

# Network Security - Continued

## PART 3

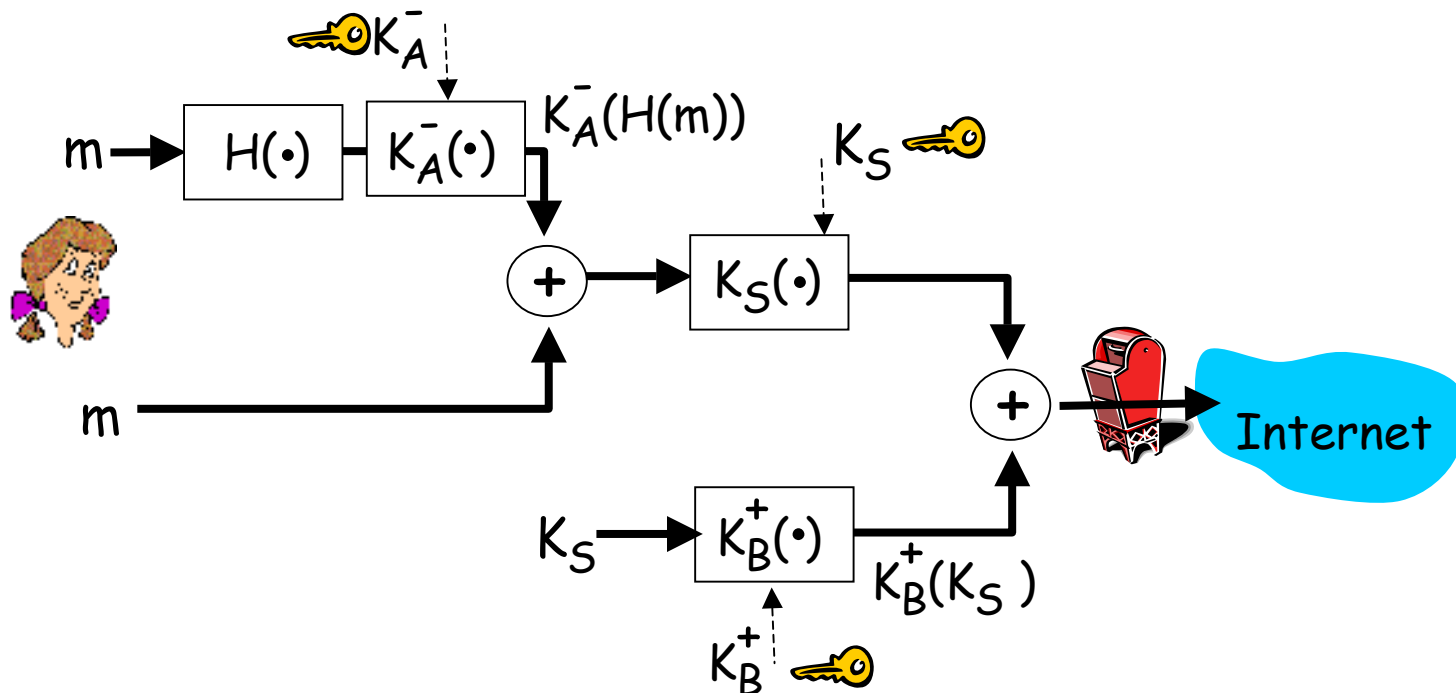
In this lesson...

- Security Continued
- Case studies



# Secure E-mail & PGP

Alice wants to provide secrecy, sender authentication, message integrity.



Alice uses three keys: her private key, Bob's public key, newly created symmetric key

# Secure sockets layer (SSL)

➤ transport layer security to any TCP-based app using SSL services.

➤ used between Web browsers, servers for e-commerce (shttp).

➤ security services:

- ★ server authentication
- ★ data encryption
- ★ client authentication (optional)

➤ server authentication:

- ★ SSL-enabled browser includes public keys for trusted CAs.
  - ★ Browser requests server certificate, issued by trusted CA.
  - ★ Browser uses CA's public key to extract server's public key from certificate.
- check your browser's security menu to see its trusted CAs.



