows an attacker to bypass network security configurations
  - Usually set up by an insider (employee)
  - May be set up behind a firewall, opening the network to attacks
- Evil twin
  - AP set up by an attacker
  - Attempts to mimic an authorized AP
  - Attackers capture transmissions from users to evil twin AP
- Intercepting Wireless Data
  - Wireless traffic captured to decode and analyze packet contents by using a protocol analyzer
  - Network interface card (NIC) adapter must be in the correct mode in order for data to be captured

Wireless Local Area Network (WLAN) Attacks

- Wireless Replay Attack
  - Also known as “hijacking”
  - A passive attack in which the attacker captures transmitted wireless data, records it, and then sends it on to the original recipient without the attacker’s presence being detected
  - Can be accomplished using an evil twin AP
- Wireless Denial of Service Attack
  - RF jamming - attackers use intentional RF interference to flood the RF spectrum with enough interference to prevent a device from communicating with the AP
  - Spoofing - attackers craft a fictitious frame that pretends to come from a trusted client when it actually comes from the attacker
  - Manipulating duration field values - attackers send a frame with the duration field set to a high value, preventing other devices from transmitting for that period of time

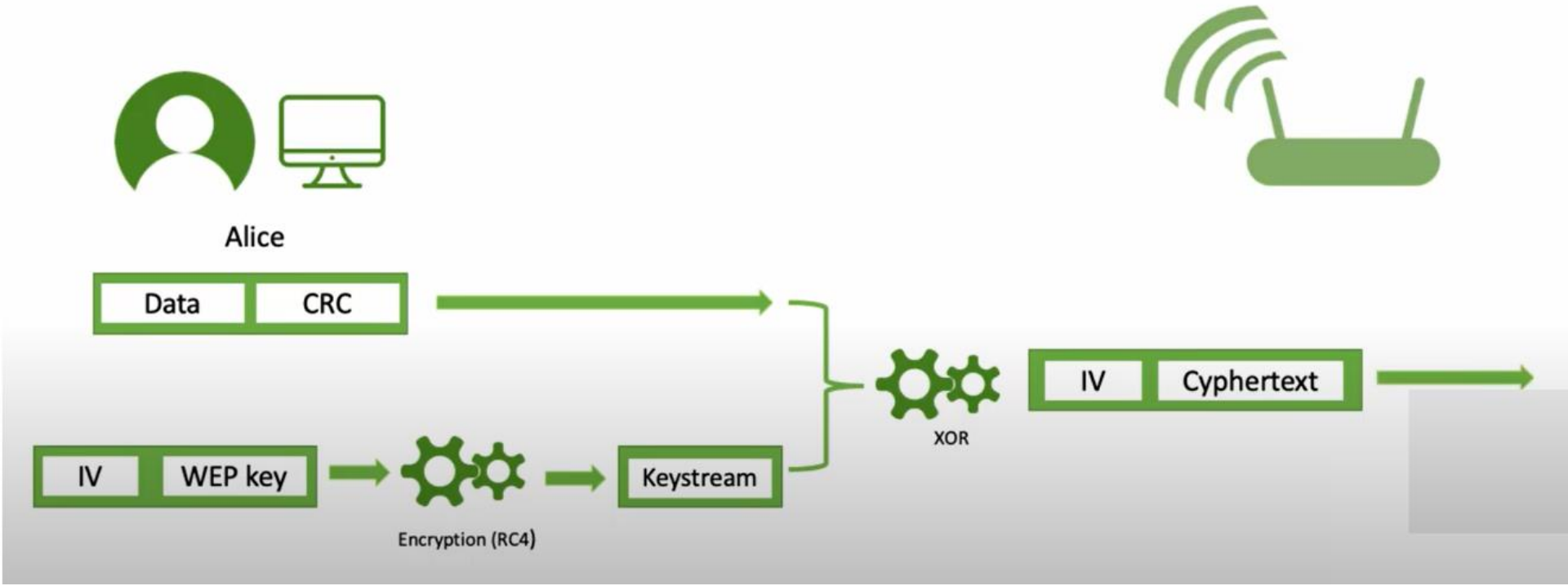
Vulnerabilities of IEEE 802.11 Security

- Original IEEE 802.11 committee recognized wireless transmissions could be vulnerable
  - Implemented several wireless security protections in the standard
  - Left others to WLAN vendor's discretion
  - Protections were vulnerable and led to multiple attacks

Wired Equivalent Privacy (WEP)

- IEEE 802.11 security protocol designed to ensure that only authorized parties can view transmissions
  - Encrypts plaintext into ciphertext
- Secret key is shared between wireless client device and AP
- WEP vulnerabilities
  - WEP can only use 64-bit or 128-bit number to encrypt
    - **Initialization vector (IV)** is only 24 of those bits
    - Short length makes it easier to break
  - Violates cardinal rule of cryptography: avoid a detectable pattern
    - Attackers can see duplication when IVs start repeating

802.11b WEP


Alice
Data
CRC
IV
WEP key
Encryption (RC4)
Keystream
XOR
IV
Cyphertext

WEP Notation - RC4

- RC4 (Rivest Cipher 4) is a stream cipher.
- RC4 generates a pseudorandom stream of bits (a keystream).
- It can be used for encryption by combining it with the plaintext using bit-wise exclusive-or; decryption is performed the same way (since exclusive-or with given data is an involution).
- This is similar to the one-time pad except that generated pseudorandom bits, rather than a prepared stream, are used.

WEP Notation - RC4

- To generate the keystream, the cipher makes use of a secret internal state which consists of two parts:
  - A permutation of all 256 possible bytes (denoted "S" below).
  - Two 8-bit index-pointers (denoted "i" and "j").

- The permutation is initialized with a variable length key, typically between 40 and 2048 bits, using the key-scheduling algorithm (KSA).
- Once this has been completed, the stream of bits is generated using the pseudo-random generation algorithm (PRGA).

WEP Notation - RC4

Key-scheduling algorithm (KSA):

- The key-scheduling algorithm is used to initialize the permutation in the array "S".
- "keylength" is defined as the number of bytes in the key and can be in the range $1 \leq \text{keylength} \leq 256$, typically between 5 and 16, corresponding to a key length of 40 – 128 bits.
- First, the array "S" is initialized to the identity permutation.
- S is then processed for 256 iterations in a similar way to the main PRGA, but also mixes in bytes of the key at the same time.

