COMP412

Computer Security

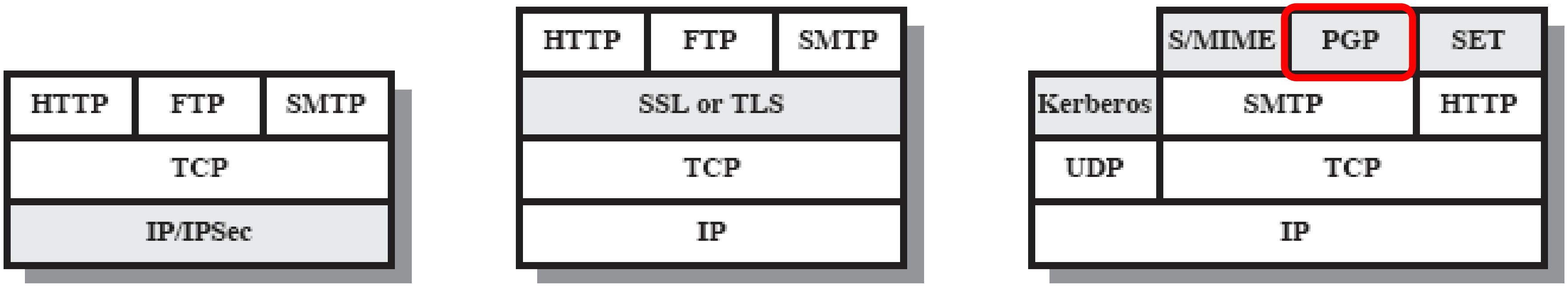
Lec 11 Network Security Application

Dr. Xiaochen Yuan
2021/2022

Contents

- Pretty Good Privacy (PGP)
  - Services & format
  - Keys
- IPSec
- Wireless Security
  - WEP, WPA & WPA2

Security Technology in OSI (Open Systems Interconnection) Model



(a) Network Level (b) Transport Level (c) Application Level

Pretty Good Privacy (PGP)

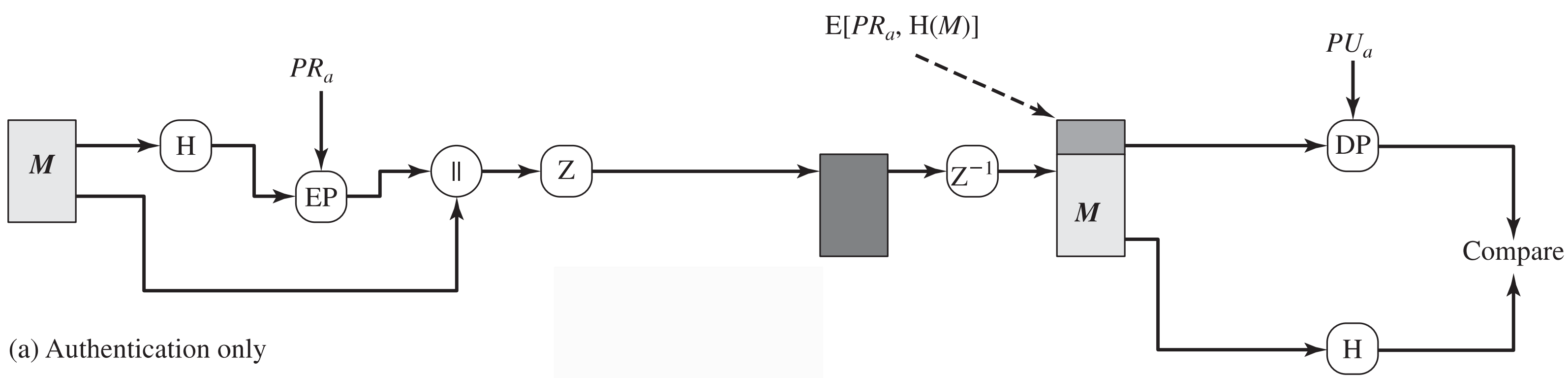
- PGP provides a **confidentiality** and **authentication** service that can be used in email and file storage applications
- It supports best available cryptographic algorithms
- It integrates these algorithms into a general-purpose application that is independent of OS and processor
- It is open-source!

PGP Services

Function	**Algorithms Used**
Digital signature	DSS/SHA or RSA/SHA
Message encryption	CAST or IDEA or 3DES with Diffie-Hellman (ElGamal) or RSA
Compression	ZIP
Email compatibility	Radix 64

PGP Authentication Only Service

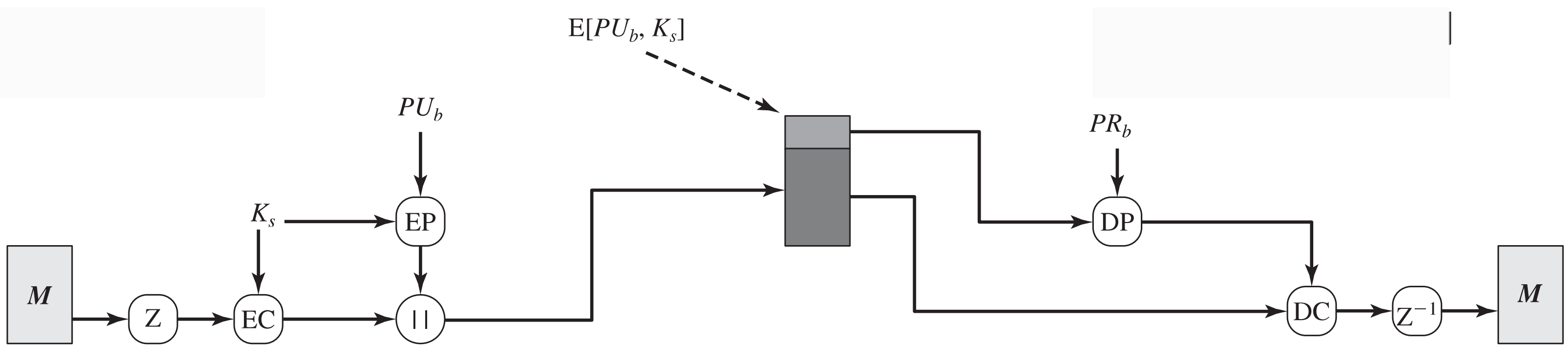
- SHA-1 hash code encrypted with sender's RSA (Or DSS) private key
- Message is compressed with ZIP during transmission
- Signature is verified with sender's public key



