Module 3.4
Mandatory Access Control (MAC)
and Covert Channels

Ravi Sandhu

Spring 2021

MAC

- Operational model

  MAC

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

- Administrative

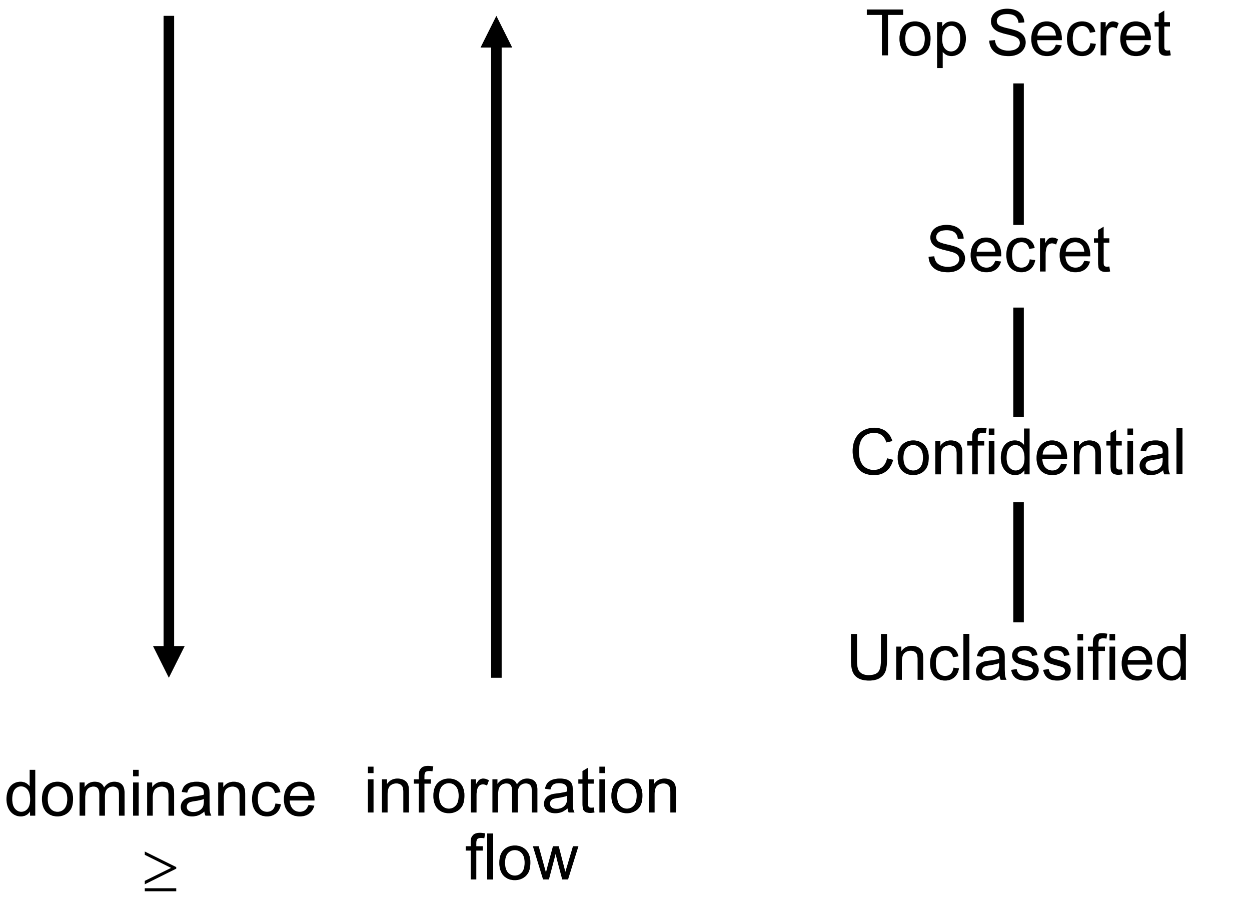
  Centralized

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

MAC

- Core concept:
  - Extend control to copies via security labels
- Core drawback:
  - Covert/side channels bypass MAC
  - Inference not prevented
  - Too strict
  - Too reductionist
- Sophistication:
  - Dynamic labels

