Introduction to Computer Security
Study Questions

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

1. 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.

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. 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. 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.

5. 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.