(a) Authentication only

PGP Confidentiality Only Service

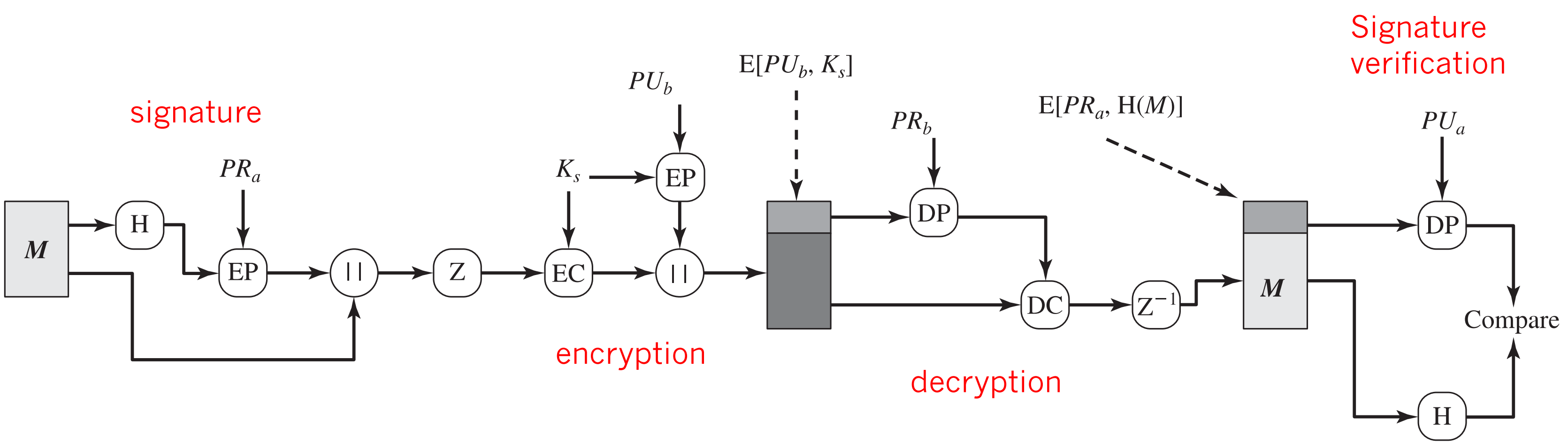
- Sender generates a random **128-bit session key** for message encryption, using CAST-128 (or IDEA or 3DES)
- Session key is encrypted with recipient's public key (RSA or ElGamal) and is appended to the message
- Receiver obtains the session key with his private key and decrypts the message with the key



(b) Confidentiality only

Confidentiality and Authentication Service

- A combination of the two services
- Signature uses RSA/SHA or DSS/SHA
- Use session key KS for CAST-128, IDEA or 3DES encryption
- Session key is hidden by RSA or ElGamal

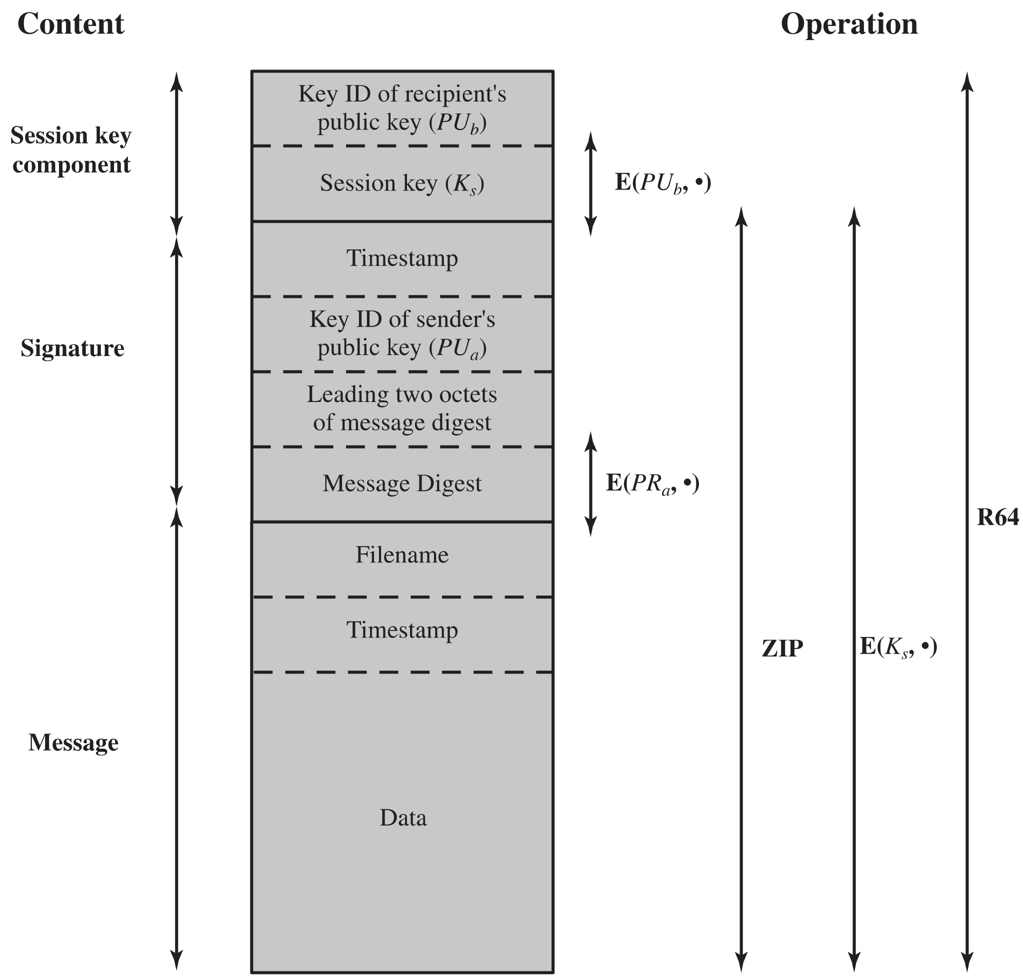


(c) Confidentiality and authentication

Other Functions

- ZIP compression
  - Saving space for transmission and file storage
  - Compressed message is more stronger in cryptographic security
  - Signature is generated before compression
    - Various compression algorithm implementations achieve different tradeoffs in **running speed** versus **compression ratios** and produce different compressed forms. Thus use of compression algorithms in PGP is restricted
- Email compatibility
  - Radix-64 is used for converting binary compressed email to ASCII plaintext
  - Radix-64 expansion is compensated by ZIP compression (Radix-64: 3 bytes to 4 chars)
  - Typical overall effect: 1.33 × 0.5 × file length

Format of PGP Message



Notation:

E(PU_b, •) = encryption with user b's public key
E(PR_a, •) = encryption with user a's private key
E(K_s, •) = encryption with session key
ZIP = Zip compression function
R64 = Radix-64 conversion function

Format of PGP Message

- **Message** component
  - Actual data
  - Filename of the data
  - Timestamp of the data created
- **Session key** component
  - Key ID of the recipient's public key
  - Encrypted session key

Format of PGP Message

- **Signature** component
  - Timestamp of the signature created
  - Message digest
    - ✓ Calculated over the signature timestamp and data in message component
    - ✓ Signature timestamp assures against replay attack
    - ✓ Exclusion of filename and timestamp of message component ensures that signature is created on data independently
  - Leading two octets of message digest is *for recipient to determine if the correct public key is used*
  - Key ID of sender's public key

