Unit- 6 Network Security

Network Security refers to the measures taken by any enterprise or organisation to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network. Every company or organisation that handles large amount of data, has a degree of solutions against many **cyber threats**.

The most basic example of Network Security is password protection where the user of the network oneself chooses. In the recent times, Network Security has become the central topic of cyber security with many organisations inviting applications of people who have skills in this area. The network security solutions protect various **vulnerabilities of the computer systems** such as:

1. Users

2. Locations

3. Data

4. Devices

5. Applications

Network Security : Working

The basic principle of network security is protecting huge stored data and network in layers that ensures a bedding of rules and regulations that have to be acknowledged before performing any activity on the data.

These levels are:

1. Physical

2. Technical

3. Administrative

These are explained as following below.

1. **Physical Network Security:**

   This is the most basic level that includes protecting the data and network though unauthorized personnel from acquiring the control over the confidentiality of the network. These includes external peripherals and routers might be used for cable connections. The same can be achieved by using devices like bio-metric systems.

2. **Technical Network Security:**

   It primarily focuses on protecting the data stored in the network or data involved in transitions through the network. This type serves two purposes. One, protection from the unauthorized users and the other being protection from malicious activities.

3. **Administrative Network Security:**

   This level of network security protects user behavior like how the permission has been granted and how the authorization process takes place. This also ensures the level of sophistication the network might need for protecting it through all the attacks. This level also suggests necessary amendments that have to be done over the infrastructure.

Types of Network Security:

The few types of network securities are discussed as below :

1. **<u>Access Control</u>:**

   Not every person should have complete allowance to the accessibility to the network or its data. The one way to examine this is by going through each personnel's details. This is done through Network Access Control which ensures that only a handful of authorized personnel must be able to work

with allowed amount of resources.

2. **Antivirus and Anti-malware Software:**

   This type of network security ensures that any malicious software does not enter the network and jeopardize the security of the data. The malicious software like Viruses, Trojans, Worms are handled by the same. This ensure that not only the entry of the malware is protected but also that the system is well equipped to fight once it has entered.

3. **Cloud Security:**

   Now a day, a lot many organisations are joining hands with the cloud technology where a large amount of important data is stored over the internet. This is very vulnerable to the malpractices that few unauthorized dealers might pertain. This data must be protected an it should be ensured that this protection is not jeopardize over anything. Many businesses embrace SaaS applications for providing some of its employees the allowance of accessing the data stored over the cloud. This type of security ensures in creating gaps in visibility of the data.

Network Concepts:

Open system:

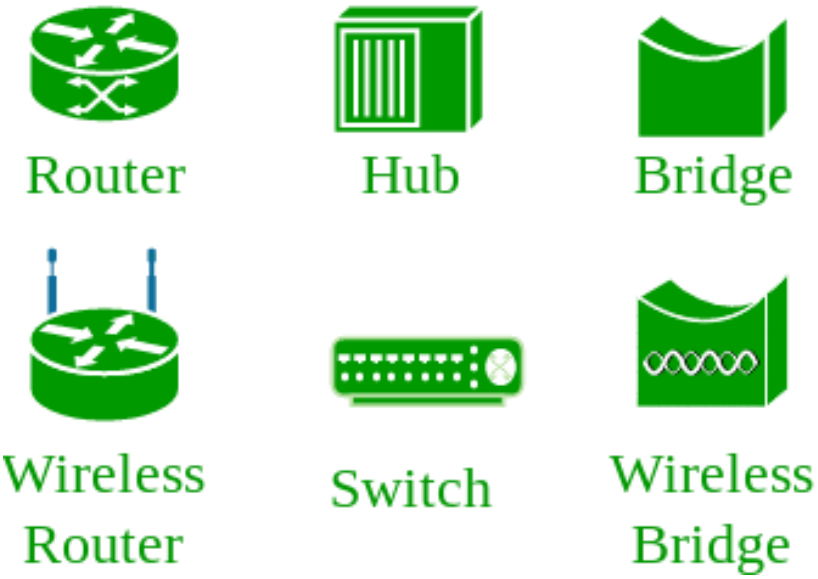
A system which is connected to the network and is ready for communication.

Closed system:

A system which is not connected to the network and can't be communicated with.

