Module 3.3
Discretionary Access Control (DAC) and Trojan Horses

Ravi Sandhu

Spring 2021

DAC

- Operational model **Access Matrix**
  - specify the decision function for the access decision triple or quad

- Administrative **DAC**
  - specify the model's dynamics
  - dynamics change the system state and modify the outcome of some access decision triple or quads

DAC

- Operational model — **Access Matrix, MAC, RBAC, ABAC**
  - specify the decision function for the access decision triple or quad
- Administrative — **DAC**
  - specify the model's dynamics
  - dynamics change the system state and modify the outcome of some access decision triple or quads

DAC

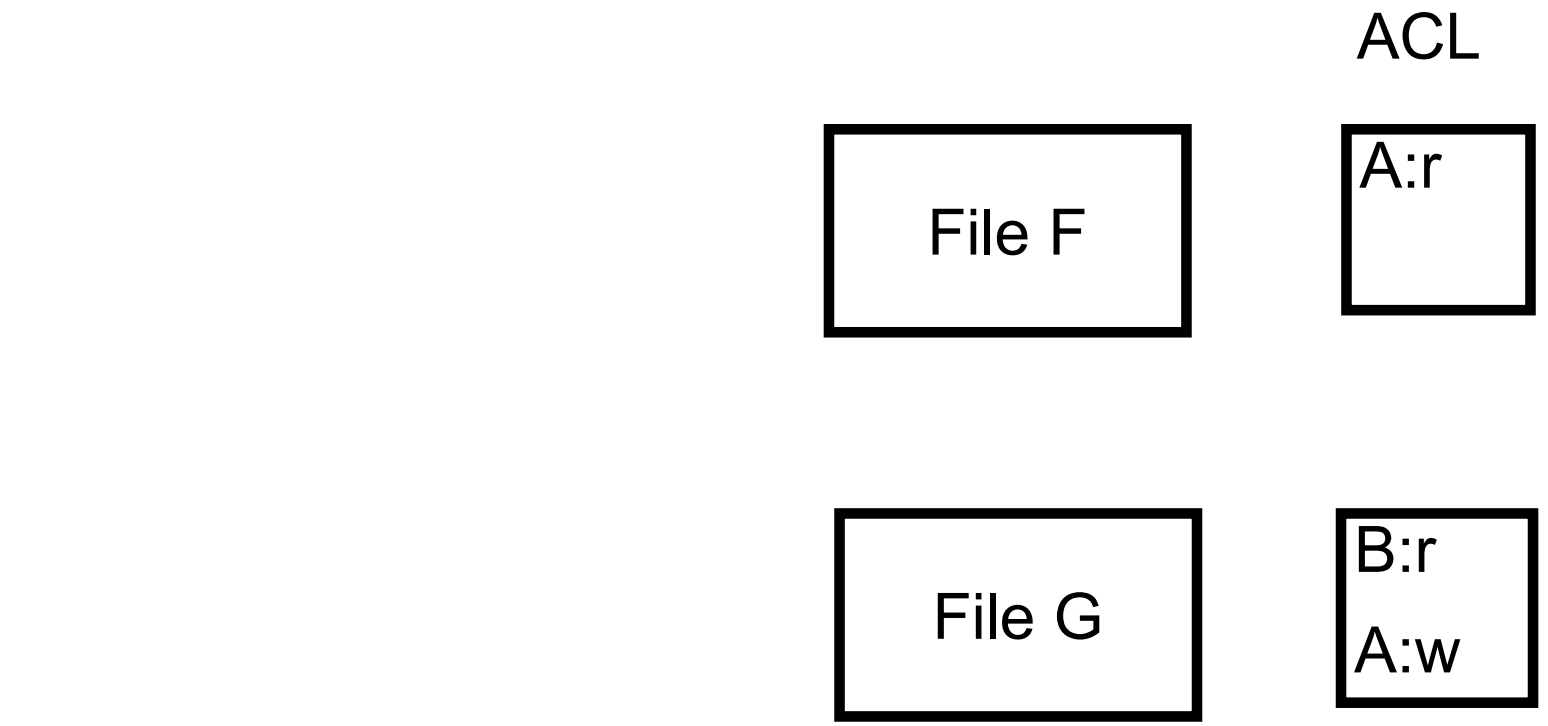
- Core concept:
  - Custodian/owner of resource determines access
- Core drawback:
  - Does not protect copies
  - OK for integrity but not for confidentiality
- Sophistication:
  - Delegation of custody
  - Denials or negative rights
  - Grouping mechanisms
  - Inheritance mechanisms

