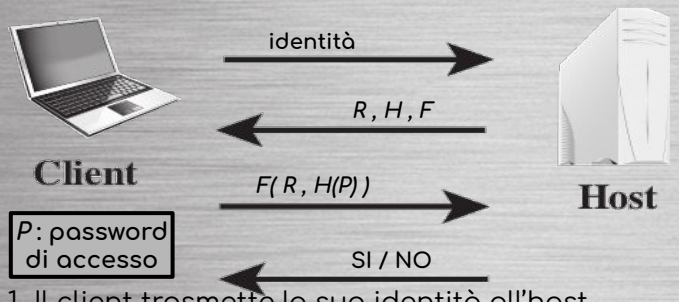
PROTOCOLLI C-R

Ogni protocollo **challenge-response** (C-R) presenta una fase iniziale in cui il client trasmette la sua identità all'host e una fase finale in cui l'host decide se ammettere il client nel sistema. Interposte tra queste due fasi si hanno le fasi di **sfida** - challenge - (presentata dall'host al client) e di **risposta** - response - (inviata dal client all'host).

La "**sfida-risposta**" si può basare su diverse fonti di autenticazione, tra cui dispositivi di **token**, **biometria** (statica o dinamica) e la più comune basata su **password**.

Protocollo C-R basato su password



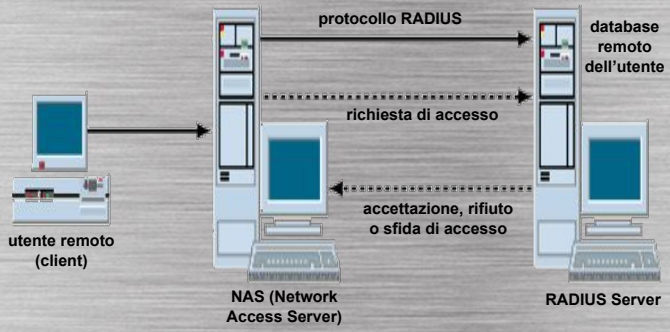
1. Il client trasmette la sua identità all'host.
2. L'host 'sfida' il client inviandogli una funzione *H* (**funzione di hash**), un numero casuale *R* e una funzione *F*.
3. Il client userà *H* per generare l'hash della password *H(P)* e risponderà alla sfida inviando il risultato di *F*, che prende in input *R* e *H(P)*.
4. Per autenticare il client, l'host si calcola la quantità *F* in locale (cosa che può fare siccome *H(P)* lo ha memorizzato in fase di registrazione dell'utente) e verifica che sia uguale alla quantità *F* ricevuta.

Si può notare come questo schema si protegge sia dall'**eavesdropping**, poiché scegliendo *F* ed *H* adeguatamente, l'attaccante non sarà in grado di recuperare la password, sia dai **replay attack**, in quanto grazie alla quantità casuale *R*, il valore di *F* sarà diverso per ogni sessione di accesso.

PROTOCOLLO RADIUS

Il protocollo **RADIUS** (Remote Authentication Dial-In User Service) è lo standard de facto per l'autenticazione remota. La maggior parte degli **ISP** (Internet Service Provider) e delle aziende lo utilizzano per gestire l'accesso a Internet, reti interne, reti wireless e servizi di posta elettronica.

Funzionamento: il punto di accesso al dispositivo remoto è chiamato **NAS** (Network Access Server). Il *client* inoltra la richiesta di accesso al **NAS** tramite un *pacchetto RADIUS* che contiene le credenziali di accesso. Il *server RADIUS* comunica con il **NAS** verificando che le informazioni siano corrette e può rispondere eventualmente con una **challenge** da presentare all'utente remoto. Una volta che l'utente è stato autenticato, il *server RADIUS* verifica che l'utente sia autorizzato ad utilizzare il servizio di rete richiesto.



RIFERIMENTI

➢ https://www.c3t.it/projects/awareness/articoli&brochure/autenticazione_remoto/

AUTENTICAZIONE DA REMOTO

Scopri cosa vuol dire autenticarsi da remoto, quali sono i problemi e le tecniche usate per garantirne la sicurezza.

