Rapid7

By Rapid7

Archived: 2026-04-05 14:11:48 UTC

What is a man-in-the-middle (MITM) attack?

Man-in-the-middle attacks (MITM) are a common type of cybersecurity attack that allows a threat actor to eavesdrop on the communication between two targets—often as part of a broader phishing attack or credential harvesting campaign. The attack takes place in between two legitimately communicating hosts, allowing the attacker to "listen" to a conversation they should normally not be able to listen to, hence the name "man-in-the-middle."

MITM attack analogy

Here's an analogy: Alice and Bob are having a conversation; Eve wants to eavesdrop on the conversation but also remain transparent. Eve could tell Alice that she was Bob and tell Bob that she was Alice.

This would lead Alice to believe she's speaking to Bob, while actually revealing her part of the conversation to Eve. Eve could then gather information from this, alter the response, and pass the message along to Bob (who thinks he's talking to Alice). As a result, Eve is able to transparently hijack their conversation.

Types of man-in-the-middle attacks

Rogue access point

Devices equipped with wireless cards will often try to auto-connect to the access point that is emitting the strongest signal. Attackers can set up their own wireless access point and trick nearby devices to join its domain. All of the victim's network traffic can now be manipulated by the attacker. This is dangerous because the attacker does not even have to be on a trusted network to do this—the attacker simply needs a close enough physical proximity.

ARP spoofing

ARP is the Address Resolution Protocol. It is used to resolve IP addresses to physical MAC (media access control) addresses in a local area network. When a host needs to talk to a host with a given IP address, it references the ARP cache to resolve the IP address to a MAC address. If the address is not known, a request is made asking for the MAC address of the device with the IP address.

An attacker wishing to pose as another host could respond to requests it should not be responding to with its own MAC address. With some precisely placed packets, an attacker can sniff the private traffic between two hosts. Valuable information can be extracted from the traffic, such as the exchange of session tokens, yielding full access to application accounts that the attacker should not be able to access.

mDNS spoofing

Multicast DNS is similar to DNS, but it's done on a local area network (LAN) using broadcast like ARP. This makes it a perfect target for spoofing attacks. The local name resolution system is supposed to make the configuration of network devices extremely simple. Users don't have to know exactly which addresses their devices should be communicating with; they let the system resolve it for them.

Devices such as TVs, printers, and entertainment systems make use of this protocol since they are typically on trusted networks. When an app needs to know the address of a certain device, such as tv.local, an attacker can easily respond to that request with fake data, instructing it to resolve to an address it has control over. Since devices keep a local cache of addresses, the victim will now see the attacker's device as trusted for a duration of time.

DNS spoofing

Similar to the way ARP resolves IP addresses to MAC addresses on a LAN, DNS resolves domain names to IP addresses. When using a DNS spoofing attack, the attacker attempts to introduce corrupt DNS cache information to a host in an attempt to access another host using their domain name, such as www.onlinebanking.com. This leads to the victim sending sensitive information to a malicious host, with the belief they are sending information to a trusted source. An attacker who has already spoofed an IP address could have a much easier time spoofing DNS simply by resolving the address of a DNS server to the attacker's address.

Man-in-the-middle attack techniques

These attack techniques are often used during or after the MITM setup to extract or manipulate sensitive data.

Sniffing

Attackers use packet capture tools to inspect packets at a low level. Using specific wireless devices that are allowed to be put into monitoring or promiscuous mode can allow an attacker to see packets that are not intended for it to see, such as packets addressed to other hosts.

Packet injection

An attacker can also leverage their device's monitoring mode to inject malicious packets into data communication streams. The packets can blend in with valid data communication streams, appearing to be part of the communication, but malicious in nature. Packet injection usually involves first sniffing to determine how and when to craft and send packets.

Session hijacking

Most web applications use a login mechanism that generates a temporary session token to use for future requests to avoid requiring the user to type a password at every page. An attacker can sniff sensitive traffic to identify the session token for a user and use it to make requests as the user. The attacker does not need to spoof once he has a session token.

SSL stripping

Since using HTTPS is a common safeguard against ARP or DNS spoofing, attackers use SSL stripping to intercept packets and alter their HTTPS-based address requests to go to their HTTP equivalent endpoint, forcing the host to make requests to the server unencrypted. Sensitive information can be leaked in plain text.

How to detect a man-in-the-middle attack

Detecting a Man-in-the-middle attack can be difficult without taking the proper steps. If you aren't actively searching to determine if your communications have been intercepted, a Man-in-the-middle attack can potentially go unnoticed until it's too late. Checking for proper page authentication and implementing some sort of tamper detection are typically the key methods to detect a possible attack, but these procedures might require extra forensic analysis after-the-fact.

It's important to take precautionary measures to prevent MITM attacks before they occur, rather than relying on detection during an active attack. Being aware of your browsing habits and recognizing potentially harmful scenarios is essential to maintaining a secure network. Incorporating regular security awareness training can help users identify early warnings signs of MITM tactics like suspicious certificates, misleading redirects, or insecure login prompts. If signs of a MITM attack are detected, having a clearly defined incident response plan is essential to contain the threat, investigate the breach, and restore secure communications.

Below, we have included five of the best practices to prevent MITM attacks from compromising your communications.

Man-in-the-middle (MITM) attack prevention

Strong WEP/WAP encryption on access points

Having a strong encryption mechanism on wireless access points prevents unwanted users from joining your network just by being nearby. A weak encryption mechanism can allow an attacker to brute-force his way into a network and begin man-in-the-middle attacking. The stronger the encryption implementation, the safer.

Strong router login credentials

It’s essential to make sure your default router login is changed. Not just your Wi-Fi password, but your router login credentials. If an attacker finds your router login credentials, they can change your DNS servers to their malicious servers. Or even worse, infect your router with malicious software.

Virtual private network

VPNs can be used to create a secure environment for sensitive information within a local area network. They use key-based encryption to create a subnet for secure communication. This way, even if an attacker happens to get on a network that is shared, he will not be able to decipher the traffic in the VPN.

Force HTTPS

HTTPS can be used to securely communicate over HTTP using public-private key exchange. This prevents an attacker from having any use of the data he may be sniffing. Websites should only use HTTPS and not provide HTTP alternatives. Users can install browser plugins to enforce always using HTTPS on requests.

Public key pair based authentication

Man-in-the-middle attacks typically involve spoofing something or another. Public key pair based authentication like RSA can be used in various layers of the stack to help ensure whether the things you are communicating with are actually the things you want to be communicating with.
