Cryptography and Network Security Principles

In the present day scenario security of the system is the sole priority of any organisation. The main aim of any organisation is to protect their data from attackers. In cryptography, attacks are of two types such as Passive attacks and Active attacks.

Passive attacks are those that retrieve information from the system without affecting the system resources while active attacks are those that retrieve system information and make changes to the system resources and their operations.

The Principles of Security can be classified as follows:

1. **Confidentiality:**
   The degree of confidentiality determines the secrecy of the information. The principle specifies that only the sender and receiver will be able to access the information shared between them. Confidentiality compromises if an unauthorized person is able to access a message. For example, let us consider sender A wants to share some confidential information with receiver B and the information gets intercepted by the attacker C. Now the confidential information is in the hands of an intruder C.

2. **Authentication:**

   Authentication is the mechanism to identify the user or system or the entity. It ensures the identity of the person trying to access the information. The authentication is mostly secured by using username and password. The authorized person whose identity is preregistered can prove his/her identity and can access the sensitive information.

3. **Integrity:**

   Integrity gives the assurance that the information received is exact and accurate. If the content of the message is changed after the sender sends it but before reaching the intended receiver, then it is said that the integrity of the message is lost.

4. **Non-Repudiation:**

   Non-repudiation is a mechanism that prevents the denial of the message content sent through a network. In some cases the sender sends the message and later denies it. But the non-repudiation does not allow the sender to refuse the receiver.

5. **Access control:**

   The principle of access control is determined by role management and rule management. Role management determines who should access the data while rule management determines up to what extent one can access the data. The information displayed is dependent on the person who is accessing it.

6. **Availability:**

   The principle of availability states that the resources will be available to authorize party at all times. Information will not be useful if it is not available to be accessed. Systems should have sufficient availability of information to satisfy the user request.

Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two key one to encrypt and the other one to decrypt.
The size of cipher text is same or smaller than the original plain text.	The size of cipher text is same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amount of data.
It only provides confidentiality.	It provides confidentiality, authenticity and non-repudiation.
Examples: 3DES, AES, DES and RC4	Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA
In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption.	In asymmetric key encryption, resource utilization is high.

Security services and mechanisms

Failed to connect to MySQL: Access denied for user 'u688631385_eezytut'@'localhost' (using password: YES)

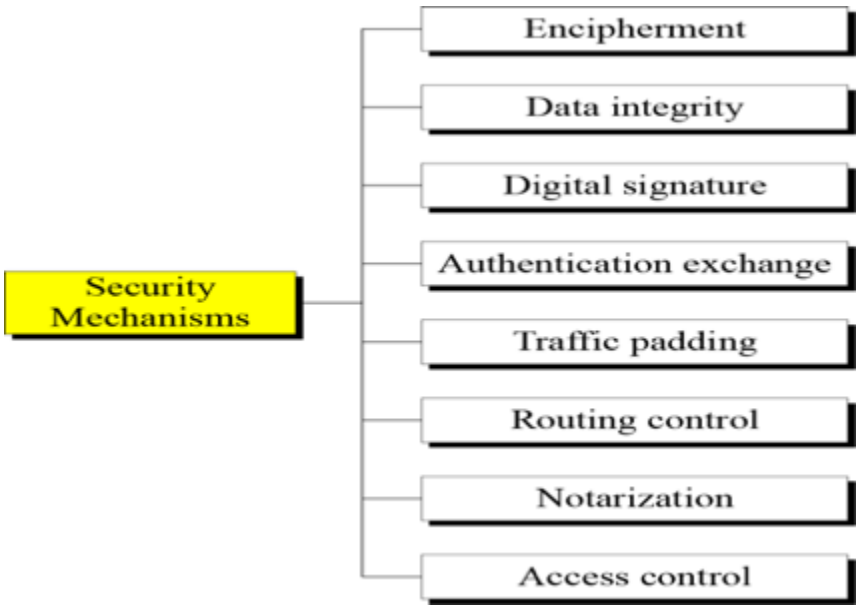
- ITU-T provides some security services and some mechanisms to implement those services.
- Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service..

Security services

- **Authentication:** assures recipient that the **message is from the source** that it **claims to** be from.
- **Access Control:** controls who can have **access to resource** under what **condition**
- **Availability:** available to authorized entities for 24/7.

- **Confidentiality:** information is not made available to unauthorized individual
- **Integrity:** assurance that the message is unaltered
- **Non-Repudiation:** protection against denial of sending or receiving in the communication

Security Mechanisms

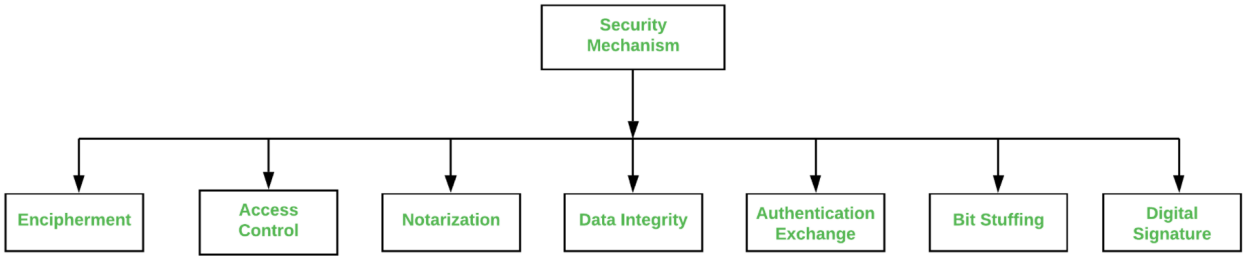


Relation between security services and mechanisms

Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

Types of Security Mechanism

Network Security is a field in computer technology that deals with ensuring security of computer network infrastructure. As the network is very necessary for sharing of information whether it is at hardware level such as printer, scanner, or at software level. Therefore security mechanism can also be termed as is set of processes that deal with recovery from security attack. Various mechanisms are designed to recover from these specific attacks at various protocol layers.



Types of Security Mechanism are :

1. **Encipherment :**

   This security mechanism deals with hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form. It is achieved by two famous techniques named Cryptography and Encipherment. Level of data encryption is dependent on the algorithm used for encipherment.
2. **Access Control :**

   This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying passwords, using firewall, or just by adding PIN to data.
3. **Notarization :**

   This security mechanism involves use of trusted third party in communication. It acts as mediator between sender and receiver so that if any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.
4. **Data Integrity :**

   This security mechanism is used by appending value to data to which is created by data itself. It is similar to sending packet of information known to both sending and receiving parties and checked before and after data is received. When this packet or data which is appended is checked and is the same while sending and receiving data integrity is maintained.
5. **Authentication exchange :**

   This security mechanism deals with identity to be known in communication. This is achieved at the TCP/IP layer where two-way handshaking mechanism is used to ensure data is sent or not

6. **Bit stuffing :**
   This security mechanism is used to add some extra bits into data which is being transmitted. It helps data to be checked at the receiving end and is achieved by Even parity or Odd Parity.
7. **Digital Signature :**
   This security mechanism is achieved by adding digital data that is not visible to eyes. It is form of electronic signature which is added by sender which is checked by receiver electronically. This mechanism is used to preserve data which is not more confidential but sender's identity is to be notified.

Difference between Active Attack and Passive Attack

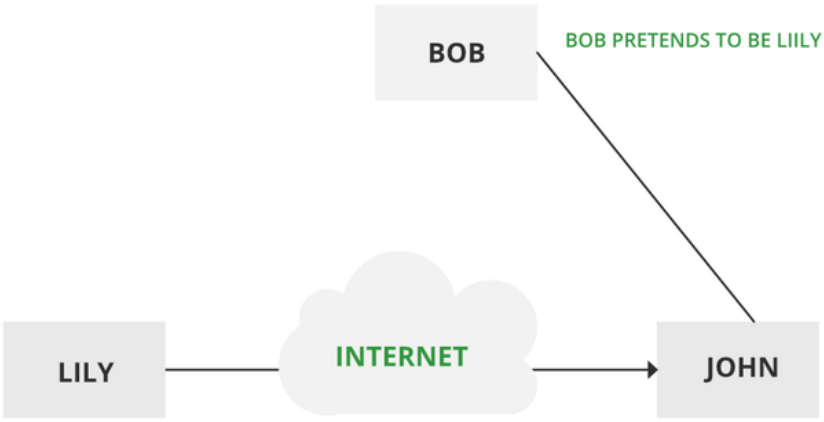
Active Attacks:

Active attacks are the type of attacks in which, The attacker efforts to change or modify the content of messages. Active Attack is danger for Integrity as well as availability. Due to active attack system is always damaged and System resources can be changed. The most important thing is that, In active attack, Victim gets informed about the attack.

- Masquerade
- Modification of messages
- Repudiation
- Replay
- Denial of Service

Masquerade –

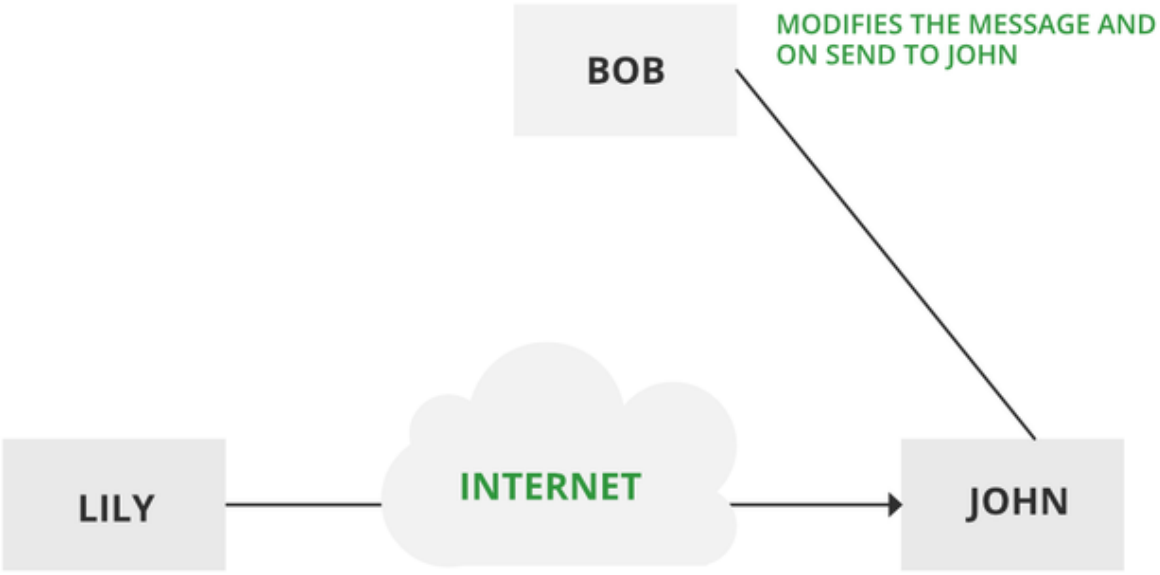
A masquerade attack takes place when one entity pretends to be a different entity. A Masquerade attack involves one of the other forms of active attacks. If an authorization procedure isn't always absolutely protected, it is able to grow to be extraordinarily liable to a masquerade assault. Masquerade assaults may be performed using the stolen passwords and logins, with the aid of using finding gaps in programs, or with the aid of using locating a manner across the authentication process.



