MCA : MCA23203

CRYPTOGRAPHY
&
NETWORK SECURITY

UNIT - 5

Unit-5: IP Security and wireless Network Security

IP Security : Architecture – Authentication Header – Encapsulating security payloads – Combining Security Associations – Wireless Network Security: Wireless Security – Mobiles Device Security

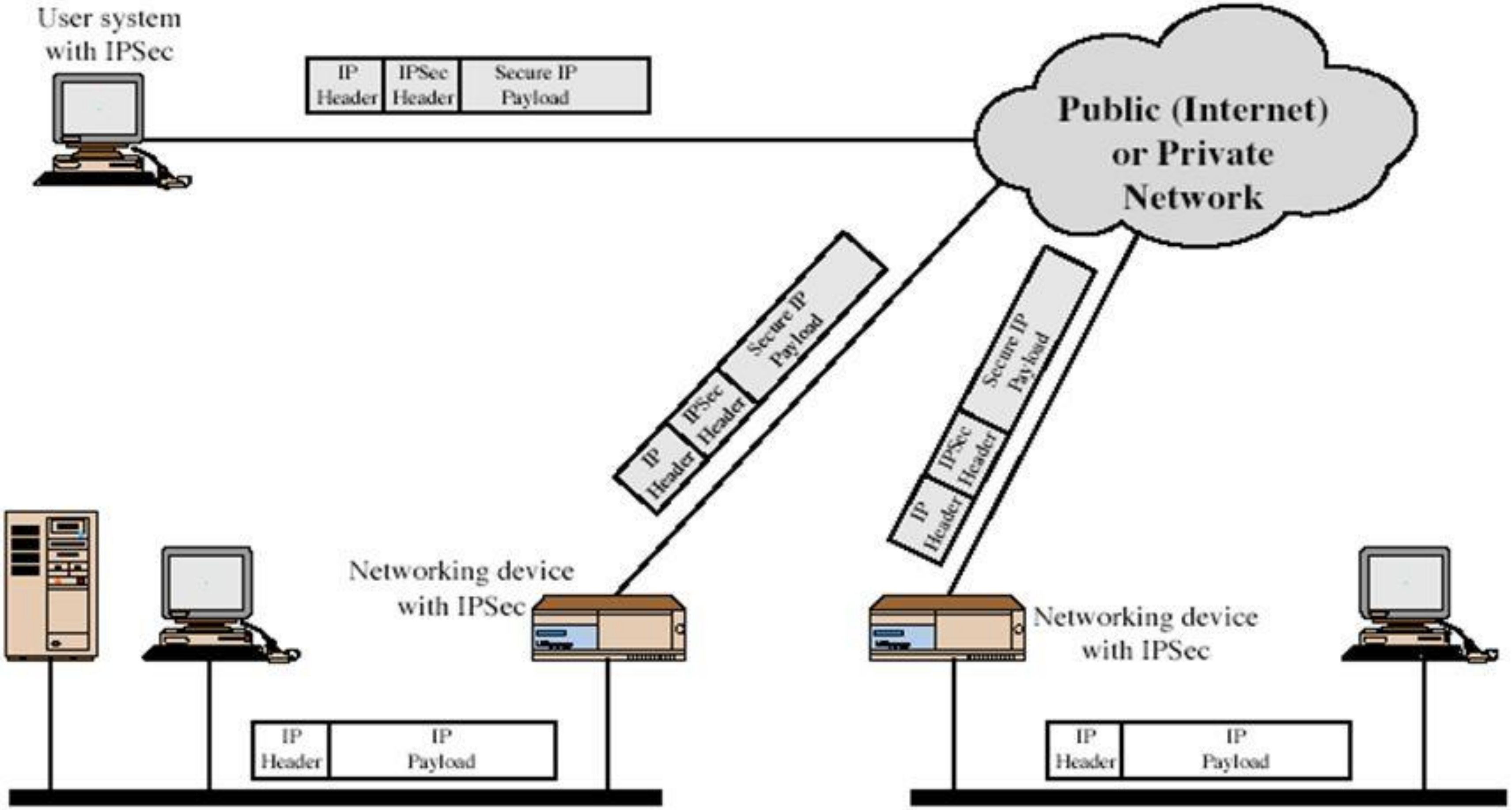
IP Security

- have considered some application specific security mechanisms
  - eg. S/MIME, PGP, Kerberos, SSL/HTTPS
- however there are security concerns that cut across protocol layers
- would like security implemented by the network for all applications

IPSec

- general IP Security mechanisms
- provides
  - authentication
  - confidentiality
  - key management
- applicable to use over LANs, across public & private WANs, & for the Internet

IPSec Uses


User system with IPSec
IP Header
IPSec Header
Secure IP Payload
Public (Internet) or Private Network
IP Header
IPSec Header
Secure IP Payload
IP Header
IPSec Header
Secure IP Payload
Networking device with IPSec
Networking device with IPSec
IP Header
IP Payload
IP Header
IP Payload

Benefits of IPSec

- in a firewall/router provides strong security to all traffic crossing the perimeter
- is resistant to bypass
- is below transport layer, hence transparent to applications
- can be transparent to end users
- can provide security for individual users if desired

IP Security Architecture

- specification is quite complex
- defined in numerous RFC’s
  - incl. RFC 2401/2402/2406/2408
  - many others, grouped by category
- mandatory in IPv6, optional in IPv4

IPSec Services

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
  - a form of partial sequence integrity
- Confidentiality (encryption)
- Limited traffic flow confidentiality