WEP Notation - RC4

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := (j + S[i] + key[i mod keylength]) mod 256
    swap values of S[i] and S[j]
endfor
```

WEP Notation - RC4

Pseudo-random generation algorithm (PRGA):

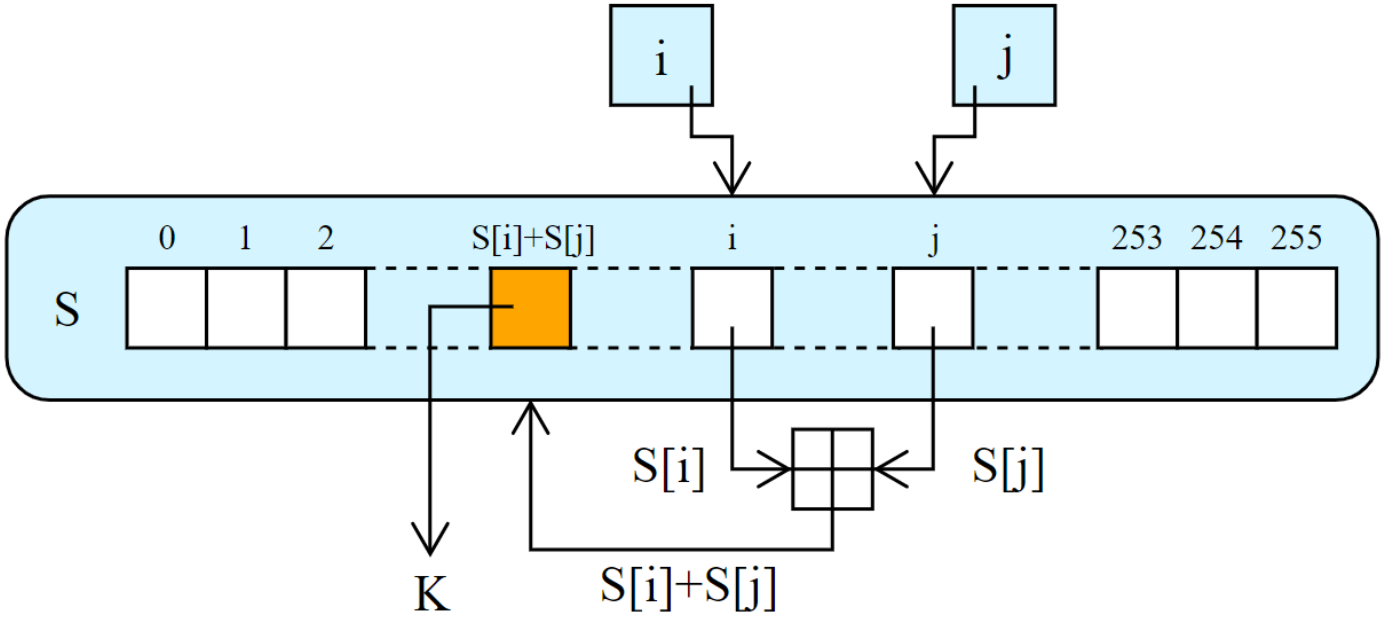
- For as many iterations as are needed, the PRGA modifies the state and outputs a byte of the keystream.
- In each iteration, the PRGA:
  - increments i
  - looks up the ith element of S, S[i], and adds that to j
  - exchanges the values of S[i] and S[j] then uses the sum S[i] + S[j] (modulo 256) as an index to fetch a third element of S (the keystream value K below)
  - then bitwise exclusive ORed (XORed) with the next byte of the message to produce the next byte of either ciphertext or plaintext.
  - Each element of S is swapped with another element at least once every 256 iterations.

WEP Notation - RC4

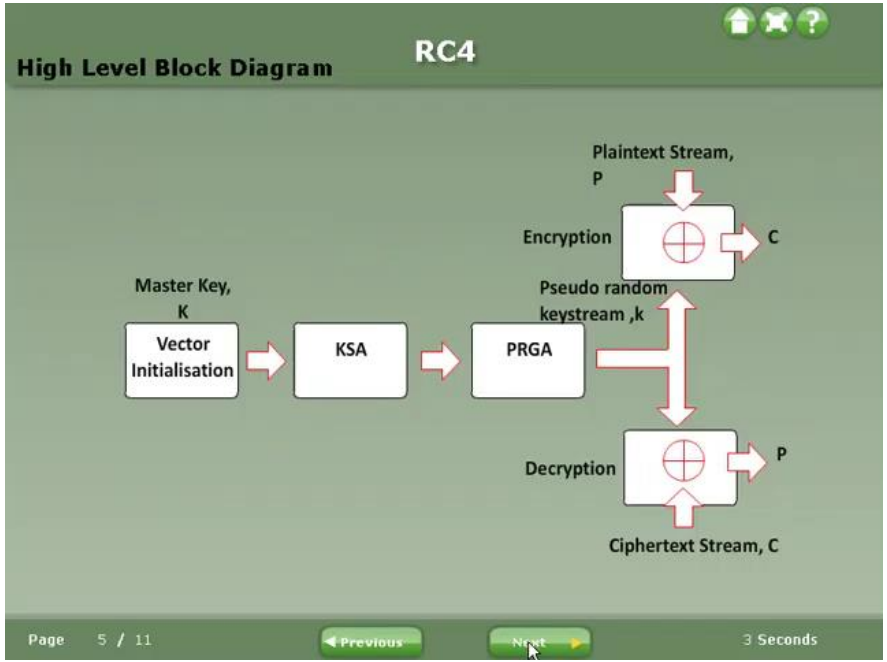
```
i := 0
j := 0
while GeneratingOutput:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap values of S[i] and S[j]
    K := S[(S[i] + S[j]) mod 256]
    output K
endwhile
```

- Thus, this produces a stream of K[0], K[1],... which are XOR'ed with the plaintext to obtain the ciphertext.
- So ciphertext[l] = plaintext[l] $\oplus$ K[l] .

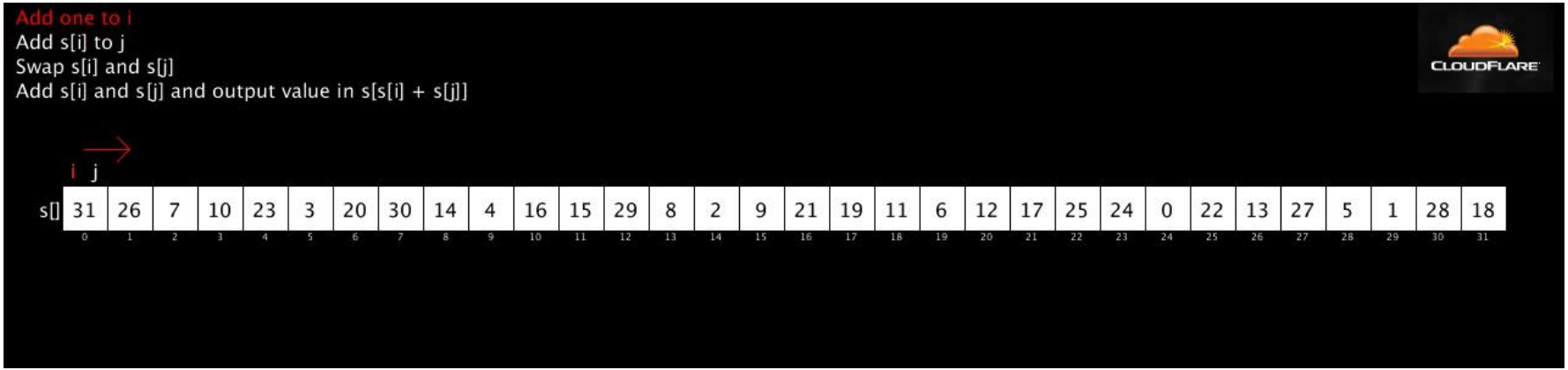
WEP Notation - RC4



WEP Notation - RC4



WEP Notation - RC4



WEP Notation

- WEP encryption uses the RC4 stream cipher. We let RC4(s) denote the pseudo random sequence generated by RC4 given the seed s.
- We let CRC(m) denote the 32-bit CRC checksum of a message $m \in \{0,1\}^*$. The details of CRC are irrelevant for our discussion and it suffices to view CRC as some fixed function from bit strings to $\{0,1\}^{32}$.

Let m be an 802.11b cleartext frame. The first few bits of m encode the length of m. To encrypt an 802.11b frame m the sender picks a 24-bit IV and computes:

$$c \leftarrow (m \parallel \text{CRC}(m)) \oplus \text{RC4}(\text{IV} \parallel k)$$
$$c_{\text{full}} \leftarrow (\text{IV},\ c)$$

WEP encryption process

The WEP encryption process is shown in Fig. 9.4. The receiver decrypts by first computing $c \oplus \text{RC4}(\text{IV} \parallel k)$ to obtain a pair (m, s). The receiver accepts the frame if $s = \text{CRC}(m)$ and rejects it otherwise.

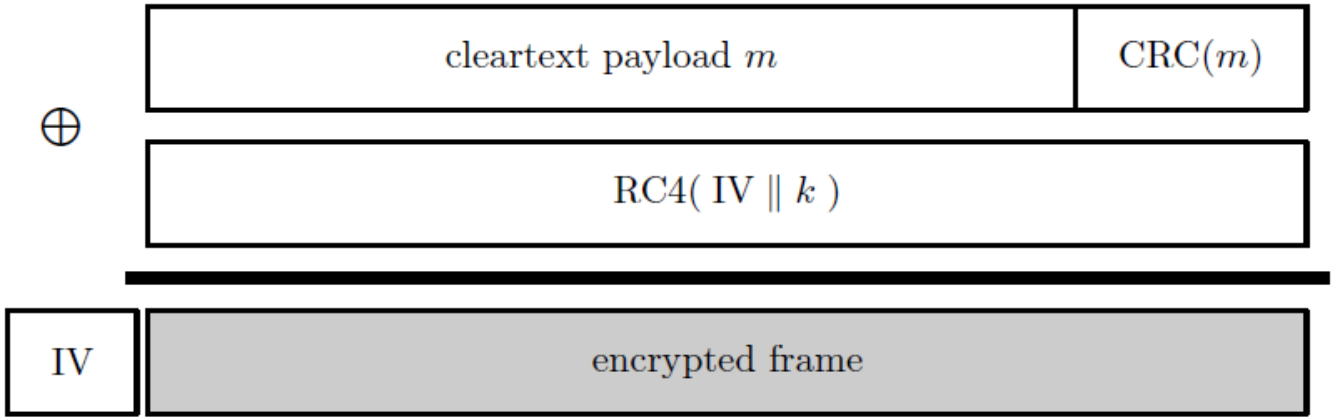


Figure 9.4: WEP Encryption

WEP Attacks

Attack 1: IV collisions. The designers of WEP understood that a stream cipher key should never be reused. Consequently, they used the 24-bit IV to derive a per-frame key $k_f := \text{IV} \parallel k$. The standard, however, does not specify how to choose the IVs and many implementations do so poorly. We say that an IV collision occurs whenever a wireless station happens to send two frames, say frame number i and frame number j, encrypted using the same IV. Since IVs are sent in the clear, an eavesdropper can easily detect IV collisions. Moreover, once an IV collision occurs the attacker can use the two-time pad attack discussed in Section 3.3.1 to decrypt both frames i and j.

