Module 3.3
Discretionary Access Control (DAC) and Trojan Horses

Ravi Sandhu

Spring 2021
Operational model

- specify the decision function for the access decision triple or quad

Administrative

- specify the model’s dynamics
- dynamics change the system state and modify the outcome of some access decision triple or quads
Operational model

- specify the decision function for the access decision triple or quad

Administrative

- 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
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

ACL

File F

A:r

File G

B:r
A:w
User A executes Program Goodies, which contains a Trojan Horse.

- User A has read (A:r) access to File F.
- User B has read (B:r) access to File G.
- User A has write (A:w) access to File G.

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