Andrew Plum

Mr. Alves-Foss

Cyb 110

9/5/21

Ch. 3 Homework

1) Authorization is the process of determining exactly what an authenticated party can do. Authorization is crucial to enable various parties to access certain resources. Access controls are what are typically used to implement authorization. Access controls are mechanisms that allow or prevent an authenticated subject from performing and action on various objects. Access controls are used to allow access, deny access, limit access, and revoke access.

2) The Brewer and Nash model protects against conflicts of interest. The Brewer and Nash model is commonly used in the financial, medical, or legal industries. The Brewer and Nash model helps to prevent conflicts of interest by having the level of access for a person to resources and materials dynamically change based on what a person has previously accessed. This model makes use of both discretionary and mandatory access controls. The subject can only access objects from the same data set as an object already accessed by the subject or objects that belong to a conflict of interest that the subject has not yet accessed any information from.

3) Access control based on the Media Access Control address of the systems on your network does not represent strong security because the software settings in most operating systems can override a network interface's Media Access Control address. Media Access Control addresses are not a good choice for a unique identifier of a device on a network because the address is easy to change.

5) In the discretionary access control model, the owner of the file gets to control access of it. Discretionary access controls are implemented in most operating systems. In the mandatory access control model, the system enforces limits. The owner of the object or file does not decide who gets access to it. A separate entity, whether it be a group or individual, has the authority to set access to the resources. Government organizations often have mandatory access controls implemented.

7) It would be a security issue if I had a file containing sensitive data on a Linux operating system with the permissions set to rw-rw-rw-. This is because anyone could read or overwrite the file, as the permissions of reading and writing are not limited to only the user. Confidentiality of the data on the CIA triad would be affected because anyone can read the file even if the user doesn't want them to. Integrity of the data could be affected if anyone wanted to change the data so that it did not reflect reality. Accessibility of the data would not be affected because anybody would still be able to access it when they need to.

8) The access control model I could use to prevent users from logging into their accounts after business hours is the attribute-based access control. I could set the attribute to time so that after the hours of permitted use, users would not be able to access resources in the system. A possible downside in implementing this access control could be a loss in productivity because the users would only be able to access resources in the system during permitted times, but the resources would be more secure after business hours.