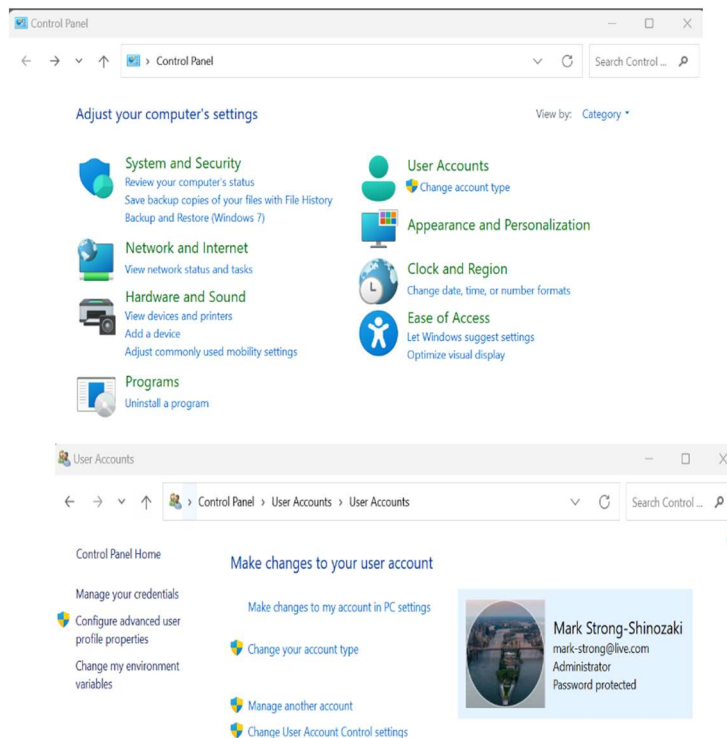
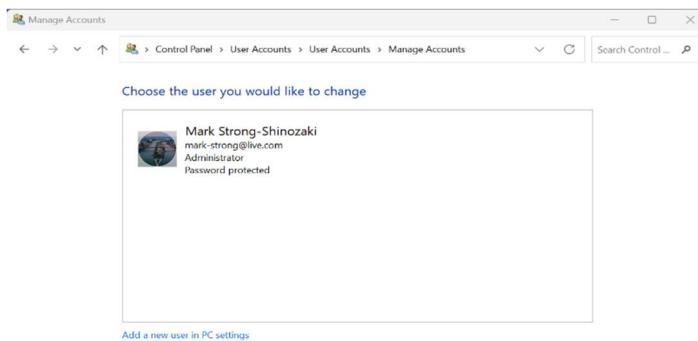


Mark Shinozaki
HW02 – Observations Report
Professor: Ananth Jillepalli
Date: 10/5/2023
Assignment Description:

- Every student will first identify their main computing environment i.e. Windows or MacOS or *nix, and so on.
- Students can then discover all forms of access control systems on their main computing environment. The discovery must be documented with screenshots.
- Students then categorize the discovered access control systems into DAC, MAC, RBAC, or other access control models.
- Finally, students will evaluate the discovered access control systems from the lens of a malicious agent. That is, the evaluation should try to identify any weaknesses in the access control options.

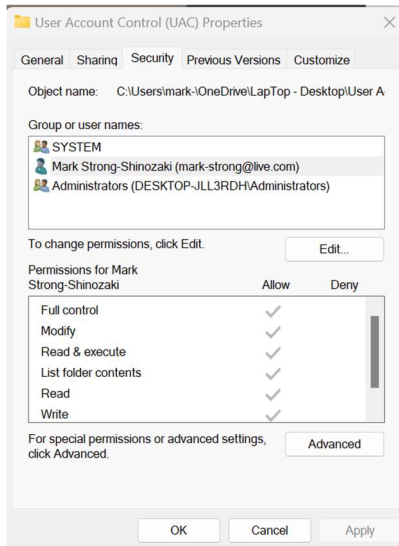
User Account Control (UAC)



User Account Control (UAC):

- Access Control System: DAC (Discretionary Access Control)
- Description UAC is primarily a DAC mechanism. It allows or restricts actions based on the discretion of the user or administrator. It prompts users for consent or admin credentials to perform certain actions, giving them discretionary control.