Masquerade Attack

Modification of messages –

It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. Modification is an attack on the integrity of the original data. It basically means that unauthorized parties not only gain access to data but also spoof the data by triggering denial-of-service attacks, such as altering transmitted data packets or flooding the network with fake data. Manufacturing is an attack on authentication. For example, a message meaning “Allow JOHN to read confidential file X” is modified as “Allow Smith to read confidential file X”.



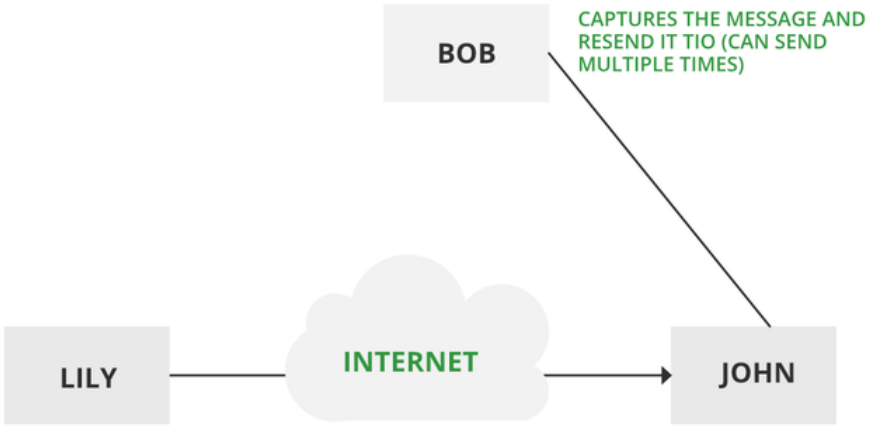
Modification of messages

Repudiation –

This attack occurs when the network is not completely secured or the login control has been tampered with. With this attack, the author's information can be changed by actions of a malicious user in order to save false data in log files, up to the general manipulation of data on behalf of others, similar to the spoofing of e-mail messages.

Replay –

It involves the passive capture of a message and its subsequent transmission to produce an authorized effect. In this attack, the basic aim of the attacker is to save a copy of the data originally present on that particular network and later on use this data for personal uses. Once the data is corrupted or leaked it is insecure and unsafe for the users.

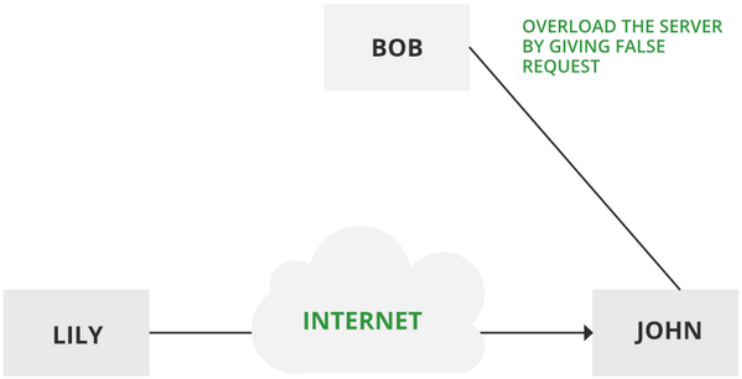


Replay

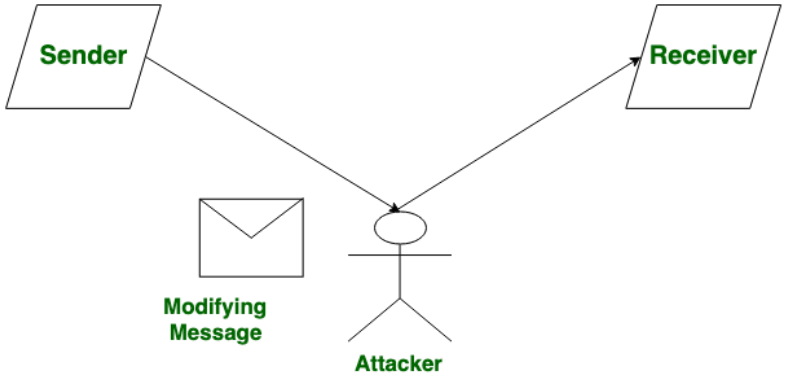
Denial of Service –

It prevents the normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a

particular destination. Another form of service denial is the disruption of an entire network either by disabling the network or by overloading it with messages so as to degrade performance.



Denial of Service



Active Attack

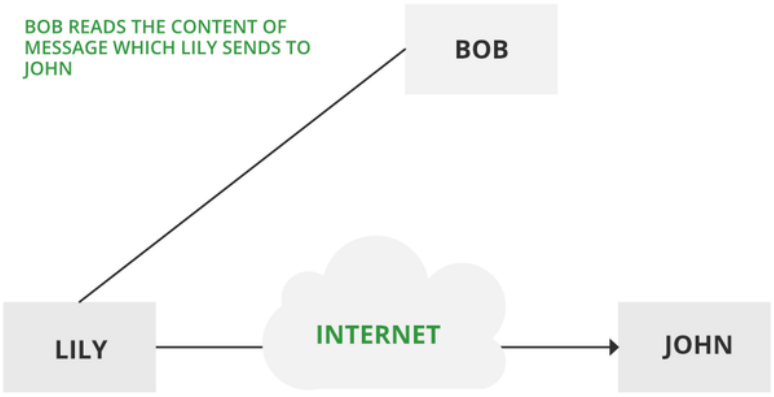
Passive Attacks:

Passive Attacks are the type of attacks in which, The attacker observes the content of messages or copy the content of messages. Passive Attack is danger for Confidentiality. Due to passive attack, there is no any harm to the system. The most important thing is that In passive attack, Victim does not get informed about the attack.

- The release of message content
- Traffic analysis

The release of message content –

Telephonic conversation, an electronic mail message, or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



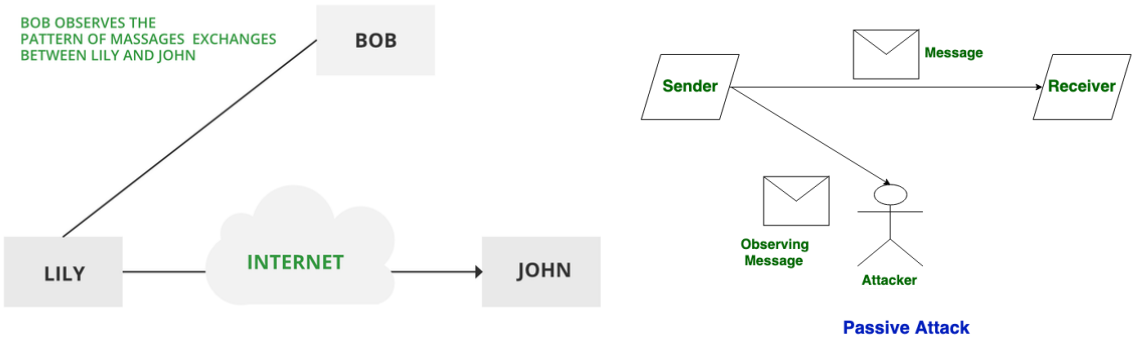
Passive attack

Traffic analysis –

Suppose that we had a way of masking (encryption) information, so that the attacker even if captured the message could not extract any information from the message.

The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

The most useful protection against traffic analysis is encryption of SIP traffic. To do this, an attacker would have to access the SIP proxy (or its call log) to determine who made the call.



Traffic analysis

Difference between Active Attack and Passive Attack:

S.NO	Active Attack	Passive Attack

1.	In active attack, Modification in information take place.	While in passive attack, Modification in the information does not take place.
2.	Active Attack is danger for **Integrity** as well as **availability**.	Passive Attack is danger for **Confidentiality**.
3.	In active attack attention is on detection.	While in passive attack attention is on prevention.
4.	Due to active attack system is always damaged.	While due to passive attack, there is no any harm to the system.
5.	In active attack, Victim gets informed about the attack.	While in passive attack, Victim does not get informed about the attack.

6.	In active attack, System resources can be changed.	While in passive attack, System resources are not change.
7.	Active attack influence the services of the system.	While in passive attack, information and messages in the system or network are acquired.
8.	In active attack, information collected through passive attacks are used during executing.	While passive attack are performed by collecting the information such as passwords, messages by itself.
9.	Active attack is tough to restrict from entering systems or networks.	Passive Attack is easy to prohibited in comparison to active attack.

Network Security

Kerberos

Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. In Kerberos Authentication server and database is used for client authentication. Kerberos runs as a third-party trusted server known as the Key Distribution Center (KDC). Each user and service on the network is a principal.

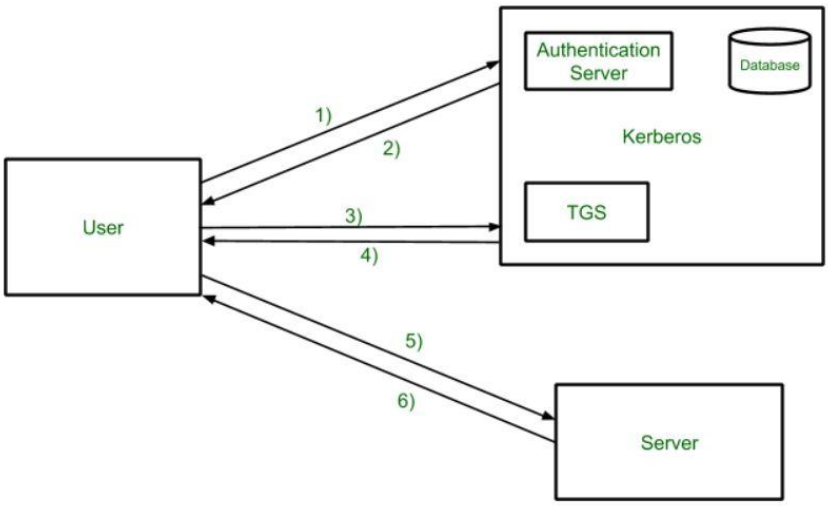
The main components of Kerberos are:

- **Authentication Server (AS):**
  The Authentication Server performs the initial authentication and ticket for Ticket Granting Service.