POR FESR 2014-2020 obiettivo Crescita e Occupazione (CreO)

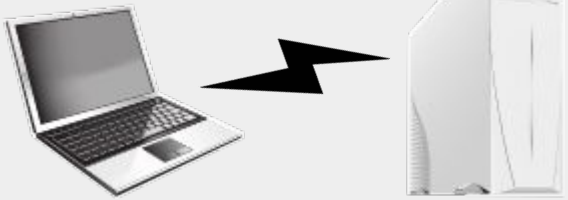
AUTENTICAZIONE DA REMOTO

Si parla di autenticazione locale quando un utente tenta di accedere un sistema che è localmente presente (es. un PC di un ufficio o uno sportello ATM).
Nel caso più complesso di **autenticazione remota**, l'utente cerca di accedere al sistema attraverso **internet** o comunque una rete o un link di comunicazione.

L'autenticazione remota comporta **minacce aggiuntive** alla sicurezza dei sistemi. Le due principali minacce, che si basano sulla figura del cosiddetto **man-in-the-middle**, sono:

- l' **"eavesdropping"**: in cui l'attaccante cerca passivamente di intercettare e decodificare le informazioni trasmesse attraverso il mezzo di comunicazione;
- il **"replay attack"**: un attacco in cui l'esecutore intercetta, e in seguito ripete, una trasmissione di dati valida all'interno della rete. La trasmissione può essere, ad esempio, una sequenza di dati per l'autenticazione di un certo utente e, dato che i messaggi originali vengono intercettati e ri-trasmessi alla lettera, gli hacker che si servono di replay attack non devono necessariamente decifrarli.

Per contrastare le minacce all'autenticazione da remoto, i sistemi si basano generalmente su delle forme di **protocolli challenge-response** (in breve **protocolli C-R**).

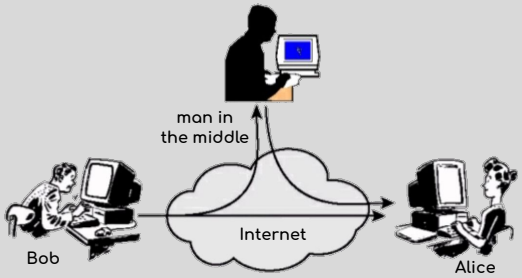


Client Host

Il **man-in-the-middle** è un malintenzionato che si inserisce (intercettando i messaggi inviati) tra due entità che stanno lecitamente cercando di comunicare tra loro.

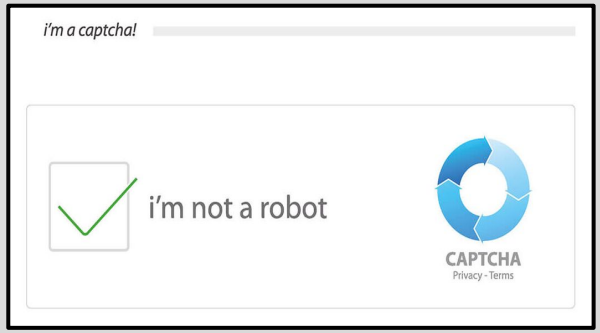
Nel caso di comunicazione **wireless**, ad esempio, è sufficiente che il **man-in-the-middle** si trovi nel raggio di trasmissione e, con appositi apparecchi scanner, potrà raccogliere tutti i dati relativi alla trasmissione.

Un esempio comune di replay attack si può avere quando un certo utente (**Bob**) tenta di autenticarsi in un certo sistema (gestito da **Alice**) per fruire di un certo servizio. Il **man-in-the-middle** che intercetta il messaggio di autenticazione, lo spedisce ad Alice lasciandolo cifrato (siccome il sistema di autenticazione se lo aspetta cifrato). In questo modo il man-in-the-middle verrà autenticato come se fosse Bob.



In questi scenari si considera un client (es. un utente) che cerca di connettersi ad un host (es. un server che fornisce un servizio).
Gli step generali di funzionamento sono i seguenti.

1. Il client trasmette la sua identità all'host remoto.
2. L'host presenta una **sfida** (*challenge*) al client.
3. Il client **risponde** (*response*) alla sfida trasmettendola all'host.
4. L'host decide se autenticare il client sulla base dell'esito della sfida.



L'implementazione dettagliata della sfida può variare da protocollo a protocollo e può fare uso di dispositivi e metodologie diverse.
I principali protocolli C-R si basano sulle seguenti fonti di autenticazione.

- Password.
- Token.
- Biometria statica.
- Biometria dinamica.