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. 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

4. Define the following terms:

   (a) Diffie-Hellman Algorithm

   (b) Symmetric Encryption

   (c) Public key Cryptography

   (d) Message digest

   (e) Message digest collision

5. 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.

6. 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.

7. 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.

8. 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?

9. 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.

10. 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.