s

SNS COLLEGE OF ENGINEERING

AN AUTONOMOUS INSTITUTION

Accredited by NAAC – UGC with 'A' Grade

Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

19EC625 – CYBER FORENSIC AND DATA SECURITY

UNIT I

NETWORK LAYER SECURITY &TRANSPORT LAYER SECURITY

IPSec Protocol – IP Authentication Header – IP ESP – Key Management Protocol for IPSec. Transport layer Security: SSL protocol, Cryptographic Computations – TLS Protocol.

Part-A

1. **Define IPsec Protocol.**

The IPsec protocol is a set of security extensions developed by the IETF and it provides Privacy and authentication services at the IP layer by using modern cryptography. To protect the contents of an IP datagram, the data is transformed using encryption algorithms.

There are two main transformation types that form the basics of IPsec,

1. The Authentication Header (AH).
2. The Encapsulating Security Payload (ESP).

- ✓ Both AH and ESP are two protocols that provide connectionless integrity, data origin authentication, confidentiality and an anti-replay service.

2. **write the basic components of IPsec architecture Protocol.**

The basic components of the IPsec security architecture are explained in terms of the following functionalities:

- Security Protocols for AH and ESP
- Security Associations for policy management and traffic processing
- Manual and automatic key management for the Internet Key Exchange (IKE), the Oakley key determination protocol and ISAKMP.
- Algorithms for authentication and encryption

3. Define IPsec Protocol Documents

The seven-group documents describing the set of IPsec protocols are explained in the following:

***Architecture*:**

The main architecture document covers the general concepts, security Requirements, definitions and mechanisms defining IPsec technology.

ESP:

This document covers the packet format and general issues related to the use of the ESP for packet encryption and optional authentication.

***AH*:**

This document covers the packet format and general issue related to the use of AH for packet authentication.

Encryption algorithm:

This is a set of documents that describe how various encryptions algorithms are used for ESP.

***Authentication algorithm*:**

This is a set of documents that describe how various authentication algorithms are used for AH and for the authentication option of ESP.

***Key management*:**

This is a set of documents that describe key management schemes. These documents also provide certain values for the DOI. Currently the key management represents the Oakley, ISAKMP and Resolution protocols.

***DOI* :**

This document contains values needed for the other documents to relate each other. These include identifiers for approved encryption and authentication algorithms, as well as operational parameters such as key lifetime.

4. Define Security Associations (SAs)

An SA is a simplex connection between a sender and receiver that affords security services to the traffic carried on it. If both AH and ESP protection are applied to a traffic stream, then two SAs are required for two-way secure exchange.

An SA is uniquely identified by three parameters as follows:

- ***Security Parameters Index (SPI)***
- ***IP Destination Address***
- ***Security Protocol Identifier***

5. **Define Hashed Message Authentication Code (HMAC)**

- ✓ A mechanism that provides a data integrity check based on a secret key is usually called the Message Authentication Code (MAC).
- ✓ An HMAC mechanism can be used with any iterative hash functions in combination with a secret key.
- ✓ MACs are used between two parties (e.g. client and server) that share a secret key in order to validate information transmitted between them. An MAC mechanism based on a cryptographic hash function is called HMAC. MD5 and SHA-1 are examples of such hash functions. HMAC uses a secret key for computation and verification of the message authentication values.

6. **Define IP Authentication Header.**

- ✓ The IP AH is used to provide data integrity and authentication for IP packets.
- ✓ It also provides protection against replays. The AH provides authentication for the IP header, as well as for upper-level protocol (TCP, UDP) data.
- ✓ But some IP header fields may change in transit and the sender may not be able to predict the value of these fields when the packet arrives at the receiver.
- ✓ The AH can be used in conjunction with ESP or with the use of tunnel mode. Security services can be provided between a pair of hosts, between a pair of security gateway or between a security gateway and a host.

