

Man-in-the-middle attack

In cryptography and computer security, a **man-in-the-middle attack (MITM)** is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other. One example of a MITM attack 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 wireless access point (Wi-Fi^{[1][2]}) could insert themselves as a man-in-the-middle.^[3]

As an attack that aims at circumventing mutual authentication, or lack thereof, an MITM attack can succeed only when the attacker can impersonate each endpoint to their satisfaction as expected from the legitimate ends. 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.^[2]

Contents

Example

Defense and detection

- Authentication

- Tamper detection

- Forensic analysis

Notable instances

See also

References

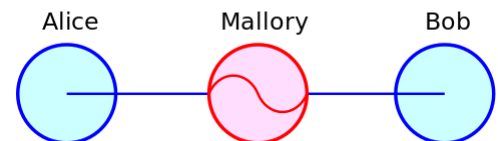
External links

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, an MITM 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



An illustration of the man-in-the-middle attack

alters it if she wants, and re-enciphers it using the public key she intercepted from Bob when he originally tried to send it 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.

This example^{[4][5]} shows the need for Alice and Bob to have some way to ensure that they are truly each 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. A variety of techniques can help defend against MITM attacks.

Defense and detection

MITM attacks can be prevented or detected by two means: authentication and tamper detection. Authentication provides some degree of certainty that a given message has come from a legitimate source. Tamper detection merely shows evidence that a message may have been altered.

Authentication

All cryptographic systems that are secure against MITM attacks provide some method of authentication for messages. Most require an exchange of information (such as public keys) in addition to the message over a secure channel. Such protocols, often using key-agreement protocols, have been developed with different security requirements for the secure channel, though some have attempted to remove the requirement for any secure channel at all.^[6]

A public key infrastructure, such as Transport Layer Security, may harden Transmission Control Protocol against MITM attacks. In such structures, clients and servers exchange certificates which are issued and verified by a trusted third party called a certificate authority (CA). If the original key to authenticate this CA has not been itself the subject of a MITM attack, then the certificates issued by the CA may be used to authenticate the messages sent by the owner of that certificate. Use of mutual authentication, in which both the server and the client validate the other's communication, covers both ends of a MITM attack, though the default behavior of most connections is to only authenticate the server.

Attestments, such as verbal communications of a shared value (as in ZRTP), or recorded attestments such as audio/visual recordings of a public key hash^[7] are used to ward off MITM attacks, as visual media is much more difficult and time-consuming to imitate than simple data packet communication. However, these methods require a human in the loop in order to successfully initiate the transaction.

In a corporate environment, successful authentication (as indicated by the browser's green padlock) does not always imply secure connection with the remote server. Corporate security policies might contemplate the addition of custom certificates in workstation's web browsers in order to be able to inspect encrypted traffic. As a consequence, a green padlock does not indicate that the client has successfully authenticated with the remote server but just with the corporate server/proxy used for SSL/TLS inspection.

HTTP Public Key Pinning (HPKP), sometimes called "certificate pinning," helps prevent a MITM attack in which the certificate authority itself is compromised, by having the server provide a list of "pinned" public key hashes during the first transaction. Subsequent transactions then require one or more of the keys in the list must be used by the server in order to authenticate that transaction.

DNSSEC extends the DNS protocol to use signatures to authenticate DNS records, preventing simple MITM attacks from directing a client to a malicious IP address.

Tamper detection

Latency examination can potentially detect the attack in certain situations,^[8] such as with long calculations that lead into tens of seconds like hash functions. To detect potential attacks, parties check for discrepancies in response times. For example: Say that two parties normally take a certain amount of time to perform a particular transaction. If one transaction, however, were to take an abnormal length of time to reach the other party, this could be indicative of a third party's interference inserting additional latency in the transaction.

Quantum Cryptography, in theory, provides tamper-evidence for transactions through the no-cloning theorem. Protocols based on quantum cryptography typically authenticate part or all of their classical communication with an unconditionally secure authentication scheme e.g. Wegman-Carter authentication.^[9]

Forensic analysis

Captured network traffic from what is suspected to be an attack can be analyzed in order to determine whether or not there was an attack and determine the source of the attack, if any. Important evidence to analyze when performing network forensics on a suspected attack includes:^[10]

- 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?

Notable instances

A notable non-cryptographic MITM 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 responded 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.^[11]

In 2011, a security breach of the Dutch certificate authority DigiNotar resulted in the fraudulent issuing of certificates. Subsequently, the fraudulent certificates were used to perform MITM attacks^[12].

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.^[13]

In 2017, Equifax withdrew its mobile phone apps following concern about MITM vulnerabilities.