Keys in PGP

- One-time unpredictable 128-bit **session key** KS
  - Generated at each encryption using CAST-128
  - CAST-128 is a symmetric encryption algorithm. Key size varies from 40-bit to 128-bit
- **Public keys**
  - Other people public keys
- **Private keys**
  - Your own private keys

Keys in PGP

- Passphrase-based conventional keys
  - Keys to encrypt your private keys using CAST-128
- Use the hash code of CAST-128 of passphrase keys for encryption of private keys
  - It is compact and effective
  - It avoids the problem of saving it in a file
  - It is easy to remember and not easily guessed

Keys in PGP

- Multiple public-key/private-key pairs are allowed
  - Users maintain their key pairs and change their keys over time
- How does the recipient know which of its public keys was used to encrypt session key?
  - Each public key is attached with a user ID and key ID. It raises management and overhead problem
  - Use the least significant 64 bits of public key as key ID solves the problem
    - Key ID = KU_A mod 2^64

Private Key Ring

- Keys in PGP are stored and organized in a systematic way for efficient and effective use by all parties
- Each user will have two key rings. One for public keys of other users and one for user's private keys
- Private key is encrypted by passphrase key
- User ID, typically, will be the user email address or something else.
  Reuse of user ID is allowed

Private-Key Ring

Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
• • •	• • •	• • •	• • •	• • •
T_i	$PU_i \bmod 2^{64}$	PU_i	$E(H(P_i), PR_i)$	User i
• • •	• • •	• • •	• • •	• • •

