Introduction to Computer Security
Study question for midterm exam

Draft questions I am considering for the exam. Please consider past study questions, past exams, and these questions when preparing for the exam.

Some of the questions below may be simplified for the exam.

1. (a) In English, state the security policy for a voting system. Identify which requirements address confidentiality, integrity, and availability concerns.
   (b) Summarize the vote stealing attack presented in the Felton paper.
   (c) What aspects of the security policy does the vote stealing attack violate?
   (d) Felton also sketches denial of service attacks; describe a denial of service attack.
   (e) What aspects of the security policy does the denial of service attack violate?

2. Use the Biba integrity model to propose a formal integrity policy for an idealized voting machine based on the Diebold machine Fenton studied.

   System Components:

   - Hardware
     - Processor
     - Volatile Memory
     - EPROM
     - On-board flash
     - Removable Flash (key access)
     - Printer (key access)
     - Smart card reader (open)
   - Software
     - Boot loader
     - Operating System
     - Task Manager
     - Voting Software
   - Logical Operations
     (a) Update boot loader
     (b) Update OS and applications
     (c) Define Ballot
     (d) Start election
     (e) Vote

(f) End election

(g) Post-election reporting

(a) Use the Biba integrity model to describe a formal integrity policy for the voting machine. Identify the subjects, objects, and integrity levels explicitly.

(b) Argue that the intended operations can be carried out by appropriate subjects without violating the policy.

(c) Argue that if mechanisms were in place to enforce the policy that Fenton's vote stealing and denial of service attacks would not be allowed.

(d) Suggest mechanisms to implement the policy.

3. A question like this based on the Clark-Wilson model.

4. Information-flow security.

   Consider the four program fragments:

```
1   l := h
2   h := l
3   l := false; if h then l := true
4   h := false; if l then h := true
```

   (a) Assume `h > l`. Explain informally which flows are desired and which flows should be prevented (undesired flows).

   (b) Which flows are direct; which are indirect?

   (c) Use the type system presented in Sabelfeld and Myers (reproduced separately) to show the desired flows are allowed.

   (d) Use the type system to argue that the undesired flows are not allowed.