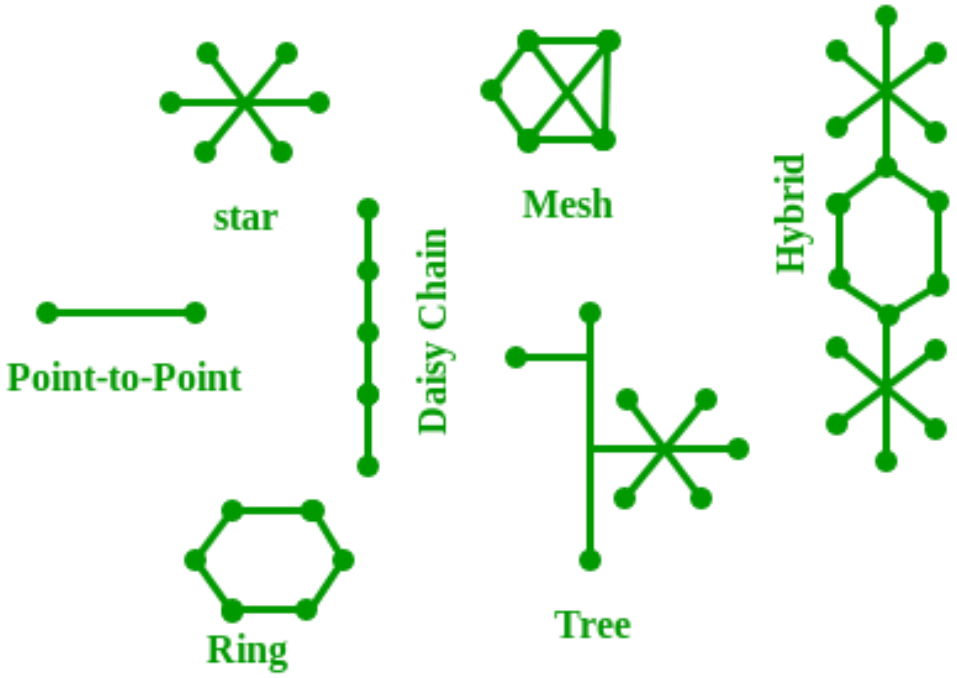
Computer Network:

An interconnection of multiple devices, also known as hosts, that are connected using multiple paths for the purpose of sending/receiving data or media. Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as **Network devices** and include things such as routers, switches, hubs, and bridges.



Network Topology:

The layout arrangement of the different devices in a network. Common examples include: Bus, Star, Mesh, Ring, and Daisy chain.



OSI:

OSI stands for **Open Systems Interconnection**. It is a reference model that specifies standards for communications protocols and also the functionalities of each layer.

Protocol:

A protocol is the set of rules or algorithms which define the way how two entities can communicate across the network and there exists different protocol defined at each layer of the OSI model. Few of such protocols are TCP, IP, UDP, ARP, DHCP, FTP and so on.

UNIQUE IDENTIFIERS OF NETWORK

Host name:

Each device in the network is associated with a unique device name known as Hostname.

Type “hostname” in the command prompt(Administrator Mode) and press ‘Enter’, this displays the hostname of your machine.

IP Address (Internet Protocol address):

Also known as the Logical Address, the IP Address is the network address of the system across the network.

To identify each device in the world-wide-web, the Internet Assigned Numbers Authority (IANA) assigns an IPV4 (Version 4) address as a unique identifier to each device on the Internet.

The length of an IPv4 address is 32-bits, hence, we have 2^{32} IP addresses available. The length of an IPv6 address is 128-bits.

Type “ipconfig” in the command prompt and press ‘Enter’, this gives us the IP address of the device.

MAC Address (Media Access Control address):

Also known as physical address, the MAC Address is the unique identifier of each host and is associated with its NIC (Network Interface Card).

A MAC address is assigned to the NIC at the time of manufacturing.

The length of the MAC address is : 12-nibble/ 6 bytes/ 48 bits

Type “ipconfig/all” in the command prompt and press ‘Enter’, this gives us the MAC address.

Port:

A port can be referred to as a logical channel through which data can be sent/received to an application. Any host may have multiple applications running, and each of these applications is identified using the port number on which they are running.

A port number is a 16-bit integer, hence, we have 2^{16} ports available which are categorized as shown below:

Port Types	Range
Well known Ports	0 – 1023
Registered Ports	1024 – 49151
Ephemeral Ports	49152 – 65535

Number of ports: 65,536

Range: 0 – 65535

*Type "**netstat -a**" in the command prompt and press 'Enter', this lists all the ports being used.*

Socket:

The unique combination of IP address and Port number together are termed as Socket.

