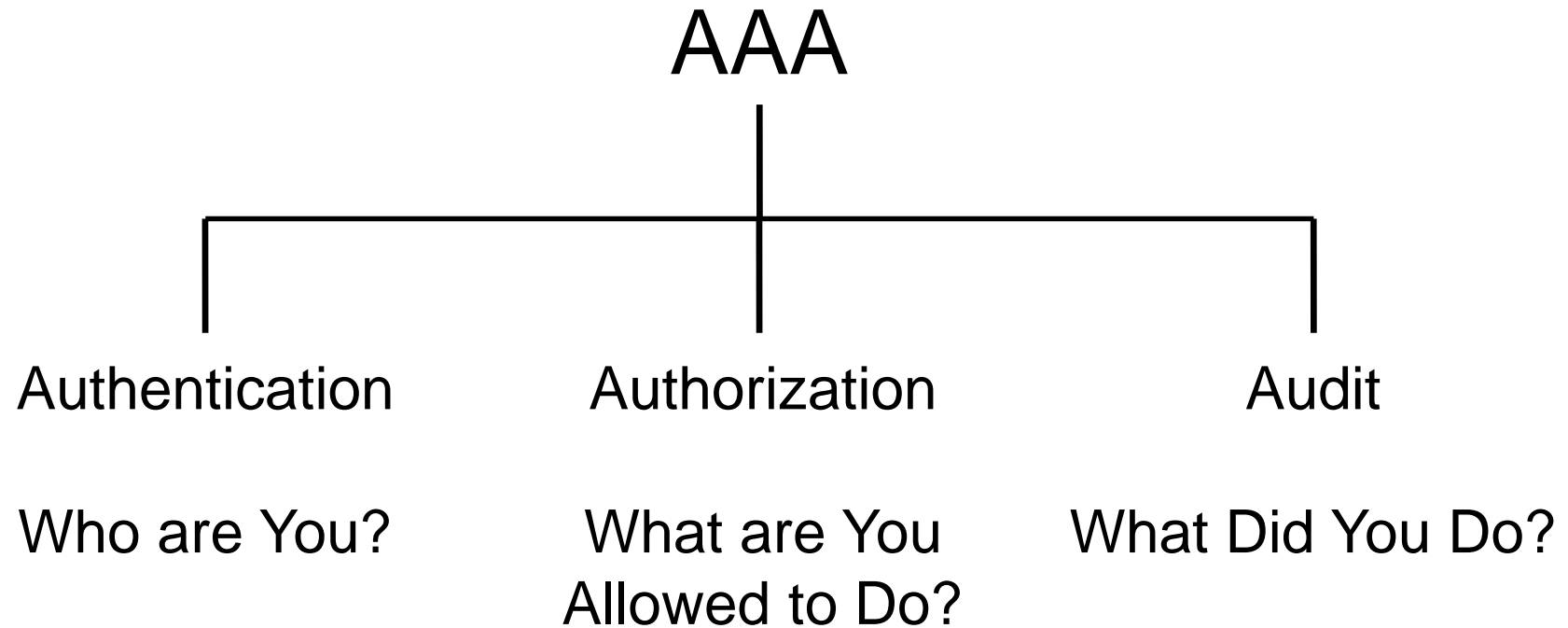


Discretionary Access Control (DAC)

