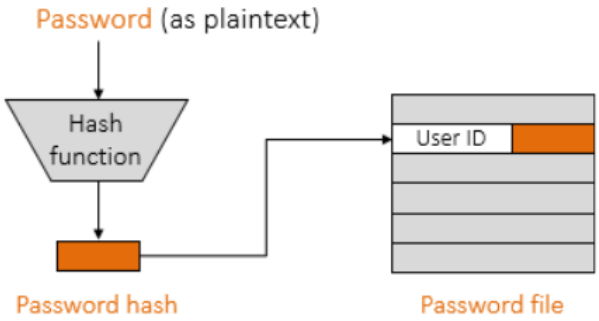
4. laboratorijska vježba: Password hashing

Studentica: Emilija Sarić

Smjer: 112

Predmet: Sigurnost računala i podataka

→Lozinke su najzastupljeniji način autentikacije korisnika. Nikad se ne pohranjuju "u čisto" jer bi to znatno povećalo rizik krađe, umjesto toga se pohranjuje hash vrijednost lozinke.



Slika 1: Način pohrane lozinki pomoću hash funkcije

→Na lozinke pohranjene na ovaj način može se izvesti Pre-computed Dictionary Attack gdje se pohranjuje lista kandidata za lozinke, hashiraju te lozinke i uspoređuju sa hash vrijednosti tražene lozinke. Dodatne sigurnosti koje se mogu poduzeti protiv ovog napada su iterativno hashiranje i salt lozinke. Salt dodaje niz karaktera na kraj lozinke i tek onda se hashira, na taj način napadači ne mogu doći do lozinke pretraživanjem po rječniku.

→U ovoj se vježbi uspoređuju klasične kriptografske hash funkcije i specijalizirane kriptografske funkcije za sigurnu pohranu zaporki.

ZAKLJUČAK:

Pokretanjem koda u windows terminalu uočavamo da su hash funkcije dosta brže u odnosu na specijalizirane funkcije te da je za što precizniji rezultat potrebno napraviti što više iteracija. U vježbi se uočavaju i primjer salt-a koji se također koristi za preciznije mjerenje brzine izvođenja funkcija.