Man-in-the-Middle Attacks

What are they, and how can we prevent them?

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 banks records, b) the bank receives the password in its correct form, and c) third parties cannot see, intercept or change your password as it is sent to the bank. This is a simple example, but in essence a "man-in-the-middle attack" (MITM) works by breaking the second and/or third of those assumptions.

A MITM attack can not only disrupt communications between humans, but also affect machine-to-machine communications that are vital to trusted communications on the Internet. 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 security risks such as fraud, impersonation, malware, and others. If your connected devices and objects cannot communicate securely and reliably, they may put you and your household at risk.

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

A MITM attack is one in which a third-party intercepts a communication between users (or machines). Usually this is done covertly, but sometimes the user may be aware. MITM attacks usually take two forms: the first is where an adversary may want to read the contents of a message; the second would involve the adversary changing the contents of the message or otherwise modifying the communication, like infecting a victim with malware. The first is an attack on the **confidentiality** of the message, 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, media reported 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 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 threaten communication confidentiality and reduce user confidence that their communication has not been altered in transit. MITM attacks undermine the trust underpinning the Internet's core functions and reliability.[1]

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 postman, anyone at the sorting office, and anyone with access to the recipient's doormat can, if they choose, read the contents.[2]

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 make sure the original message has not been tampered with, similar to a broken 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 creates mandatory forward secrecy for Internet traffic, ensuring that intercepted traffic cannot be decrypted even if an attacker got a hold of a private key in the future. This is because each session is encrypted with a new session key. It means that an adversary has to discover the encryption keys for every session, vastly increasing the difficulty of MITM attacks.

MITM attacks to obtain access to encrypted content

Governments around the world have proposed, or implemented, various measures to provide access to encrypted communications or devices for national security or law enforcements purposes. One category of such methods is MITM attacks.

Example: A MITM attack on HTTPS traffic

According to Zdnet[3], in 2019 users of Kazakh mobile operators trying to access the Internet received text messages indicating that they need to 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 see, monitor, record, and even block interactions between Kazakh users and any website, including banks, email providers, social networks – and critical public services like electricity, elections, hospitals, and transportation. Once these certificates are installed, users have no way of knowing if their communications are no longer secure. Browsers will 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 Internet and erodes trust in the global public key infrastructure.

1 https://datatracker.ietf.org/doc/rfc7258/

2 https://www.internetsociety.org/resources/doc/2018/encryption-brief/

3 https://www.zdnet.com/article/kazakhstan-government-is-now-intercepting-all-https-traffic/

MITM attacks not only break confidentiality and integrity – they can also disrupt Internet access. For instance, in 2012 a security agency's attempted MITM attack in Syria broke a core part of the country's Internet infrastructure, leaving Syrians without access to the global Internet.[4]

Conclusion

Governments must refrain from using man-in-the-middle attacks to enable law enforcement access to private communications. Creating these capabilities greatly undermines security for all users and the infrastructure of the Internet. Bad actors could use the same methods created for law enforcement to perform their own attacks.[5] 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.

References to learn more:

"Keys Under Doormats" – Technical Report, MIT Computer Science and Artificial Intelligence Laboratory, 2015

4 https://www.wired.com/2014/08/edward-snowden/

5 https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal