Outline for May 14, 1997

1. Greetings and Felicitations
   a. All UC students: please get me homework #1 by tomorrow if you've not done so, so I can turn them all back by Friday, and homework #2s by Monday. NTU students: add one week, please.
2. BLP
   a. Add in discretionary security policy
3. BLP: formally
   a. Elements of system: si subjects, oi objects,
   b. State space V = B×M×F where:
      B set of current accesses (ie, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: fs is security level associated with each subject, fo security level associated with each object, and fc current security level for each subject
   c. Set of requests is R
   d. Set of decisions is D
   e. W < R×D×V×V is motion from one state to another.
   f. System S(R, D, W, z0) < X×Y×Z such that (x, y, z) in S(R, D, W, z0) iff (xt, yt, zt, zt–1) in W for each i in T; latter is an action of system
   g. THM: S(R, D, W, z0) satisfies the simple security property for any initial state z0 that satisfies the simple security property iff W satisfies the following conditions for each action (Ri, Di, (b', M', f'), (b, M, f)):
      (i) each (s, o, x) in b' – b satisfies the simple security condition relative to f' (ie, x is not read, or x is read and fs(s) dominates fo(o)
      (ii) if (s, o, x) in b does not satisfy the simple security condition relative to f', then (s, o, x) not in b'
   h. THM: S(R, D, W, z0) satisfies the *-property relative to S', a subset of S, for any initial state z0 that satisfies the *-property relative to S' iff W satisfies the following conditions for each action (Ri, Di, (b', M', f'), (b, M, f)):
      (i) for each s in S', any (s, o, x) in b' – b satisfies the *-property with respect to f'
      (ii) for each s in S', if (s, o, x) in b does not satisfy the *-property with respect to f', then (s, o, x) not in b'
   i. THM: S(R, D, W, z0) satisfies the ds-property iff the initial state z0 satisfies the ds-property and W satisfies the following conditions for each action (Ri, Di, (b', M', f'), (b, M, f)):
      (i) if (sk, oi, x) in b' – b, then x in M'k, i;
      (ii) if (sk, oi, x) in b and x not in M'k,i then (sk, oi, x) not in b'
   j. THM: BST: A system S(R, D, W, z0) is secure iff z0 is a secure state and W satisfies the conditions of the above three theorems for each action.
4. Biba
   a. Integrity levels and trust
   b. No reads down
   c. No writes up

5. 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: “Condtrained 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
   c. 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 preformed.
      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