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
Ahad Niknia, M.Sc.

E-Mail: security@m-chair.de

Information and Communications Security
WS 2020/21
Assignment 3
Access Control

Please prepare your answers for the following questions before the exercise session on the **8th of December 2020** which we will discuss them.

Exercise 1 (Access Control Matrix)
Alice can read file X, can append to file Y, and can write to file Z. Bob can append to file X, can write to file Y, and cannot access file Z. Write the access control matrix M that specifies the described set of access rights for subjects Alice and Bob to objects file X, file Y and file Z.

Exercise 2 (Access Control Lists and Capability Lists)
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 (Bell-LaPadula Model)
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 $L_{file\ A}$ = Unclassified, $L_{file\ B}$ = Secret, $L_{file\ C}$ = 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 model, which of the following actions are allowed? Explain and justify your answer.
1. Alice reads file X
2. Alice reads file Y
3. Bob appends to file X
4. Bob appends to file Z

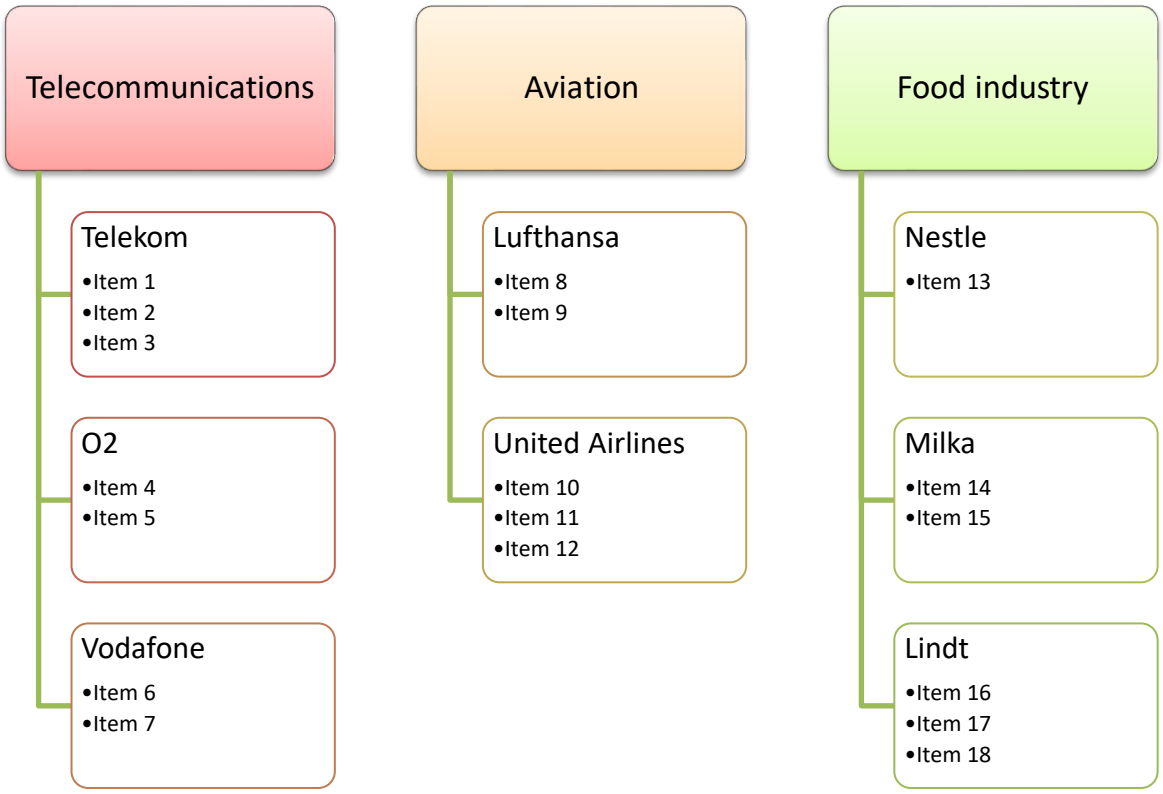
Exercise 4 (Role-Based Access Control)
Consider a simplified scenario in a bank and the concept of RBAC. In order to perform a change (transaction) on an account (to mandate deposits and withdrawals), a customer uses his card to authorize the transaction. He can do this by being registered in the bank in the role of a "client" and using his bank card with a card reader. The account of this customer then is authorized for the duration of this session, and authorized subjects can perform changes to this account.

The following roles and corresponding rights are defined 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 an RBAC diagram for this scenario.
b) The subject *cash machine (ATM)* has the role *cashier*. Can it perform the following actions?
- **(1)** Withdraw cash from an authorized account
- **(2)** Withdraw cash from an unauthorized account
- **(3)** Show account balance

Exercise 5 (Chinese Wall Model)
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?