UNIT-5

Network and Internet security.

PART-A

(1) Internet Mail Architecture (components, protocols)

(2) Email Format

(3) Email Threats and comprehensive Email security.

(4) S/MIME

PART-B

(1) IP security overview

(2) Ip security policy

(3) Encapsulating security payload.

(4) Internet Key Exchange.

PART-A

1. Internet Mail Architecture (Components, protocols)

(1) The internet mail architecture is currently defined in RFC 5598 (Internet mail Architecture, July 2009)

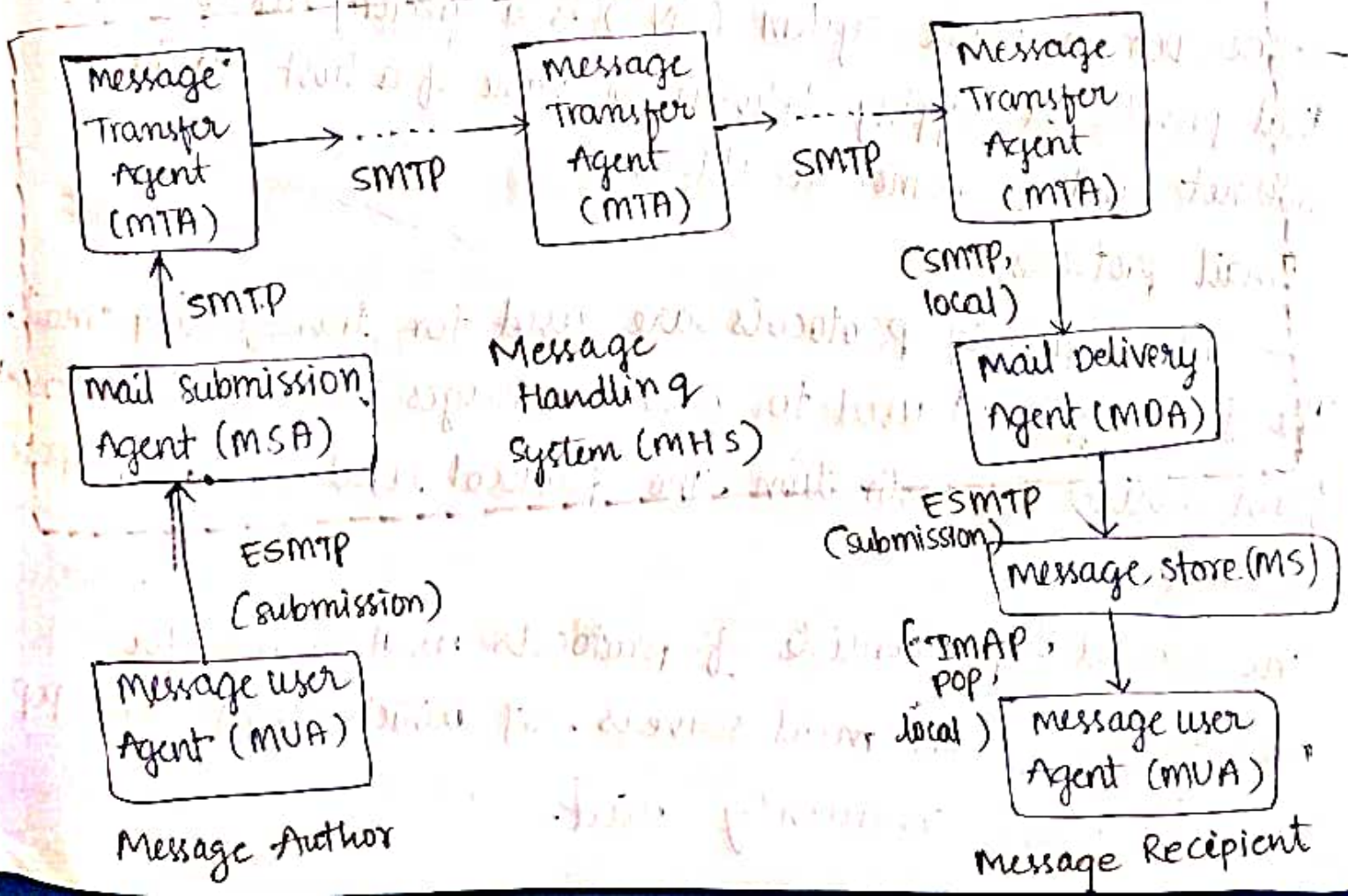
Email Components:

At its most fundamental level, the internet mail architecture consists of a user world in the form of Message user Agents (MUA), and the Transfer world, in the form of the Message Handling service (MHS), which is composed of Message Transfer Agents (MTA).

The key components of the Internet Mail Architecture which includes the following

(1) Message User Agent (MUA):

Message user Agent operates on behalf of user actors and user applications. It is their representative within the email service



(2) Mail Submission Agent (MSA)

Mail submission Agent accepts the message submitted by an MUA and enforces the policies of the hosting domain and the requirements of internal standards.

(3) Message Transfer Agent (MTA):

Message Transfer Agent Relays mail from one application-level hop. It is like a packet switch or IP router inthat its job is to make routing assessments and to move the message closer to the recipients.

(4) Mail delivery Agent (MDA)

mail delivery Agent is responsible for transferring the message from the MHS to the MS.

(5) Message store (MS):

An MUA can employ a long-term MS. An MS can be located on a remote server or on the same machine as the MUA.

→ The Domain Name system (DNS) is a directory look up service that provides a mapping between the name of a host on the Internet and its numerical address.

Email protocols:

Two types of protocols are used for transferring email. The first type is used to move messages through the internet from source to destination. The protocol used for this purpose is SMTP.

The second type consists of protocols used to transfer messages between mail servers, of which IMAP and POP are the most commonly used.

Simple Mail Transfer protocol (SMTP)

(1) SMTP encapsulates an email message in an envelope and is used to relay the encapsulated messages from source to destination through multiple MTA's.

(2) SMTP is a text-based client server protocol where the client (email sender) contacts the server (next-hop recipient) and issues a set of commands to tell the server about the message to be sent, then sending the message itself.

(3) The transfer of a message from the source to its ultimate destination can occur over a single SMTP client/server conversation over a single TCP connection.

(4) The operation of SMTP consists of a series of commands and responses exchanged between the SMTP sender and receiver. The initiative is with the SMTP sender, who establishes the TCP connection. once the connection is established, the SMTP sender sends commands over the connection to the receiver.

2. Email Formats.

There are two types of E-mail Formats. They are,

(1) RFC 5322

(2) MIME.

(1) RFC 5322 :

→ RFC 5322 defines a format for text messages that are sent using electronic mail.

→ The overall structure of a message that conforms to RFC 5322 is very simple.

→ A message consists of some number of header lines

(the header) followed by unrestricted text (the body).

Header
Date: December 11, 2023 1:21:25 PM EDT
From: "William stallings" <ws@shore.net>
Subject: The syntax in RFC 5322
TO: smith@other-host.com
CC: Jones@yet-Another-Host.com

Body
Hello. This section begins the actual message body, which is delimited from the message heading by a blank line.

(2) MIME (multipurpose Internet Mail Extension)

(1) Multipurpose Internet mail Extension (MIME) is an extension to the RFC 5322

(2) The Five header Fields defined in MIME are as follows.

(a) MIME-Version

Must have the parameter value 1.0. This Field Indicates that the message conforms to the RFC's 2045 and 2046

(b) Content-Type:

Describes the data contained in the Body with sufficient detail that the receiving user agent can pick an appropriate agent or mechanism to represent the data to the user or otherwise deal with the data in an appropriate manner.

(c) Content - Transfer - Encoding :

Indicates the type of Transformation that has been used to represent the body of the message in a way that is acceptable for mail Transport.

(d) Content - ID :

used to identify MIME entities uniquely in multiple contexts.