* = field used to index table

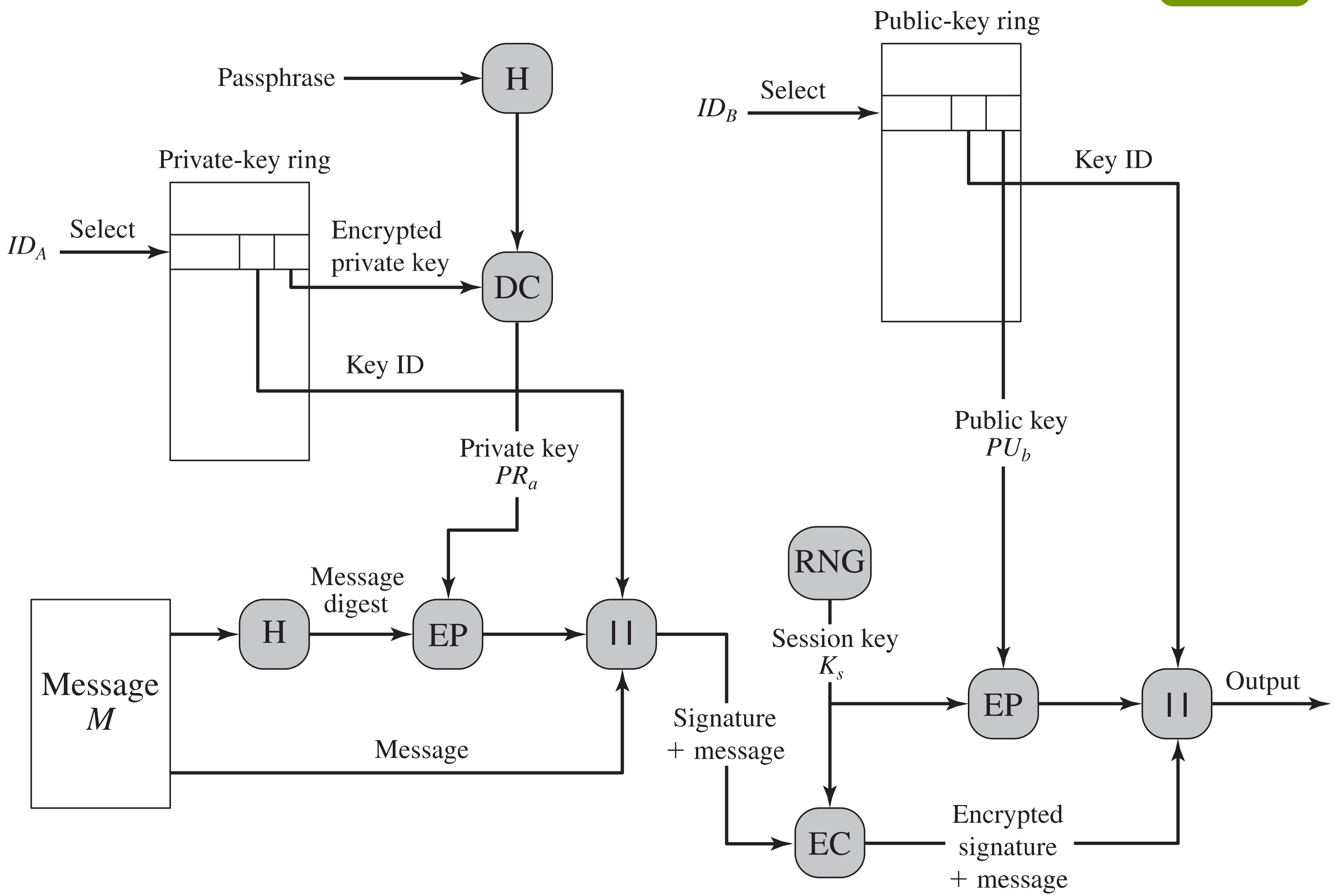
Public Key Rings

Public-Key Ring

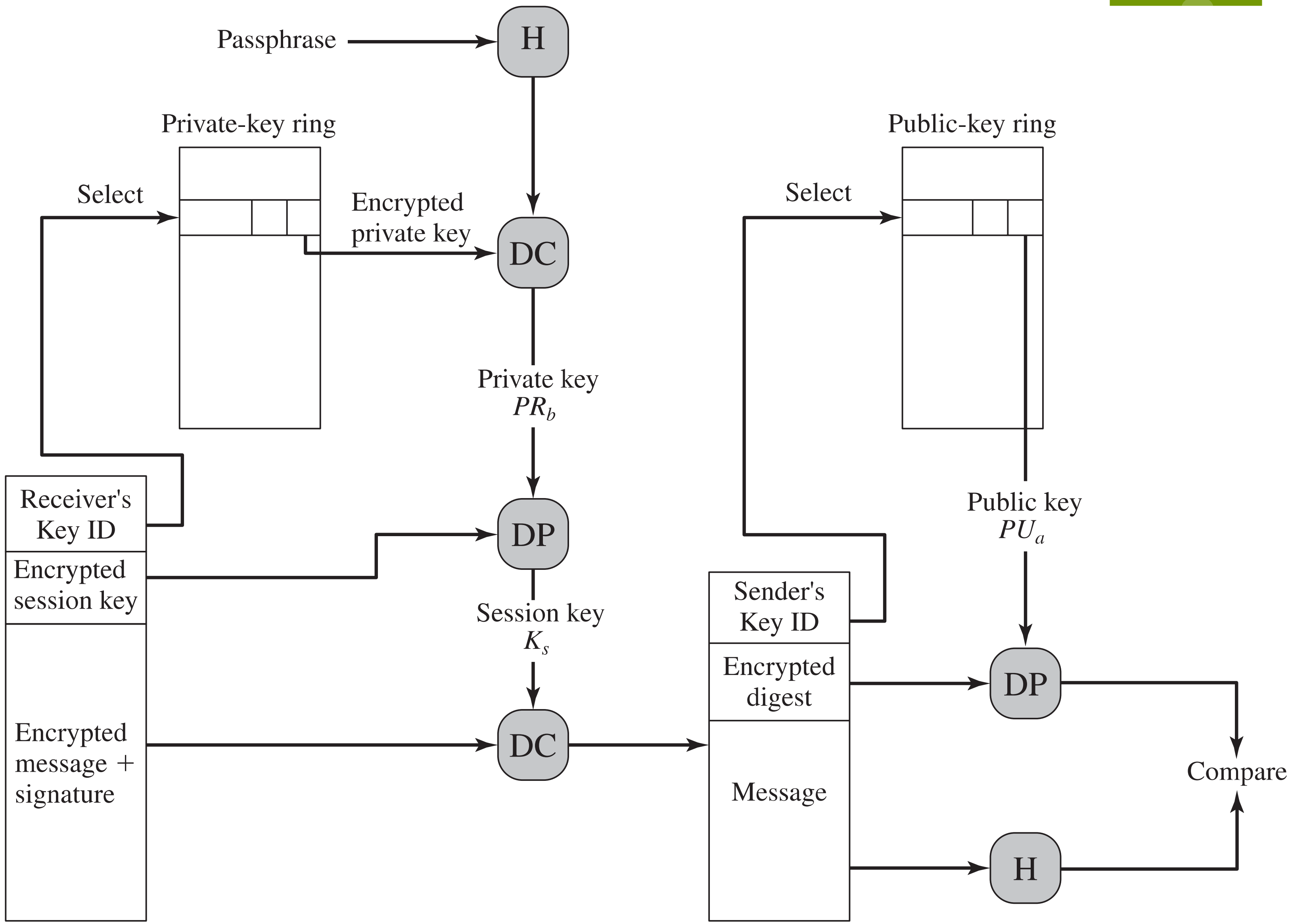
Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •
T_i	$PU_i \bmod 2^{64}$	PU_i	trust_flag $_i$	User i	trust_flag $_i$		
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •

* = field used to index table

Message Generation



Message Reception



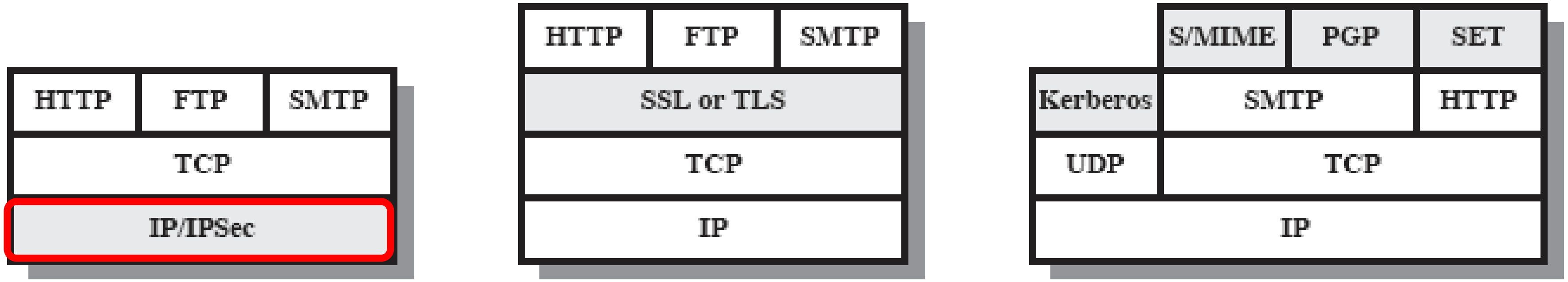
Public Key Distribution

- Make your public key available through a public key server
- Include your public key in an email message
- Export your public key or copy it to a text file
- Copy your public key from a smart card directly to someone's key ring
- Import keys and X.509 certificate

Public Key Revocation

- A user may wish to revoke his current public key
- Public key revocation certificate must be signed by the corresponding private key
- The owner should attempt to disseminate this certificate as widely and as quickly as possible
- To revoke a key is very simple. A function is available.

Security Technology in OSI Model



(a) Network Level (b) Transport Level (c) Application Level

IP Security Overview

- **IPSec** is a capability that can be added to either current version of the Internet Protocol (IPv4 or IPv6) by means of additional headers.
- IPSec encompasses three functional areas:
  - **Authentication** makes use of the HMAC message authentication code.
    - Authentication can be applied to the entire original IP packet (tunnel mode) or to all of the packet except for the IP header (transport mode).
  - **Confidentiality** is provided by an encryption format known as encapsulating security payload.
    - Both tunnel and transport modes can be accommodated.
  - **IKE** (Internet Key Exchange) defines a number of techniques for key management.

