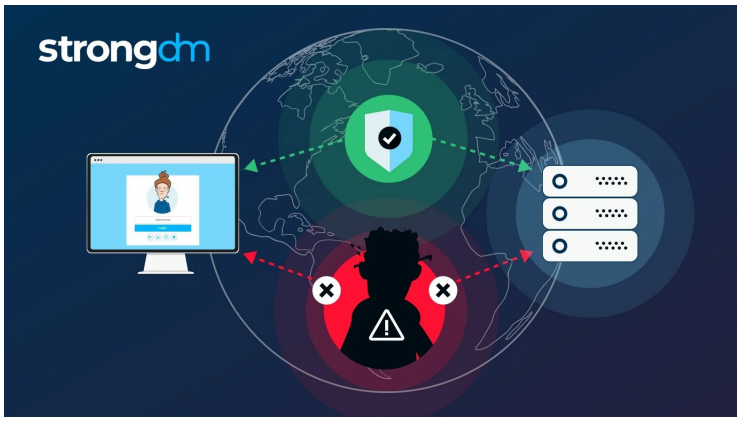
Man-in-the-Middle (MITM) Attack: Definition, Examples & More



Written by John Martinez
Technical Evangelist
StrongDM

Reviewed by Justin McCarthy
Co-founder / CTO
StrongDM

10 min read

Last updated on:
September 30, 2024

Get the Zero Trust eBook PDF

Found in:
Security
Zero Trust

In this article, we go over the **man-in-the-middle attack** definition and discuss the different types of these attacks. We'll take a deep dive into the dangers of man-in-the-middle attacks and address some examples. By the end of this article, you'll have a complete understanding of how a man-in-the-middle attack works and how to detect and prevent one.

What is a Man-in-the-Middle (MITM) Attack?

A man-in-the-middle (MITM) attack is a cyber attack in which a threat actor puts themselves in the middle of two parties, typically a user and an application, to intercept their communications and data exchanges and use them for malicious purposes like making unauthorized purchases or hacking.

By secretly standing between the user and a trusted system, such as a website or application, a cybercriminal can easily obtain sensitive data. The user assumes they're interacting exclusively with a trustworthy site and willingly relinquishes login credentials, financial information, or other compromising data.

Estimates show that 35% of exploitation activity involves man-in-the-middle attacks.

r listen in on the interactions by inserting themselves between a line of
ions or directly impersonate a party through website spoofing for
ttacks. As logins and data entries occur, a hacker can obtain the
someone's identity, access or control a user's account, make purchases
reach a perimeter into an organization's network.

The Danger of Man-in-the-Middle Attacks

Man-in-the-middle attacks offer hackers a path to intercept sensitive information such as usernames, passwords, credit card numbers, and bank account details. It's dangerous because the user has no idea there is another presence between them and the application they're interacting with or that their data is rerouting to a malicious party.

Once a criminal has this information, they can manipulate account credentials, steal funds, or make unauthorized purchases. Because of its scope, MITM attackers often target banking, online retailers, and software-as-a-service (SaaS) platform customers.

> **Nearly 58% of all posts on criminal forums and marketplaces contain banking data of others collected by MITM or other attack types.**

Man-in-the-middle attacks are often used as an initial gateway for long-term advanced persistent threat (APT) campaigns within organizations. By obtaining a user's credentials for specific applications, hackers can penetrate numerous points on the attack surface to make their way into an entire network to mine company data, disrupt production environments, or take over the entire IT infrastructure.

Types of Man-in-the-Middle Attacks

A man-in-the-middle attack in cyber security qualifies as any circumstance where a threat actor places themselves between a user and an entity such as a network, website, or application to obtain information. The method by which hackers obtain that information varies using different forms of spoofing, a method of impersonating trusted online entities or websites. The main types of MITM attacks include:

