Week 2 Practice Quiz

1. Fill in the blanks: The principle of _____ says that security mechanisms should not add to the difficulty of accessing a resource; it is an idealized version of the principle of _____, which says that security mechanisms should match the user's mental model, so he or she is not surprised by what is required.
   - psychological acceptability, least astonishment
   - economy of mechanism, open design
   - least privilege, psychological acceptability
   - least astonishment, least privilege

The Saltzer and Schroeder principle is called "psychological acceptability". The problem is that's an idealistic statement, but in practice it's infeasible. Because, for example, a password is a security mechanism. When you log in, you type in your login name, and then it asks you for your password,— and it violates this principle. It's a very small violation, but in order to keep things clean, that's why they change it to least astonishment.

2. Which of the following is part of the principle of fail-safe defaults?
   - If an action fails, the system or program shuts down to prevent any compromise.
   - If an action succeeds, attackers will fail and the system will be safe.
   - If an action fails, the system ensures it enters a safe state.
   - If an action succeeds, log entries are not made as they are unnecessary; logs record problems.

When failure occurs, the system should always "fail safe" in the sense that when failure occurs, the system is just as secure as when this process that failed began. So, in other words, in failing, you don't give away any information or privileges.

3. Which of the following is a violation of the principle of open design?
   - Keeping the code in a cryptographic library secret to keep attackers from breaking it
   - Keeping source code secret to protect proprietary rights over it
   - Publishing a design in a classified journal to comply with a regulation
   - Keeping passwords and cryptographic keys secret to keep attackers from logging into systems and reading files

Open design simply says security should not depend upon secrecy of design or implementation. That's it. Programs that do depend on the security does depend on this are often called security by obscurity, and it's very bad because that means if the secrecy is broken, you're wide open. You're completely vulnerable.

4. Which principle is reflected by the structure of a castle with a moat, two walls, and a keep?

- Principle of complete mediation
- Principle of economy of mechanism
- Principle of least privilege
- Principle of separation of privilege

Separation of privilege requires multiple conditions to be satisfied in order to gain access, such as overcoming the moat, climbing the walls, and entering the keep.

5. Which of the following is part of the principle of fail-safe defaults?

- Deny access by default
- Neither grant nor deny access by default; when a request to access a resource is made, notify a system administrator to decide whether the access is safe or it should fail.
- Grant access by default; this makes the users safe against a failure to get access to needed resources
- Neither grant nor deny access by default; when a request to access a resource is made, notify the owner of the resource to decide whether the access is safe or it should fail.

6. Which of the principles does using complex interfaces and code violate? Pick the best one.

- Principle of economy of mechanism
- Principle of least privilege
- Principle of least common mechanism
- Principle of complete mediation

Correct Economy of mechanism speaks to simplicity, the opposite of complexity. If it relates to privilege, sharing, and access checking, it would not be wrong.