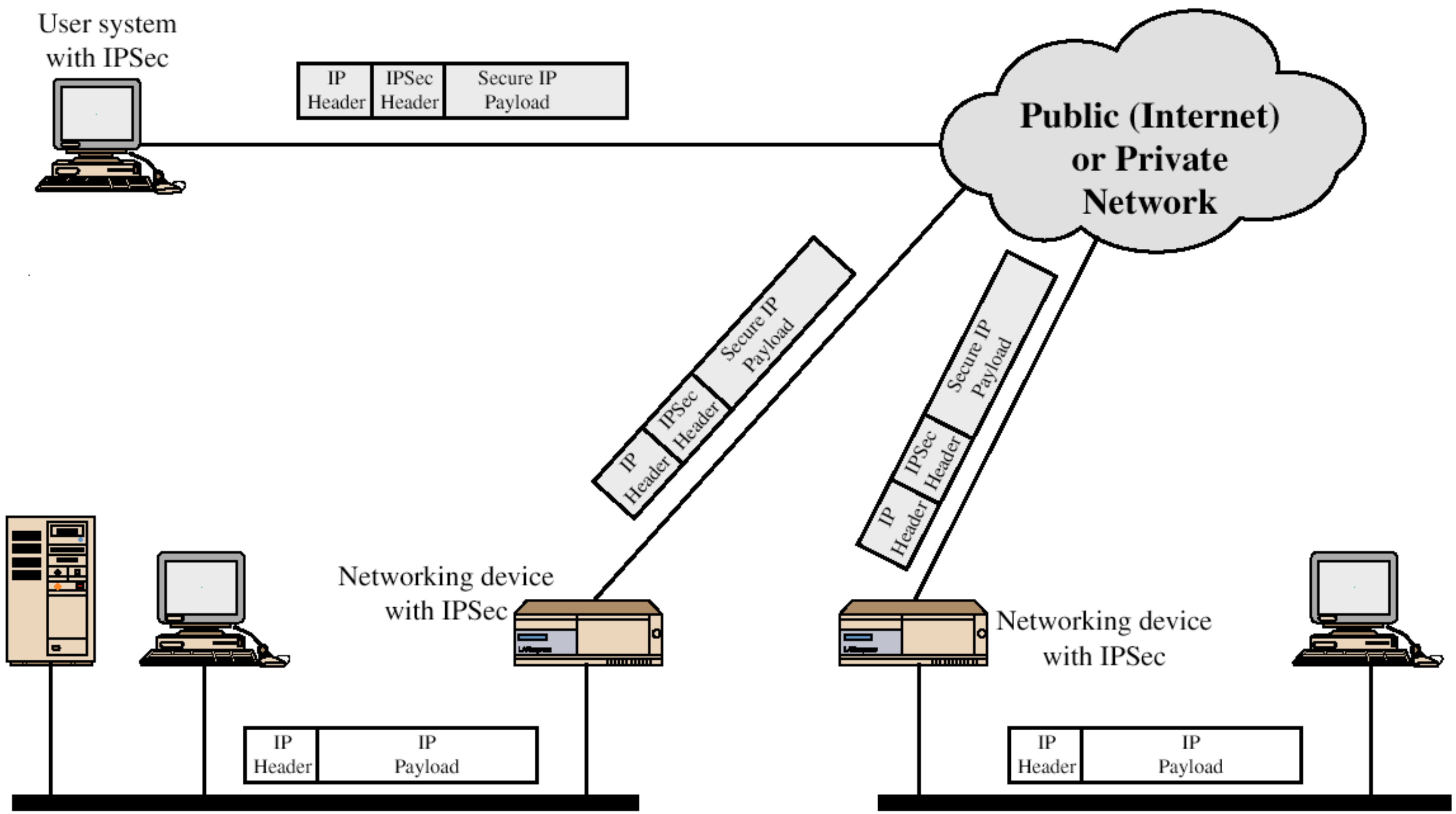
IP Security Overview

- 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
- Applications of IPSec
  - Secure branch office connectivity over the Internet
  - Secure remote access over the Internet
  - Establishing extranet and intranet connectivity with partners
  - Enhancing electronic commerce security

IP Security Overview

- Benefits of IPSec
  - Transparent to applications, below transport layer (TCP, UDP)
    - No software update needed
  - Provide security for individual users
    - No user training needed
- IPSec can assure that:
  - 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

IP Security Scenario



IPSec Services

	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access control	✔	✔	✔
Connectionless integrity	✔		✔
Data origin authentication	✔		✔
Rejection of replayed packets	✔	✔	✔
Confidentiality		✔	✔
Limited traffic flow confidentiality		✔	✔

Transport and Tunnel Modes

	Transport Mode SA	Tunnel Mode SA
AH (Authentication Header)	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 (Encapsulation Security Payload)	Encrypts IP payload and any IPv6 extension header	Encrypts inner IP packet
ESP with authentication	Encrypts IP payload and any IPv6 extension header. Authenticates IP payload but no IP header	Encrypts inner IP packet. Authenticates inner IP packet.