<u>Other related concepts</u>

DNS Server:

DNS stands for **Domain Name system**.

DNS is basically a server which translates web addresses or URLs (ex: www.google.com) into their corresponding IP addresses. We don't have to remember all the IP addresses of each and every website.

The command '**nslookup**' gives you the IP address of the domain you are looking for. This also provides the information of our DNS Server.

ARP:

ARP stands for **Address Resolution Protocol**.

It is used to convert an IP address to its corresponding physical address(i.e., MAC Address).

ARP is used by the Data Link Layer to identify the MAC address of the Receiver's machine.

RARP:

RARP stands for **Reverse Address Resolution Protocol**.

As the name suggests, it provides the IP address of the device given a physical address as input. But RARP has become obsolete since the time DHCP has come into the picture.

Threats in Networks:

Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.

Threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.

Software attacks means attack by Viruses, Worms, Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things. But they are not same, only similarity is that they all are malicious software that behaves differently.

Malware is a combination of 2 terms- Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or anything that is designed to perform malicious operations on system. Malware can be divided in 2 categories:

1. Infection Methods

2. Malware Actions

Malware on the **basis of Infection** Method are following:

1. **Virus –** They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. The Creeper Virus was first detected on ARPANET. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.
2. **Worms –** Worms are also self-replicating in nature but they don't hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network-aware. They can easily travel from one computer to another if network is available and on the target machine they will not do much harm, they will, for example, consume hard disk space thus slowing down the computer.
3. **Trojan –** The Concept of Trojan is completely different from the viruses and worms. The name Trojan is derived from the 'Trojan Horse' tale in Greek mythology, which explains how the Greeks were able to enter the fortified city of Troy by hiding their soldiers in a big wooden horse given to the Trojans as a gift. The Trojans were very fond of horses and trusted the gift blindly. In the night, the soldiers emerged and attacked the city from the inside.

   Their purpose is to conceal themselves inside the software that seem legitimate and when that software is executed they will do their task of either stealing information or any other purpose for which they are designed.

   They often provide backdoor gateway for malicious programs or malevolent users to enter your system and steal your valuable data without your

knowledge and permission. Examples include FTP Trojans, Proxy Trojans, Remote Access Trojans etc.

4. **Bots –**: can be seen as advanced form of worms. They are automated processes that are designed to interact over the internet without the need for human interaction. They can be good or bad. Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called **Botnet.**

Malware on the **basis of Actions:**

1. **Adware –** Adware is not exactly malicious but they do breach privacy of the users. They display ads on a computer's desktop or inside individual programs. They come attached with free-to-use software, thus main source of revenue for such developers. They monitor your interests and display relevant ads. An attacker can embed malicious code inside the software and adware can monitor your system activities and can even compromise your machine.
2. **Spyware –** It is a program or we can say software that monitors your activities on computer and reveal collected information to an interested party. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they install themselves and sits silently to avoid detection.
   One of the most common example of spyware is KEYLOGGER. The basic job of keylogger is to record user keystrokes with timestamp. Thus capturing interesting information like username, passwords, credit card details etc.

3. **Ransomware –** It is type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or wholly. Then a screen will be displayed asking for money i.e. ransom in exchange.
4. **Scareware –** It masquerades as a tool to help fix your system but when the software is executed it will infect your system or completely destroy it. The software will display a message to frighten you and force to take some action like pay them to fix your system.
5. **Rootkits –** are designed to gain root access or we can say administrative privileges in the user system. Once gained the root access, the exploiter can do anything from stealing private files to private data.
6. **Zombies –** They work similar to Spyware. Infection mechanism is same but they don't spy and steal information rather they wait for the command from hackers.

- **Theft of intellectual property** means violation of intellectual property rights like copyrights, patents etc.
- **Identity theft** means to act someone else to obtain person's personal information or to access vital information they have like accessing the computer or social media account of a person by login into the account by using their login credentials.
- **Theft of equipment and information** is increasing these days due to the mobile nature of devices and increasing information capacity.
- **Sabotage** means destroying company's website to cause loss of confidence on part of its customer.
- **Information extortion** means theft of company's property or information to receive payment in exchange. For example ransomware may lock victims file

making them inaccessible thus forcing victim to make payment in exchange. Only after payment victim's files will be unlocked.

These are the old generation attacks that continue these days also with advancement every year. Apart from these there are many other threats. Below is the brief description of these new generation threats.