Trojan Horse Vulnerability of DAC

- Information from an object which can be read can be copied to any other object which can be written by a subject

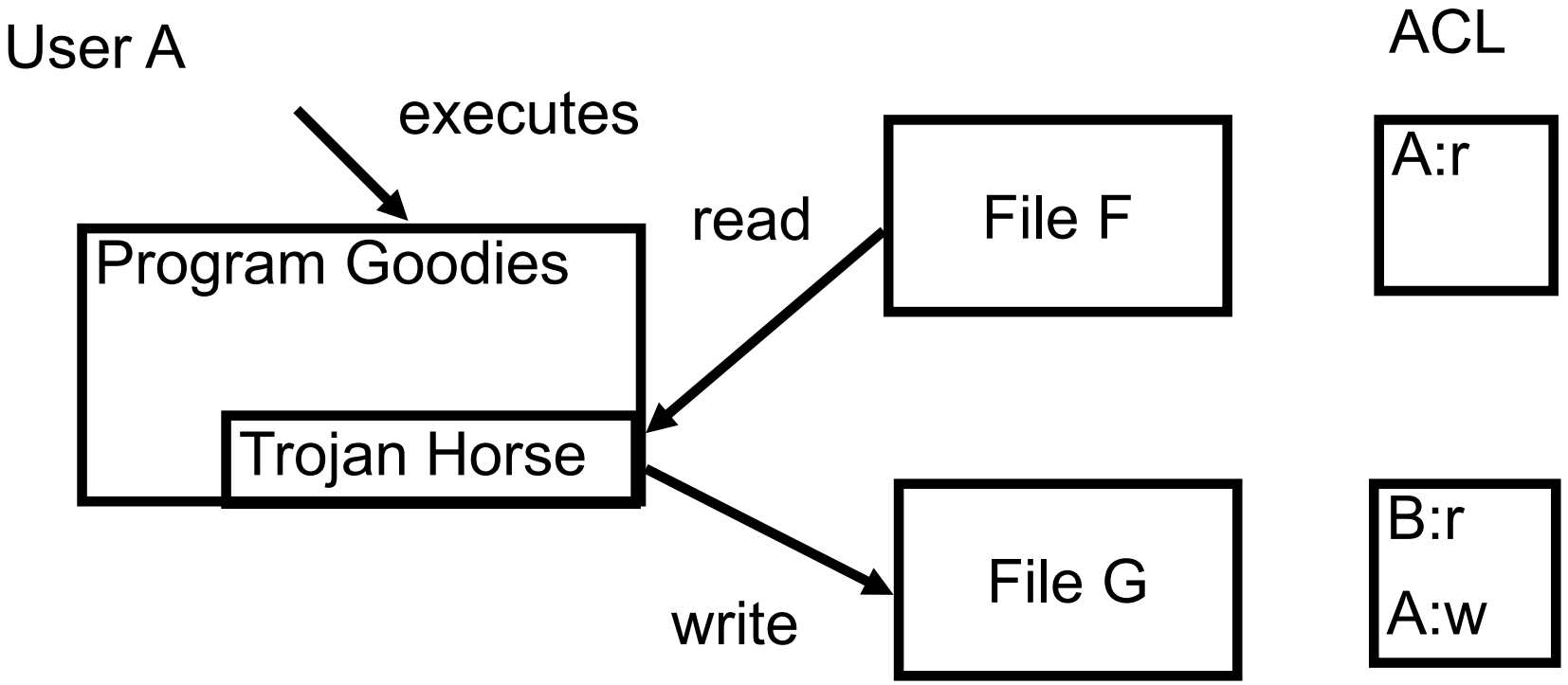
- Suppose our users are trusted not to do this deliberately. It is still possible for Trojan Horses to copy information from one object to another.

Trojan Horse Vulnerability of DAC



User B cannot read file F

Trojan Horse Vulnerability of DAC



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

Copy Difference for rw

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