Assignment 2:

Access Control

Information and Communications Security
(SS 2016)

Prof. Dr. Kai Rannenberg

M.Sc. Ahmed S. Yesuf

Deutsche Telekom Chair of Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt a. M.
www.m-chair.de

Exercise 1: Access Control Matrix

Exercise 2: Access Control Lists and Capability Lists

Exercise 3: Bell-LaPadula Model - Example 1

Exercise 5: Role Based Access Control

Exercise 5: Chinese Wall Model

Exercise 1: Access Control Matrix

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.

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.

1. 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.

	FileX	FileY	FileZ
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

Exercise 2

2 a) What are the basic differences between **access control lists** (ACL) and **capability lists** (CLists)? Compare these approaches in terms of revocation of a user's access to a particular set of files.

- **Capability lists** are subject-focused:
  - For each subject, there is a list of objects
- **Access control lists** are object-focused.
  - For each object, there is a list of subjects

→ Therefore, revocation of an user's access to a particular file is easy when capability lists are used

Exercise 2

	FileX	FileY	FileZ
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

2 b) Write a set of **access control lists** for the situation given in exercise 1.

- **ACL(FileX) =** Alice: {read}, Bob: {append}
- **ACL(FileY) =** Alice: {append}, Bob: {write}
- **ACL(FileZ) =** Alice: {write}, Bob: {}

	FileX	FileY	FileZ
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

Exercise 2

2 c) Write a set of **capability lists** for the situation given in exercise 1.

- **CList(Alice)** = FileX: {read}, FileY: {append}, FileZ: {write}
- **CList(Bob)** = FileX: {append}, FileY: {write}, FileZ: {}

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,

the object's security levels are

L_{FileX} = Unclassified,
L_{FileY} = Secret,
L_{FileZ} = Top Secret.

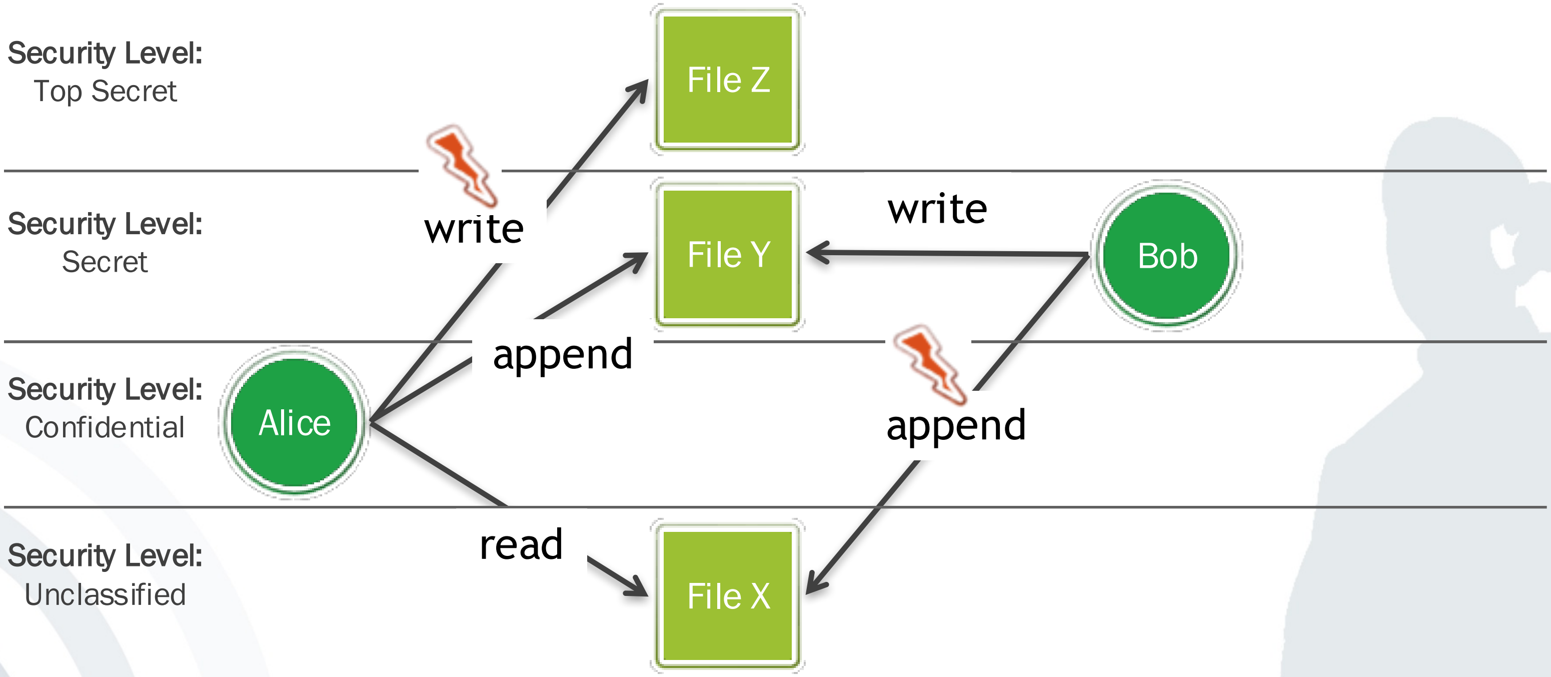
Top Secret > Secret > Confidential > Unclassified

