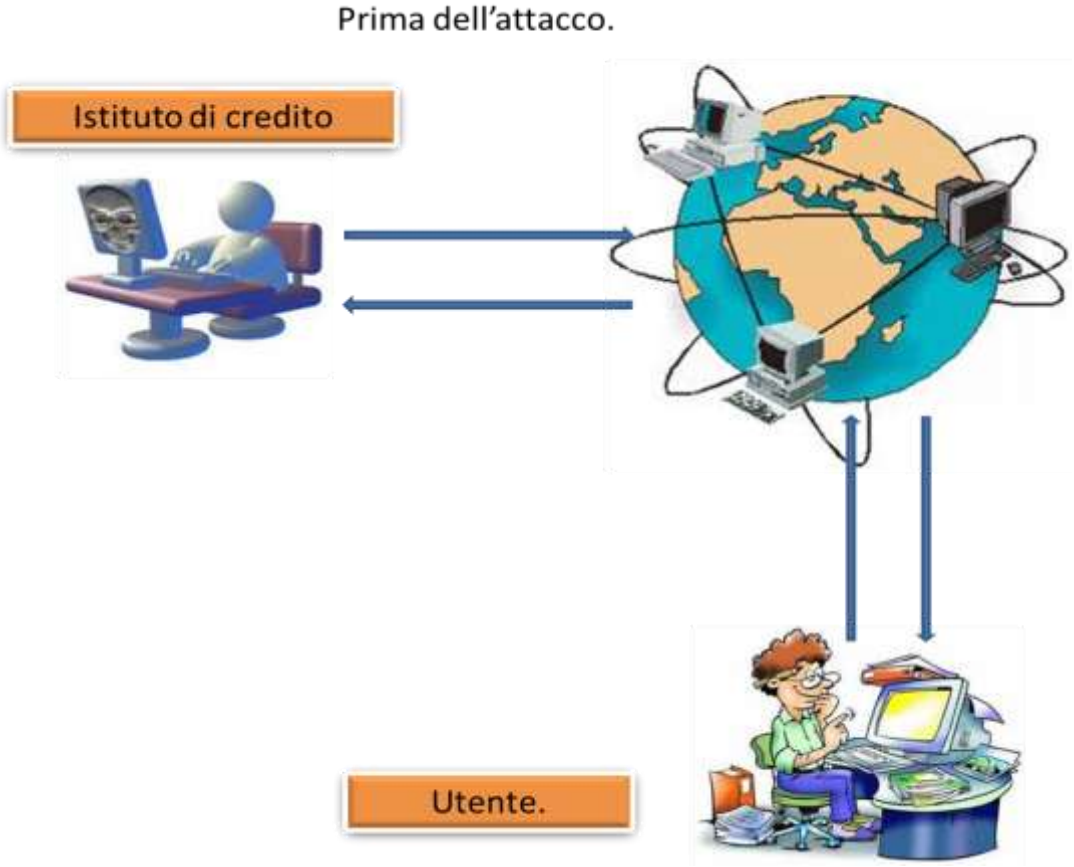
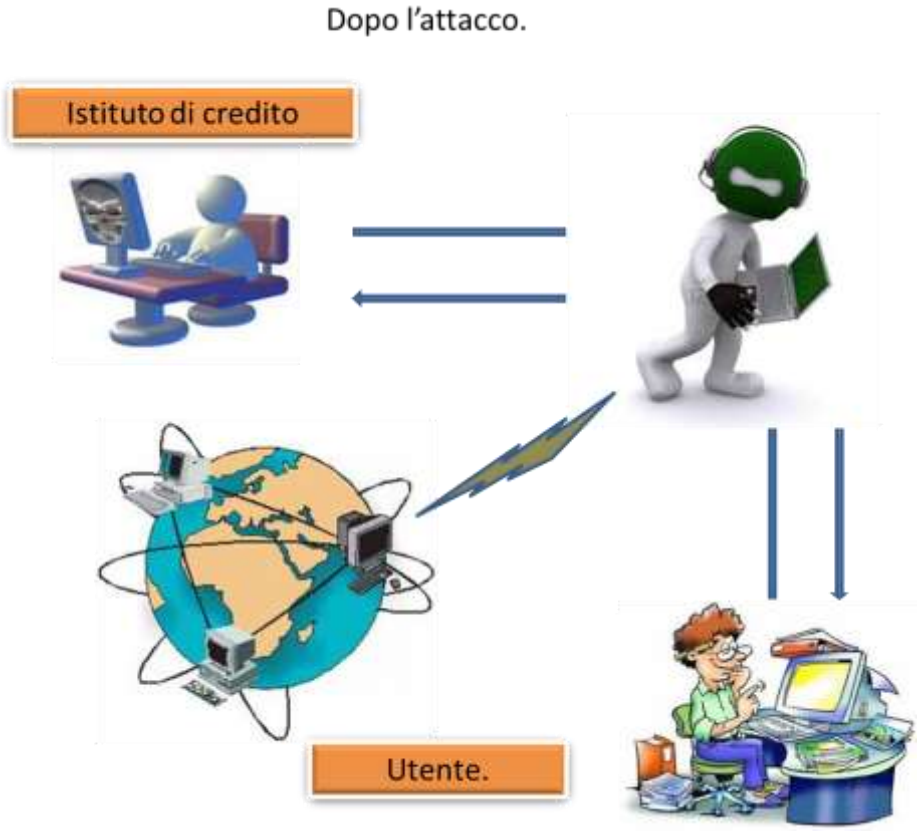
## Lesson 1: MitM "Man In The Middle"

