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.net

Prof. Dr. Kai Rannenberg
M.Sc. Christopher Schmitz
M.Sc. Fatbardh Veseli
M.Sc. Ahmed S. Yesuf

E-Mail sec@m-chair.net

Information and Communications Security WS 14/15 Assignment 2 *Access Control* Solution

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.

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

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.

- Access control lists are object-focused. For each object, there is a list of subjects.
- Capability lists are subject-focused. For each subject, there is a list of objects.
- When using access control lists, one would have to enumerate through the access control lists for each file in the set and delete the user from that file's ACL. Using capability lists, one would directly get the user’s capability list. So one could easily see and revoke the user’s access rights to a particular set of files. ACLs require accessing and updating multiple ACLs (one per file), whereas CLists require accessing and updating one CList (the user's).

b) Write a set of access control lists for the situation given in exercise 1. With what is each list associated?

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

ACCREDITED AACSB INTERNATIONAL

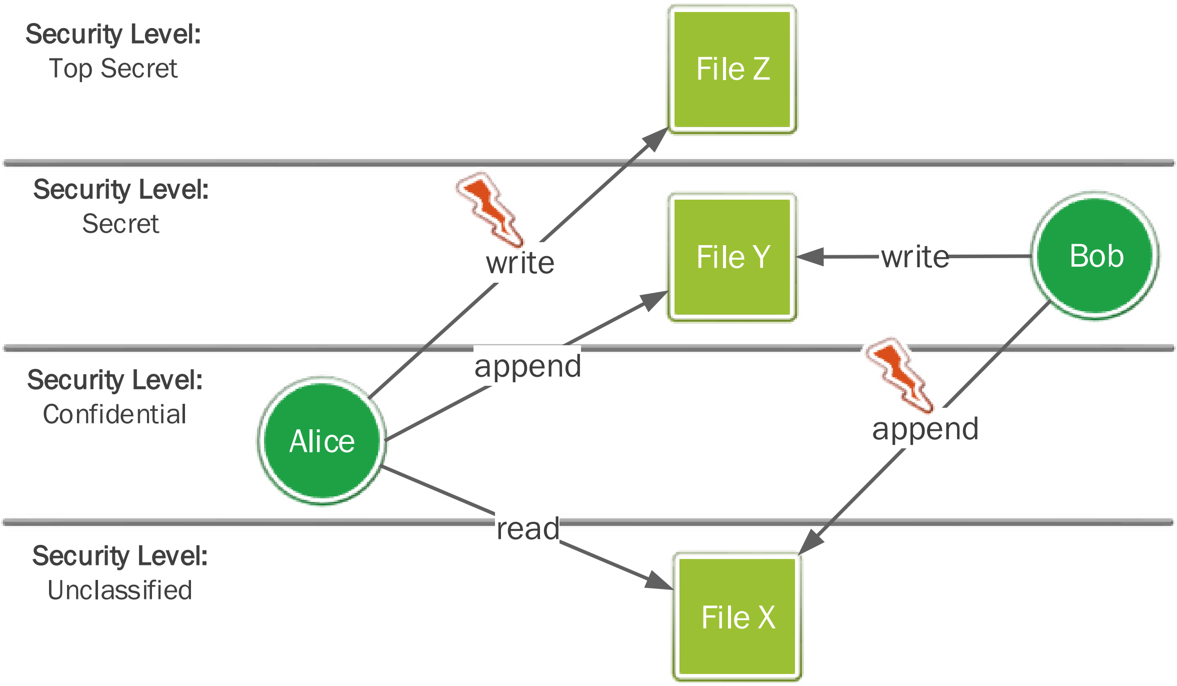
c) Write a set of capability lists for the situation given in exercise 1. With what is each list associated?

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

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) Which of the following actions are allowed? Explain and justify your answer.

1. Alice reads FileX

- Access Control Matrix:

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

Condition: read ∈ M(Alice, FileX) → ✓

- Security Levels:

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

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

→ Grant access: Alice is allowed to read FileX ✓

2. **Alice reads FileY**

- Access Control Matrix:

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

Condition: read $\in M(\text{Alice, FileY})$ → ✗

- Security Levels:

L_{Alice} = Confidential, L_{FileY} = Secret

Condition: $L_{\text{Alice}} \geq L_{\text{FileY}}$ → ✗

→ Deny access: Alice is not allowed to read FileY ✗

3. **Bob appends to FileX**

- Access Control Matrix:

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

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

- Security Levels:

L_{Bob} = Secret, L_{FileX} = Unclassified

Condition: $L_{\text{Bob}} \leq L_{\text{FileX}}$ → ✗

→ Deny access: Bob is not allowed to append to FileY ✗

4. **Bob appends to FileZ**

- Access Control Matrix:

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

Condition: append $\in M(\text{Bob, FileZ})$ → ✗

- Security Levels:

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

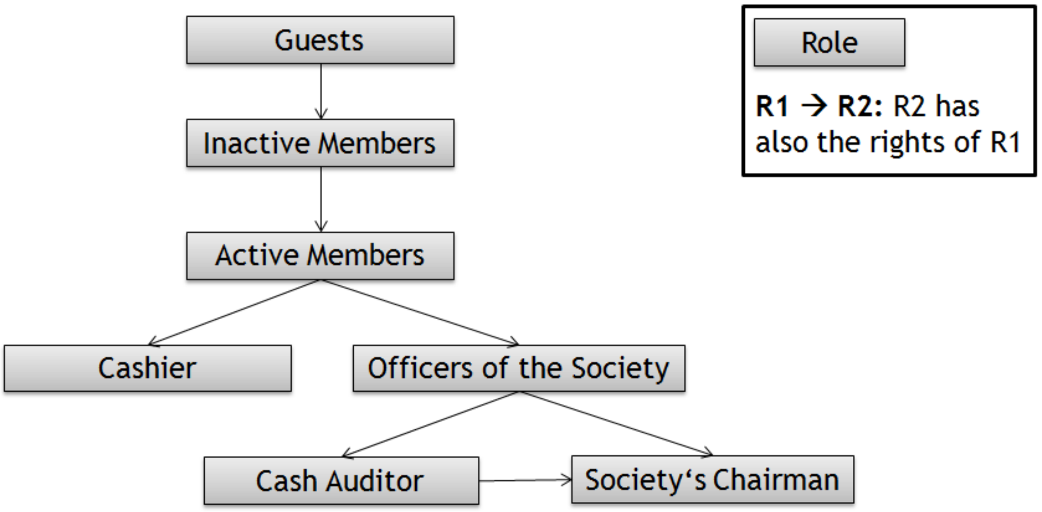
Condition: $L_{\text{Bob}} \leq L_{\text{FileZ}}$ → ✓

→ Deny access: Bob is not allowed to append to FileZ ✗

Exercise 4:

Create a role based access control model for a local society. Bring the following roles in a meaningful hierarchy: Guests, active and inactive members, cashier, cash auditor, and society's chairman.

Note that cashier and cash auditor are always active members, and that the society's chairman and the cash auditor are officers of the society.


Guests
Inactive Members
Active Members
Cashier
Officers of the Society
Cash Auditor
Society‘s Chairman
Role
R1 → R2: R2 has also the rights of R1