Man-In-The-Middle Attacks

Prevention And Diagnosis

By Pouya Sattari

2021-2022

Definition

- Man-in-the-Middle (MitM) attacks happen when traffic between two parties is observed or manipulated by an unknown third party.

- A MitM attack is a cybercrime method used to steal personal information or login credentials. Cyber criminals also use MitM attacks as a means to spy on, corrupt information, or disrupt communications between two parties.

Since the 1980s, MitM attacks have been used to infiltrate traffic between innocent parties.

Methods

Man-in-the-Middle attacks can happen in a number of ways:

- Types of Spoofing (IP, DNS, HTTPS)
- Hijacking (Secure Socket Layer, Email)
- Wi-Fi Eavesdropping
- Theft of Browsing Cookies

Man-in-the-Browser:

- When a Man-in-the-Browser attack takes place, the attacker uses a Phishing method in order to administer malware to a device.

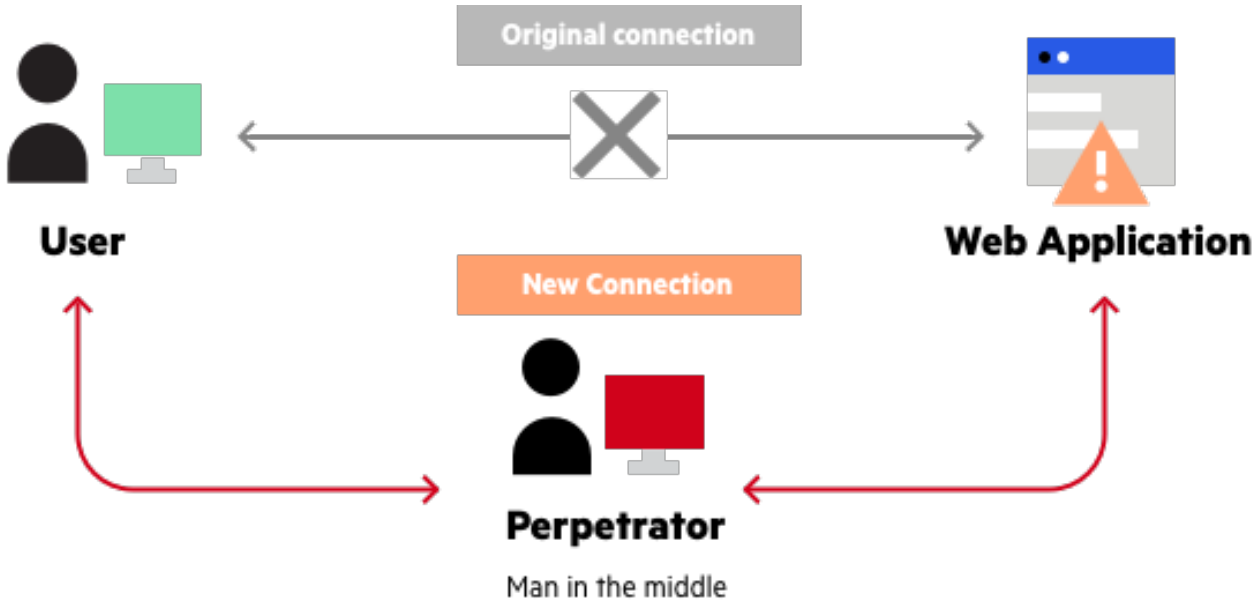
- Malware is software meant to damage a network, server or personal computer.

Phishing is a method of sending fraudulent emails or text messages to trick a user into revealing personal information.

Man-in-the-Browser Continued

- A Man-in-the-Browser attack happens when malware installs itself on a victim’s browser in order to record information sent between targeted websites and the user.
- Online banking institutions are prone to this form of cybercrime.

