Introduction to Computer Security
Exam Study Guide

1 Introduction, Overview, Usability

1. Usability. [15 points]

   Ross Anderson stresses usability as a critical issue in practical computer security. He points out that many of the most devastating security failures have had a significant human component. Give an anecdote about usability in the domain of voting that supports Anderson's thesis.

2. Define availability, integrity and confidentiality. Give examples of violations of each.

2 Electronic Voting, Access Control

1. Basic Principles and Voting Machines [15 points]

   (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 Feldman, Halderman, and Felten paper.

   (c) What aspects of the security policy does the vote stealing attack violate?

   (d) Feldman, Halderman, and Felten also sketch denial of service attacks; describe a denial of service attack on the Diebold voting machine.

   (e) What aspects of the security policy does the denial of service attack violate?

2. Define and contrast discretionary access control, mandatory access control and originator controlled access control. Which of these can coexist? Which cannot? Illustrate with examples.

3. Access Control [12 points]

   (a) Describe what an access control list is.

   (b) Explain how UNIX permissions can be regarded as access control lists.

   (c) Describe capability based access control.

   (d) Contrast access control lists and capability based access control.

4. In Chapter 2 Bishop introduces the Access Control Matrix model. This model is universal in the sense that all access control mechanisms that are at the granularity of monolithic objects can be explained with an Access Control Matrix. In Chapter 14 Bishop presents two major families of access control mechanisms: Access Control Lists and Capability Lists.

   (a) Summarize the definitions of Access Control Matrix, Access Control List, and Capability Lists.

   (b) Relate Access Control Lists and Capability Lists to the Access Control Matrix model.

   (c) Explain how UNIX permissions can be viewed as Access Control List abbreviations.

   (d) Describe an extension of UNIX permissions that permits finer control.

3 Access Control, Policy, and Historical notes

1. Reference Monitor [15 points]

   In his seminal 1972 report on Computer Security, James P. Anderson introduced a concept called a reference monitor. Define a reference monitor. Give an example.

2. SecureSoft has a subcontract form NuHard to develop software for a new product that NuHard is about to release. The IP agreement allows SecureSoft to share information within the company on a need to know basis, but prohibits SecureSoft from sharing this information with anyone outside of the company.

   As SecureSoft's director of security, you are asked to propose a set of policies and mechanisms to support this business relationship. Outline your proposal making reference to established confidentiality and integrity policies and access control mechanisms.

3. Define and contrast the terms policy and mechanism. Illustrate with examples.

4 Confidentiality models

1. BLP

   Summarize the Bell LaPadula security model. Describe the two conditions that define it. Paraphrase the security theorem that these conditions establish.

2. In the Bell LaPadula model there is an apparent anomaly that prevents dialog between agents with different clearances. To address this anomaly Bell LaPadula include the notion of current security level.

- Bell LaPadula is defined by two rules, which are sometimes quoted as slogans. Give either the two rules or the two slogans.
- Describe the anomaly.
- Explain how the concept of current security level addresses the anomaly
- Outline how this is dealt with in the DG/UX system described in the text.

5 Information Warfare

1. Information Warfare [20 points]

   In a March 29, 2009 article the New York Times reported on an information warfare initiative targeted against the Office of His Holiness the Dalai Lama (OHHDL). Ngaraja and Anderson wrote a technical report giving details of the incident.

   (a) What does the term information warfare mean? Why do Ngaraja and Anderson use that term to describe this incident?

   (b) How did OHHDL come to suspect that they had been infiltrated?

   (c) How do Ngaraja and Anderson conjecture the initial infiltration was accomplished?

   (d) Once a trusted machine was compromised, how did the attack proceed?

   (e) Are such attacks easily preventable? Are Nagaraja and Anderson optimistic or pessimistic about the ability of other organizations to resist such attacks?

6 Integrity Models

1. Integrity Model applied to Voting Machine [55 points]

   This question explores how the Clark-Wilson model can be applied to the voting machine described in the paper by Feldman, Halderman, and Felten (FHF).