(e) Content - Description :

A Text - Description of the object with the body. This is useful when the object is not readable (eg. audio data)

MIME content types :

(1) Text : unformatted Text ; may be ASCII or ISO 8859.

(2) Message : The Body is itself an encapsulated message that conforms to RFC 822

(3) Image : The image is in JPEG Format ; JFIF encoding.

(4) Video : MPEG Format.

(5) Audio : Single - channel 8-bit

(6) Application : Adobe postscript format.

MIME Transfer Encodings :

(1) 8-bit : The lines are short, but there may be non-ASCII characters.

(2) Binary : Not only may non-ASCII characters be present but the lines are not necessarily short enough for SMTP Transport.

(3) Base 64 : Encodes data by mapping 6-bit blocks of input to 8-bits blocks of output, all of which are

printable ASCII characters.

3. Email Threats and comprehensive Email security.

Email Threats:

(1) Authenticity related Threats: could result in unauthorized access to an enterprise's email system.

(2) Integrity - related Threats: could result in unauthorized modification of email content.

(3) Confidentiality - related Threats: could result in unauthorized disclosure of sensitive information.

(4) Availability - reated Threats: could prevent end users from being able to send or receive Email.

Email security:

(1) STARTTLS: An SMTP security extension that provides authentication, integrity, non-repudiation (via digital signatures) and confidentiality (via encryption) for the entire SMTP message by running SMTP over TLS.

(2) S/MIME: provides authentication, integrity, non repudiation (via digital signatures) and confidentiality (via encryption) of the message body carried in SMTP messages.

(3) DNS Security Extensions (DNSSEC):

provides authentication and integrity protection of DNS data, and is an underlying tool used by various email security protocols.

(4) DNS-based Authentication of Named Entities (DANE):

It is designed to overcome problems in the certificate authority (CA) system by providing an alternative channel for authenticating public keys based on DNSSEC, with the result that the same trust relationships used to certify IP addresses are used to certify servers operating on those addresses.

(5) Sender policy Framework (SPF):

uses the Domain Name system (DNS) to allow domain owners to create records that associate the domain name with a specific IP address range of authorized message senders.

4. S/MIME.

Secure/Multipurpose Internet mail Extension (S/MIME) is a security enhancement to the MIME Internet email format standard based on Technology from RSA.

The most important documents relevant to S/MIME include the following.

(1) RFC 5750, S/MIME version 3.2 certificate Handling:

specifies conventions for X.509 certificate usage by (S/MIME) V 3.2

(2) RFC 5751, S/MIME version 3.2 Message specification:

The principal defining document for S/MIME message creation and processing.

(3) RFC 4134, Examples of S/MIME messages:

Gives examples of message bodies formatted using

S/MIME.

(4) RFC 2634, Enhanced security services for S/MIME:

Describes four optional security service extension for S/MIME.

(5) RFC 5652, Cryptographic Message syntax (CMS):

Describes the cryptographic message syntax (CMS). This syntax is used to digitally sign, digest, authenticate, or crypt arbitrary message content.

(6) RFC 3370, CMS Algorithms:

Describes the conventions for using several cryptographic algorithms with the CMS.

(7) RFC 5752, Multiple signatures in CMS:

Describes the use of multiple, parallel signatures for a message.

(8) RFC 1847, Security Multiparts for MIME - Multipart/Signed and Multipart/Encrypted:

Defines a Framework within which security services may be applied to mime Body parts. The use of a digital signature is relevant to S/MIME, as explained subsequently.

Operational description:

S/MIME provides for four message-related services. They are

(1) Authentication
(2) Confidentiality
(3) Compression
(4) Email compatibility.

(1) Authentication :

→ Authentication uses the Digital signatures Function and uses the algorithm called RSA | SHA - 256.

→ The action done by Authentication is a hash code of a message is created using SHA - 256. This message digest is encrypted using SHA - 256 with the sender's private key and included with the message.

(2) Confidentiality :

→ confidentiality uses the message encryption function and uses the algorithm called AES-128 with CBC.