- **IP Spoofing:** A cybercriminal alters the Internet Protocol (IP) address of a website, email address, or device and spoofs the entity—making the user think they're interacting with a trusted source when they're really passing information to a malicious actor.
- **DNS Spoofing:** For Domain Name System (DNS) spoofing, a spammer creates and operates a fake website that the user is familiar with and routes them to it to acquire user credentials or other information.
- **HTTPS Spoofing:** A user assumes a website has the HyperText Transfer Protocol Secure (HTTPS), meaning they have their computer data encrypted to the website host. However, they were secretly redirected to a non-secure HTTP website, allowing criminals to track interactions and steal information.
- **Email Hijacking:** Attackers secretly gain access to a banking or credit card company's email accounts to monitor transactions and steal information. They might also use the email account or a spoofed email address slightly different from the actual one to provide false instructions to the customers, such as wiring money into a new checking account.
- **Wi-Fi Eavesdropping:** Spammers create public Wi-Fi networks or hotspots that appear to be a nearby business or other trusted source. Users who connect then have all their activity and sensitive data intercepted.
- **SSL Hijacking:** An extension of HTTPS spoofing, hijacking the Secure Sockets Layers (SSL) is when a hacker takes this protocol responsible for encrypting HTTPS connections and intercepts user data traveling between them and the server they're connecting to.
- **Session Hijacking:** Commonly known as browser cookie theft, an attacker will steal information stored on web browser cookies, such as saved passwords.

> **Business email compromise (BEC), an incident that commonly leads to email hijacking, resulted in over $1.8 billion made by scammers in 2020.**

> **3% of all phishing attacks are carried out through malicious websites, assisting in IP, HTTPS, and DNS spoofing attacks.**

Examples of Man-in-the-Middle Attacks

Man-in-the-middle attacks cause significant harm to businesses and their customers. Here are a few real examples of MITM attacks that took some organizations by storm:

Equifax website spoofing compromises millions of users

In 2017, there was a confirmed data breach at Equifax that exposed over 143 million Americans. As a result, Equifax created a website called equifaxsecurity2017.com to let customers see whether the breach impacted them. The issue was that the website used a shared SSL for hosting—with thousands of other websites using the same certificate. DNS (through fake websites) and SSL spoofing took place to redirect users to a phony website or intercept data from the site.

> **2.5 million customers were impacted by the man-in-the-middle attacks, putting the total at 145.5 million for the total incident at Equifax.**

Lenovo machines distributed to customers with adware installed

A 2014 incident occurred when Lenovo distributed computers with Superfish Visual Search adware. This made it possible to create and deploy ads on encrypted web pages and alter SSL certificates to add their own — so attackers could view web activity and login data while someone was browsing on Chrome or Internet Explorer.

> **Security software vendors like Microsoft and McAfee coordinated directly with Lenovo to make software updates just after a few days of discovering the vulnerability to remove Superfish adware.**

Who is at Risk of Man-in-the-Middle Attacks?

Both consumers and businesses can fall victim to MITM incidents in their respective capacities.

Customers who are tricked into connecting to a phony Wi-Fi network, entering a spoofed website, or communicating with a hijacked email account risk having their information tracked, stolen, and used for harm. In particular, users of any website or application that requires a login authentication process or stores financial data make ideal targets.

Alternatively, businesses with interactive websites and software apps that store a lot of customer information could find themselves at high risk. In addition to operation slowdowns from mitigating or responding to a man-in-the-middle attack, the recovery process of handling legal liability issues and rebuilding brand trust makes it essential for firms to allocate resources toward detecting and protecting against a MITM attack.

How Does a Man-in-the-Middle Attack Work?

The man-in-the-middle attack process has a two-stage approach: interception and decryption.

Interception

During the interception step, the cybercriminal attempts to put themselves between the client and server—typically a user and web application. Depending on the type of man-in-the-middle attack, there are a few ways the attacker could approach this:

- Creating a non-secure Wi-Fi network or hotspot in a crowded area for people to connect and view their information.
- Accessing a Wi-Fi network, typically by taking advantage of a weak password or by installing a packet sniffer to analyze traffic and scan for vulnerabilities, points of entry, and ideal targets.
- Creating a fake website with spoofed DNS and routing the user through phishing or redirecting them from the intended HTTPS site.
- Manipulating IP protocols to persuade users to change passwords or log in to an app.

Decryption

After targets are determined and fall for the bait, cybercriminals use data capture tools to transmit any login information and web activity back to them and decrypt it into readable text. During the decryption phase, the intercepted data becomes usable to the criminal.

For example, the cybercriminal will take login credentials captured from the fake website and use them on the actual one. From there, they could change the user's password, steal vital financial information, or use the credentials for longer-term initiatives such as a company network or a more severe attack.

