# Outline for October 16, 2014

**Reading:** *text*, §5.1–5.2.1, 5.3–5.4, 6.1–6.2, 6.4

1. Goals of confidentiality policies
2. Bell-LaPadula Model with levels only
   a. Security levels
   b. Simple security property
   c. *-property
   d. Discretionary security property
3. Full Bell-LaPadula Model
   a. Add in compartments
   b. *dom* relation
   c. BLP as lattice structure
   d. Simple security property
   e. *-Property
   f. Discretionary security property
4. Range of levels
5. Basic Security Theorem
6. Example: Trusted Solaris System
7. Tranquility
   a. Strong tranquility
   b. Weak tranquility
   c. Declassification problem
8. System Z and the controversy
9. Requirements of integrity models
10. Biba Model
    a. Low-water-mark policy
    b. Ring policy
    c. Strict integrity
11. Clark-Wilson Model
    a. Theme: military model does not provide enough controls for commercial fraud, etc. because it does not cover the right aspects of integrity
    b. Components
       i. Constrained Data Items (CDI) to which the model applies
       ii. Unconstrained Data Items (UDIs) to which no integrity checks are applied
       iii. Integrity Verification Procedures (IVP) that verify conformance to the integrity spec when IVP is run
       iv. Transaction Procedures (TP) takes system from one well-formed state to another
12. Certification and enforcement rules of the Clark-Wilson Model
    a. C1. All IVPs must ensure that all CDIs are in a valid state when the IVP is run.
    b. C2. All TPs must be certified to be valid, and each TP is associated with a set of CDIs it is authorized to manipulate.
    c. E1. The system must maintain these lists and must ensure only those TPs manipulate those CDIs.
    d. E2. The system must maintain a list of User IDs, TP, and CDIs that that TP can manipulate on behalf of that user, and must ensure only those executions are performed.
    e. C3. The list of relations in E2 must be certified to meet the separation of duty requirement.
    f. E3. The system must authenticate the identity of each user attempting to execute a TP.
    g. C4. All TPs must be certified to write to an append-only CDI (the log) all information necessary to reconstruct the operation.

h. C5. Any TP taking a UDI as an input must be certified to perform only valid transformations, else no transformations, for any possible value of the UDI. The transformation should take the input from a UDI to a CDI, or the UDI is rejected (typically, for edits as the keyboard is a UDI).
i. E4. Only the agent permitted to certify entities may change the list of such entities associated with a TP. An agent that can certify an entity may not have any execute rights with respect to that entity