Linear Lattice



Top Secret

Secret

Confidential

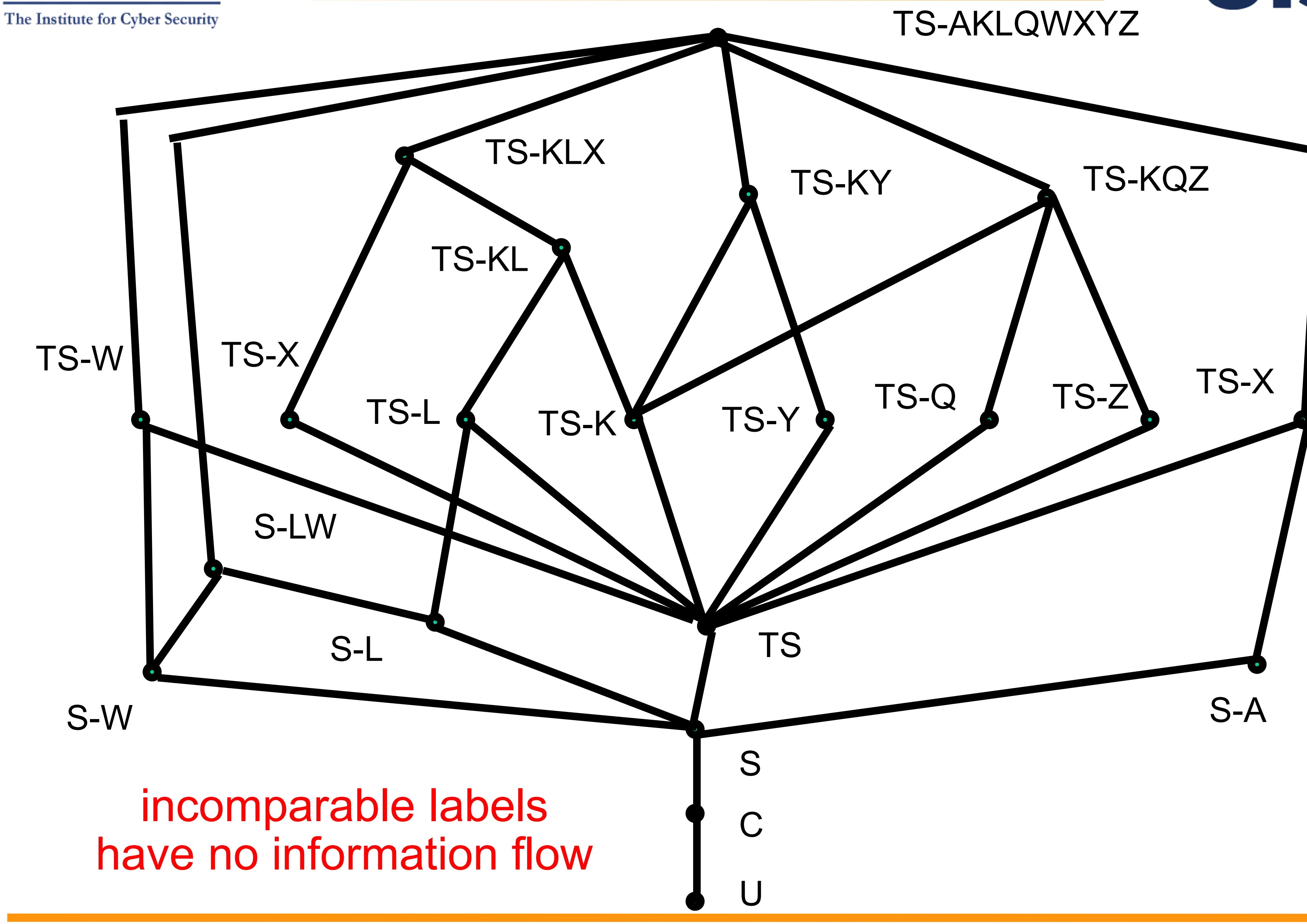
Unclassified

dominance
≥

information
flow

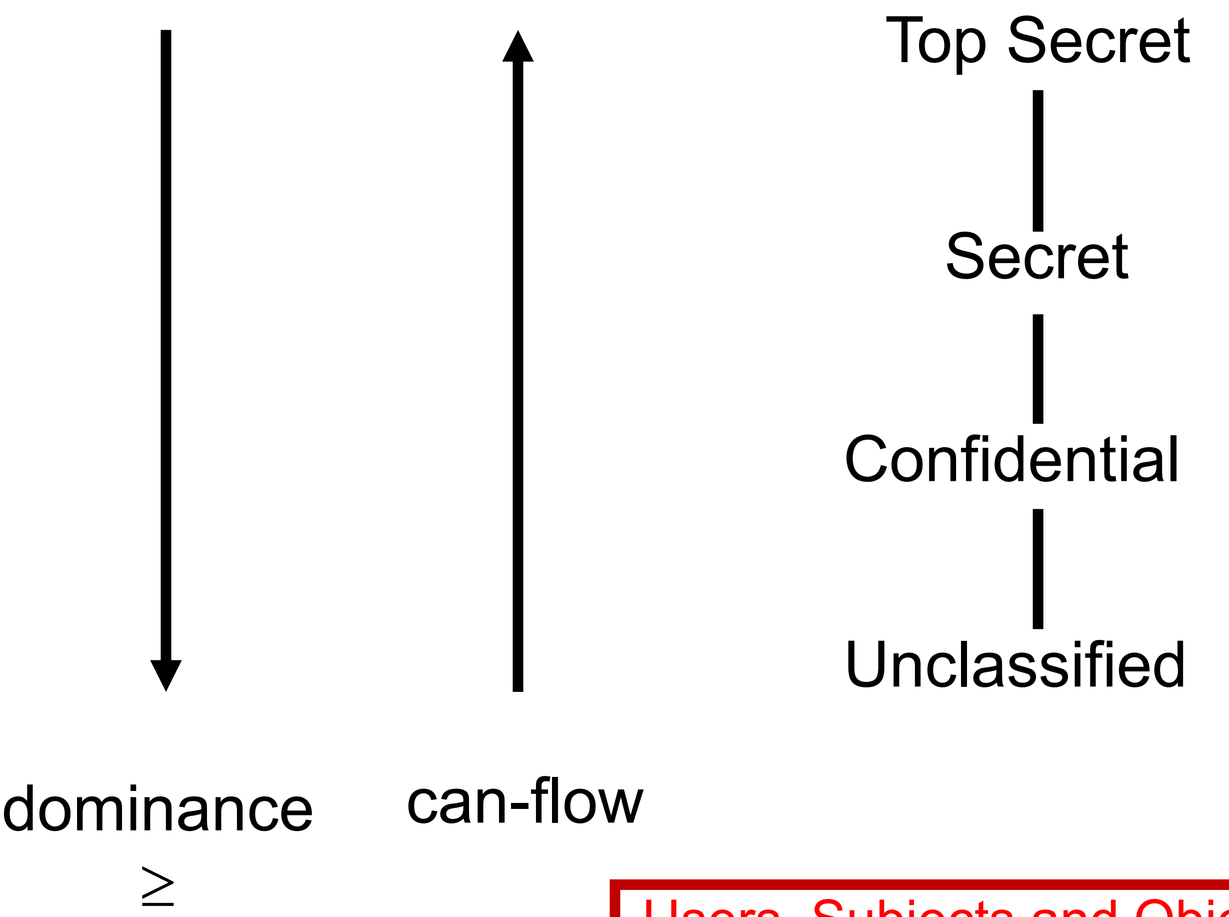
