

Man-in-the-Middle (MiTM) Attack

[Return to Glossary](#)

A **Man-in-the-Middle (MiTM) Attack** is one in which the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other. The attack is a type of eavesdropping in which the entire conversation is controlled by the attacker. Sometimes referred to as a session hijacking attack, MiTM has a strong chance of success when the attacker can impersonate each party to the satisfaction of the other. MiTM attacks pose a serious threat to online security because they give the attacker the ability to capture and manipulate sensitive information in real-time.

A common method of executing a MiTM attack involves distributing malware that provides the attacker with access to a user's Web browser and the data it sends and receives during transactions and conversations. Once the attacker has control, he can redirect users to a fake site that looks like the site the user is expecting to reach. The attacker can then create a connection to the real site and act as a proxy in order to read, insert and modify the traffic between the user and the legitimate site. Online banking and e-commerce sites are frequently the targets of MITM attacks so that the attacker can capture login credentials and other sensitive data.

Most cryptographic protocols include some form of endpoint [authentication](#) specifically to prevent MITM attacks. For example, the Transport Layer Security (TLS) protocol can be required to authenticate one or both parties using a mutually trusted certification authority. Unless users take heed of warnings when a suspect certificate is presented, however, a MITM attack can still be carried out with fake or forged certificates.

An attacker can also exploit vulnerabilities in a wireless router's security configuration caused by weak or default passwords. For example, a malicious router, also called an evil twin, can be set up in a public place like a café or hotel to intercept information traveling through the router. Other ways that attackers often carry out man-in-the-middle attacks include [Address Resolution Protocol \(ARP\) Spoofing](#), [Domain Name System \(DNS\) spoofing](#), Spanning Tree Protocol (STP) mangling, port stealing, Dynamic Host Configuration Protocol (DHCP) spoofing, Internet Control Message Protocol (ICMP) redirection, traffic tunneling, and route mangling.

Source: <https://internetofthingsagenda.techtarget.com/definition/man-in-the-middle-attack-MitM>

From:
<https://www.omgwiki.org/dido/> - **DIDO Wiki**

Permanent link:
https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a_glossary:m:mitm&rev=1628181671

Last update: **2021/08/05 12:41**

