

# Machine-in-the-Middle Attacks



## What Are They, and How Can We Prevent Them

August 2022

When using the Internet, we expect that our communications are confidential and have not been changed or tampered with in transit. When you enter your password for online banking, you rely on the assumption that a) your password matches the bank's records, b) the bank receives the password in its correct form, and c) third parties cannot see, change, forge or re-use your password. This is a simple example, but in essence, a "machine-in-the-middle attack" (MITM) works by breaking the second and/or third of those assumptions.

A MITM attack can not only disrupt digital communications between humans, but also affect the kinds of machine-to-machine communication that are vital to trust in connected products and Internet services. For example, an IoT device like a virtual assistant typically shares information with a central server hosting content.

If you cannot trust the connections you make to websites and online services, you could be vulnerable to fraud, impersonation, malware, and other risks. If your connected devices and objects cannot communicate securely and reliably, they can put you and your household in physical danger.

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

A MITM attack is one in which a third-party intercepts a communication between users (or machines). MITM attacks usually take two forms. The first is essentially eavesdropping: an adversary passively monitors a conversation or reads the contents of a message; the second – an "active" attack – involves the adversary changing the contents of the message or otherwise modifying the communication (e.g., infecting a victim with malware). The first is an attack on the confidentiality of the communication, the second an attack on its integrity. While some MITM attacks are done without the knowledge of communications service providers, others are designed into the infrastructure of communication services.

In 2013, the media reported<sup>1</sup> that some governments had implemented significant data collection regimes on the Internet using MITM techniques. Adding MITM capabilities to parts of Internet infrastructure, sometimes with the aid of Internet service providers, allowed national security

---

<sup>1</sup> <https://www.amnesty.org/en/latest/news/2013/06/usa-revelations-about-government-surveillance-raise-red-flags/>



agencies to intercept and read bulk Internet traffic. If all traffic had been encrypted, it would have been more difficult for those agencies to access the content. After learning about these surveillance activities, major service providers took steps to encrypt their services, add end-to-end encryption, and turn on encryption by default.

MITM attacks are a real threat to the Internet, regardless of what entity is using them. MITM attacks reduce users' confidence that their communication is private and has not been altered in transit. MITM attacks undermine the trust underpinning the Internet's core functions and reliability.<sup>2</sup>

## Encryption Helps Protect Against MITM Attacks

Encryption is one way people can protect themselves against a MITM attack. It can help prevent the contents of their communications from being read or modified by third parties. For instance, if you send an unencrypted email the contents are visible to every intermediary and network node through which the traffic passes. Unencrypted email is like sending a postcard: the postal worker, anyone at the sorting office, and anyone with access to the recipient's doormat can, if they choose, read the contents.<sup>3</sup>

Encrypting the message protects its confidentiality: it may not prevent an adversary from seeing the contents, but what they read will be incomprehensible, because it has been scrambled.

Using encryption to digitally sign data, a document or a communication, helps ensure that if an adversary manages to modify the content, the tampering will be evident. With most encryption algorithms, changing any piece of the initial message results in a completely different encrypted version of the message. This property can be used to help the recipient check that the original message has not been tampered with, like a seal on an envelope.

Transport Layer Security 1.3 (TLS 1.3) is an important Internet security protocol that provides an added layer of defense against MITM attacks. TLS 1.3 makes forward secrecy<sup>4</sup> mandatory for TLS sessions. This ensures that a separate key is used for each encrypted session, which means that cracking one session key neither gives access to past sessions' encrypted data, nor helps discover subsequent session keys. It means that an adversary has to discover the encryption key specific to each session, increasing the difficulty of MITM attacks.

---

<sup>2</sup> <https://datatracker.ietf.org/doc/rfc7258/>

<sup>3</sup> <https://www.internetsociety.org/resources/doc/2018/encryption-brief/>

<sup>4</sup> <https://blogs.cisco.com/security/tls-1-3-and-forward-secrecy-count-us-in-and-heres-why>



## MITM Attacks to Obtain Access to Encrypted Content

Governments around the world have proposed or implemented, various methods for providing access to encrypted communications or devices for national security or law enforcement purposes. One such method is the MITM attack. Certain kinds of MITM attacks – such as the example below – can even undermine the forward secrecy protection of protocols like TLS 1.3, because they potentially subvert the whole secure key exchange mechanism on which forward secrecy relies.

### Example: A MITM Attack on HTTPS Traffic

According to ZDNet<sup>5</sup>, in 2019 users of Kazakh mobile operators trying to access the Internet received text messages indicating that they must install government-issued root certificates on their mobile and desktop devices. Requiring Internet users to install root certificates that belong to the government could give the government the ability to intercept encrypted HTTPS traffic and perform a MITM attack to break secure communication. This means that the government could monitor, record, and even block interactions between Kazakh users and any website, including banks, email providers, social networks – and critical public services like electricity, hospitals, transportation, and polling. Once these certificates are installed, users have no way of knowing if their communications are no longer secure. Browsers might still show a lock symbol or other indicator that the traffic is “encrypted and secure”, but traffic that appears secure is not. Introducing this weakness undermines the security of the global public key infrastructure and erodes trust in the information and services reached using the Internet.

MITM attacks not only break confidentiality and integrity – but they can also disrupt Internet access. For instance, in 2012 a security agency’s attempted MITM attack in Syria is reported to have broken a core part of the country’s Internet infrastructure, leaving Syrians without access to the global Internet.<sup>6</sup>

## Conclusion

Governments must refrain from using machine-in-the-middle attacks to enable law enforcement access to private communications. Creating these capabilities compromises security for all users and undermines the infrastructure of the Internet. The same methods created for law enforcement can be used as a means of attack, both by authorized users and malicious third parties.<sup>7</sup> MITM attacks present a real threat not only to the trust users have in the confidentiality and integrity of online communications, but to the security and reliability of the global Internet.

---

<sup>5</sup> <https://www.zdnet.com/article/kazakhstan-government-is-now-intercepting-all-https-traffic/>

<sup>6</sup> <https://www.wired.com/2014/08/edward-snowden/>

<sup>7</sup> <https://www.lawfareblog.com/open-letter-qchq-threats-posed-ghost-proposal>



## Additional Information:

[“Keys Under Doormats” – Technical Report, MIT Computer Science and Artificial Intelligence Laboratory, 2015](#)