So, how likely is an IV collision? By the birthday paradox, an implementation that chooses a random IV for each frame will cause an IV collision after only an expected $\sqrt{2^{24}} = 2^{12} = 4096$ frames. Since each frame body is at most 1156 bytes, a collision will occur after transmitting about 4MB on average.

WEP Attacks

Attack 2: related keys. A far more devastating attack on WEP encryption results from the use of related RC4 keys. In Chapter 3 we explained that a new and *random* stream cipher key must be chosen for every encrypted message. WEP, however, uses keys $1 \| k$, $2 \| k, \ldots$ which are all closely related — they all have the same suffix k. RC4 was never designed for such use, and indeed, is completely insecure in these settings. Fluhrer, Mantin, and Shamir [59] showed that after about a million WEP frames are sent, an eavesdropper can recover the entire long term secret key k. The attack was implemented by Stubblefield, Ioannidis, and Rubin [138] and is now available in a variety of hacking tools such as WEPCRACK and AIRSNORT.

Generating per frame keys should have been done using a PRF, for example, setting the key for frame i to $k_i := F(k, \text{IV})$ — the resulting keys would be indistinguishable from random, independent keys. Of course, while this approach would have prevented the related keys problem, it would not solve the IV collision problem discussed above, or the malleability problem discussed next.

WEP Attacks

Attack 3: malleability. Recall that WEP attempts to provide authenticated encryption by using a CRC checksum for integrity. In a sense, WEP uses the MAC-then-encrypt method, but it uses CRC instead of a MAC. We show that despite the encryption step, this construction utterly fails to provide ciphertext integrity.

The attack uses the linearity of CRC. That is, given $\mathrm{CRC}(m)$ for some message m, it is easy to compute $\mathrm{CRC}(m \oplus \Delta)$ for any Δ. More precisely, there is a public function L such that for any m and $\Delta \in \{0,1\}^{\ell}$ we have that

$$\mathrm{CRC}(m \oplus \Delta) = \mathrm{CRC}(m) \oplus L(\Delta)$$

This property enables an attacker to make arbitrary modifications to a WEP ciphertext without ever being detected by the receiver. Let c be a WEP ciphertext, namely

$$c = \big(m, \mathrm{CRC}(m)\big) \;\oplus\; \mathrm{RC4}(\mathrm{IV} \,\|\, k)$$

WEP Attacks

For any $\Delta \in \{0,1\}^{\ell}$, an attacker can create a new ciphertext $c' \leftarrow c \oplus (\Delta, L(\Delta))$, which satisfies

$$\begin{aligned} c' &= \text{RC4}(\text{IV} \,\|\, k) \oplus (m,\ \text{CRC}(m)) \oplus (\Delta,\ L(\Delta)) = \\ &\quad \text{RC4}(\text{IV} \,\|\, k) \oplus (m \oplus \Delta,\ \text{CRC}(m) \oplus L(\Delta)) = \\ &\quad \text{RC4}(\text{IV} \,\|\, k) \oplus (m \oplus \Delta,\ \text{CRC}(m \oplus \Delta)) \end{aligned}$$