- **Database:**
  The Authentication Server verifies the access rights of users in the database.

- **Ticket Granting Server (TGS):**
  The Ticket Granting Server issues the ticket for the Server

Kerberos Overview:



- **Step-1:**
  User login and request services on the host. Thus user requests for ticket-granting service.

- **Step-2:**
  Authentication Server verifies user’s access right using database and then gives ticket-granting-ticket and session key. Results are encrypted using the Password of the user.

- **Step-3:**
  The decryption of the message is done using the password then send the ticket to Ticket Granting Server. The Ticket contains authenticators like user names and network addresses.

- **Step-4:**
  Ticket Granting Server decrypts the ticket sent by User and authenticator verifies the request then creates the ticket for requesting

services from the Server.

- **Step-5:**
  The user sends the Ticket and Authenticator to the Server.

- **Step-6:**
  The server verifies the Ticket and authenticators then generate access to the service. After this User can access the services.

Kerberos Limitations

- Each network service must be modified individually for use with Kerberos
- It doesn’t work well in a timeshare environment
- Secured Kerberos Server
- Requires an always-on Kerberos server
- Stores all passwords are encrypted with a single key
- Assumes workstations are secure
- May result in cascading loss of trust.
- Scalability

Is Kerberos Infallible?

No security measure is 100% impregnable, and Kerberos is no exception. Because it's been around for so long, hackers have had the ability over the years to find ways around it, typically through forging tickets, repeated attempts at password guessing (brute force/credential stuffing), and the use of malware, to downgrade the encryption.

Despite this, Kerberos remains the best access security protocol available today. The protocol is flexible enough to employ stronger encryption algorithms to combat new threats, and if users employ good password-choice guidelines, you shouldn't have a problem!

What is Kerberos Used For?

Although Kerberos can be found everywhere in the digital world, it is commonly used in secure systems that rely on robust authentication and auditing capabilities. Kerberos is used for Posix, Active Directory, NFS, and Samba authentication. It is also an alternative authentication system to SSH, POP, and SMTP.

Kerberos Version 4 :

Kerberos version 4 is an update of the Kerberos software that is a computer-network authentication system. Kerberos version 4 is a web-based authentication software which is used for authentication of users information while logging into the system by DES technique for encryption. It was launched in late 1980s.

S.No.	Kerberos Version 4	Kerberos Version 5
1.	Kerberos version 4 was launched in late 1980s.	Kerberos version 5 was launched in 1993.
2.	It provides ticket support.	It provides ticket support with extra facilities for forwarding, renewing and postdating tickets.
3.	Kerberos version 4 works on the Receiver-makes-Right encoding system.	Kerberos version 5 works on the ASN.1 encoding system.
4.	It does not support transitive cross-realm authentication.	It supports transitive cross-realm authentication.
5.	It uses Data Encryption Standard technique for encryption.	It uses any encryption techniques as the cipher text is tagged with an encryption identifier.

6.	In Kerberos version 4, the ticket lifetime has to be specified in units for a lifetime of 5 minutes.	In Kerberos version 5, the ticket lifetime is specified with the freedom of arbitrary time.

PGP – Authentication and Confidentiality

PGP (Pretty Good Privacy), is a popular program that is used to provide confidentiality and authentication services for electronic mail and file storage. It was designed by **Phil Zimmermann** way back in 1991. He designed it in such a way, that the best cryptographic algorithms such as RSA, Diffie-Hellman key exchange, DSS are used for the public-key encryption (or) asymmetric encryption; CAST-128, 3DES, IDEA are used for symmetric encryption and SHA-1 is used for hashing purposes. PGP software is an open source one and is not dependent on either of the OS (Operating System) or the processor. The application is based on a few commands which are very easy to use.

The following are the services offered by PGP:

1. Authentication
2. Confidentiality
3. Compression
4. Email Compatibility

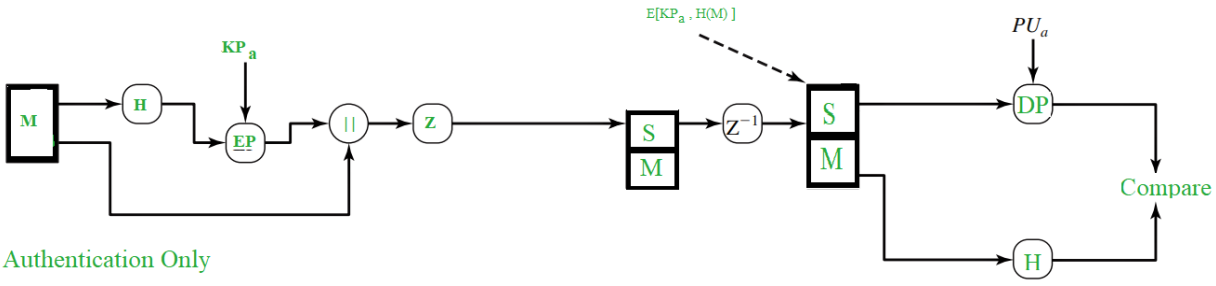
5. Segmentation

In this article, we will see about Authentication and Confidentiality.

1. Authentication:

Authentication basically means something that is used to validate something as true or real. To login into some sites sometimes we give our account name and password, that is an authentication verification procedure.

In the email world, checking the authenticity of an email is nothing but to check *whether it actually came from the person it says*. In emails, authentication has to be checked as there are some people who spoof the emails or some spams and sometimes it can cause a lot of inconvenience. The Authentication service in PGP is provided as follows:



As shown in the above figure, the Hash Function (H) calculates the Hash Value of the message. For the hashing purpose, **SHA-1** is used and it produces a **160 bit** output hash value. Then, using the sender's private key (KP_a), it is encrypted and it's called as **Digital Signature**. The Message is then appended to the signature. All the process happened till now, is sometimes described as *signing*

the message . Then the message is compressed to reduce the transmission overhead and is sent over to the receiver.

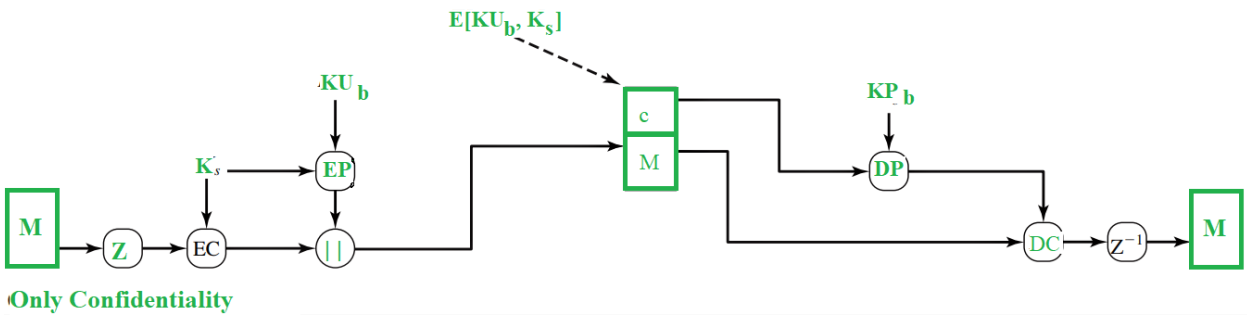
At the receiver's end, the data is decompressed and the message, signature are obtained. The signature is then decrypted using the sender's public key(PU_a) and the hash value is obtained. The message is again passed to hash function and it's hash value is calculated and obtained.

Both the values, one from signature and another from the recent output of hash function are compared and if both are same, it means that the email is actually sent from a known one and is legit, else it means that it's not a legit one.

2. Confidentiality:

Sometimes we see some packages labelled as 'Confidential', which means that those packages are not meant for all the people and only selected persons can see them. The same applies to the email confidentiality as well. Here, in the email service, only the sender and the receiver should be able to read the message, that means the contents have to be kept secret from every other person, except for those two.

PGP provides that Confidentiality service in the following manner:



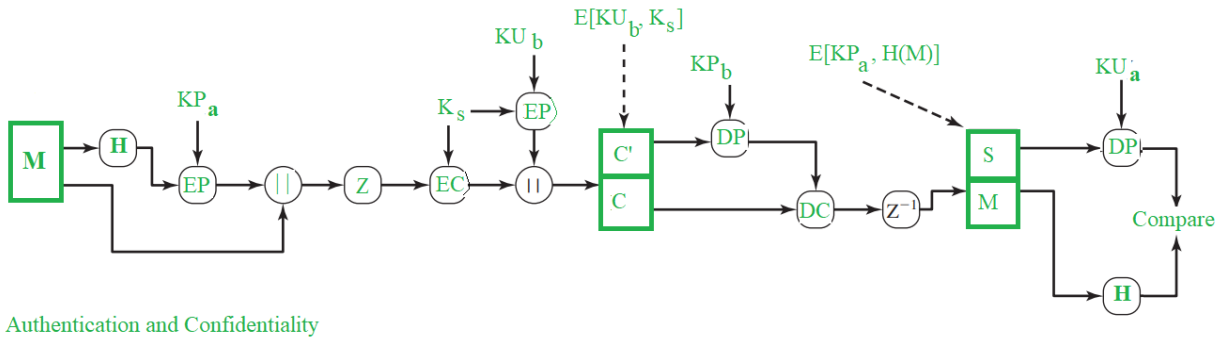
The message is first compressed and a 128 bit session key (K_s), generated by the PGP, is used to encrypt the message through symmetric encryption. Then, the session key (K_s) itself gets encrypted through public key encryption (EP) using receiver's public key(KU_b) . Both the encrypted entities are now concatenated and sent to the receiver.

As you can see, the original message was compressed and then encrypted initially and hence even if any one could get hold of the traffic, he cannot read the contents as they are not in readable form and they can only read them if they had the session key (K_s). Even though session key is transmitted to the receiver and hence, is in the traffic, it is in encrypted form and only the receiver's private key (KP_b)can be used to decrypt that and thus our message would be completely safe.

At the receiver's end, the encrypted session key is decrypted using receiver's private key (KP_b) and the message is decrypted with the obtained session key. Then, the message is decompressed to obtain the original message (M).

RSA algorithm is used for the public-key encryption and for the symmetric key encryption, CAST-128(or IDEA or 3DES) is used.

