Week 1 Practice Quiz

1. What is the difference between robust programming and secure programming?
   - Robust programming deals with errors whether or not they are a security problem; secure programming deals with errors that are security problems
   - Robust programming deals with speed and secure programming deals with security.
   - Robust programming prevents buffer overflows; secure programming handles them should they occur.
   - Robust programming is the opposite of secure programming.

2. Fill in the blanks with the correct phrases from options below:

   Security policies _____ and security mechanisms _____.

   - say what is and is not allowed, enforce the policy
   - state an ideal of what is, and is not, allowed - describe what is, and is not, allowed and can be properly implemented
   - enforce what is and is not allowed, check that the enforcement is effective here
   - is derived from government requirements, are based on, or are, commercial offerings

3. Consider a program that uses a cryptographic library obtained from a third party.

   Which of the following is most likely to be true?

   - If the cryptographic algorithms are used in the library have been examined and confirmed to be strong by experts, then the library is safe to use.
   - The cryptographic routines in the library have been thoroughly tested, so the library can be used without precautions.
   - The programmer must take care that all inputs to the library are checked to ensure they match what the library expects.
   - The programmer should never use a library from a third party; she should implement the cryptography herself, to ensure the algorithms are implemented correctly.

   Correct This is also true for other programs when your program depends upon them. When you get things from the environment, from the registry or from environment variables, that's really a form of input, so check your input.

4. When a user tries to log in, she enters a login name and a password. The computer checks that the login name is that of an authorized user and if not, gives the error message "Bad login name" and requests another name and password. If the login name is valid, it checks the password and if that does not correspond to the named user, it gives the error message "Bad password" and requests another password.

   Which of the following best describes this procedure?

   - It is poor security, because if the password is wrong, the system tells the user the password is wrong and then requests another password. It should restart the login process.
   - It is good security, because it tells the user exactly what the problem is; that way, the user can report the precise error to the help desk.
   - It is good security, because unless a valid login name and correct corresponding password are entered, the system denies access.
   - It is poor security, because a user can tell whether a guessed login name is a valid one.

   Correct If either the login name or password is invalid, the system should print simply "Error in login" after both have been entered.

5. What are the two key concepts of secure programming?

   - Protection and programming
   - Privilege and protection
   - Logging and auditing
   - Programming and privilege

   Correct Privilege means, that as a user you have certain rights and abilities to affect a computer system. A regular user has privileges to affect his own account. An administrator or root user can affect more domains. A protection domain means everything that a program can access and everything it can do when the user has access.

6. Which of the following should you do in secure programming?

- Buffer overflows
- Numeric overflows
- Checking the input for validity
- Grant more privileges than necessary

Correct Checking inputs is particularly critical if the inputs contain instructions; for example, if the input consists of commands that your program is to run, spawning a subcommand interpreter, or subshell, you must know how the execution of those commands are constrained.

7. Complete the sentence:

   Buffer overflows are _____ a security problem.

   - Never
   - Not yet
   - Sometimes
   - Always

   Correct If I write a program that has a buffer overflow in it, then I exploit that buffer overflow. I am therefore able to get access to my own account through that buffer overflow, because the program does not escalate privileges. That's not a security problem, because I am authorized to have access to my account. But it's certainly a robustness problem because I got the program to do something that it shouldn't do.