Outline for May 10, 2005

1. 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
2. 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
3. Chinese Wall Policy
   a. Arises as legal defense to insider trading on London stock exchange
   b. Low-level entities are objects; all objects concerning the same corporation form a CD (company dataset); CDs whose corporations are in competition are grouped into COIs (Conflict of Interest classes)
   c. Intuitive goal: keep one subject from reading different CDs in the same COI, or reading one CD and writing to another in same COI
   d. Simple Security Property: Read access granted if the object (a) is in the same CD as an object already accessed by the subject, or (b) is in a CD in an entirely different COI. Assumes correct initialization
   e. Theorems: (1) Once a subject has accessed an object, only other objects in that CD are available within that COI; (2) subject has access to at most 1 dataset in each COI class
   f. Exceptions: sanitized information
   g. *-Property: Write access is permitted only if (a) read access is permitted by the simple security property; and (b) no object in a different CD in that COI can be read, unless it contains sanitized information
   h. Key result: information can only flow within a CD or from sanitized information
   i. Comparison to BLP: (1) ability to track history; (2) in CW, subjects choose which objects they can access but not in BLP; (3) CW requires both mandatory and discretionary parts, BLP is mandatory only.
   j. Comparison to Clark-Wilson: specialization of Clark-Wilson
4. CISS
   a. Intended for medical records; goals are confidentiality, authentication of annotatorsa and integrity
   b. Patients, personal health information, clinician
   c. Assumptions and origin of principles
   d. Access principles
   e. Creation principle
   f. Deletion principle
   g. Confinement principle
   h. Aggregation principle
   i. Enforcement principle

   j. Comparison to Bell-LaPadula: lattice structure but different focus
   k. Comparison to Clark-Wilson: specialization

5. ORCON
   a. Originator controls distribution
   b. DAC, MAC inadequate
   c. Solution is combination
6. Role-based Access Control (RBAC)
   a. Definition of role
   b. Partitioning as job function
   c. Containment