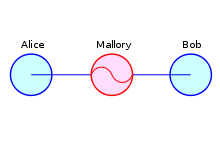
**Attacco man in the middle** (spesso abbreviato in MITM, MIM, MIM attack o MITMA, in italiano *"uomo nel mezzo"*) è una terminologia impiegata nella [crittografia](https://it.wikipedia.org/wiki/Crittografia) e nella [sicurezza informatica](https://it.wikipedia.org/wiki/Sicurezza_informatica) per indicare un [attacco informatico](https://it.wikipedia.org/wiki/Attacco_informatico) in cui qualcuno segretamente ritrasmette o altera la comunicazione tra due parti che credono di comunicare direttamente tra di loro.[[1]](https://it.wikipedia.org/wiki/Attacco_man_in_the_middle#cite_note-1)Un esempio di attacco man in the middle è l'[eavesdropping](https://it.wikipedia.org/wiki/Eavesdropping" \o "Eavesdropping), in cui l'attaccante crea connessioni indipendenti con le vittime e ritrasmette i messaggi per far credere loro che stiano comunicando direttamente tramite una connessione privata, mentre in realtà l'intera conversazione è controllata dal malintenzionato che deve essere in grado di intercettare tutti i messaggi importanti che passano tra le due vittime e iniettarne di nuovi. In molte circostanze questo è semplice, per esempio, un attaccante all'interno di un [WI-FI](https://it.wikipedia.org/wiki/Wi-Fi) [access point](https://it.wikipedia.org/wiki/Access_point) non criptato, può inserire se stesso come *"uomo nel mezzo"*[[2]](https://it.wikipedia.org/wiki/Attacco_man_in_the_middle#cite_note-2).

L'attacco può funzionare solo se nessuna delle due parti è in grado di sapere che il collegamento che li unisce reciprocamente è stato effettivamente compromesso da una terza parte, cosa di cui potrebbero venire a conoscenza comunicando con un canale diverso non compromesso. La maggior parte dei protocolli di crittografia includono una qualche forma di [autenticazione](https://it.wikipedia.org/wiki/Autenticazione) endpoint specificamente per prevenire attacchi MITM. Ad esempio, [TLS](https://it.wikipedia.org/wiki/Transport_Layer_Security) può autenticare una o entrambe le parti utilizzando una [Certificate authority](https://it.wikipedia.org/wiki/Certificate_authority) reciprocamente attendibile

[](https://it.wikipedia.org/wiki/File:Man_in_the_middle_attack.svg)

Rappresentazione dell'attacco *Man in the middle*

Supponiamo che [Alice](https://it.wikipedia.org/wiki/Alice_e_Bob) voglia comunicare con [Bob](https://it.wikipedia.org/wiki/Alice_e_Bob) e che [Mallory](https://it.wikipedia.org/wiki/Alice_e_Bob) voglia spiare la conversazione e, se possibile, consegnare a Bob dei falsi messaggi. Per iniziare, Alice deve chiedere a Bob la sua [chiave pubblica](https://it.wikipedia.org/wiki/Crittografia_asimmetrica). Se Bob invia la sua chiave pubblica ad Alice, ma Mallory è in grado di intercettarla, può iniziare un attacco Man in the middle. Mallory può semplicemente inviare ad Alice una chiave pubblica della quale possiede la corrispondente [chiave privata](https://it.wikipedia.org/wiki/Crittografia_asimmetrica). Alice poi, credendo che questa sia la chiave pubblica di Bob, cifra i suoi messaggi con la chiave di Mallory ed invia i suoi messaggi cifrati a Bob. Mallory quindi li intercetta, li decifra, ne tiene una copia per sé, e li re-cifra (dopo averli alterati se lo desidera) usando la chiave pubblica che Bob aveva originariamente inviato ad Alice. Quando Bob riceverà il messaggio cifrato, crederà che questo provenga direttamente da Alice.