→ The action done by confidentiality is a message is encrypted using AES - 128 with CBC with a one-time session key generated by the sender. The session key is encrypted using RSA with the recipients public key and included with the message.

(3) Compression :

→ compression itself used the compression function with an unspecified Algorithm.

→ The action performed by compression is a message may be compressed for storage or Transmission.

(4) Email compatibility :

→ Email compatibility itself used the email compatibility and uses the algorithm called Radix - 64 conversion.

→ The action performed by the Email compatibility to provide transparency for email applications, an encrypted message may be converted to an ASCII string using radix - 64

Conversion.

→ S/MIME provides confidentiality by encrypting messages. Most commonly AES with a 128-bit key, is used, with the cipher block chaining (CBC) mode. The key itself is also encrypted. typically with RSA.

S/MIME Content types:

S/MIME Message content types.

S/MIME uses the following message content types, which are defined in RFC 5652, Cryptographic Message syntax.

(1) Data: Refers to the inner MIME-encoded message content, which may then be encapsulated in a signed Data, Enveloped data or compressed data content type.

(2) Signed Data: used to apply a digital signature to a message

(3) Enveloped Data: This consists of encrypted content of any type and encrypted content encryption keys for one or more recipients.

(4) Compressed data: used to apply data compression to a message.

PART-B: IP security

(1) Ip security overview.

Ip security overview consists of

(1) Applications of Ipsec
(2) Benefits of Ipsec
(3) Ipsec documents
(4) Ip sec services
(5) Transport and Tunnel modes.

(1) Applications of Ipsec :

Ipsec provides the capability to secure communications across a LAN, across private and public WAN's and across the Internet. Examples of its use include.

(i) 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, save costs and network management overhead.

(ii) 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 travelling employees and Telecommuters.

(iii) 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.

(iv) Enhancing electronic commerce security:

Even through some web and electronic commerce applications have built in security protocols, the use of Ipsec enhances that security. Ipsec guarentees that all traffic designated by the network administrator is both encrypted and authenticated, adding an additional layer of security to whatever is provided at the application layer.

(2) Benefits of Ipsec:

Some of the Benefits of Ipsec:

(1) When Ipsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.

(2) Ipsec in a Firewall is resistant to bypass if all traffic from the outside must use Ip and the firewall is the only means of entrance from the Internet into the organization.

(3) Ipsec is below the Transport layer (TCP, UDP) and so is transparent to applications. There is no need to change software on a user or server system when Ipsec is implemented in the firewall or router. Even if Ipsec is implemented in end systems, upper-layer software, including applications, is not affected.

(4) Ipsec can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material

when users leave the organization.

(5) Ipsec can provide security for individual users if needed. This is useful for off-site workers and for setting up a secure virtual subnetwork within an organization for sensitive applications.

(3) Ipsec Documents:

The documents can be categorized into the following groups.

(i) Architecture:

Covers the general concepts, security requirements, definitions and mechanisms defining Ipsec Technology. The current specification is RFC 4301, security Architecture for the internet protocol.

(ii) Authentication Header (AH):

AH is an extension header to provide message authentication. The current specification in RFC 4302, Ip authentication Header. Because message authentication is provided by Esp, the use of AH is deprecated. It is included in $Ipsec V_3$ for backward Compatibility but should not be used in new applications.

(iii) Encapsulating security payload (ESP):

Esp consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication. The current specification is RFC 4303, Ip Encapsulating security payload (ESP)

(iv) Internet key Exchange (IKE):

This is a collection of documents describing the key management schemes for use with Ipsec. The main specification is RFC 7296, Internet Key Exchange (IKE) V_2 protocol, but there are a number of related RFC's

(V) Cryptographic Algorithms:

This category encompasses a large set of documents that define and describe cryptographic algorithms for encryption and message authentication, pseudorandom functions (PRF's) and cryptographic key exchange.