7. **Draw AH Format.**

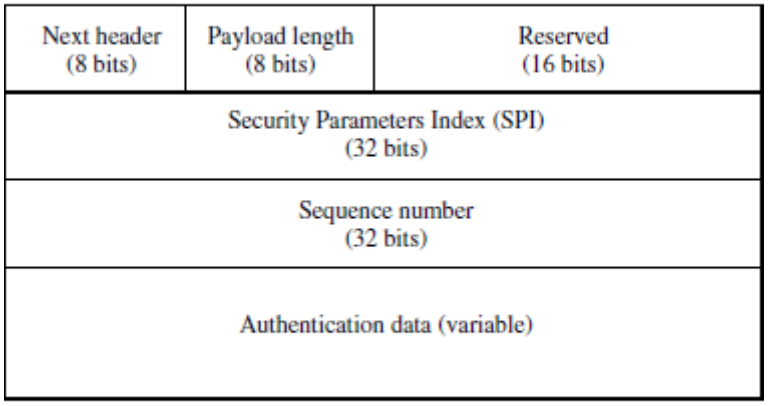

Figure 7.4 IPsec AH format.

8. **Define IP ESP.**
   - ✓ The ESP header is designed to provide security services in IPv4 and IPv6. ESP can be applied alone, in combination with the IP AH or through the use of tunnel mode.
   - ✓ Security services are provided between a pair of hosts, between a pair of security gateways or between a security gateway and a host.
   - ✓ The ESP header is inserted after the IP header and before the upper-layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode).
   - ✓ ESP is used to provide confidentiality (encryption), data authentication, integrity and anti-replay service, and limited traffic flow confidentiality. Confidentiality could be selected independent of all other services.
9. **Define Packet Format**

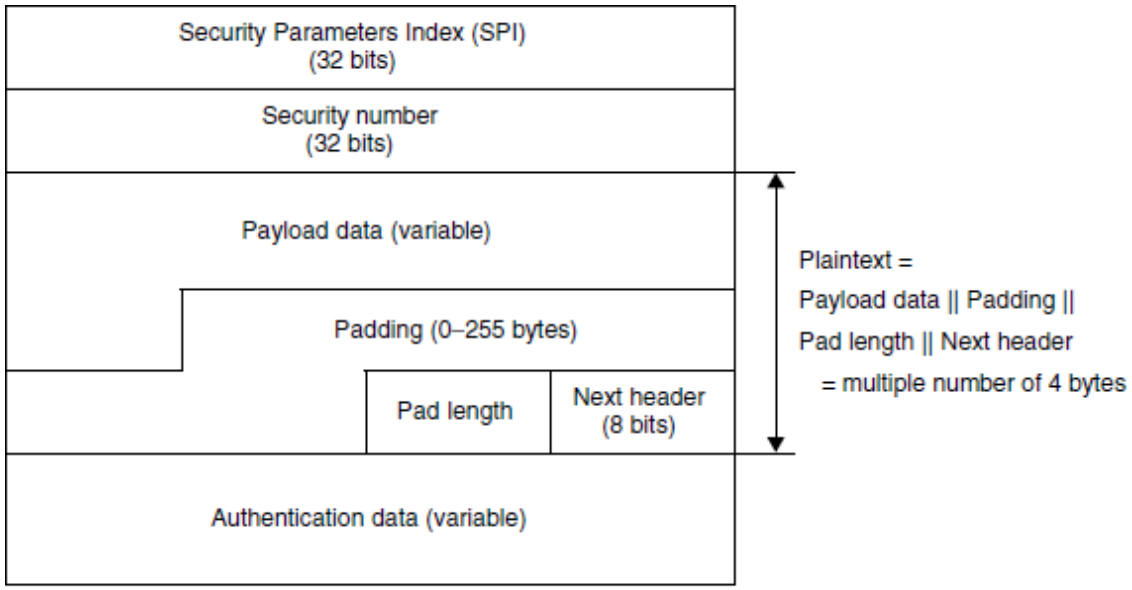

Figure 7.6 IPsec ESP format.

8. Define Key Management Protocol for IPSec.

- ✓ The key management mechanism of IPsec involves the determination and distribution of a secret key. Key establishment is at the heart of data protection

that relies on cryptography.