   The Clark-Wilson model has several components. These include identifying constrained data items (CDI), integrity constraints, integrity verification procedures (IVP), transaction processes (TP), and the allows and certifies relations. **A synopsis of the Clark-Wilson certification and enforcement rules is provided following the question.**

   Assume the following set of Constrained Data Items:

   (a) Boot loader

   (b) Operating System and Trusted Applications

(c) Voting Application
(d) Ballot Definition
(e) Vote Tally
(f) Completed Ballot

A partial set of integrity constraints includes:

(a) New images of the boot loader, OS, Trusted Applications, and Voting Applications must include a certificate of origin signed by a trusted party. The certificate must include a message digest of the image.
(b) The OS, Trusted Applications, and Voting Applications must pass an integrity check based on their certificate of origin before being executed.
(c) The Ballot Definition must be signed digitally by an election official distinct from the official operating the voting machine.

The transaction processes (TPs) are:

(a) Update Boot Loader
(b) Update OS and Trusted Applications
(c) Update Voting Application
(d) Define Ballot
(e) Start Election
(f) End Election
(g) Vote

Problems

(a) Complete the model by listing additional integrity constraints. Every CDI should appear in at least one integrity constraint. [5 points]
(b) Sketch the *certifies* relation. (The certifies relation assocates a set of CDIs with a particular TP.) [5 points]
(c) Sketch the *allowed* relation. Specifically call out any separation of duty concerns. (The allowed relation defines a set of triples to capture the associate of users, TPs, and (sets of) CDIs.) [5 points]
(d) Discuss the tension between the Clark-Wilson model and the secret ballot requirement. [5 points]
(e) Given a system conforming to this model, discuss the feasibility of (1) FHF's vote stealing attack, (2) FHF's denial of service attack, and (3) FHF's mechanism for propagation of malware. Identify which (if any) integrity constraints would be violated by these attacks. Be specific about how mechanisms implementing the Clark-Wilson rules would prevent these violations. [10 points]

(f) Given a system conforming to this model, discuss the feasibility of (1) updating the voting software, (2) defining a ballot, and (3) voting. Be specific about which CDIs are modified, which integrity constraints are maintained, which relationships are verified, and which rules require which actions. [10 points]

(g) If the requirement for a secret ballot is eliminated and all aspects of the Clark-Wilson model you describe above are implemented is the resulting system robust against external threats? Is it robust against internal (insider) threats? [10 points]

(h) Several researchers have recommended the use of a Voter Verified Paper Audit Trail (VVPAT) inserted into a conventional ballot box. If this mechanism were used would it be possible to have a secret ballot without compromising the integrity properties provided by the Clark-Wilson model? Discuss. [5 points]

Synopsis of Clark-Wilson:

CR1 When any IVP is run, it must ensure that all CDIs are in a valid state.

CR2 For some associated set of CDIs, a TP must transform those CDIs in a valid state into a (possibly different) valid state.

ER1 The system must maintain the certified relations, and must ensure that only TPs certified to run on a CDI manipulate that CDI.

ER2 The system must associate a user with each TP and set of CDIs. The TP may access those CDIs on behalf of the associated user. If the user is not associated with a particular TP and CDI, then the TP cannot access that CDI on behalf of that user.

This defines a set of triples (user, TP, CDI set) to capture the association of users, TPs and CDIs. This is called the *allowed* relation.

CR3 The allowed relations must meet the requirements imposed by the principle of separation of duty.

ER3 The system must authenticate each user attempting to execute a TP.

CR4 All TPs must append enough information to reconstruct the operation to an append-only CDI.

CR5 Any TP that takes as input a UDI may perform only valid transformations, or no transformations, for all possible values of the UDI. The transformation either rejects the UDI or transforms it into a CDI.

EF4 Only the certifier of a TP may change the list of entities associated with that TP. No certifier of a TP, or of any entity associated with that TP, may ever have execute permission with respect to that entity.

2. BMA Model [20 points]

   The British Medical Association model addresses mechanisms to keep medical records confidential. The model is distilled into nine principles, which are partially reproduced below

   1 Access control: each identifiable clinical record shall be marked with an access control list . . . .

   2 Record opening: a clinician may open a record with herself and the patient on the access control list. When a patient has been referred, she may open a record with herself, the patient and the referring clinician(s) on the access control list.

   3 Control: One of the clinicians on the access control list must be marked as being responsible. . . .

   4 Consent and notification: . . .

   5 Persistence: no-one shall have the ability to delete clinical information until the appropriate time period has expired.

   6 Attribution: all access to clinical records shall be marked on the record with the subject's name, as well as date and time. An audit trail must also be kept of all deletions.