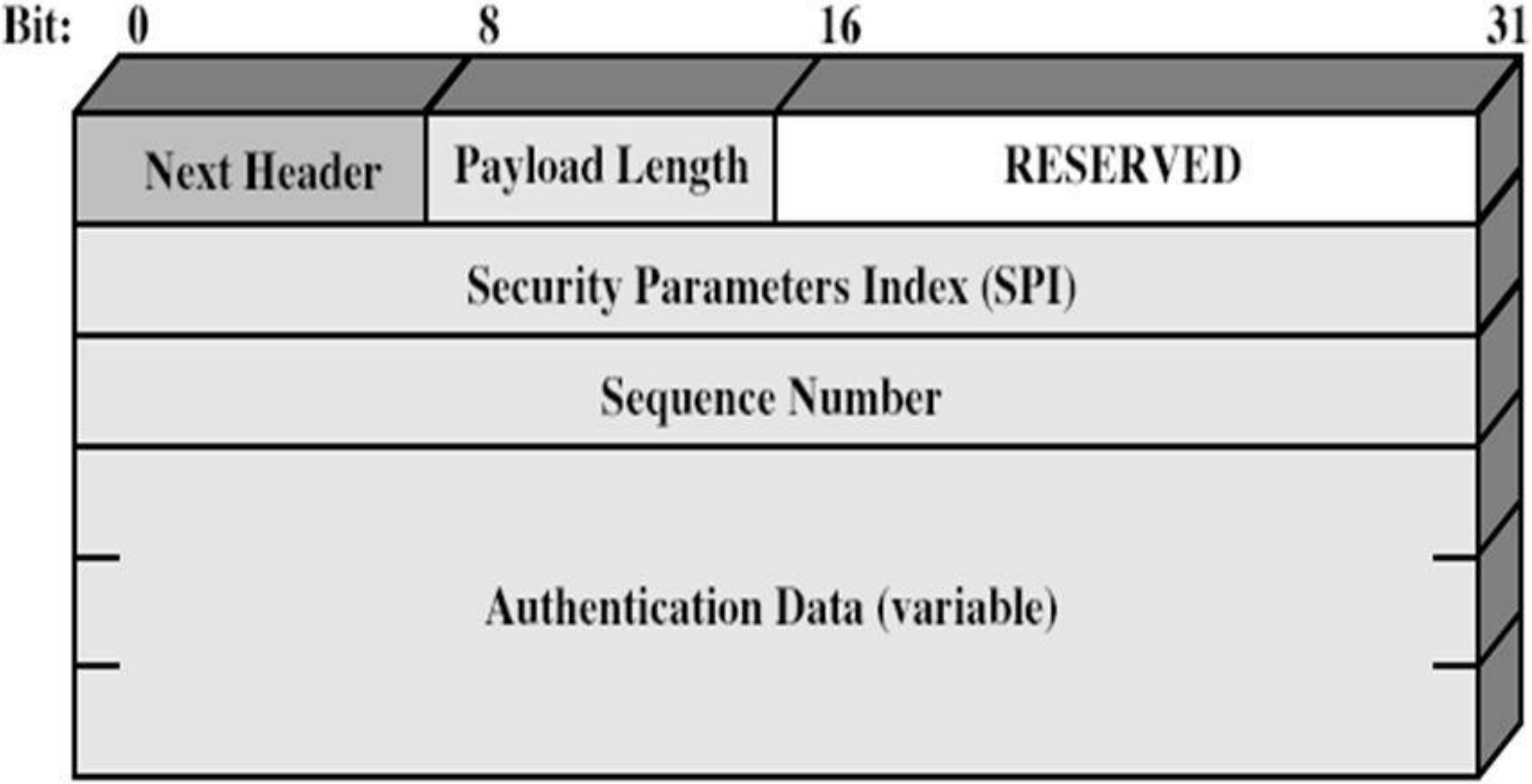
Security Associations

- a one-way relationship between sender & receiver that affords security for traffic flow
- defined by 3 parameters:
  - Security Parameters Index (SPI)
  - IP Destination Address
  - Security Protocol Identifier
- has a number of other parameters
  - seq no, AH & EH info, lifetime etc
- have a database of Security Associations

Authentication Header (AH)

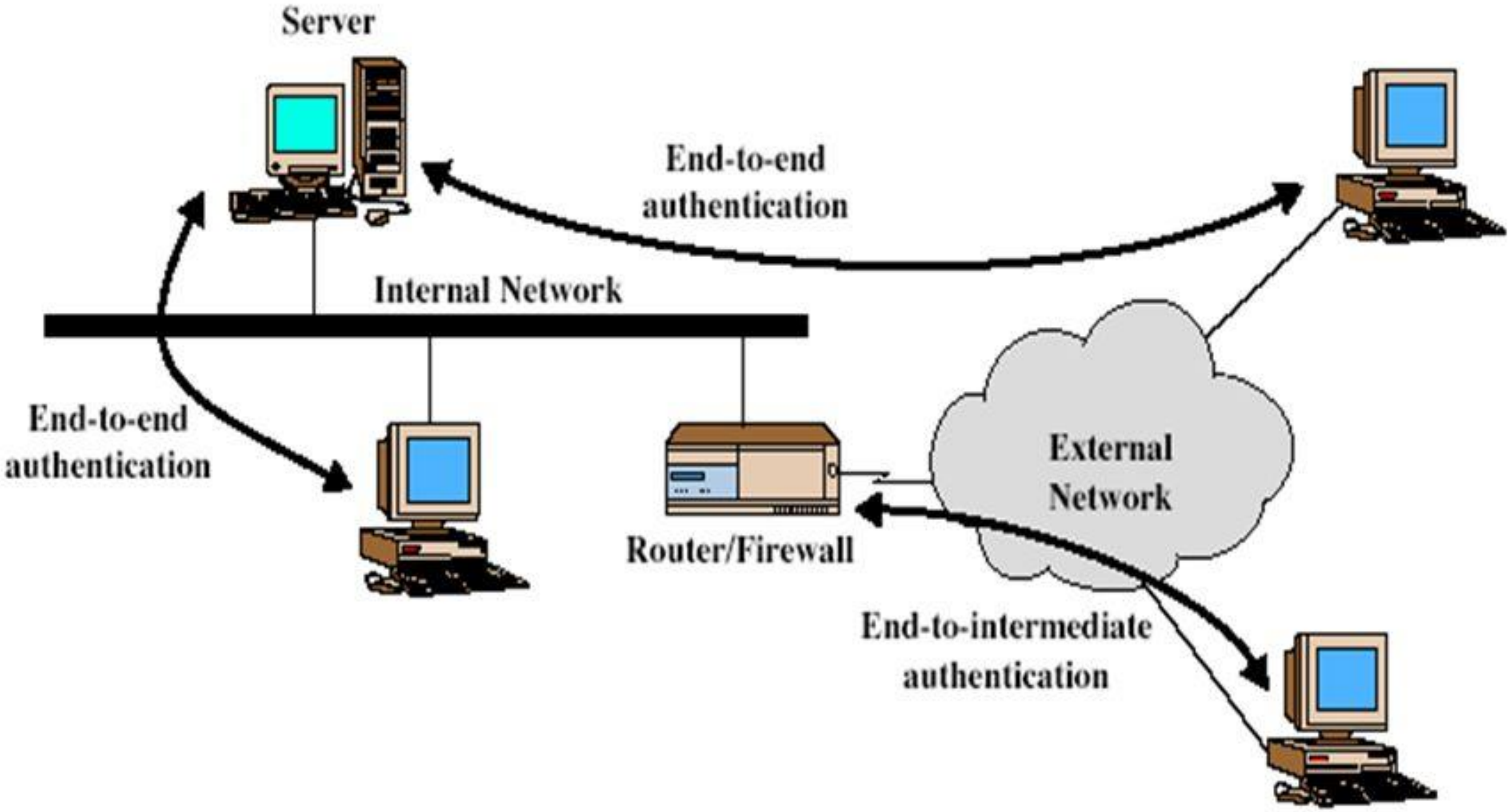
- provides support for data integrity & authentication of IP packets
  - end system/router can authenticate user/app
  - prevents address spoofing attacks by tracking sequence numbers
- based on use of a MAC
  - HMAC-MD5-96 or HMAC-SHA-1-96
- parties must share a secret key