- **Technology with weak security –** With the advancement in technology, with every passing day a new gadget is being released in the market. But very few are fully secured and follows Information Security principles. Since the market is very competitive Security factor is compromised to make device more up to date. This leads to theft of data/ information from the devices
- **Social media attacks –** In this cyber-criminal identify and infect a cluster of websites that persons of a particular organization visit, to steal information.
- **Mobile Malware –**There is a saying when there is a connectivity to Internet there will be danger to Security. Same goes for Mobile phones where gaming applications are designed to lure customer to download the game and unintentionally, they will install malware or virus on the device.
- **Outdated Security Software –** With new threats emerging every day, updating in security software is a prerequisite to have a fully secured environment.
- **Corporate data on personal devices –** These days every organization follows a rule BYOD. BYOD means Bring your own device like Laptops, Tablets to the workplace. Clearly BYOD pose a serious threat to security of data but due to productivity issues organizations are arguing to adopt this.
- **Social Engineering –** is the art of manipulating people so that they give up their confidential information like bank account details, password etc. These

criminals can trick you into giving your private and confidential information or they will gain your trust to get access to your computer to install a malicious software- that will give them control of your computer. For example, email or message from your friend, that was probably not sent by your friend. Criminal can access your friend's device and then by accessing the contact list, he can send infected email and message to all contacts. Since the message/ email is from a known person recipient will definitely check the link or attachment in the message, thus unintentionally infecting the computer.

Network Security Controls:

1. **Access Control:**
   Not every person should have complete allowance to the accessibility to the network or its data. The one way to examine this is by going through each personnel's details. This is done through Network Access Control which ensures that only a handful of authorized personnel must be able to work with allowed amount of resources.

2. **Antivirus and Anti-malware Software:**
   This type of network security ensures that any malicious software does not enter the network and jeopardize the security of the data. The malicious software like Viruses, Trojans, Worms are handled by the same. This ensure that not only the entry of the malware is protected but also that the system is well equipped to fight once it has entered.

3. **Cloud Security:**

   Now a day, a lot many organizations are joining hands with the cloud technology where a large amount of important data is stored over the internet. This is very vulnerable to the malpractices that few unauthorized dealers might pertain. This data must be protected an it should be ensured that this protection is not jeopardize over anything. Many businesses embrace SaaS applications for providing some of its employees the

allowance of accessing the data stored over the cloud. This type of security ensures in creating gaps in visibility of the data.

IP Security:

The **IP security (IPSec)** is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

Uses of IP Security –
IPsec can be used to do the following things:

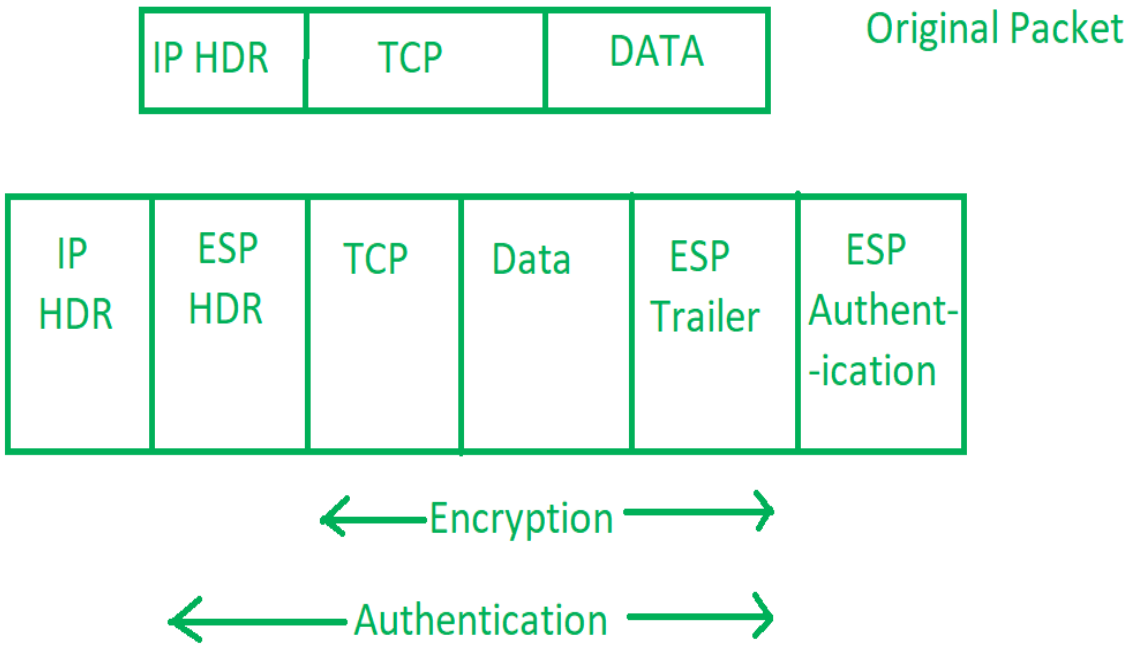
- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

