Introduction to Computer Security
Midterm Exam

This is a closed-book, closed-notes exam. All problems have equal weight.

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

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

3. 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?

4. 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.

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

6. 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?

7. 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.

8. Recall the Needham-Schroeder protocol:

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

   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.

9. 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

10. Define the following terms:

    (a) Diffie-Hellman Algorithm

    (b) Symmetric Encryption

    (c) Public key Cryptography

    (d) Message digest

    (e) Message digest collision