

Assignment 2:

Access Control

Information and Communications
Security (SS 2010)

Prof. Dr. Kai Rannenberg

Dr. Ioannis Krontiris

T-Mobile Chair for
Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt a. M.
www.m-chair.net

Authentication Mode

Choose the authentication mode.

Windows Authentication Mode

Mixed Mode (Windows Authentication and SQL Server Authentication)

Add password for the sa login:

Enter password:

Confirm password:

Blank Password (not recommended)

Buttons: Help, < Back, Next >, Cancel

- Which operating system did produce the following directory listing (hint: access control attributes)?

```
-rwxr-xr-x 1 student123 hrz 10764 Nov 27 1993 lsu118
-rw-r--r-- 1 student123 hrz 226 Nov 27 1993 lsu118.c
-rwxr-xr-x 1 student123 hrz 11679 Nov 29 1993 rk
-rw-r--r-- 1 student123 hrz 1624 Jul 18 1994 rk.c
-rwxr-xr-x 1 student123 hrz 12366 Nov 27 1993 t
```

■ UNIX

```

-rwxr-xr-x  1 student123      hrz      10764 Nov 27  1993 lsu118
-rw-r--r--  1 student123      hrz           226 Nov 27  1993 lsu118.c
-rwxr-xr-x  1 student123      hrz     11679 Nov 29  1993 rk
-rw-r--r--  1 student123      hrz           1624 Jul 18  1994 rk.c
-rwxr-xr-x  1 student123      hrz     12366 Nov 27  1993 t
  
```

position	Meaning
1	directory flag, 'd' if a directory, '-' if a normal file
2,3,4	read, write, execute permission for User (Owner) of file
5,6,7	read, write, execute permission for Group
8,9,10	read, write, execute permission for Other

value	Meaning
-	in any position means that flag is not set
r	file is readable by owner, group or other
w	file is writeable. On a directory, write access means you can add or delete files
x	file is executable (only for programs and shell scripts - not useful for data files). Execute permission on a directory means you can list the files in that directory
s	in the place where 'x' would normally go is called the set-UID or set-groupID flag.