reflexive and transitive
edges are implied

Partial Order Lattice



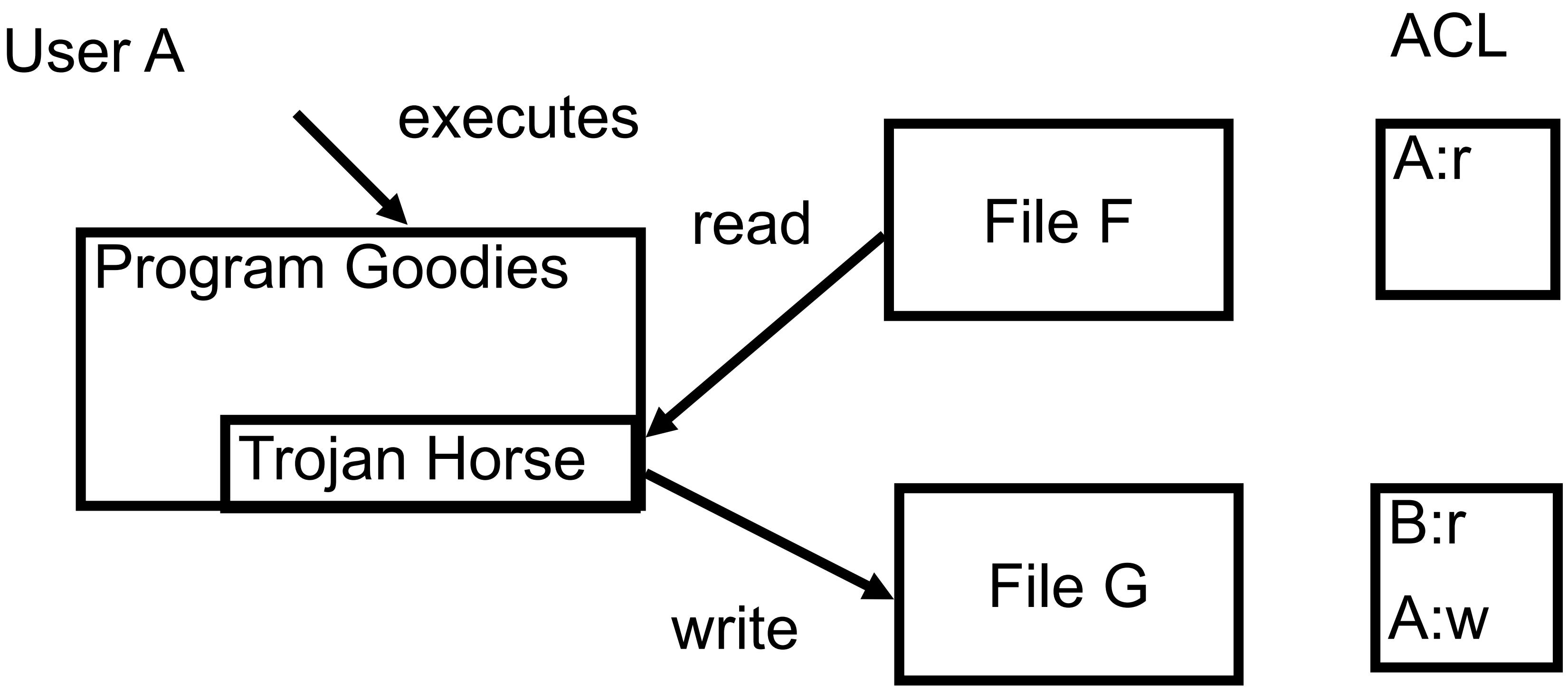
incomparable labels
have no information flow

