Sample Midterm

These are sample questions that are very similar to the ones I will ask on the midterm.

1. Why is a precise statement of security requirements critical to the determination of whether a given system is secure?

2. Which of the following does the Needham-Schroeder protocol require?

   (a) A trusted third party

   (b) A public key cryptosystem

   (c) A certificate authority to identify the users

   (d) A connection to the Internet

3. Which of the following demonstrate violations of the principle of least privilege? Please justify your answer.

   (a) The Linux *root* account, to which no access controls are applied.

   (b) A user whose function is to maintain and install system software. This user has access to the source files and directories, access to only those programs needed to build and maintain software, and can copy executables into system directories for other users. This user has no other special privileges.

4. How does the Clark-Wilson model require authentication of users to be done?

   (a) A trusted user must vouch for the new user

   (b) Two-factor authentication must be used

   (c) If passwords are used, they must be at least 12 characters long, and use a mixture of letters, digits, and other characters

   (d) None of the above

5. What is a certificate? What is it used for?

6. Represent a security compartment label using the notation

   $$(\textit{security level} ; \textit{set of categories})$$

   where the security levels are "high", "medium", "low", or "unknown" (in decreasing order of trust) and the security categories are "dog", "cat", and "pig". Can a user cleared for $(\textit{medium} ; \{ \textit{dog} , \textit{cat} \})$ have read or write access (or both or neither) to documents classified in each of the following ways under the Bell-LaPadula model?

   (a) $(\textit{high} ; \{ \textit{dog} \})$

   (b) $(\textit{low} ; \{ \textit{dog} \})$

   (c) $(\textit{medium} ; \{ \textit{dog} , \textit{cat} \})$

   (d) $(\textit{unknown} ; \{ \textit{pig} \})$

   (e) $(\textit{high} ; \{ \textit{dog} , \textit{pig} , \textit{cat} \})$