Access Control Verification Module

Access control is a critical element of system security. It identifies who is allowed to access which files, as well as what operations that user is allowed to perform. This helps protect the integrity of files in a file sharing environment.

Access Control Matrix

- A column is used to identify a user, and a row to identify a file.
- The corresponding cell contains the access rights a user has for a given file.
- Intuitive and easy to implement.
- Works well for systems with relatively few users and/or few files.
- As number of users and files increase, matrix grows extremely large and may not fit in memory.
- Inefficient use of space due to numerous null entries.
- 4 bits are used to denote **R**ead, **W**rite, **E**xecute, and **D**elete access modes.

	User 1	**User 2**	**User 3**	**User 4**
File 1	RWED	R-E-	----	RWE-
File 2	----	R-E-	R-E-	--E-
File 3	----	RWED	----	--E-
File 4	R-E-	----	----	----

Access Control Lists

- Modification of the Access Control Matrix.
- Each file has a list of 2-tuples comprised of a user and their access rights.
- Only users with access to a given file are in the file list.
- A group entry such as WORLD is listed to denote the group of users denied access.
- Other groups are used such as WHEEL, OWNER, ADMIN, etc. to designate access broadly and reduce list length.
- A file's owner can grant access to other uses.
- By default, only the system administrator can access system files.
- Uses storage space more efficiently than an Access Control Matrix.
- More suitable for systems with a stable user base as every file entry for which a user has access must be modified when the user is removed from the system.
- Most commonly used access control verification module.
- Analogous to a restaurant reservation list with reserved seating assignments.

File	**Access**
File 1	USER1 (RWED), USER2 (R-E-), USER4 (RWE-), WORLD (----)
File 2	USER2 (R-E-), USER3 (R-E-), USER4 (--E-), WORLD (----)
File 3	USER2 (RWED), USER4 (--E-), WORLD (----)
File 4	USER1 (R-E-), WORLD (----)

Capability Lists

- Converse to the Access Control List, each user has a list of 2-tuples comprised of a file and the access rights the user has to the file.
- When users are added to or deleted from the system, capability lists are easier to maintain than Access Control Lists.
- Requires less storage space than an Access Control Matrix.
- Gaining in popularity because Unix-like systems treat everything as a file.
- Analogous to specific concert tickets that are made available only to names on a list.

User	Access
User 1	File 1 (RWED), File 4 (R-E-)
User 2	File 1 (R-E-), File 2 (R-E-), File 3 (RWED)
User 3	File 2 (R-E-)
User 4	File 1 (RWE-), File 2 (--E-), File 3 (--E-)