	File X	File Y	File Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

Exercise 3

Subjects' Level: L_{Alice} = Confidential, L_{Bob} = Secret
Objects ' Level : L_{FileX} = Unclassified, L_{FileY} = Secret, L_{FileZ} = Top Secret

3 a) Draw a Bell-LaPadula model which visualizes the access rights defined in access control matrix M.



	File X	File Y	File Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

Exercise 3

Subjects’ Level: L_{Alice} = Confidential, L_{Bob} = Secret
Objects ’ Level : L_{FileX} = Unclassified, L_{FileY} = Secret, L_{FileZ} = Top Secret

3 b) 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

	FileX	FileY	FileZ
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

Exercise 3

Subjects' Level: L_{Alice} = Confidential, L_{Bob} = Secret
Objects ' Level : L_{FileX} = Unclassified, L_{FileY} = Secret, L_{FileZ} = Top Secret

1. Alice reads FileX

- Access Control Matrix:

	FileX	FileY	FileZ
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

Condition: read ∈ M(Alice, FileX) → ✓

- Security Levels:

Condition: $L_{Alice} \geq L_{FileX}$ → ✓

L_{Alice} = Confidential, L_{FileX} = Unclassified

→ **Grant access** ✓

	FileX	FileY	FileZ
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

Exercise 3

Subjects' Level: L_{Alice} = Confidential, L_{Bob} = Secret
Objects ' Level : L_{FileX} = Unclassified, L_{FileY} = Secret, L_{FileZ} = Top Secret

2. Alice reads FileY

- Access Control Matrix:

	FileX	FileY	FileZ
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

Condition: read ∈ M(Alice, FileY) → ✗

- Security Levels:

Condition: $L_{Alice} \geq L_{FileY}$ → ✗
L_{Alice} = Confidential, L_{FileY} = Secret

→ **Deny access** ✗

	FileX	FileY	FileZ
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

Exercise 3

Subjects' Level: L_{Alice} = Confidential, L_{Bob} = Secret
Objects ' Level : L_{FileX} = Unclassified, L_{FileY} = Secret, L_{FileZ} = Top Secret

3. Bob appends to FileX

- Access Control Matrix:

	FileX	FileY	FileZ
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

Condition: append $\in$ M(Bob, FileX) → ✓

- Security Levels:

Condition: $L_{Bob} \leq L_{FileX}$ → ✗
L_{Bob} = Secret, L_{FileX} = Unclassified

→ **Deny access** ✗

Exercise 3

	FileX	FileY	FileZ
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

Subjects' Level: L_{Alice} = Confidential, L_{Bob} = Secret
Objects ' Level : L_{FileX} = Unclassified, L_{FileY} = Secret, L_{FileZ} = Top Secret

4. Bob appends to FileZ

- Access Control Matrix:

	FileX	FileY	FileZ
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

Condition: append ∈ M(Bob, FileZ) → ✗

- Security Levels:

Condition: $L_{Bob} \leq L_{FileZ}$ → ✓

L_{Bob} = Secret, L_{FileZ} = Top Secret

→ Deny access ✗

Exercise 4: Role Based Access Control (RBAC)

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 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”.

