COM-301 Computer Security
Exercise sheet: Access Control

1. Which of these principles are related to access control and how?

   (a) Least common mechanism

   (b) Least privilege

   (c) Open design

   (d) Complete mediation

   Justify your answer, both when positive and when negative

2. When you decide to assign permissions to users according to a job function, what is this called?

3. ACME Corporation is planning to implement an access control mechanism in which employees control who has access to their own information assets. What is this type of access control?

4. What is a negative permission? How are negative permissions different from blacklisting permissions as access control? Provide an example from Linux access control.

5. Check the following table and list all files which Alice can write into.

   - Alice is a member of groups *alice* and *pcrack*
   - Dave is a member of groups *dave* and *gdev*

Permissions	Owner	Group	Size	Last update	File name
- rws - - - - -x	dave	gdev	134516	Sep 08 21h10	hello
drwxrwxrwt	dave	gdev	14586	Aug 01 14h30	program
- rwx - - x - - x	alice	alice	214768	Sep 10 07h35	hosts
- rw - r - - - - -	alice	pcrack	12486	Sep 10 08h09	config
- rw - r - - r - -	dave	pcrack	98774	Aug 28 15h10	data
- rw - - wxr - -	root	pcrack	12257	Sep 15 10h46	setup

6. Imagine a grocery store in which the only way of leaving with goods is having a cashier scan the barcode of each bought item to determine the total cost. A user willing to cheat the system could replace some of the barcodes of his expensive items with a barcode of cheaper items such that, when the cashier scans the items, the bill is lower than the actual price. What is the role the cashier plays in this situation?

7. What principle is supported by user Nobody in UNIX? Justify your answer.

8. Consider two mechanisms to access a bank account. In Mechanism A, each owner is authorized in multiple accounts. By showing your userID, you are provided with a token to access to all accounts you are authorized. In Mechanism B, each account has associated a list of userIDs (accountID,userIDs). If your userID is in the account's list, you can access the account. Which one implements ACL and which one Capabilities. In this scenario how are the problems of these approaches materialized?