**COSC 359**

**User Authentication**

Description

A widely used password security technique is the use of hashed passwords and a salt value. This scheme is found on virtually all UNIX variants as well as on a number of other operating systems as shown in Figure 3.1 bellow.

To load a new password into the system, the user selects or is assigned a password. This password is combined with a fixed-length salt value. In older implementations, this value is related to the time at which the password is assigned to the user. Newer implementations use a pseudorandom or random number. The password and salt serve as inputs to a hashing algorithm to produce a fixed-length hash code. The hash algorithm is designed to be slow to execute to thwart attacks. The hashed password is then stored, together with a plaintext copy of the salt, in the password file for the corresponding user ID. The hashed-password method has been shown to be secure against a variety of cryptanalytic attacks [WAGN00].

When a user attempts to log on to a UNIX system, the user provides an ID and a password. The operating system uses the ID to index into the password file and retrieve the plaintext salt and the encrypted password. The salt and user-supplied passwords are used as input to the encryption routine. If the result matches the stored value, the password is accepted.

**// PART A: ID/PASSWORD CREATION**

Write the necessary C++ code (or a language of your choice) for the following activities:

1. Create user ID and Password pair by asking users to input ID/Password. Check the input and help users to choose an acceptable ID/Password based on the company security policy.
2. Create a Salt value, add it to the Password and use a hash function to encrypt both Salt and Password.
3. Store user ID, Salt and hashed password in ID-PASSWORD.TXT

**// PART B: USER AUTHENTICATION**

Enhance your code from PART A for the following activities:

1. Ask users for ID/Password pair
2. Authenticate users using ID.txt and the ID-PASSWORD.TXT files.

