FIT 3031 – Information and Network Security
Tutorial 8 Sample Solutions

Q1 Give examples of applications of IPSec.

Answer:

Secure branch office connectivity over the Internet: A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.

Secure remote access over the Internet: An end user whose system is equipped with IP security protocols can make a local call to an Internet service provider (ISP) and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecommuters.

Establishing extranet and intranet connectivity with partners: IPSec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.

Enhancing electronic commerce security: Even though some Web and electronic commerce applications have built-in security protocols, the use of IPSec enhances that security.

IPSec can assure that:

a. A router or neighbour advertisement comes from an authorized router
b. A redirect message comes from the router to which the initial packet was sent
c. A routing update is not forged

Q2 What are the services provided by IPSec?

Answer:

IPSec provides the following services:

Access control; *Prevention of unauthorized use of a resource*
connectionless integrity; *Assurance that received traffic has not been modified. Integrity includes anti-reply defenses*.
data origin authentication; *Assurance that traffic is sent by legitimate party or parties*.

rejection of replayed packets (a form of partial sequence integrity); *Replayed packet can be detected by the unique sequence number relationship to a SA and thus rejected.*
confidentiality (encryption); *Assurance that user's traffic is not examined by non-authorized parties* and
limited traffic flow confidentiality *Using tunnel mode,the entire IP packet is encrypted, the header info is limited*

Q3 What parameters identify an SA (security association) and what parameters characterize the nature of a particular SA?

Answer:
A security association (SA) is the establishment of shared security information between two network entities to support secure communications. An SA may include cryptographic keys, initialization vectors or digital certificates.
A security association is uniquely identified by three parameters:

1. **Security Parameters Index (SPI):** A bit string assigned to this SA and having local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.

2. **IP Destination Address:** Currently, only unicast addresses are allowed; this is the address of the destination endpoint of the SA, which may be an end user system or a network system such as a firewall or router. Unicast: The most common concept of an IP address is a unicast address. It normally refers to a single sender or a single receiver, and can be used for both sending and receiving. Usually, a unicast address is associated with a single device or host, but it is not a one-to-one correspondence. Some individual PCs have several distinct unicast addresses, each for its own distinct purpose

3. **Security Protocol Identifier:** This indicates whether the association is an AH or ESP security association.

A security association is normally defined by the following parameters:

1. **Sequence Number Counter:** A 32-bit value used to generate the Sequence Number field in AH or ESP headers, described in Section 6.3 (required for all implementations).

2. **Sequence Counter Overflow:** A flag indicating whether overflow of the Sequence Number Counter should generate an auditable event and prevent further transmission of packets on this SA (required for all implementations).

3. **Anti-Replay Window:** Used to determine whether an inbound AH or ESP packet is a replay, described in Section 6.3 (required for all implementations).

4. **AH Information:** Authentication algorithm, keys, key lifetimes, and related parameters being used with AH (required for AH implementations).

5. **ESP Information:** Encryption and authentication algorithm, keys, initialization values, key lifetimes, and related parameters being used with ESP (required for ESP implementations).

6. **Lifetime of this Security Association:** A time interval or byte count after which an SA must be replaced with a new SA (and new SPI) or terminated, plus an indication of which of these actions should occur (required for all implementations).

7. **IPSec Protocol Mode:** Tunnel, transport, or wildcard (required for all implementations). These modes are discussed later in this section.

8. **Path MTU:** Any observed path maximum transmission unit (maximum size of a packet that can be transmitted without fragmentation) and aging variables (required for all implementations).

Q4 What is the difference between transport mode and tunnel mode?

Answer:
Transport mode provides protection primarily for upper-layer protocols. That is, transport mode protection extends to the payload of an IP packet. Transport mode is meant to be used between two fixed hosts, or to put it another way, when the VPN endpoints are the final destinations of the traffic in the VPN. In particular, transport mode cannot be used to connect two networks or a network and a host.

Tunnel mode provides protection to the entire IP packet.
The typical use of tunnel mode is to connect either two networks or a host and a network: for example, a remote office network to a home office network. It is more flexible than transport mode, but this flexibility comes at the expense of increased bandwidth requirements.

Q5 What is a replay attack and how can IPSec prevent it?

Answer:
A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence.

The sequence number field in AH or ESP header associated with a particular SA is not duplicated. When a packet with duplicated sequence number with same SA is received, it is discarded.

Q6 Why does ESP include a padding field?

Answer:
It is included for the following reasons:

1. If an encryption algorithm requires the plaintext to be a multiple of some number of bytes (e.g., the multiple of a single block for a block cipher), the Padding field is used to expand the plaintext (consisting of the Payload Data, Padding, Pad Length, and Next Header fields) to the required length.

2. The ESP format requires that the Pad Length and Next Header fields be right aligned within a 32-bit word. Equivalently, the ciphertext must be an integer multiple of 32 bits. The Padding field is used to assure this alignment.

3. Additional padding may be added to provide partial traffic flow confidentiality by concealing the actual length of the payload.

