Security Issues

Network security techniques, Password and Authentication, VPN, IP Security, security in electronic transaction, Secure Socket Layer(SSL), Secure Shell (SSH)

Network security is any activity designed to protect the usability and integrity of your network and data.

- It includes both hardware and software technologies
- It targets a variety of threats
- It stops them from entering or spreading on your network
- Effective network security manages access to the network

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.

Authentication is the process of verifying the identity of a user or information. User authentication is the process of verifying the identity of a user when that user logs in to a computer system.

There are different types of authentication systems which are: –

1. Single-Factor authentication: – This was the first method of security that was developed. On this authentication system, the user has to enter the username and the password to confirm whether that user is logging in or not. Now if the username or password is wrong, then the user will not be allowed to log in or access the system.

Advantage of the Single-Factor Authentication System: –

- It is a very simple to use and straightforward system.
- it is not at all costly.
- The user does not need any huge technical skills.

The disadvantage of the Single-Factor Authentication

- It is not at all password secure. It will depend on the strength of the password entered by the user.
- The protection level in Single-Factor Authentication is much low.

2. Two-factor Authentication: – In this authentication system, the user has to give a username, password, and other information. There are various types of authentication systems that are used by the user for securing the system. Some of them are: – wireless tokens and virtual tokens. OTP and more.

Advantages of the Two-Factor Authentication

- The Two-Factor Authentication System provides better security than the Single-factor Authentication system.
- The productivity and flexibility increase in the two-factor authentication system.
- Two-Factor Authentication prevents the loss of trust.

Disadvantages of Two-Factor Authentication

- It is time-consuming.

3. Multi-Factor authentication system,: – In this type of authentication, more than one factor of authentication is needed. This gives better security to the user. Any type of keylogger or phishing attack will not be possible in a Multi-Factor Authentication system. This assures the user, that the information will not get stolen from them.

The advantage of the Multi-Factor Authentication System are: –

- No risk of security.

- No information could get stolen.
- No risk of any key-logger activity.
- No risk of any data getting captured.

The disadvantage of the Multi-Factor Authentication System are: –

- It is time-consuming.
- it can rely on third parties. The main objective of authentication is to allow authorized users to access the computer and to deny access to unauthorized users. Operating Systems generally identify/authenticates users using the following 3 ways: Passwords, Physical identification, and Biometrics. These are explained as following below.
    1. **Passwords:** Password verification is the most popular and commonly used authentication technique. A password is a secret text that is supposed to be known only to a user. In a password-based system, each user is assigned a valid username and password by the system administrator. The system stores all usernames and Passwords. When a user logs in, their user name and password are verified by comparing them with the stored login name and password. If the contents are the same then the user is allowed to access the system otherwise it is rejected.
    2. **Physical Identification:** This technique includes machine-readable badges(symbols), cards, or smart cards. In some companies, badges are required for employees to gain access to the organization's gate. In many systems, identification is combined with the use of a password i.e the user must insert the card and then supply his /her password. This kind of authentication is commonly used with ATMs. Smart cards can enhance this scheme by keeping the user password within the card itself. This allows authentication without the storage of passwords in the computer system. The loss of such a card can be dangerous.
    3. **Biometrics:** This method of authentication is based on the unique biological characteristics of each user such as fingerprints, voice or face recognition, signatures, and eyes.
    4. A scanner or other devices to gather the necessary data about the user.
    5. Software to convert the data into a form that can be compared and stored.
    6. A database that stores information for all authorized users.
    7. **Facial Characteristics –** Humans are differentiated on the basis of facial characteristics such as eyes, nose, lips, eyebrows, and chin shape.
    8. **Fingerprints –** Fingerprints are believed to be unique across the entire human population.
    9. **Hand Geometry –** Hand geometry systems identify features of the hand that includes the shape, length, and width of fingers.
    10. **Retinal pattern –** It is concerned with the detailed structure of the eye.
    11. **Signature –** Every individual has a unique style of handwriting, and this feature is reflected in the signatures of a person.
    12. **Voice –** This method records the frequency pattern of the voice of an individual speaker.

What is VPN?

VPN stands for the **Virtual Private Network**. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. A Virtual Private Network is a way to extend a private network using a public network such as the internet. The name only suggests that it is a Virtual "private network" i.e. user can be part of a local network sitting at a remote location. It makes use of tunneling protocols to establish a secure connection.