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 7

ravi.utsa@gmail.com
www.profsandhu.com



siloes → **integrated**

**Fixed
policy**



**Discretionary Access Control
(DAC), 1970**

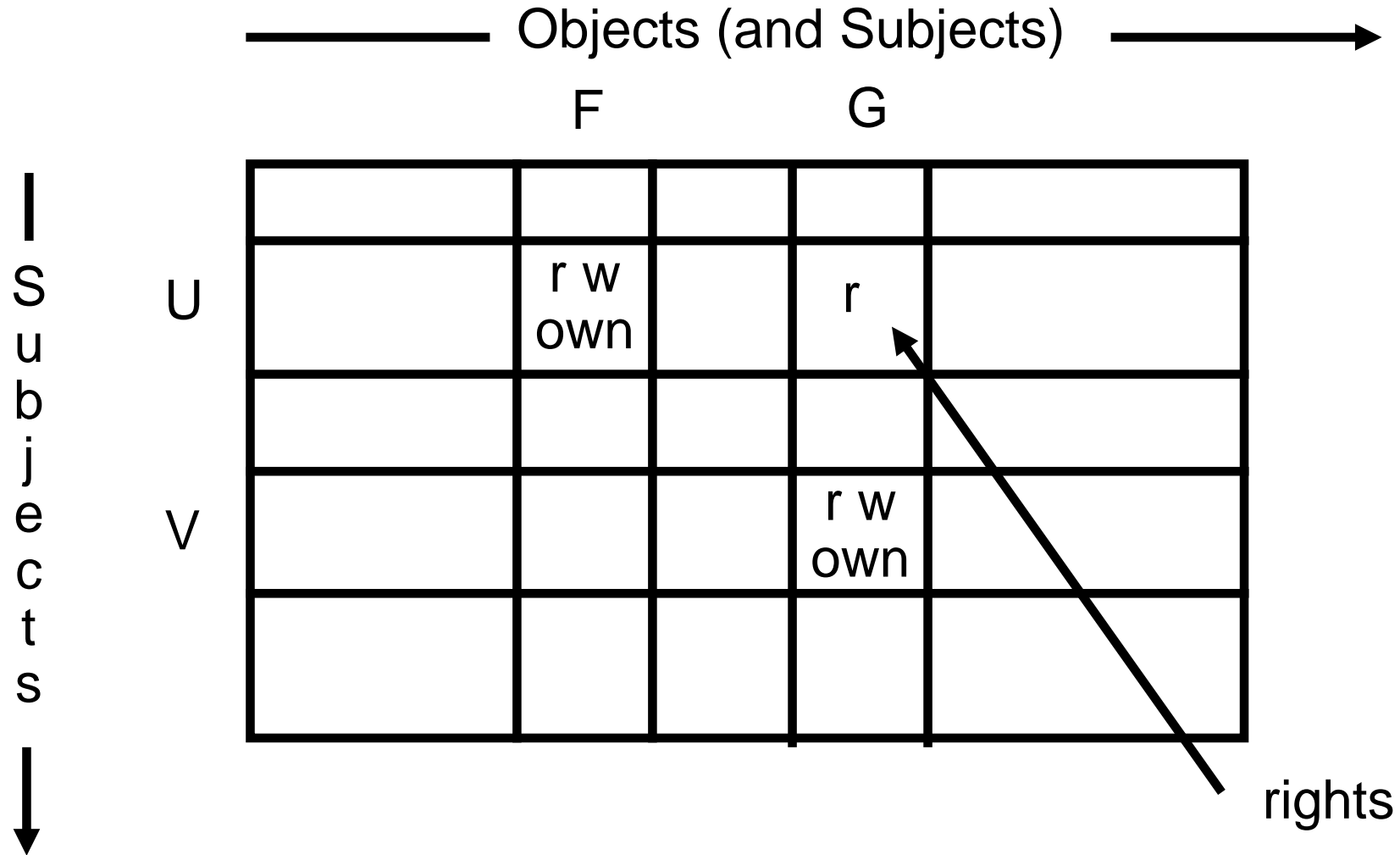
**Mandatory Access Control
(MAC), 1970**