Hence, c' decrypts without errors to $m \oplus \Delta$. We see that given the encryption of m, an attacker can create a valid encryption of $m \oplus \Delta$ for any Δ of his choice. We explained in Section 3.3.2 that this can lead to serious attacks.

Attack 4: Chosen ciphertext attack. The protocol is vulnerable to a chosen ciphertext attack called **chop-chop** that lets the attacker decrypt an encrypted frame of its choice. We describe a simple version of this attack in Exercise 9.5.

WEP Attacks

Attack 5: Denial of Service. We briefly mention that 802.11b suffers from a number of serious Denial of Service (DoS) attacks. For example, in 802.11b a wireless client sends a "disassociate" message to the wireless station once the client is done using the network. This allows the station to free memory resources allocates to that client. Unfortunately, the "disassociate" message is unauthenticated, allowing anyone to send a disassociate message on behalf of someone else. Once disassociated, the victim will take a few seconds to re-establish the connection to the base station. As a result, by sending a single "disassociate" message every few seconds, an attacker can prevent a computer of their choice from connecting to the wireless network. These attacks are implemented in 802.11b tools such as `Void11`.

- A type of DoS attack in which the attacker breaks the wireless connection between the victim device and the access point. The method is based on the use of a special disassociation frame specified under IEEE 802.11. Transferring such a frame to the target device breaks the connection, and the Wi-Fi protocol does not require any encryption for it. For a successful attack, the cybercriminal needs to know only the victim's MAC address.

Wi-Fi Protected Setup (WPS)

- WPS is an optional means of configuring security on WLANS
- Two common WPS methods:
  - PIN method - utilizes a PIN printed on a sticker of the wireless router or displayed through a software wizard
  - Push-button method - user pushes buttons and security configuration takes place
- Design and implementation flaws:
  - There is no lockout limit for entering PINs
  - The last PIN character is only a checksum

MAC Address Filtering

- Method of controlling WLAN access
  - Limit a device's access to AP
- Media Access Control (MAC) address filtering
  - Used by nearly all wireless AP vendors
  - Permits or blocks device based on MAC address
- Vulnerabilities of MAC address filtering
  - Addresses exchanged in unencrypted format : Attacker can see address of approved device and substitute it on his own device
  - Managing large number of addresses is challenging

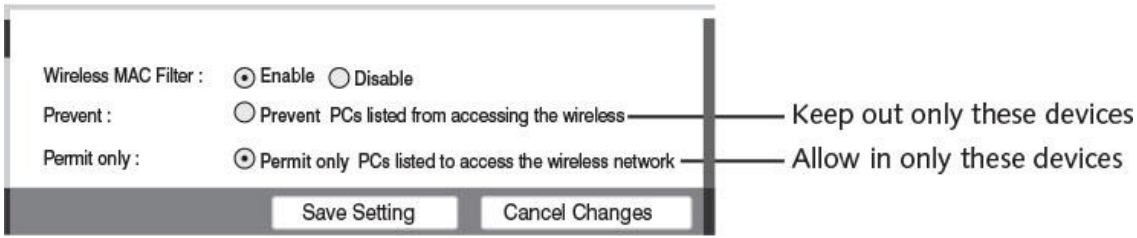


Figure 9-10 MAC address filtering

Disabling SSID Broadcasts

- Each device must be authenticated prior to connecting to the WLAN
- Service Set Identifier (SSID)
  - The user-supplied network name of a wireless network; usually broadcast so that any device can see it: The broadcast can be restricted