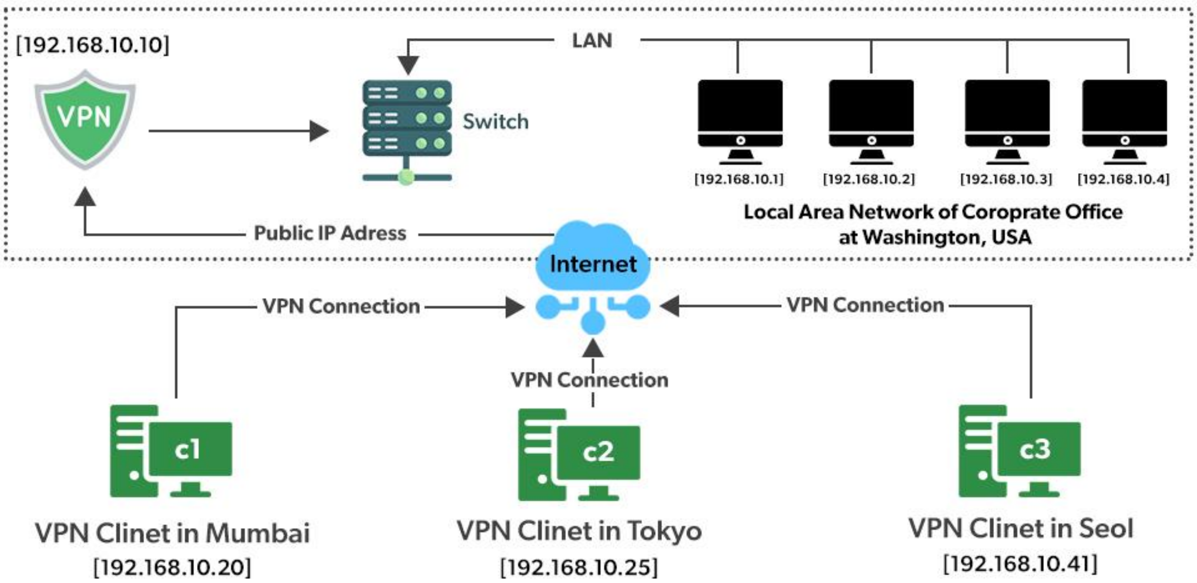
How does a VPN work?

Lets understand VPN by an example:

Think of a situation where corporate office of a bank is situated in Washington, USA. This office has a local network consisting of say 100 computers. Suppose other branches of the bank are in Mumbai, India, and Tokyo, Japan. The traditional method of establishing a secure connection between head office and branch was to have a leased line between the branches and head office which was a very costly as well as troublesome job. VPN lets us overcome this issue in an effective manner.

The situation is described below:

- All 100 hundred computers of the corporate office at Washington are connected to the VPN server(which is a well-configured server containing a public IP address and a switch to connect all computers present in the local network i.e. in US head office).
- The person sitting in the Mumbai office connects to The VPN server using a dial-up window and the VPN server returns an IP address that belongs to the series of IP addresses belonging to a local network of the corporate office.
- Thus person from the Mumbai branch becomes local to the head office and information can be shared securely over the public internet.
- So this is the intuitive way of extending the local network even across the geographical borders of the country.



<u>Understanding IPSec</u>

- **Definition and Purpose Of IPSec** – IPSec is a set of protocols that provide security services for data transmitted over the internet or other public networks. By using cryptographic techniques, IPSec's main goal is to guarantee the confidentiality, integrity, and authenticity of data transmitted between parties in a network.

- **Components of IPSec Such As AH, ESP, And SA** − IPSec has different components that work together to provide secure communication, including Authentication Header (AH), Encapsulating Security Payload (ESP), and Security Associations (SA). AH is responsible for authenticating the source of data by adding a header to each IP packet, ESP encrypts data using symmetric encryption algorithms like AES or 3DES, and SA manages negotiations between communicating devices in securing an encrypted connection.
- **How IPSec Provides Secure Communication** − IPsec provides secure communication by using a combination of authentication and encryption protocols. By doing this, you may be confident that no one else can access or intercept any data that is sent between two devices. Encryption also scrambles data into an unintelligible format so that only authorized users can have access of it.