Bell-LaPadula (BLP) Rules



Users, Subjects and Objects are labelled
A user can create subjects down
A subject can Read down Write up

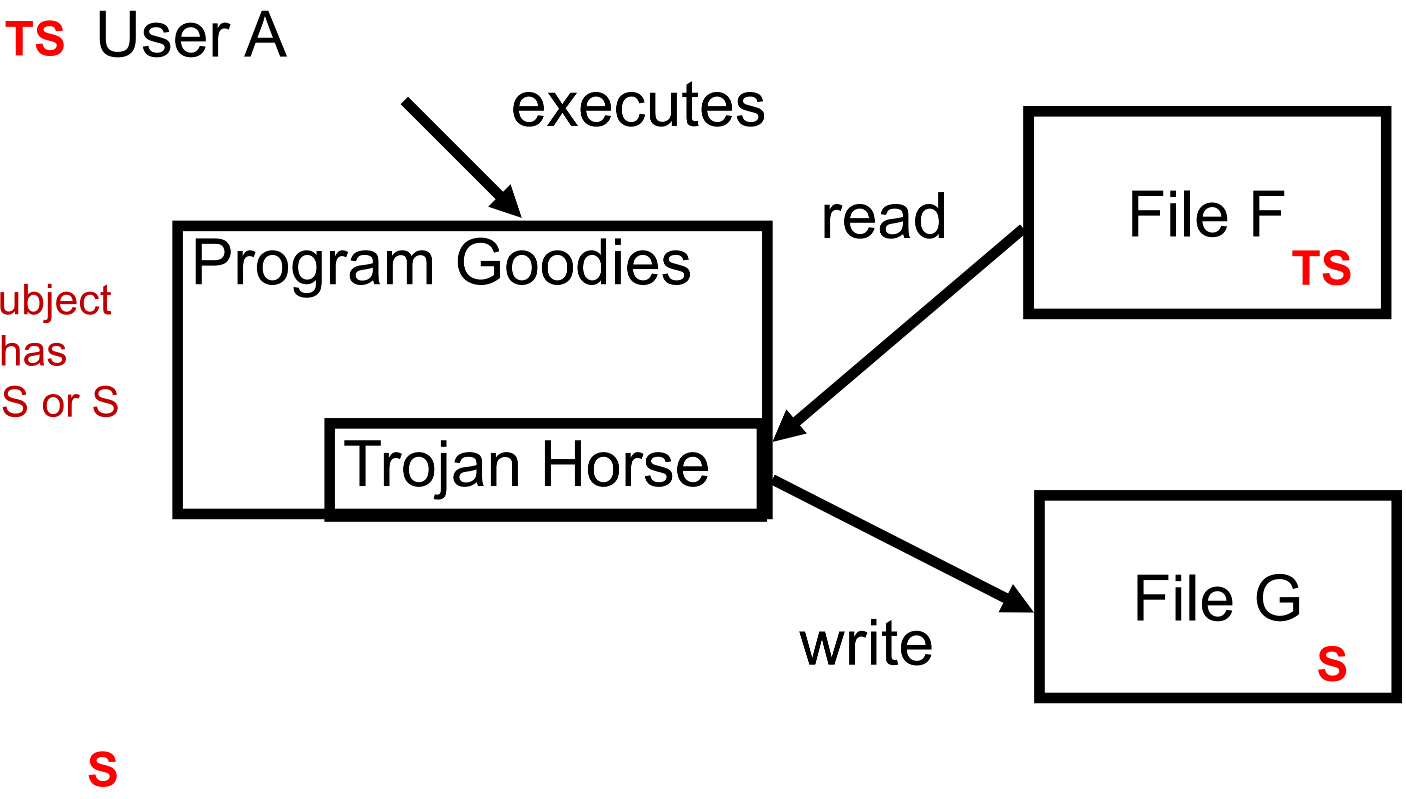
Trojan Horse Vulnerability of DAC



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

Trojan Horse Vulnerability Eliminated

Only 2 labels: TS, S



TS User A

executes

Program Goodies

