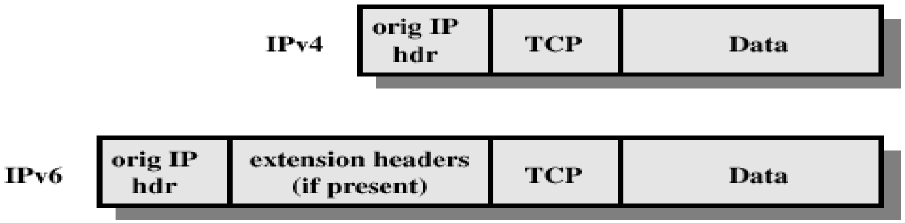
Tutorial 11 Solutions

CS5285

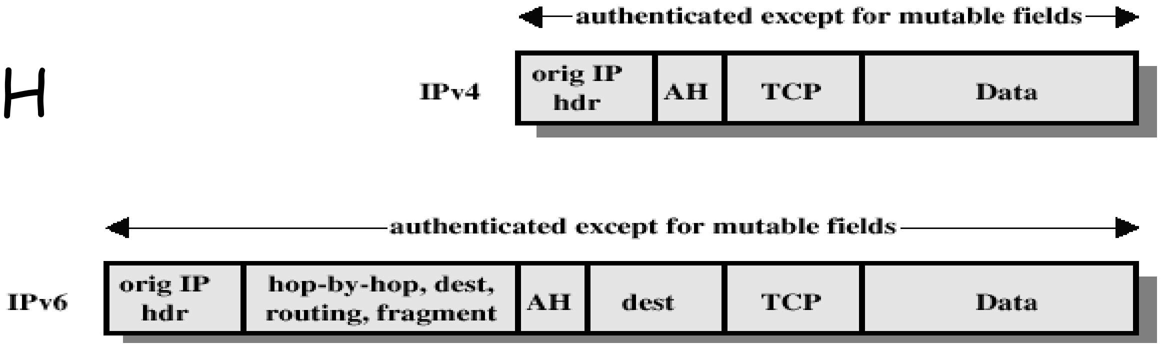
Gerhard Hancke

Authentication Header (AH) Protocol

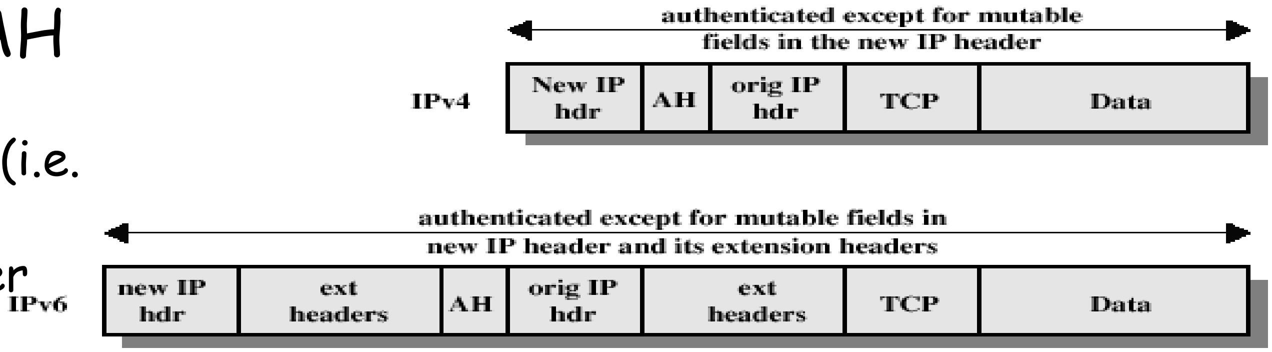
- Original IP packets



- Transport Mode AH
  - Host-to-host authentication

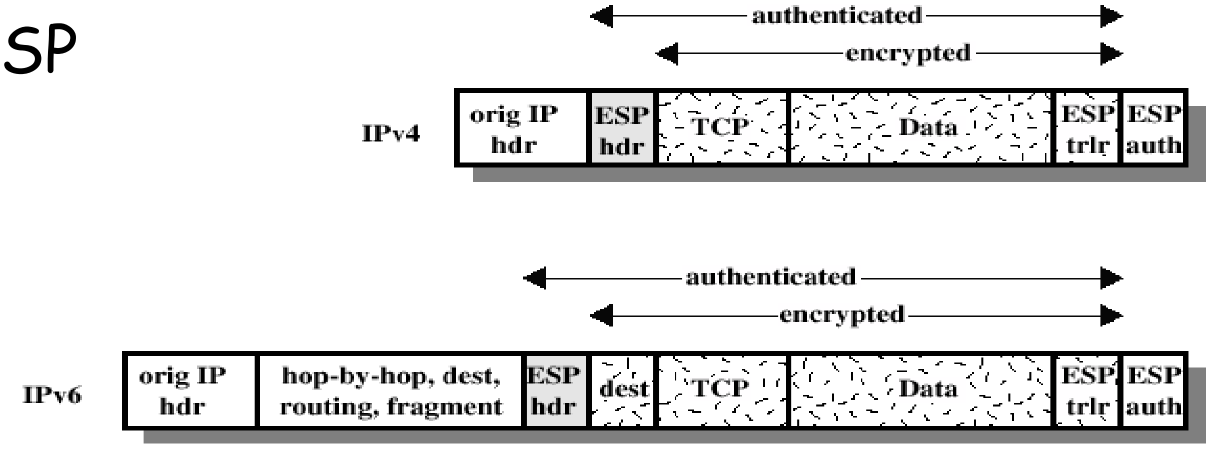

authenticated except for mutable fields
IPv4
orig IP hdr
AH
TCP
Data
authenticated except for mutable fields
IPv6
orig IP hdr
hop-by-hop, dest, routing, fragment