Iniziamo con il definire quando e perché si configura un attacco avente le caratteristiche del "Man In The Middle":

Questa tipologia di attacco **(uomo in mezzo)**, si configura solo quando l'attaccante mette in atto una serie di procedure tese a porlo di fatto nelle condizioni di leggere, inserire e modificare a suo uso e consumo i messaggi che intercorrono tra altri due utenti senza che nessuno di questi ultimi sia nella condizione di sapere che il collegamento tra di loro stabilito è stato compromesso da un terzo individuo, l'attaccante. In altre parole il malintenzionato, controllando a priori lo scambio di informazioni tra i due utenti, può volgere a proprio vantaggio la comunicazione sottraendo credenziali e dati personali agli ignari utenti. Durante un attacco si fatto l'hacker è in grado di sostituirsi in toto a un utente replicando la trasmissione dei messaggi, opportunamente modificati, verso uno solo od entrambi gli utenti.






**I passi tipici di un attacco sono:**

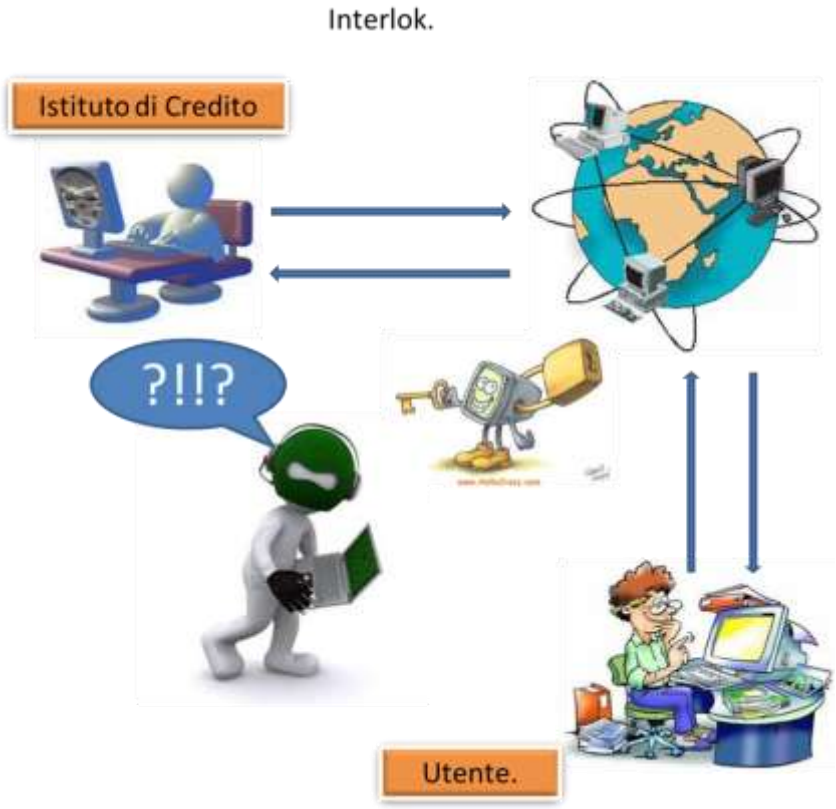
- Identificare il sistema da attaccare (per trovare il punto più vulnerabile e le modalità d'attacco).
- Ottenere un accesso utente (per penetrare nel sistema e tentare di ottenere accessi privilegiati).
- Ottenere un accesso privilegiato (per prendere il controllo completo del sistema tramite un attacco diretto a servizi o account con questi livelli).
- Coprire le proprie tracce (in modo che non sia possibile risalire all'attaccante e agli eventi esaminando i log del sistema).
- Installare backdoors (per rientrare nel sistema qualora venga individuato e/o eliminato il precedente metodo di penetrazione).
- Attaccare altri sistemi (una volta resosi anonimo e non individuabile).
- Prendere o alterare informazioni (presenti sulla macchina o sulla rete).
- Attuare altre attività non autorizzate (al fine di procurarsi un vantaggio o profitto).

Supponiamo ora che tra i due utenti sopra riportati intercorresse una comunicazione criptata con scambio di Chiavi Pubblica e privata e vediamo come agisce il truffatore "Man In The Middle".

