Man in the middle (MitM)

Medium is one of the major cyber threats that gets its name from the fact that an attacker inserts themselves between 2 communicating parties. If all communications pass through the attacker en route to their destination, this creates the possibility for the attacker to drop, read, or modify messages before they reach the final destination.

How does it work?

First, they need to insert themselves into the communication in a way that allows them to intercept traffic en route to their destination, some of the ways the attacker could achieve this is:

- Malicious Wi-Fi: All traffic flows through a wireless access point that the attacker controls and can trick users into connecting to it.
- ARP Spoofing: ARP is used to map IP addresses to MAC addresses. By using fake ARP messages, an attacker maps the target's IP address to their MAC address, causing the target's traffic to be sent to them instead.
- DNS Spoofing: DNS maps domain names to IP addresses. Poisoning a DNS cache with fake DNS records can cause traffic to the target domain to be routed to the attacker's IP address.
- BGP Hijacking: BGP is used to identify the autonomous system (AS) with the best route to a particular IP address. This hijacking involves advertising a false route to cause certain traffic to flow through the attacker's systems.

Once in the middle of a communication, the attacker needs to be able to read the messages; however, a large percentage of internet traffic is encrypted using SSL/TLS. If the traffic is encrypted, reading and modifying the messages requires spoofing capability or breaking the SSL/TLS connection.

Examples

Fake Digital Certifications

SSL/TLS are designed to protect against MitM attacks by providing confidentiality, integrity, and authentication to network traffic. However, it relies on the user only accepting digital certificates valid for the particular domain.