JOHANN WOLFGANG GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

Fachbereich Wirtschaftswissenschaften
Institut für Wirtschaftsinformatik
Lehrstuhl für M-Business & Multilateral Security

Fachbereich
Wirtschaftswissenschaften

Institut für Wirtschaftsinformatik
Lehrstuhl für M-Business & Multilateral Security
www.m-chair.de

Prof. Dr. Kai Rannenberg
M.Sc. Ahmed S. Yesuf

E-Mail sec@m-chair.de

Information and Communications Security
WS 16/17
Assignment 2
Access Control

Please prepare your answers for the following questions before the exercise session on the **15th of November 2016.**

Exercise 1:
Alice can read FileX, can append to FileY, and can write to FileZ. Bob can append to FileX, can write to FileY, and cannot access FileZ. Write the access control matrix M that specifies the described set of access rights for subjects Alice and Bob to objects FileX, FileY and FileZ.

Exercise 2:
a) What are the basic differences between access control lists (ACL) and capability lists (CList)? Compare these approaches in terms of revocation of a user's access to a particular set of files.
b) Write a set of access control lists for the situation given in exercise 1. With what is each list associated?
c) Write a set of capability lists for the situation given in exercise 1. With what is each list associated?

Exercise 3:
Given the access rights defined in exercise 1, the subject's security levels are L_{Alice} = Confidential and L_{Bob} = Secret, and the object's security levels are L_{FileX} = Unclassified, L_{FileY} = Secret, L_{FileZ} = Top Secret (Top Secret > Secret > Confidential > Unclassified).

a) Draw a Bell-LaPadula model which visualizes the access rights defined in access control matrix M.
b) Using the Bell-LaPadula mode, which of the following actions are allowed? Explain and justify your answer.
   1. Alice reads FileX
   2. Alice reads FileY
   3. Bob appends to FileX
   4. Bob appends to FileZ

Exercise 4: RBAC

Consider a simplified scenario in a bank and the concept of Role-Based Access Control (RBAC). In order to perform a change (transaction) on an account (to mandate deposits and withdrawals), a customer use his card to "unlock" the account (authorize the transaction). He can do this by being registered in the bank in the role of a "Customer" and bringing his chip-card (bank card) to a card reader. The account of this customer is then authorized (unlocked) during the duration of this session, and authorized subjects can perform changes to this account. In the following, this kind of account "unlocking" will be denoted as "authorization".

The following roles and their corresponding rights are valid in this scenario:

Role	**Rights**
Bank employee	Read all account data
Base	Read Terms of Use
Auditor	Perform audit
Branch Manager	Open and authorize account(s)' transactions (even without a chip card)
Cashier	Change an authorized account
Client Advisor	Open bank account
Client	Authorize own account

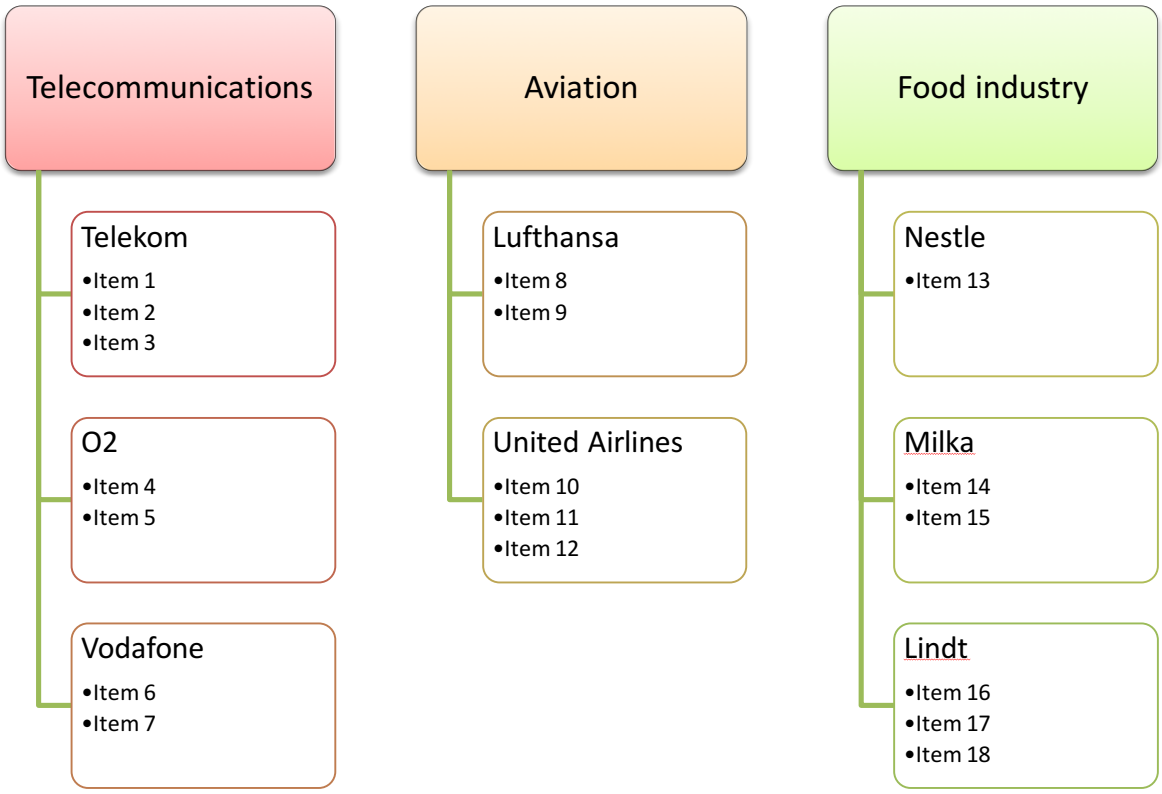
a) draw a role-based access control diagram for this scenario

b) The subject *Cash machine (ATM)* has the role *Cashier*. Can the ATM from this function perform the following?

- *Withdraw cash from an authorized account:* Yes / No
- *Withdraw cash from an unauthorized account:* Yes / No
- *Show account balance*: Yes / No.

Exercise 5:

Take the Chinese Wall Model and the COI classes for three different industries: telecommunications, aviation, and food industry.



a) Which COI classes do you have access to in the beginning?

b) You are assigned to consult and given access to the company datasets of Telekom, Lufthansa, and Lindt. Which individual company files do you have access to now?

c) Which individual files do you not have access to?