SYSTEM SECURITY

•A protected file system

•For a given folder and files inside, the system only allows the account Alice to use certain programs to create/read/edit/delete it

•You need to assign correct permissions

•Other accounts are not able to read the content

•Purely user level file system is fine

MINIMAL

•Supporting file creation/read/write/deletion for Alice only in a specific folder

•Root user cannot get the file content

LINUX PERMISSIONS

•We will cover this topic right after crypto related topics  
•Linux has permissions to isolate accesses

•Alice can be (almost) the only one to read/write/delete/create files

•What is the challenge?

•ROOT user

•Root accounts can revert all protections you may add to the system

HOW DO WE SOLVE IT?

•There are two ways of protection

•Hide the existence →Access control

•Hide the content →Crypto

•Crypto introduces new challenges: performance

•If edit is supported, how do we encrypt?

•Where do we store the key?

•If cannot fully prevent it, audit the modification

•Linux audit

REQUIREMENT

•As long as your implemented system prevents the other users as well as root from reading the real content

•There are many possible decision choices

•TEXT files only

•There is no need to implement a text editor (although, you can enhance simple ones by adding more functionalities)

•You can use a wrapper, which calls other editors

WHAT DO YOU EXPECT

•Please explain how you encrypt and decrypt files

•Please explain how do you deal with random access/edit

•Please explain the trade-off in the design

•Please explain how do you store keys

•Please explain how do you authenticate Alice

•Please explain the provided security features

Project SYSTEM SECURITY: Group members jp1476, acp163, asp209, cyk17, ttm30, sss309

Email Id for bitbucket access:

jp1476@scarletmail.rutgers.edu; acp163@scarletmail.rutgers.edu; asp209@scarletmail.rutgers.edu; cyk17@scarletmail.rutgers.edu; ttm30@scarletmail.rutgers.edu;sss309@scarletmail.rutgers.edu

Task done so far:

Program menu.(Anish)

ed2 editor to create new file and edit existing file. (Anish)

Audit Repository: That stores filename and checksum to validate file tampered(Anish)

Alice authentication method (Sagar)

List files from Audit repository (Sagar)

**To do:**

Key based encryption program and manage key file. (Right now it uses basic shift cipher where the shift is 3.)

Delete files

Linux permission to hide file existence and permissions.

....more task to be added, every one validate

Provide name of team members who will be working on above todo items, reply on email chain.

**Basic ed2 editor commands:**

a: to append text to file.

.<ret>w filename: To save.

q: to quit

,l : to display file contents.