  - Some wireless security sources encourage users to configure their APs to prevent the broadcast of the SSID
- Not advertising the SSID only provides a weak degree of security and has limitations:
  - SSID can be discovered when transmitted in other frames
  - May prevent users from being able to freely roam from one AP coverage area to another
  - It's not always possible to turn off SSID beaconing

Wireless Security Solutions

- A unified approach to WLAN security was needed
  - IEEE and Wi-Fi Alliance began developing security solutions
- Resulting standards used today
  - IEEE 802.11i
  - WPA and WPA2

802.11i

- Following the failures of the 802.11b WEP protocol, a new standard called 802.11i was ratified in 2004.
- 802.11i provides authenticated encryption using a MAC-then-encrypt mode called CCM.
- In particular, CCM uses (raw) CBC-MAC for the MAC and counter mode for encryption.
- Both are implemented in 802.11i using AES as the underlying PRF. CCM was adopted by NIST as a federal standard.

Wi-Fi Protected Access (WPA)

- A subset of IEEE 802.11i
  - Introduced in 2003 by the Wi-Fi Alliance
- Temporal Key Integrity Protocol (TKIP) Encryption
  - Used in WPA
  - Uses a longer 128 bit key than WEP
  - Dynamically generated for each new packet
  - Includes a *Message Integrity Check (MIC),* designed to prevent man-in-the-middle attacks

Wi-Fi Protected Access (WPA)

- Pre-shared Key (PSK) Authentication
  - After AP configured, client device must have same key value entered
  - Key is shared prior to communication taking place
  - Uses a passphrase to generate encryption key
    - Must be entered on each AP and wireless device in advance
  - Not used for encryption
    - Serves as starting point for mathematically generating the encryption keys

Wi-Fi Protected Access (WPA)

- WPA Vulnerabilities
  - Key management
    - Key sharing is done without security protection
    - Keys must be changed on a regular basis
    - Key must be disclosed to guest users
  - Passphrases
    - PSK passphrases of fewer than 20 characters subject to cracking

Wi-Fi Protected Access 2 (WPA2)

- Second generation of WPA is known as WPA2
- WPA2 mandates the use of a new protocol, Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP).
- CCMP uses the AES block cipher, replacing the RC4 cipher used in Wired Equivalent Privacy (WEP) and Temporal Key Integrity Protocol (TKIP).
    - A block cipher processes data in blocks, while a streaming cipher like Rivest Cipher 4 (RC4) processes data bit by bit, in a serial stream.
- The encryption method is commonly referred to as CCMP/AES.
    - AES uses a 128-bit key and encrypts data in 128-bit blocks.
- CCMP/AES uses several enhancements, including temporal keys (TK), packet numbers (PN), nonce [number or bit string used only once], upper layer encryption, and additional authentication data (AAD).

Wi-Fi Protected Access 2 (WPA2)

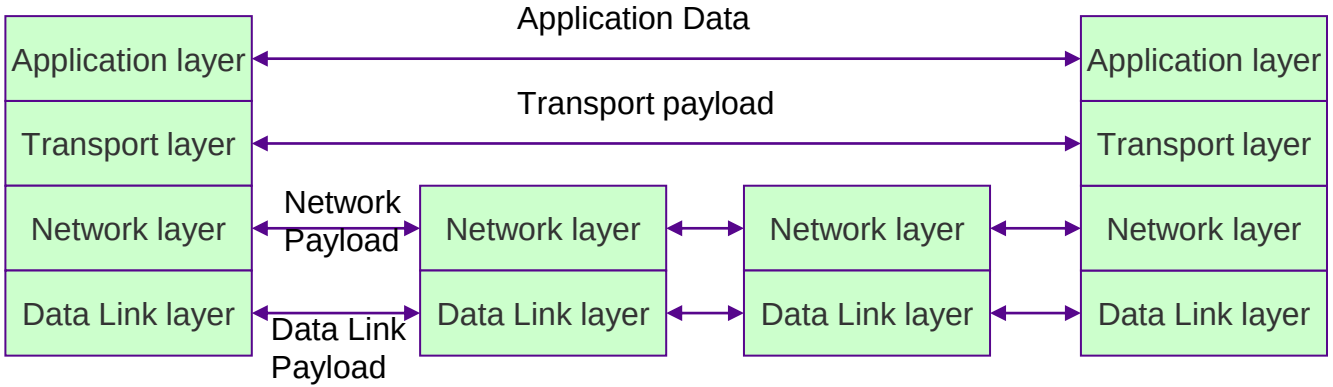