   7 Information flow: Information derived from record A may be appended to recrod B if and only if B's access contro list is contained in A's.

   8 Aggregation control: . . .

   9 Trusted computing base: . . .

   The following questions explore the BMA model:

   (a) What is pretexting? Give an example of a pretexting attack on a medical organization.

   (b) How did Anderson propose medical records be automated? Specifically address the issue of a single centralized record vs. a set of distributed records? How is this decision reflected in the principles?

   (c) How did the aggregation of National Health Service data across multiple practices change the significance of the insider threat for inappropriate disclosure of information?

   (d) How did the BMA model address this significant threat? How do the principles prevent my dentist's recptionist from reading my therapist's notes about my mental health?

   (e) How does the Information Flow principle (7) relate to Bell LaPadula?

   (f) Why did Anderson reject just adapting military style confidentiality to the health domain? What went wrong with having AIDS-like information secret, normal patient records confidential, and prescription information sensitive?

3. Integrity Models [15 points]

   Contrast the Biba and Clark-Wilson integrity models. You may wish to use examples, such as the voting machine case study, to illustrate your points. Please address:

   (a) Simplicity of mechanism.

   (b) Guidance to security architects in developing requirements.

   (c) Protection from external threats.

   (d) Protection from internal threats.

   (e) Integration with existing security practices in government and industry.

4. Integrity Model applied to Voting Machine [40 points]

   You are being asked to re-engineer the voting machine that Felten's lab studied. To increase assurance you have been asked to apply the Biba integrity model to the design.

   In the new design you are to implement four distinct levels of integrity, corresponding to the following agents:

Agent	Level	Abbreviation
Trusted Vendor	TCB	T
System Administrator	Admin	A
Election Official	Official	O
Voter	Voters	V

   The levels are listed in order from most trusted (T) to least trusted (V).

   You have learned that the smart card reader/writer is a trustworthy device. You can trust this unit to authenticate users of the system. In particular, each smart card indicates what kind of agent is authentication (T, A, O or V), and for all agents except voters provides a reliable unique identity.

   System Components:

   - Hardware
     - Processor
     - EPROM
     - On-board flash
     - Removable Flash (key access)
     - Printer (key access)
     - Smart card reader/writer (open)
     - Display (open)
   - Key files
     - Boot loader

- Operating System
- Task Manager
- Voting Software
- Vote Tally

- 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) [5 points] Elaborate the Biba integrity model for this system by assigning integrity levels to all key files. Specifically assign integrity levels for creating or modifying these files.

(b) [5 points] Several known exploits of the system rely on infection via removable media. Propose a mechanism that uses the trusted authentication mechanism and integrity model to prevent these exploits.

(c) [5 points] Argue that the intended operations listed above in **bold face** can be carried out by appropriate subjects without violating the policy. If it is necessary to specify that any software run at a higher level of integrity than the currently authenticated user please note which software and what level of integrity is should assume.

(d) [5 points] Argue that with these mechanisms and a faithful implementation of the integrity model that Felten's vote stealing and denial of service attacks would not be allowed.

(e) [5 points] Having developed this design, it is now time to critique it! Are you satisfied with the protection against external threats? Are you satisfied with the protection against insider threats? Discuss.

(f) [5 points] If the Clark-Wilson model were applied, the vote tally would be a constrained data item (CDI) and voting would be a transaction process (TP).

What audit requirements would be dictated by these designations?

(g) [5 points] Are these requirements in conflict with the confidentiality policy expected of a voting machine?

(h) [5 points] Suggest a mechanism that balances the need for audit requirement with the confidentiality policy.

5. In the DG/UX system the MAC lattice is divided into regions as shown in Figure 5-3 (reproduced separately). A set of rules implement a form of Bell LaPadula protection. This design exploits a duality between Bell LaPadula and Biba.

(a) How does DG/UX modify the Bell LaPadula notion of current security level to achieve both security and integrity?

(b) Explain how the DG/UX design is a confidentiality mechanism. What data is protected?

(c) Explain how the DG/UX design is an integrity mechanism. What data is protected?

6. Explain the Chinese Wall model. Give its motivating scenario and enumerate its mechanisms. To what extent can the Chinese Wall model be modeled by Bell LaPadula? In what sense is the Bell LaPadula framework inappropriate to model the Chinese Wall model?