- ✓ A secure key distribution for the Internet is an essential part of packet protection.
- ✓ Prior to establishing a secure session, the communicating parties need to negotiate the terms that are defined in the SA. An automated protocol is needed in order to establish the SAs for making the process feasible on the Internet. This automated process is the IKE.
- ✓ IKE combines ISAKMP with the Oakley key exchange. We begin our discussion with an overview of Oakley and then look at ISAKMP.

1. **OAKLEY Key Determination Protocol**
2. **ISAKMP**

9. **List out the different types of Payload Types for ISAKMP.**

1. Security Association Payload
2. Proposal Payload
3. Transform Payload
4. Key Exchange Payload
5. Identification Payload
6. Certificate Payload
7. Certificate Request Payload
8. Hash Payload
9. Signature Payload
10. Nonce Payload
11. Notification Payload
12. Delete Payload
13. Vendor ID Payload

10. Define SSL Protocol.

- SSL is a layered protocol. It is not a single protocol but rather two layers of protocols.
- At the lower level, the SSL Record Protocol is layered on top of some reliable transport protocol such as TCP.
- The SSL Record Protocol is also used to encapsulate various higher level protocols. A higher-level protocol can layer on top of the SSL protocol

transparently.

11. Draw the SSL Protocol Overview stack.

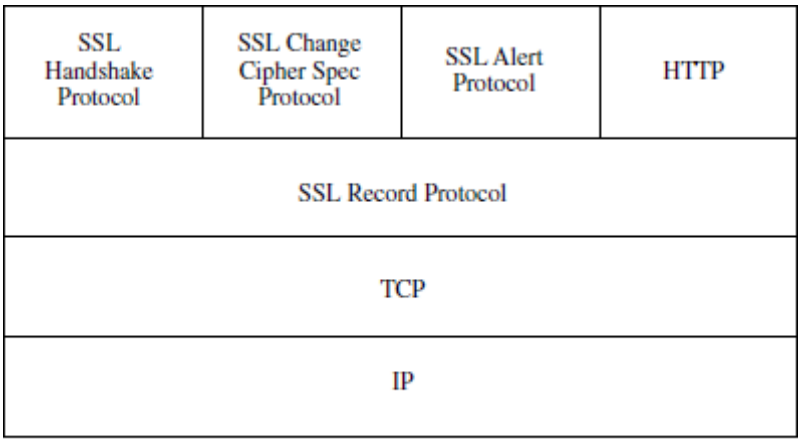

Figure 8.1 Two-layered SSL protocols.

12. Difference between SSL Session and SSL Connection.

SSL Session	***SSL Connection***
An SSL session is an association between a client and a server.	A connection is a transport (in the OSI layering model definition) that provides a suitable type of service.
They define a set of cryptographic security parameters, which can be shared among	For SSL, such connections are peer-to-peer relationships.
multiple connections.	
Sessions are created by the Handshake Protocol.	The connections are transient.
An SSL session coordinates the states of the client and server.	Every connection is associated with one session.

13. List out the SSL session elements.

1. Session identifier
2. Peer certificate
3. Compression method
4. Cipher spec:
5. Master secret
6. Is resumable

14. List out the SSL Connection elements.

1. Server and client random
2. Server write MAC secret
3. Client write MAC secret
4. Server write key
5. Client write key
6. Initialization vectors
7. Sequence numbers