**Role Based Access Control
(RBAC), 1995**

**Attribute Based Access Control
(ABAC), ????**

**Flexible
policy**

Access Matrix Model

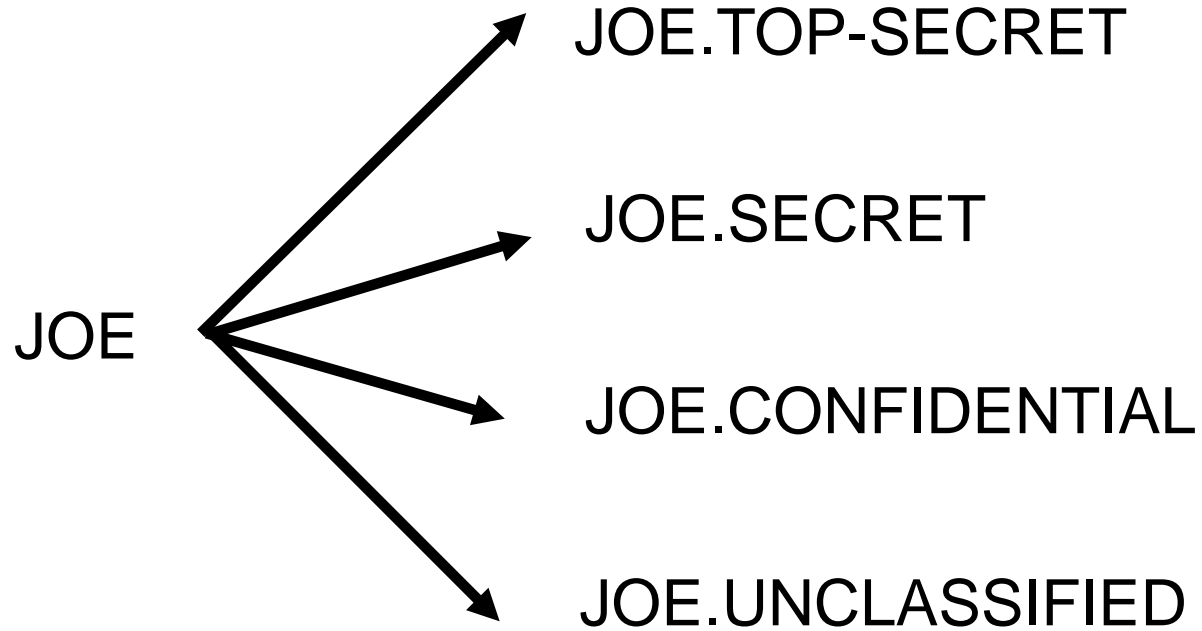


➤ Basic Abstractions

- ❖ Subjects
- ❖ Objects
- ❖ Rights

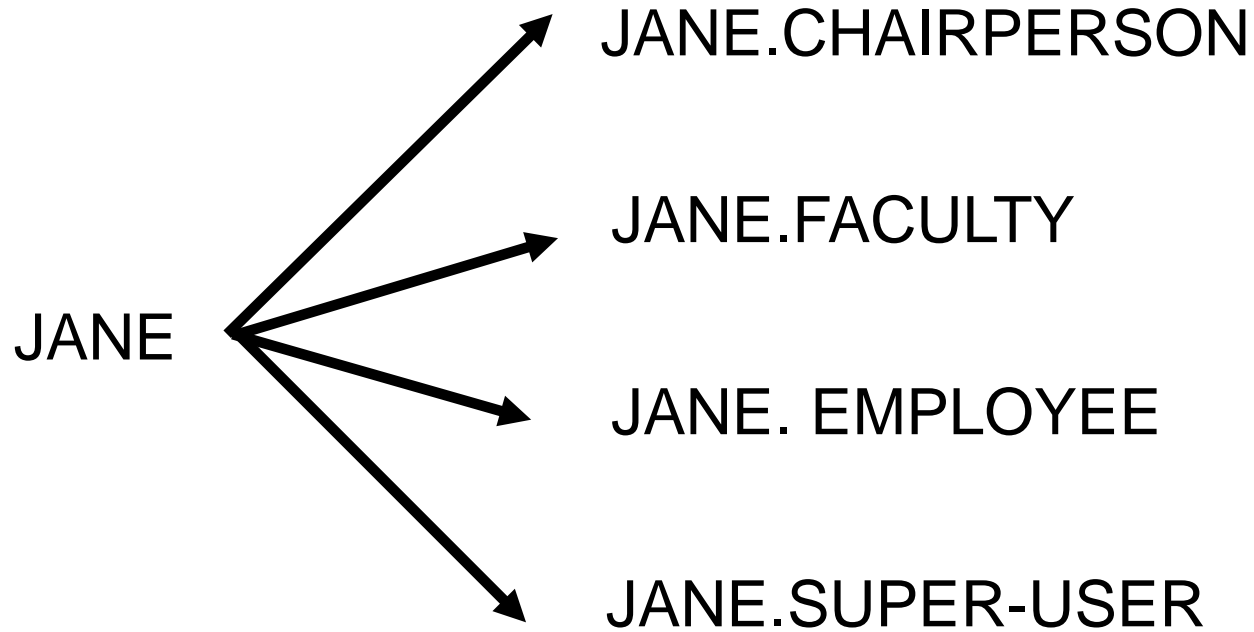
➤ The rights in a cell specify the access of the subject (row) to the object (column)