Components of IP Security –
It has the following components:

1. **Encapsulating Security Payload (ESP) –**
   It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.

2. **Authentication Header (AH) –**
   It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentiality.

3. **Internet Key Exchange (IKE) –**
   It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange. ISAKMP tells how the setup of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.
   Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP sec users produces a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets which are not authorized are discarded and not given to receiver.



Working of IP Security –

1. The host checks if the packet should be transmitted using IPsec or not. These packet traffic triggers the security policy for themselves. This is done when the system sending the packet apply an appropriate encryption. The incoming packets are also checked by the host that they are encrypted properly or not.
2. Then the **IKE Phase 1** starts in which the 2 hosts(using IPsec) authenticate themselves to each other to start a secure channel. It has 2 modes.

The **Main mode** which provides the greater security and the **Aggressive mode** which enables the host to establish an IPsec circuit more quickly.

3. The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit.
4. Now, the **IKE Phase 2** is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and agreeing on secret keying material to be used with those algorithms.
5. Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.
6. When the communication between the hosts is completed or the session times out then the IPsec tunnel is terminated by discarding the keys by both the hosts.

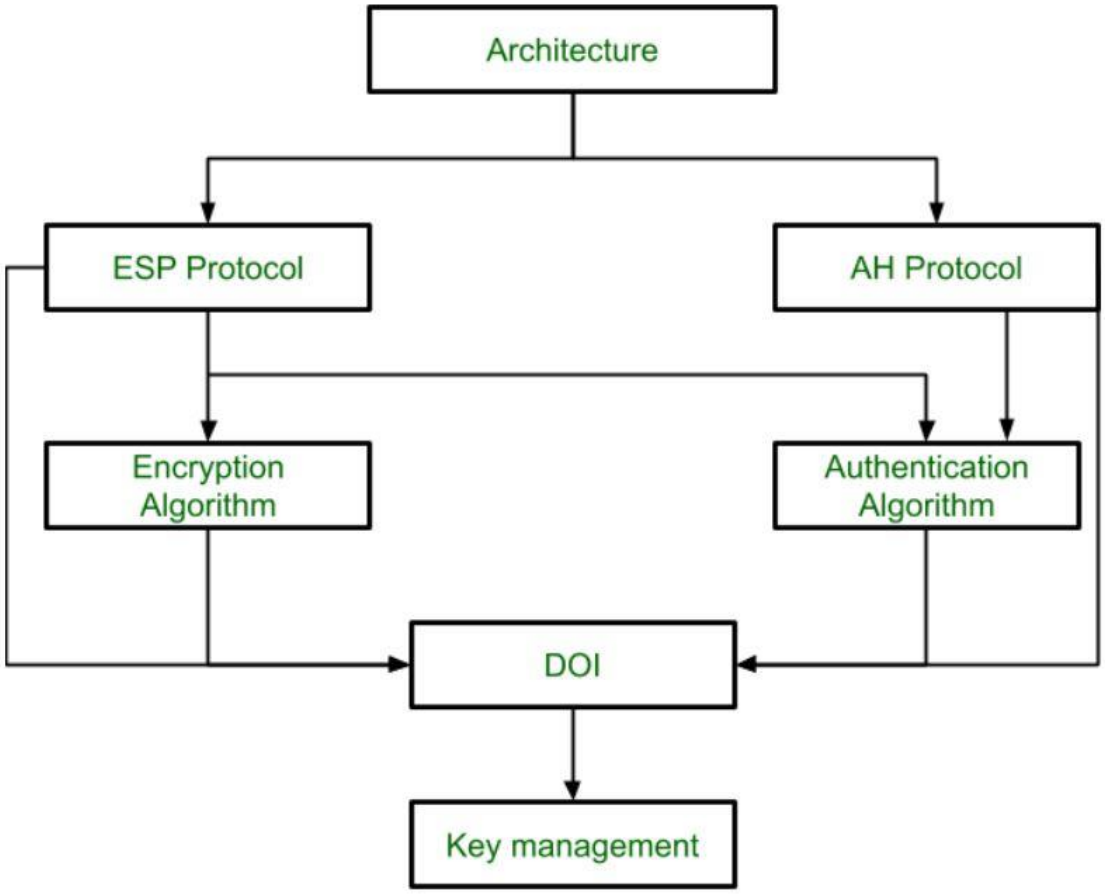
The **IP security** (**IPSec**) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets.

