Notes for February 9, 1998

1. Greetings and felicitations!
   a. **Reading**: Pfleeger, pp. 176–198, 277–280; Garfinkel & Spaddord, pp. 327–340
2. Puzzle
3. Capabilities
   a. C-Lists
   b. copy right (copy flag)
4. Lattice Model
   a. Set of classes *SC* is a partially ordered set under relation ≤ with GLB (⊗), LUB (⊕)
   b. Note: ≤ is reflexive, transitive, antisymmetric
   c. Application to MLS: forms a lattice with elements being the Cartesian product of the linear lattice of levels and the subset lattics of categories
   d. Examples: (A, C) ≤ (A', C') iff A ≤ A' and C ⊆ C';
   (A, C) ⊕ (A', C") = (max(A, A'), C ∪ C')
   (A, C) ⊗ (A', C') = (min(A, A'), C ∩ C')
5. 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 clearinghouse to categorize data; originator makes rules.
6. 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)
7. Malicious logic
   a. Quickly review Trojan horses, viruses, bacteria

   b. Logic Bombs
   c. Worms (Schoch and Hupp)
8. Review trust and TCB
   a. Notion is informal
   b. Assume trusted components called by untrusted programs

[*ended here*]