OS Practical 9 Lee Hsien Xiang 194841J

SELinux prevent giving any process too much access by limiting what they can do on a system, one way is using container which ensure process that are meant to operate within the container and can do anything inside the container base on the governance of the container rule but can’t execute anywhere outside the container. SELinux also uses MAC which allow system administrator to set policies to govern the access. With these policies in place not even account with root privileges can override the policies, this way the security of the file and process is independent of the file owner.