Q7 What are the roles of the Oakley key determination protocol and ISAKMP in IPSec?

Answer:

ISAKMP by itself does not dictate a specific key exchange algorithm; rather, ISAKMP consists of a set of message types that enable the use of a variety of key exchange algorithms. Oakley is the specific key exchange algorithm mandated for use with the initial version of ISAKMP, using the Diffie-Hellman key exchange algorithm.
Oakley Key determination protocol is a key exchange protocol based on the Diffie-Hellman algorithm but providing added security. Oakley is generic in that it does not dictate specific formats.

ISAKMP provides a framework for Internet key management and provides the specific protocol support, including formats, for negotiation of security attributes.
ISAKMP defines procedures and packet formats to establish, negotiate, modify and delete security associations.
It defines payloads for exchanging key generation and authentication data. It provides a consistent framework independent of the key exchange protocol, encryption algorithm, and authentication mechanism.

Q8 What are the basic approaches to bundling SAs?

Answer:
Transport adjacency: Refers to applying more than one security protocol to the same IP packet, without invoking tunneling. This approach to combining AH and ESP allows for only one level of combination; further nesting yields no added benefit since the processing is performed at one IPSec instance: the (ultimate) destination.
Iterated tunneling: Refers to the application of multiple layers of security protocols affected through IP tunneling. This approach allows for multiple levels of nesting, since each tunnel can originate or terminate at a different IPSec site along the path.

PROBLEMS:

1. Describe and explain each of the entries in the Table 8.2.

Table 8.2 Host SPD Example

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

Answer:
row 1: Traffic between this host and any other host, both using port 500, and

using UDP, bypasses IPsec. This is used for IKE traffic.

row 2: ICMP message to or from any remote address are error messages, and bypass IPsec.

row 3: Traffic between 1.2.3.101 and 1.2.3.0/24 is intranet traffic and must be protected by ESP, with the exception of traffic defined in earlier rows.

row 4: TCP traffic between this host (1.2.3.101) and the server (1.2.4.10) on server port 80 is ESP protected.

row 5: TCP traffic between this host (1.2.3.101) and the server (1.2.4.10) on server port 443 is protected by HTTPS secure socket SSL/TLS and so can bypass IPsec.

row 6: Any other traffic between 1.2.3.101 and 1.2.4.0/24 is prohibited and is discarded.

row 7: Any other traffic between 1.2.3.101 goes to the Internet and bypasses IPsec.