Exercise 4 - RBAC (2)

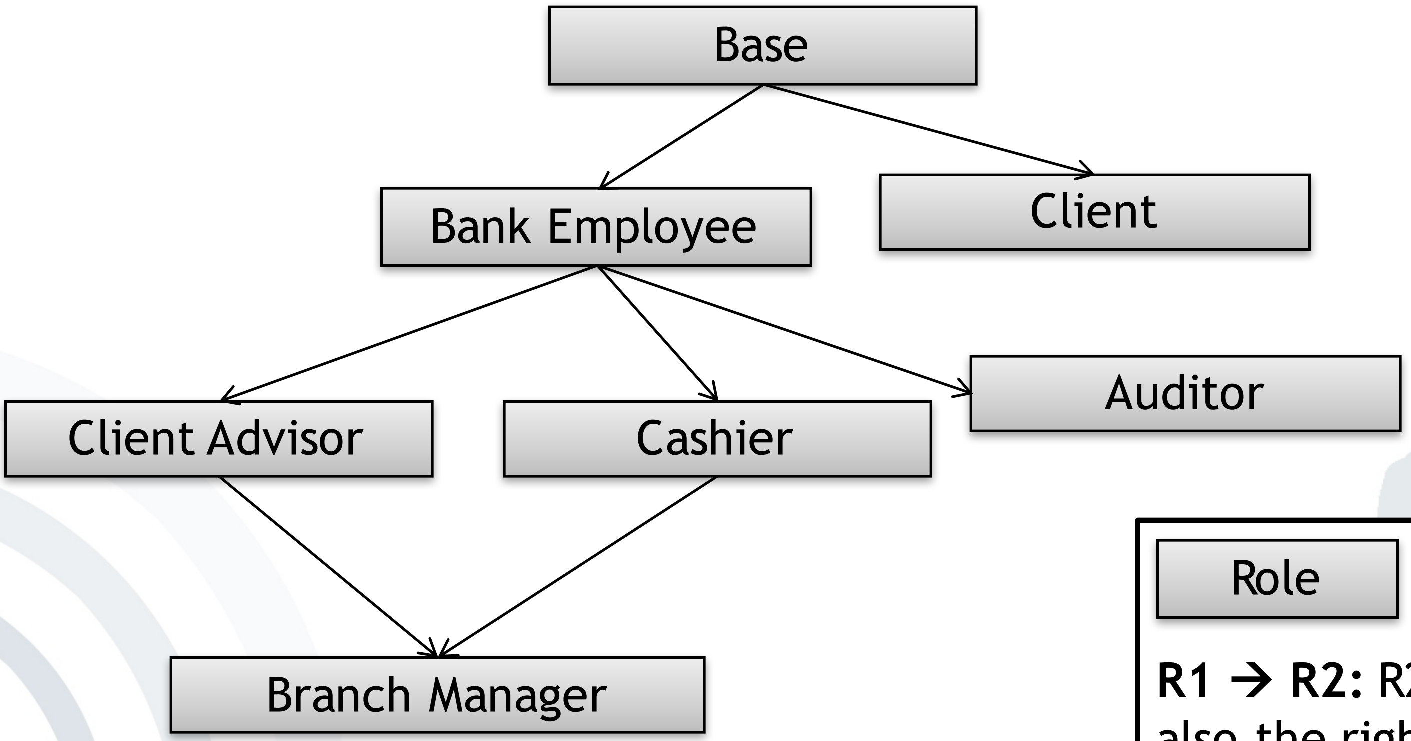
The following roles and their corresponding rights are valid in this scenario:

