Outline for May 1, 2003

1. Requirements
   a. Users will not write their own programs, but will use existing production programs and databases.
   b. Programmers will develop and test programs on a non-production system; if they need access to actual data, they will be given production data via a special process, but will use it on their development system.
   c. A special process must be followed to install a program from the development system onto the production system.
   d. The special process must be controlled and audited.
   e. The management and auditors must have access to both the system state and to the system logs that are generated.
2. Biba
   a. Low-water-mark policy
   b. Ring policy
   c. Strict integrity
3. Lipner
   a. Bell-LaPadula component
   b. Add in Biba
4. Clark-Wilson
   a. Theme: military model does not provide enough controls for commercial fraud, etc. because it does not cover the right aspects of integrity
   b. Data items: "Constrained Data Items" (CDI) to which the model applies, "Unconstrained Data Items (UDIs) to which no integrity checks are applied, "Integrity Verification Procedures" (IVP) that verify conformance to the integrity spec when IVP is run, "Transaction Procedures" (TP) takes system from one well-formed state to another
5. Certification and enforcement rules:
   C1. All IVPs must ensure that all CDIs are in a valid state when the IVP is run
   C2. All TPs must be certified to be valid, and each TP is assocated with a set of CDIs it is authorized to manipulate
   E1. The system must maintain these lists and must ensure only those TPs manipulate those CDIs
   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.
   C3. The list of relations in E2 must be certified to meet the separation of duty requirement.
   E3. The sysem must authenticate the identity of each user attempting to execute a TP.
   C4. All TPs must be certified to write to an append-only CDI (the log) all information necessary to resonstruct the operation.
   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).
   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