(4) Ip sec services:

→ Access control
→ Connectionless integrity
→ Data origin authentication
→ Rejection of replayed packets (a form of partial sequence integrity)
→ Confidentiality (encryption)
→ Limited Traffic flow confidentiality

(5) Transport and Tunnel modes:

Both AH and ESP support two modes of use:
Transport and Tunnel mode.

→ Transport mode: Transport mode provides protection primarily for upper-layer protocols.

→ Tunnel mode: Tunnel mode provides protection to the entire Ip packet.

(2) Ip security policy:

Ip security policy consists of
(1) Security Associations
(2) Security Association DataBase
(3) Security policy DataBase.

→ Security policy applied to each Ip packet that transits from a source to a destination.

→ Ip sec policy is determined primarily by the interaction of two databases, The security association database (SAD) and the security policy database (SPD).

(I) Security Associations:

A security association is uniquely identified by Three parameters.

(i) Security parameters Index (SPI):

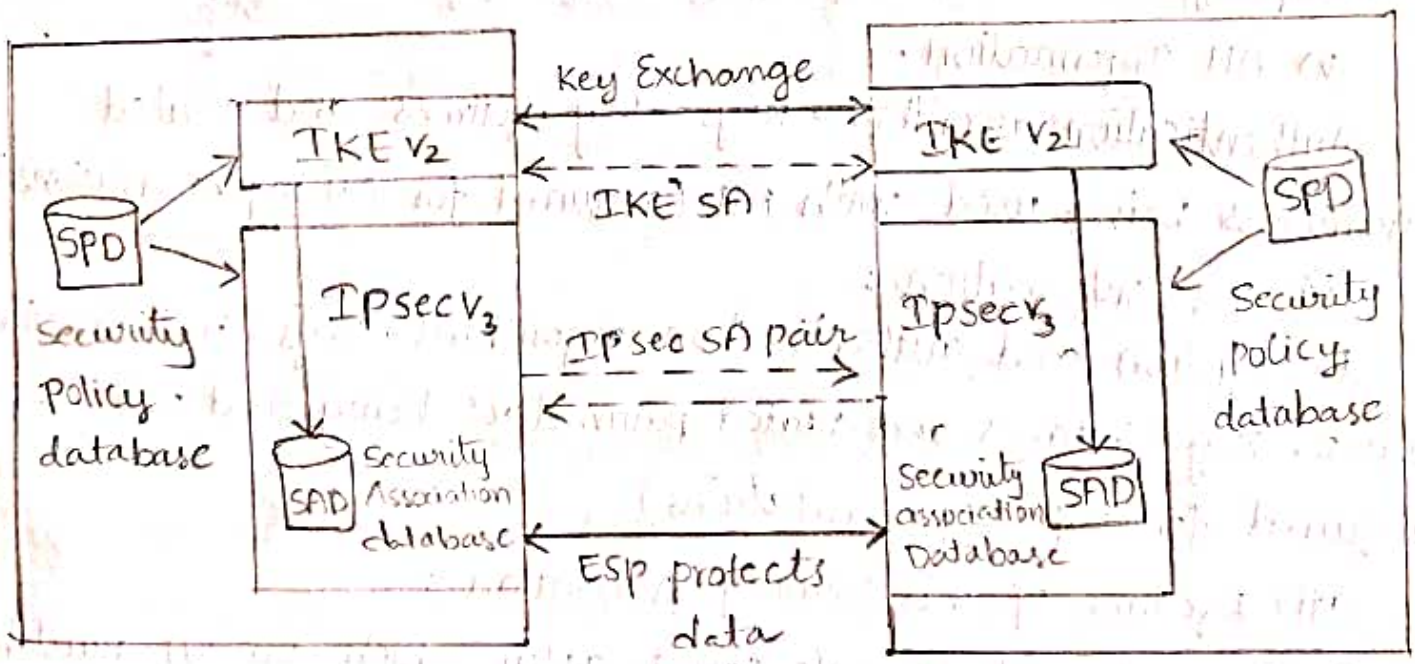
A 32-bit unsigned integer assigned to this SA and having local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.

