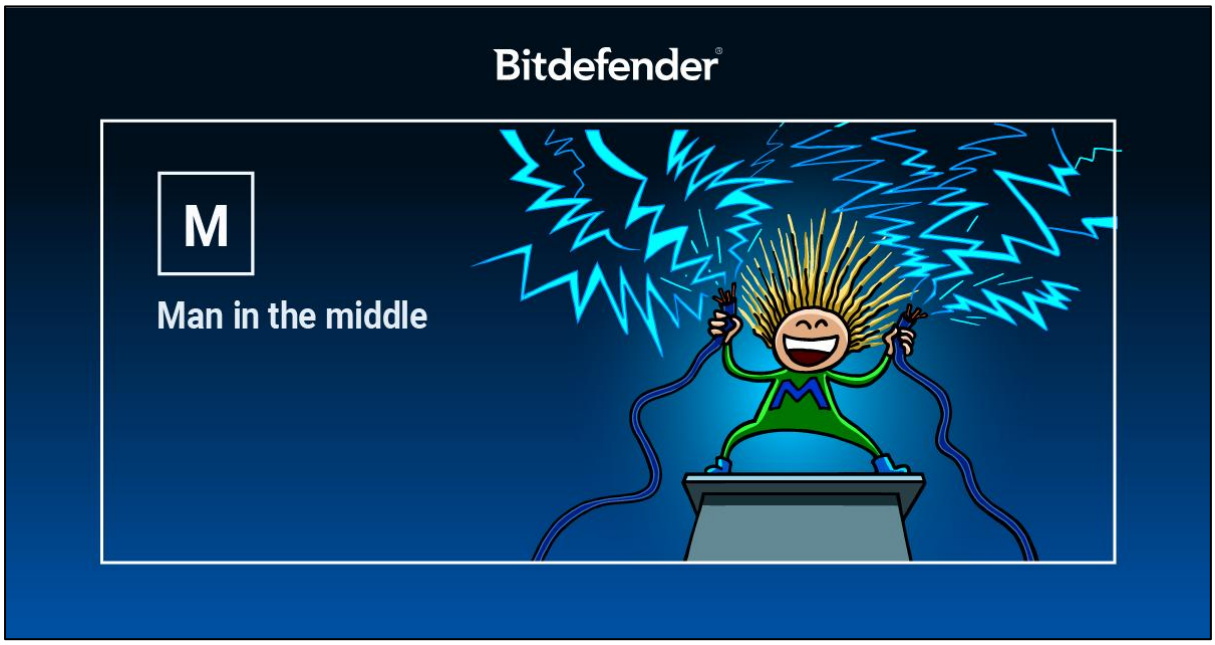
What is a Man-in-the-Middle attack (MiTM)?

While browsing online, you may have noticed that some websites display a small padlock on the left side of the address bar, indicating that the content is secure and that the connection between your browser and the website is encrypted to prevent Man-in-the-Middle attacks (MiTM).

What is a Man-in-the-Middle attack (MiTM)?

When you try to access a webpage, the information travels from the server to your computer via a super-highway of cables, routers, and computer switches that stretch the Internet across the world. Like highway robbers of old, modern attackers know you are vulnerable at every “junction”. These spots are where your data can be intercepted, read, and even altered. A man-in-the-middle attack is a procedure that allows an attacker to interpose between you and the computer you are communicating with to read the conversation or alter it. The procedure was extremely common before the massive switch to HTTP-Secure, and it is still common nowadays, although a little more complicated to carry out.

