Cifratura delle password nei sistemi UNIX

Esempio di identificazione su canale sicuro (lettura e scrittura non intercettabili né alterabili).

Quando un utente fornisce per la prima volta la propria password p, viene memorizzata nel file delle password la coppia $(s, h(ps))$, dove:

- s è un seme casuale;
- h è una funzione hash;
- ps è la concatenazione di p ed s.

Si concatena s per impedire che password uguali abbiano lo stesso hash.

Per gli accessi successivi si recupera s dal file, si concatena alla password fornita e si calcola l'hash. Se coincide con quello memorizzato l'identificazione ha successo.

Un accesso illecito al file delle password non fornisce informazioni interessanti, visto che è computazionalmente difficile ricavare la password dall'hash (h è one-way).