Outline for January 26, 1999

1. Greetings and felicitations!
   a. Please get your project proposals in as soon as possible, so you can get started
2. Bell-LaPadula Model
   a. Go through security levels, categories, compartments
   b. Describe simple security property (no reads up) and *-property (no writes down)
   c. State Basic Security Theorem: if it's secure and transformations follow these rules, it's still secure
   d. Add in discretionary security policy
3. BLP: formally
   a. Elements of system: si subjects, oi objects,
   b. State space $V = B \times M \times F$ where:
      B set of current accesses (*i.e.*, access modes each subject has currently to each object);
      M access permission matrix;
      F consists of 3 functions: f_s is security level associated with each subject, f_o security level associated with each object, and f_c current security level for each subject
   c. Set of requests is R
   d. Set of decisions is D
   e. $W \subseteq R \times D \times V \times V$ is motion from one state to another.
   f. System $\Sigma(R, D, W, z_0) \subseteq X \times Y \times Z$ such that $(x, y, z) \in \Sigma(R, D, W, z_0)$ iff $(x_t, y_t, z_t, z_{t-1}) \in W$ for each $i \in T$; latter is an action of system
   g. Theorem: $\Sigma(R, D, W, z_0)$ satisfies the simple security property for any initial state z_0 that satisfies the simple security property iff W satisfies the following conditions for each action $(R_i, D_i, (b', M', f'), (b, M, f))$:
      (i) each $(s, o, x) \in b' - b$ satisfies the simple security condition relative to f' (ie, x is not read, or x is read and $f_s(s)$ dominates $f_o(o)$
      (ii) if $(s, o, x) \in b$ does not satisfy the simple security condition relative to f', then $(s, o, x) \notin b'$
   h. Theorem: $\Sigma(R, D, W, z_0)$ satisfies the *-property relative to $S' \subseteq S$, for any initial state z_0 that satisfies the *-property relative to S' iff W satisfies the following conditions for each action $(R_i, D_i, (b', M', f'), (b, M, f))$:
      (i) for each $s \in S'$, any $(s, o, x) \in b' - b$ satisfies the *-property with respect to f'
      (ii) for each $s \in S'$, if $(s, o, x) \in b$ does not satisfy the *-property with respect to f', then $(s, o, x) \notin b'$
   i. Theorem: $\Sigma(R, D, W, z_0)$ satisfies the ds-property iff the initial state z_0 satisfies the ds-property and W satisfies the following conditions for each action $(R_i, D_i, (b', M', f'), (b, M, f))$:
      (i) if $(s_k, o_i, x) \in b' - b$, then $x \in M'[k, i]$;
      (ii) if $(s_k, o_i, x) \in b$ and $x \notin M'[k, i]$ then $(s_k, o_i, x) \notin b'$
   j. Basic Security Theorem: A system $\Sigma(R, D, W, z_0)$ is secure iff z_0 is a secure state and W satisfies the conditions of the above three theorems for each action.
4. Biba
   a. Integrity levels and trust
   b. No reads down
   c. No writes up