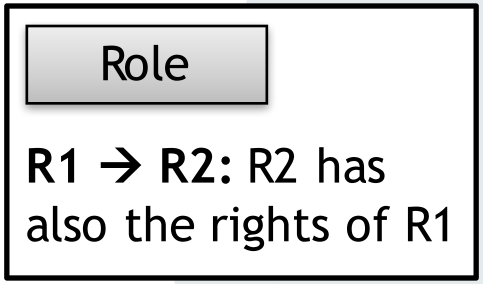
Role	**Rights**
Bank employee	Read all account data
Base	Read Terms of Use
Auditor	Perform audit
Branch Manager	Open and authorize account(s)' transactions (even without a chip card)
Cashier	Change an authorized account
Client Advisor	Open bank account
Client	Authorize own account

Exercise 4 – RBAC (3)

Roles: Bank employee, Base, Auditor, Branch Manager, Cashier, Client Advisor, Client.

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





R1 → R2: R2 has also the rights of R1

Exercise 4 – RBAC (4)

Roles: Bank employee, Base, Auditor, Branch Manager, Cashier, Client Advisor, Client.

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

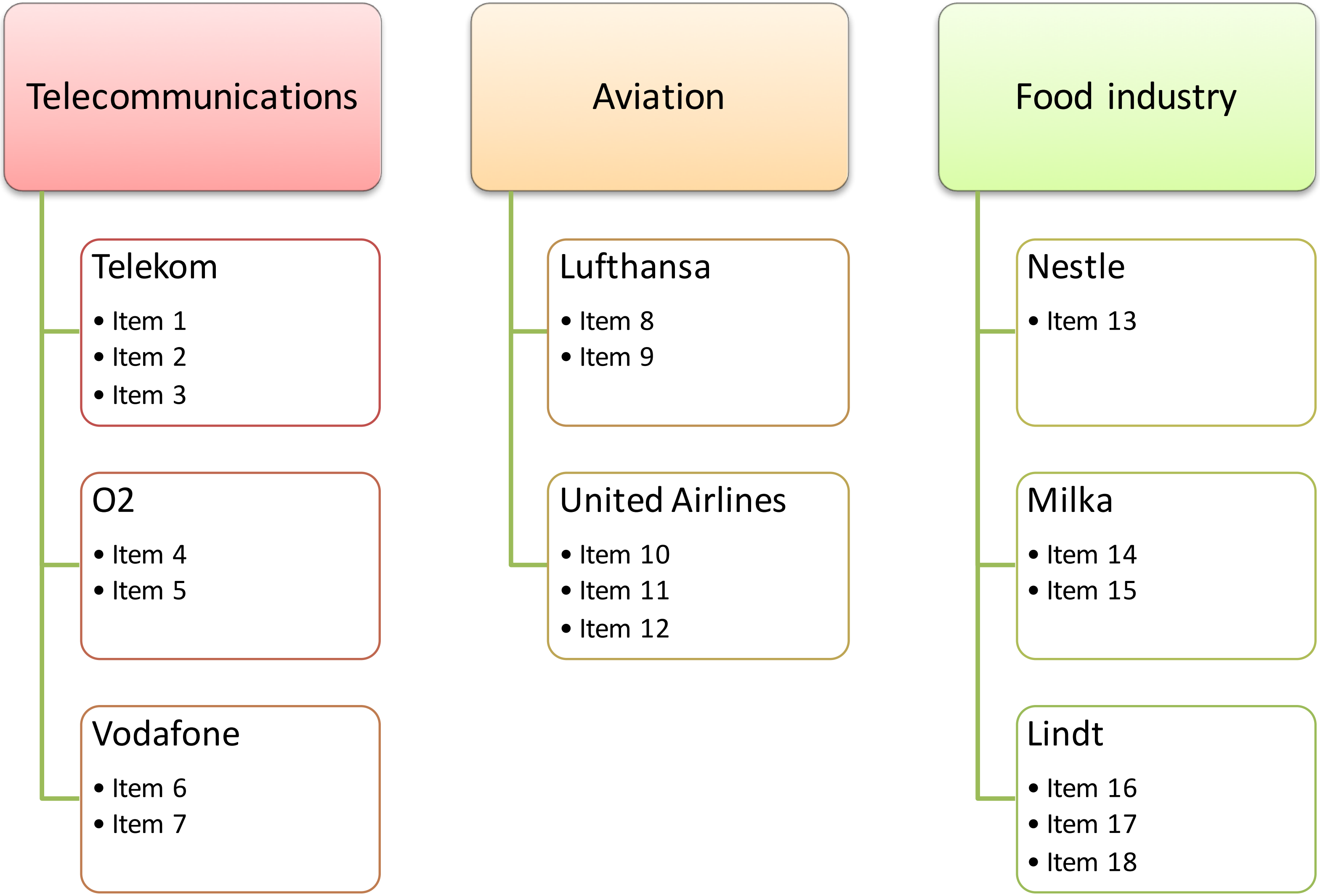
- Withdraw cash from an authorized account: ✔
- Withdraw cash from an unauthorized account: ✖
- Show account balance: ?

