CSE321 Theory Assignment 02

Research and **Explore** the limitations of standard Unix file permissions and the necessity of Extended Access Control Lists (ACLs) by analyzing the following key areas:

- Limitations of the rwx (User-Group-Others) Model
- Granularity of Extended ACLs

Report Requirements:

Write a comprehensive analysis focusing on the following two key factors:

Standard Permission Bottlenecks:

- Explain the architectural limitations of the traditional 3-tier (Owner, Group, Others) permission model when dealing with complex multi-user environments.
- Describe scenarios where a standard group-based permission scheme fails to provide necessary isolation (e.g., granting read access to a specific individual without adding them to a group).

Mechanism of Extended ACLs:

- Describe the structure of a POSIX ACL entry and how it extends the file system inode metadata.
- Compare the command-line implementation differences between changing standard modes (chmod) and managing ACL entries (setfacl / getfacl).
- Discuss the priority logic the OS uses when checking permissions (e.g., specific user entry vs group entry vs mask).

Study Resources:

- Arch Linux Wiki - Access Control Lists: (Read the "Usage" section) [https://wiki.archlinux.org/title/Access_Control_Lists]
- GeeksforGeeks - Access Control Lists (ACL) in Linux: (Good for basic setfacl commands) [https://www.geeksforgeeks.org/linux-unix/access-control-listsacl-linux/]

- Red Hat Enterprise Linux Guide: (Focus on "Setting Access ACLs") [https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/7/html/system_administrators_guide/ch-access_control_lists]

Submission guidelines: Can be found in the submission form given below.

Submission Link

Deadline: ***8 January, 11:00 PM***

(Submissions outside the Google Form will be automatically rejected.)