2. Draw a Figure similar to Figure 8.8 for AH.

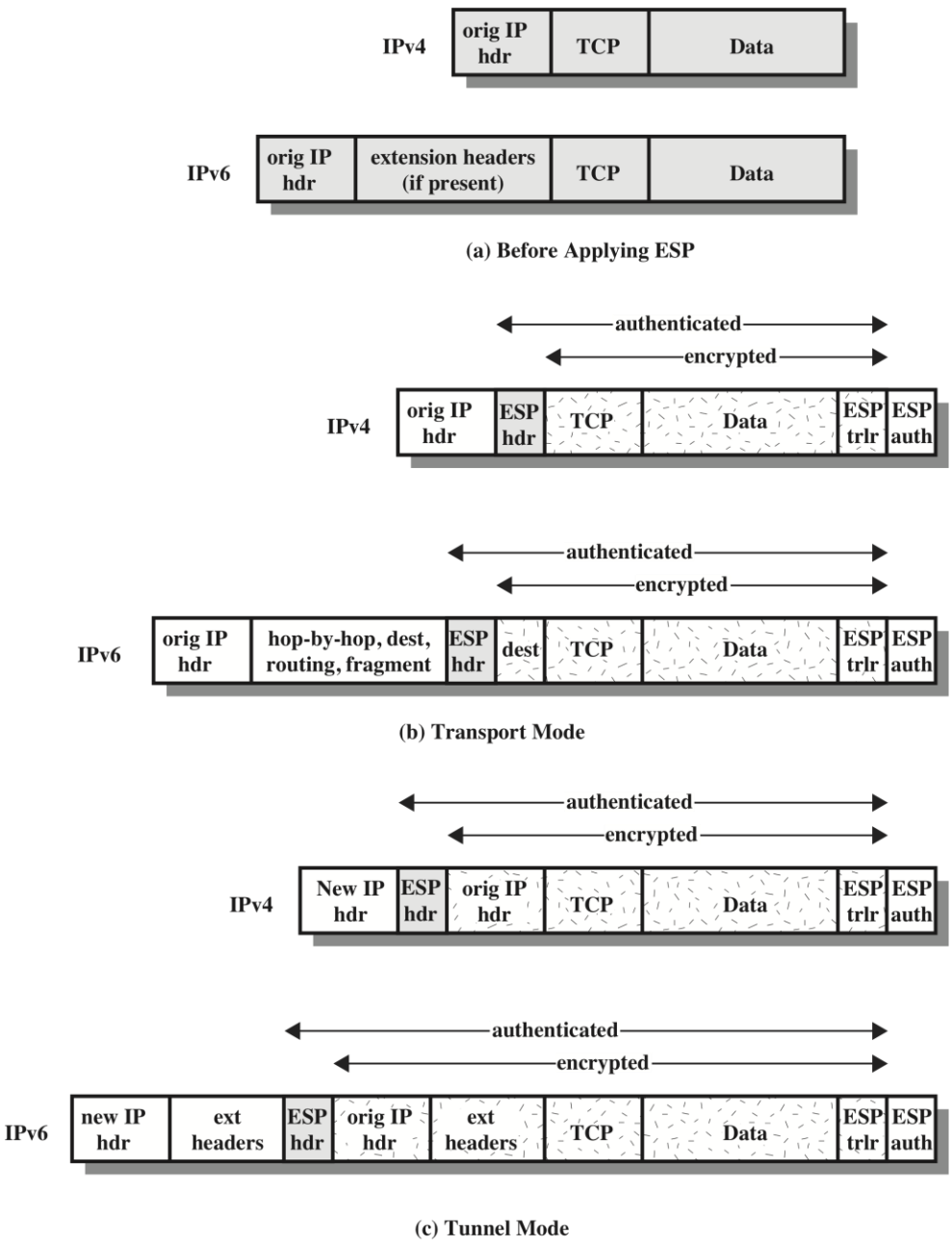
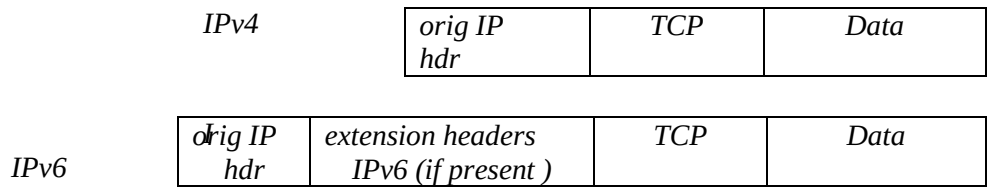
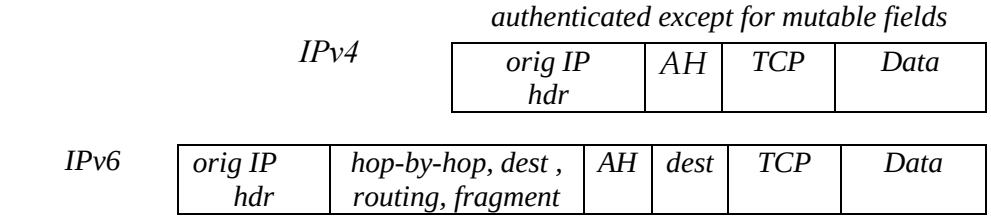


Figure 8.8 Scope of ESP Encryption and Authentication

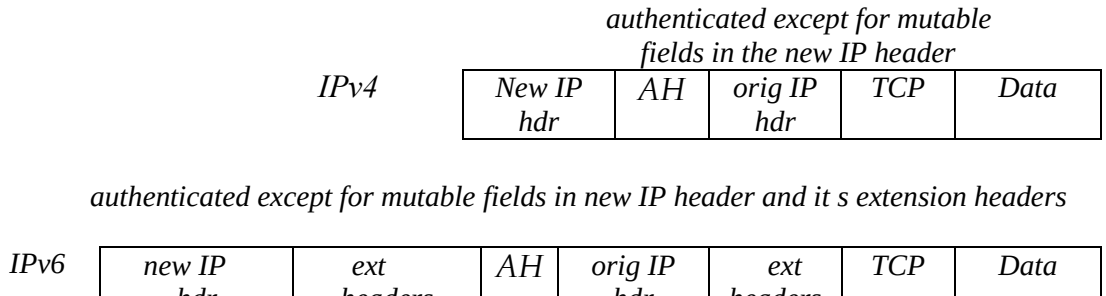
Answer: The Figure for AH is given below:



a) Before Applying AH



b) Transport Mode



c) Tunnel Mode

3. List the major security services provided by AH and ESP respectively.

Answer:
AH provides access control, connectionless integrity, data origin authentication, and rejection of replayed packets. ESP provides all of these plus confidentiality and limited traffic flow confidentiality.

4. The IPSec architecture document states that when two transport mode SAs are bundled to allow for both AH and ESP protocols on the same end-to-end flow, only one ordering of security protocols seems appropriate: performing

the ESP protocol before performing the AH protocol. Why is this approach recommended rather than authentication before encryption?

Answer:
This order of processing facilitates rapid detection and rejection of replayed or bogus packets by the receiver, prior to decrypting the packet, hence potentially reducing the impact of denial of service attacks. It also allows for the possibility of parallel processing of packets at the receiver, i.e., decryption can take place in parallel with authentication.

5. Where does IPSec reside in a protocol stack?

Answer:
It is an addition to the IP layer.