- A subject is a program (application) executing on behalf of a user
- A user may at any time be idle, or have one or more subjects executing on its behalf
- User-subject distinction is important if subject's rights are different from a user's rights
 - ❖ Usually a subset
 - ❖ In many systems a subject has all the rights of a user
- A human user may manifest as multiple users (accounts, principals) in the system



USER

SUBJECTS



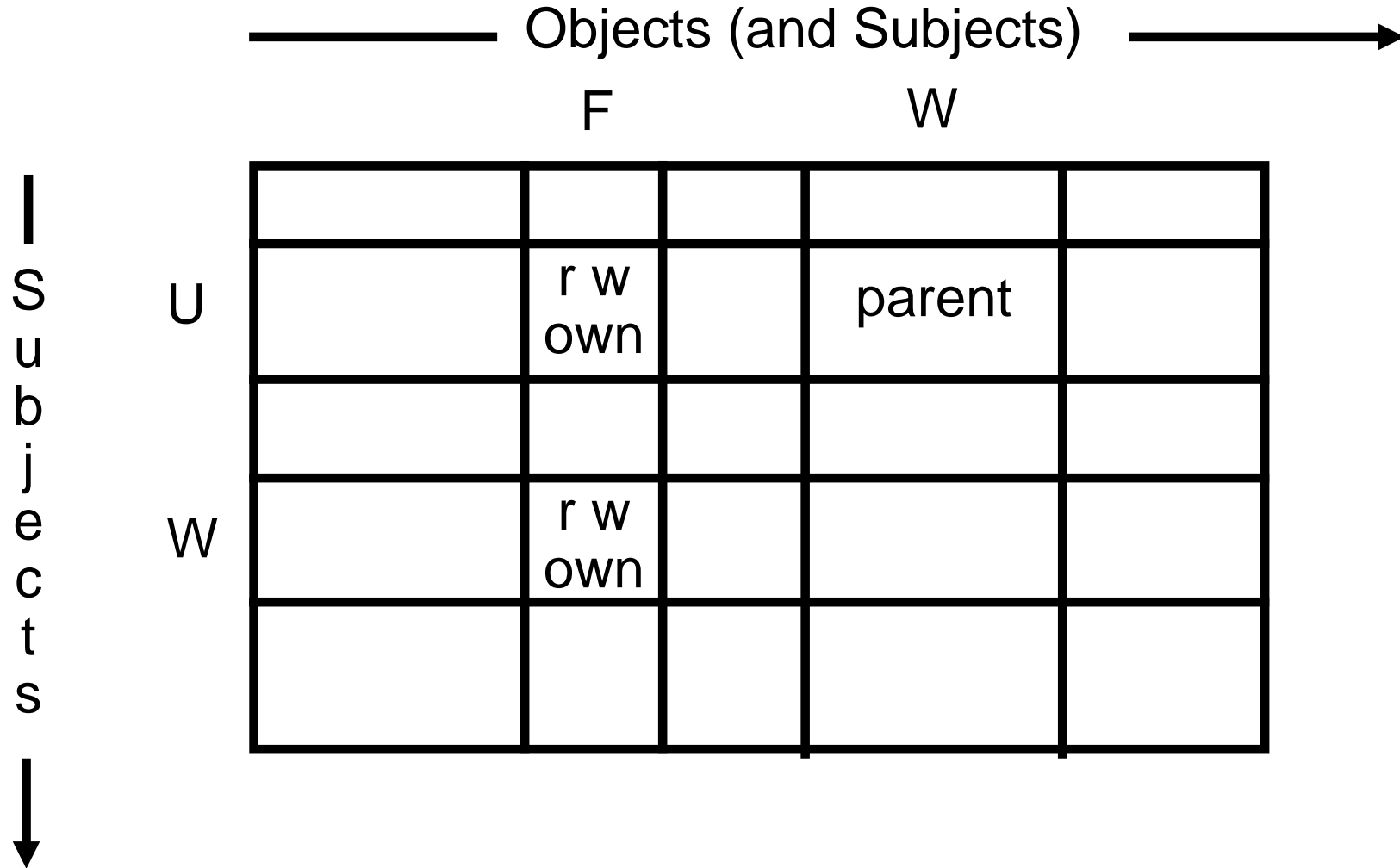
USER

SUBJECTS

- An object is anything on which a subject can perform operations (mediated by rights)

- Usually objects are passive, for example:
 - ❖ File
 - ❖ Directory (or Folder)
 - ❖ Memory segmentwith CRUD operations (create, read, update, delete)

- But, subjects can also be objects, with operations
 - ❖ kill
 - ❖ suspend
 - ❖ resume



- Access Control Lists
- Capabilities
- Relations

F

U:r
U:w
U:own

G

U:r
V:r
V:w
V:own

each column of the access matrix is stored with the object corresponding to that column

U F/r, F/w, F/own, G/r

V G/r, G/w, G/own

each row of the access matrix is stored with the subject corresponding to that row

Subject	Access	Object
U	r	F
U	w	F
U	own	F
U	r	G
V	r	G
V	w	G
V	own	G

commonly used in relational
database management systems

- Authentication
 - ❖ ACL's require authentication of subjects and ACL integrity
 - ❖ Capabilities require integrity and propagation control
- Access review
 - ❖ ACL's are superior on a per-object basis
 - ❖ Capabilities are superior on a per-subject basis
- Revocation
 - ❖ ACL's are superior on a per-object basis
 - ❖ Capabilities are superior on a per-subject basis
- Least privilege
