Man in the Middle Attack

https://blog.cloudflare.com/monsters-in-the-middleboxes/

A man-in-the middle attack is when an intruder monitors your communication. This could be used by someone maliciously to gain information about you.

All crypto systems that use public/private key pairs need to authenticate the sender before accepting the message. This process requires an exchange of information, such as public keys. Some crypto systems also authenticate the receiver, but many do not. TLS uses a Certificate Authority to verify the authenticity of the public key of the server. In order to prevent MITM attacks, the SSL protocol requires both parties authenticate each other.Attestments, such as verbally communicated values, or recorded attestments, such as audio/video recordings of public keys, are used to prevent man-in-the-middle attacks. Visual media is much harder to imitate than simple data packets. This method requires a human being in the loop to successfully initiate the transaction. In a corporate environment, a green padlock doesn't necessarily mean that your client has successfully authenticated with a remote server. Your company may use custom certificates in your clients' web browsers to inspect encrypted traffic. Thus, a green padlock could mean that you've successfully authenticated with the corporate proxy, but not with the remote server.HPKP prevents an attacker from impersonating a website by replacing the original certificate with a forged version. This makes it harder for attackers to perform man-in-the-middle attacks. DNSSEC uses digital signatures to verify the integrity of DNS data. These signatures make it impossible to forge DNS information.

A man-in-the middle attack is when someone intercepts your communication and changes the information you send or receive. In this case, the attacker could be a hacker who wants to steal your personal information. For example, he could try to get your credit card number or social security number.Attackers use malware to compromise routers and steal sensitive data. Victims' traffic is intercepted by attackers who then decrypt the data using decryption keys stolen from the victims.