Authentication Header



Bit: 0	8	16	31
Next Header	Payload Length	RESERVED	
Security Parameters Index (SPI)			
Sequence Number			
Authentication Data (variable)			

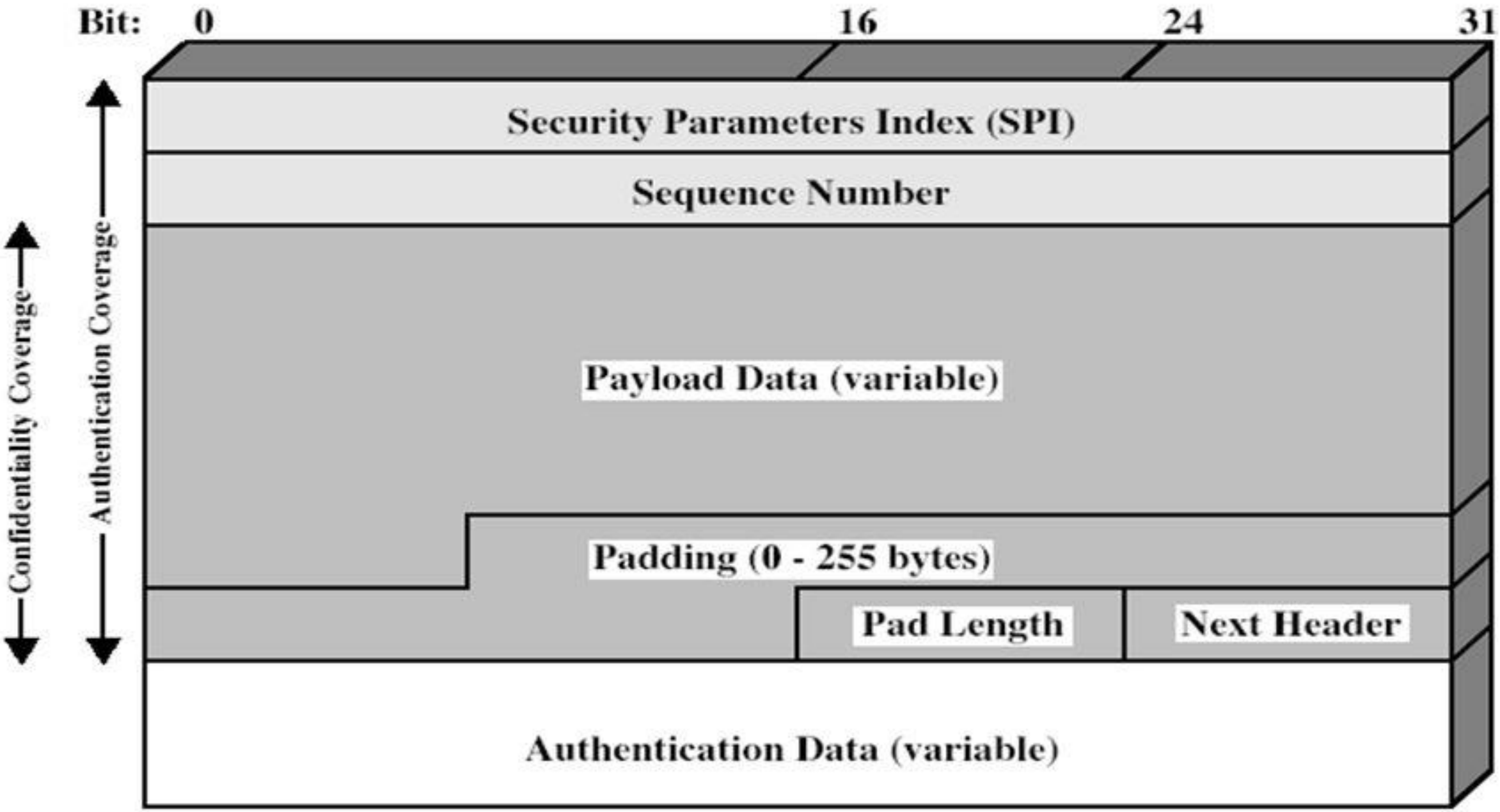
Transport & Tunnel Modes



Encapsulating Security Payload (ESP)

- provides message content confidentiality & limited traffic flow confidentiality
- can optionally provide the same authentication services as AH
- supports range of ciphers, modes, padding
  - incl. DES, Triple-DES, RC5, IDEA, CAST etc
  - CBC most common
  - pad to meet blocksize, for traffic flow

Encapsulating Security Payload



Bit: 0 16 24 31

Security Parameters Index (SPI)

Sequence Number

Payload Data (variable)

Padding (0 - 255 bytes)

Pad Length

Next Header

Authentication Data (variable)