Exercise 5: Chinese Wall Model

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

Chinese Wall Model (1)

5a) Which COI classes do you have access to in the beginning?



Telecommunications

- Telekom
  - Item 1
  - Item 2
  - Item 3
- O2
  - Item 4
  - Item 5
- Vodafone
  - Item 6
  - Item 7

Aviation

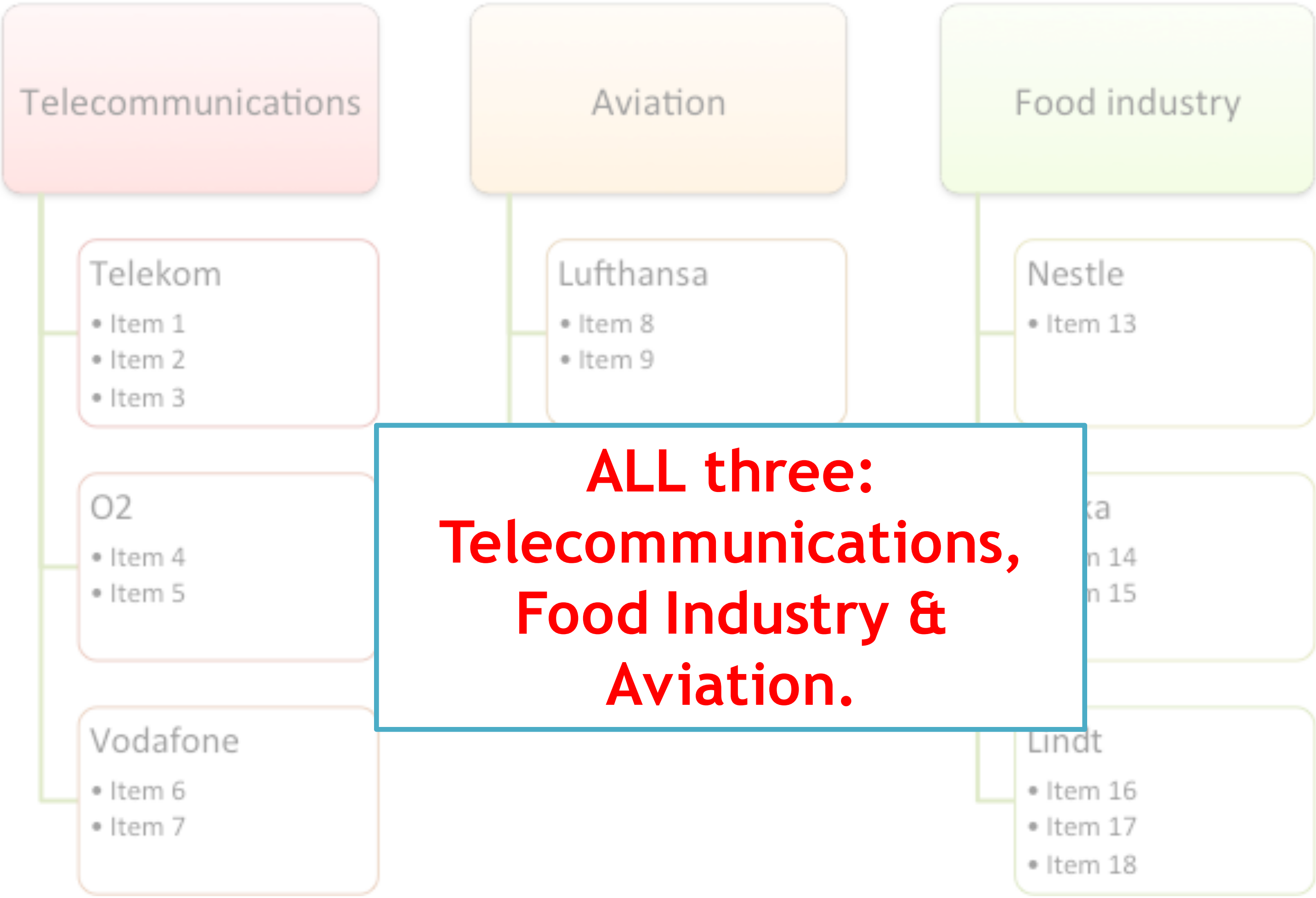
- Lufthansa
  - Item 8
  - Item 9
- United Airlines
  - Item 10
  - Item 11
  - Item 12

