Notes for February 23, 1998

1. Greetings and felicitations!
   a. **Reading**: Pfleeger, pp. 273–276; Garfinkel & Spafford, pp. 271–288, 340–356
2. Puzzle
3. Practise: detecting writing
   a. Integrity check files à la binaudit, tripwire; go through signature block

[*ended here*]

   b. LOCUS approach: encipher program, decipher as you execute.
   c. Co-processors: checksum each sequence of instructions, compute checksum as you go; on difference, complain
4. Biba: mathematical dual of BLP
   a. P may read O if $L(P) \leq L(O)$ and $C(P) \subseteq C(O)$
   b. P may write O if $L(O) \leq L(P)$ and $C(O) \subseteq C(P)$
   c. Combined with BLP: continue example
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 performed.

[*ended here*]

   d. 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 associ-

ated with a TP. An agent that can certify an entity may not have any execute rights with respect to that entity.

6. Chinese Wall
   a. Theme: market analyst must uphold confidentiality requirements (no use of insider knowledge) but can advise different corporations.
   b. Data items: "objects" (axiomatic), "company datasets" (CD; sets of objects belonging to a company), "conflict of interest classes" (COI; sets of company datasets for companies in competition)
   c. Simple Security Property: Access is only granted if the object requested (a) is in the same CD as an object already accessed by the subject, or (b) belongs to an entirely different COI.
   d. Can derive: if subject accesses object, only other objects in that same CD can be accessed within the same COI. Also, subject has access to at most one CD in each COI.
   e. Sanitization: if it's sanitized then the model does not impose any restrictions.
   f. *-Property: Write access is only granted if (a) access is permitted by the simple security rule, and (b) no object can be read which is in a different CD to the one for which write access is requested and contains unsanitized information.
   g. Can derive: the flow of unsanitized information is confined to its own CD, but sanitized information may flow freely throughout system
   h. BLP: not satisfactory. Say user A accesses company dataset B. But then A is sick, so management has user C do the access. Not possible unless we know for certain C has not accessed anything else in B's COI; BLP doesn't save this info. Also, BLP fixes what datasets a subject can access; the Wall allows access.
   i. Clark-Wilson: can model it exactly.