7. In medicine the roles of physician and pharmacist are separated. This inhibits abuse of prescription drugs by physicians and pharmacists. What principle describes this separation? Describe a mechanism that implements this principle for an information system.

8. The Clark-Wilson model is an integrity model that can be applied to transaction processing systems. Using the student registration system described below, illustrate each of the following Clark-Wilson concepts (you only need to illustrate each concept once; you don't need to use the whole scenario):

   (a) An unconstrained data item.

   (b) A constrained data item.

   (c) An integrity verification procedure.

   (d) A transaction process.

   Scenario: The student system keeps track of students, their schedules, and their grades. Each student has a name, an ID, an advisor, a favorite kind of pizza, a planned course of study, and a transcript. At the beginning of every term the student proposes a planned course of study to an advisor, who reviews it, either approving it or rejecting it. Courses have instructors. At the end of a term the instructor assigns a grade, and the course moves from the planned course of study to the transcript. The system maintains two invariants: the course of study is agreed to by the student and their advisor and all grades are assigned by the appropriate instructor.

7 Identity and Data Mining

1. Telephone Fraud

   Outline the telephone fraud detection problem. In your discussion please address the following points:

   (a) Define "subscription fraud" and "superposition fraud."

   (b) How does the concept of "Communities of Interest" apply to telephone fraud detection?

   (c) What data sources are used in telephone fraud detection?

   (d) Define and contrast "guilt by association" and "linkage using COI-based matching".

2. Identity [12 points]

   When doing commerce on the web, users expect to have some level of assurance that they are in fact interacting with the vendor associated with the web site they think they are visiting. Describe a mechanism that is used to establish identity for e-commerce transactions. Does the mechanism you describe have a tree structure with a distinguished root, or is it a general graph (web of trust) without a distinguished root.

8 Confinement and Virtualization

1. The Confinement Problem

   In his October 1973 CACM article, Butler Lampson articulates the "confinement problem". He articulates three kinds of channels: storage, legitimate, and covert.

   (a) Describe each kind of channel.

   (b) Give an example of each.

   (c) In a subsequent note Lipner comments on the confinement problem. Which of Lampson's channels was Lipner not optimistic about closing? Why?

2. Virtualization

   How does virtualization address the confinement problem? If security is a primary objective do you expect the virtual machine monitor (VMM) to be optimized for: simplicity, performance, or feature richness? Discuss.

3. Virtualization

   Following Popek and Goldberg's 1974 article on virtualization, Bishop articulates two requirements for an architecture to be virtualizable:

   (a) All sensitive instructions cause traps when executed by processes at lower levels of privilege.

   (b) All references to sensitive data structures cause traps when executed by processes at lower levels of privilege.

   In the article "Intel Virtualization Technology," Uhlig, *et al.* write:

> . . . the IA-32 and Itanium architectures both include instructions that access privileged state and do not fault when executed with insufficient privilege. For example, the IA-32 registers GDTR, IDTR, LDTR, and TR contain pointers to data structures that control CPU operation. Software can execute the instructions that write to, or *load*, these registers (LGDT, LIDT, LLDT, and LTR) at any privilege level. If the VMM maintains these registers with unexpected values, a guest OS using the latter instructions could determine that it does not have full control of the CPU.

Three approaches to virtualizing IA-32 have been implemented: Vmware performs binary translation, Xen uses paravirtualization, and VT-x revises the architecture. Summarize each of the three approaches. Give strengths and shortcomings of each approach.

4. Virtual machines and sandboxes (software fault isolation) are two mechanisms used to isolate entities to achieve confinement. Outline the problem that these mechanisms are solving. Describe each mechanism. Contrast the two mechanisms.

9 Information Flow

1. Information-flow security [20 points]

   Consider the four program fragments:

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

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

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

   (c) Use the Sabelfeld and Myers type system to show that two of these programs are typable and two are not.

2. Information-flow security [24 points]

   Consider the six program fragments:

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

```
5   l := false;
    while h do l := true

6   l := false;
    while h do skip
```

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

(b) Which flows are explicit (direct in the study questions); which are implicit (indirect)?

(c) Use the Sabelfeld and Myers type system to show that three of these programs are typable and three are not.