- **AES** is a standard and not a protocol.
  - A protocol is a series of steps designed to achieve a specific end,
  - while a standard is a set of rules and guidelines that define an overall design structure.
- The AES standard specifies the use of the Rijandel symmetric block cipher that can process data blocks of 128 bits, using cipher keys of 128, 192, and 256 bits.

- **CCMP** is a security protocol.
  - It uses a block cipher, as previously noted.
- CCMP is made up of different specialized components providing specific functions.
  - Counter-mode is used to provide data privacy, while Cipher Block Chaining Message Authentication Code (CBC-MAC) is used for authentication and data integrity.
- CCMP uses one temporal key to accomplish all encryption processes.

IPsec

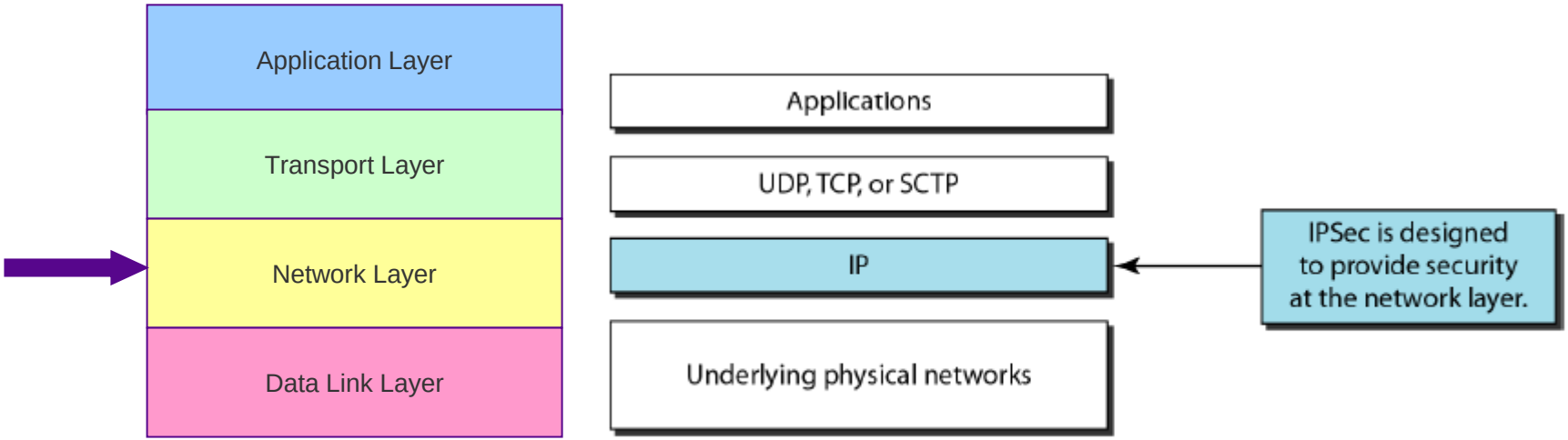
Network Layer

- Routing (routers): determine the path a packet has to traverse to reach its destination
- Defines addressing mechanism
  - Hosts should conform to the addressing mechanism



IPsec

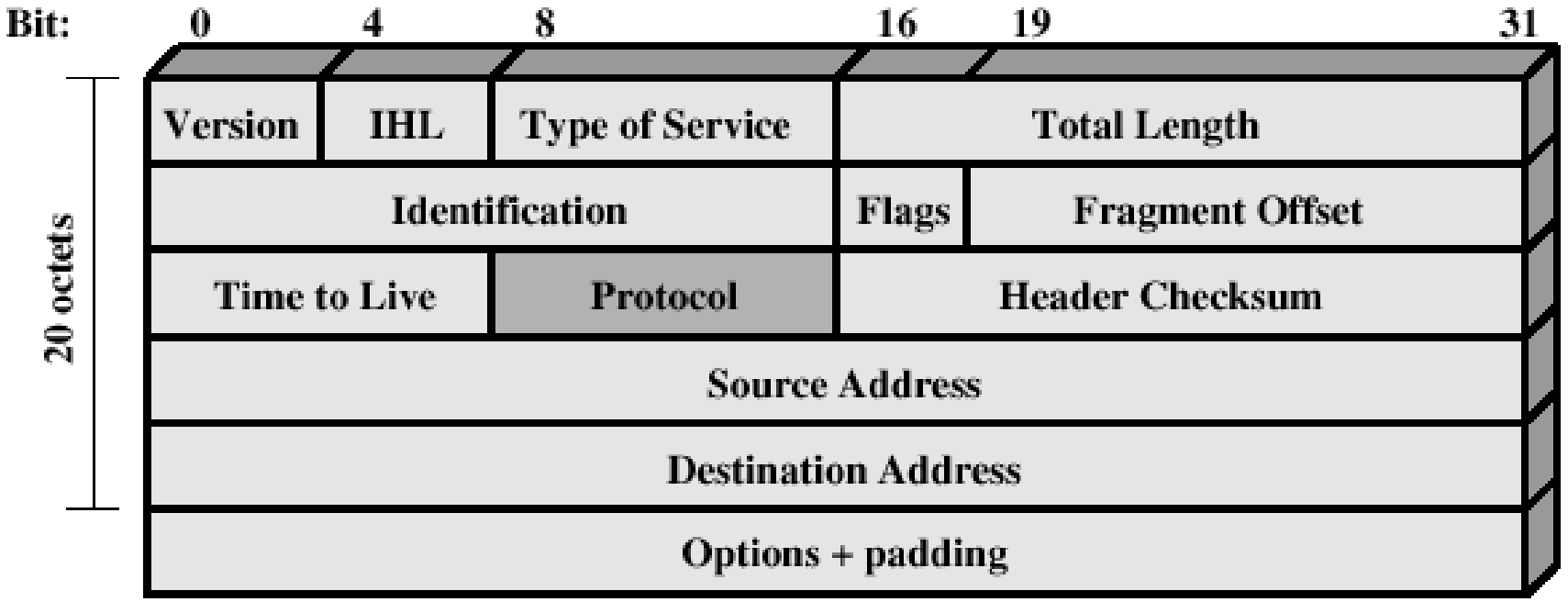
- IPSec is not a single protocol. Instead, IPSec provides a set of security algorithms plus a general framework that allows a pair of communicating entities to use whichever algorithms provide security appropriate for the communication.



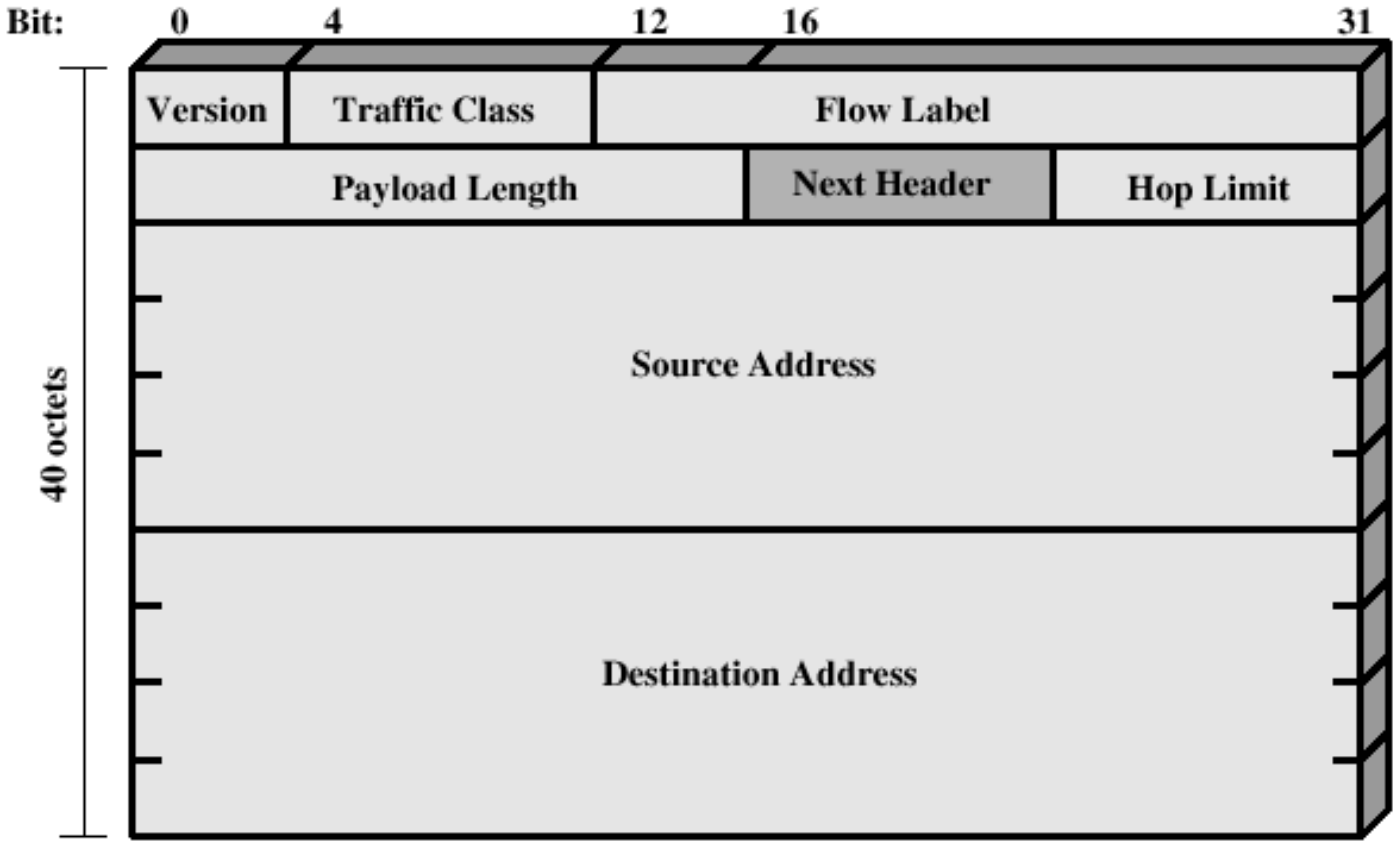
IPv4 & IPv6

- IP protocol version 4 (IPv4)
  - Developed in 1981
  - Number of available IP address is limited to 4.3 billion
    - This is no longer sufficient for the number of devices that are connected to the Internet
  - Has security weaknesses
- Internet Protocol version 6 (IPv6)
  - Next generation of IP protocol
  - Addresses weaknesses of IPv4
- IPv6 provides enhanced security features
  - Cryptographic protocols provide secure data communication
  - New authentication headers prevent IP packets from being altered

IPv4


Bit:
0
4
8
16
19
31
20 octets
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options + padding

IPv6


Bit:
0
4
12
16
31
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address
40 octets

IPv6

IPv4 field name	IPv6 field name	Explanation
Internet Header Length (IHL)	Not used	IPv6 uses a fixed packet header size of 40 bytes, so information always appears in the same place. This is a much smaller header size than IPv4 because packets contain only the header information that they need. The smaller size speeds up finding information in the packet and processing the packet.
Type of Service	Traffic Class	Currently there are no standard requirements for the content of this field.
Not Used	Flow Label	Packets belonging to the same stream, session, or flow share a common flow value, making it more easily recognizable without looking deeper into the packet.
Total Length	Payroll Length	Payroll Length, which includes any additional headers, no longer includes the length of the header (as in IPv4), so the host or router does not need to check if the packet is large enough to hold the IP header.