Confidentiality Coverage

Authentication Coverage

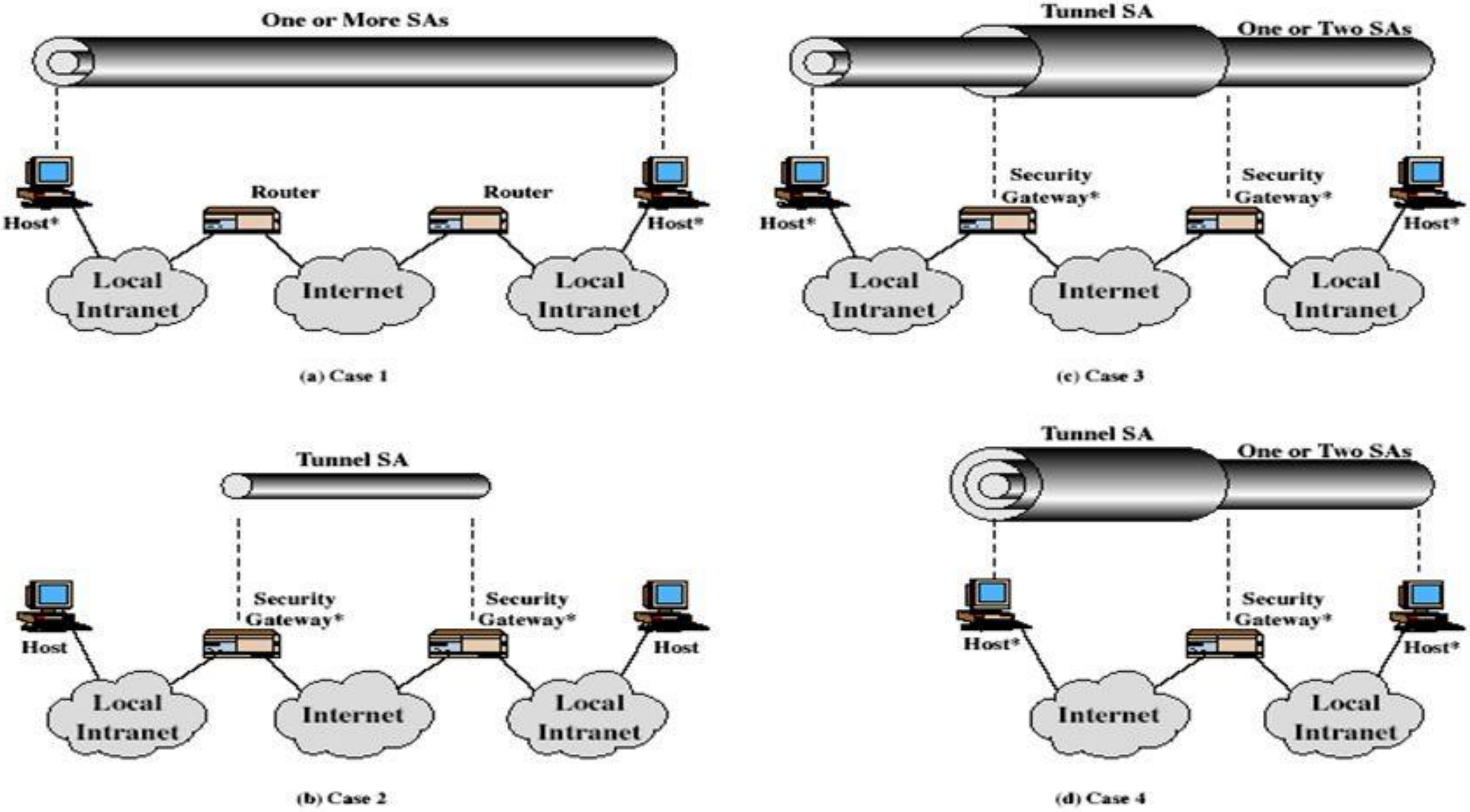
Transport vs Tunnel Mode ESP

- transport mode is used to encrypt & optionally authenticate IP data
  - data protected but header left in clear
  - can do traffic analysis but is efficient
  - good for ESP host to host traffic
- tunnel mode encrypts entire IP packet
  - add new header for next hop
  - good for VPNs, gateway to gateway security

Combining Security Associations

- SA’s can implement either AH or ESP
- to implement both need to combine SA’s
  - form a security bundle
- have 4 cases (see next)

Combining Security Associations



(a) Case 1

(c) Case 3

(b) Case 2

(d) Case 4

Key Management

- handles key generation & distribution
- typically need 2 pairs of keys
  - 2 per direction for AH & ESP
- manual key management
  - sysadmin manually configures every system
- automated key management
  - automated system for on demand creation of keys for SA’s in large systems
  - has Oakley & ISAKMP elements

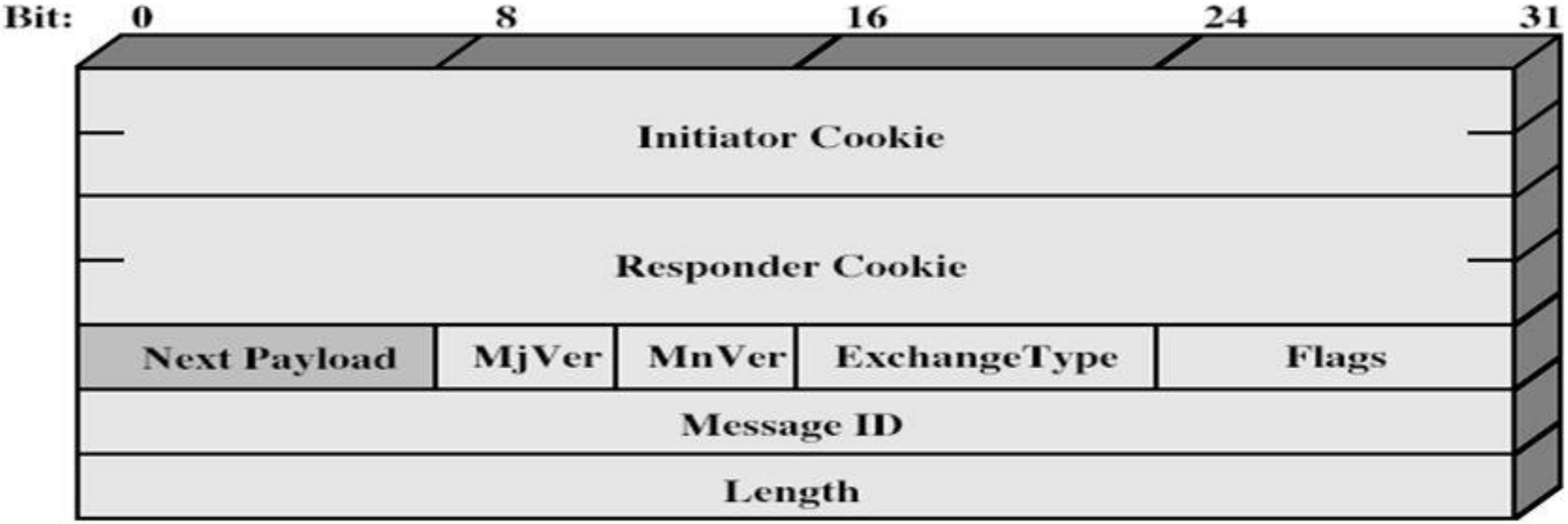
Oakley

- a key exchange protocol
- based on Diffie-Hellman key exchange
- adds features to address weaknesses
  - cookies, groups (global params), nonces, DH key exchange with authentication
- can use arithmetic in prime fields or elliptic curve fields