(ii) Ip Destination Address:

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.

(iii) Security protocol Identifier:

This Field from the outer Ip header indicates whether the association is an AH or ESP security association.



Ip sec Architecture.

(2) Security Association Database:

(i) Security parameter Index:

A 32-bit value selected by the receiving end of an SA to uniquely identify the SA. In an SAD Entry for an outbound SA, the SPI is used to construct the packet's AH and ESP header. In an SAD Entry for an inbound SA, the SPI is used to map traffic to the appropriate SA.

(ii) Sequence Number counter:

A 32-bit value used to generate the sequence Number Field in AH or ESP headers, described in section 20.3 (required for all implementations)

(iii) 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)

(iv) Anti-Replay Window:

used to determine whether an inbound AH or ESP packet is a replay, distributed in section 20.3 (required for all implementations)

(v) AH Information:

Authentication algorithm, keys, key lifetimes and related parameters being used with AH (required for AH implementations)

(vi) ESP Information:

Encryption and authentication algorithms, keys, initialization values, key lifetimes and related parameters being used with ESP (required for ESP implementations)

(vii) Life time 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)

(3) security policy Database:

The following selectors determine an SPD entry.

(i) - Remote Ip address:

This may be a single Ip address, an enumerated list or range of addresses, or a wildcard (mask) address. The latter two are required to support more than one destination system sharing the same SA (eg. behind a firewall)

(ii) Local Ip address:

This may be a single Ip address, an enumerated list or range of addresses, or a wildcard (mask) address. The latter two are required to support more than one source system sharing the same SA (eg. behind a firewall)

(iii) Next layer protocol:

The Ip protocol header (IPv_4, IPv_6 or IPv_6 Extension) includes a Field (protocol for IPv_4, Next header for IPv_6 or IPv_6 extension) that designates the protocol operating over Ip. This is an individual protocol number, ANY or for IPv_6 only, OPAQUE. If AH or ESP is used, then this Ip protocol header immediately precedes the AH or ESP header in the packet.

(iv) Name:

A user identifier from the operating system. This is not a field in the Ip or upper-layer headers but is available if Ipsec is running on the same operating system as the user.

(v) Local and Remote ports:

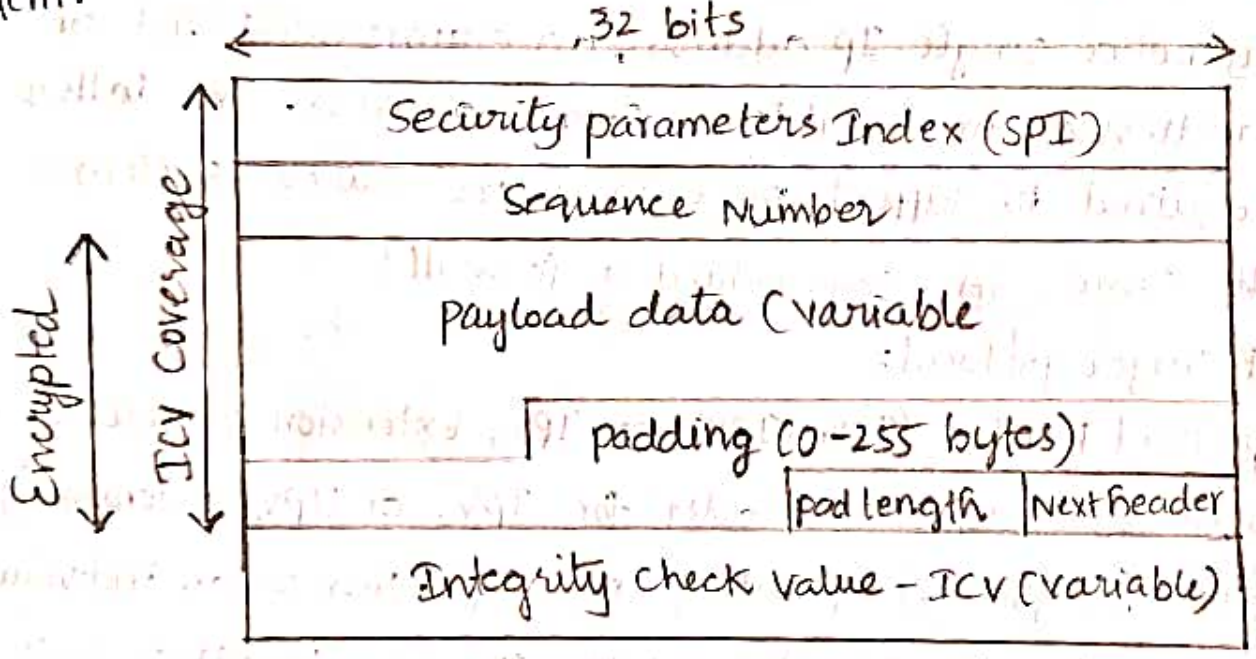
These may be individual TCP or UDP ports values, an enumerated list of ports, or a wildcard port.