 - ❖ Capabilities provide for finer grained least privilege control with respect to subjects, especially dynamic short-lived subjects created for specific tasks

- Authentication
 - ❖ ACL's require authentication of subjects and ACL integrity
 - ❖ Capabilities require integrity and propagation control
- Access review
 - ❖ ACL's are superior on a per-object basis
 - ❖ Capabilities are superior on a per-subject basis
- Revocation
 - ❖ ACL's are superior on a per-object basis
 - ❖ Capabilities are superior on a per-subject basis
- Least privilege
 - ❖ Capabilities provide for finer grained least privilege control with respect to subjects, especially dynamic short-lived subjects created for specific tasks

Most Operating Systems use ACLs often in abbreviated form: owner, group, world

- content dependent controls
 - ❖ you can only see salaries less than 50K, or
 - ❖ you can only see salaries of employees who report to you

- beyond the scope of Operating Systems and are provided by Database Management Systems

- context dependent controls
 - ❖ cannot access classified information via remote login
 - ❖ salary information can be updated only at year end
 - ❖ company's earnings report is confidential until announced at the stockholders meeting
- can be partially provided by the Operating System and partially by the Database Management System
- more sophisticated context dependent controls such as based on past history of accesses definitely require Database support

- Information from an object which can be read can be copied to any other object which can be written by a subject
- Suppose our users are trusted not to do this deliberately. It is still possible for Trojan Horses to copy information from one object to another.