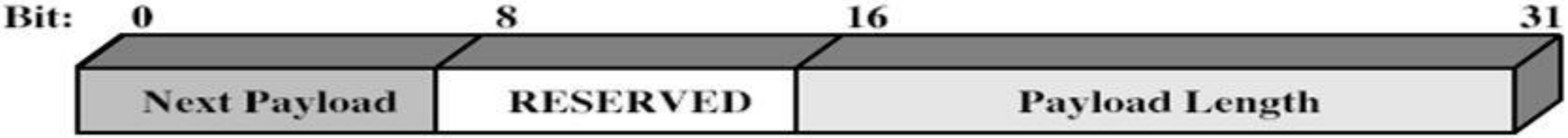
ISAKMP

- Internet Security Association and Key Management Protocol
- provides framework for key management
- defines procedures and packet formats to establish, negotiate, modify, & delete SAs
- independent of key exchange protocol, encryption alg, & authentication method

ISAKMP



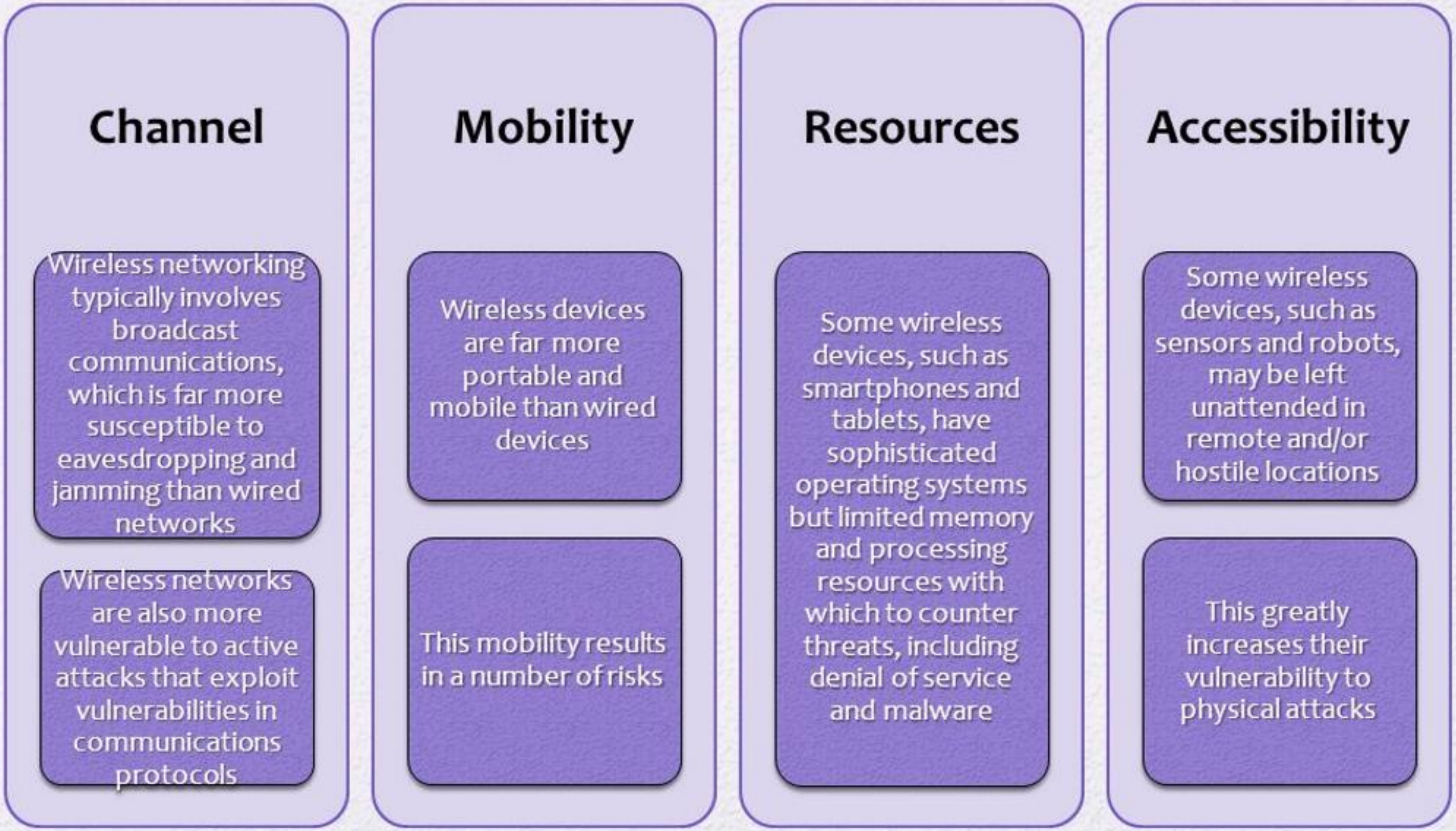
(a) ISAKMP Header



(b) Generic Payload Header

Wireless Security

- Some of the key factors contributing to the higher security risk of wireless networks compared to wired networks include:



Channel

Wireless networking typically involves broadcast communications, which is far more susceptible to eavesdropping and jamming than wired networks

Wireless networks are also more vulnerable to active attacks that exploit vulnerabilities in communications protocols

Mobility

Wireless devices are far more portable and mobile than wired devices

This mobility results in a number of risks

Resources

Some wireless devices, such as smartphones and tablets, have sophisticated operating systems but limited memory and processing resources with which to counter threats, including denial of service and malware

Accessibility

Some wireless devices, such as sensors and robots, may be left unattended in remote and/or hostile locations