1. Alice invia un messaggio a Bob, il quale viene intercettato da Mallory:

Alice *"Ciao Bob, sono Alice. Dammi la tua chiave."* →     Mallory     Bob

1. Mallory ritrasmette il messaggio a Bob, Bob non può sapere che non si tratta realmente di Alice:

Alice     Mallory *"Ciao Bob, sono Alice. Dammi la tua chiave."* →     Bob

1. Bob risponde con la propria chiave:

Alice     Mallory     ← *[chiave di Bob]* Bob

1. Mallory sostituisce la chiave di Bob con la propria e la ritrasmette ad Alice, sostenendo sia la chiave di Bob:

Alice     ← *[chiave di Mallory]* Mallory     Bob

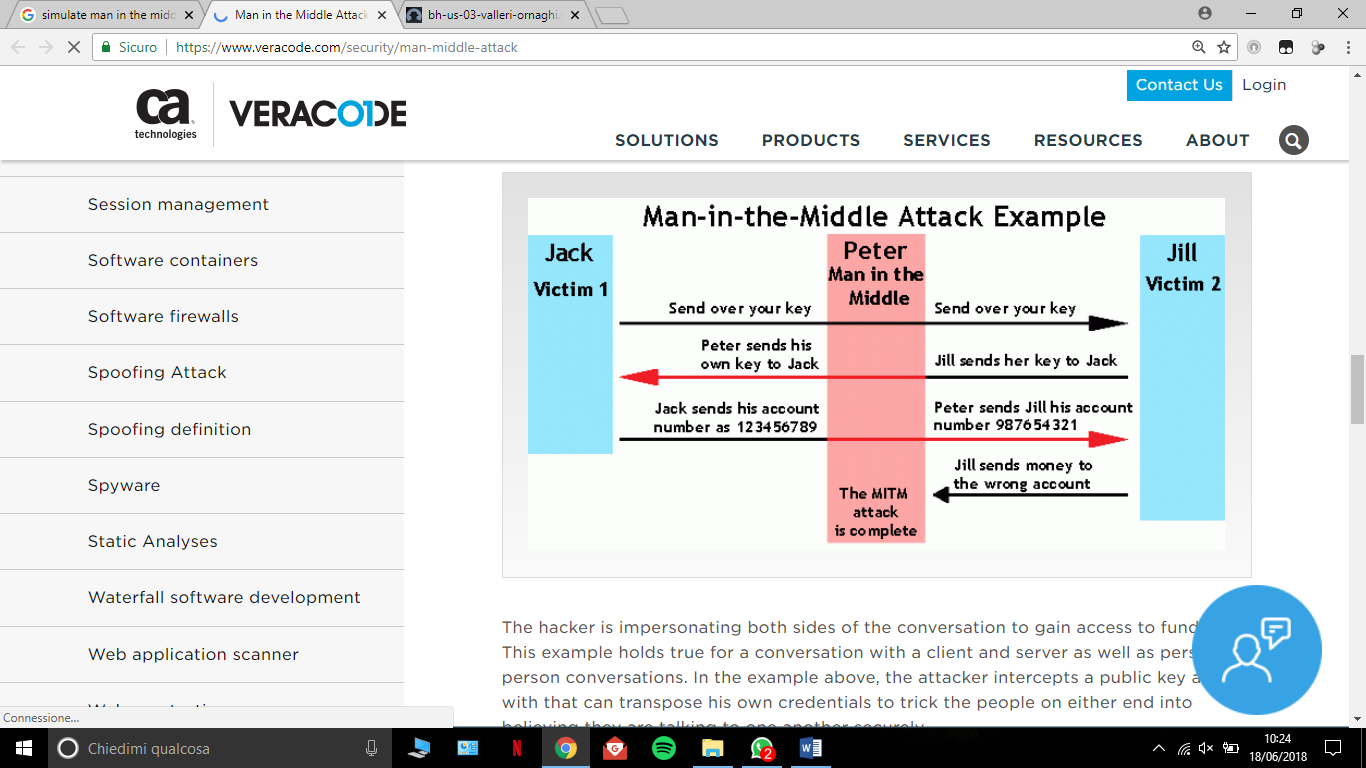
1. Alice cripta un messaggio con quella che crede essere la chiave di Bob, pensando che solo Bob potrà leggerlo:

Alice *"Incontriamoci in piazza!" [criptato con la chiave di Mallory]* →     Mallory     Bob

1. Ora Mallory può decriptare il messaggio, essendo stata usata la sua chiave, leggerlo, modificarlo se lo desidera, criptarlo con la chiave di Bob e infine inviarlo a Bob:

Alice     Mallory *"Incontriamoci in stazione!" [criptato con la chiave di Bob]* →     Bob

1. Bob crede che questo messaggio provenga da una comunicazione sicura con Alice.



Questo esempio[[4]](https://it.wikipedia.org/wiki/Attacco_man_in_the_middle#cite_note-4) mostra la necessità per Alice e Bob di avere un modo per garantire che essi stiano utilizzando le rispettive chiavi pubbliche, piuttosto che quella di un attaccante. Tali attacchi sono generalmente possibili contro ogni comunicazione che utilizzi la tecnologia a **chiave pubblica**. Fortunatamente, esistono una varietà di tecniche per difendersi contro gli attacchi MITM.