**Esempio con scambio di chiavi  pubblica e privata.**

Supponiamo che il nostro utente intenda comunicare con il proprio Istituto di Credito tramite Home Banking per fare un pagamento e che il nostro malintenzionato, dopo essere riuscito ad ottenere in modalità truffaldina un accesso utente si sia posto nelle condizioni di spiare la comunicazione che avviene tra l'utente ed il suo Istituto di Credito. All'inizio della transazione l'utente deve chiedere all'Istituto di Credito la sua chiave pubblica. Quando L'Istituto di Credito invia la chiave il nostro malfattore, posto in mezzo, la intercetta ed inizia un attacco Man in the middle. Il malfattore  invia semplicemente all'utente una chiave pubblica della quale possiede la corrispondente chiave privata. L'utente, credendo che questa sia la chiave pubblica dell'Istituto di Credito, cifrerà i suoi messaggi con la chiave del malintenzionato e invierà così i messaggi cifrati all'Istituto di Credito. A questo punto il malfattore è nelle condizioni di intercettare tutti i messaggi, di decifrarli, di tenerne copia, di alterarli e inviarli cifrati all'Istituto di Credito usando la chiave pubblica che l'utente gli aveva inviato in origine. In questo modo è possibile impartire all'Istituto di Credito ordini di bonifici verso conti correnti fantasma e contemporaneamente rassicurare l'utente con messaggi che gli facciano credere della buona riuscita dell'operazione impostata. E' possibile, in teoria, intraprendere un simile attacco nei confronti di qualsiasi messaggio inviato tramite tecnologia a chiave pubblica, e questo anche se gli utenti sono nella realtà dei computer o dei server che si scambiano pacchetti di dati trasportati da reti informatiche.

E' ovvio che, una volta svelata la modalità dell'agire truffaldino, è possibile instaurare una nuova procedura che di fatto impedisca l'azione criminosa; per cui, solo a scopo esemplificativo, di seguito un suggerimento per impedire quanto sopra spiegato.




