Notes for February 6, 1998

1. Greetings and felicitations!
   a. **Reading**: Pfleeger, pp. 277–280
2. Puzzle
   a. Anyone can drop anything in there – and they usually do!
3. Lock and Key
   a. Associate with each object a lock; associate with each process that has access to object a key (it's a cross between ACLs and C-Lists)
   b. Example: use crypto (Gifford). *X* object enciphered with key *K*. Associate an opener *R* with *X*. Then:
   OR-Access: *K* can be recovered with any D_i in a list of *n* deciphering transformations, so $R = (E_1(K), E_2(K), ..., E_n(K))$ and any process with access to any of the D_i's can access the file
   AND-Access: need all *n* deciphering functions to get *K*: $R = E_1(E_2(...E_n(K)...))$
4. Mandatory vs. Discretionary;
   a. security levels
   b. categories
5. Bell-LaPadula Model
   a. Simple Security Property: no reads up
   b. Star Property: no writes down
   c. Discretionary Security Property: if mandatory controls say it's okay, check discretionary controls.
   d. Basic Security Theorem: A system is secure if its initial state is secure and no action violates the above rules.

[*ended here*]

6. ORCON (Originator Controlled; Graubert)
   a. Document/information can be passed on with approval of originator; real world justification is that originator of document trusts recipients not to release documents which they should not.
   b. Untrusted subject *x* marks object *O* ORCON on behalf of organization *X* and indicates it is releasable to subjects acting on behalf of organization *Y.*
   not releasable to subjects acting on behalf of other organizations without *X*'s permission
   any copies made have the same restriction
   c. DAC: can't do this as the restriction would not copy over (*y* reads *O* into *C*, puts its own ACL on *C*)
   d. MAC: separate category with*O*, *x*, *y. y* wants to read *O*, copy to *C*; MAC means *C* has same category as *O*, *x*, *y*, so can't give *z* access to *C*.
   Say a new organization *w* wants to provide data in *B* to *y* but not to be shared with *x* or *z*.

Can't use *O*'s category. Hence you get explosion of categories.
Real world parallel: individuals are "briefed" into a category and those represent a formal "need to know" policy that is standard across the entity; ORCON has no central clearing-house to categorize data; originator makes rules.

7. Solution?
   a. owner of object can't change ACL's relationship with object (MAC characteristic)
   b. on copy, ACL is copied as well (MAC characteristic)
   c. access control restrictions can be tailored on a subject/object basis (DAC characteristic)