# Secure sockets layer (SSL)

## Encrypted SSL session:

- Browser generates *symmetric session key*, encrypts it with server's public key, sends encrypted key to server.
- Using private key, server decrypts session key.
- Browser, server know session key
  - ★ All data sent into TCP socket (by client or server) encrypted with session key.

- SSL: basis of IETF Transport Layer Security (TLS).
- SSL can be used for non-Web applications, e.g., IMAP.
- Client authentication can be done with client certificates.



# IPsec: Network Layer Security

**FYORP**

## ➤ Network-layer secrecy:

- ★ sending host encrypts the data in IP datagram
- ★ TCP and UDP segments; ICMP and SNMP messages.

## ➤ Network-layer authentication

- ★ destination host can authenticate source IP address

## ➤ Two principle protocols:

- ★ authentication header (AH) protocol
- ★ encapsulation security payload (ESP) protocol

## ➤ For both AH and ESP, source, destination handshake:

- ★ create network-layer logical channel called a security association (SA)

## ➤ Each SA unidirectional.

## ➤ Uniquely determined by:

- ★ security protocol (AH or ESP)
- ★ source IP address
- ★ 32-bit connection ID



# Authentication Header (AH) Protocol

- provides source authentication, data integrity, no confidentiality
  - AH header inserted between IP header, data field.
  - protocol field: 51
  - intermediate routers process datagrams as usual
- AH header includes:**
- connection identifier
  - authentication data: source-signed message digest calculated over original IP datagram.
  - next header field: specifies type of data (e.g., TCP, UDP, ICMP)



IP header

AH header

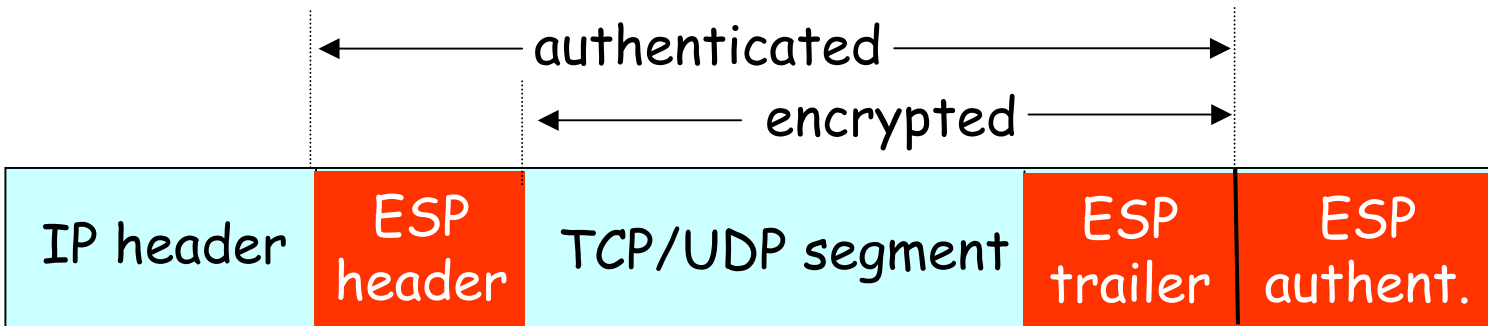
data (e.g., TCP, UDP segment)



# ESP Protocol

**FYORP**

- provides secrecy, host authentication, data integrity.
- data, ESP trailer encrypted.
- next header field is in ESP trailer.
- ESP authentication field is similar to AH authentication field.
- Protocol = 50.



## Further Reading

**FYORP**

- Security in IEEE 802.11
  - ★ Wireless Networks: - 802.11 a/b/g
  - ★ Security Mechanisms:
    - WEP – Wireless Equivalent Privacy
    - 802.11i
- Out of Scope!!!

~ **Best Wishes** ~