IP Security Architecture:

IPSec (IP Security) architecture uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture include protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services:

- Confidentiality
- Authentication
- Integrity

IP Security Architecture:



Security Associations (SA):

The concept of a security association (SA) is fundamental to IPSec. An SA is a relationship between two or more entities that describes how the entities will use security services to communicate securely. IPSec provides many options for performing network encryption and authentication. Each IPSec connection can provide encryption, integrity, authenticity, or all three. When the security service is determined, the two IPSec peers must determine exactly which algorithms to use (for example, DES or 3DES for encryption, MD5 or SHA for integrity). After deciding on the algorithms, the two devices must share session keys. As you can

see, there is quite a bit of information to manage. The security association is the method that IPSec uses to track all the particulars concerning a given IPSec communication session. You will need to configure SA parameters and monitor SAs on Cisco routers and the PIX Firewall.

A separate pair of IPSec SAs are set up for AH and ESP transform. Each IPSec peer agrees to set up SAs consisting of policy parameters to be used during the IPSec session. The SAs are unidirectional for IPSec so that peer 1 will offer peer 2 a policy. If peer 2 accepts this policy, it will send that policy back to peer 1. This establishes two one-way SAs between the peers. Two-way communication consists of two SAs, one for each direction.

Each SA consists of values such as destination address, a security parameter index (SPI), the IPSec transforms used for that session, security keys, and additional attributes such as IPSec lifetime. The SAs in each peer have unique SPI values that will be recorded in the Security Parameter Databases of the devices. The Security Parameter Database is set up in dynamic random-access memory (DRAM) and contains parameter values for each SA

Table 1-1 SA Parameters

Parameter	Description
outbound esp sas: spi: 0x1B781456(460854358)	Security parameter index, which matches inbound SPI for that SA
transform: esp-des	IPSec transform

Parameter	Description
in use settings ={Tunnel, }	IPSec transform mode (tunnel or transport)
slot: 0, conn id: 18, crypto map:mymap	Crypto engine and crypto map information
sa timing: (k/sec)	SA lifetime in KB and seconds
replay detection support: N	Replay detection either on or off

Authentication Header (AH):

An Authentication Header or AH is a security mechanism used in authenticating the origins of datagrams (packets of data transmitted under Internet Protocol or IP conditions), and in guaranteeing the integrity of the information that's being sent. Authentication Headers are a protocol under the Internet Protocol Security (IPSec) suite.

IP Authentication Header is used to provide connection-less integrity and data origin authentication. There are two main advantages that Authentication Header provides,

- **Message Integrity –**

  It means, message is not modified while coming from source.
- **Source Authentication –**