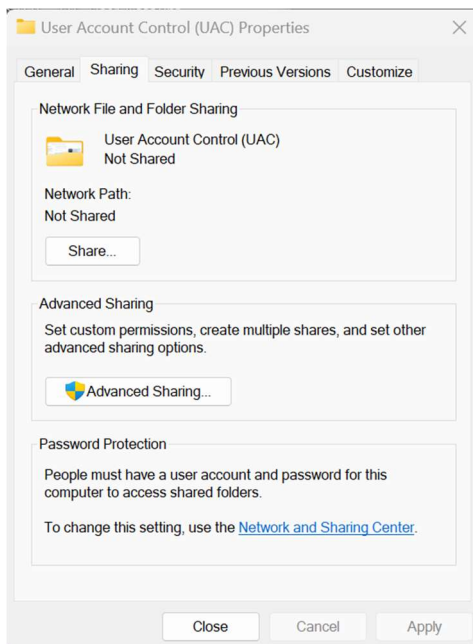
NTFS Permissions



NTFS Permissions :

- Access Control System: DAC (Discretionary Access Control)
- NTFS permissions grant or deny access to files and folders based on the discretion of the owner or administrators. Users with appropriate permissions can modify access to resources.

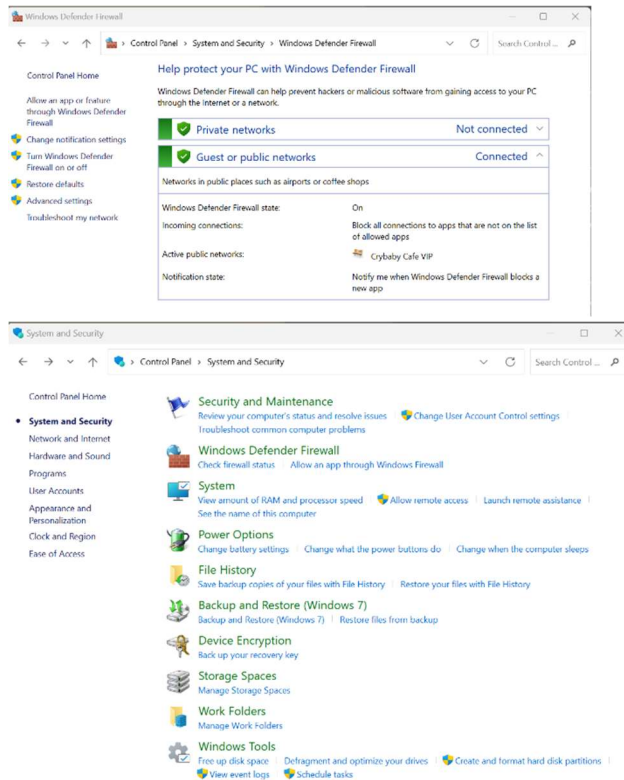
Share Permissions



Share Permissions :

- Access Control System: DAC (Discretionary Access Control)
- Share Permissions control access to shared resources, such as folders, on a network. Like NTFS permissions, share permissions are based on the discretion of the resource owner or administrators

Mark Shinozaki
HW02 – Observations Report
Professor: Ananth Jillepalli
Date: 10/5/2023
Windows Firewall



Windows Firewall:

- Access Control System: RBAC (Role-Based Access Control)
- The Windows Firewall allows or blocks network traffic based on rules set by the user or administrator. This control is discretionary because it's based on the choices made by the system administrator.

User Right Assignments

```
root@DESKTOP-JLL3RDH: ~  
python-numpy-doc python3-dev python3-pytest  
python3-numpy-dbg setools-gui  
The following NEW packages will be installed:  
checkpolicy libauparse0 libblas3 libgfortran5 liblapack3 m4  
policycoreutils-dev policycoreutils-python-utils  
python3-audit python3-decorator python3-ipyp  
python3-networkx python3-numpy python3-selinux  
python3-semantize python3-sepolgen python3-sepolicy  
python3-setools selinux-policy-dev semodule-utils setools  
0 upgraded, 21 newly installed, 0 to remove and 262 not upgrade  
d.  
Need to get 736 kB/8635 kB of archives.  
After this operation, 47.0 MB of additional disk space will be  
used.  
Do you want to continue? [Y/n] Y  
Ign:1 http://archive.ubuntu.com/ubuntu focal-updates/main amd64  
libgfortran5 amd64 10.3.0-1ubuntu1~20.04  
Err:1 http://security.ubuntu.com/ubuntu focal-updates/main amd6  
4 libgfortran5 amd64 10.3.0-1ubuntu1~20.04  
404 Not Found [IP: 185.125.190.36 80]  
E: Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/  
g/gcc-10/libgfortran5_10.3.0-1ubuntu1~20.04_amd64.deb 404 Not  
Found [IP: 185.125.190.36 80]  
E: Unable to fetch some archives, maybe run apt-get update or t  
ry with --fix-missing?  
root@DESKTOP-JLL3RDH:~# sudo setenforce 0  
setenforce: SELinux is disabled  
root@DESKTOP-JLL3RDH:~# sudo setenforce 1  
setenforce: SELinux is disabled  
root@DESKTOP-JLL3RDH:~#
```

Windows Firewall:

- Access Control System: MAC (Mandatory Access Control)
- MAC is a more complex access control model commonly associated with high-security environments. In the example on the left, I tried to set up or config SELinux.