Example of Man-in-the-Browser

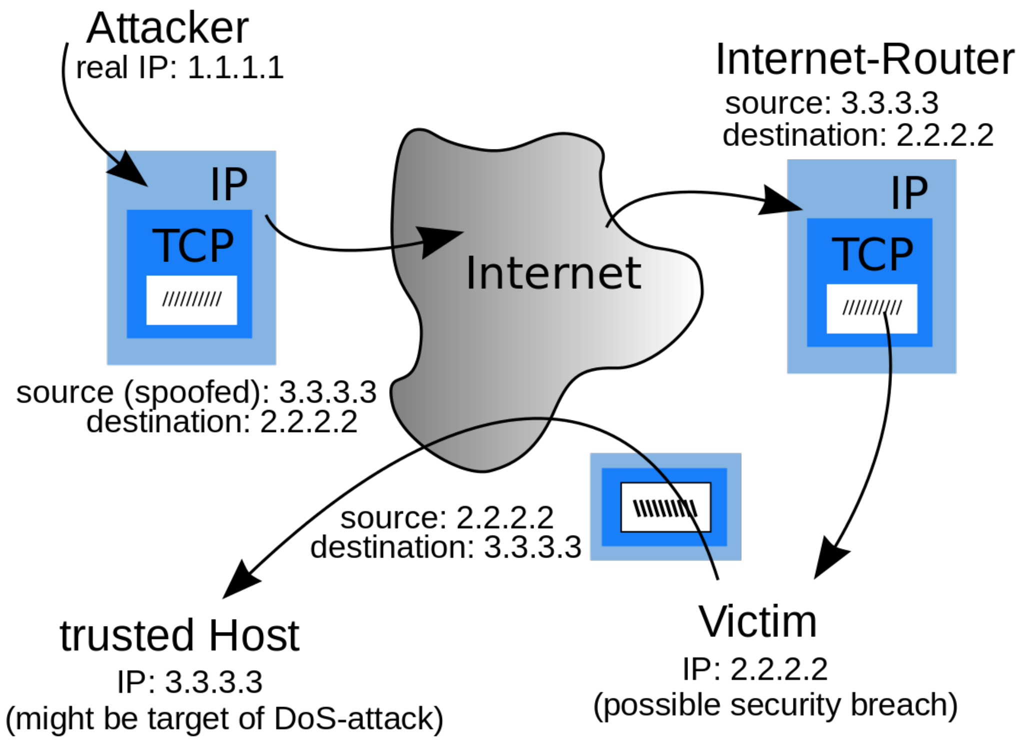


IP Spoofing

- All devices that connect to the internet have an IP Address.
- Spoofing happens when someone or something impersonates a trusted source.
- Attackers use IP Spoofing in order to deceive users into revealing sensitive information by “spoofing” their IP and posing as a website or someone familiar.

An IP Address is like your home address.

Example of IP Spoofing



DNS Spoofing

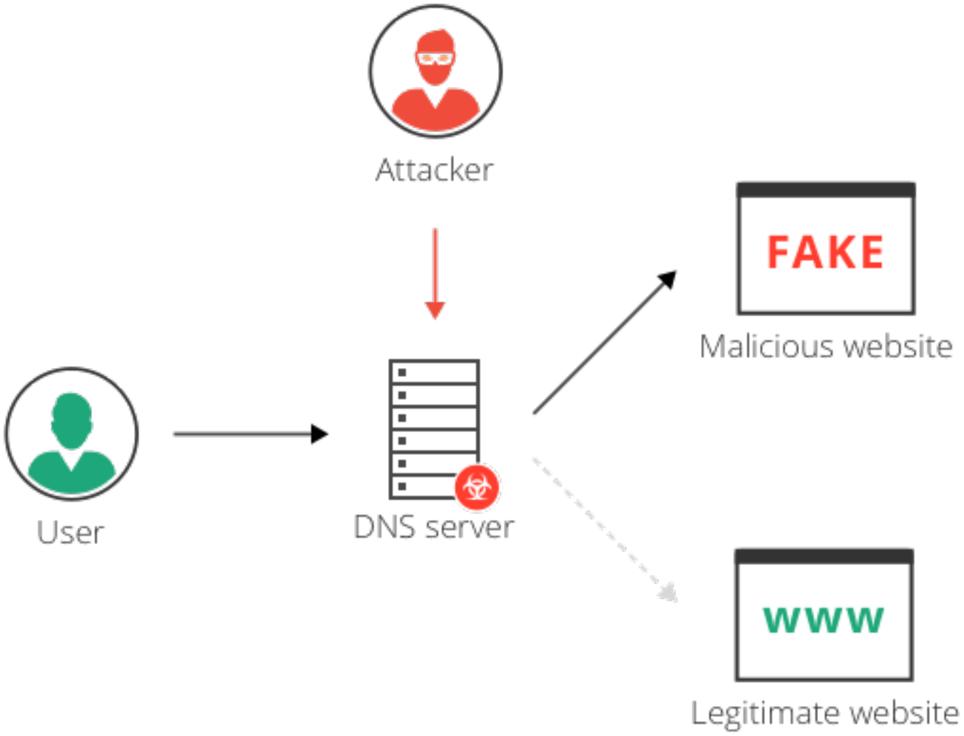
- DNS refers to “Domain Name Server/System”. The DNS system converts names to IP Addresses.

- When Spoofing a DNS, a user is forced to an imitation website, similar to the one intended to be viewed.

- The goal of the attacker is to divert traffic or retrieve login credentials.

Example: The DNS will return the IP address of a visited website when it is typed into a browser.

Example of DNS Spoofing



SSL Hijacking

- SSL stands for Secure Sockets Layer, which was a protocol developed in order to communicate over the internet securely.