By implementing strong encryption methods, key management policies, and regularly monitoring for suspicious activity, organizations can maintain a robust security framework to keep their networks safe from threats while ensuring secure communication at all times.

IPsec provides the following security services for traffic at the IP layer:

- Data origin authentication—identifying who sent the data.
- Confidentiality (encryption)—ensuring that the data has not been read en route.
- Connectionless integrity—ensuring the data has not been changed en route.
- Replay protection—detecting packets received more than once to help protect against denial of service attacks.

Secure Sockets Layer (SSL) was the most widely deployed cryptographic protocol to provide security over internet communications before it was succeeded by TLS (Transport Layer Security) in 1999. Despite the deprecation of the SSL protocol and the adoption of TLS in its place, most people still refer to this type of technology as 'SSL'.

SSL provides a secure channel between two machines or devices operating over the internet or an internal network. One common example is when SSL is used to secure communication between a web browser and a web server. This turns a website's address from HTTP to HTTPS, the 'S' standing for 'secure'.

HTTP is insecure and is subject to eavesdropping attacks because the data being transferred from the web browser to the web server or between other endpoints, is transmitted in plaintext. This means attackers can intercept and view sensitive data, such as credit card details and account logins. When data is sent or posted through a browser using HTTPS, SSL ensures that such information is encrypted and secure from interception.

Why Do I Need SSL?

With so much of our day to day transactions and communications happening online, there is very little reason for not using SSL. SSL supports the following information security principles:

- Encryption: protect data transmissions (e.g. browser to server, server to server, application to server, etc.)
- Authentication: ensure the server you're connected to is actually the correct server
- Data integrity: ensure that the data that is requested or submitted is what is actually delivered.

SSL can be used to secure:

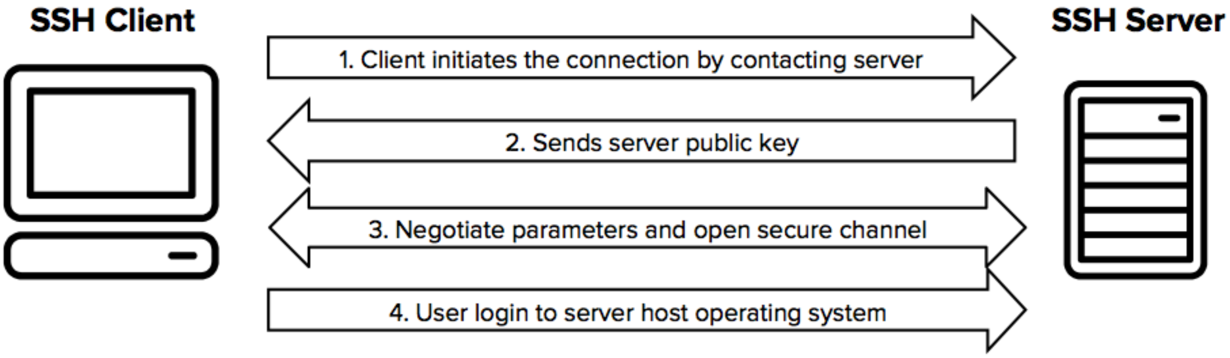
- Online credit card transactions or other online payments.
- Intranet-based traffic, such as internal networks, file sharing, extranets and database connections.
- Webmail servers like Outlook Web Access, Exchange and Office Communications Server.
- The connection between an email client such as Microsoft Outlook and an email server such as Microsoft Exchange.
- The transfer of files over HTTPS and FTP(s) services, such as website owners updating new pages to their websites or transferring large files.
- System logins to applications and control panels like Parallels, cPanel and others.
- Workflow and virtualization applications like Citrix Delivery Platforms or cloud-based computing platforms.

- Hosting control panel logins and activity like Parallels, cPanel and others.

How Do I Get SSL?

To adopt SSL in your business, you should purchase an SSL Certificate.

The Secure Shell (SSH) protocol is a method for securely sending commands to a computer over an unsecured network. SSH uses cryptography to authenticate and encrypt connections between devices. SSH also allows for tunneling, or port forwarding, which is when data packets are able to cross networks that they would not otherwise be able to cross. SSH is often used for controlling servers remotely, for managing infrastructure, and for transferring files.



SSH Client
SSH Server
1. Client initiates the connection by contacting server
2. Sends server public key
3. Negotiate parameters and open secure channel
4. User login to server host operating system