IP Security Policy

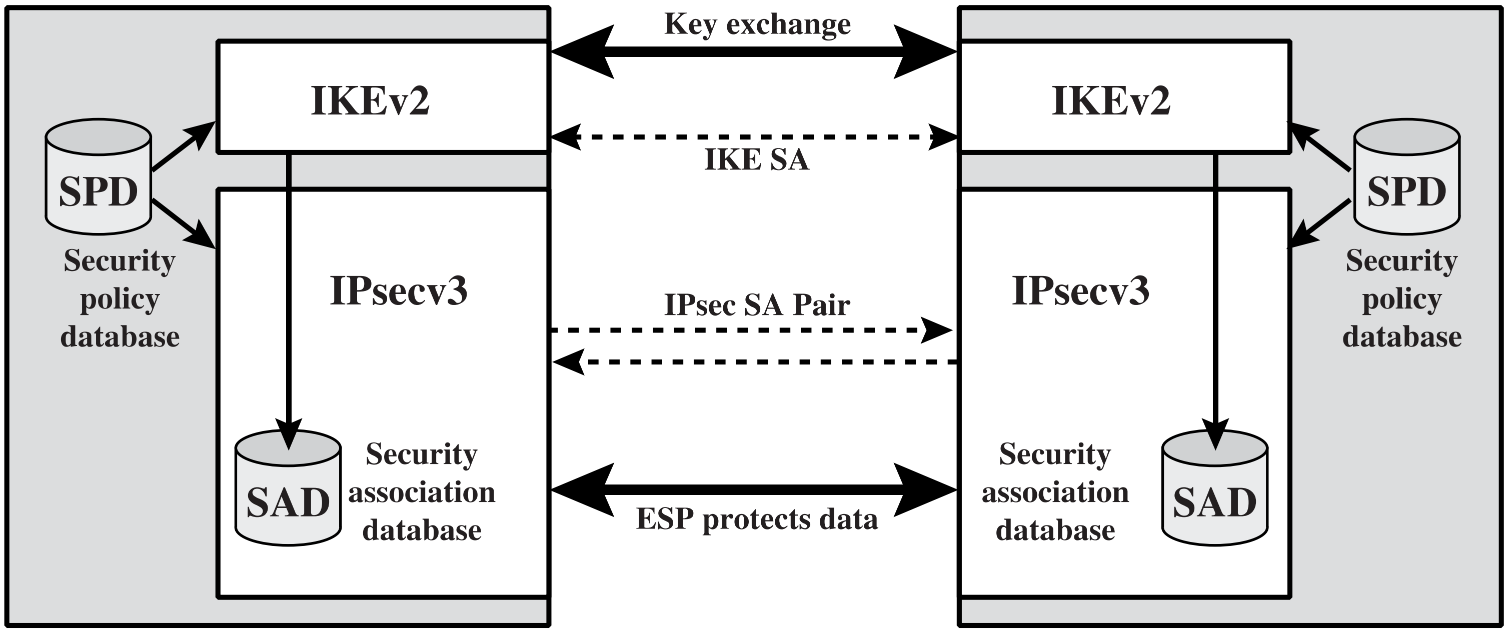


Figure 19.2 IPsec Architecture

IP Security Policy

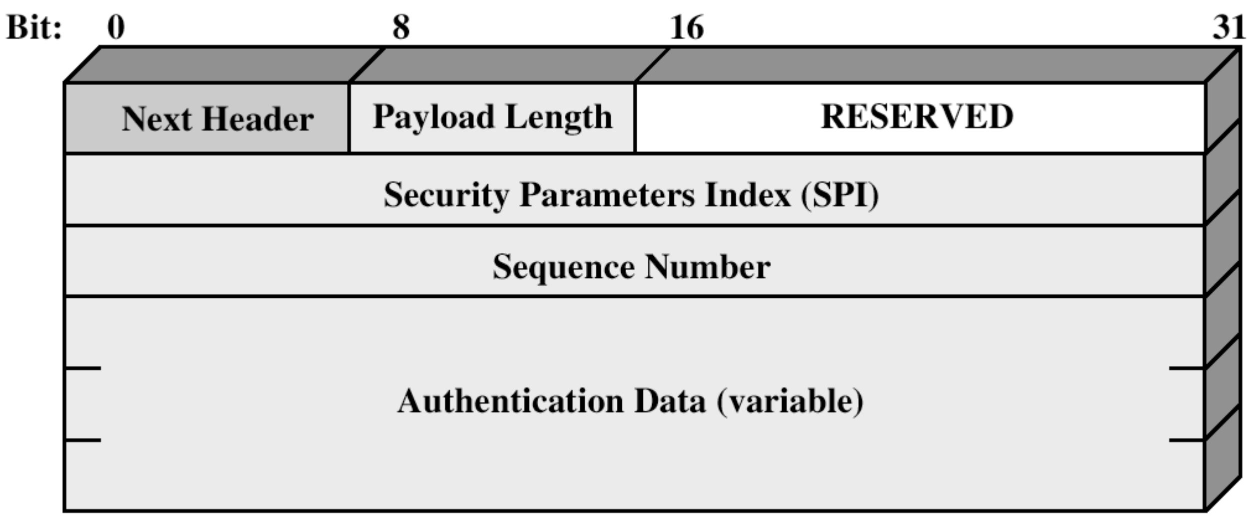
- **Security Associations (SA)**
  - A one way logical connection between a sender and a receiver.
  - Identified by three parameters:
    - Security Parameter Index (SPI)
      - Index to a SA (Security parameters)
    - IP Destination address
      - Destination endpoint
    - Security Protocol Identifier
      - AH or ESP

IP Security Policy

- **Security Association Database (SAD)**
  - Defines the parameters associated with each SA
  - A SAD entry contains parameters such as
    - Security Parameter Index
    - AH and ESP information
    - Lifetime of this SA, etc
- **Security Policy Database (SPD)**
  - By which IP traffic is related to specific SAs
  - A SPD entry defines a subset of IP traffic and points to an SA for that traffic, containing parameters such as
    - Protocol
    - Remote IP address
    - Local IP address
    - Local and Remote ports

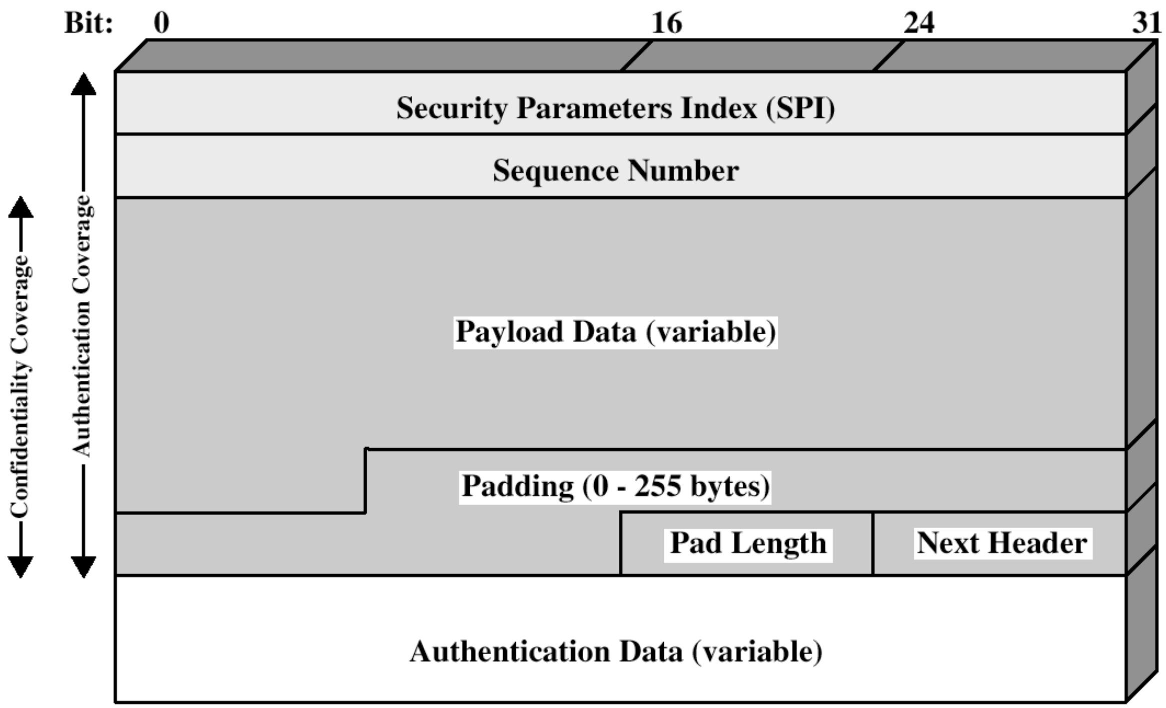
Authentication Header (AH)

- Provides support for data integrity and authentication (MAC code) of IP packets.
- Guards against replay attacks.



Encapsulating Security Payload (ESP)