Si tratta del protocollo conosciuto con il sinonimo "lucchetto intermedio", noto anche col nome di **interlock**. Funziona più o meno come segue:

L'utente invia il suo messaggio utilizzando per la cifratura la chiave ricevuta dall'Istituto di Credito ma solo per la metà della sua lunghezza. L'istituto di Credito a sua volta cifra il suo messaggio con la chiave ricevuta dall'utente e invia anch'egli solo una metà del messaggio. Soltanto quando l'utente riceve la metà del messaggio invia l'altra metà all'Istituto di Credito, il quale a sua volta invia la sua altra metà all'utente. **Il gioco è fatto!** Il trucco risiede nel fatto che, "**avere solo metà di un messaggio cifrato non consente la sua decifrazione**". Quindi, se il nostro malintenzionato intercetta entrambe le chiavi dell'utente e dell'Istituto di Credito non sarà comunque in grado di decifrare solo mezzo-messaggio (cifrato usando la sua chiave), e di re-cifrarlo e quindi inviarlo usando la chiave dell'Istituto di Credito. Dovrà gioco forza attendere la ricezione di entrambe le metà del messaggio, leggerle e spedirle, ma questo è possibile solo componendo e quindi cifrando un nuovo messaggio. Così facendo potrà provare ad imbrogliare una sola delle due parti che alla transazione successiva si accorgerà dell'anomalia.

Un altro metodo per evitare un attacco MITM per i sistemi di cifratura a chiave pubblica è l'uso di **chiavi firmate**: se la chiave dell'Istituto di Credito fosse stata firmata da una terza parte, che si rende garante dell'autenticità, il nostro utente avrebbe potuto essere abbastanza tranquillo che la chiave firmata e ricevuta non avrebbe rappresentato un tentativo truffaldino.

E' infatti diffuso l'impiego di chiavi firmate ( Autorità Certificante CA). Quanto citato è una delle strade primarie per rendere più sicuro il traffico WEB (HTTPS, SSL o protocolli Transport Layer Security).

Detto questo…… **"attenzione!!"**

**Chiunque può rimanere vittima di un'intrusione o di un attacco!**

Le ragioni di questa affermazione possono anche sfuggire a chi si considera "**low profile**" o non comprende bene l'importanza dei dati che custodisce sui propri sistemi.

Sono estremamente diffusi nelle comunità degli hacker tool che permettono di verificare con estrema facilità ed in breve tempo la presenza di determinate vulnerabilità partendo ad esempio da un elenco "**pseudocasuale**" di indirizzi IP (per esempio, tutti i domini.it, oppure tutte le macchine della subnet 151.4.*.*, etc.).

Spesso gli utenti ricorrono a soluzioni hardware e software per risolvere problemi di sicurezza specifici ma, proprio per la natura intrinseca delle problematiche, le soluzioni adottate diventano obsolete con il tempo in quanto continuamente superate dalla tecnologia.

**Per questo non esiste e non esisterà mai una soluzione definitiva a questo problema.**

La sicurezza di un sistema viene valutata a partire dalla resistenza del suo anello più debole, per ottenere un sistema che riesca a garantire al meglio gli obbiettivi di sicurezza richiesti, bisogna valutare nelle varie componenti del proprio sistema informativo i rischi che si vengono a generare, tenendo conto dei livelli di protezione che vengono garantiti.

Le informazioni che consideriamo banali o di scarsa importanza, possono risultare invece estremamente interessanti per altri, a tal punto che spesso si ignora quale sovrabbondanza di dati passi tramite le legittime informazioni considerate pubbliche:

- versione di S.O.
- Tipo e versione applicativi.
- Utenti e gruppi di lavoro.
- Configurazione zone DNS.

- Configurazione SMTP.
- Servizi di informazioni erroneamente accessibili come SNMP, NetBIOS, sunrpc, finger.
- Protocolli non sicuri come FTP, POP3, http.

Tutti i servizi superflui e le informazioni che sono liberamente accessibili diventano, nelle mani delle persone od organizzazioni sbagliate, un potenziale problema per la sicurezza dell'intero sistema in quanto rappresentano i dati o le porte d'accesso alla rete da attaccare.