AH
dest
TCP
Data

- Tunnel Mode AH
  - Host-to-host
  - Host-to-router (i.e. remote access)
  - Router-to-router


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

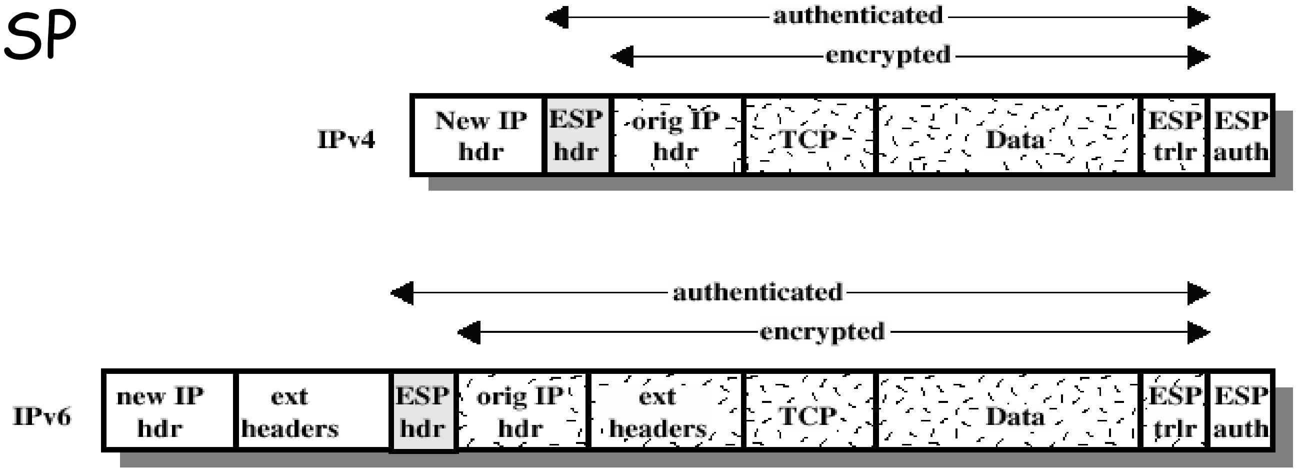
Encapsulating Security Payload (ESP) Protocol

- Transport Mode ESP



(a) Transport Mode

- Tunnel Mode ESP



(b) Tunnel Mode

Question 1

- (a) How many different methods are there if two hosts would like to authenticate packets between them?