Food industry

- Nestle
  - Item 13
- Milka
  - Item 14
  - Item 15
- Lindt
  - Item 16
  - Item 17
  - Item 18

Exercise 5 – Chinese Wall Model

5a) Which COI classes do you have access to in the beginning?



Telecommunications

Telekom
- Item 1
- Item 2
- Item 3

O2
- Item 4
- Item 5

Vodafone
- Item 6
- Item 7

Aviation

Lufthansa
- Item 8
- Item 9

Food industry

Nestle
- Item 13

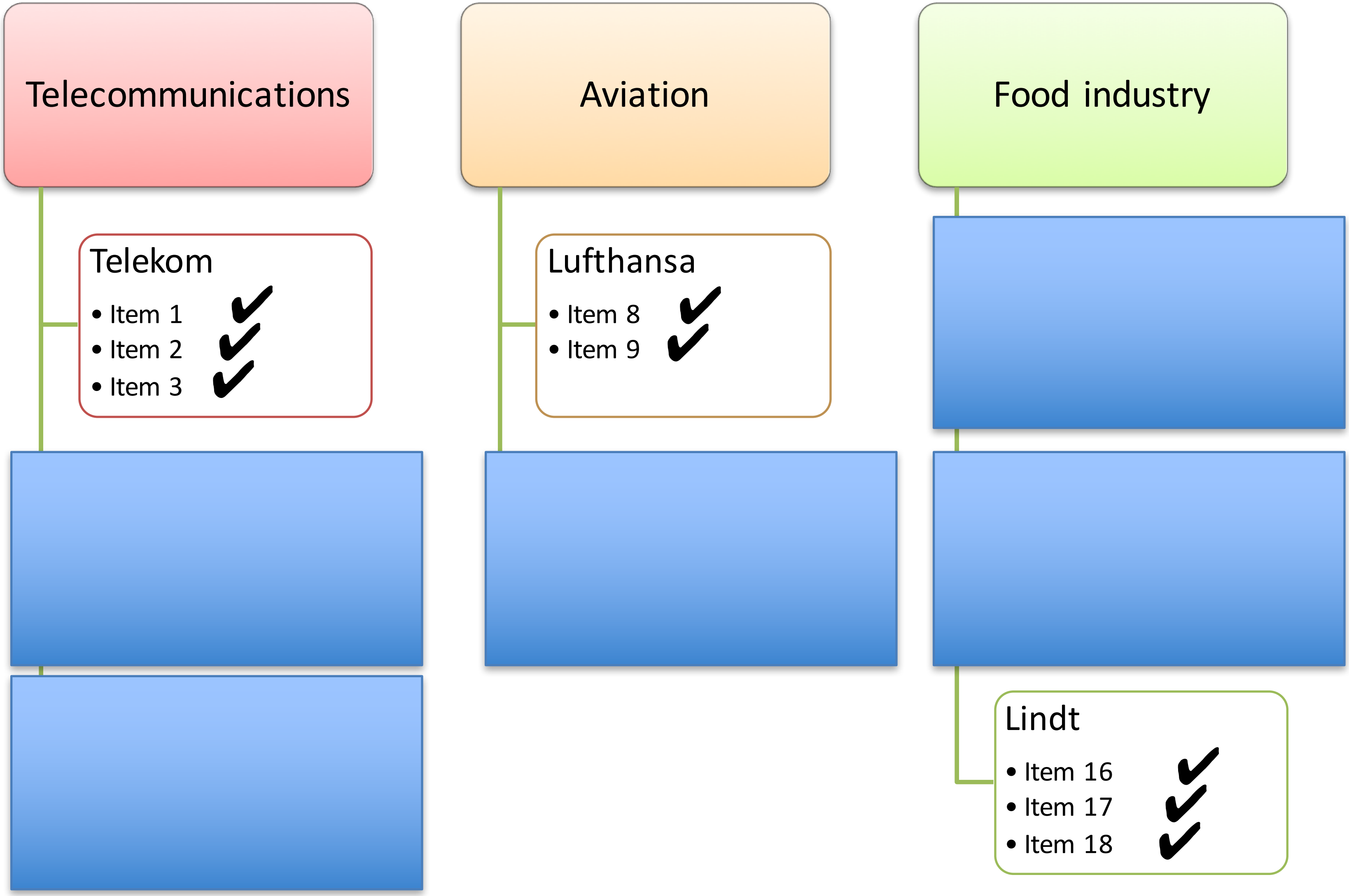
ka
- n 14
- n 15

Lindt
- Item 16
- Item 17
- Item 18

ALL three: Telecommunications, Food Industry & Aviation.

Chinese Wall Model (2)