3. Encapsulating security payload (ESP)

(1) ESP can be used to provide confidentiality, data origin authentication, Connectionless integrity, an anti-replay service (a form of partial Sequence integrity) and (limited) traffic flow confidentiality.

(2) The set of services provided depends on options selected at the time of security Association (SA) establishment and on the location of the implementation in a network topology

(3) ESP can work with a variety of encryption and authentication algorithms, including authenticated encryption algorithms such as GCM.



Top-level format of an ESP packet

ESP Format:

(i) security parameters Index (32 bits):

Identifies a security association

(ii) Sequence Number (32 bits):

A monotonically increasing counter value; this provides an anti-replay function, as discussed for AH.

(iii) payload Data (variable):

This is a Transport-level segment (transport mode)

or Ip packet (tunnel mode) that is protected by encryption:

(iv) padding (0-255 bytes):

The purpose of this field is discussed later.

(v) pad length (8 bits):

Indicates the number of pad bytes immediately preceding this field.

(vi) Next header (8 bits):

Identifies the type of data contained in the payload data field by identifying the first header in that payload (eg. an extension header in Ipv_6, or an upper-layer protocol such as TCP)

(vii) Integrity check value (Variable):

A variable-length field (must be an integral number of 32-bit words) that contains the integrity check value computed over the ESP packet minus the Authentication Data Field.

4. Internet Key Exchange (IKE)

(1) The key management portion of Ipsec involves the determination and distribution of secret keys.

(2) A Typical requirement is four keys for communication between two applications: Transmit and receive pairs for both integrity and confidentiality.

(3) The Ipsec Architecture document mandates support for two types of key management:

Manual: A system administrator manually configures each system with its own keys and with the keys of other communicating systems. This is practical for small, relatively static environments.

Automated: An automated system enables the on-demand creation of keys for SA's and facilitates the use of keys in a large distributed system with an evolving configuration

The default automated key management protocol for Ipsec is referred to as ISAKMP/oakley and consists of the following elements.

→ oakley key determination protocol:

oakley 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.

→ Internet Security Association and key management protocol (ISAKMP):

ISAKMP provides a framework for internet key management and provides the specific protocol support, including formats, for negotiation of security attributes.

Key Determination protocol:

→ IKE key determination is a refinement of the Diffie-Hellman key exchange algorithm.

→ The Diffie-Hellman algorithm has two attractive features.

(1) Secret keys are created only when needed. There is no need to store secret keys for a long period of time, exposing them to increased vulnerability.

(2) The exchange requirements no pre-existing infrastructure other than an agreement on the global parameters.

Features of IKE Key Determination:

The IKE key determination algorithm is characterized by five important features.

(1) It employs a mechanism known as cookies to thwart clogging attacks.

