# MAN IN THE MIDDLE (MITM) ATTACK

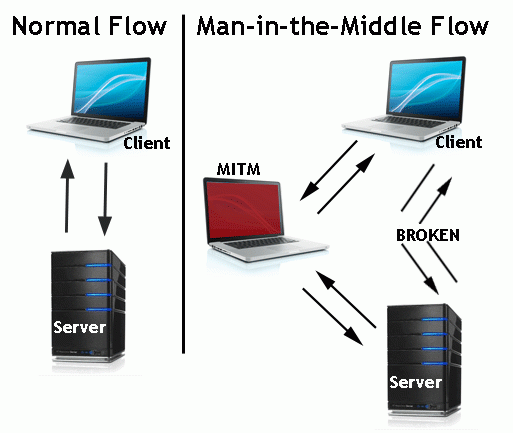
### What Is a Man-in-the-Middle Attack?

A man-in-the-middle attack is a type of cyberattack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. A man-in-the-middle attack allows a malicious actor to intercept, send and receive,modify data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late. Man-in-the-middle attacks can be abbreviated in many ways, including MITM, MitM, MiM or MIM.

### Key Concepts of a Man-in-the-Middle Attack

* Man-in-the-middle is a type of eavesdropping attack that occurs when a malicious actor inserts himself as a relay/proxy into a communication session between people or systems.
* A MITM attack exploits the real-time processing of transactions, conversations or transfer of other data.
* Man-in-the-middle attacks allow attackers to intercept, send and receive data never meant to be for them without either outside party knowing until it is too late.

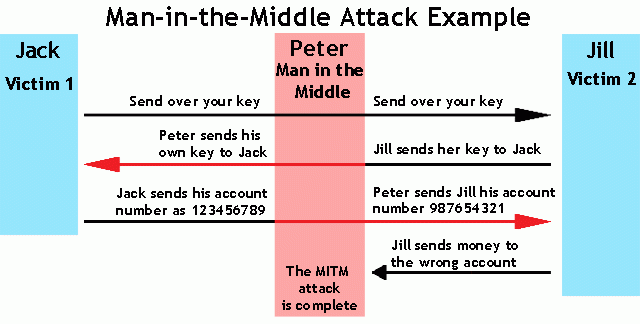
### Man-in-the-Middle Attack Examples



**Man-in-the-Middle Flow**

In the image above, you will notice that the attacker inserted him/herself in-between the flow of traffic between client and server. Now that the attacker has intruded into the communication between the two endpoints, he/she can inject false information and intercept the data transferred between them.

Below is another example of what might happen once the man in the middle has inserted him/herself.



Man-in-the-Middle Example

The hacker is impersonating both sides of the conversation to gain access to funds. This example holds true for a conversation with a client and server as well as person-to-person conversations. In the example above, the attacker intercepts a public key and with that can transpose his own credentials to trick the people on either end into believing they are talking to one another securely.

### Interactions Susceptible to MITM Attacks

* Financial sites – between login and authentication
* Connections meant to be secured by public or private keys
* Other sites that require logins – where there is something to be gained by having access

### Other Forms of Session Hijacking

Man-in-the-middle is a form of session hijacking. Other forms of session hijacking similar to man-in-the-middle are:

* Sidejacking - This attack involves sniffing data packets to steal session cookies and hijack a user’s session. These cookies can contain unencrypted login information, even if the site was secure.
* Evil Twin - This is a rogue Wi-Fi network that appears to be a legitimate network. When users unknowingly join the rogue network, the attacker can launch a man-in-the-middle attack, intercepting all data between you and the network.
* Sniffing - This involves a malicious actor using readily available software to intercept data being sent from, or to, your device.