Outline for January 29, 2008

1. **BLP: formally**
   - Elements of system: s, subjects, o, objects
   - State space $V = B \times M \times F \times H$ where:
     - $B$ set of current accesses (i.e., access modes each subject currently to each object);
     - $M$ access permission matrix;
     - $F$ consists of 3 functions: $f_s$ security level associated with each subject, $f_o$ security level associated with each object, and $f_c$ current security level for each subject;
     - $H$ hierarchy of system objects, functions $h: O \rightarrow \mathcal{R}(O)$ with two properties:
       - If $o_i \neq o_j$, then $h(o_i) \cap h(o_j) = \emptyset$
       - There is no set $\{o_1, ..., o_k\} \subseteq O$ such that for each $i$, $o_{i+1} \in h(o_i)$ and $o_{k+1} = o_1$
   - Set of requests is $R$
   - Set of decisions is $D$
   - $W \subseteq R \times D \times V \times V$ is motion from one state to another.
   - 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 $(x_i, y_i, z_i, z_{i+1}) \in W$ for each $i \in T$; latter is an action of system
   - Theorem: $\Sigma(R, D, W, z_0)$ satisfies the simple security condition for any initial state $z_0$ that satisfies the simple security condition iff $W$ satisfies the following conditions for each action $(r, d, (b', m', f', h'), (b, m, f, h))$:
     - Each $(s, o, x) \in b' - b$ satisfies the simple security condition relative to $f$ (i.e., $x$ is not read, or $x$ is read and $f_s(s) \subseteq \text{dom} f_o(o))$
     - If $(s, o, x) \in b$ does not satisfy the simple security condition relative to $f$, then $(s, o, x) \notin b' - b$
   - 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 $(r, d, (b', m', f', h'), (b, m, f, h))$:
     - For each $x \in S'$, any $(s, o, x) \in b' - b$ satisfies the *-property with respect to $f'$
     - For each $x \in S'$, if $(s, o, x) \in b$ does not satisfy the *-property with respect to $f'$, then $(s, o, x) \notin b' - b'$
   - 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 $(r, d, (b', m', f', h'), (b, m, f, h))$:
     - If $(s, o, x) \in b' - b$, then $x \in m'[s, o]$;
     - If $(s, o, x) \in b$ and $x \in m'[s, o]$, then $(s, o, x) \notin b' - b'$
   - 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.

2. **Using the model**
   - Define ssc-preserving, *-property-preserving, ds-property-preserving
   - Define relation $W(o)$
   - Show conditions under which rules are ssc-preserving, *-property-preserving, ds-property-preserving
   - Show when adding a state preserves those properties
   - Example instantiation: get-read for Multics

3. **Tranquility**
   - Strong tranquility
   - Weak tranquility

4. **System Z and the controversy**