Trojan Horse

read

File F TS

write

File G S

S

Each subject of A has Label TS or S

~~ACL~~

BLP Rules

Every subject of B has Label S and can read File G but cannot read File F

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

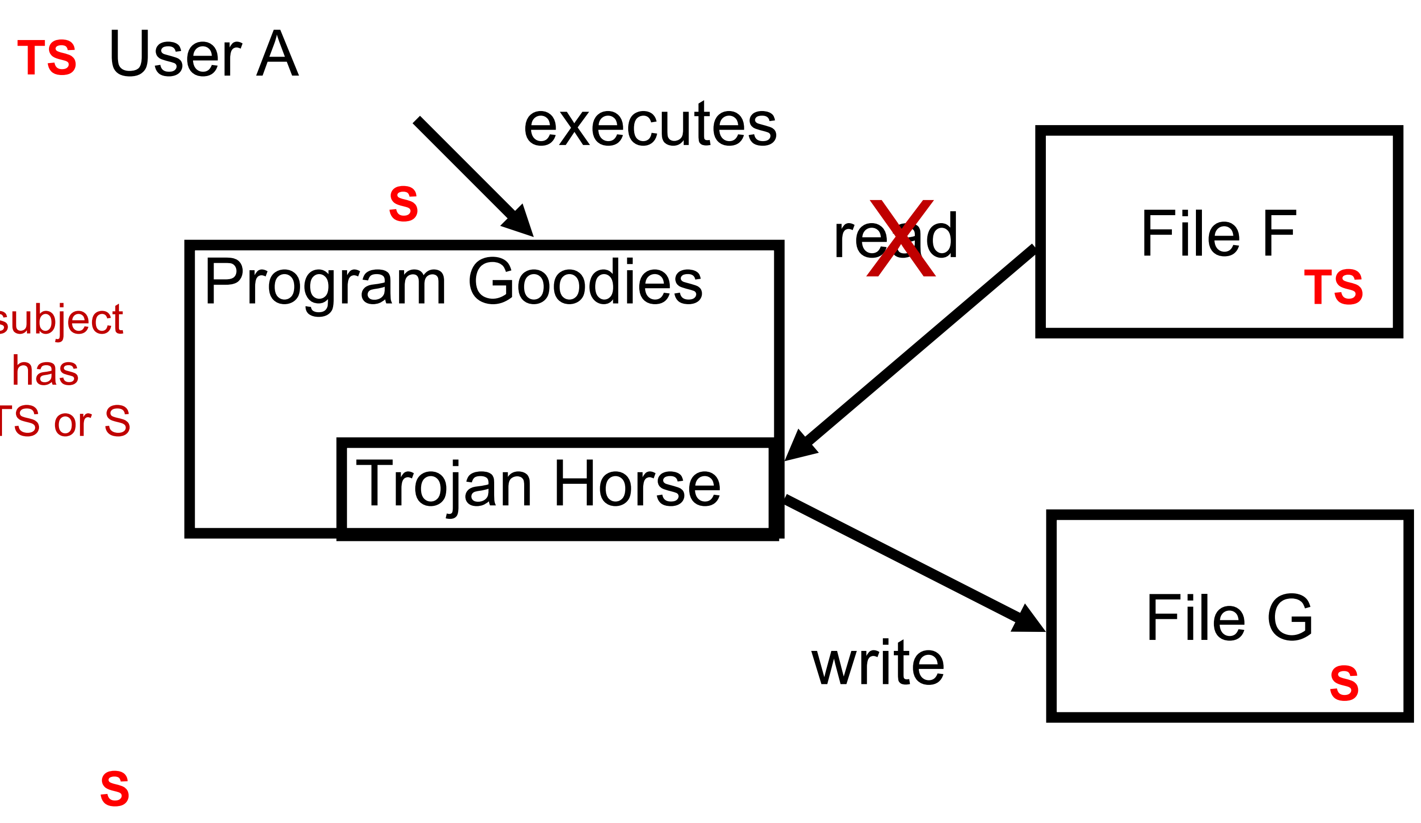
Trojan Horse Vulnerability Eliminated

Only 2 labels: TS, S

~~ACL~~

BLP Rules