Time to Live (TTL)	Hop Limit	TTL was a misnomer because it never contained an actual time value.
Protocol	Next Header	This indicates the type of header that follows.
Source Address and Destination Address	Source Address and Destination Address	These serve the same function in IPv6 except they are expanded from 32 bits to 128 bits.

Table 8-3 Comparison of IPv4 and IPv6 headers

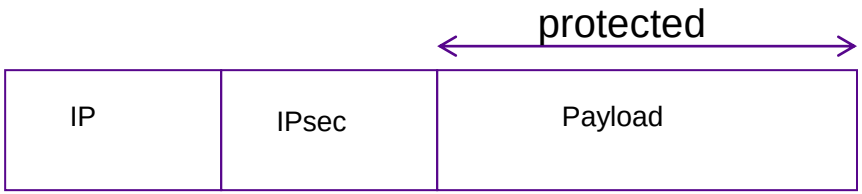
IP Security

- **IPSec Services:**
  - Data origin authentication
  - Connectionless data integrity authentication
  - Data content confidentiality
  - Access Control
  - Rejection of replayed packets
  - Limited traffic flow confidentiallity

- **Benefits of IPSec:**
  - Transparent to applications (below transport layer (TCP, UDP)
  - Provide security for individual users
  - A router or neighbor advertisement comes from an authorized router
  - A redirect message comes from the router to which the initial packet was sent
  - A routing update is not forged

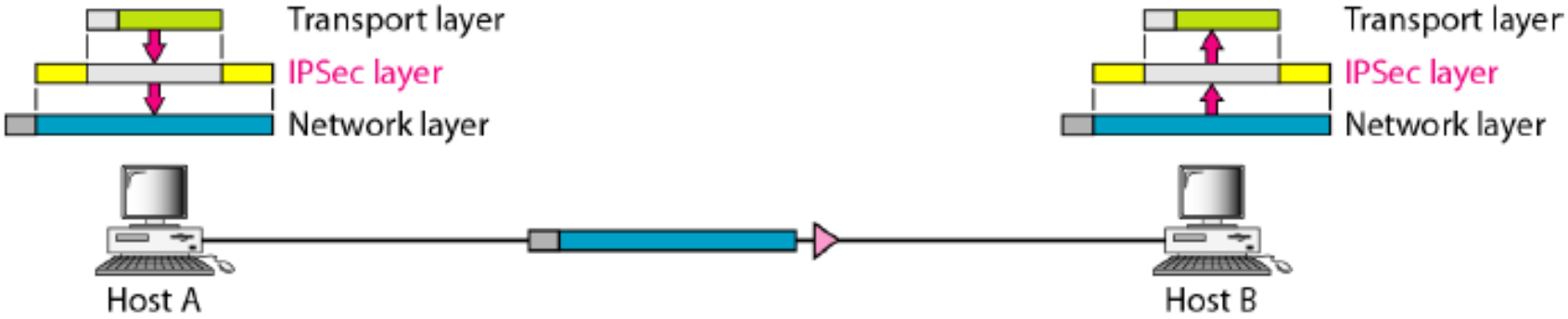
Transport mode

- Transport mode: protect upper layer protocols
  - IPSec header is inserted between the IP header and the upper-layer protocol header
  - Communication endpoints must be cryptographic endpoints



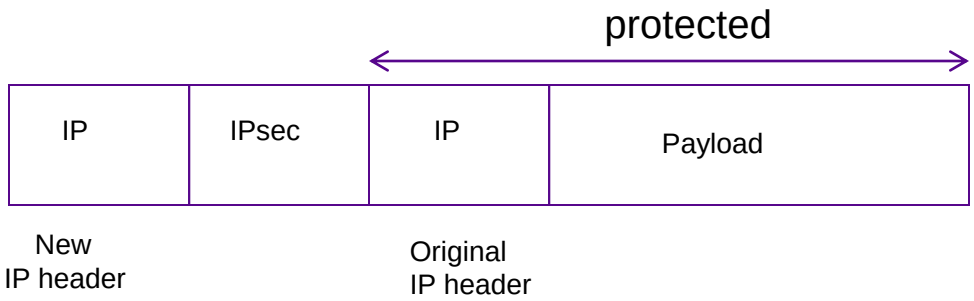
IPsec (Transport mode)

- IPSec in the transport mode does not protect the IP header; it only protects the information coming from the transport layer.



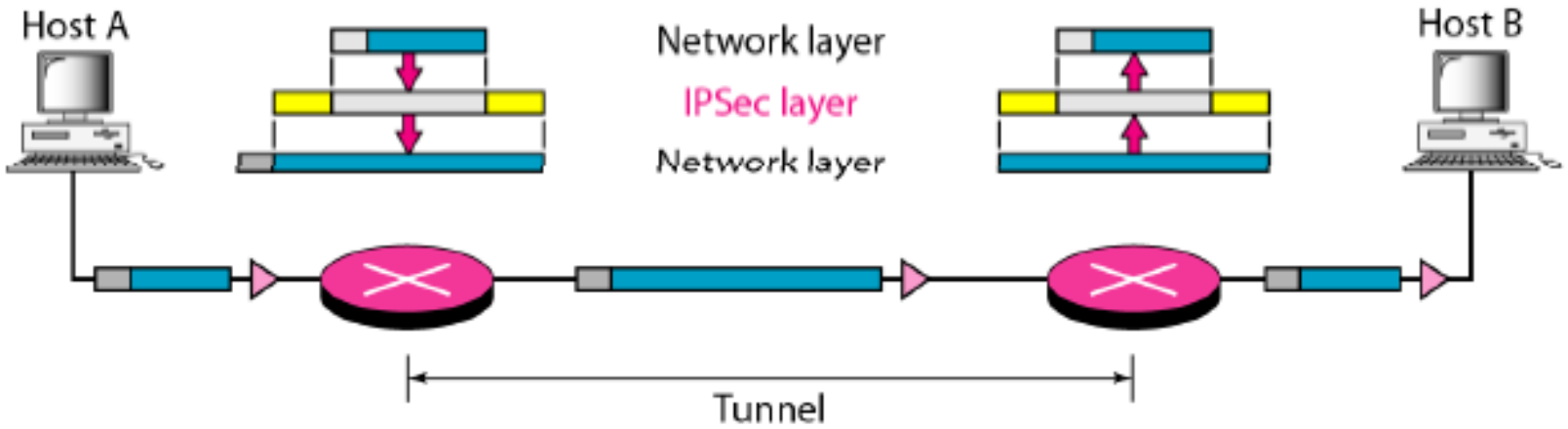
Tunnel mode

- Tunnel mode: protect entire IP datagram
  - Entire IP packet to be protected is encapsulated in another IP datagram and an IPsec header is inserted between the outer and inner IP headers

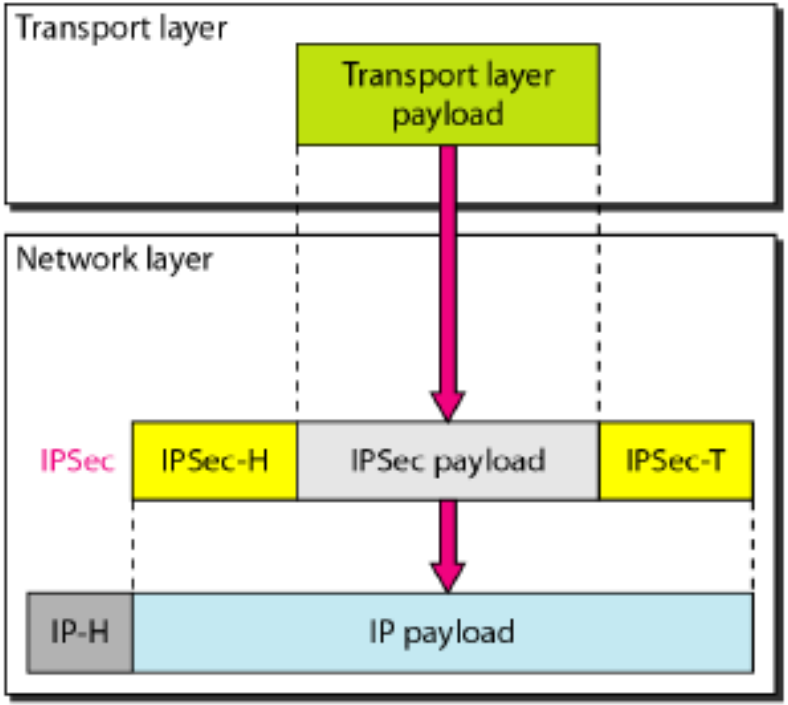


IPsec (Tunnel mode)

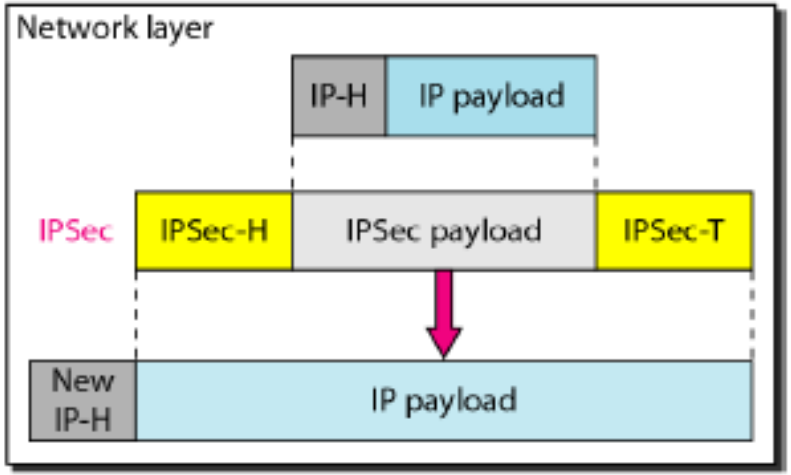
- IPSec in tunnel mode protects the original IP header.



IPsec



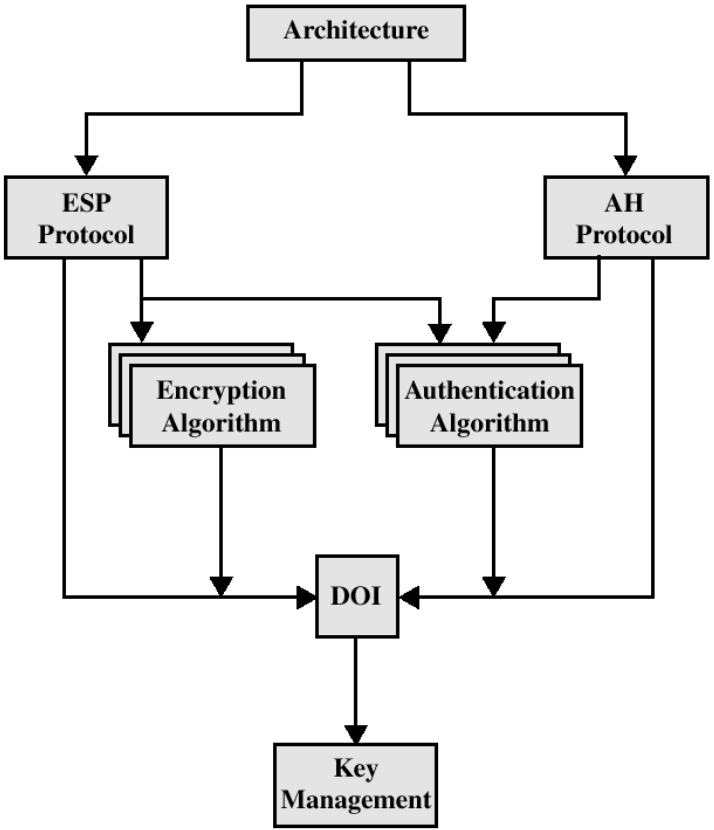
a. Transport mode



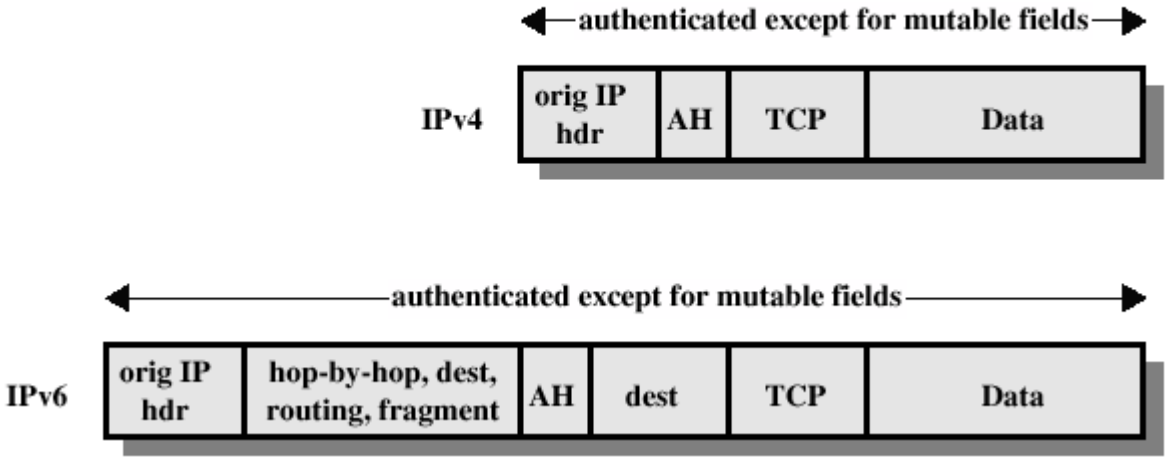
b. Tunnel mode

IPSec Protocols

- *Encapsulating Security Payload (ESP)*
  - Proof of data origin, data integrity, anti-replay protection
  - Data confidentiality and limited traffic flow confidentiality
- *Authentication Header (AH)*
  - Proof of data origin, data integrity, anti-replay protection

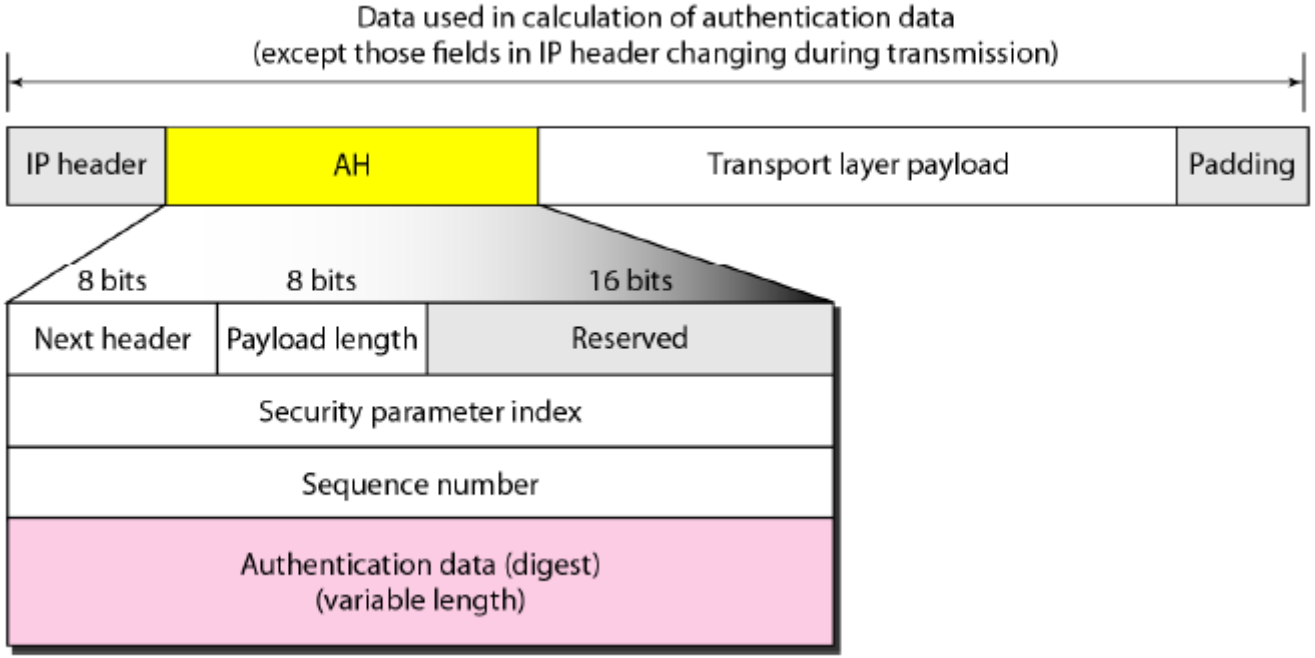


Transport Mode (AH Authentication)

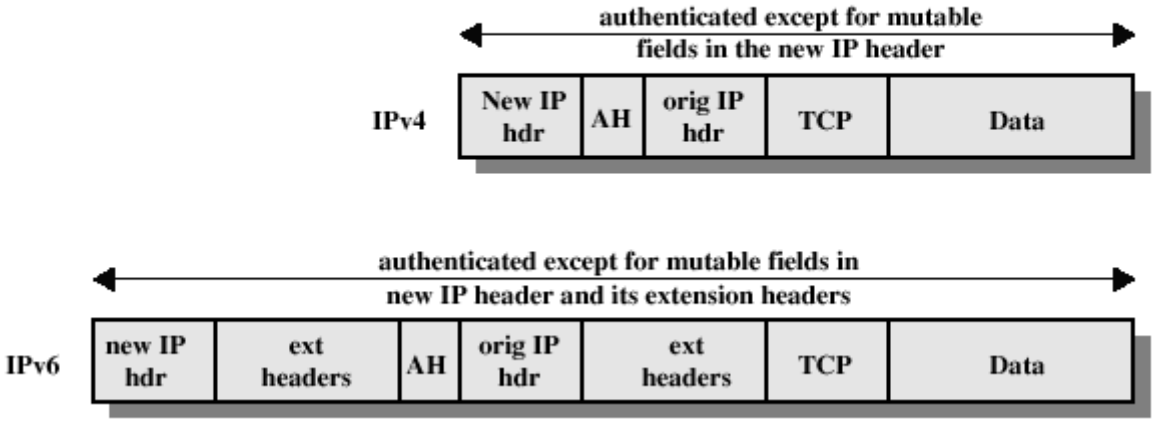


Authentication Header (AH) Protocol in Transport Mode

- The AH Protocol provides source authentication and data integrity, but not privacy. It also support for data integrity and authentication (MAC code) of IP packets and guards against replay attacks. It may provide Non-repudiation.



Tunnel Mode (AH Authentication)



Encapsulating Security Payload (ESP)

- ESP provides
  - Confidentiality,
  - Authentication
  - Limited traffic flow confidentiality,
  - Anti-replay protection.
- ESP packet processing:
  - Verify sequence number,
  - Verify integrity,
  - Decrypt