<https://www.kaspersky.it/blog/che-cose-un-attacco-man-in-the-middle/706/>

**Che cos’è un attacco Man-in-the-Middle?**

10 Apr 2013

L’obiettivo di molti hacker, a differenza del settore a cui si dedicano, è rubare dati agli utenti. Si può trattare di attacchi circoscritti, indirizzati a singoli utenti, o di un attacco di grandi dimensioni  che ha come obiettivo compromettere un sito web popolare o un data base contenente preziosi dati di tipo finanziario. I metodi possono variare, ma l’obiettivo è lo stesso. In genere, gli hacker cercano di infettare i computer delle vittime con un malware, di quelli che gli permettono di avvicinarsi il più possibile ai dati. Ma se per qualche ragione non fosse possibile, esiste un altro metodo molto popolare, un tipo di attacco noto con il nome di [*man-in-the-middle*](http://it.wikipedia.org/wiki/Attacco_man_in_the_middle). Come il nome stesso suggerisce, si tratta di un attacco in cui un hacker (o un*tool*malevolo) si introduce tra vittima e server (per esempio, un server di una banca online o di posta elettronica). Sono attacchi piuttosto efficaci e abbastanza difficili da individuare, specialmente per quegli utenti che non conoscono questi nuovi tipi di attacchi.

**Definizione di attacco Man-in-the-Middle**

Un attacco [Man-in-the-Middle](https://threatpost.com/en_us/blogs/new-attack-uses-ssltls-information-leak-hijack-https-sessions-090512) (MITM) è piuttosto semplice e non si limita al mondo online o agli home computer. Attraverso questi attacchi (nella loro forma semplice) l’hacker si inserisce tra due entità che stanno cercando di comunicare tra loro, ‘avvelena’ la comunicazione e intercetta i messaggi inviati. L’hacker potrebbe, inoltre, fingersi una delle due parti e ‘avvelenare’ i messaggi. Nel mondo offline, potremmo rendere l’idea con il seguente esempio: qualcuno crea false fatture o pagamenti, le colloca nella cassetta delle lettere della vittima e poi cerca di intercettare il pagamento di tali fatture. Nel mondo online, è un po’ più complesso, ma l’idea è la stessa. L’hacker si inserisce tra il target (la vittima) e la fonte (il server o il router) che la prima sta cercando di contattare. La presenza dell’hacker non è percepita né dalla vittima, né dalla fonte che l’hacker sta personificando.