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 and which not?**



Telecommunications

Telekom
- Item 1 ✓
- Item 2 ✓
- Item 3 ✓

Aviation

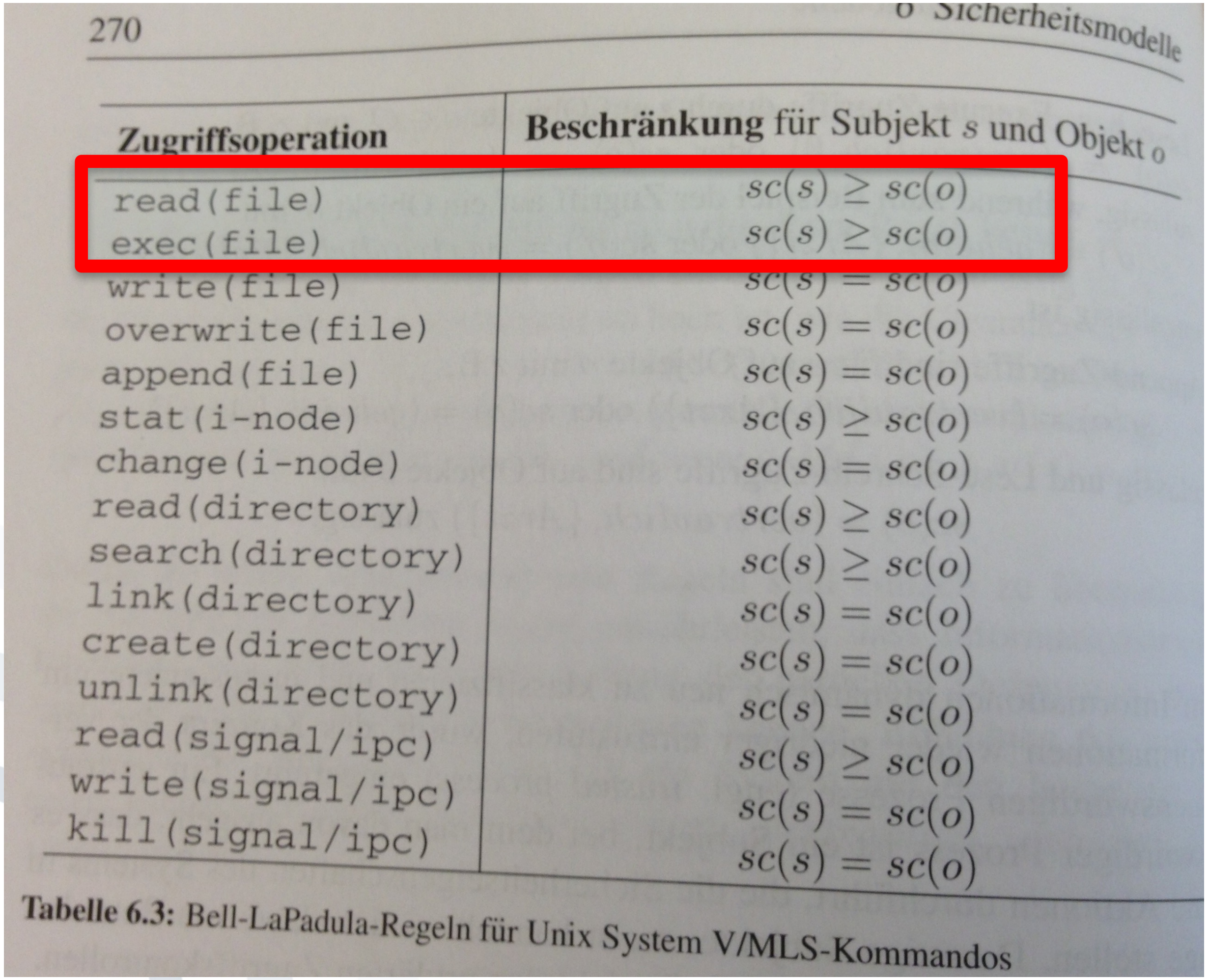
Lufthansa
- Item 8 ✓
- Item 9 ✓

Food industry

Lindt
- Item 16 ✓
- Item 17 ✓
- Item 18 ✓

Misc:

- Bell-LaPadula and Execution rights



270 6 Sicherheitsmodelle

Zugriffsoperation	Beschränkung für Subjekt s und Objekt o
`read(file)`	$sc(s) \geq sc(o)$
`exec(file)`	$sc(s) \geq sc(o)$
`write(file)`	$sc(s) = sc(o)$
`overwrite(file)`	$sc(s) = sc(o)$
`append(file)`	$sc(s) = sc(o)$
`stat(i-node)`	$sc(s) \geq sc(o)$
`change(i-node)`	$sc(s) = sc(o)$
`read(directory)`	$sc(s) \geq sc(o)$
`search(directory)`	$sc(s) \geq sc(o)$
`link(directory)`	$sc(s) = sc(o)$
`create(directory)`	$sc(s) = sc(o)$
`unlink(directory)`	$sc(s) = sc(o)$
`read(signal/ipc)`	$sc(s) \geq sc(o)$
`write(signal/ipc)`	$sc(s) = sc(o)$
`kill(signal/ipc)`	$sc(s) = sc(o)$

Tabelle 6.3: Bell-LaPadula-Regeln für Unix System V/MLS-Kommandos

Claudia Eckert. *IT-Sicherheit*. München, Wien: Oldenbourg, 2004

Job Offer
Student Assistant

The **Chair of Mobile Business & Multilateral Security** offers jobs for student workers (m/f) who are interested in a long-term cooperation, to strengthen the team of the TREsPASS (Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security) project.

What we offer to you:

- An interesting, varied and practical work
- Insights into current research topics in the fields of Mobile Business, Information Security & Privacy, and Identity Management
- The opportunity for independent and flexible work
- Participation in the organization and execution of user studies for different typesf of prototypes

What we expect from you:

- Good knowledge of systems security (socio-technical systems security in particular) or Information security
- Systematic literature search in scientific literature databases
- Self-management and the willingness to become familiar with new topics independently
- Students from computer science or related background (optional)
- Good skills in English
- Motivation and enjoyment of work
- Skills in the following areas are of advantage:
  - Programing skills in Java, C#, C++, …
  - Software development, esp. for Microsoft Office and/or smartphone applications (e.g. VBA macros, Android, iOS, Web Apps)
  - Document markup and preparation with LaTeX, reference management (e.g. BibTeX, Mendeley, Citavi)
  - Web Content Management (e.g. TYPO3, Joomla)

Applicants are requested to send their application documents to:
ahmed.yesuf@m-chair.de

www.m-chair.de | www.twitter.com/mchair