This greatly increases their vulnerability to physical attacks

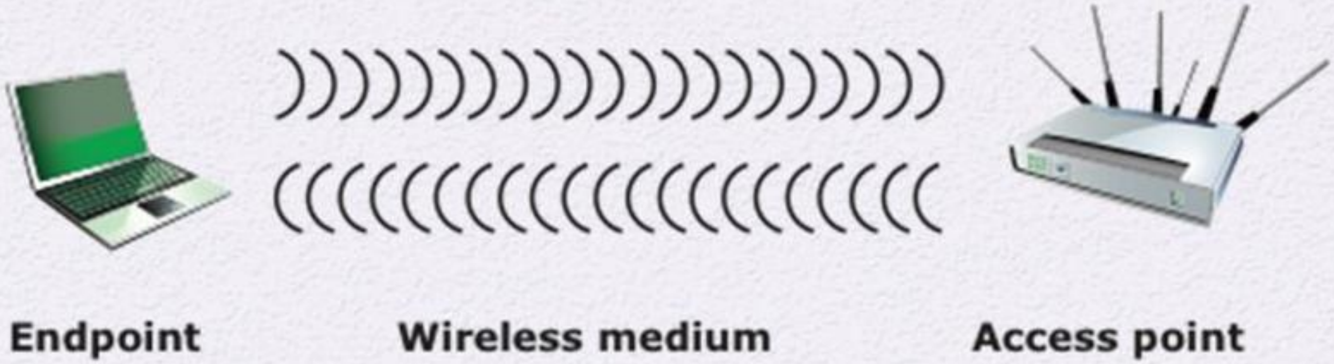
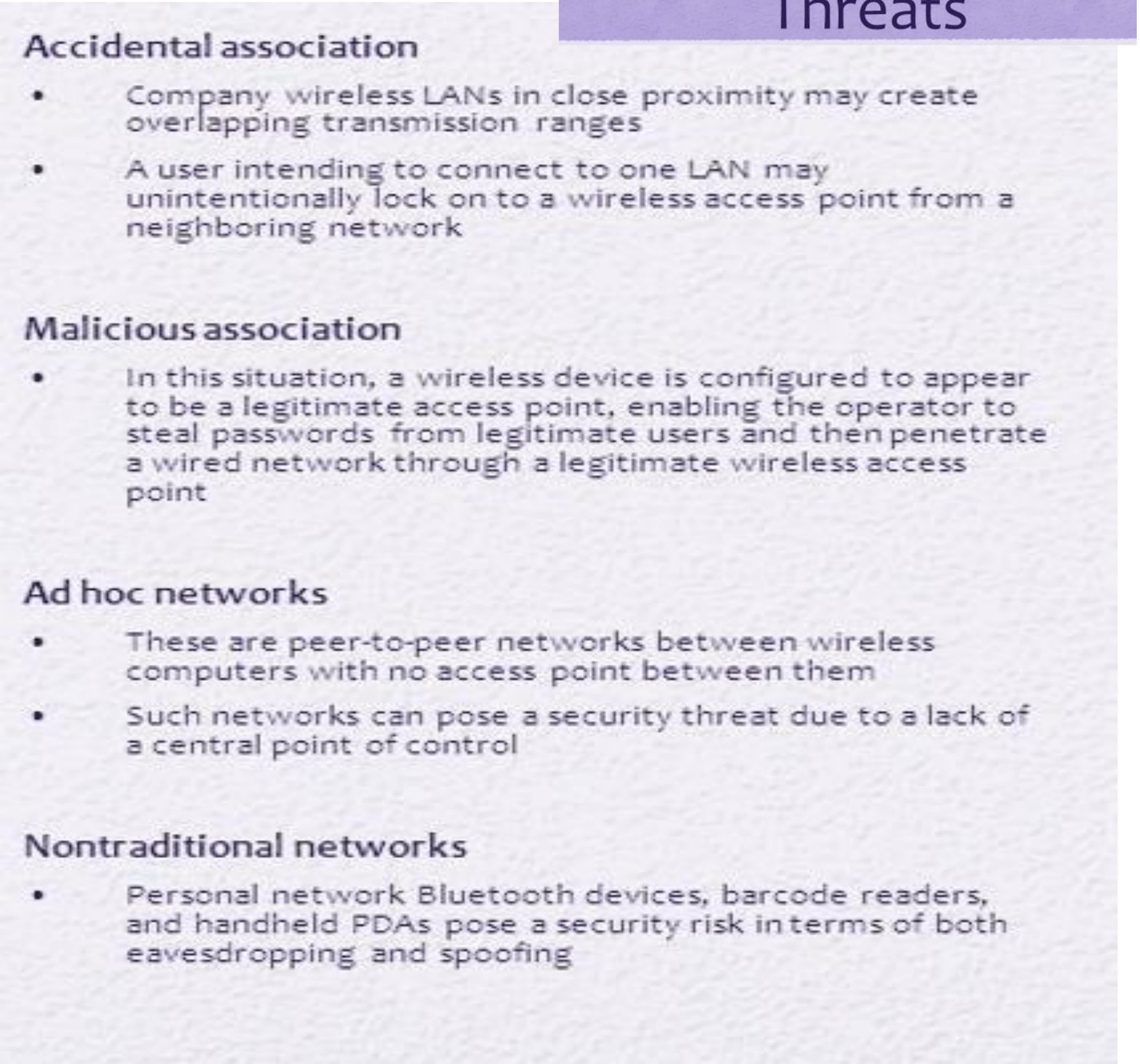


Figure 18.1 Wireless Networking Components

Wireless Network Threats



Accidental association

- Company wireless LANs in close proximity may create overlapping transmission ranges
- A user intending to connect to one LAN may unintentionally lock on to a wireless access point from a neighboring network

Malicious association

- In this situation, a wireless device is configured to appear to be a legitimate access point, enabling the operator to steal passwords from legitimate users and then penetrate a wired network through a legitimate wireless access point