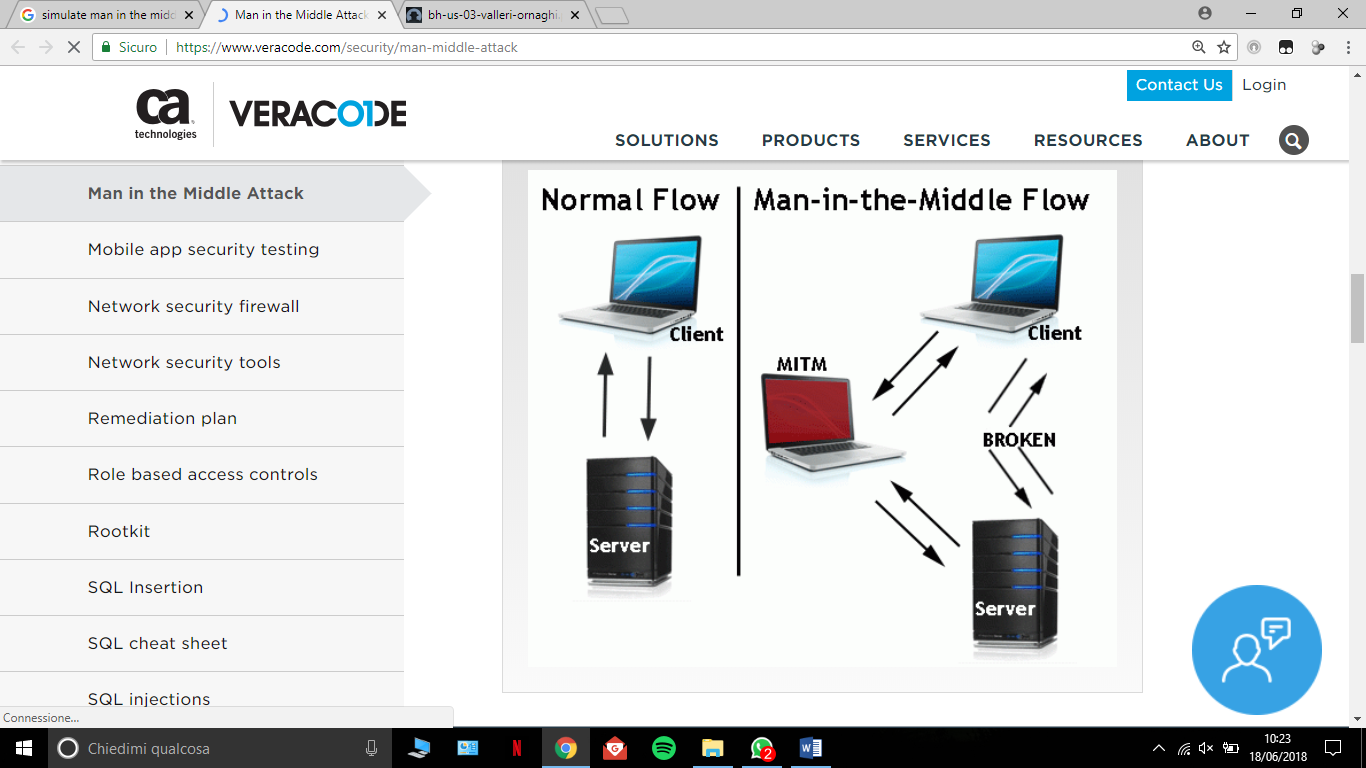
**Tipologie di MITM**

Durante un attacco MITM di tipo comune, un hacker usa una rete Wi-Fi per intercettare le comunicazioni dell’utente. In genere questo funziona ‘avvelenando’ la connessione del router a prima vista ‘sana’, o sfruttando una falla nel setup del router con il fine di intercettare le sessioni degli utenti sul router. In quest’ultimo caso, un hacker potrebbe configurare il dispositivo wireless della vittima, per esempio un portatile,’truccando’ un hotspot Wi-Fi gratuito, dandogli uno di quei nomi comunemente usati nelle aree Wi-Fi pubbliche come aeroporti o caffetterie. In seguito, quando l’utente si connette al ‘falso’ router e cerca di accedere a siti sensibili, come possono essere il sito della sua banca o pagine commerciali, l’hacker identifica una [debolezza nella configurazione o nel sistema di criptografia](https://threatpost.com/en_us/blogs/new-attack-breaks-confidentiality-model-ssl-allows-theft-encrypted-cookies-091911) del router e sfrutta la falla per intercettare la comunicazione tra l’utente e il router. Questo è il caso più complesso, ma è anche il più efficace se l’hacker è in grado di stabilire una comunicazione costante e duratura (ore o giorni) con il router compromesso. Questo gli darebbe la possibilità di spiare silenziosamente le sessioni che la vittima stabilisce con il router, in teoria sicuro (immaginate il caso di una comunicazione con il server della posta elettronica aziendale) e rubare un grande quantità di dati sensibili.

Una variante recente di MITM è l’attacco conosciuto con il nome di *man-in-the-browser*. In questo caso, l’hacker usa diversi metodi attraverso i quali ‘pianta’ un codice malware nel computer di una vittima, codici che agiscono all’interno del browser. Il malware è poi in grado di registrare i dati scambiati tra il browser e i siti target in cui l’hacker ha inserito il codice malware. Questo tipo di attacco è diventato abbastanza popolare negli ultimi anni perché permette all’hacker di colpire varie vittime allo stesso tempo e il colpo può essere realizzato in modalità remota.

**Metodi di difesa**

Ci sono vari metodi per difendersi dagli attacchi MITM. Tuttavia quasi tutti gli attacchi sono diretti ai router e ai server e questo impedisce agli utenti di controllare in prima persona la sicurezza delle transazioni. Tuttavia qualcosa possiamo fare. Per esempio, possiamo usare un programma di crittografia efficace che agisca tra client e server. Grazie a questi programmi, il server può autenticarsi presentando un certificato digitale e il client e il server possono stabilire un canale criptato attraverso il quale inviare dati sensibili. Ma è importante che la crittografia sia abilitata sul server. Un’altra possibilità è evitare in toto le connessioni Wi-Fi gratuite o utilizzare un plug-in per browser come [HTTPS Everywhere](https://www.eff.org/https-everywhere) o [ForceTLS](http://forcetls.sidstamm.com/) in grado di stabilire connessioni sicure. Ad ogni modo, questi metodi di difesa hanno dei limiti e si sono registrati casi di attacchi come [SSLStrip](https://threatpost.com/en_us/blogs/how-render-ssl-useless-081810) o SSLSniff che mettono in dubbio la sicurezza delle connessioni SSL.



Simulation test su ubuntu

1)

<http://www.ayomaonline.com/security/man-in-the-middle-attack-lab-setup-with-virtualbox/>

2)

<https://null-byte.wonderhowto.com/how-to/hack-like-pro-conduct-simple-man-middle-attack-0147291/>