Question 1

- **Solution to (1):** There are 4 methods:

(1) AH in transport mode

(2) AH in tunnel mode

(3) ESP with NULL encryption in transport mode

(4) ESP with NULL encryption in tunnel mode

How many modes if hosts want to encrypt messages?

Only 2 (ESP(3+4))

Question 1

(b) Can you think of an advantage of transport mode over tunnel mode if only authentication is required?

Solution: Transport mode has a slightly lower bandwidth overhead over tunnel mode.

Question 1

- (c) Can you think of a reason why in transport mode AH could be slightly better for authentication than ESP?
- **Solution:** AH provides somewhat stronger protection than ESP because it also protects the actual IP header fields.

Question 1

- (d) What is the purpose of padding when using ESP?

Question 1

- **Solution**: The padding in ESP has several purposes:

(1) If the encryption algorithm used is a block cipher and not a stream cipher then the padding is used to expand the plaintext to a multiple of the block size.

(2)Padding may also be used to conceal the actual length of the payload by adding a certain amount of padding.

Question 1

- (e) Discuss advantages/disadvantages to IKE main and aggressive mode.

Main mode advantages:

(1) The main mode protects the identity of the two entities involved in the exchange. An eavesdropper cannot learn the identities in the exchange.

(2) The system parameters such as g and p can be negotiated, thus there is no need to pre-share the parameter.

Aggressive mode advantage:

(1) The main mode obviously requires twice as many messages to complete.

Question 2(a)

- Attackers can gain knowledge about the plaintext of the message if the keystream happens to repeat. You are sending 10,000 new WEP messages, on average, every second. How long does the attacker need to wait for the keystream to repeat?
- WEP uses RC4 stream cipher. Keystream is function of what?
- IV and K (K stays the same, IV changes each message)
- IV is a 24-bit counter. How many possible values?
- Only 2^24 = 16.7 million
- If we send 10,000 message each second counter will start repeating after 0.5 hours.
- (2^24 /10,000)/60/60 = 0.466 hours

Question 2 (a)

- An attacker knows the plaintext of one of your messages. How can he modify the message so the receiver receives and accepts his new message?
- Standard stream cipher problem
- M= text||CRC_M, attacker has A= attack_text||CRC_A
- RC4 generates keystream KS
- C= M XOR KS, attacker recovers KS by KS = C XOR M
- Attacker makes C’ = A XOR KS
- Receiver recovers M’= C’ XOR KS instead of M

Question 2 (b)

- You wish to use public WiFi at the shopping mall but it is set up to use WEP. What can you do to ensure you have improved security for you connection?
  - Use a Virtual Private Network using something like IPSec (safest)
  - Make sure of TLS/SSL (https) connection (not guaranteed as some traffic can still be seen – like initial visit to website)

Question 3(a)

- What basic security services does a 2nd generation mobile network provide?
  - Authentication of mobile station (phone)
  - Encryption (only between phone and base station)

Note: Uses proprietary cryptography A3/A5/A8

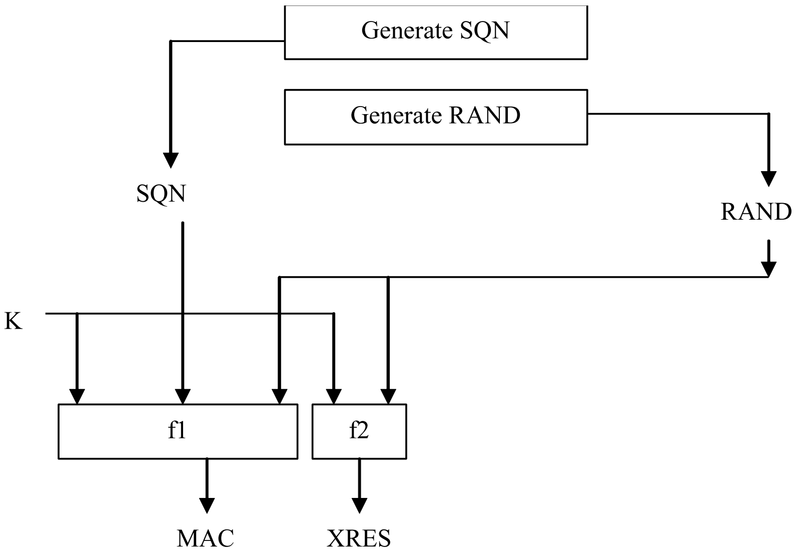
Question 3(b)

