1. What is the difference between mandatory and discretionary access control?

Mandatory access control is set by the system and discretionary access control is set by the user. E.g., when you adjust whether other users can read your files, that is discretionary access control.

1. For each scenario below, discuss if a breach of C, I, or A has occurred.
   1. Scenario: My credit card number is stolen when ordering something online.
   2. Scenario: The stolen credit card number is used to make a purchase.
   3. Scenario: The credit card company detects the fraudulent activity and does not allow any more purchases with the credit card.
2. If a policy is not enforced with a technical mechanism, how else can it be enforced? Give an example.
   1. My favorite: the machines login requires a keycard. The policy is that keycards cannot be left on machines. The enforcement is that employees must hang their keycards from their neck. If an employee is seen in the hall without their keycard on their neck, they get in trouble
   2. Policy is that no food is allowed in the computer room. This is enforced by managers walking through the computer rooms.
3. “traditional” Linux access control uses abbreviations of access control that is specified by 9 letters (e.g., rwxrwxrwx gives full access). What are the letters and what do they mean?
4. Role-based access control
   1. Consider the following
      1. Let trans(r) = the set of files someone can read in role r, where
         1. trans(CTO) = {plans for project A, plans for project B, hiring plans, engineering salaries, project A status, project B status}
         2. trans(programmer in group A) = {code set A, plans for project A}
         3. trans(programmer in group B) = {code set B, plans for project B}
         4. trans(tech lead in group A) = {code set A, plans for project A, project A status}
         5. trans(tech lead in group B) = {code set B, plans for project B, project B status}
         6. trans(CEO) = {hiring place, engineering salaries, project A status, project B status}
      2. Let actr(s) be role subject s is in at the current time (now) , where
         1. Actr(Stephan) = CTO
         2. Actr(Sam) = CEO
         3. Actr(Lisa) = tech lead in group B
         4. Actr(Ivan) = programmer in group A
      3. Let Authr(s) is the set of all possible roles that subject s can take
         1. Authr(John) = {student}
         2. Authr(Stephan) = {CTO, tech lead in group A}
         3. Authr(Sam) = {CEO)
         4. Authr(Lisa) = {tech lead in group B, programmer in group B)
         5. Authr(Ivan) = {programmer in group A)
   2. Answer the following true or false and if false explain why
      1. Canexec(Ivan, code set A) = true/false ? TRUE
      2. Canexec(Sam, status project A) = true/false ? TRUE
      3. Canexec(Lisa, code set A) = true/false ? FALSE
      4. Canexec(Stephan, code set A) = true/false ? FALSE, because the CTO does not have access to code set A
   3. Suppose Lisa becomes co-CTO, what changes are required
      1. We need to change Authr(Lisa) so that Authr(Lisa)={CTO} and log Lisa out so that she needs to relogin and get the new access and remove the old access
5. Consider the ordered detailed access control list below. Give the end results and the steps taken in deciding the following requests made to the operating system
   1. Stephan is in Group A and Group B and seeks to write to the object
   2. Linda is in Group B and seeks to execute the object
   3. Joe is in Group A and seeks to read the object
   4. Chris is in Group C and seeks to read the object

DACL

Access denied

Stephan

Read, write, execute

ACE 1

Access denied

Group A

Read, write, execute

ACE 2

Access allowed

Group B

Write

ACE 3

Access allowed

everyone

Read

ACE 4