MAN-IN-THE-MIDDLE ATTACKS: AN INSIDER'S GUIDE

By Brandon Vigliarolo

TechRepublic

INTRODUCTION

Eavesdropping, fraud, and message interception are crimes as old as communication itself. Everything but the information contained in our brains is accessible to other people, and not all those people have your best intentions in mind.

Intercepting and altering communication has happened for centuries, and the advent of the internet made it easier than ever for criminals to inject their interests into private transmissions. These nefarious acts are called man-in-the-middle (MITM) attacks. This type of cybercrime is common, potent, and devastating.

Here's what you need to know about MITM attacks, including how to defend yourself and your organization against them.

WHAT ARE MAN-IN-THE-MIDDLE ATTACKS?

The concept behind a man-in-the-middle attack is simple: intercept traffic coming from one computer and send it to the original recipient without their knowing someone has read, and potentially altered, their traffic.

MITM attacks enable their perpetrator to do things like insert their own cryptocurrency wallet to steal funds, redirect a browser to a malicious website, or passively steal information to be used in later cybercrimes.

Any time a third party intercepts internet traffic, it can be called a MITM attack, and without proper authentication it's incredibly easy for an attacker to do. Public Wi-Fi networks, for example, are a common source of MITM attacks because neither the router nor a connected computer verifies its identity.

In the case of a public Wi-Fi attack, an attacker would need to be nearby and on the same network or have placed a computer on the network capable of sniffing out traffic. Not all MITM attacks require an attacker to have physical proximity to their victim, though—plenty of strains of malware exist that can hijack traffic and inject malicious information wherever an infection spreads.

Combatting MITM attacks requires some form of endpoint authentication, such as TLS or SSL, that uses an authentication key that ideally can't be spoofed. Authentication methods have become stronger, leading to end-to-end encryption of some systems.

Two-factor authentication methods are one example of enhanced security against MITM attacks. Passwords are increasingly unreliable as a way to secure accounts and systems, and by adding a second factor like a hardware key, a software code, or other factor input separately, it becomes harder for attackers to intercept traffic or break encryption. That doesn't mean encryption cracking doesn't happen—hackers often manage to fake certificates and pose as banking websites, login portals, and other sites, which they use to steal information.

MITM attacks are the perfect example of the cybersecurity arms race: As soon as a new form of encryption is broken, organizations come up with a new one, which is in turn broken, repeating the cycle.

Additional resources

- Mobile device security: A guide for business leaders (Tech Pro Research)
- Why router-based attacks could be the next big trend in cybersecurity (TechRepublic)
- China has been 'hijacking the vital internet backbone of western countries' (ZDNet)
- Why 5G (and even 6G) could put your business at risk for a cyberattack (TechRepublic)
- New Wi-Fi attack cracks WPA2 passwords with ease (ZDNet)
- Cheat sheet: How to become a cybersecurity pro (TechRepublic)

WHAT ARE FAMOUS EXAMPLES OF MAN-IN-THE-MIDDLE ATTACKS?

There have been a number of well-known MITM attacks since the advent of the internet, but to paint a picture of just how widespread and powerful MITM attacks are it's important to look back in history to one of the most powerful—which happened well before the invention of the computer: The Babington Plot.

In 1568, supporters of the imprisoned Mary, Queen of Scots, wrote her a letter asking her to support an assassination attempt on Queen Elizabeth I. Mary's reply was intercepted by Elizabeth's agents, who altered the letter to ask for the identities of the conspirators. The conspirators' reply, complete with a list of names, was again intercepted by the men in the middle, leading to the execution of Mary and her co-conspirators.

There are plenty of examples of internet-based MITM attacks as well:

- The US National Security Agency posing as Google was revealed in 2013 when Edward Snowden leaked NSA documents to the public. Using its ability to intercept traffic and spoof SSL certificates, the NSA was able to keep tabs on potentially anyone's Google searches.
- Comcast was caught injecting JavaScript into its web traffic to show its own advertisements in place of those hosted by third-party sites.
- Superfish, an adware program, was found to be scanning SSL traffic and installing certificates that allowed it to intercept and redirect secure traffic.
- A major flaw in banking apps on Android smartphones opened up dozens of apps to MITM attacks.

There are many more examples to pull from, and likely even more attacks that go by unnoticed, but it all comes back to one thing: MITM attacks happen and will keep being attempted for as long as there is an internet.

Additional resources

- How 85% of mobile apps violate security standards (TechRepublic)
- The most interesting Internet-connected vehicle hacks on record (ZDNet)
- New MaMi macOS malware is hijacking DNS settings (TechRepublic)
- Cross-site scripting attacks: A cheat sheet (TechRepublic)
- It's 2018, and network middleware still can't handle TLS without breaking encryption (ZDNet)

WHO IS THE TYPICAL TARGET OF A MAN-IN-THE-MIDDLE ATTACK?

Any person or any organization could be the target of a MITM attack, but most of these crimes have a common theme: financial gain. Banks and banking apps are popular targets for malware-based MITM attacks, as malicious code can wait until it detects traffic to a target site to steal packets, hijack traffic, or otherwise compromise secure connections.

That doesn't mean only finance-related connections are popular targets: Any secure connection that might be compromised for private gain could motivate an attacker. This includes social media accounts, ecommerce site credentials, and confidential databases.

