Network Security

Threats and the basics of securing a network

- Network security is continually becoming an area of tremendous focus for companies of all sizes.
- Whether you’re a corporation or a small-to-medium sized business (SMB), you’re a target for a variety of network attacks that can stop your business in its tracks.
- Computer Security means to protect information.
- It deals with prevention and detection of unauthorized actions by users of a computer.

Network Security Threats

- Network security threats fall into two categories

1. Passive threats

(a) Release of message contents

(b) Traffic analysis

2. Active threats

(a) Masquerade

(b) Replay

(c) Modification of message contents

(d) Denial of service

Passive threats

Passive threats, sometimes referred to as eavesdropping dropping, involve attempts by an attacker to obtain information relating to communication.

(a) Release of message contents

- A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information.
- We would like to prevent the opponent from learning the content of these transmissions.

- **Traffic analysis**

- It is a kind of attack done on encrypted messages.
- The opponent might be able to observe the pattern of such encrypted message.
- The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged .

Active threats

involve some modification of the data stream or the creation of a false stream

(a) Masquerade

- **It takes place when one entity pretends to be a different entity.**
- **A masquerade attack usually includes one of the other forms of active attack.**
- **For e.g. authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.**

(b) Replay

- **It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.**

(c) Modification of message

- It means that some position of a message is altered, or that messages are delayed or rendered, to produce an unauthorized effect.

(d) Denial of service (DOS)

A denial of service attack takes place when the availability to a resource is intentionally blocked or degraded by an attacker.

Improve wired network security

- We sometimes focus more on the wireless side of the network when it comes to security because Wi-Fi has no physical fences.
- After all, a war-driver can detect your SSID and launch an attack while sitting out in the parking lot.

- But in a world of insider threats, targeted attacks from outside, as well as hackers who use social engineering to gain physical access to corporate networks, the security of the wired portion of the network should also be top of mind.

Some methods to improve the Wired Network Security

- Perform auditing and mapping
- Keep the network up-to-date
- Physically secure the network
- Consider MAC address filtering
- Implement VLANs to segregate traffic
- Encrypt the entire network

Aadhar based authentication

- Aadhaar Authentication means the process by which the Aadhaar number along with the demographic information or biometric information of a Aadhaar number holder is submitted to the Central Identities Data Repository (CIDR) for its verification and such repository verifies the correctness, or the lack thereof, on the basis of the information available with it.
- The Aadhaar number or the authentication thereof shall not, by itself, confer any right of, or be proof of, citizenship or domicile in respect of an Aadhaar number holder.

- Several requesting entities (or service providers) require individuals to submit their identity proofs that serve as an enabler for providing consumer services, subsidies or benefits. While collecting such identity proofs, these service providers face challenges in verifying/validating the correctness of identity information documents or proofs submitted by individuals.

- The purpose of Aadhaar Authentication is to provide a digital, online identity platform so that the identity of Aadhaar number holders can be validated instantly anytime, anywhere.

Modes of Authentication

Authentication may be carried out through the following modes:

- **Demographic authentication:** The Aadhaar number and demographic information of the Aadhaar number holder obtained from the Aadhaar number holder is matched with the demographic information of the Aadhaar number holder in the CIDR.
- **One-time pin based authentication:** A One Time Pin (OTP), with limited time validity, is sent to the mobile number and/ or e-mail address of the Aadhaar number holder registered with the Authority, or generated by other appropriate means. The Aadhaar number holder shall provide this OTP along with his Aadhaar number during authentication and the same shall be matched with the OTP generated by the Authority.

- **Biometric-based authentication:**

The Aadhaar number and biometric information submitted by an Aadhaar number holder are matched with the biometric information of the said Aadhaar number holder stored in the CIDR. This may be fingerprints-based or iris-based authentication or other biometric modalities based on biometric information stored in the CIDR.

- **Multi-factor authentication:**

A combination of two or more of the above modes may be used for authentication.

Wi-fi security considerations.

- **Use stronger encryption**

Some Wi-Fi access points still offer the older WEP (Wired Equivalent Privacy) standard of protection, but it is fundamentally broken. That means that hackers can break in to a WEP-protected network using a hacking suite like Aircrack-ng in a matter of minutes.

- **Use a secure WPA password**

Make sure that any password (or passphrase) that protects your Wi-Fi network is long and random so it can't be cracked by a determined hacker.

- **Check for rogue Wi-Fi access points**
- Rogue access points present a huge security risk. These aren't your company's "official" Wi-Fi access points, but ones that have been brought in by employees (perhaps because they can't get a good Wi-Fi signal in their office) or conceivably by hackers who have entered your building and surreptitiously connected one to an Ethernet point and hidden it.
- **Hide your network name**

  Hide your SSID for avoid hacking or unauthorized attacks.
- Wi-Fi access points are usually configured by default to broadcast the name of your wireless network - known as the service set identifier, or SSID - to make it easy to find and connect to. But the SSID can be also be set to "hidden" so that you have to know the name of the network before you can connect to it.