(d) Volpano, Smith and Irvine define two properties, *simple security* and *confinement*. Simple security says that, when $\vdash e : \tau$, “only variables at level τ or lower in e will have their contents read when e is evaluated (no read up).” Confinement says that, when $[\tau] \vdash c$ “no variable below level τ is updated in c”.

For each program fragment, discuss if it violates these properties.

(e) Consider program fragments 5 and 6. Did the type system get the right answer? Discuss any anomalies concerning 5 and 6 in your answers above.

(f) Bishop’s presentation gives a rule for while loops that requires that each loop terminates. This condition is omitted in the Sabelfeld and Myers system presented in class. Does Bishop’s requirement that all while loops terminate eliminate any anomalies? Discuss.

3. In the Denning and Denning information flow model traditional exception mechanisms allow information to flow in dangerous ways.

(a) Illustrate a prohibited information flow that communicates via an exceptional event.

(b) Describe how explicit static declaration of exceptions and handlers can address this. If you are familiar with Java you may want to discuss Java’s exception mechanism and its restrictions.

4. Information Flow [12 points]

(a) Give an example program that has at least three variables, a, b, and c. Construct the program so that there is an explicit flow from a to c and an implicit flow from b to c. There should be no explicit flow from b to c.

(b) Use the type system presented in Sabelfeld and Myers (reproduced separately, but included with this exam) to show that if a and b are low variables and c is a high variable that the program you construct can be typechecked.

5. Information flow type systems, such as those proposed initially by Denning and Denning and implemented in Simonet's Flow Caml system, statically predict the security level of values in a computation. Assuming that user input and output are "low" and the password file is "high" security, what label would be assigned to the result of a password checking function? Discuss why this may be theoretically correct but impractical. What additional mechanisms are needed? Discuss the considerations of using those mechanisms.

6. In the Denning and Denning information flow model traditional exception mechanisms allow information to flow in dangerous ways.

   (a) Illustrate a prohibited information flow that communicates via an exceptional event.

   (b) Describe how explicit static declaration of exceptions and handlers can address this. If you are familiar with Java you may want to discuss Java's exception mechanism and its restrictions.

7. When information flow rules are applied srictly it is impossible to express a password checking program (assuming passwords are confidential and unauthenticated users do not have access to the passwords). Explain why this is the case. Describe mechanisms that have been proposed to deal with this issue.

10 Assurance and Evaluation

1. Any questions?

11 Cryptography

1. Certification of integrity of origin of software [15 points]

   One mechanism to establish the integrity of software is to verify that the software has not been modified since it was released. This is done by having the creator of the software generate a certificate. Propose a mechanism to generate such certificates. Propose a mechanism to test these certificates. Explain why these mechanisms guarantee origin integrity. What additional mechanisms does your solution require? Are there vulnerabilities that derive from these assumptions?

2. Key Management [15 points]

   Define the terms *session key* and *interchange key.* Describe a protocol that uses session and interchange keys. Discuss why it is important to distinguish these two kinds of keys.

3. Crypto [15 points]

   Explain how public-key cryptography might be used to encrypt an email message between Alice and Bob.

4. Describe the following simple cipher techniques. Illustrate how they can be used to encipher "cat". For key material use prefixes of "bad".

   (a) Caesar cipher

   (b) Vigenère cipher

   (c) One-Time pad

5. Recall the Needham-Schroeder protocol:

   1. $A \to C\colon A||B||n_1$
   2. $C \to A\colon \{A||B||n_1||k_s||\{A||k_s\}_{k_B}\}_{k_A}$
   3. $A \to B\colon \{A||k_s\}_{k_B}$
   4. $B \to A\colon \{n_2\}_{k_s}$
   5. $A \to B\colon \{n_2 - 1\}_{k_s}$

   What role do the random values, n_1 and n_2 (called nonces), serve in this protocol? Describe an attack on a simplified protocol that omits one or both nonces but is otherwise identical.

6. How, in general, does an attacker approach cracking a symmetric key-based system in which the attacker only has access to the ciphertext (and the function if needed). Hint: answer this in terms of a 20 bit binary key, or a 128 bit binary key.