15. Define SSL Record Protocol format.

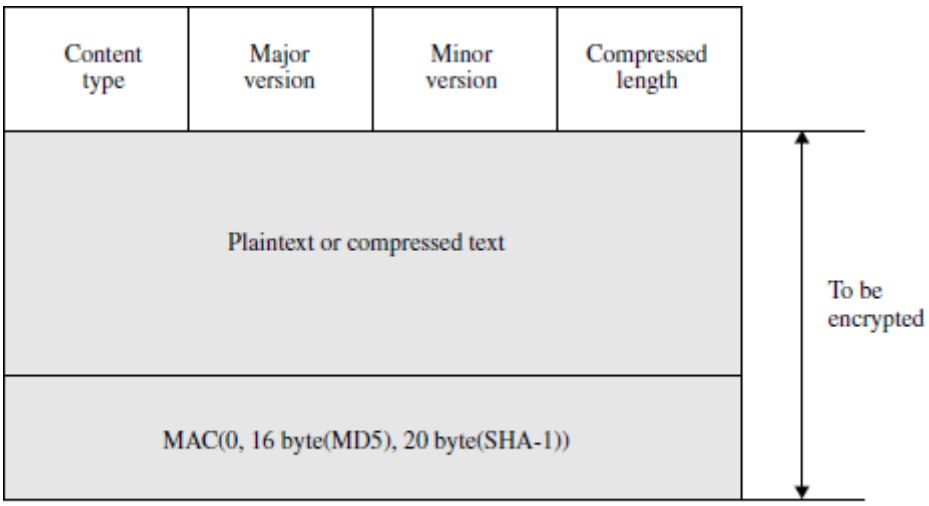

Figure 8.4 SSL Record Protocol format.

16. List out the phases of SSL Handshake Protocol.

- *Phase 1: Hello Messages for Logical Connection*
- Phase 2: Server Authentication and Key Exchange
- *Phase 3: Client Authentication and Key Exchange*
- *Phase 4: End of Secure Connection*

17. How to compute the master-secret for *Diffie–Hellman.*

master_secret = MD5(pre_master_secret||SHA('A'||
pre_master_secret||ClientHello.random||
ServerHello.random))||
MD5(pre_master_secret||SHA('BB'||

pre_master_secret||ClientHello.random||
ServerHello.random))||
MD5(pre_master_secret||SHA('CCC'||
pre_master_secret||ClientHello.random||
ServerHello.random))

18. Define HMAC-Algorithm and how to calculate the HMAC Algorithm.

A Keyed-hashing Message Authentication Code (HMAC) is a secure digest of some data protected by a secret. Forging the HMAC is infeasible without knowledge of the MAC secret. HMAC can be used with a variety of different hash algorithms, namely MD5 and SHA-1, denoting these as HMAC MD5(secret, data) and HMAC SHA-1(secret, data).

$$\text{HMAC} = H[(K \oplus \text{opad})||H[(K \oplus \text{ipad})||M]]$$

where

ipad = 00110110*(*0x36*)* repeated 64 times (512 bits)

opad = 01011100*(*0x5c*)* repeated 64 times (512 bits)

H = one-way hash function for TLS (either MD5 or SHA-1)

M = message input to HMAC

K = padded secret key equal to the block length of the hash code (512 bits for MD5 and SHA-1)

19. List out the ISAKMP Payload Processing.

1. General Message Processing
2. ISAKMP Header Processing
3. Generic Payload Header Processing
4. Security Association Payload Processing
5. Proposal Paylaod Processing
6. Proposal Paylaod Processing
7. Transform Payload Processing
8. Key Exchange Payload Processing

9. Identification Payload Processing
10. Certificate Payload Processing
11. Certificate Request Payload Processing
12. Hash Payload Processing
13. Signature Payload Processing
14. Delete Payload Processing
15. Nonce Payload Processing
16. Notification Payload Processing

20. Define Cryptographic Computations.

- The key exchange, authentication, encryption and MAC algorithms are determined by the cipher suite selected by the server and revealed in the server hello message.
- The compression algorithm is negotiated in the hello messages, and the random values are exchanged in the hello messages.
- The creation of a shared master secret by means of the key exchange and the generation of cryptographic parameters from the master secrete.
  - ✓ the ICV and the comparison rules and processing steps for validation.

✓ message, both parties immediately close the connection.

Part-B

1. Explain in detail about the IPSec Protocol.
2. Write short notes on the following protocol:
   - ✓ IP Authentication Header
   - ✓ IP ESP
3. Explain in detail about the Key Management Protocol for IPSec.
4. Explain in detail about the SSL protocol in Transport layer Security.
5. Explain in detail about the Cryptographic Computations in Transport layer Security.
6. Explain in detail about the TLS Protocol in Transport layer Security.