Module 3.4
Mandatory Access Control (MAC) and Covert Channels

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
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

dominance \geq information flow

Top Secret
Secret
Confidential
Unclassified

reflexive and transitive edges are implied
Partial Order Lattice

incomparable labels have no information flow
Users, Subjects and Objects are labelled
A user can create subjects down
A subject can Read down Write up

\[ \text{dominance} \geq \text{can-flow} \]
Trojan Horse Vulnerability of DAC

User A executes Program Goodies

- read File F
- write File G

ACL:
- A:r
- B:r
- A:w

User B can read contents of file F copied to file G
Trojan Horse Vulnerability Eliminated

Only 2 labels: TS, S

User A (TS) executes Program Goodies
- Reads File F (TS)
- Writes File G (S)

User B (S)
- Can read contents of File F copied to File G

Every subject of A has Label TS or S

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

ACL X

BLP Rules

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Trojan Horse Vulnerability Eliminated

Only 2 labels: TS, S

TS User A

executes

S

read

File F

TS

write

File G

S

S

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

Each subject of A has Label TS or S

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

Program Goodies

Trojan Horse

User A executes Program Goodies. The Trojan Horse then writes to File G with Label S. User B, with Label S, can read the contents of File F (TS) copied to File G.
Trojan Horse Vulnerability Eliminated

Only 2 labels: TS, S

User A executes Program Goodies

Trojan Horse

File F

File G

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

Each subject of A has Label TS or S

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

ACL

BLP Rules

© Ravi Sandhu

World-Leading Research with Real-World Impact!
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 Subject

TS Trojan Horse Infected Subject

S Subject

S Trojan Horse Infected Subject

Information is leaked unknown to the high subject
Covert Channels

TS Subject → TS Trojan Horse Infected Subject

S Subject → S Trojan Horse Infected Subject

Information is leaked unknown to the high 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