Practically, **both** the Authentication and Confidentiality services are provided in parallel as follows :



Authentication and Confidentiality

Note:

M – Message

H – Hash Function

K_s – A random Session Key created for Symmetric Encryption purpose

DP – Public-Key Decryption Algorithm

EP – Public-Key Encryption Algorithm

DC – Asymmetric Encryption Algorithm

EC – Symmetric Encryption Algorithm

KP_b – A private key of user B used in Public-key encryption process

KP_a – A private key of user A used in Public-key encryption process

PU_a – A public key of user A used in Public-key encryption process

PU_b – A public key of user B used in Public-key encryption process

|| – Concatenation

Z – Compression Function

Z^{-1} – Decompression Function

IP Security

Internet Protocol Authentication Header

Prerequisite: Internet Protocol version 6 (IPv6) Header

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.

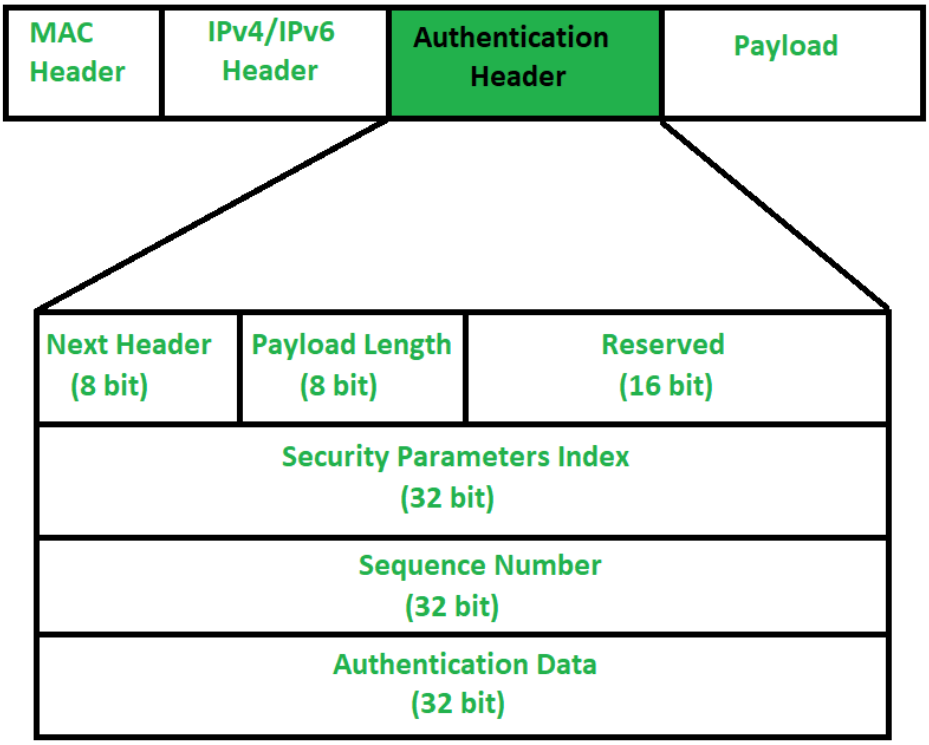
When packet is sent from source A to Destination B, it consists of data that we need to send and header which consist of information regarding packet. Authentication Header verifies origin of data and also payload to confirm if there has been modification done in between, during transmission between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

IP security (IPSec)

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 –

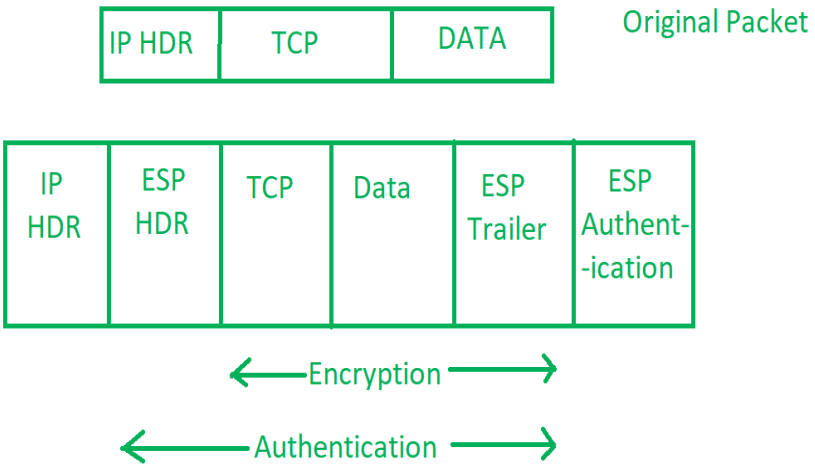
It has the following components:

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 set up 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.

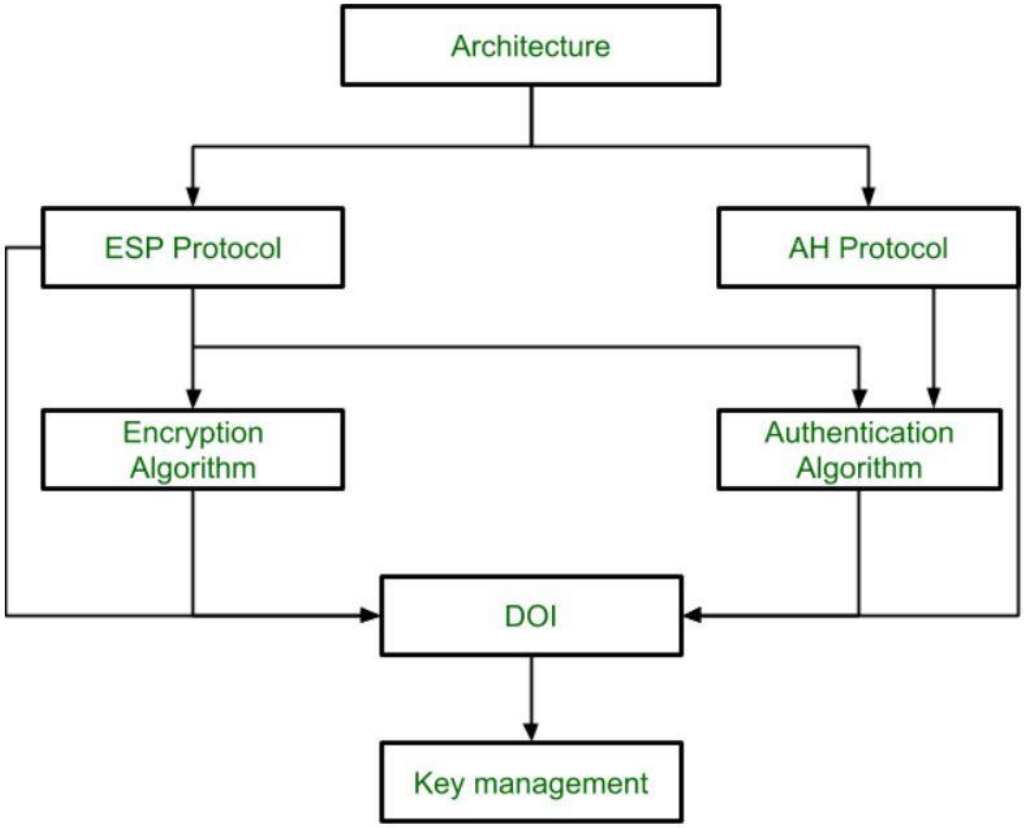
2. Then the **IKE Phase 1** starts in which the 2 hosts(using IPsec) authenticate themselves to each other to start a secure channel. It has 2 modes. The **Main mode** which provides the greater security and the **Aggressive mode** which enables the host to establish an IPsec circuit more quickly.
3. 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.

IPSec 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:



1. Architecture:

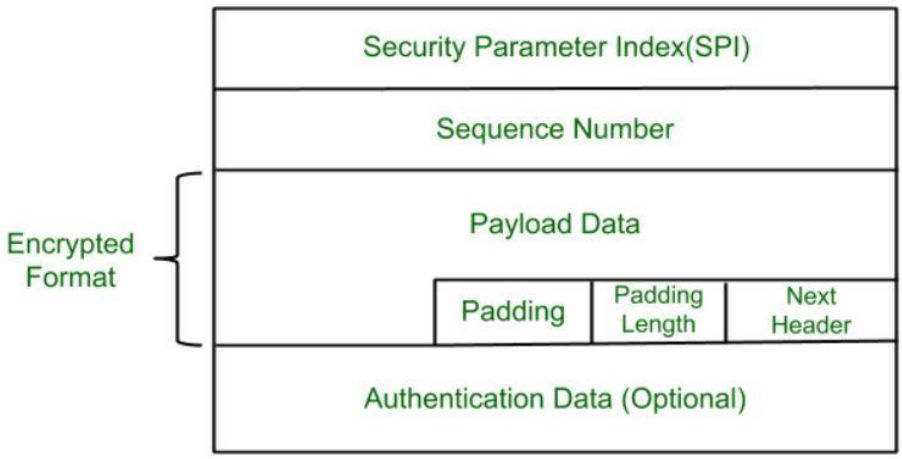
Architecture or IP Security Architecture covers the general concepts, definitions, protocols, algorithms and security requirements of IP Security technology.

2. ESP Protocol:

ESP(Encapsulation Security Payload) provide the confidentiality service. Encapsulation Security Payload is implemented in either two ways:

- ESP with optional Authentication.
- ESP with Authentication.

Packet Format:



- **Security Parameter Index(SPI):**
  This parameter is used in Security Association. It is used to give a unique number to the connection build between Client and Server.

- **Sequence Number:**
  Unique Sequence number are allotted to every packet so that at the receiver side packets can be arranged properly.

- **Payload Data:**
  Payload data means the actual data or the actual message. The Payload data is in encrypted format to achieve confidentiality.

- **Padding:**
  Extra bits or space added to the original message in order to ensure confidentiality. Padding length is the size of the added bits or space in the original message.

- **Next Header:**
  Next header means the next payload or next actual data.

