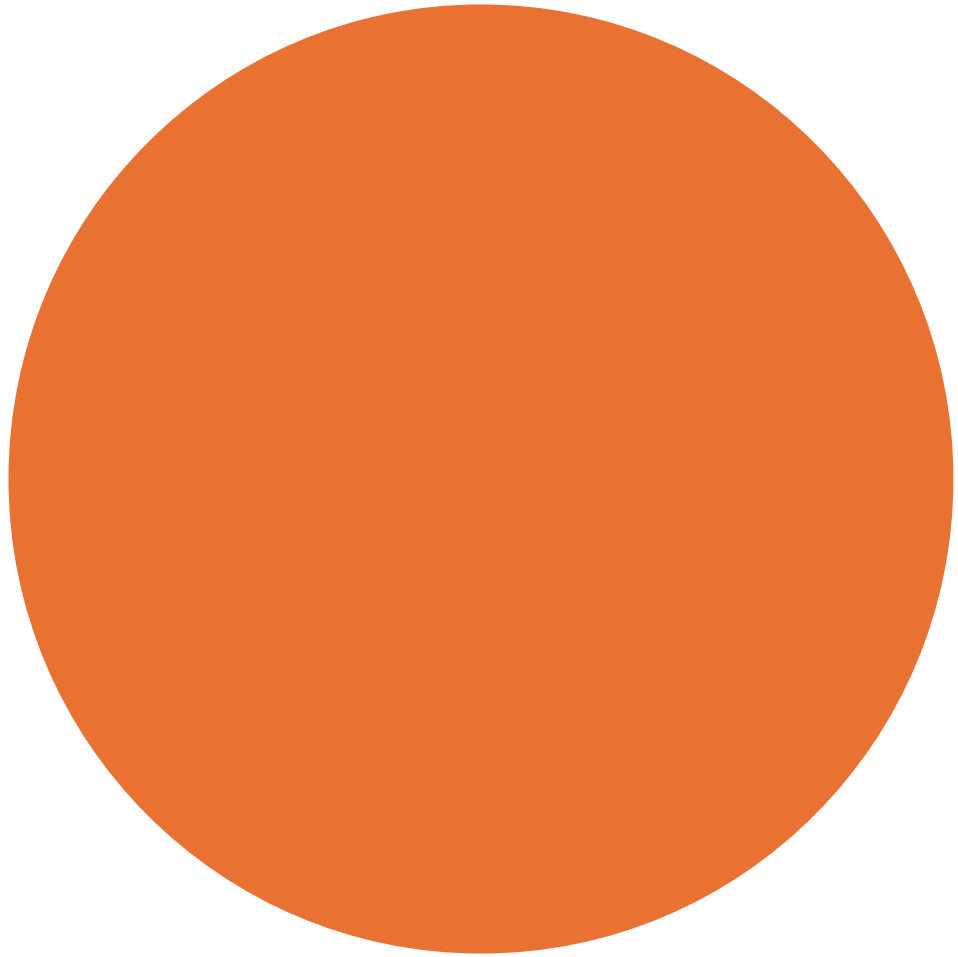
Ch8:
Users and Groups



Purpose

- **Primary purpose of user and group IDs is:**
  - Determine ownership of various system resources.
  - Control the permissions granted to processes accessing those resources.

The Password File: /etc/passwd

- **/etc/passwd contains one line for each user account:**
  - Login name: *unique, human-readable*
  - Encrypted Password: *empty means no password*, *ignored if shadow passwords have been enabled*
  - User ID (UID): *32-bit, 0 means root account*
  - Group ID (GID): *32-bit*
  - Comment
  - Home Directory
  - Login shell: *empty means /bin/sh*

The Group File: /etc/group

→ 4.2BSD introduced the concept of multiple simultaneous group memberships.

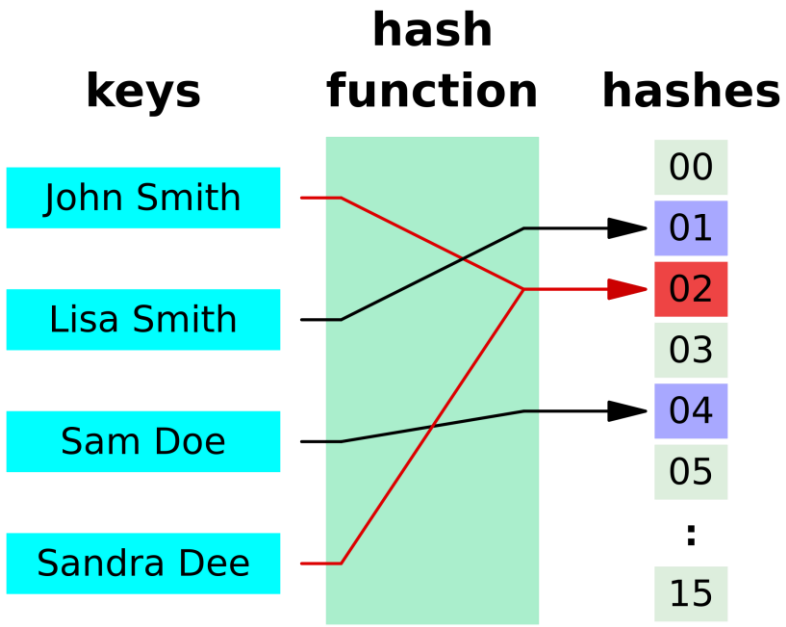
→ **/etc/group contains one line for each user account:**