- ESP header is not encrypted
  - Contains: SPI and sequence number
- ESP trailer is partially encrypted
  - Contains: padding, length of padding, next protocol, authentication data

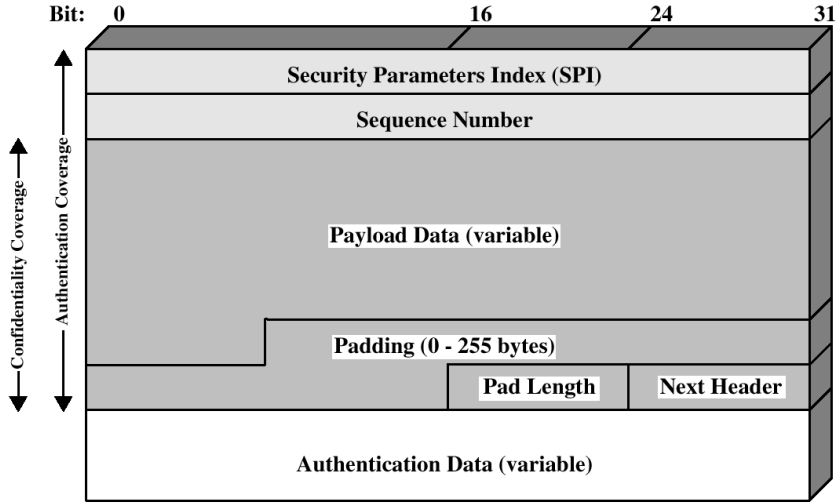
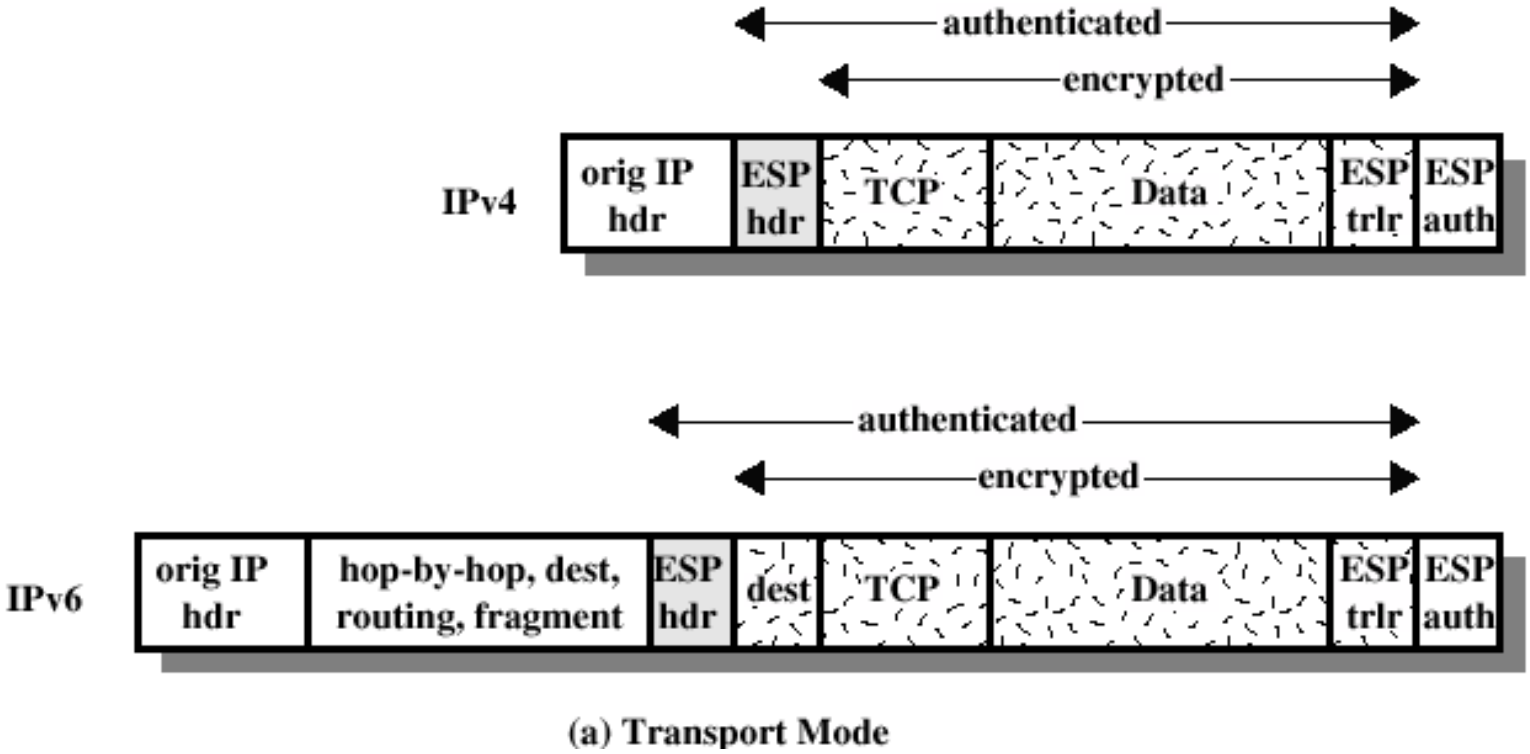


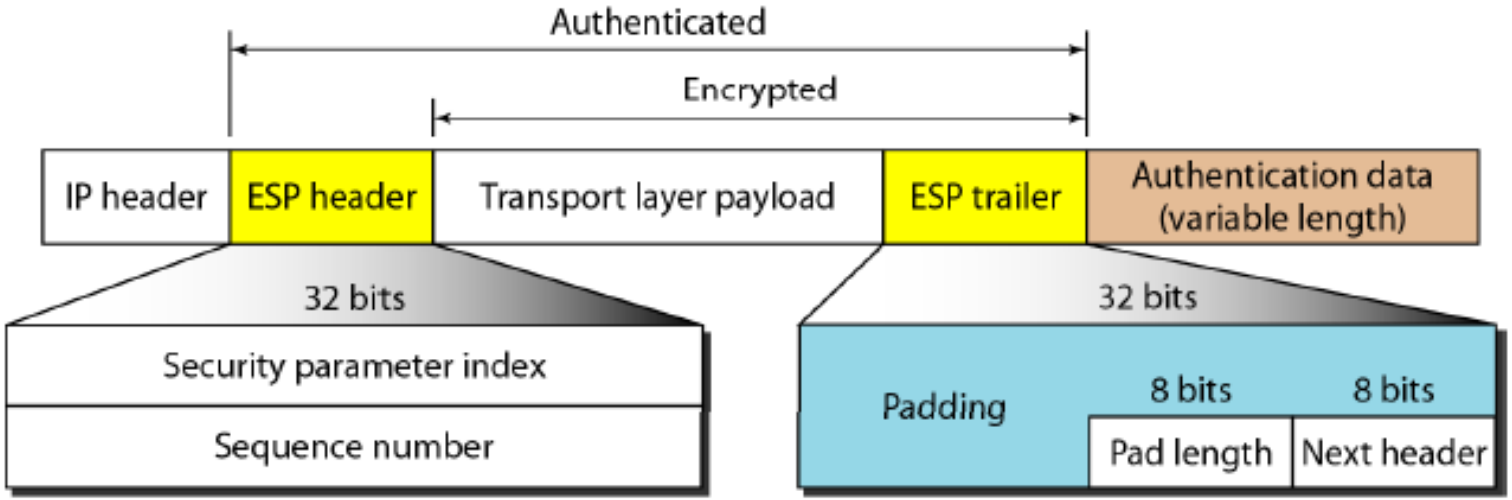
Figure 6.7 IPSec ESP Format

Transport Mode (ESP Encryption and Authentication)

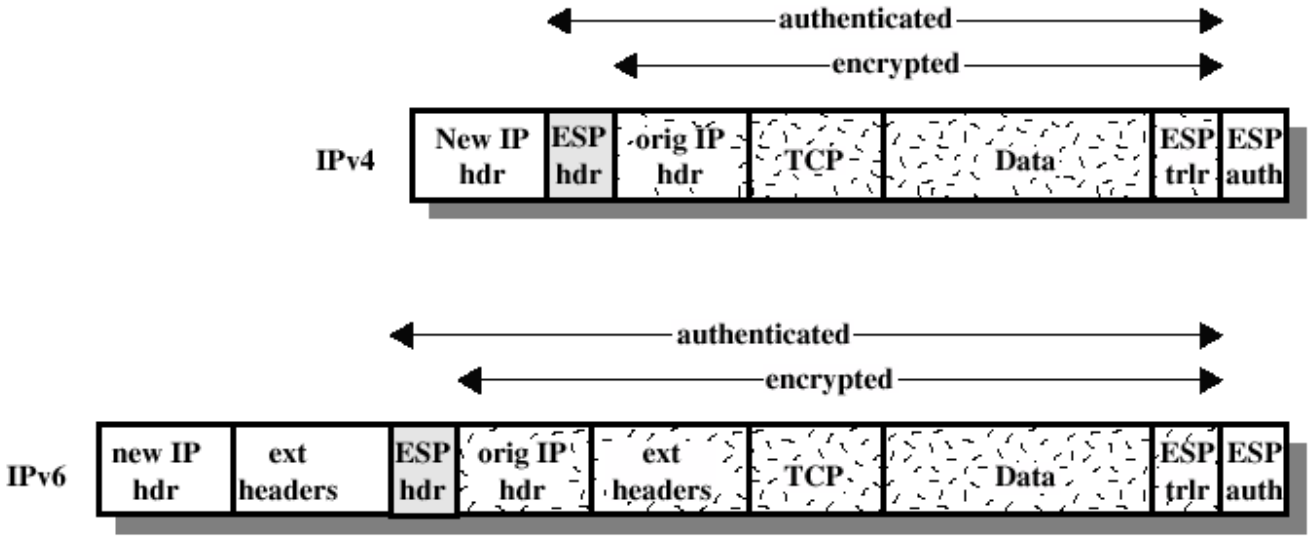


(a) Transport Mode

Encapsulating Security Payload (ESP) Protocol in Transport Mode



Tunnel Mode (ESP Encryption and Authentication)



(b) Tunnel Mode

IPsec

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers	Authenticates entire inner IP packet plus selected portions of outer IP header
ESP	Encrypts IP payload and any IPv6 extesion header	Encrypts inner IP packet
ESP with authentication	Encrypts IP payload and any IPv6 extesion header. Authenticates IP payload but no IP header	Encrypts inner IP packet. Authenticates inner IP packet.

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

Security Association

- Defines *security services* and *mechanisms* between two end points (or IPsec modules):
  - Hosts
  - Network security gateways (e.g., routers, application gateways)
  - Hosts and security gateways
- Security service, parameters, mode of operation, and initialization vector
  - e.g., Confidentiality using ESP with DES in CBC mode with IV initialization vector
- May use either Authentication Header (AH) or Encapsulating Security Payload (ESP) but not both → if both AH and ESP are applied, need two SAs

Encryption Algorithms

- AES (Advanced Encryption Standard) — AES is the strongest encryption algorithm available. (AES encryption keys of these lengths: 128, 192, or 256 bits.)
- 3DES (Triple-DES) — An encryption algorithm based on DES that uses the DES cipher algorithm three times to encrypt the data. The encryption key is 168-bit.
- DES (Data Encryption Standard) — Uses an encryption key that is 56 bits long. DES is the weakest of the three algorithms, and it is considered to be insecure.

Authentication Algorithms

- HMAC-MD5 (Hash Message Authentication Code — Message Digest Algorithm 5)
  - MD5 produces a 128-bit (16 byte) message digest, which makes it faster than SHA1 or SHA2. This is the least secure algorithm.
- HMAC-SHA1 (Hash Message Authentication Code — Secure Hash Algorithm 1)
  - SHA1 produces a 160-bit (20 byte) message digest. Although slower than MD5, this larger digest size makes it stronger against brute force attacks. SHA-1 is considered to be mostly insecure because of a vulnerability.
- HMAC-SHA2 (Hash Message Authentication Code — Secure Hash Algorithm 2)
- SHA2 is the most secure algorithm.
  - SHA2-256 — produces a 265-bit (32 byte) message digest
  - SHA2-384 — produces a 384-bit (48 byte) message digest
  - SHA2-512 — produces a 512-bit (64 byte) message digest
- SHA2 is stronger than either SHA1 or MD5.

Simple inbound and outbound security associations