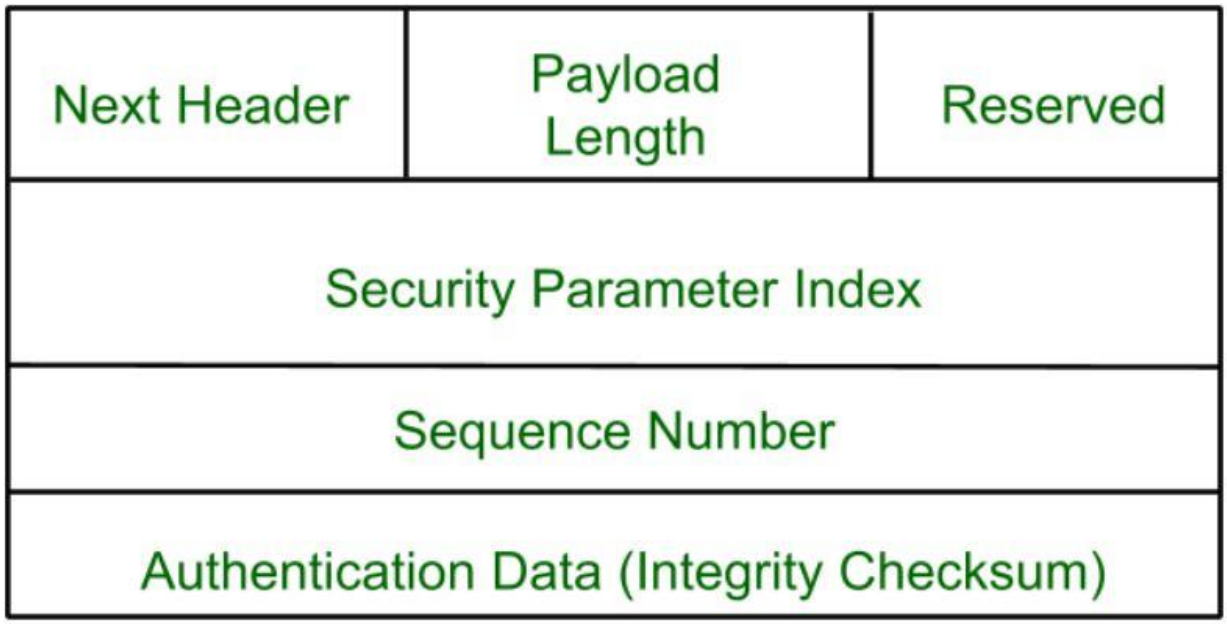
- **Authentication Data**
  This field is optional in ESP protocol packet format.

3. Encryption algorithm:

Encryption algorithm is the document that describes various encryption algorithm used for Encapsulation Security Payload.

4. AH Protocol:

AH (Authentication Header) Protocol provides both Authentication and Integrity service. Authentication Header is implemented in one way only: Authentication along with Integrity.



Authentication Header covers the packet format and general issue related to the use of AH for packet authentication and integrity.

5. Authentication Algorithm:

Authentication Algorithm contains the set of the documents that describe authentication algorithm used for AH and for the authentication option of ESP.

6. DOI (Domain of Interpretation):

DOI is the identifier which support both AH and ESP protocols. It contains values needed for documentation related to each other.

7. Key Management:

Key Management contains the document that describes how the keys are exchanged between sender and receiver.

Web Security

Web Security Defined

Web security refers to protecting networks and computer systems from damage to or the theft of software, hardware, or data. It includes protecting computer systems from misdirecting or disrupting the services they are designed to provide.

Web security is synonymous with cybersecurity and also covers website security, which involves protecting websites from attacks. It includes cloud security and web application security, which defend cloud services and web-based applications, respectively. Protection of a virtual private network (VPN) also falls under the web security umbrella.

Web security is crucial to the smooth operation of any business that uses computers. If a website is hacked or hackers are able to manipulate your systems or software, your website—and even your entire network—can be brought down, halting business operations.

Factors That Go Into Web Security and Web Protection

To comply with internal policies, government-imposed criteria, or Open Web Application Security Project (OWASP) standards, security professionals consider a variety of factors. Keeping abreast

with OWASP standards helps security staff stay up to date with industry-standard web safety expectations.

In addition, encryption must be kept up to date, the latest threats in the Web Hacking Incident Database (WHID) monitored, and user authentications properly managed. When vulnerabilities emerge, security personnel must install the most recent patches to address them. To secure data, software development teams have to implement protocols that shield code from being stolen during or after writing it.

Technologies for Web Security

Various technologies are available to help companies achieve web security, including web application firewalls (WAFs), security or vulnerability scanners, password-cracking tools, fuzzing tools, black box testing tools, and white box testing tools.

Web Application Firewalls (WAFs)

A web application firewall (WAF) protects web applications by monitoring and filtering internet traffic that flows between an application and the internet. In this way, a WAF works as a secure web gateway (SWG). It provides protection for web applications against attacks, including cross-site scripting, file inclusion, cross-site forgery, Structured Query Language (SQL) injection, and other threats.

In the Open Systems Interconnection (OSI) model, a WAF works within Layer 7. Even though it works against many internet threats, it is not intended to defend against all kinds of threats. A WAF often works within a suite of protective tools meant to defend a network, computer, or application. Learm more about what is WAF.

Security or Vulnerability Scanners

Vulnerability scanners refer to tools that organizations use to automatically examine their systems, networks, and applications to check for weaknesses in their security. Once a vulnerability scanner has finished checking the target system, security teams can use the results to address critical vulnerabilities.

Password-cracking Tools

With password-cracking tools, you can still gain access to your system even if you have lost or forgotten your password. This helps maintain web security for business in a couple of different ways.

First, if you need to reset your password but cannot remember the original one, a password-cracking tool allows you to gain access. Second, if someone has penetrated your system and changed the password, you can use a password-cracking tool to get back in and change the password to something harder to figure out, thereby regaining control.

Fuzzing Tools

Fuzzing tools are used to check software, networks, or operating systems for coding errors that may result in security weaknesses. Once an error is found, a fuzzer pinpoints the potential causes of the problem.

Fuzzing tools can be valuable at various stages of the software development process as well. Whether implemented during initial testing, before final deployment, or somewhere in between, developers can use them to gain insights into vulnerabilities so they can be addressed.

Black Box Testing Tools

Black box testing refers to checking a system without any knowledge regarding how it works. The only thing the tester sees is the input they key in and the resulting output. In many ways, the tester has only as much knowledge of the system as a random user would have.

Black box testing tools are used to see how the system responds to unexpected actions taken by users. They can help security personnel inspect response times and detect issues in software performance and whether or not the system is reliable.

White Box Testing Tools

Black box testing happens from the user's point of view, without any insight into the code itself, while white box testing gives you a look inside how the software works. With white box testing, the design, coding, and internal structure of software is tested to enhance its design, as well as ensure the smooth flow of data into and out of the application.

During white box testing, you can see the code, so it is sometimes also called clear box testing or transparent box testing.

Threats to Web Security

SQL Injection

SQL injection is a technique an attacker uses to exploit vulnerabilities in a database's search process. With SQL injection, an attacker can obtain access to privileged information, create user permissions, modify permissions, or execute plans to change, manipulate, or destroy data. In this way, a hacker can capture sensitive information or alter it to interrupt or control the functioning of a crucial system.

Cross-site Scripting

Cross-site scripting (XSS) refers to a vulnerability that gives hackers an opening to insert client-side scripts inside a page. This is then used to gain access to critical data directly. XSS can also be used by a hacker to pretend to be another user or to fool a user into disclosing crucial information.

Remote File Inclusion

With remote file inclusion, an attacker references external scripts using vulnerabilities in a web application. The attacker can then attempt to use the referencing function within an application to upload malware. These types of malware are also referred to as backdoor shells. All this is done from a different Uniform Resource Locator (URL) within a separate domain.

Password Breach

Breaching a user's password is a common technique to gain access to web resources. In many cases, the hacker will use a password that the user or administrator had used to log in to another site for which the hacker has a list of login credentials.

In other cases, hackers use a technique called password spraying, in which they use common passwords like "12345678" or "password123," and try them out one after the other until they gain access. There are several other techniques like keyloggers or simply finding your password written down and using it.

Data Breach

A data breach refers to when confidential or sensitive information gets exposed. Data breaches can sometimes happen by accident, but they are often perpetrated by hackers with the intention of using or selling the data.

Code Injection

Code injection involves an attacker using an input validation vulnerability in a computer's software system to introduce and run malicious code. This code then proceeds to make changes to how the software and computer work.

Best Defense Strategies for Developer for Web Security

Resource Assignment

With a resource assignment strategy, a developer designates the needed resources in a way that lets the developer know about new issues as they arise. With constant updates, the developer can identify and take action against threats before security actually gets breached.

Web Scanning

Web scanning involves using an application to crawl a website in search for vulnerabilities that can leave it open to a bot, spyware, rootkit, Trojan horse, or distributed denial-of-service (DDoS) attack. The scanner checks all the pages on the website, forming a diagram complete with a structure representing the layout of the site. It then systematically checks the entire site for potential weaknesses.

Protection Provided by Web Security

Web security protects an organization against some of the most common internet threats on the landscape.

Stolen Data

Attackers often try to steal data to gain access to payment systems, email accounts, or other sites or applications that require authentication. In some cases, the hacker will use the data themselves, but they may also sell it to someone else.

Phishing Schemes

Hackers use phishing to fool users into disclosing sensitive information. They may do this using emails or by setting up fake websites that look real. The user then enters sensitive data into the fake website, which makes it available for the attacker.

Session Hijacking

With session hijacking, an attacker will take control of a user's session and then do things on a site in the user's name. Because it appears that the user is the one performing the actions, the attacker can hide their identity, potentially getting away with whatever illicit activity they engaged in while on the site.

Malicious Redirects

Malicious redirects involve sending a user to a malicious site they never intended to visit. Once on this site, the user's computer can be infected with malware.

SEO Spam

In a search engine optimization (SEO) spam attack, abnormal links, comments, or pages are put on a site by attackers to distract visitors or cause them to visit malicious sites.

