Man-in-the-Middle Attack: Types and Examples

Discover how MITM attacks work, get examples, and how to protect against them.

GLOBAL THREAT LANDSCAPE REPORT 2H 2023

SPEAK WITH AN EXPERT

MITM Definition

Man-in-the-Middle Attack Definition

A man-in-the-middle (MITM) attack is a form of cyberattack in which criminals exploiting weak web-based protocols insert themselves between entities in a communication channel to steal data.

None of the parties sending email, texting, or chatting on a video call are aware that an attacker has inserted their presence into the conversation and that the attacker is stealing their data.

While most cyberattacks are silent and carried out without the victims' knowledge, s
MITM attacks are the opposite. They might include a bot generating believable text

messages, impersonating a person's voice on a call, or spoofing an entire communications system to scrape data the attacker thinks is important from participants' devices.

Types Of Industries And Personas That Are Most Vulnerable To MITM Attacks

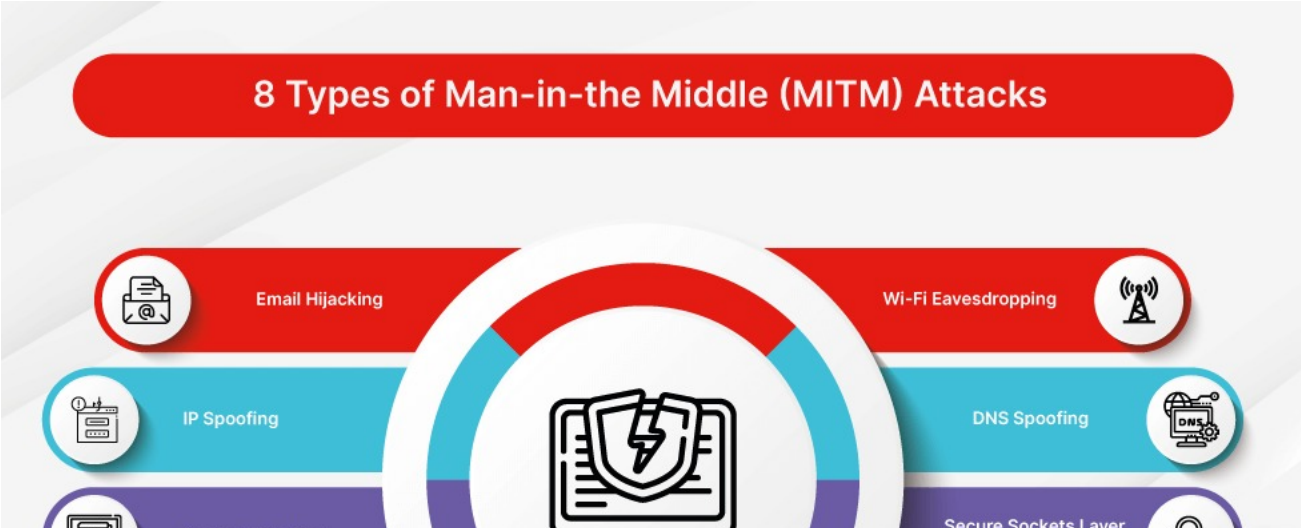
A MITM attack may target any business, organization, or person if there is a perceived chance of financial gain by cyber criminals. The larger the potential financial gain, the more likely the attack.

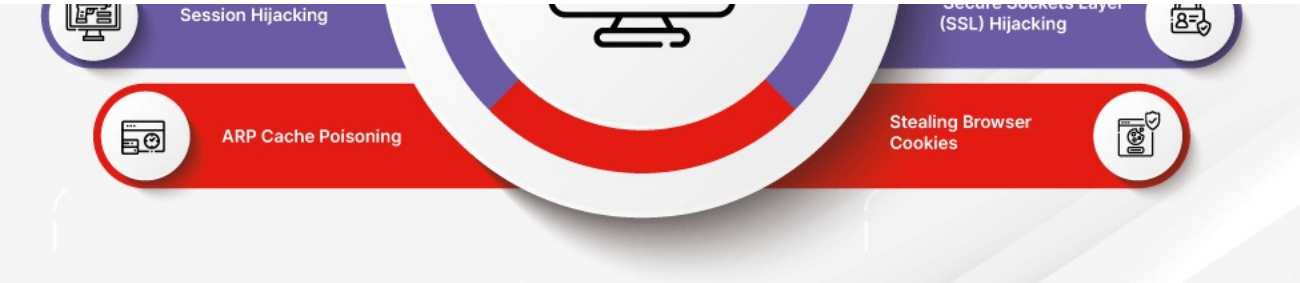
Sales of stolen personal financial or health information may sell for a few dollars per record on the **dark web**. At first glance, that may not sound like much until one realizes that millions of records may be compromised in a single data breach.

