ECS 235B Module 19 Tranquility

Principle of Tranquility

- Raising object's security level
  - Information once available to some subjects is no longer available
  - Usually assume information has already been accessed, so this does nothing
- Lowering object's security level
  - The *declassification problem*
  - Essentially, a "write down" violating *-property
  - Solution: define set of trusted subjects that *sanitize* or remove sensitive information before security level lowered

Types of Tranquility

- Strong Tranquility
  - The clearances of subjects, and the classifications of objects, do not change during the lifetime of the system
- Weak Tranquility
  - The clearances of subjects, and the classifications of objects, do not change in a way that violates the simple security condition or the *-property during the lifetime of the system

Example: Trusted Solaris

- Security administrator can provide specific authorization for a user to change the MAC label of a file
  - “downgrade file label” authorization
  - “upgrade file label” authorization
- User requires additional authorization if not the owner of the file
  - “act as file owner” authorization

Principles of Declassification

- Principle of Semantic Consistency
  - As long as semantics of components that do not do declassification do not change, the components can be altered without affecting security
- Principle of Occlusion
  - A declassification operation cannot conceal an *improper* declassification
- Principle of Conservativity
  - Absent any declassification, the system is secure
- Principle of Monotonicity of Release
  - When declassification is performed in an authorized manner by authorized subjects, the system remains secure

Quiz

What is the difference between strong and weak tranquility?

1. Strong tranquility is when only one trusted subject is required to change the security classification of an object; weak tranquility is when many are required.
2. Strong tranquility is when many trusted subjects are required to change the security classification of an object; weak tranquility is when only one is required.
3. Strong tranquility disallows changes to the security classification of an object; weak tranquility allows such changes provided they do not change in a way that violates the simple security condition, *-property, or the ds-property.
4. Strong tranquility disallows changes to the security classification of an object; weak tranquility allows the security classification to be raised but not lowered.