

Man-in-the-middle attack

From Wikipedia, the free encyclopedia

In cryptography and computer security, a **man-in-the-middle attack** (often abbreviated **MitM**, **MiM attack**, **MitMA** or the same using all capital letters) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. A man-in-the-middle attack can be used against many cryptographic protocols.^[1] One example of man-in-the-middle attacks is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. This is straightforward in many circumstances; for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point can insert himself as a man-in-the-middle.^[2]

As an attack that aims at circumventing mutual authentication, or lack thereof, a man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to their satisfaction as expected from the legitimate other end. Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. For example, TLS can authenticate one or both parties using a mutually trusted certificate authority.^[3]

Contents

- 1 Example
- 2 Defences against the attack
- 3 Forensic analysis
- 4 Quantum cryptography
- 5 Beyond cryptography
- 6 Implementations
- 7 See also
- 8 References
- 9 External links

Example

Suppose Alice wishes to communicate with Bob. Meanwhile, Mallory wishes to intercept the conversation to eavesdrop and optionally to deliver a false message to Bob.

First, Alice asks Bob for his public key. If Bob sends his public key to Alice, but Mallory is able to intercept it, a man-in-the-middle attack can begin. Mallory sends a forged message to Alice that purports to come from Bob, but instead includes Mallory's public key.

Alice, believing this public key to be Bob's, encrypts her message with Mallory's key and sends the enciphered message back to Bob. Mallory again intercepts, deciphers the message using her private key, possibly alters it if she wants, and re-enciphers it using the public key Bob originally sent to Alice. When Bob receives the newly enciphered message, he believes it came from Alice.

1. Alice sends a message to Bob, which is intercepted by Mallory:

Alice "Hi Bob, it's Alice. Give me your key." →
Mallory Bob

2. Mallory relays this message to Bob; Bob cannot tell it is not really from Alice:

Alice Mallory "Hi Bob, it's Alice. Give me your key." → Bob

3. Bob responds with his encryption key:

Alice Mallory ← [Bob's key] Bob

4. Mallory replaces Bob's key with her own, and relays this to Alice, claiming that it is Bob's key:

Alice ← [Mallory's key] Mallory Bob

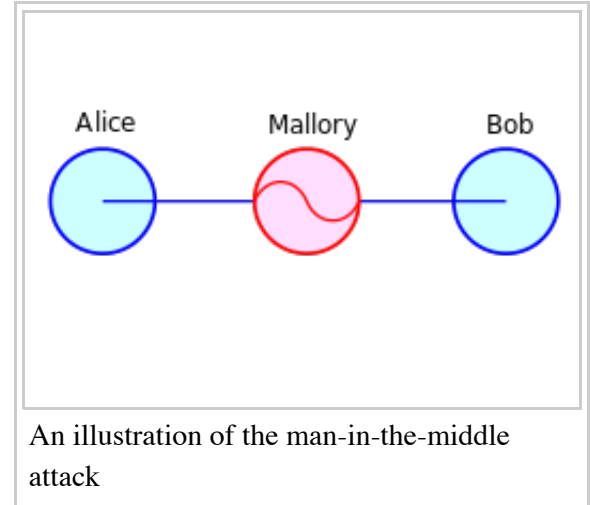
5. Alice encrypts a message with what she believes to be Bob's key, thinking that only Bob can read it:

Alice "Meet me at the bus stop!" [encrypted with Mallory's key] → Mallory Bob

6. However, because it was actually encrypted with Mallory's key, Mallory can decrypt it, read it, modify it (if desired), re-encrypt with Bob's key, and forward it to Bob:

Alice Mallory "Meet me at the van down by the river!" [encrypted with Bob's key] → Bob

7. Bob thinks that this message is a secure communication from Alice.
8. Bob goes to the van down by the river and gets robbed by Mallory.



This example^{[4][5][6]} shows the need for Alice and Bob to have some way to ensure that they are truly using each other's public keys, rather than the public key of an attacker. Otherwise, such attacks are generally possible, in principle, against any message sent using public-key technology. Fortunately, a variety of techniques can help defend against MITM attacks.

Defences against the attack

All cryptographic systems that are secure against MITM attacks require an additional exchange or transmission of information over some kind of secure channel. Many key agreement methods have been developed, with different security requirements for the *secure* channel. Interlock Protocol attempts to address this.

Various defenses against MITM attacks use authentication techniques that include:

- DNSSEC: Secure DNS extensions
- Public key infrastructures: Transport Layer Security is an example of implementing public key infrastructure over Transmission Control Protocol. This is used to prevent Man-in-the-middle attack over a secured HTTP connection on internet. Client and server exchange PKI certificates issued and verified by a common certificate authority.
 - PKI mutual authentication: The main defense in a PKI scenario is mutual authentication. In this case applications from both client and server mutually validate their certificates issued by a common root certificate authority. Virtual private networks do mutual authentication before sending data over the created secure tunnel; however mutual authentication over internet for HTTP connections is seldom enforced.
- Certificate pinning
- A recorded media attestation (assuming that the user's identity can be recognized from the recording), which can either be:
 - A verbal communication of a shared value for each session (as in ZRTP)
 - An audio/visual communication of the public key hash (which can be easily distributed via PKI)^[7]
- Stronger mutual authentication, such as:
 - Secret keys (which are usually high information entropy secrets, and thus more secure), or
 - Passwords (which are usually low information entropy secrets, and thus less secure)
- Latency examination, such as with long cryptographic hash function calculations that lead into tens of seconds; if both parties take 20 seconds normally, and the calculation takes 60 seconds to reach each party, this can indicate a third party
- Second (secure) channel verification
- Testing is being carried out on deleting compromised certificates from issuing authorities on the actual computers and compromised certificates are being exported to sandbox area before removal for analysis
- Quantum Cryptography

The integrity of public keys must generally be assured in some manner, but need not be secret. Passwords and shared secret keys have the additional secrecy requirement. Public keys can be verified by a certificate authority, whose public key is distributed through a secure channel (for example, with a web browser or OS installation). Public keys can also be verified by a web of trust that distributes public keys through a secure channel (for example by face-to-face meetings).

