2.5. Summary

The access control matrix is the primary abstraction mechanism in computer security. In its purest form, it can express any expressible security policy. In practice, it is not used directly because of space requirements; most systems have (at least) thousands of objects and could have thousands of subjects, and the storage requirements would simply be too much. However, its simplicity makes it ideal for theoretical analyses of security problems.

Transitions change the state of the system. Transitions are expressed in terms of commands. A command consists of a possible condition followed by one or more primitive operations. Conditions may involve ownership or the ability to copy a right. The principle of attenuation of privilege leads to the condition that no subject may give a right it does not possess to any other subject.