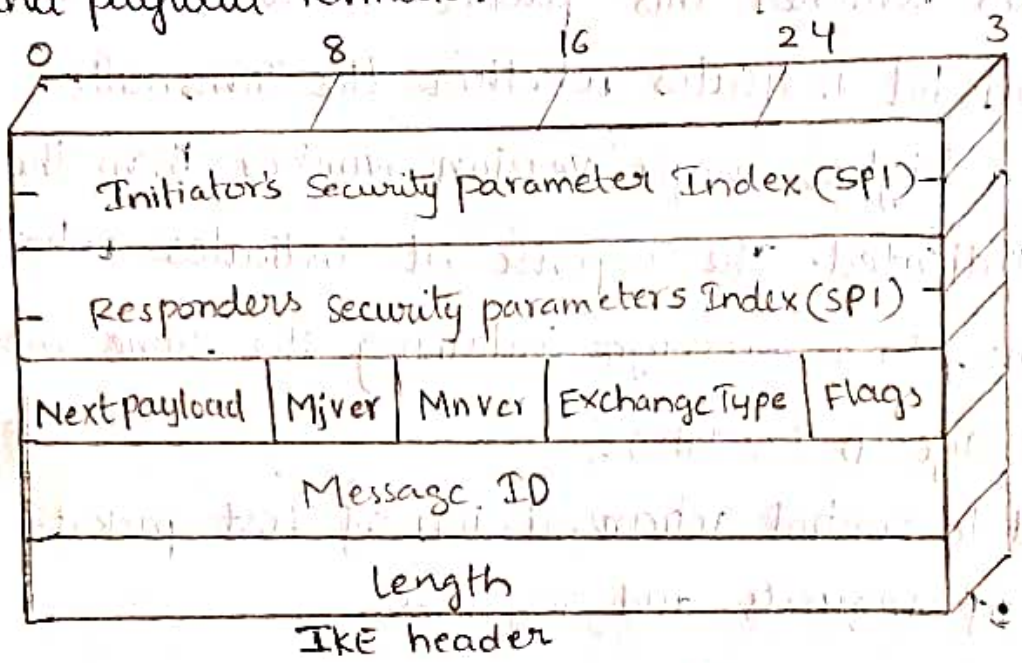
(2) It enables the two parties to negotiate a group, This, in essence, specifies the global parameters of the Diffie-Hellman key exchange.

(3) It uses nonces to ensure against replay attacks.

(4) It enables the exchange of Diffie-Hellman public key values.

(5) It authenticates the Diffie-Hellman exchange to thwart man-in-the-middle attacks.

Header and payload formats:



IKE header

Generic payload header.

IKE formats:

→ IKE consists of the following Fields:

(i) Initiator SPI (64 bits): A value choosen by the initiator to identify a unique IKE security Association (SA)

(ii) Responder SPI (64 bits): A value choosen by the responder to identify a unique IKE SA.

(iii) Next payload (8-bits): Indicates the type of a first payload in the message, payloads are discussed in next

subsection.

(iv) Major Version (4-bits): Indicates major version of IKE in use.

(v) Minor Version (4 bits): Indicates minor version in use.

(vi) Exchange Type (8-bits): Indicates the type of exchange

(vii) Flags (8 bits): Indicates specific options set for this IKE exchange. Three bits are defined sofar. The initiator bit indicates whether this packet is sent by the SA initiator. The Version bit indicates whether the Transmitter is capable of using a higher major version number than the one currently indicated. The response bit indicates whether this is a response to a message containing the same message ID.

(viii) Message ID (32 bits):

used to control retransmission of lost packets and matching of requests and responses.

(ix) Length (32 bits):

Length of total message (header plus all payloads) in octets.

IKE payload types:

→ (1) Security Association : proposals
→ (2) Key exchange : DH Group #, Key exchange Data
→ (3) Identification : ID type, ID Data
→ (4) Certificate : Cert Encoding, certificate data
→ (5) Authentication : Auth method, Authentication Data.
→ (6) Nonce : Nonce data.
→ (7) Encrypted : IV, Encrypted IKE payloads, padding, ICV, padlength.