7. Contrast block and stream ciphers. What property characterizes a block cipher? What property characterizes a stream cipher? Classify the following according to block or stream cipher:

   (a) Caesar cipher

   (b) Vigenère cipher

   (c) One-Time pad

8. Define the following terms:

   (a) Diffie-Hellman Algorithm

   (b) Symmetric Encryption

   (c) Public key Cryptography

   (d) Message digest

   (e) Message digest collision

9. What is a digital signature? What properties are expected of a digital signature? In lecture we presented a bogus digital signature and several legitimate digital signatures. The bogus signature used classical cryptography with a shared key between Alice and Bob, k. In the bogus scenario Alice sends Bob $m||\{m\}_k$. In one legitimate scenario Alice and Bob use public key cryptography, with Alice's key pairs being d_{Alice}, e_{Alice}. In this case Alice sends Bob $m||\{m\}_{d_{Alice}}$. Identify a property of digital signatures that the legitimate mechanism has but the bogus one does not. Justify your answer.

12 Comprehensive

1. Short Answer. [15 points]

   Please give a **short** description of each of the following:

   (a) Access Control Matrix

   (b) Originator controlled access control

   (c) Classic (secret key) cryptography

   (d) Public key cryptography

   (e) Message digests

2. Short Answer. [20 points]

   Please give a **short** description of each of the following:

   (a) Integrity

   (b) Confidentiality

   (c) Availability

   (d) Access Control Matrix

   (e) Originator controlled access control

   (f) Virtualization

   (g) Separation of duty

3. Short Answer. [15 points]

   Please give a **short** description of each of the following:

   (a) Integrity

   (b) Confidentiality

   (c) Availability

   (d) Access Control Matrix

   (e) Originator controlled access control

   (f) Sandboxing

(g) Separation of duty

(h) Separation of function

4. True or False. [15 points]

   (a) Covert channels are easily detected and eliminated.

   (b) Storage channels can be addressed with well known security engineering techniques.

   (c) The Orange book attempts to correct issues that led to paralysis under the Common Criteria.

   (d) The Bell La Padula model is used in the context of mandatory access control.

   (e) The Bell La Padula model supports discretionary access control.

   (f) The Biba model addresses confidentiality.

   (g) The protection state enforced by the Chinese Wall model at any particular point in time can be described with BLP.

   (h) The 1972 Anderson report failed to identify network security as an important field deserving further study.

5. Short Answer. [15 points]

   Please give a **short** description of each of the following:

   (a) Integrity

   (b) Confidentiality

   (c) Availability

   (d) Access Control Matrix

   (e) Originator controlled access control

   (f) Separation of duty

   (g) Common Criteria

   (h) British Medical Association policy for clinical information

6. Short Answer. [16 points]

   Please give a **short** description of each of the following:

   (a) Access Control Matrix

   (b) Originator controlled access control

   (c) Classic (secret key) cryptography

   (d) Public key cryptography

   (e) Message digests

   (f) Virtualization

   (g) Sandboxing

(h) Separation of duty

7. Short Answer. [15 points]

   Please give a **short** description of each of the following:

   (a) Access Control Matrix
   (b) Common Criteria
   (c) Originator controlled access control
   (d) Capability based access control
   (e) Lampson's definition of a storage channel

8. Short Answer. [12 points]

   Please give a **short** description of each of the following:

   (a) Covert channel.
   (b) Common criteria.
   (c) Software fault isolation
   (d) Virtualization

13 Out of Scope

1. Malicious Logic [12 points] What is a polymorphic virus? What class of defensive mechanisms do polymorphic viruses circumvent? Justify.

2. Design Principles [40 points]

   In their 1975 paper, Saltzer and Schroeder articulated eight principles for "The Protection of Information in Computer Systems". These principles are:

   - Least Privilege
   - Fail-safe Defaults
   - Economy of Mechanism
   - Complete Mediation
   - Open Design
   - Separation of Privilege
   - Least Common Mechanism
   - Psychological Acceptability

   (a) [16 points] Give a short description of each of the principles.
   (b) [12 points] In class we have discussed the Feldman, Halderman, and Felten study of the Diebold voting machine. Evaluate the Diebold design as described in the paper with respect to the principles of (1) least privilege, (2) open design, and (3) psychological acceptability.

(c) [12 points] In class and in previous exams we have discussed the application of the Biba and Clark-Wilson integrity models to the voting machine. Briefly summarize the two approaches. Discuss how the design principles could be applied to these two approaches. Specifically address the following principles in your discussion: (1) least privilege, (2) economy of mechanism, (3) complete mediation.