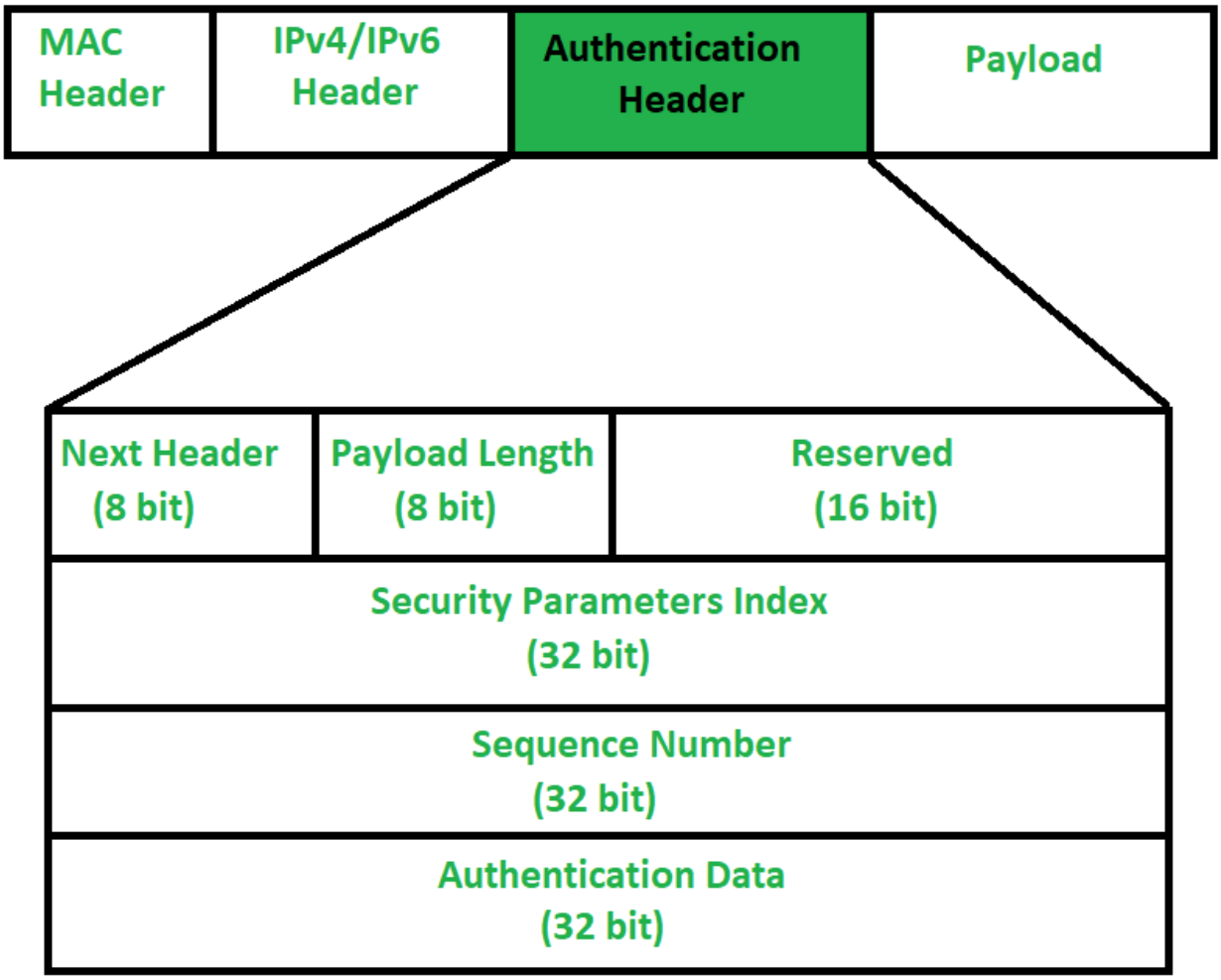
  It means, source is exactly source from whom we were expecting data.

When packet is sent from source A to Destination B, it consists of data that we need to send and header which consist of information regarding packet. Authentication Header verifies origin of data and also payload to confirm if there has been modification done in between, during transmission between source and destination.

However, in transit, values of some IP header fields might change (like- Hop count, options, extension headers). So, values of such fields cannot be protected from Authentication header. Authentication header cannot protect every field of IP header. It provides protection to fields which are essential to be protected.

Authentication Header :

The question may arise, that how IP header will know that adjacent Extension header is Authentication Header. Well, there is protocol field in IP Header which tells type of header that is present in packet. So, protocol field in IP Header should have value of “51” in order to detect Authentication Header.



1. **Next Header –**

   Next Header is 8-bit field that identifies type of header present after Authentication Header. In case of TCP, UDP or destination header or some other extension header it will store correspondence IP protocol number . Like, number 4 in this field will indicate IPv4, number 41 will indicate IPv6 and number 6 will indicate TCP.

2. **Payload Length –**

   Payload length is length of Authentication header and here we use scaling factor of 4. Whatever be size of header, divide it by 4 and then

subtract by 2. We are subtracting by 2 because we're not counting first 8 bytes of Authentication header, which is first two row of picture given above. It means we are not including Next Header, Payload length, Reserved and Security Parameter index in calculating payload length. Like, say if payload length is given to be X. Then (X+2)*4 will be original Authentication header length.

3. **Reserved –**

   This is 16-bit field which is set to "zero" by sender as this field is reserved for future use.

