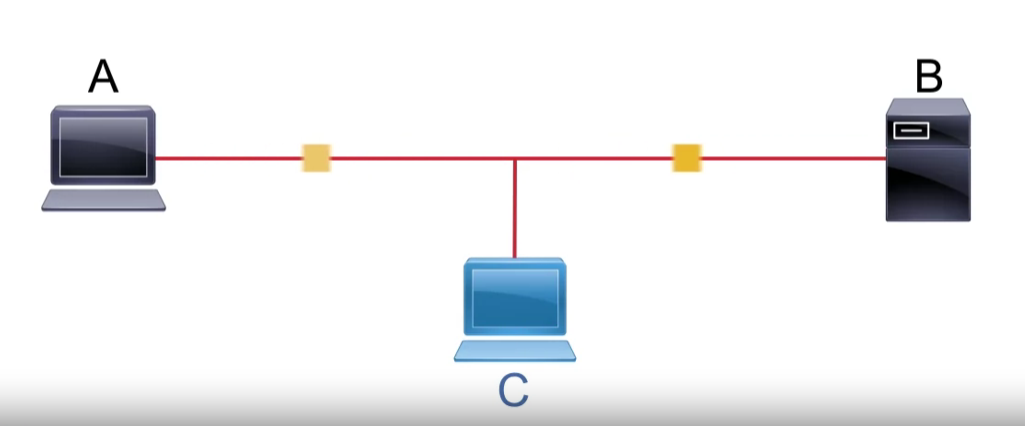
Man in the middle attack

Attacker deflects and relays messages bw 2 parties who falsely think they are communicating with each other directly.

Eg. Telephone tapping is one of the oldest concepts of MITM.

Eavesdropping plays a key role in this type of attack.

Wireless access points with weak security measures pose a major threat in terms of MITM.



Attacker injects itself into a conversation by making host B believe he is host A.

This can be done by spoofing IP and MAC addresses.

Telnet is very susceptible to MITM attacks because data is sent in clear text.

This security concern can be tackled by using SSH instead.

HTTP is also susceptible to MITM attacks because no encryption and no digital signatures.

Instead use HTTPS as it uses SSL for safety and digital certificates.

Common tools used for MITM

Ettercap

Dsniff

Securing against MITM

1. Use VPN which makes sure data is encrypted.
2. Use Digital certificates for authentication.
3. Strong passwords and Multifactor authentication
4. Dynamic ARP inspection
5. IP spoofing detection
6. DHCP snooping

<https://chatgpt.com/c/618b3dc4-cb15-4365-bff9-61dcf176189e>