The Internet of Things (IoT) is becoming an increasingly popular target for MITM attacks because of rapid growth of IoT devices has outpaced security. IoT devices also have the potential to deliver a large amount of personally identifying information about individuals and businesses, making hijacking their traffic an appealing prospect for cybercriminals.

Businesses that operate Industrial Internet of Things (IIoT) hardware are at particular risk for MITM attacks because of lax security practices and sensitive proprietary information that IIoT machines have access to. MITM attacks on IIoT systems could cause business downtime, manipulate products to make them weaker or less secure, and steal proprietary information that IIoT machines use in manufacturing.

In short, everyone transmitting sensitive information over the internet is a potential MITM target, though business attacks that could financially benefit hackers or give competitors an edge are a larger threat due to the sheer volume of damage they could do.

Additional resources

- As IoT attacks increase 600% in one year, businesses need to up their security (TechRepublic)
- IoT security warning: Your hacked devices are being used for cybercrime says FBI (ZDNet)
- The challenge IoT poses for enterprises (TechRepublic)
- Five nightmarish attacks that show the risks of IoT security (ZDNet)
- Man-in-the-disk attacks: A cheat sheet (TechRepublic)

WHAT ARE THE TYPES OF MAN-IN-THE-MIDDLE ATTACKS?

Protecting your computers from MITM attacks, whether at home, on the road, or in the office, depends on knowing what you're protecting yourself from. MITM attacks take different forms, target multiple vulnerabilities, and come from a variety of sources. Staying safe requires knowing what kinds of MITM attacks are possible and how to protect against all of them.

These are the various types of man-in-the-middle attacks:

- **Rogue access points** are set up to trick computers that automatically connect to Wi-Fi by posing as legitimate public networks. These rogue networks often monitor traffic and steal sensitive information.
- **Address resolution spoofing** involves a malicious node on a local area network posing as another machine to trick a victim into connecting to it before passing traffic on to the legitimate node.
- **mDNS spoofing** fools network devices into connecting to fake addresses. mDNS is used to match names to addresses on local area networks and when spoofed, to give malicious machines access to vulnerable computers and IoT hardware.
- **DNS spoofing** is commonly used to trick internet users into connecting to fake websites set up to look like real ones. This method is common in online banking fraud and other account hijacking attacks.

Additional resources

- Why your company should consider implementing DNS security extensions (TechRepublic)
- Network security is top IT concern for SMBs, but few have security pros on staff (TechRepublic)
- Firefox add-on snoops on 200,000 users' browsing activities (ZDNet)
- Despite the security measures you've taken, hacking into your network is trivial (TechRepublic)

HOW DO I PREVENT MAN-IN-THE-MIDDLE ATTACKS?

Protecting yourself against these various forms of MITM attacks requires several steps, and each is essential at stopping a particular form of attack:

- Don't allow computers or mobile devices to connect to Wi-Fi networks automatically—make sure you're connecting only to known, trusted Wi-Fi networks.
- Make sure all access points you control are secured and encrypted. Attackers that rely on physical proximity to deploy MITM attacks can be kept off a network by good security.
- If you are connecting to an unknown or public Wi-Fi network, be sure to use a VPN to secure your traffic.
- Never share sensitive information with a website that doesn't use secured HTTP, indicated by a URL that begins with https://.
- Add a second authentication factor to any accounts that allow it.
- Keep an eye out for phishing attempts or any email that requests that you click on a link to log on to a website. If you're unsure of the legitimacy of an email, navigate to the website in question manually and log on without using the email link. If you are still unsure, contact the organization that operates the site to see if it is a legitimate message.
- Make sure operating systems are updated to prevent MITM attacks that exploit system weaknesses.
- Install an up-to-date antivirus application and be sure it's set to scan your computer on a regular basis.

You're never completely secure from a MITM attack or any other kind of cybercrime, but by being vigilant you can greatly reduce your risks and help ensure that you're too tough a target to waste time on.

Additional resources

- IT leader's guide to cyberattack recovery (Tech Pro Research)
- Reducing the risks of BYOD in the enterprise (free PDF) (TechRepublic)
- You've been breached: Eight steps to take within the next 48 hours (free PDF) (TechRepublic)
- Russian hacker warning: How to protect yourself from network attacks (ZDNet)
- How to secure your IoT devices from botnets and other threats (TechRepublic)

CREDITS

Senior Director, B2B Editorial
Jason Hiner

Editor in Chief, UK
Steve Ranger

Senior Managing Editor
Bill Detwiler

Associate Managing Editor
Mary Weilage

Senior Editor
Alison DeNisco Rayome

Editor, Australia
Chris Duckett

Senior Features Editor
Jody Gilbert

Senior Writer
Teena Maddox

Chief Reporter
Nick Heath

Staff Writer
Macy Bayern

Associate Editor
Melanie Wachsman

Multimedia Producer
Derek Poore

Cover image
Image: iStock/utah778

TechRepublic

ABOUT TECHREPUBLIC

TechRepublic is a digital publication and online community that empowers the people of business and technology. It provides analysis, tips, best practices, and case studies aimed at helping leaders make better decisions about technology.

DISCLAIMER

The information contained herein has been obtained from sources believed to be reliable. CBS Interactive Inc. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. CBS Interactive Inc. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.