4. **Security Parameter Index (SPI) –**

   It is arbitrary 32-bit field. It is very important field which identifies all packets which belongs to present connection. If we're sending data from Source A to Destination B. Both A and B will already know algorithm and key they are going to use. So for Authentication, hashing function and key will be required which only source and destination will know about. Secret key between A and B is exchanged by method of Diffie Hellman algorithm. So Hashing algorithm and secret key for Security parameter index of connection will be fixed. Before data transfer starts security association needs to be established.

   In **Security Association**, both parties needs to communicate prior to data exchange. Security association tells what is security parameter index, hashing algorithm and secret key that are being used.

5. **Sequence Number –**

   This unsigned 32-bit field contains counter value that increases by one for each packet sent. Every packet will need sequence number. It will start from 0 and will go till 232 – 1 and there will be no wrap around. Say, if all sequence numbers are over and none of it is left but we cannot wrap around as it is not allowed. So, we will end connection and re-establish connection again to resume transfer of remaining data from sequence number 0. Basically sequence numbers are used to stop replay attack.

   In Replay attack, if same message is sent twice or more, receiver won't be able to know if both messages are sent from a single source or not. Say, I am requesting 100$ from receiver and Intruder in between asked for another 100$. Receiver won't be able to know that there is intruder in between.

6. **Authentication Data (Integrity Check Value) –**

   Authentication data is variable length field that contains Integrity Check Value (ICV) for packet. Using hashing algorithm and secret key, sender will create message digest which will be sent to receiver. Receiver on other hand will use same hashing algorithm and secret key. If both message digest matches then receiver will accept data. Otherwise, receiver will discard it by saying that message has been modified in between. So basically, authentication data is used to verify integrity of transmission. Also length of Authentication data depends upon hashing algorithm you choose.

Conclusion :

How Authentication Header can be useful ?

- Message Integrity also known as Connection-less Integrity
- Source Authentication
- Replay attack protection

Encapsulating Security Payload (ESP):

The Encapsulating Security Payload (ESP) protocol provides data confidentiality, and also optionally provides data origin authentication, data integrity checking, and replay protection.

The difference between ESP and the Authentication Header (AH) protocol is that ESP provides encryption, while both protocols provide authentication, integrity checking, and replay protection. With ESP, both communicating systems use a shared key for encrypting and decrypting the data they exchange.

If you decide to use both encryption and authentication, then the responding system first authenticates the packet and then, if the first step succeeds, the system proceeds with decryption. This type of configuration reduces processing overhead, as well as reduces your vulnerability to denial-of-service attacks.

Two ways of using ESP

You can apply ESP in two ways: transport mode or tunnel mode. In transport mode, the ESP header follows the IP header of the original IP datagram.

If the datagram already has an IPSec header, then the ESP header goes before it. The ESP trailer and the optional authentication data follow the payload.

Transport mode does not authenticate or encrypt the IP header, which might expose your addressing information to potential attackers while the datagram is in transit. Transport mode requires less processing overhead than tunnel mode, but does not provide as much security. In most cases, hosts use ESP in transport mode.

Tunnel mode creates a new IP header and uses it as the outermost IP header of the datagram, followed by the ESP header and then the original datagram (both the IP header and the original payload). The ESP trailer and the optional authentication data are appended to the payload. When you use both encryption and authentication, ESP completely protects the original datagram because it is now the payload data for the new ESP packet. ESP, however, does not protect the new IP header. Gateways must use ESP in tunnel mode.

Internet Key Exchange

Internet Key Exchange (IKE) is a key management protocol standard used in conjunction with the Internet Protocol Security (IPSec) standard protocol. It provides security for virtual private networks' (VPNs) negotiations and network access to random hosts. It can also be described as a method for exchanging keys for encryption and authentication over an unsecured medium, such as the Internet.

IKE is a hybrid protocol based on:

- ISAKMP (RFC2408): Internet Security Association and Key Management Protocols are used for negotiation and establishment of security associations. This protocol establishes a secure connection between two IPSec peers.
- Oakley (RFC2412): This protocol is used for key agreement or key exchange. Oakley defines the mechanism that is used for key exchange over an IKE session. The default algorithm for key exchange used by this protocol is the Diffie-Hellman algorithm.
- SKEME: This protocol is another version for key exchange.

IKE enhances IPsec by providing additional features along with flexibility. IPsec, however, can be configured without IKE.

IKE has many benefits. It eliminates the need to manually specify all the IPSec security parameters at both peers. It allows the user to specify a particular lifetime for the IPsec security association. Furthermore, encryption can be changed during IPsec sessions. Moreover, it permits certification authority. Finally, it allows dynamic authentication of peers.