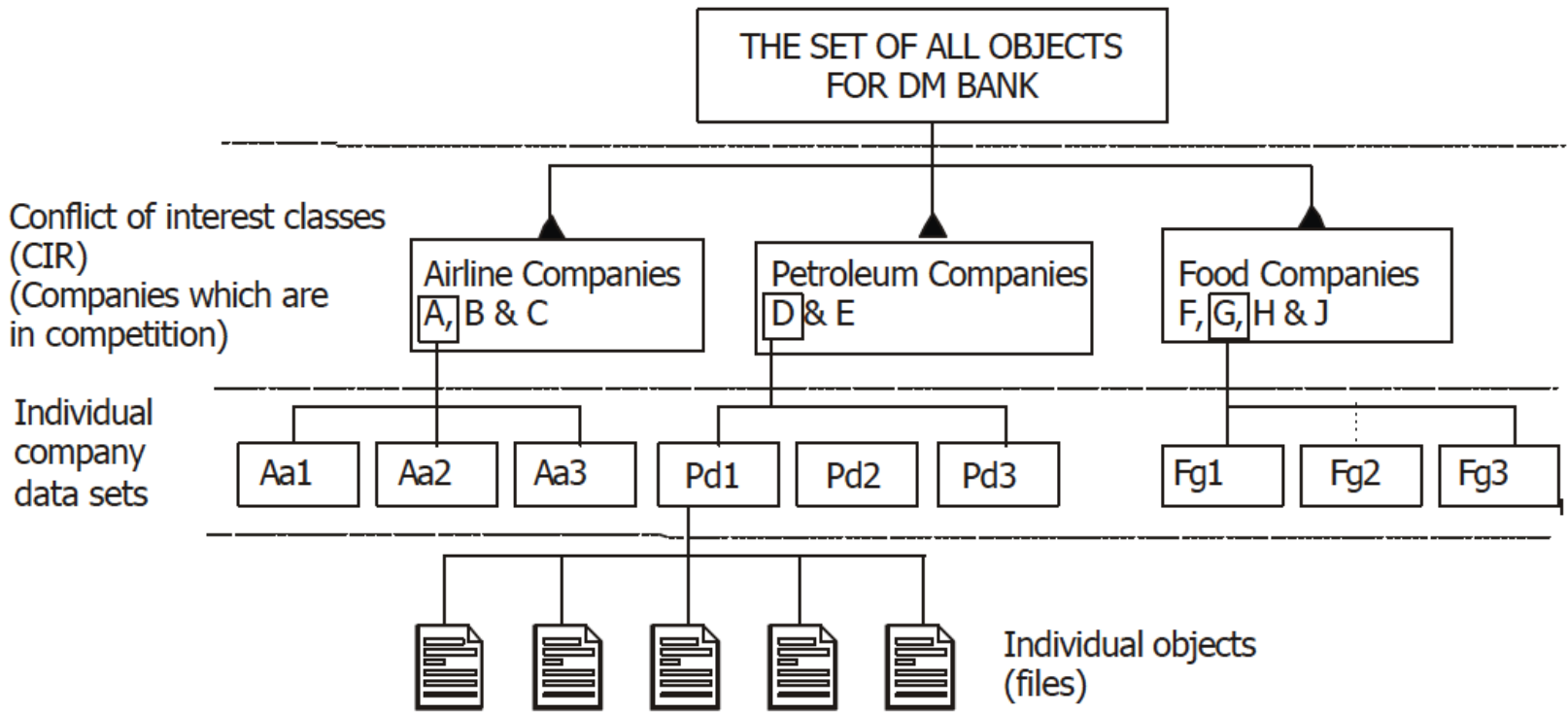
- Windows NT supports multiple file systems, but the protection issues we will consider are only associated with one: NTFS. NTFS permissions are closer to extended permissions in UNIX than to the 9 mode bits. The permission offer a rich set of possibilities:
 - * R -- read
 - * W -- write
 - * X -- execute
 - * D -- delete
 - * P -- modify the ACL
 - * O -- make current account the new owner ("take ownership")
- NT access control is richer than UNIX, but not fundamentally different.

- Alice can read and write to the file x, can read the file y, and can execute the file z. Bob can read x, can read and write to y, and cannot access z.
 - Write a set of access control lists for this situation. Which list is associated with which file?
 - Write a set of capability lists for this situation. What is each list associated with?

- x Alice: read, write; Bob: read
- y Alice: read; Bob: read, write
- z Alice: execute
- Each list is associated with the object

- Alice's capabilities:
 - x: read, write;
 - y: read;
 - z: execute
- Bob's capabilities:
 - x: read;
 - y: read, write;

- Name a fundamental difference between the security model of Bell-LaPadula and the Chinese Wall Model. What are the additional security assets that the Chinese Wall Model is supposed to refer to?
 - The critical difference from Bell-LaPadula is that the Chinese Wall Model needs to retain state in order to keep track of the objects that someone accessed. Initially someone is free to access all objects in the Chinese Wall Model, but then, the more he accesses, the more constrained he becomes. The BLP Model constrains from the beginning the set of objects that someone can access.
 - Bell-LaPadula Model refers only to confidentiality: who can read a message
 - The Chinese Wall (CW) model is a model of a security policy that refers equally to confidentiality: who can read a message
 - and *integrity*: who gets permission to modify a data set.



- The concept of roles has been introduced to you during the last lectures. Please describe this concept briefly.
- A role is a collection of job functions. Each role r is authorized to perform one or more transactions. The set of authorized transactions for r is written $trans(r)$.

- Please assume that you are working for the University of Frankfurt as a research assistant after having received your diploma. Please identify four different roles that you might be authorised to assume. Please note for each identified role one or two problems that might be encountered by a role-based access control model.

- The nature of roles is static, so RBAC lacks flexibility and responsiveness to the environment in which they are used.
- Secondly, RBAC does not encompass the overall context associated with any collaborative activity, so it is a passive security system that serves the function of maintaining permission assignments.
- Thirdly, RBAC lacks the ability to specify a fine-grained control on individual users in certain roles and on individual object instances, so it is not enough for collaborative environments.