- → group name: *unique, human-readable*
- → Encrypted Password: *rarely used (newgrp), empty means no password*, *ignored if shadow passwords have been enabled (/etc/gshadow)*
- → Group ID (GID): *32-bit*
- → User list: *groups command*

The Shadow Password File: /etc/shadow

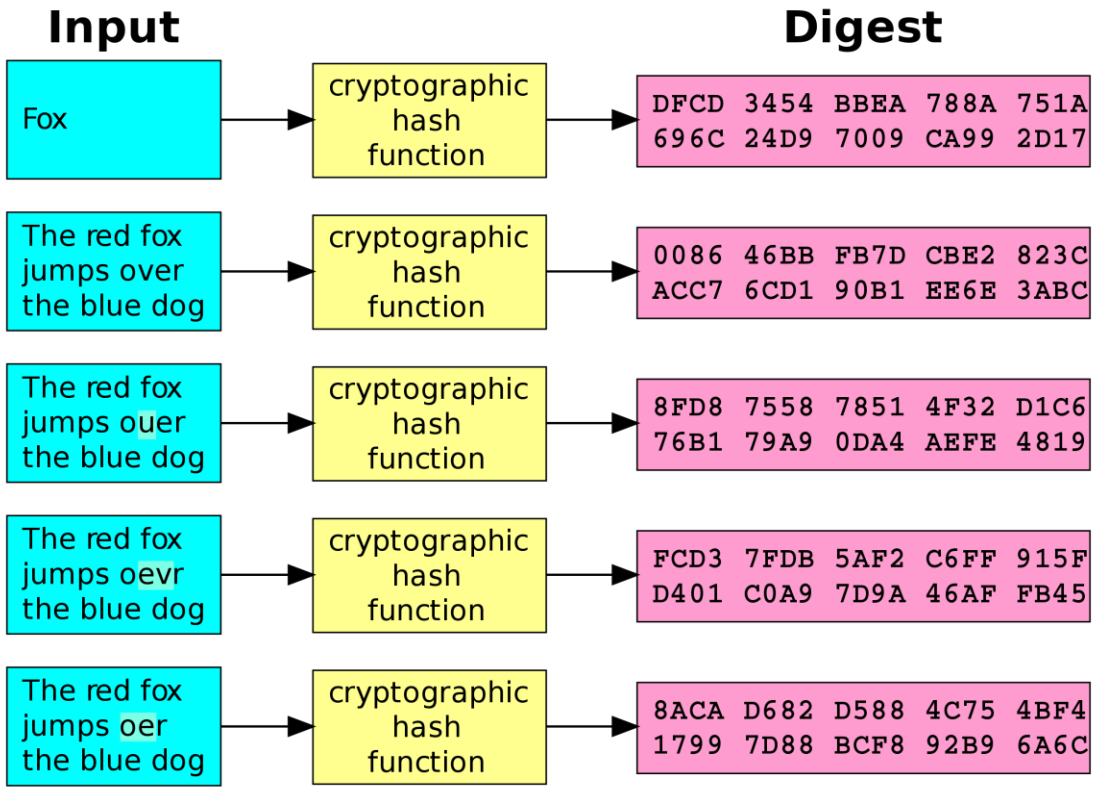
- **Rational:** **a security problem in /etc/passwd**
- Contains:
  - Login name: *unique, human-readable matching /etc/passwd*
  - Encrypted Password: *empty means no password*
  - Aging information
- *How does the password get encrypted?!*

Hash functions



- What is a hash function?
  - A hash function is a mathematical function or algorithm that simply takes a variable number of characters (called a ”message”) and converts it into a string with a fixed number of characters (called a hash value or simply, a hash).

Cryptographic Hash functions



- → Important Properties:
  - → **Pre-image resistance.**
    - → a one-way function.
  - → **Collision resistance.**
- → **Examples:**
  - → DES: no longer trusted for encrypting sensitive data.
  - → MD5: outdated and insecure.
  - → SHA1
  - → SHA-256
  - → SHA-512

Password Encryption and User Authentication

- **Authentication** is the process by which a person or system verifies that they are who they say they are.
- UNIX uses the hashing for verifying the user passwords.
  - *man 3 crypt*

Retrieving User and Group Information

- **/etc/passwd:**
  - getpwnam()
  - getpwuid()
  - Scanning: getpwent(), endpwent(), and setpwent()
- **/etc/group**
  - getgrnam()
  - getgrgid()
  - Scanning: getgrent(), setgrent(), and endgrent()

Retrieving User and Group Information

→ **/etc/shadow:**

- → getspnam()
- → ~~getspuid()~~
- → Scanning: getspent(), endspent(), and setspent()