L'atteggiamento di chi, pur essendo responsabile della sicurezza di sistemi informativi, confida nel fatto che proprio la non conoscenza o meglio ancora la diffusione di informazioni false lo possa aiutare a mantenere la sicurezza viene definito come "**Security through obscurity**". Questo atteggiamento è guardato con superiorità dai puristi della sicurezza che ritengono questo approccio del tutto inutile a garantire anche un ben che minimo baluardo contro gli attacchi informatici a cui una rete può essere sottoposta. Al di là del loro modo di pensare anche questo modo di agire può essere uno degli strumenti utili per ottenere lo scopo di sicurezza che ci si prefigge quanto meno nei confronti dei malintenzionati meno abili. Il rischio della brutta figura nei confronti di chi ti ha dato la responsabilità del sistema informativo è comunque molto alta.


Per questo motivo è comunque consigliabile impedire l'accesso a priori a tutte le informazioni superflue per mantenere la sicurezza dei sistemi.

Prendiamo ora come oggetto del nostro discorso una rete dati che sta alla base di un sistema informativo qualunque.

Questa è una rete che funziona.....ma.....!!!!!

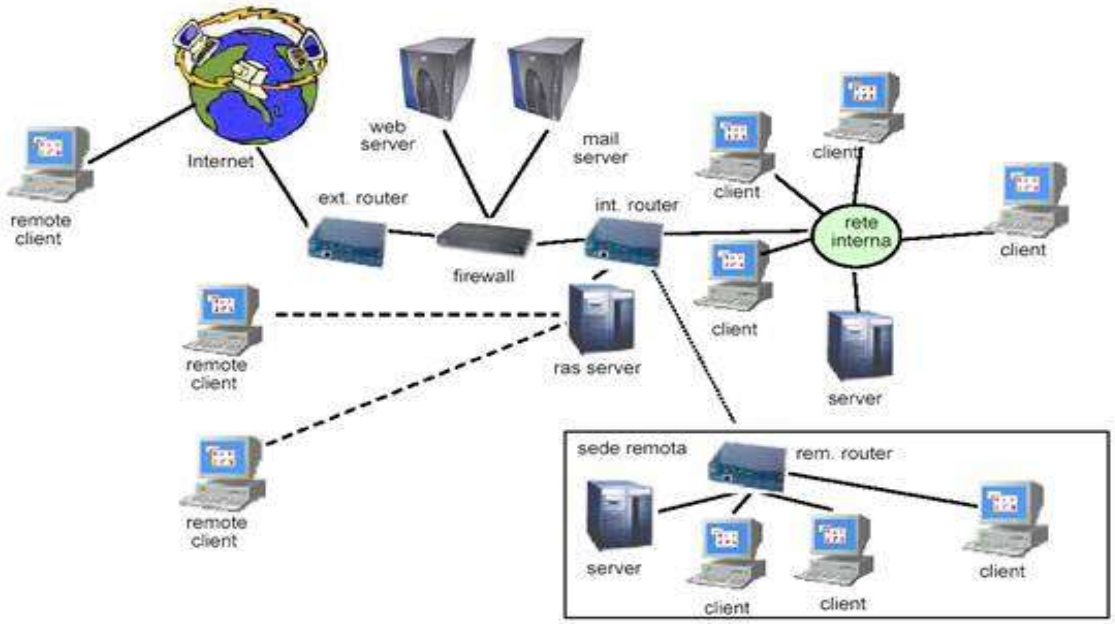



**Figura 3 - Esempio architettura rete non "protetta"**

....è sicura ?