Popular industries for MITM attacks include banks and their banking applications, financial companies, health care systems, and businesses that operate industrial networks of devices that connect using the Internet of Things (IoT). Millions of these vulnerable devices are subject to attack in manufacturing, industrial processes, power systems, critical infrastructure, and more.

SCORE and the SBA report that small and midsize business face greater risks, with 43% of all cyberattacks targeting SMBs due to their lack of robust security.

Types of Man-in-the Middle (MITM) Attacks





Click to See Larger Image

1. Email hijacking

As its name implies, in this type of attack, cyber criminals take control of the email accounts of banks, financial institutions, or other trusted companies that have access to sensitive data—and money. Once inside, attackers can monitor transactions and correspondence between the bank and its customers.

In more malicious scenarios, attackers spoof, or fake, the bank's email address and send customers emails instructing them to resend their credentials—or worse, send money—to an account controlled by the attackers. In this MITM attack version, **social engineering**, or building trust with victims, is key for success.

2. Wi-Fi eavesdropping

In Wi-Fi eavesdropping, cyber criminals get victims to connect to a nearby **wireless network** with a legitimate-sounding name. But in reality, the network is set up to engage in malicious activity. The wireless network might appear to be owned by a nearby business the user frequents or it could have a generic-sounding, seemingly harmless name, such as "Free Public Wi-Fi Network." In some cases, the user does not even need to enter a password to connect.

Once victims are connected to the malicious Wi-Fi, the attacker has options: monitor the user's online activity or scrape login credentials, credit or payment card information, and other sensitive data.

To guard against this attack, users should always check what network they are connected to. With mobile phones, they should shut off the Wi-Fi auto-connect feature when moving around locally to prevent their devices from automatically being connected to a malicious network.

3. DNS spoofing

Domain Name System (DNS) spoofing, or DNS cache poisoning, occurs when manipulated DNS records are used to divert legitimate online traffic to a fake or spoofed website built to resemble a website the user would most likely know and trust.

As with all spoofing techniques, attackers prompt users to log in unwittingly to the fake website and convince them that they need to take a specific action, such as pay a fee or transfer money to a specific account. The attackers steal as much data as they can from the victims in the process.

4. Session hijacking

Session hijacking is a type of MITM attack in which the attacker waits for a victim to log in to an application, such as for banking or email, and then steals the session cookie. The attacker then uses the cookie to log in to the same account owned by the victim but instead from the attacker's browser.

A session is a piece of data that identifies a temporary information exchange between two devices or between a computer and a user. Attackers exploit sessions because they are used to identify a user that has logged in to a website. However, attackers need to work quickly as sessions expire after a set amount of time, which could be as short as a few minutes.

5. Secure Sockets Layer (SSL) hijacking

Most websites today display that they are using a secure server. They have "HTTPS," short for Hypertext Transfer Protocol Secure, instead of "HTTP" or Hypertext Transfer Protocol in the first portion of the Uniform Resource Locator (URL) that appears in the browser's address bar. Even when users type in HTTP—or no HTTP at all—the HTTPS or secure version will render in the browser window. This is a standard security protocol, and all data shared with that secure server is protected.

SSL and its successor transport layer security (TLS) are protocols for establishing security between networked computers. In an SSL hijacking, the attacker intercepts all data passing between a server and the user’s computer. This is possible because SSL is an older, vulnerable security protocol that necessitated it to be replaced—version 3.0 was deprecated in June 2015—with the stronger TLS protocol.

5. ARP cache poisoning

The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a media access control (MAC) address, associated with a given internet layer address. The ARP is important because it translates the link layer address to the Internet Protocol (IP) address on the local network.

In this scheme, the victim's computer is tricked with false information from the cyber criminal into thinking that the fraudster's computer is the network gateway. As such, the victim's computer, once connected to the network, essentially sends all of its network traffic to the malicious actor instead of through the real network gateway. The attacker then utilizes this diverted traffic to analyze and steal all the information they need, such as **personally identifiable information (PII)** stored in the browser.

6. IP spoofing

IP spoofing is similar to DNS spoofing in that the attacker diverts internet traffic headed to a legitimate website to a fraudulent website. Instead of spoofing the website's DNS record, the attacker modifies the malicious site's IP address to make it appear as if it is the IP address of the legitimate website users intended to visit.

7. Stealing browser cookies

In computing, a cookie is a small, stored piece of information. A browser cookie, also known as an HTTP cookie, is data collected by a web browser and stored locally on a user's computer. The browser cookie helps websites remember information to enhance the user's browsing experience. For example, with cookies enabled, a user does not have to keep filling out the same items on a form, such as first name and last name.