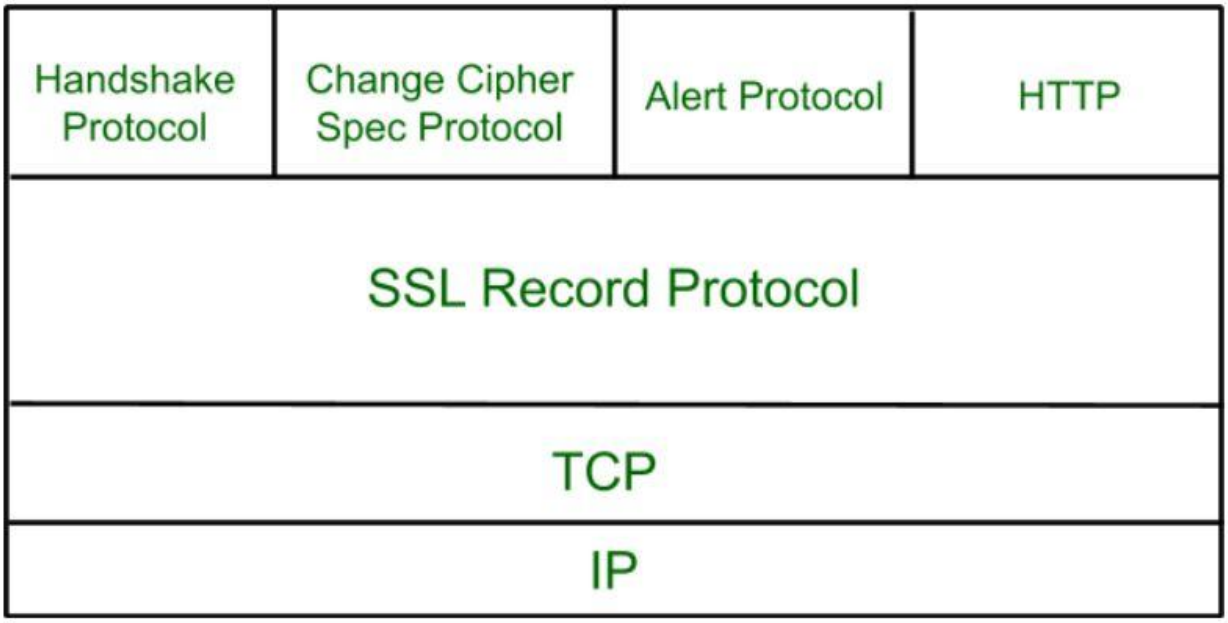
Secure Socket Layer (SSL)

Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

Secure Socket Layer Protocols:

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol

SSL Protocol Stack:

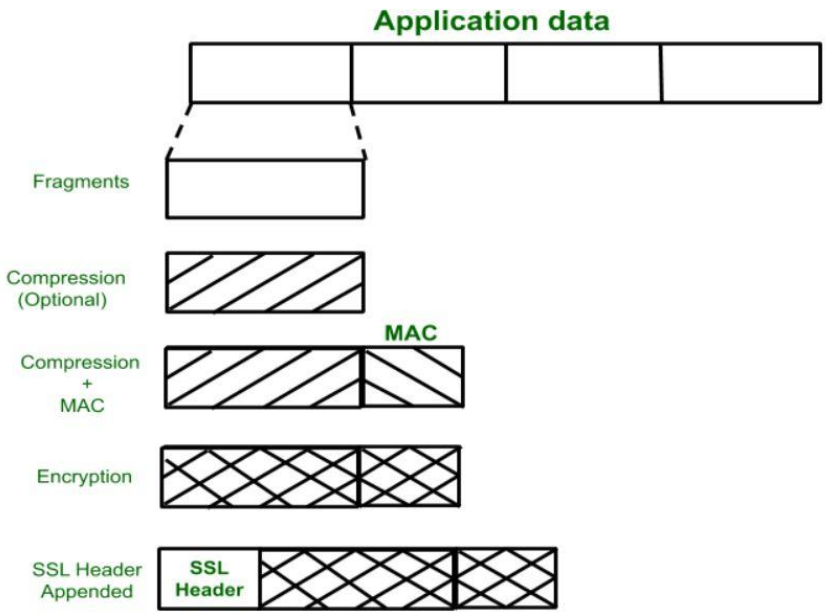


SSL Record Protocol:

SSL Record provides two services to SSL connection.

- Confidentiality
- Message Integrity

In the SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended. After that encryption of the data is done and in last SSL header is appended to the data.



Handshake Protocol:

Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

- **Phase-1:** In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purposes.
- **Phase-2:** Server sends his certificate and Server-key-exchange. The server end phase-2 by sending the Server-hello-end packet.
- **Phase-3:** In this phase, Client replies to the server by sending his certificate and Client-exchange-key.

- **Phase-4:** In Phase-4 Change-cipher suite occurred and after this Handshake Protocol ends.

Change-cipher Protocol:

This protocol uses the SSL record protocol. Unless Handshake Protocol is completed, the SSL record Output will be in a pending state. After handshake protocol, the Pending state is converted into the current state.

Change-cipher protocol consists of a single message which is 1 byte in length and can have only one value. This protocol's purpose is to cause the pending state to be copied into the current state.

Alert Protocol:

This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contains 2 bytes.

The level is further classified into two parts:

Warning (level = 1):

This Alert has no impact on the connection between sender and receiver. Some of them are:

Bad certificate: When the received certificate is corrupt.

No certificate: When an appropriate certificate is not available.

Certificate expired: When a certificate has expired.

Certificate unknown: When some other unspecified issue arose in processing the certificate, rendering it unacceptable.

Close notify: It notifies that the sender will no longer send any messages in the connection.

Fatal Error (level = 2):

This Alert breaks the connection between sender and receiver. Some of them are :

Handshake failure: When the sender is unable to negotiate an acceptable set of security parameters given the options available.

Decompression failure: When the decompression function receives improper input.

Illegal parameters: When a field is out of range or inconsistent with other fields.

Bad record MAC: When an incorrect MAC was received.

Unexpected message: When an inappropriate message is received.

The second byte in the Alert protocol describes the error.

Silent Features of Secure Socket Layer:

- The advantage of this approach is that the service can be tailored to the specific needs of the given application.
- Secure Socket Layer was originated by Netscape.
- SSL is designed to make use of TCP to provide reliable end-to-end secure service.
- This is a two-layered protocol.

Transport Layer Security (TLS)

Transport Layer Securities (TLS) are designed to provide security at the transport layer. TLS was derived from a security protocol called Secure Socket Layer (SSL). TLS ensures that no third party may eavesdrop or tampers with any message.

There are several benefits of TLS:

- **Encryption:**
  TLS/SSL can help to secure transmitted data using encryption.
- **Interoperability:**
  TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.
- **Algorithm flexibility:**
  TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.
- **Ease of Deployment:**
  Many applications TLS/SSL temporarily on a windows server 2003 operating systems.
- **Ease of Use:**
  Because we implement TLS/SSL beneath the application layer, most of

its operations are completely invisible to client.

Working of TLS:

The client connect to server (using TCP), the client will be something. The client sends number of specification:

1. Version of SSL/TLS.
2. which cipher suites, compression method it wants to use.

The server checks what the highest SSL/TLS version is that is supported by them both, picks a cipher suite from one of the clients option (if it supports one) and optionally picks a compression method. After this the basic setup is done, the server provides its certificate. This certificate must be trusted either by the client itself or a party that the client trusts. Having verified the certificate and being certain this server really is who he claims to be (and not a man in the middle), a key is exchanged. This can be a public key, “PreMasterSecret” or simply nothing depending upon cipher suite.

Both the server and client can now compute the key for symmetric encryption. The handshake is finished and the two hosts can communicate securely. To close a connection by finishing. TCP connection both sides will know the connection

was improperly terminated. The connection cannot be compromised by this through, merely interrupted.

Intruders

The most common threat to security is the attack by the intruder. Intruders are often referred to as hackers and are the most harmful factors contributing to the vulnerability of security. They have immense knowledge and an in-depth understanding of technology and security. Intruders breach the privacy of users and aim at stealing the confidential information of the users. The stolen information is then sold to third-party, which aim at misusing the information for their own personal or professional gains.

Intruders are divided into three categories:

- **Masquerader:** The category of individuals that are not authorized to use the system but still exploit user's privacy and confidential information by possessing techniques that give them control over the system, such category of intruders is referred to as Masquerader. A Masquerader is people that are outsiders and they don't have direct access to the system, which aims to attack unethically by stealing data/ information.
- **Misfeasor:** The category of individuals that are authorized to use the system, but misuse the granted access and privilege. These are individuals that take undue advantage of the permissions and access given to them, such category of intruders is referred to as Misfeasor. Masqueraders are people that are insiders and they have direct access to the system, which they aim to attack unethically by stealing data/ information.
- **Clandestine User:** The category of individuals that have supervision control over the system and misuse the authoritative power given to them. The misconduct of power is done often done by superlative

authorities for financial gains, such a category of intruders is referred to as Clandestine User. A Clandestine User is people that can be any of the two, insiders or outsiders, and accordingly, they can have direct/ indirect access to the system, which they aim to attack unethically by stealing data/ information.

Below are the different ways adopted by intruders for cracking passwords for stealing confidential information:

- Regressively try all short passwords that may open the system for them.
- Try unlocking the system with default passwords, which will open the system if the user has not made any change to the default password.
- Try unlocking the system by personal information of the user such as their name, family member names, address, phone number in different combinations.
- Making use of Trojan horse for getting access to the system of the user.
- Attacking the connection of the host and remote user and getting entry through their connection gateway.
- Trying all the applicable information, relevant to the user such as plate numbers, room numbers, locality info.

To prevent intruders from attacking the computer system, it is extremely important to be aware of the preventive measures which may make the system vulnerable to security. Also, whenever there is potential detection for the system being attacked make sure to reach cyber security experts as soon as possible.

Intrusion Technique

Asymmetric Routing

In this method, the attacker attempts to utilize more than one route to the targeted network device. The idea is to have the overall attack evade detection by having a significant portion of the offending packets bypass certain network segments and their network intrusion sensors. Networks that are not set up for asymmetric routing are impervious to this attack methodology.

Buffer Overflow Attacks

This approach attempts to overwrite specific sections of computer memory within a network, replacing normal data in those memory locations with a set of commands that will later be executed as part of the attack. In most cases, the goal is to initiate a denial of service (DoS) situation, or to set up a channel through which the attacker can gain remote access to the network. Accomplishing such attacks is more difficult when network designers keep buffer sizes relatively small, and/or install boundary-checking logic that identifies executable code or lengthy URL strings before it can be written to the buffer.

Common Gateway Interface Scripts

The Common Gateway Interface (CGI) is routinely used in networks to support interaction between servers and clients on the Web. But it also provides easy openings—such as "backtracking"—through which attackers can access supposedly secure network system files. When systems fail to include input verification or check for backtrack characters, a covert CGI script can easily add the directory label ".." or the pipe "|" character to any file path name and thereby access files that should not be available via the Web.

Protocol-Specific Attacks

When performing network activities, devices obey specific rules and procedures. These protocols—such as ARP, IP, TCP, UDP, ICMP, and various application protocols—may inadvertently leave openings for network intrusions via protocol impersonation ("spoofing") or malformed protocol messages. For example, Address Resolution Protocol (ARP) does not perform authentication on messages, allowing attackers to

execute "man-in-the-middle" attacks. Protocol-specific attacks can easily compromise or even crash targeted devices on a network.

Traffic Flooding
An ingenious method of network intrusion simply targets network intrusion detection systems by creating traffic loads too heavy for the system to adequately screen. In the resulting congested and chaotic network environment, attackers can sometimes execute an undetected attack and even trigger an undetected "fail-open" condition.

Trojans
These programs present themselves as benign and do not replicate like a virus or a worm. Instead, they instigate DoS attacks, erase stored data, or open channels to permit system control by outside attackers. Trojans can be introduced into a network from unsuspected online archives and file repositories, most particularly including peer-to-peer file exchanges.