Popular Man-in-the-Middle Attack Tools

Cybercriminals, researchers, and other professionals commonly utilize automation and intelligence tools to target or orchestrate penetration testing in an IT environment. For the most part, MITM software lets users scan networks to find vulnerabilities and potentially weak passwords. Some of the most popular MITM attack software tools include:

- **Ettercap:** Open-source tool for analyzing network protocols, hosts, and activity. Can intercept network traffic data, capture credentials, and decrypt password data.
- **dSniff:** A suite of password and network analysis tools that lets users pull passwords, email contents, and files, intercept network traffic data, and deploy man-in-the-middle attacks using HTTPS redirects.
- **Cain and Abel:** Initially created as a password recovery tool, it developed into a packet sniffing and analysis software to evaluate a network and perform spoofing while also being able to carry out other cyber attacks such as brute force.

How to Detect Man-in-the-Middle Attacks

While man-in-the-middle attack prevention is the ideal scenario, early identification of MITM threats leads to smooth and swift mitigation. Here are a few man-in-the-middle attack symptoms and detection methods:

- **Observing slow or disconnected services:** If a user attempts to log in to an account and keeps getting timed out, that's a possible indication that a spammer is disconnecting the session so they can intercept credentials. The service itself may also be noticeably slow because it is spoofed and, therefore, not configured correctly in the way of an actual website or app.
- **Seeing obscure websites or email addresses:** Small alterations such as a few characters off in the addresses on the website search bar indicate a possible DNS spoof. Additionally, one form of email hijacking is when a spammer uses a domain similar to the one they're impersonating to send and receive messages or deliver commands.
- **Deploying packet inspections:** Packet inspection techniques such as deep packet inspection (DPI) analyze network traffic to find abnormal events such as an outsider scanning vulnerabilities or intercepting traffic data.
- **Connecting to unsecured WiFi or websites:** Without realizing it, a user may find themselves connected to a WiFi network tagged as "unsecure"—a possible MITM attack to lure devices. They also could intend to go to a particular website they know uses HTTPS but be rerouted to a non-secure, HTTP site.

How to Prevent Man-in-the-Middle Attacks

Putting your teams in a proactive position to defend against man-in-the-middle requires a holistic framework incorporating certain best practices and technology into the mix. Here are some preventive controls you can use to protect your users and network:

- **Prioritize HTTPS connections:** Avoid websites with no HTTPS connection indicated in the website address. You can also implement DNS over HTTPS, which encrypts DNS requests, hiding your online activity.
- **Avoid unsecure/public WiFi:** Though it may seem convenient, public WiFi could be a trap used to target users that don't have solid cyber awareness.
- **Incorporate MFA:** Multi-factor authentication (MFA) helps avoid issues you might have after a cybercriminal obtains credentials. Acquiring an additional authentication factor such as a hardware token or face scan prevents the hacker from being able to access an account.
- **Practice network segmentation:** Zero Trust Architecture is an excellent framework for network security, particularly for using principles such as network segmentation to defend against man-in-the-middle attacks. This element of Zero Trust refers to dividing the network into secured segments to isolate incidents and prevent lateral movement by threat actors.
- **Encrypt your emails:** For email hijacking, secure/multipurpose internet mail extensions (S/MIME) encrypt email contents and certify emails with certificates to authenticate senders.
- **Use a certificate management system:** Automated solutions for managing network SSL certificates ensure a centralized and streamlined method for remediating expired ones susceptible to hijacking.

- **Utilize** Privileged Access Management (PAM)**:** Implement privileged access controls to enforce least privilege and restrict account creation and permissions to the minimal level technical staff need to do their job.

MITM Attack Concepts to Know

Some concepts to know to get an easier grasp on a MITM attack include:

- **Spoofing:** Technique commonly used in man-in-the-middle attacks where a trusted system, such as a website or IP address, pretends to be something else through replication or delusion to gain a target's confidence.
- **Hijacking:** Tactics for MITM where an attacker entirely takes control over an email account, website, or SSL to insert themselves between a user and system.
- **Phishing:** Often done through email or on websites, it's a tactic commonly used in MITM attacks where a spammer or criminal attempts to steal information or deliver malware by pretending to be a trusted sender or legitimate website.
- **Eavesdropping:** Part of the MITM attack process where a successful hacker intercepts data transmissions and communications between two users or users and services.