- What basic security services does a 3rd generation mobile network provide?
  - Mutual authentication
  - Encryption (plus integrity check MAC)
    - Extends to base station controller

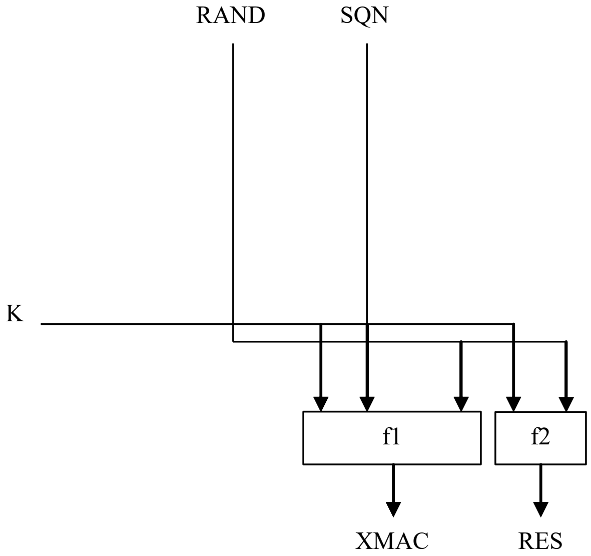
Note: Uses standard cryptography based on AES

Question 3c

AuC



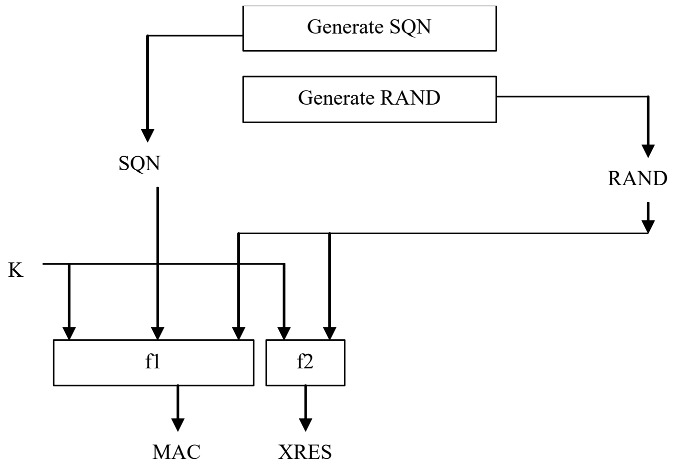
Mobile station



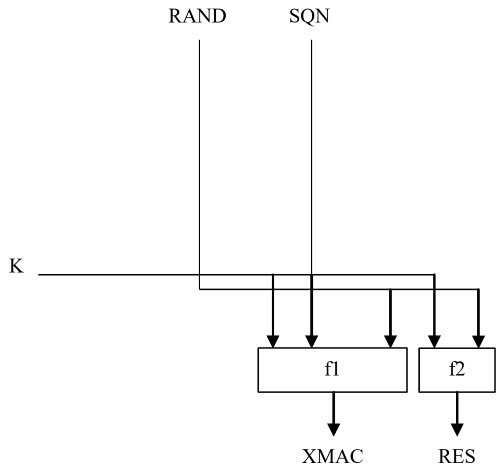
- Consider the simplified 3G system shown. Construct a suitable protocol and explain how mutual authentication is achieved.

Question 3c

AuC



Mobile station



- In this simplified system SQN is a logical timestamp (counter kept by AuC and MS)
- MAC, XRES and RAND passed to base station

  BS > MS: *MAC, RAND* (MS calculates XMAC and RES)

  MS > BS: *RES*

- If MS matches XMAC to MAC then network authenticated
  - SQN is the freshness, f1 (K,SQN,RAND) is the origin authentication
- If RES matches XRES then mobile station authenticated
  - RAND is the freshness and f2(K,RAND) is the origin authentication