See key-agreement protocol for a classification of protocols that use various forms of keys and passwords to prevent man-in-the-middle attacks.

Forensic analysis

Captured network traffic from what is suspected to be a MITM attack can be analyzed in order to determine if it really was a MITM attack or not. Important evidence to analyze when doing network forensics of a suspected TLS MITM attack include:^[8]

- IP address of the server
- DNS name of the server
- X.509 certificate of the server

- Is the certificate self signed?
- Is the certificate signed by a trusted CA?
- Has the certificate been revoked?
- Has the certificate been changed recently?
- Do other clients, elsewhere on the Internet, also get the same certificate?

Quantum cryptography

Quantum cryptography protocols typically authenticate part or all of their classical communication with an unconditionally secure authentication scheme e.g. Wegman-Carter authentication.^[9]

Beyond cryptography

A notable non-cryptographic man-in-the-middle attack was perpetrated by a Belkin wireless network router in 2003. Periodically, it would take over an HTTP connection being routed through it: this would fail to pass the traffic on to destination, but instead itself respond as the intended server. The reply it sent, in place of the web page the user had requested, was an advertisement for another Belkin product. After an outcry from technically literate users, this 'feature' was removed from later versions of the router's firmware.^[10]

In 2013, the Nokia's Xpress Browser was revealed to be decrypting HTTPS traffic on Nokia's proxy servers, giving the company clear text access to its customers' encrypted browser traffic. Nokia responded by saying that the content was not stored permanently, and that the company had organizational and technical measures to prevent access to private information.^[11]

Implementations

Notable man-in-the-middle attack implementations include the following:


- DSniff – the first public implementation of MITM attacks against SSL and SSH
- Fiddler2 HTTP(S) diagnostic tool
- NSA impersonation of Google^[12]
- Opendium Icen Content-control software, used to perform inspection of HTTPS traffic at the gateway.
- Subterfuge – a framework to launch multiple MITM attacks
- Superfish malware
- Websense Content Gateway – used to perform inspection of SSL traffic at the proxy
- wsniff – a tool for 802.11 HTTP/HTTPS based MITM attacks

See also

- Aspidistra transmitter – a British radio transmitter used for World War II "intrusion" operations, an early man-in-the-middle attack.
- Babington Plot – the plot against Elizabeth I of England, where Francis Walsingham intercepted the correspondence.

- Boy-in-the-browser – a simpler type of web browser MITM
- Computer security – the design of secure computer systems.
- Cryptanalysis – the art of deciphering encrypted messages with incomplete knowledge of how they were encrypted.
- Digital signature – a cryptographic guarantee of the authenticity of a text, usually the result of a calculation only the author is expected to be able to perform.
- Evil Maid Attack – attack used against full disk encryption systems
- Interlock protocol – a specific protocol to circumvent a man-in-the-middle attack when the keys may have been compromised.
- Key management – how to manage cryptographic keys, including generation, exchange and storage.
- Key-agreement protocol – a cryptographic protocol for establishing a key in which both parties can have confidence.
- Man-in-the-browser – a type of web browser MITM
- Mutual authentication – how communicating parties establish confidence in one another's identities.
- Password-authenticated key agreement – a protocol for establishing a key using a password.
- Quantum cryptography – the use of quantum mechanics to provide security in cryptography (while older methods rely on one-way functions).
- Secure channel – a way of communicating resistant to interception and tampering.
- Spoofing attack

References

1. "What is Man in the Middle Attack". internetofthings. Retrieved 27 May 2016.
2. Tanmay Patange (November 10, 2013). "How to defend yourself against MITM or Man-in-the-middle attack".
3. Callegati, Franco; Cerroni, Walter; Ramilli, Marco (2009). "IEEE Xplore - Man-in-the-Middle Attack to the HTTPS Protocol". *ieeexplore.ieee.org*: 78–81. Retrieved 13 April 2016.
4. MiTM on RSA public key encryption (<http://crypto.stackexchange.com/questions/31224/mitm-on-rsa-public-key-encryption>)
5. How Encryption Works (<http://crypto.stackexchange.com/questions/31224/mitm-on-rsa-public-key-encryption>)
6. Public-key cryptography
7. Heinrich, Stuart (2013). "Public Key Infrastructure based on Authentication of Media Attestments". arXiv:1311.7182v1 .
8. "Network Forensic Analysis of SSL MITM Attacks". *NETRESEC Network Security Blog*. Retrieved March 27, 2011.
9. "5. Unconditionally secure authentication". *liu.se*.
10. Leyden, John (2003-11-07). "Help! my Belkin router is spamming me". *The Register*.
11. Meyer, David (10 January 2013). "Nokia: Yes, we decrypt your HTTPS data, but don't worry about it". Gigaom, Inc. Retrieved 13 June 2014.
12. "NSA disguised itself as Google to spy, say reports". CNET. 12 Sep 2013. Retrieved 15 Sep 2013.

External links

- Finding Hidden Threats by Decrypting SSL (<http://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840>)(PDF). SANS Institute.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Man-in-the-middle_attack&oldid=751637563"