Stealing browser cookies must be combined with another MITM attack technique, such as Wi-Fi eavesdropping or session hijacking, to be carried out. Cyber criminals can gain access to a user's device using one of the other MITM techniques to steal browser cookies and exploit the full potential of a MITM attack. With access to browser cookies, attackers can gain access to passwords, credit card numbers, and other sensitive information that users regularly store in their browsers.

How Does a Man-in-the-Middle (MITM) Attack Work?

Regardless of the specific techniques or stack of technologies needed to carry out a MITM attack, there is a basic work order:

1. Person A sends Person B a message.
2. The MITM attacker intercepts the message without Person A's or Person B's knowledge.
3. The MITM attacker changes the message content or removes the message altogether, again, without Person A's or Person B's knowledge.

In computing terms, a MITM attack works by exploiting vulnerabilities in network, web, or browser-based security protocols to divert legitimate traffic and steal information from victims.

Examples of Man-In-The-Middle attacks

In 2013, Edward Snowden leaked documents he obtained while working as a consultant at the National Security Administration (NSA). The documents showed that the **NSA pretended to be Google** by intercepting all traffic with the ability to spoof SSL encryption certification. The NSA used this MITM attack to obtain the search records of all Google users, including all Americans, which was illegal domestic spying on U.S. citizens.

Internet Service Provider **Comcast used JavaScript to substitute its ads** for advertisements from third-party websites. This kind of MITM attack is called code injection. The web traffic passing through the Comcast system gave Comcast the ability to inject code and swap out all the ads to change them to Comcast ads or to insert Comcast ads in

otherwise ad-free content.

A famous man-in-the-middle attack example is **Equifax**, one of the three largest credit history reporting companies. The company had a MITM data breach in 2017 which exposed over 100 million customers' financial data to criminals over many months.

A **flaw in a banking app** used by HSBC, NatWest, Co-op, Santander, and Allied Irish Bank allowed criminals to steal personal information and credentials, including passwords and pin codes.

MITM attacks contributed to massive data breaches. The **biggest data breaches in 2021** included Cognyte (five billion records), Twitch (five billion records), LinkedIn (700 million records), and Facebook (553 million records).

MITM issues in mobile apps

Everyone using a mobile device is a potential target. Many apps fail to use **certificate pinning**. Certificate pinning links the SSL encryption certificate to the hostname at the proper destination. This process needs application development inclusion by using known, valid, pinning relationships. It cannot be implemented later if a malicious proxy is already operating because the proxy will spoof the **SSL certificate** with a fake one.

A proxy intercepts the data flow from the sender to the receiver. If it is a malicious proxy, it changes the data without the sender or receiver being aware of what is occurring.

How to detect a Man-in-the Middle (MITM) attack?

Because MITM attacks rely on elements more closely associated with other cyberattacks, such as phishing or spoofing—malicious activities that employees and users may already have been trained to recognize and thwart—MITM attacks might, at first glance, seem easy to spot.

However, given the escalating sophistication of cyber criminals, detection should include a range of protocols, both human and technical. As with all cyber threats, prevention is key.

The following are signs that there might be malicious eavesdroppers on your network and that a MITM attack is underway:

1. **Unusual disconnections**: Unexpected or repeated disconnections from a service—when a user is oddly kicked out of a service and must sign in again and again—are usually a sign of a MITM attempt or attack. Cyber criminals seek as many

opportunities to scrape usernames and passwords, and while having to repeatedly enter a username and password might seem like a minor inconvenience to the user, this is an action MITM attackers need to happen over and over again to be successful.

2. **Strange URLs**: In a spoofing scam, cyber criminals create bogus websites that look identical to recognizable, trusted ones to lure victims into entering their credentials. In the MITM version of this attack, the webpage delivered to the user in their browser is a spoofed site, and the URL in the address window is clearly not the recognizable address of the trusted site or application. MITM attackers use a **DNS hijack** so that users will interact and engage with the spoofed site while malicious code intercepts their messages and collects their data. For any and all personal financial transactions, users should carefully examine the webpages of their financial institutions to determine if something seems unfamiliar.
3. **Public, unsecured Wi-Fi**: Public Wi-Fi available from unfamiliar establishments should be avoided if possible. This is different from municipal Wi-Fi, which is free connectivity offered by cities so residents can connect to the internet. Even if users do not perform banking transactions or other tasks involving sensitive data on a public Wi-Fi, a MITM attack can still send malicious code to a device to eavesdrop on chats and messages. Criminals are known to use innocent-sounding Wi-Fi network names, such as "Local Free Wireless," so beware. Attackers may be offering free connectivity, but they observe all of the user's activity, too.

Impact of Man-In-The-Middle Attacks on enterprises

MITM attacks are serious and require man-in-the-middle attack prevention. Enterprises face increased risks due to business mobility, remote workers, IoT device vulnerability, increased mobile device use, and the danger of using unsecured Wi-Fi connections.