Other notable real-life 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^[14]
- Superfish malware
- Forcepoint Content Gateway – used to perform inspection of SSL traffic at the proxy
- Comcast uses MITM attacks to inject JavaScript code to 3rd party web pages, showing their own ads and messages on top of the pages. ^{[15][16][1]}

See also

- ARP spoofing – a technique by which an attacker sends Address Resolution Protocol messages onto a local area network
- Aspidistra transmitter – a British radio transmitter used for World War II "intrusion" operations, an early MITM 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 an MITM 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
- Man-on-the-side attack – a similar attack, giving only regular access to a communication channel.
- 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. "Comcast continues to inject its own code into websites you visit" (<https://thenextweb.com/insights/2017/12/11/comcast-continues-to-inject-its-own-code-into-websites-you-visit/>). 2017-12-11.
2. Callegati, Franco; Cerroni, Walter; Ramilli, Marco (2009). "IEEE Xplore - Man-in-the-Middle Attack to the HTTPS Protocol" (http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4768661). *ieeexplore.ieee.org*: 78–81. Retrieved 13 April 2016.
3. Tanmay Patange (November 10, 2013). "How to defend yourself against MITM or Man-in-the-middle attack" (<http://hackerspace.lifehacker.com/how-to-defend-yourself-against-mitm-or-man-in-the-middle-1461796382>).
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. Merkle, Ralph C (April 1978). "Secure Communications Over Insecure Channels" (<http://dl.acm.org/citation.cfm?id=359473&CFID=457124994&CFTOKEN=90004398>). *Communications of the ACM*. **21** (4): 294–299. CiteSeerX 10.1.1.364.5157 (<https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.364.5157>). doi:10.1145/359460.359473 (<https://doi.org/10.1145%2F359460.359473>). "Received August, 1975; revised September 1977"
7. Heinrich, Stuart (2013). "Public Key Infrastructure based on Authentication of Media Attestments". *arXiv:1311.7182v1* (<https://arxiv.org/abs/1311.7182v1>) [cs.CR (<https://arxiv.org/archive/cs/CR>)].
8. Aziz, Benjamin; Hamilton, Geoff (2009). "Detecting man-in-the-middle attacks by precise timing" (<http://ieeexplore.ieee.org/abstract/document/5211025/>). *2009 Third International Conference on Emerging Security Information, Systems and Technologies*: 81–86. Retrieved 2017-02-25.
9. "5. Unconditionally secure authentication" (http://www.lysator.liu.se/~jc/mthesis/5_Unconditionally_secure_au.html). *liu.se*.
10. "Network Forensic Analysis of SSL MITM Attacks" (<http://www.netresec.com/?page=Blog&month=2011-03&post=Network-Forensic-Analysis-of-SSL-MITM-Attacks>). *NETRESEC Network Security Blog*. Retrieved March 27, 2011.
11. Leyden, John (2003-11-07). "Help! my Belkin router is spamming me" (https://www.theregister.co.uk/2003/11/07/help_my_belkin_router/). *The Register*.
12. Zetter, Kim (2011-09-20). "DigiNotar Files for Bankruptcy in Wake of Devastating Hack" (<https://www.wired.com/2011/09/diginotar-bankruptcy/>). *Wired*. ISSN 1059-1028 (<https://www.worldcat.org/issn/1059-1028>). Retrieved 2019-03-22.
13. Meyer, David (10 January 2013). "Nokia: Yes, we decrypt your HTTPS data, but don't worry about it" (<http://gigaom.com/2013/01/10/nokia-yes-we-decrypt-your-https-data-but-dont-worry-about-it/>). Gigaom, Inc. Retrieved 13 June 2014.
14. "NSA disguised itself as Google to spy, say reports" (http://news.cnet.com/8301-13578_3-57602701-38/nsa-disguised-itself-as-google-to-spy-say-reports/). CNET. 12 Sep 2013. Retrieved 15 Sep 2013.
15. "Comcast using man-in-the-middle attack to warn subscribers of potential copyright infringement" (<https://www.techspot.com/news/62887-comcast-using-man-middle-attack-warn-subscribers-potential.html>).
16. "Comcast still uses MITM javascript injection to serve unwanted ads and messages" (<https://www.privateinternetaccess.com/blog/2016/12/comcast-still-uses-mitm-javascript-injection-serve-unwanted-ads-messages/>). 2016-12-28.

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.
- SSH MITM Penetration Testing Tool (<https://github.com/jtesta/ssh-mitm>)
- | MITM attack guide (<https://texial.net/everything-you-wanna-know-about-mitm-attack>)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Man-in-the-middle_attack&oldid=895152565"

This page was last edited on 2019-05-02, at 18:18:14.

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the [Terms of Use](#) and [Privacy Policy](#). Wikipedia® is a registered trademark of the [Wikimedia](#)

Foundation, Inc., a non-profit organization.