ACL

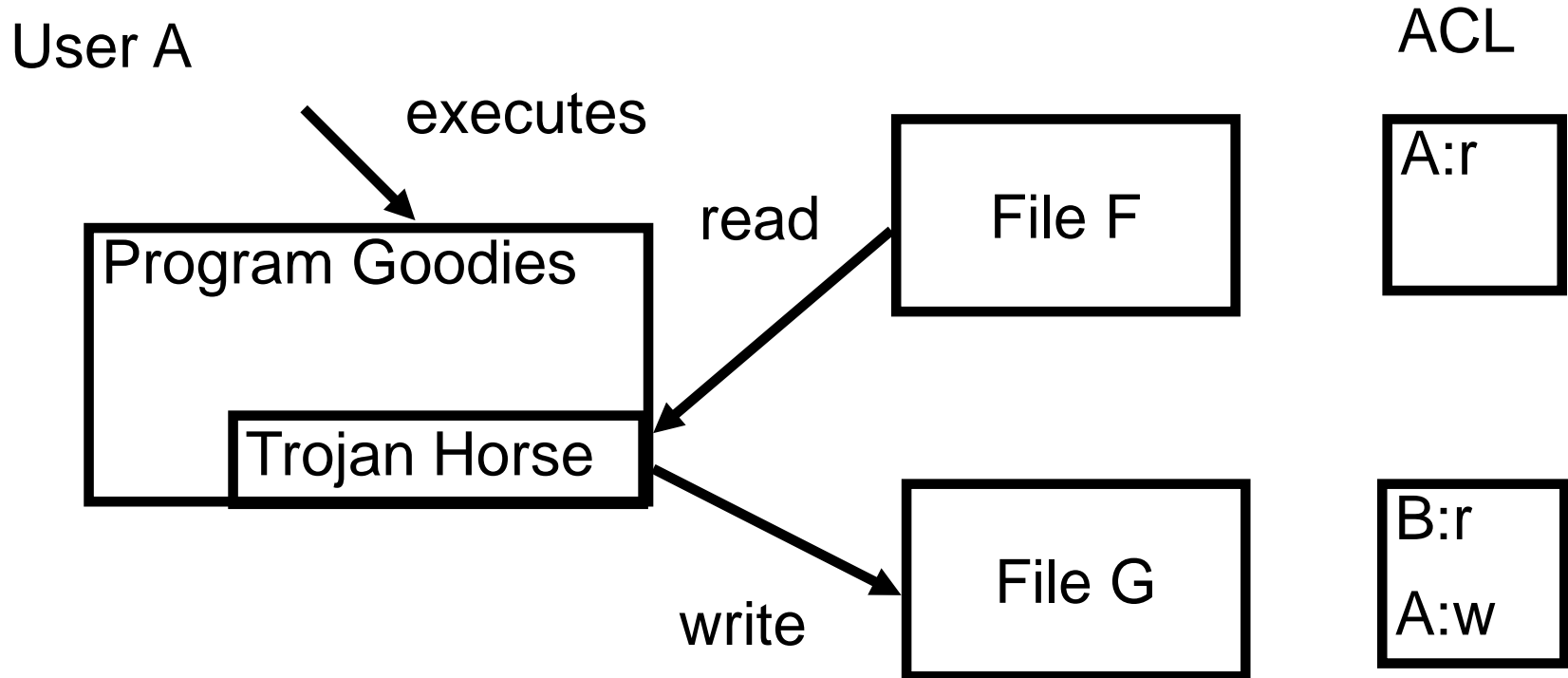
File F

A:r

File G

B:r
A:w

User B cannot read file F



User B can read contents of file F copied to file G

- Read of a digital copy is as good as read of original
- Write to a digital copy is not so useful

- Chains of grants and revokes
- Inheritance of permissions
- Negative rights