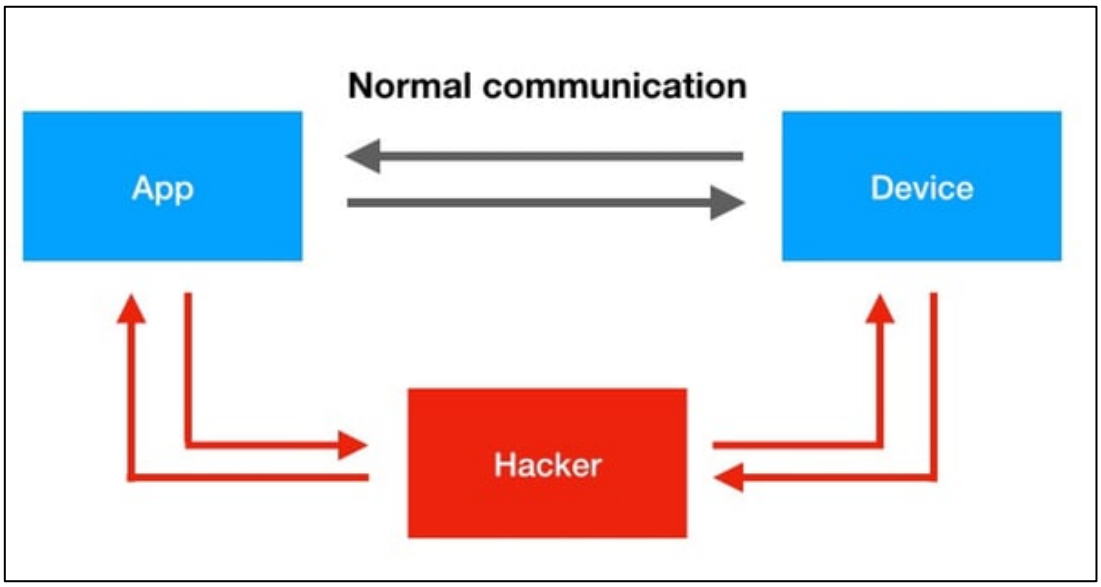


After targeting PCs for years, the omnipresent man-in-the-middle attacks have moved on to mobiles. Because of failing to assess the impact of these attacks, consumers connect their phones to public networks to stay connected, especially when on vacation.

The biggest threat arises from the slow detection rate. Users cannot always figure out if the network they are on is legitimate or if someone is listening to the traffic, whether at the airport, hotel, or coffee place down the street. Our internet addiction has also driven us to use the same device for both business and pleasure, automatically exposing us to risks. End-users are the biggest threat to enterprises. Once connected to an unreliable network, credentials or email could be leaked.

Examples

When two parties start a conversation, they typically establish a connection and exchange what are called public keys – keys used to encrypt conversations before they get sent across the wires. Let's imagine Alice and Bob chatting on the web. When Alice reaches out to Bob, she sends her public key. Bob will encrypt all the messages for Alice with her public key. Bob in turn would also send Alice his public key. When Alice gets the encrypted message from Bob, she decrypts it with her private key and reads it. Now imagine a third person between Alice and Bob. His name is Peter. Peter intercepts Alice's public key as it travels to Bob and substitutes it with his own public key. He also intercepts Bob's public key and substitutes it with his own as it travels to Alice. Now both Alice and Bob encrypt information with Peter's public key and Peter can decrypt them with his own private key. After decryption, he reads the message, maybe alters it, then encrypts it with Alice's public key intercepted in the first step and forwards the message to Alice. He proxies all communication to and from Bob or Alice and neither of them knows he's eavesdropping.



Rogue or unprotected Wi-Fi networks are not the only entry point a hacker can use to launch a man-in-the-middle attack. Each time you go online and use a proxy service to anonymize your IP address or circumvent the restrictions at your workplace, remember that the proxy server normally acts as a man in the middle.

Your page visits and online activity like file transfers, financial transactions, or emails can be captured by cyber criminals through a hostile proxy server. You are exposing all your information to third parties.

VPN servers should safeguard your infrastructure by keeping your connection encrypted. Compromised or rogue VPN servers also could allow third parties to steal your data but, even worse, they can reroute your traffic and use your internet connection for illegal schemes. In the absence of a secure connection, by the time you figure out you have installed a malicious program it could be too late.

MiTM attack prevention

If you are not tech-savvy, there is not much you can do about this. Man-in-the-middle attacks are very difficult to detect, so prevention is better than cure.

If you are on vacation and your phone automatically connects to a network, you could fall victim to a MitM attack. If asked to install a VPN app or accept a digital certificate, you are on your way to a man-in-the-middle attack. The easiest way to identify man-in-the-middle attacks is to check whether the SSL certificate is issued for the entity you are expecting to visit. Ideally, it should have been issued by a legitimate, trustworthy certificate authority. If your browser objects to the validity or legitimacy of a certificate, close the page immediately and ask for help before entering any credentials. You can check the SSL certificate by looking in the upper left corner of your browser to make sure it says HTTPS in green. This means your connection is encrypted and your data hidden.

Because there is no way of properly detecting these attacks, it is better to play safe from the very beginning:

- Make sure the connections are HTTPS and not HTTP.
- Double-check that the SSL certificate is not expired and is issued by a reliable provider.
- Avoid free VPNs and proxies.
- Regularly change passwords and do not reuse them.
- Do not connect to suspicious public networks, be distrustful even when it comes to hotel Wi-Fi, and never install or download anything.
- Use a security solution that can scan HTTPS connections.
- If there is no alternative and you must connect to such a network, avoid making payments and logging in to social media accounts or email accounts.

Now that we gave you the shivers, let’s look at the bright side of man-in-the-middle. Not all MiTM is bad. Such techniques can be used for your own safety. Because more malicious websites and malware are switching to secure HTTPS communication to exfiltrate data and make sure your security solution cannot intercept rogue traffic, some security solutions use SSL proxies – modules that decrypt the SSL / TLS traffic, inspect it for badware then re-encrypt and forward it to the destination. Some parental control solutions also take this road to make sure your child’s encrypted conversations don’t contain something for you to worry about.