Outline for April 14, 2006

Reading: *text*, §4.1, 4.7, 5.1—5.2, 30

1. Greetings and felicitations!
2. Security policies and mechanisms
   a. Policy vs. mechanism
   b. Secure, precise
   c. Observability postulate
   d. Theorem: for any program p and policy c, there is a secure, precise mechanism m^* such that, for all security mechanisms m associated with p and c, $m^* \approx m$
   e. Theorem: There is no effective procedure that determines a maximally precise, secure mechanism for any policy and program
3. Bell-LaPadula Model (security classifications only)
   a. Security clearance, classification
   b. Simple security condition (no reads up)
   c. *-property (no writes down)
   d. Discretionary security property
   e. Basic Security Theorem: if it is secure and transformations follow these rules, it will remain secure
4. Lattice models
   a. Poset, $\leq$ the relation
   b. Reflexive, antisymmetric, transitive
   c. Greatest lower bound, least upper bound
   d. Example with complex numbers