PASSWORD MANAGEMENT

- The front line of defense against intruders is the password system, where a user provides a name/login identifier (ID) and a password.
- The password serves to authenticate the ID of the individual logging on to the system.
- Passwords are usually stored encrypted rather than in the clear

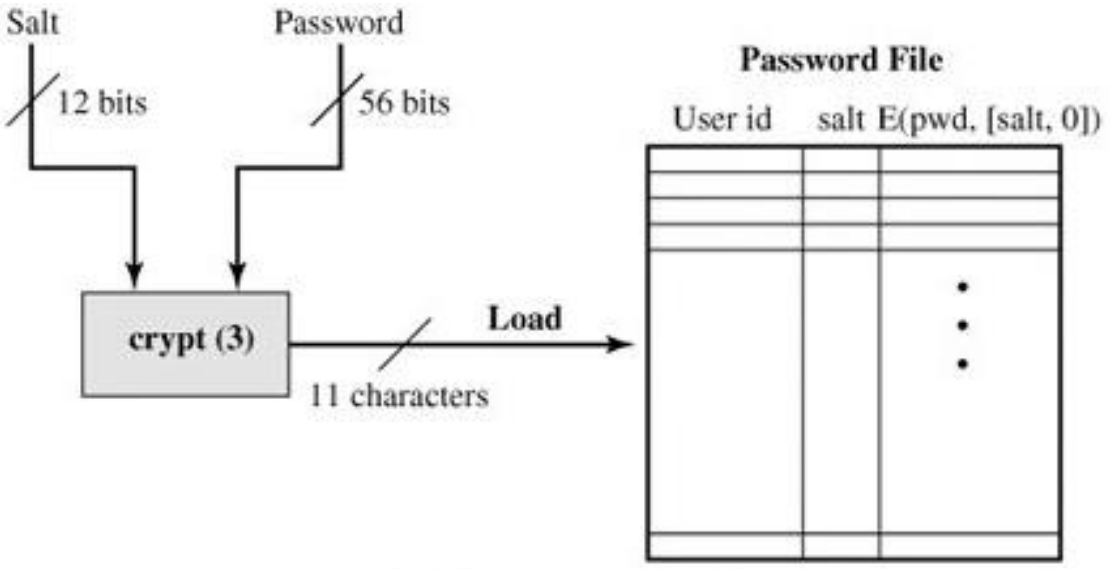
The Vulnerability of Passwords: let us consider a scheme that is widely used on UNIX:

- Each user selects a password up to eight characters.
- This is converted into a 56-bit value (key input to an encryption routine).
- The encryption routine is based on DES. The DES algorithm is modified using a 12-bit.
- This value is related to the time at which the password is assigned to the user.
- The modified DES algorithm is exercised with a data input consisting of a 64-bit block of zeros.
- The output of the algorithm then serves as input for a second encryption.
- This process is repeated for a total of 25 encryptions.
- The resulting 64-bit output is then translated into an 11-character sequence.
- The hashed password is then stored, together with a plaintext copy of the salt, in the password file

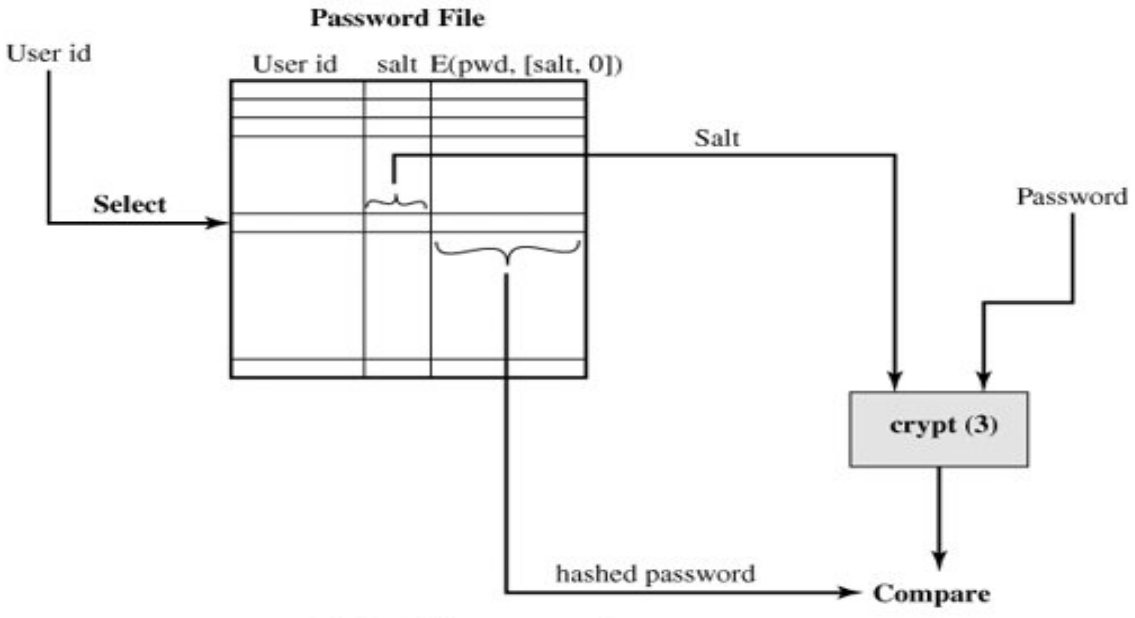
The salt serves three purposes:

- It prevents duplicate passwords from being visible in the password file.
- It effectively increases the length of the password without requiring the user to remember additional characters.

Access Control: One way to thwart a password attack is to deny the opponent access to the password file. If the encrypted password portion of the file is accessible only by a privileged user, then the opponent cannot read it without already knowing the password of a privileged user.



(a) Loading a new password



(b) Verifying a password

Password Selection Strategies: The goal is to eliminate guessable passwords while allowing the user to select a password that is memorable. Four basic techniques are in use:

- User education.
- Computer-generated passwords.
- Reactive password checking.

- Proactive password checking.

User education

- Users can be told the importance of using hard-to-guess passwords and can be provided with guidelines for selecting strong passwords.

Computer-generated passwords

- passwords are quite random in nature

Reactive password checking

- the system periodically runs its own password cracker to find guessable passwords. The system cancels any passwords that are guessed

Proactive password checking

- user is allowed to select his or her own password. However, at the time of selection, the system checks to see if the password is allowable and, if not, rejects it.

The first approach is a simple system for rule enforcement, enforcing say guidelines from user education. May not be good enough. Another approach is to compile a large dictionary of possible “bad”passwords, and check user passwords against this disapproved list. But this can be very large & slow to search. A third approach is based on rejecting words using either a Markov model of guessable passwords, or a Bloom filter. Both attempt to identify good or bad passwords without keeping large dictionaries.