Worms
A common form of standalone computer virus, worms are any computer code intended to replicate itself without altering authorized program files. Worms often spread through email attachments or the Internet Relay Chat (IRC) protocol. Undetected worms eventually consume so many network resources, such as processor cycles or bandwidth, that authorized activity is simply squeezed out. Some worms actively seek out confidential information—such as files containing the word "finance" or "SSN"—and communicate such data to attackers lying in wait outside the network.

Once these attack vectors are thoroughly understood, network security teams can look for opportunities to deploy technologies and strategies that will mitigate the potential effectiveness of each one.

Intrusion Detection System (IDS)

An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once send the warning notifications.

Classification of Intrusion Detection System:

IDS are classified into 5 types:

1. **Network Intrusion Detection System (NIDS):**
   Network intrusion detection systems (NIDS) are set up at a planned

point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.

2. **Host Intrusion Detection System (HIDS):**
   Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.
3. **Protocol-based Intrusion Detection System (PIDS):**
   Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

4. **Application Protocol-based Intrusion Detection System (APIDS):**
   Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.
5. **Hybrid Intrusion Detection System :**
   Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Detection Method of IDS:

1. **Signature-based Method:**
   Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1’s or number of 0’s in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.
   Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

2. **Anomaly-based Method:**
   Anomaly-based IDS was introduced to detect unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Comparison of IDS with Firewalls:

IDS and firewall both are related to network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it doesn't signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.

Password Protection

1. Use longer passwords

The longer the password, the harder it is to crack. Try using a phrase or sentence, rather than a single word. The more characters you add, the harder it is for an automated program to guess it.

2. Block common passwords

There are certain passwords that are so common that hackers use them as their first attempts. These passwords should be blacklisted, so your employees cannot use them

to protect their accounts. You may also consider limiting the number of failed login attempts to block other brute-force attacks.

3. Use two-factor authentication

Passwords aren't your only method of protection. By adding two-factor (or multi-factor) authentication, you can add an extra layer of security. After entering a password, the user is sent a one-time code or USB token. Using two-factor authentication makes it much harder for hackers to gain access to the account.

4. Encrypt passwords

When you encrypt passwords or data before transmission, it enhances your security. If a hacker intercepts the transmission, they will be unable to decrypt it, thus rendering it useless.

5. Train your employees

The weakest link in network security is often the human element. People tend to write down passwords, share passwords, or use unsecured passwords without realizing the security risks. By taking the time to train your employees, you are helping to impress upon them their part in keeping your data secure. Getting your employees on board can make a big difference in your security.

It's important to protect your network with passwords, but in a way that will stop hackers in their tracks. Long passwords and encrypted passwords, two-factor authentication, and employee training can all help increase the strength of your security. Your network is only as strong as its weakest password.

Password selection strategies

Password selection strategies:The goal is to eliminate guessable passwords while allowing the user to select a password that is memorable. Four basic techniques are in use.

- User education

Users can be told the importance of using hard-to-guess passwords and can be provided with guidelines for selecting strong passwords.This user

education strategy is unlikely to succeed at most installations, particularly where there is a large user population or a lot of turnover. Many users will simply ignore the guidelines. Others may not be good judges of what is a strong password. For example, many users (mistakenly) believe that reversing a word or capitalizing the last letter makes a password unguessable.

- Computer-generated passwords

passwords are quite random in nature.Computer-generated passwords also have problems.If the passwords are quite random in nature,users will not be able to remember them.Even if the password is pronounceable, the user may have difficulty remembering it and so be tempted to write it down. In general, computer-generated password schemes have a history of poor acceptance by users. FIPS PUB 181 defines one of the best-designed automated password generators.The standard includes not only a description of the approach but also a complete listing of the C source code of the algorithm.The algorithm generates words by forming pronounceable syllables and concatenating them to form a word.A random number generator produces a random stream of characters used to construct the syllables and words.

- Reactive password checking

A reactive password checking strategy is one in which the system periodically runs its own password cracker to find guessable passwords.The system cancels any passwords that are guessed and notifies the user.This tactic has a number of drawbacks. First it is resource intensive, if the job is done right. Because a determined opponent who is able to steal a password file can devote full CPU time to the task for hours or even days an effective reactive password checker is at a distinct disadvantage. Furthermore, any existing passwords remain vulnerable until the reactive password checker finds them.

- Proactive password checking

The most promising approach to improved password security is a proactive password checker. In this scheme, a user is allowed to select his or her own password.However,at the time of selection,the system checks to see if the password is allowable and if not, rejects it. Such checkers are based on the philosophy that with sufficient guidance from the system, users can select memorable passwords from a fairly large password space that are not likely to be guessed in a dictionary attack. The trick with a proactive password checker is to strike a balance between user acceptability and strength.If the system rejects too many passwords,users will complain that it is too hard to select a password. If the system uses some simple algorithm to define what is acceptable,this provides guidance to password crackers to refine their guessing technique. In the remainder of this subsection, we look at possible approaches to proactive password checking.

Malwares – Malicious Software

Malware is a software that gets into the system without user consent with an intention to steal private and confidential data of the user that includes bank details and password. They also generates annoying pop up ads and makes changes in system settings

They get into the system through various means:

1. Along with free downloads.
2. Clicking on suspicious link.
3. Opening mails from malicious source.
4. Visiting malicious websites.
5. Not installing an updated version of antivirus in the system.

Types:

1. Virus
2. Worm
3. Logic Bomb
4. Trojan/Backdoor
5. Rootkit
6. Advanced Persistent Threat
7. Spyware and Adware

What is computer virus:

Computer virus refers to a program which damages computer systems and/or destroys or erases data files. A computer virus is a malicious program that self-replicates by copying itself to another program. In other words, the computer virus spreads by itself into other executable code or documents. The purpose of creating a computer virus is to infect vulnerable systems, gain admin control and steal user sensitive data. Hackers design computer viruses with malicious intent and prey on online users by tricking them.

Symptoms:

- Letter looks like they are falling to the bottom of the screen.
- The computer system becomes slow.
- The size of available free memory reduces.

- The hard disk runs out of space.
- The computer does not boot.

Types of Computer Virus:

These are explained as following below.

1. **Parasitic –**
   These are the executable (.COM or .EXE execution starts at first instruction). Propagated by attaching itself to particular file or program. Generally resides at the start (prepending) or at the end (appending) of a file, e.g. Jerusalem.
2. **Boot Sector –**
   Spread with infected floppy or pen drives used to boot the computers. During system boot, boot sector virus is loaded into main memory and destroys data stored in hard disk, e.g. Polyboot, Disk killer, Stone, AntiEXE.
3. **Polymorphic –**
   Changes itself with each infection and creates multiple copies. Multipartite: use more than one propagation method. >Difficult for antivirus to detect, e.g. Involutionary, Cascade, Evil, Virus 101., Stimulate.
   Three major parts: Encrypted virus body, Decryption routine varies from infection to infection, and Mutation engine.

4. **Memory Resident –**
   Installs code in the computer memory. Gets activated for OS run and damages all files opened at that time, e.g. Randex, CMJ, Meve.
5. **Stealth –**
   Hides its path after infection. It modifies itself hence difficult to detect and masks the size of infected file, e.g. Frodo, Joshi, Whale.
6. **Macro –**
   Associated with application software like word and excel. When opening the infected document, macro virus is loaded into main memory and destroys the data stored in hard disk. As attached with documents; spreads with those infected documents only, e.g. DMV, Melissa, A, Relax, Nuclear, Word Concept.
7. **Hybrids –**
   Features of various viruses are combined, e.g. Happy99 (Email virus).

Worm:

A worm is a destructive program that fills a computer system with self-replicating information, clogging the system so that its operations are slowed down or stopped.

Types of Worm:

1. **Email worm –** Attaching to fake email messages.
2. **Instant messaging worm –** Via instant messaging applications using loopholes in network.

3. **Internet worm –** Scans systems using OS services.
4. **Internet Relay Chat (IRC) worm –** Transfers infected files to web sites.
5. **Payloads –** Delete or encrypt file, install backdoor, creating zombie etc.
6. **Worms with good intent –** Downloads application patches.

Logical Bomb:

A logical bomb is a destructive program that performs an activity when a certain action has occurred. These are hidden in programming code. Executes only when a specific condition is met, e.g. Jerusalem.

Script Virus:

Commonly found script viruses are written using the Visual Basic Scripting Edition (VBS) and the JavaScript programming language.

Trojan / Backdoor:

Trojan Horse is a destructive program. It usually pretends as computer games or application software. If executed, the computer system will be damaged. Trojan Horse usually comes with monitoring tools and key loggers. These are active only when specific events are alive. These are hidden with packers, crypters and wrappers.< Hence, difficult to detect through antivirus. These can use manual removal or firewall precaution.

RootKits:

Collection of tools that allow an attacker to take control of a system.

- Can be used to hide evidence of an attacker's presence and give them backdoor access.
- Can contain log cleaners to remove traces of attacker.
- Can be divided as:
  – Application or file rootkits: replaces binaries in Linux system
  – Kernel: targets kernel of OS and is known as a loadable kernel module (LKM)
- Gains control of infected m/c by:
  – DLL injection: by injecting malicious DLL (dynamic link library)
  – Direct kernel object manipulation: modify kernel structures and directly target trusted part of OS
  – Hooking: changing applicant's execution flow

Advanced Persistent Threat:

Created by well funded, organized groups, nation-state actors, etc. Desire to compromise government and commercial entities, e.g. Flame: used for reconnaissance and information gathering of system.

Spyware and Adware:

Normally gets installed along with free software downloads. Spies on the end-user, attempts to redirect the user to specific sites. Main tasks: Behavioral surveillance and advertising with pop up ads Slows down the system.

How The Antivirus Detects Virus?

Signature detection is a method by which antivirus keenly scans files that are brought into a system to analyze more likely hazardous files.

In essence, antivirus applications come with a directory of already checked-viruses and match the codes and patterns in files and web pages to unique bits and patterns that make up the code of a virus. If they match, the file is quarantined, means that it is moved to a new and safe location so that it does not infect any other files on the system.

Antivirus programs also checks for any malicious behavior on a system such as suspicious registry entries or executing an unknown program automatically upon system startup thus protecting our computer against encrypted viruses or viruses that are still unidentified.

Following is a list of the different virus detection methods an antivirus can use to protect our computer.

1. **Virus Definitions :**This is essentially the first method conventional antivirus software utilize to identify virus.