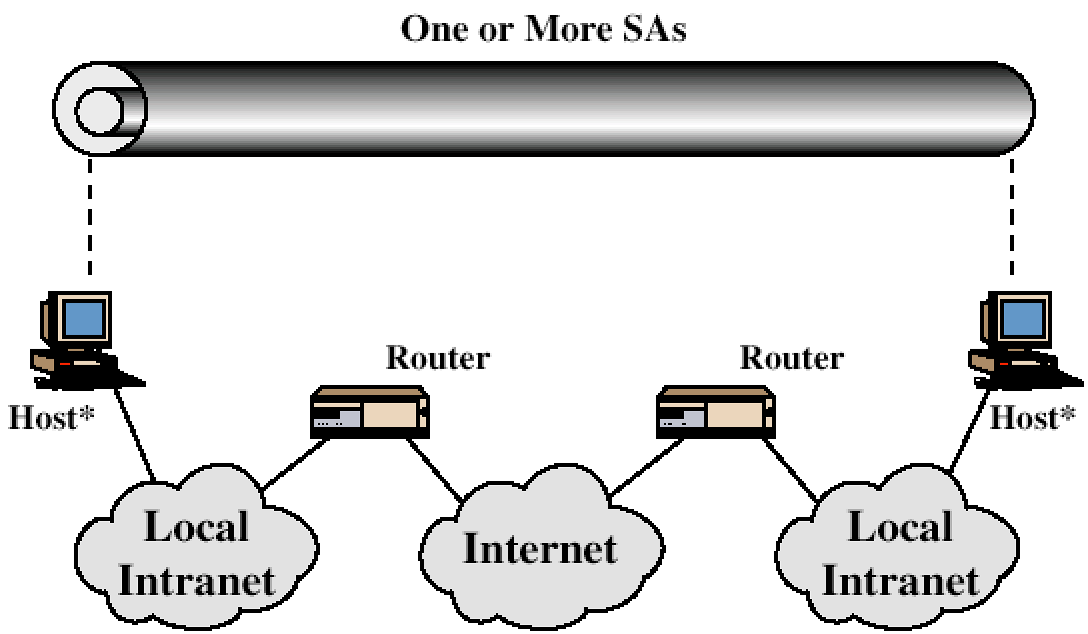
- ESP provides confidentiality services



Encryption and Authentication Algorithms

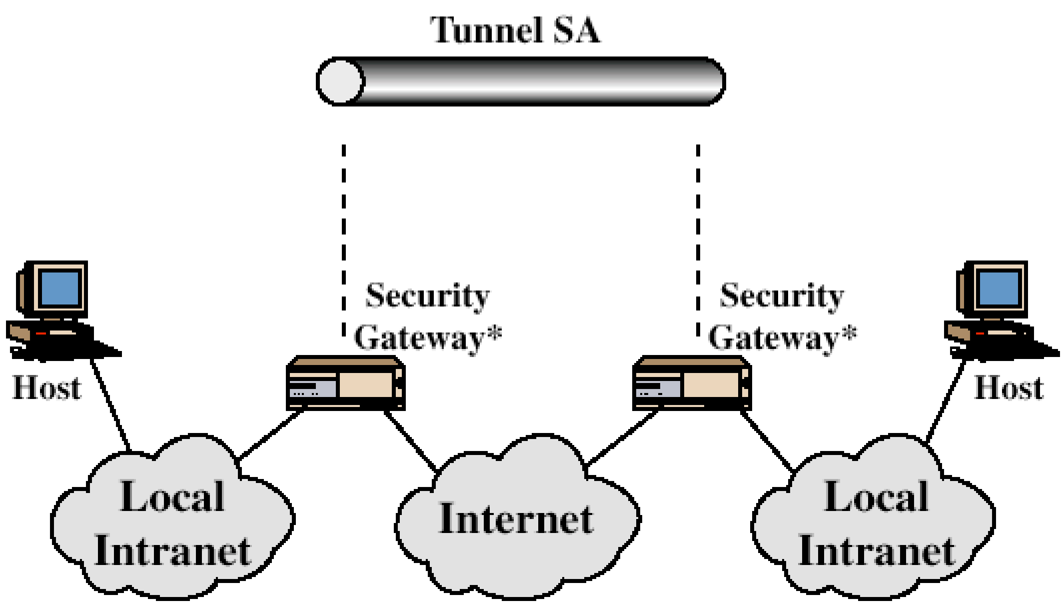
- Encryption:
  - Three-key 3DES
  - RC5
  - IDEA
  - Three-key 3IDEA
  - CAST
  - Blowfish
- Authentication:
  - HMAC-MD5-96
  - HMAC-SHA-1-96