How StrongDM Simplifies MITM Attack Protection

The StrongDM Zero Trust Privileged Access Management (PAM) platform offers a centralized authentication, permission management, and resource visibility solution. Administrators can easily manage their network, applications, and users with top-quality cybersecurity controls specific to man-in-the-middle attacks.

StrongDM helps you prevent and detect MITM attacks through MFA implementation, secure remote access tools, and the use of request signatures that validate the time and payload of client application requests to prevent data interceptions. StrongDM can be used alongside your VPN or replace it altogether. Organizations can also enforce least privilege access based on roles and approvals while continuously collecting data for activity and weblogs.

MITM Attacks: Frequently Asked Questions

Who are the three main participants in a man-in-the-middle attack?

In a man-in-the-middle (MITM) attack, the three main participants are the victim, the entity the victim is communicating with, and the attacker. The victim is typically an unsuspecting user who believes they are securely interacting with a trusted party, such as a website or application. The entity is the legitimate service or system the victim intends to communicate with. The attacker intercepts and manipulates the communication between the victim and the entity, often to steal sensitive information or impersonate one of the parties.

What causes a man-in-the-middle attack?

MITM happens because of an array of system vulnerabilities and incidents such as an unsecure website, email account compromises (EAC), and an uneducated user. When vulnerabilities occur where someone can spoof or hijack an IP address, DNS, SSL, website, or WiFi network, a cybercriminal can put themselves in between the user and the online service they are communicating with to complete the attack.

What is the effect of a man-in-the-middle attack?

Information compromise is the initial effect of successful MITM attacks. Once criminals have the data they need, they can breach user accounts or financially benefit from stealing funds or purchasing items with stolen credit cards. More prolonged-term effects, specifically against organizations, occur when hackers use MITM to penetrate company networks to disrupt or shut down a production environment.

What is the key requirement for a man-in-the-middle attack to be successful?

The key in MITM is properly executing the insertion point between the user and application. This means the cybercriminal must create a trustworthy WiFi network or website, access an email account, or find a way to mask an IP address well enough that the user believes they are interacting with the desired service.

Is man-in-the-middle a DoS attack?

Though not the same, MITM can be used as part of a Denial-of-Service (DoS) attack. DoS floods a network or server with so much false traffic that it shuts down entirely. Someone could use MITM to acquire credentials and breach a network, then deploy DoS from the inside to shut it down.

Does VPN prevent man-in-the-middle?

Yes, but not by itself. VPNs let you connect to the internet from a private and encrypted connection—making your data unreadable to criminals. With a VPN, you'll be able to protect against MITM if the objective is to target internet activity data of a specific user, as seen with WiFi eavesdropping and some forms of HTTPS spoofing. However, you're still vulnerable to MITM once you've entered the site, app, or network.

Protect Against Man-in-the-Middle with StrongDM

In man-in-the-middle attacks, cybercriminals use spoofing, hijacking, or eavesdropping techniques to put themselves between a user and services such as a web application to steal financial information or login credentials. Proper authentication, data encryption, and best practices such as avoiding non-secure WiFi or websites and constantly being aware of potential phishing or system hijacking are the best ways to protect against MITM.

Sign up for our 14-day free trial to see how StrongDM's infrastructure access platform combines authentication, authorization, networking, and observability into a simple solution for finding and defending against man-in-the-middle attacks.

About the Author

John Martinez, Technical Evangelist, has had a long 30+ year career in systems engineering and architecture, but has spent the last 13+ years working on the Cloud, and specifically, Cloud Security. He's currently the Technical Evangelist at StrongDM, taking the message of Zero Trust Privileged Access Management (PAM) to the world. As a practitioner, he architected and created cloud automation, DevOps, and security and compliance solutions at Netflix and Adobe. He worked closely with customers at Evident.io, where he was telling the world about how cloud security should be done at conferences, meetups and customer sessions. Before coming to StrongDM, he lead an innovations and solutions team at Palo Alto Networks, working across many of the company's security products.

You May Also Like

Securing Network Devices with StrongDM's Zero Trust PAM Platform

Let's talk about the unsung heroes of your on-premises infrastructure: network devices. These are the routers, switches, and firewalls that everyone forgets about…and takes for granted—until something breaks. And when one of those somethings breaks, it leads to some pretty bad stuff. If your network goes down, that's bad, bad, bad for business. But if those devices lack the necessary security, well, that can leave you exposed in an incredibly dangerous way.