Midterm Exam
Problem 1: Short Answer

- **Access Control**
  - Subject, object, rights
- **Common Criteria**
  - Government Assurance Standard
- **Originator Controlled Access Control**
  - Not RBAC
- **Capability based access control**
  - Associates a list of objects and rights with each subject (dual to Access Control List)
- **Storage Channel**
  - Unintended communication channel; for example locking mechanism in kernel
2: Information Flow

- 6 programs computing
  - \( H := l \)
  - \( L := h \)
  - \( L := \text{not} \ h \) (or running forever)

A) Desired/undesired:
  - Desired
    - \( H := l \) \([2, 4]\)
  - Undesired
    - \( L := h \) \([1, 3]\)
    - \( L := \text{not} \ h \) \([5, 6]\)
B) Direct/Indirect
   - Direct:  1,2
   - Indirect: 3,4,5,6

C) Typable/untypable
   - Typable:  2, 4, 6
   - Untypable: 1, 3, 5
D) Simple Security and Containment

- Answers varied depending on assumed context
  - \([h]\ |- \ l := h\) violates containment
  - \([l]\ |- \ l := h\) violates simple security
- I was looking for discussion of the termination channel in 5 and 6
- By my analysis 6 does not violate either property
  - To prevent 6 another property would be needed
2 cont

• E) Termination channel
  – Both 5 and 6 leak information via a termination channel
  – Type system does not detect this

• F) Termination requirement
  – This does fix problem
3) Voting Policy

- Confidentiality
  - Secret Ballot
- Integrity
  - Accurate count
- Availability
  - Eligible voters can vote in a timely manner
3 cont

• B) Vote stealing compromised task manager to launch an additional process that altered votes
• C) Violates integrity
• D) DOS could wait for election day and then crash machine
• E) DOS violates availability
4 Integrity Models

• A) Answers vary; typical:
  Boot Loader   T
  Op Sys       A
  Task Manager A
  Voting S/W   A
  Vote Tally O
4 cont

• B) Limit integrity level of files on removable media to level authenticated on smart card

• C) Show each operation feasible by informal argument
4 cont

- D) Prevent Felten:
  - Felten attack required replacing boot loader and systems software at levels A and T in new model.
  - Propagation required overwriting software at levels A and T by an election official.
  - Integrity policy together with authentication mechanism prevent initial attack by untrusted personnel and inadvertent viral propagation by election official
4 cont

• E) Critique: internal? External?
  – Answers varied considerably
  – Expected answer
    • External threat reduced (but not eliminated)
    • Internal threat not addressed
      – Malicious code introduced by trusted entity still is a concern
      – Devious behavior by a T or A can arbitrarily corrupt results
4 cont

• F, G & H) Answers varied considerably
  – Clark-Wilson would require vote be logged and the log must include the identity of the voter
  – This violates expectations of a secret ballot
  – Voter verified paper trail is an example of a transparent mechanism that balances integrity and confidentiality
Distribution

- 98 97 95 94 93
- 87 82
- 79 75 72 70
- 63 61 61
- 59 59 58
- 46 43 42

- 28 27 22

- Curve by:
  - \( F(x) = \frac{x}{2} + 50 \)