Combinations of Security Associations



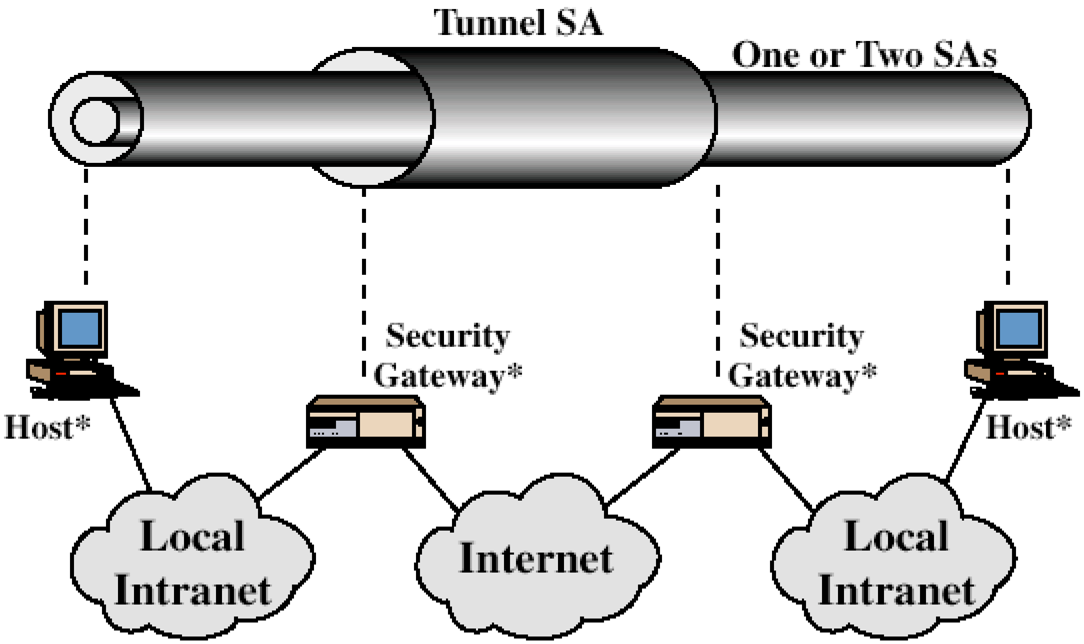
(a) Case 1

Combinations of Security Associations



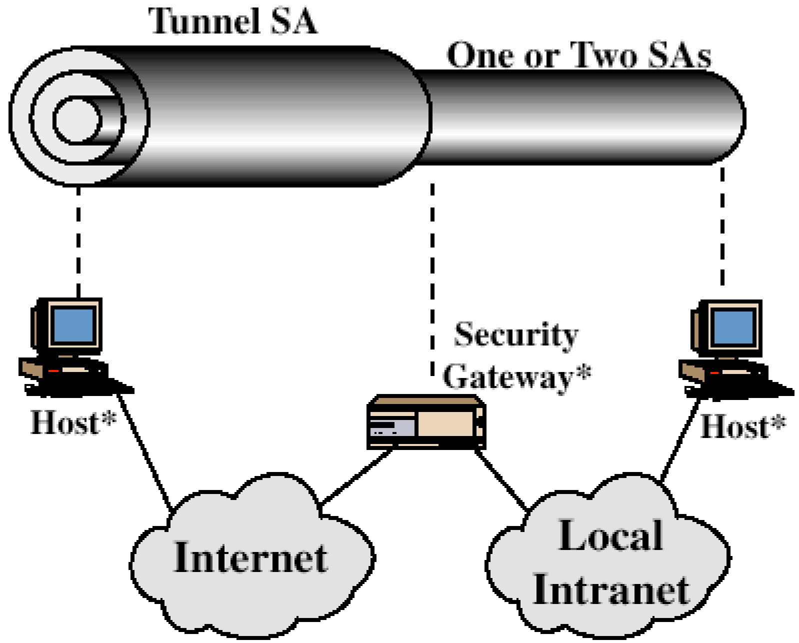
(b) Case 2

Combinations of Security Associations



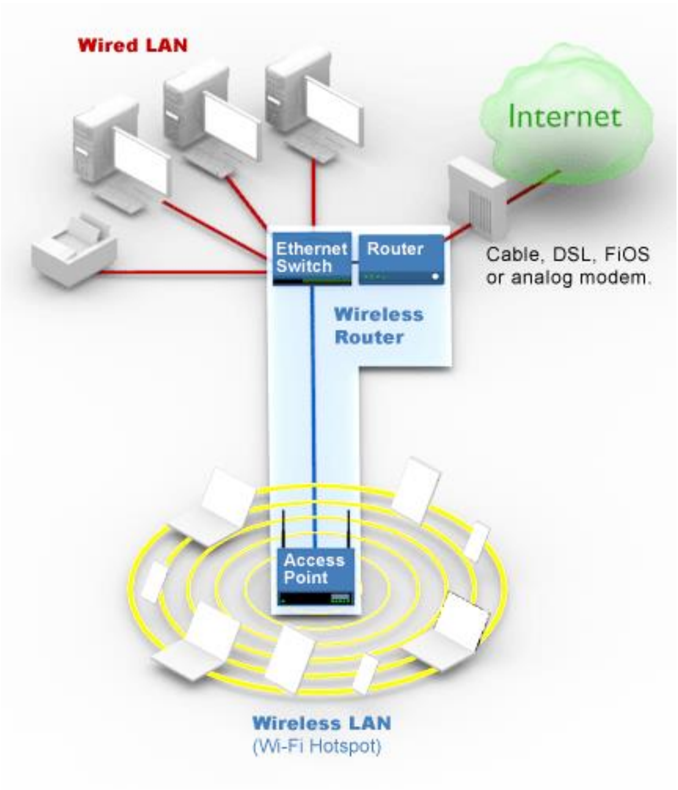
(c) Case 3

Combinations of Security Associations



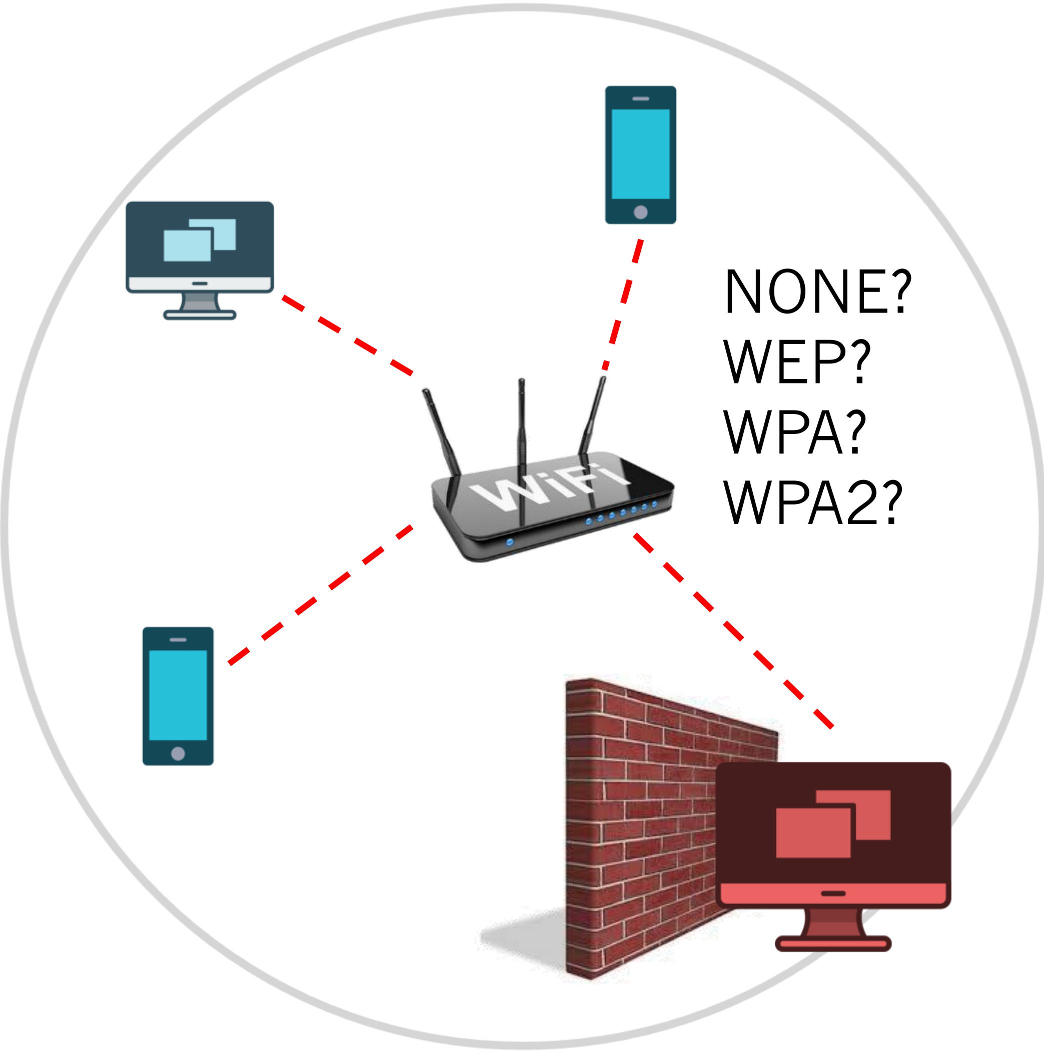
(d) Case 4

Wireless Security



- The standard **wireless local area network (WLAN)** technology for connecting computers and billions of electronic devices to each other and to the Internet.
- Wi-Fi is the wireless version of a wired Ethernet network, extending the size of the network in the air.
- Security in WLAN is about the protection of the data transmission over the air.
- Common security protocols are **WEP**, **WPA**, and **WPA2**.

Wireless Security



Wired Equivalent Privacy (WEP)

- Wi-Fi security standard in September of 1999
- U.S. restrictions on the export of various cryptographic technology → 64-bit only
- Now the key size is up to 128-bit or 256-bit.
- Numerous security flaws were discovered. WEP passwords can be cracked in minutes using freely available software.
- Wi-Fi Alliance officially retired WEP in 2004.

Wi-Fi Protected Access (WPA)

- **WPA** was the Wi-Fi Alliance's direct response and replacement to the increasingly apparent vulnerabilities of the WEP standard.
- The key size of WPA-PSK (pre-shared key) is 256-bit.
- WPA implemented with the temporal key integrity protocol (TKIP), which works as a wrapper of WEP.
- TKIP uses RC4 as its basis.
- Some improvement over WEP:
  - A cryptographic message integrity check to protect packets
  - An initialization-vector sequencing mechanism that includes hashing, as opposed to WEP's plain text transmission
  - A per-packet key-mixing function to increase cryptographic strength
  - A re-keying mechanism to provide key generation every 10,000 packets.

Wi-Fi Protected Access II (WPA2)

- Significant changes between WPA and WPA2
  - The mandatory use of AES algorithms
  - The introduction of CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol)

- The primary security vulnerability to the actual WPA2 system
  - Requires the attacker to already have access to the secured Wi-Fi network in order to gain access to certain keys and then perpetuate an attack against other devices on the network.

- The biggest hole in the WPA armor—the attack vector through the Wi-Fi Protected Setup (WPS).
  - It allows a remote attacker to recover the WPS PIN in a few hours with a brute-force attack and, with the WPS PIN, the network's WPA/WPA2 pre-shared key.