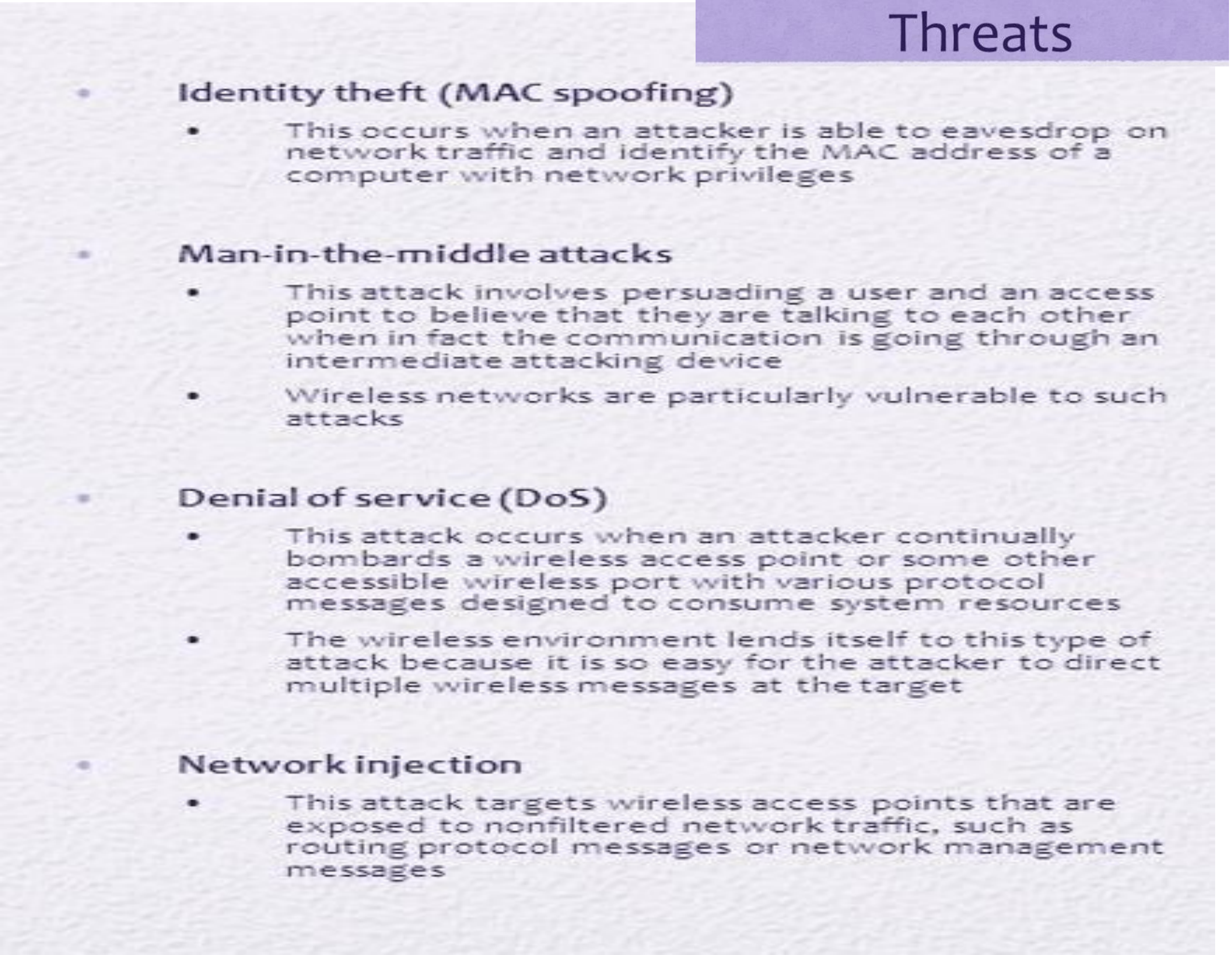
Ad hoc networks

- These are peer-to-peer networks between wireless computers with no access point between them
- Such networks can pose a security threat due to a lack of a central point of control

Nontraditional networks

- Personal network Bluetooth devices, barcode readers, and handheld PDAs pose a security risk in terms of both eavesdropping and spoofing

Wireless Network Threats



- Identity theft (MAC spoofing)
  - This occurs when an attacker is able to eavesdrop on network traffic and identify the MAC address of a computer with network privileges
- Man-in-the-middle attacks
  - This attack involves persuading a user and an access point to believe that they are talking to each other when in fact the communication is going through an intermediate attacking device
  - Wireless networks are particularly vulnerable to such attacks
- Denial of service (DoS)
  - This attack occurs when an attacker continually bombards a wireless access point or some other accessible wireless port with various protocol messages designed to consume system resources
  - The wireless environment lends itself to this type of attack because it is so easy for the attacker to direct multiple wireless messages at the target
- Network injection
  - This attack targets wireless access points that are exposed to nonfiltered network traffic, such as routing protocol messages or network management messages

Securing Wireless Transmissions

- The principal threats to wireless transmission are eavesdropping, altering or inserting messages, and disruption
- To deal with eavesdropping, two types of countermeasures are appropriate:
  - Signal-hiding techniques
    - Turn off SSID broadcasting by wireless access points
    - Assign cryptic names to SSIDs
    - Reduce signal strength to the lowest level that still provides requisite coverage
    - Locate wireless access points in the interior of the building, away from windows and exterior walls
  - Encryption
    - Is effective against eavesdropping to the extent that the encryption keys are secured

Securing Wireless Networks

- Use encryption
- Use antivirus, antispyware software and a firewall
- Turn off identifier broadcasting
- Change the identifier on your router from the default
- Change your router’s pre-set password for administration
- Allow only specific computers to access your wireless network

Mobile Device Security

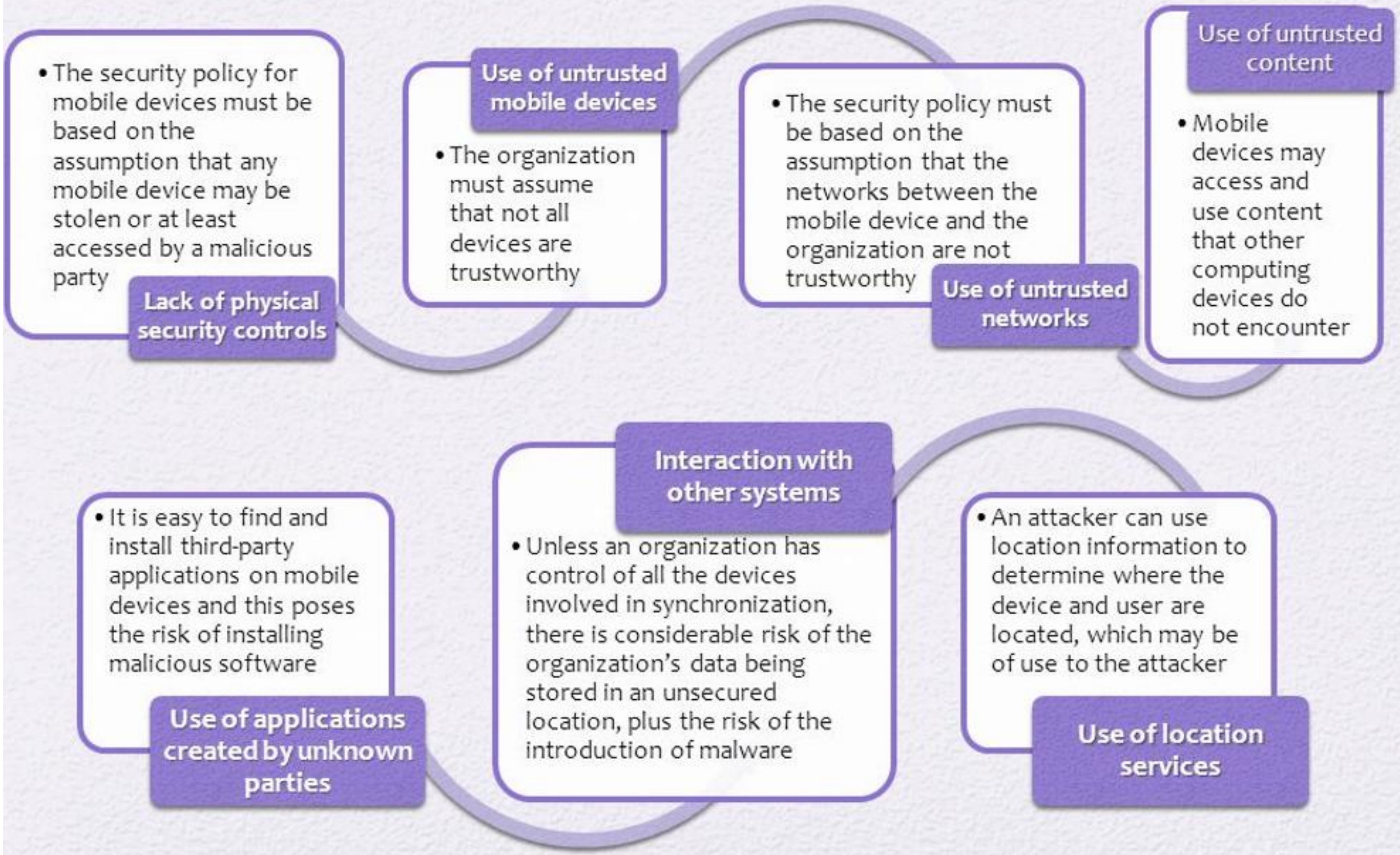
- Mobile devices have become an essential element for organizations as part of the overall network infrastructure