The **2022 Cybersecurity Almanac**, published by Cybercrime Magazine, reported $6 trillion in damage caused by cybercrime in 2021. This figure is expected to reach **$10 trillion annually by 2025**.

MITM attacks collect personal credentials and log-in information. An attack may install a compromised software update containing malware. Unencrypted communication, sent over insecure network connections by mobile devices, is especially vulnerable.

Business News Daily reports that losses from cyber attacks on small businesses average $55,000.

How to Prevent Man-in-the-Middle Attacks?

Sound cybersecurity practices will generally help protect individuals and organizations from MITM attacks.

1. **Update and secure home Wi-Fi routers:** This is perhaps the most important, as work-from-home (WFH) policies usually mandate that employees use a home router to connect to the internet to access the corporate network. **Wi-Fi router software**, known as firmware, should be updated from time to time. This process needs to be carried out manually because firmware updates are not automatic. Also, make sure that the router's security settings are set to the strongest, which according to the Wi-Fi Alliance, is currently **WPA3**.
2. **Use a virtual private network (VPN) when connecting to the internet:** VPNs encrypt the data traveling between the devices and the VPN server. Encrypted traffic is harder to modify.
3. **Use end-to-end encryption:** Where possible, instruct employees to turn on encryption for emails and other communication channels. For added security, only use communications software that offers encryption right out of the box. Some applications automatically turn on encryption in the background—such as **WhatsApp Messenger**, for example. However, if employees wish to *verify* that their messages are indeed encrypted, they will need to carry out a special process, such as scanning and comparing **QR codes** available in the WhatsApp application on each person's phone.
4. **Install patches and use antivirus software:** These might be basic cybersecurity practices, but they are worth mentioning because they are easy to forget. Further, with WFH policies, employees are now responsible for ensuring that all patches are installed and security software is updated on their devices. IT staff may need to explain the importance of this to employees to strengthen endpoint security.
5. **Use strong passwords and a password manager:** Because passwords are not going away anytime soon, encourage employees to use strong passwords and a password manager. For company-owned devices, IT staff can install **mobile device management software** that features a password policy with rules pertaining to password length, complexity (i.e., use of special characters), aging, history/reuse, and the maximum number of password attempts before the device is remotely wiped.
6. **If available, deploy multi-factor authentication (MFA):** So you do not rely on passwords alone, organizations should encourage the use of MFA for access to devices and online services. This practice has quickly become organizations' best defense against threats.
7. **Only connect to secure websites:** This means look for a tiny padlock icon all the way to the left of the website URL in the browser's address bar. It is a sign that the webpage you are visiting is secure and using the HTTPS protocol. For security, employees—and web users overall—should never connect to regular HTTP sites or ones that do not have the padlock icon visible. To ensure this, users can consider installing a free browser plugin that can enforce this rule. Further, most comprehensive cybersecurity platforms include web filtering protocols that restrict employees from accessing non-HTTPS sites. Fortinet provides this with its **FortiGuard Web Filtering service**.
8. **Encrypt DNS traffic:** The DNS is the internet's distributed directory service.

Applications use DNS to resolve a domain name to an IP address. However, when the DNS wants to connect to the external recursive DNS resolver, privacy and security become an issue because the DNS is distributed and no single security protocol exists. The handful of mechanisms that have emerged, including DNS over TLS (DoT) and DNS queries over HTTPS, encrypt DNS traffic between the user's computer and the external DNS resolver to validate the resolver's authenticity using certificates to ensure that no other party can impersonate the resolver.

9. **Adopt the zero-trust philosophy:** Zero trust is a security concept that requires organizations to not automatically trust anything inside or outside its perimeters. Instead, they must first verify anything trying to connect to their systems before granting access. The model is "never trust, always verify," and it relies on continuous verification across every device, user, and application. Zero-trust approaches can prevent a MITM attack from starting or can protect an organization's assets if a MITM attack is already underway.
10. **Deploy a UEBA solution:** User and entity behavior analytics (UEBA) uses machine learning to detect even the tiniest of anomalies in the behavior of both users and devices connected to the corporate network. As cyberattacks become more complex and as threat vectors can appear anywhere, machine learning tools are increasingly used to monitor small changes in behavior that might be suspicious and indicative of a MITM attack. The Fortinet **UEBA solution**, FortiInsight, not only continuously monitors the behavior of all users and endpoints but also employs automation to respond to threats in real time.

Man-in-the-Middle Attacks FAQs

How does a Man-in-the-Middle Attack work?

Do VPNs protect against a Man-in-the-Middle attack?

Does TLS prevent Man-in-the-Middle attacks?

Cybersecurity Resources