Each subject of A has Label TS or S



TS User A

executes

S

Program Goodies

Trojan Horse

~~read~~

File F

TS

write

File G

S

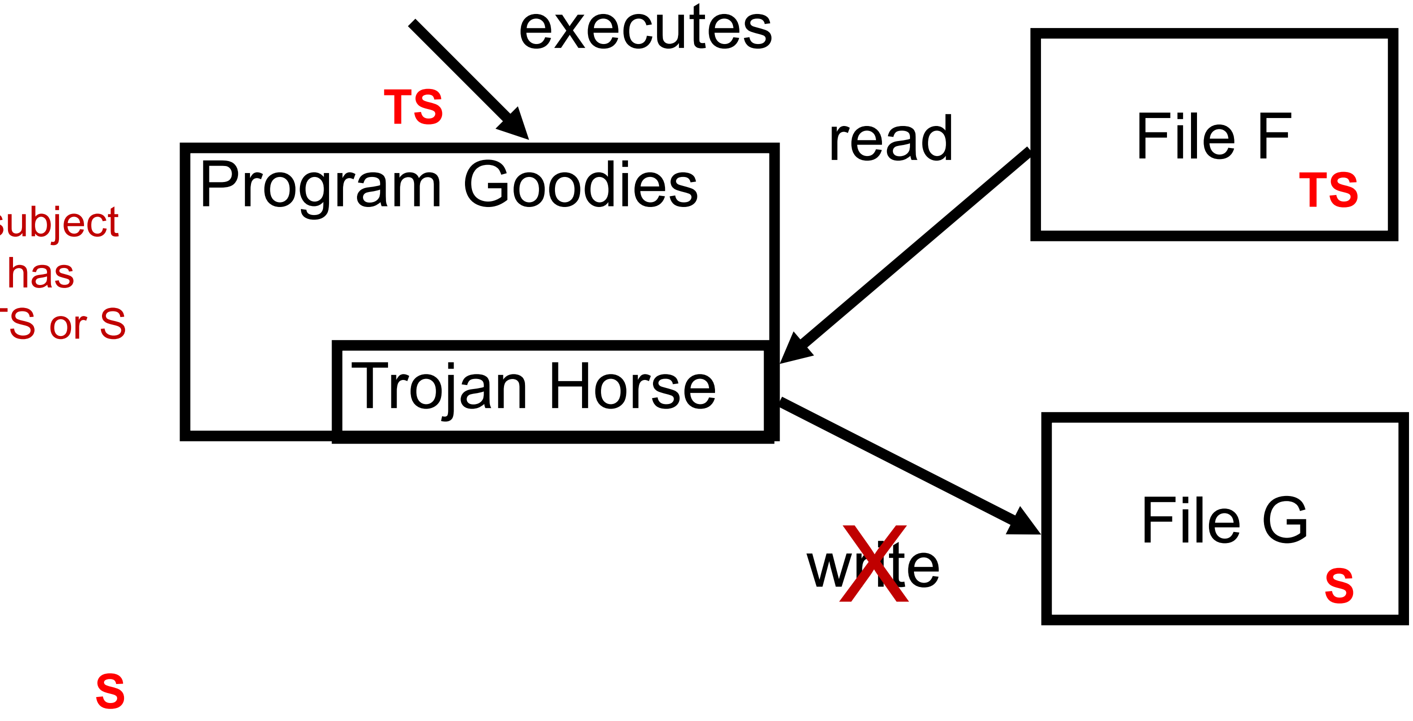
S

Every subject of B has Label S and can read File G but cannot read File F

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

Trojan Horse Vulnerability Eliminated

Only 2 labels: TS, S



Each subject of A has Label TS or S