- Prior to the widespread use of smartphones, network security was based upon clearly defined perimeters that separated trusted internal networks from the untrusted Internet

- Due to massive changes, an organization's networks must now accommodate:
  - Growing use of new devices
  - Cloud-based applications
  - De-perimeterization
  - External business requirements

Security Threats

- Major security concerns for mobile devices:



Lack of physical security controls

- The security policy for mobile devices must be based on the assumption that any mobile device may be stolen or at least accessed by a malicious party

Use of untrusted mobile devices

- The organization must assume that not all devices are trustworthy

Use of untrusted networks

- The security policy must be based on the assumption that the networks between the mobile device and the organization are not trustworthy

Use of untrusted content

- Mobile devices may access and use content that other computing devices do not encounter

Use of applications created by unknown parties

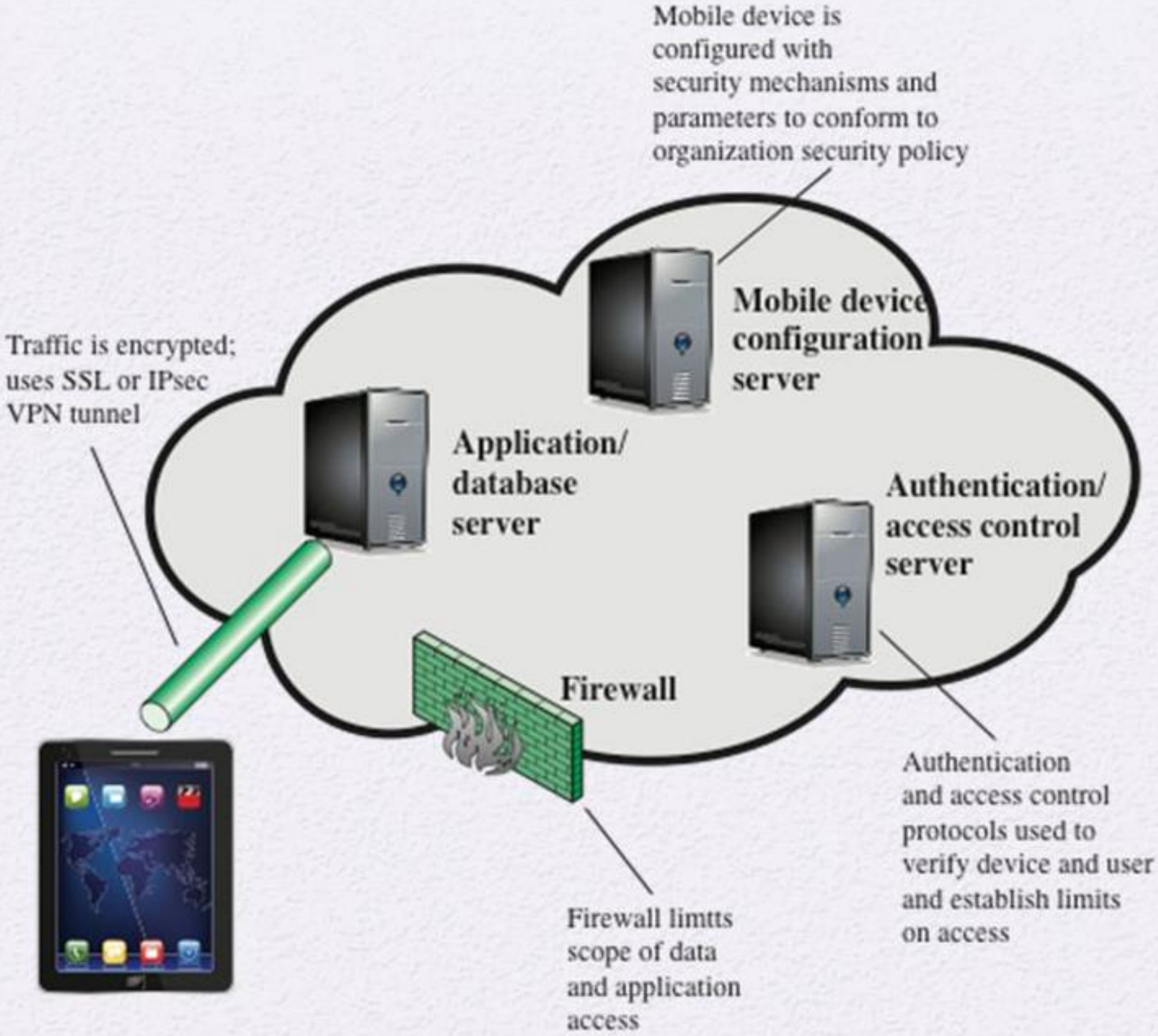
- It is easy to find and install third-party applications on mobile devices and this poses the risk of installing malicious software

Interaction with other systems

- Unless an organization has control of all the devices involved in synchronization, there is considerable risk of the organization's data being stored in an unsecured location, plus the risk of the introduction of malware

Use of location services

- An attacker can use location information to determine where the device and user are located, which may be of use to the attacker



Mobile device configuration server
Application/ database server
Authentication/ access control server
Firewall

Mobile device is configured with security mechanisms and parameters to conform to organization security policy

Traffic is encrypted; uses SSL or IPsec VPN tunnel

Authentication and access control protocols used to verify device and user and establish limits on access

Firewall limtts scope of data and application access

Figure 18.2 Mobile Device Security Elements