   The programs look for signatures to detect new malware. The antivirus companies analyze and extract an exact signature of the file and keep them in a database to which threats are compared and devices are then protected in case the signatures match.
2. **Heuristic-based detection :** This is the most common form of detection that uses an algorithm to compare the signature of known viruses against a potential threat. An antivirus packed with this type of detection can also detect viruses that have not yet been discovered and released as a new virus but it can also generate false positive matches

which means an antivirus scanner may report an uninfected file as an infected one.

3. **Behavior-based detection :**If a virus passes the above detection methods, the antivirus then observes the behavior of programs running on the computer. The antivirus triggers a warning if a program begins to perform strange actions listed below:
    - Settings of other programs are changed
    - Dozens of files are modified or deleted
    - Remotely connecting to computers
4. This is a useful method for finding viruses or any other type of malware that attempt to steal or log information.
5. **Sandbox Detection :** This is a type of detection method in which antivirus software run programs in a virtual environment and record the actions it performs to identify whether the programs are malicious or not. If the program is found safe, it is then executed in the real environment.

    This technique is rarely used in consumer antivirus solutions as it is both heavy and slow but antivirus solutions designed for corporate and network use offer this.
6. **Data Mining :** Data Mining is the recent development in malware detection that security companies now provide with their antivirus products to detect and eliminate forms of malware that has just been released. First, a series of features of files are extracted from files and then data mining and machine learning algorithms are used to determine the behavior of a file to detect whether the file is malicious or not.

Types of Scans

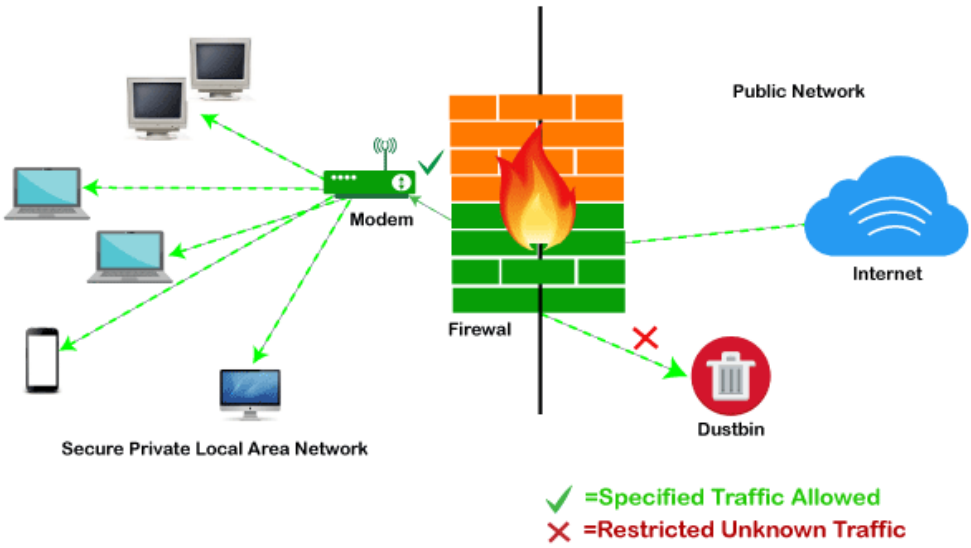
Apart from the detection methods explained above, the types of scans an antivirus offers is an equal measure of how successful it is.

1. **On-Demand Scan :** The term ‘On-demand’ scanning itself means that this feature either runs when the user wants to scan his computer on suspecting any abnormal behavior or the user schedules it to run at a specified time. It searches the contents of the disks, directories and files and boot sectors and system components as well. These are used either as a preventive maintenance activity or when a virus is suspected.
2. **Real-Time Protection :** Almost all modern antivirus programs offer this type of automatic protection that runs in background thereby increasing chances of catching malware before it does damage. Thus, these types of scans are also known as **‘background guard’**. It basically monitors the system for any suspicious activity in real time while data is loaded into the active memory. For example, when a USB drive is inserted or a downloaded file is executed.
3. **Smart Scans :** Under Smart Scans, an antivirus only scans the selected files that are more suspicious to be infected. This type of scanning lowers the need of system resources while protecting against the more common types of viruses, threats and risks.

What is a Firewall?

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.



How does a firewall work?

A firewall system analyzes network traffic based on pre-defined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.

Typically, firewalls intercept network traffic at a computer's entry point, known as a port. Firewalls perform this task by allowing or blocking specific data packets (units of communication transferred over a digital network) based on pre-defined security rules. Incoming traffic is allowed only through trusted IP addresses, or sources.

Types of Firewall

Packet-filtering Firewalls

A packet filtering firewall is the most basic type of firewall. It acts like a management program that monitors network traffic and filters incoming packets based on configured security rules. These firewalls are designed to block network traffic IP protocols, an IP address, and a port number if a data packet does not match the established rule-set.

While packet-filtering firewalls can be considered a fast solution without many resource requirements, they also have some limitations. Because these types of firewalls do not prevent web-based attacks, they are not the safest.

Circuit-level Gateways

Circuit-level gateways are another simplified type of firewall that can be easily configured to allow or block traffic without consuming significant computing resources. These types of firewalls typically operate at the session-level of the OSI model by verifying **TCP (Transmission Control Protocol)** connections and sessions. Circuit-level gateways are designed to ensure that the established sessions are protected.

Typically, circuit-level firewalls are implemented as security software or pre-existing firewalls. Like packet-filtering firewalls, these firewalls do not check for actual data, although they inspect information about transactions. Therefore, if a data contains malware, but follows the correct TCP connection, it will pass through the gateway. That is why circuit-level gateways are not considered safe enough to protect our systems.

Application-level Gateways (Proxy Firewalls)

Proxy firewalls operate at the application layer as an intermediate device to filter incoming traffic between two end systems (e.g., network and traffic systems). That is why these firewalls are called **'Application-level Gateways'**.

Unlike basic firewalls, these firewalls transfer requests from clients pretending to be original clients on the web-server. This protects the client's identity and other suspicious information, keeping the network safe from potential attacks. Once the connection is established, the proxy firewall inspects data packets coming from the source. If the contents of the incoming data packet are protected, the proxy firewall transfers it to the client. This approach creates an additional layer of security between the client and many different sources on the network.

Stateful Multi-layer Inspection (SMLI) Firewalls

Stateful multi-layer inspection firewalls include both packet inspection technology and TCP handshake verification, making SMLI firewalls superior to packet-filtering firewalls

or circuit-level gateways. Additionally, these types of firewalls keep track of the status of established connections.

In simple words, when a user establishes a connection and requests data, the SMLI firewall creates a database (state table). The database is used to store session information such as source IP address, port number, destination IP address, destination port number, etc. Connection information is stored for each session in the state table. Using stateful inspection technology, these firewalls create security rules to allow anticipated traffic.

In most cases, SMLI firewalls are implemented as additional security levels. These types of firewalls implement more checks and are considered more secure than stateless firewalls. This is why stateful packet inspection is implemented along with many other firewalls to track statistics for all internal traffic. Doing so increases the load and puts more pressure on computing resources. This can give rise to a slower transfer rate for data packets than other solutions.

Next-generation Firewalls (NGFW)

Many of the latest released firewalls are usually defined as '**next-generation firewalls**'. However, there is no specific definition for next-generation firewalls. This type of firewall is usually defined as a security device combining the features and functionalities of other firewalls. These firewalls include **deep-packet inspection (DPI),** surface-level packet inspection, and TCP handshake testing, etc.

NGFW includes higher levels of security than packet-filtering and stateful inspection firewalls. Unlike traditional firewalls, NGFW monitors the entire transaction of data, including packet headers, packet contents, and sources. NGFWs are designed in such a way that they can prevent more sophisticated and evolving security threats such as malware attacks, external threats, and advance intrusion.

Threat-focused NGFW

Threat-focused NGFW includes all the features of a traditional NGFW. Additionally, they also provide advanced threat detection and remediation. These types of firewalls are capable of reacting against attacks quickly. With intelligent security automation, threat-focused NGFW set security rules and policies, further increasing the security of the overall defense system.

In addition, these firewalls use retrospective security systems to monitor suspicious activities continuously. They keep analyzing the behavior of every activity even after the initial inspection. Due to this functionality, threat-focus NGFW dramatically reduces the overall time taken from threat detection to cleanup.

Network Address Translation (NAT) Firewalls

Network address translation or NAT firewalls are primarily designed to access Internet traffic and block all unwanted connections. These types of firewalls usually hide the IP addresses of our devices, making it safe from attackers.

When multiple devices are used to connect to the Internet, NAT firewalls create a unique IP address and hide individual devices' IP addresses. As a result, a single IP address is used for all devices. By doing this, NAT firewalls secure independent network addresses from attackers scanning a network for accessing IP addresses. This results in enhanced protection against suspicious activities and attacks.

In general, NAT firewalls works similarly to proxy firewalls. Like proxy firewalls, NAT firewalls also work as an intermediate device between a group of computers and external traffic.

Cloud Firewalls

Whenever a firewall is designed using a cloud solution, it is known as a cloud firewall or **FaaS (firewall-as-service)**. Cloud firewalls are typically maintained and run on the Internet by third-party vendors. This type of firewall is considered similar to a proxy firewall. The reason for this is the use of cloud firewalls as proxy servers. However, they are configured based on requirements.

The most significant advantage of cloud firewalls is scalability. Because cloud firewalls have no physical resources, they are easy to scale according to the organization's demand or traffic-load. If demand increases, additional capacity can be added to the cloud server to filter out the additional traffic load. Most organizations use cloud firewalls to secure their internal networks or entire cloud infrastructure.

Unified Threat Management (UTM) Firewalls

UTM firewalls are a special type of device that includes features of a stateful inspection firewall with anti-virus and intrusion prevention support. Such firewalls are designed to

provide simplicity and ease of use. These firewalls can also add many other services, such as cloud management, etc.

Which firewall architecture is best?

When it comes to selecting the best firewall architecture, there is no need to be explicit. It is always better to use a combination of different firewalls to add multiple layers of protection. For example, one can implement a hardware or cloud firewall at the perimeter of the network, and then further add individual software firewall with every network asset.

Besides, the selection usually depends on the requirements of any organization. However, the following factors can be considered for the right selection of firewall:

Size of the organization

If an organization is large and maintains a large internal network, it is better to implement such firewall architecture, which can monitor the entire internal network.

Availability of resources

If an organization has the resources and can afford a separate firewall for each hardware piece, this is a good option. Besides, a cloud firewall may be another consideration.

Requirement of multi-level protection

The number and type of firewalls typically depend on the security measures that an internal network requires. This means, if an organization maintains sensitive data, it is better to implement multi-level protection of firewalls. This will ensure data security from hackers.