~~ACL~~

BLP Rules

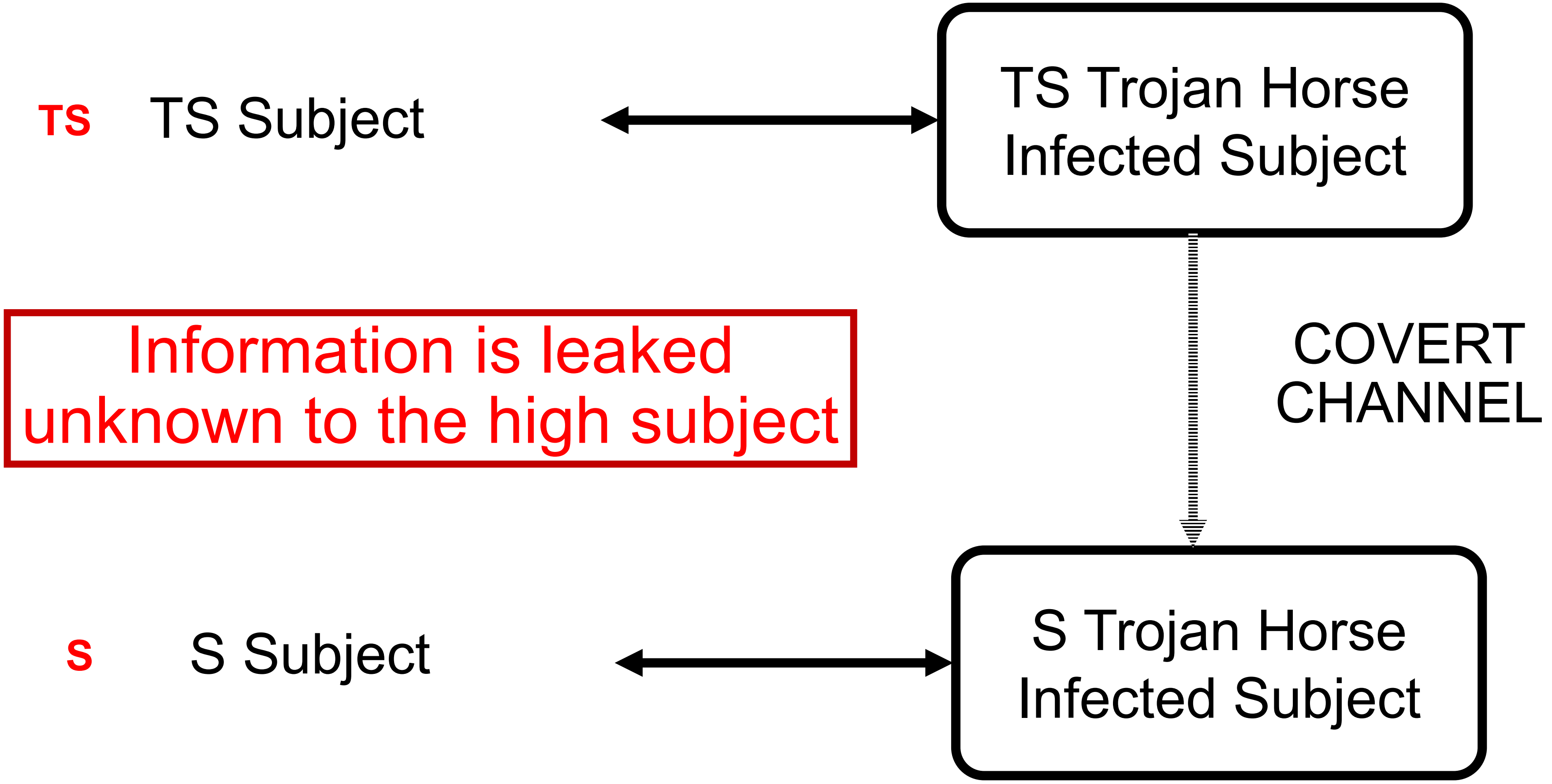
Every subject of B has Label S and can read File G but cannot read File F

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

Covert Channels

- A covert channel is a communication channel based on the use of system resources not normally intended for communication between subjects (processes)