- Sometimes when a device visits an unsecure website (http), it is automatically redirected to the secure version (https).

- An attacker utilizes a computer and secure server to reroute information of a user right before connection to a legitimate server, this is SSL Hijacking.

Email Hijacking

- Email Hijacking occurs when attackers target financial organizations for email information.

- After obtaining access to email accounts, attackers can monitor all financial transactions.

- Attackers then follow up by “spoofing” the financial institution’s email and possibly providing users with instructions that would result in the attacker receiving funds.

Wi-fi Eavesdropping

- Wi-Fi connections can be configured and appear to have a valid name, such as the Wi-fi of a favourite coffee shop.

- If a user connects to the fraudulent Wi-Fi connection, the user's online activities can be observed and personal information like banking cards can be attained.

Precautions should be taken when connecting to public Wi-Fi connections.

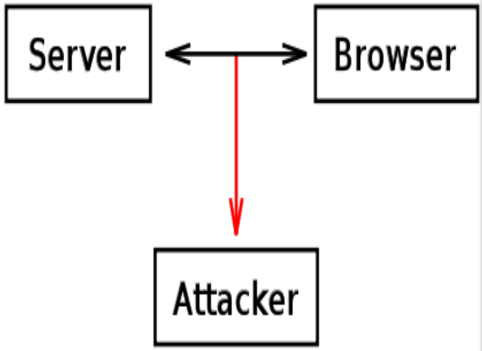
Example of Wi-fi Eavesdropping

Precautions should be taken when connecting to public Wi-Fi connections.

Browser Cookies

- A browser cookie is a small piece of data stored by the user’s web browser. This data is used to track browsing sessions.

- If browsing data is stored in a cookie and the browser cookie is hijacked, cybercriminals may be able to gain passwords, addresses and other sensitive information.



Protection

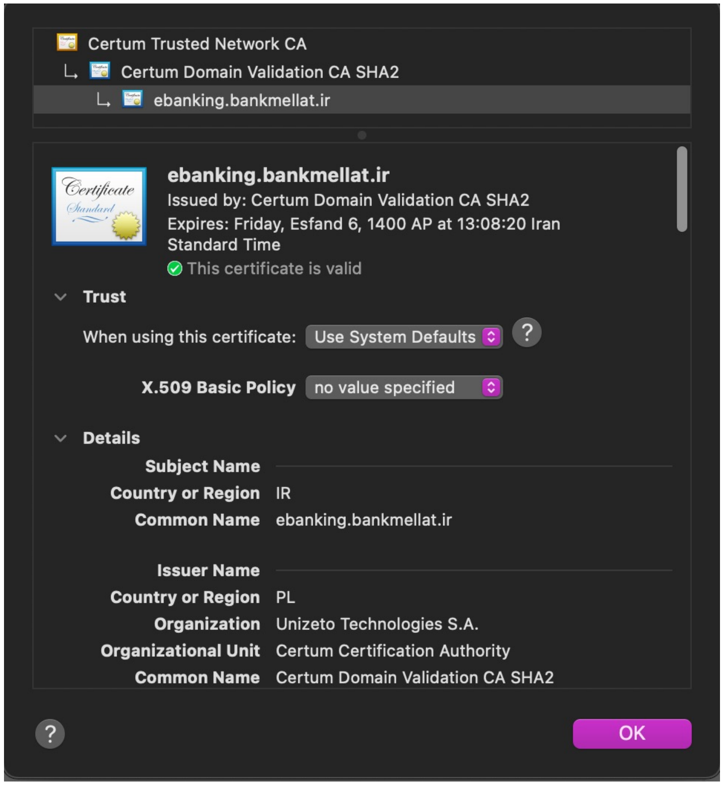
- Ensure that the browser is using “https” when browsing the web.
- Be on alert of Phishing emails that request credentials to be updated.

Protection Continued

- Refrain from connecting to public Wi-Fi connections without a VPN.

- Make use of internet security applications to thwart MitB attacks.

SSL certification



Certum Trusted Network CA
Certum Domain Validation CA SHA2
ebanking.bankmellat.ir

ebanking.bankmellat.ir
Issued by: Certum Domain Validation CA SHA2
Expires: Friday, Esfand 6, 1400 AP at 13:08:20 Iran Standard Time
✓ This certificate is valid

Trust

When using this certificate: Use System Defaults

X.509 Basic Policy no value specified

Details

Subject Name

Country or Region	IR
Common Name	ebanking.bankmellat.ir

Issuer Name

Country or Region	PL
Organization	Unizeto Technologies S.A.
Organizational Unit	Certum Certification Authority
Common Name	Certum Domain Validation CA SHA2