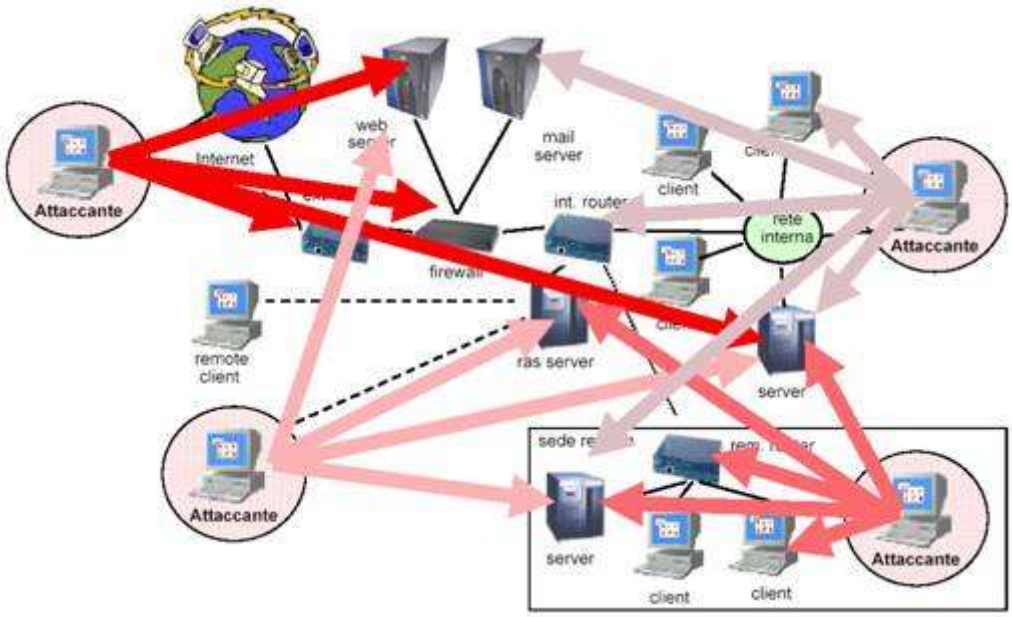



**Figura 4 - Esempio attacchi all'architettura rete non "protetta"**

Come si può notare dal disegno di rete sopra riportato, quella che Noi crediamo una rete sicura nella realtà ha una grande quantità di punti deboli attraverso i quali è possibile sferrare attacchi informatici.

## Ricapitolando:

La tipologia di attacco che va sotto il nome di "man-in-the-middle" consiste nel dirottare il traffico generato durante la comunicazione tra due host verso un terzo host (attaccante) il quale fingerà di essere l'end-point legittimo della comunicazione. Il tipico attacco man in the middle è cosi strutturato:

- Gli attori sono la vittima, il cattivo ed il server dhcp.
- La vittima fa una richiesta di IP address.
- Al primo che risponde il cattivo assegna un indirizzo IP e un gateway che corrispondono ad una certa interfaccia.
- Vengono forniti insieme anche parametri utili a dirigere il traffico verso di noi.
- Da questo punto in poi tutte le comunicazioni della vittima passano dal cattivo.
- Il cattivo le legge e per non farsi accorgere di nulla le manda a chi le deve ricevere.
- Il cattivo riceve la risposta e legge anche quella.

Fare tutto ciò non richiede particolare destrezza ma basta ad esempio scaricare dal WEB uno dei tanti tools che consentono tali operazioni spesso addirittura automatizzate.

Quale può essere l'obiettivo dell'attaccante?

Rubare le credenziali oppure memorizzare tutto il traffico che un utente fa con un altro utente.

- Ma quali sono nel dettaglio le vulnerabilità di una rete informatica come quella sopra raffigurata?
- Come difendersi dagli attacchi?
- Esistono altre forme di pericolo per il mio patrimonio informatico?
- La legge chiede di proteggere i dati?
- Dove inizia e dove finisce la mia responsabilità?
- E poi …..ancora ???????????

Nei prossimi capitoli evidenzieremo a quali vulnerabilità si è esposti se i sistemi non sono configurati in modo opportuno, quali dati possono essere acceduti mediante questa tecnica e più nel dettaglio proveremo a dare una risposta alle domande sopra riportate.

Il Tuo EterNet Team