Covert Channels



TS TS Subject

TS Trojan Horse Infected Subject

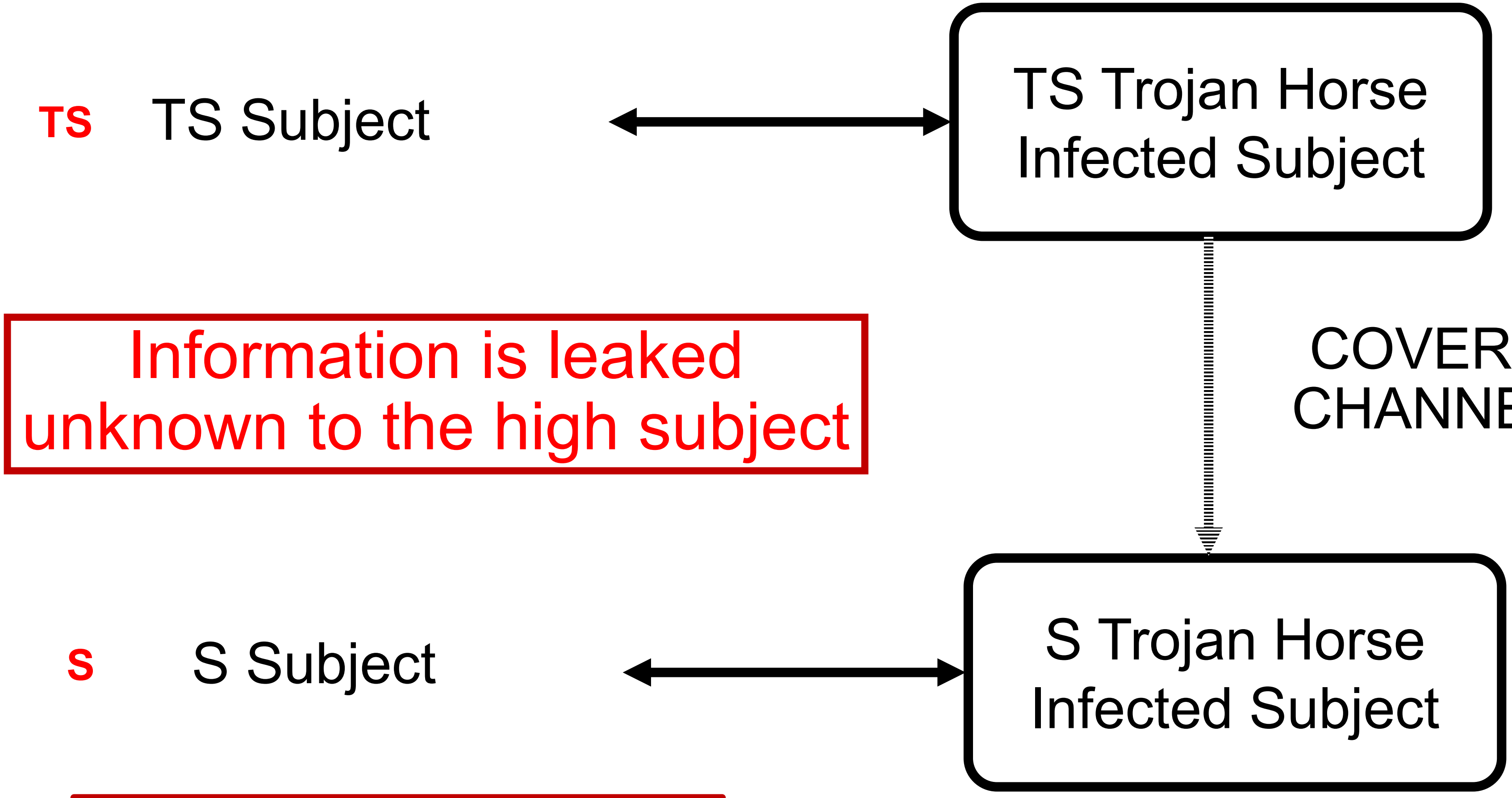
COVERT CHANNEL

Information is leaked unknown to the high subject

S S Subject

S Trojan Horse Infected Subject

Covert Channels



TS TS Subject

TS Trojan Horse Infected Subject

COVERT CHANNEL

Information is leaked unknown to the high subject

S S Subject

S Trojan Horse Infected Subject

BLP rules prevent overt leakage of information but cannot address covert channels

Storage Channels

- Also known as Resource Exhaustion Channels
- Given 5GB pool of dynamically allocated memory
  - TS PROCESS (sender)
    bit = 1 ⇒ request 5GB of memory
    bit = 0 ⇒ request 0GB of memory
  - S PROCESS (receiver)
    request 5GB of memory
    if allocated then bit = 0 otherwise bit = 1

Timing Channels

- Also known as Load Sensing Channels
- Given a shared CPU
  - TS PROCESS (sender)
    bit = 1 ⇒ enter computation intensive loop
    bit = 0 ⇒ go to sleep
  - S PROCESS (receiver)
    perform a task with known computational requirement
    if completed promptly then bit = 0 otherwise bit = 1