Outline for January 27, 2012

Reading: §4.6–4.7, [LT05], 5.2.1–5.2.2

1. English policy
   a. Authorized Use Policy
   b. Electronic Mail Policy
2. Secure, precise
   a. Observability postulate
   b. 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, $m^* \approx m$
   c. Theorem: There is no effective procedure that determines a maximally precise, secure mechanism for any policy and program
3. Bell-LaPadula Model: intuitive, security classifications only
   a. Show level, categories, define clearance and classification
   b. Lattice: poset with $\leq$ relation reflexive, antisymmetric, transitive; greatest lower bound, least upper bound
   c. Apply lattice
      i. Set of classes SC is a partially ordered set under relation dom with glb (greatest lower bound), lub (least upper bound) operators
      ii. Note: dom is reflexive, transitive, antisymmetric
      iii. Example: (A, C) dom (A', C') iff $A \leq A'$ and $C \subseteq C'$;
      $lub((A, C), (A', C')) = (max(A, A'), C \cup C')$,
      $glb((A, C), (A', C')) = (min(A, A'), C \cap C')$
   d. Simple security condition (no reads up), *-property (no writes down), discretionary security property
   e. Basic Security Theorem: if it is secure and transformations follow these rules, it will remain secure
   f. Maximum, current security level