Outline for April 24, 2013

Reading: §5.2.3–5.2.4, 5.3, 5.4; *handout* **Assignments due:** Homework #2, due April 26, 2013

1. Bell-LaPadula: formal model
   a. Set of requests is R
   b. Set of decisions is D
   c. $W \subseteq R \times D \times V \times V$ is motion from one state to another.
   d. 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 $t \in T$; latter is an action of system
   e. 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 $(r_i, d_i, (b', m', f', h'), (b, m, f, h))$:
      i. 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 $f_s(s)$ *dom* $f_o(o)$); and
      ii. if $(s, o, x) \in b$ does not satisfy the simple security condition relative to f', then $(s, o, x) \notin b'$
   f. 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 $(r_i, d_i, (b', m', f', h'), (b, m, f, h))$:
      i. for each $s \in S'$, any $(s, o, x) \in b' - b$ satisfies the *-property with respect to f'; and
      ii. for each $s \in S'$, if $(s, o, x) \in b$ does not satisfy the *-property with respect to f', then $(s, o, x) \notin b'$
   g. 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 $(r_i, d_i, (b', m', f', h'), (b, m, f, h))$:
      i. if $(s, o, x) \in b' - b$, then $x \in m'[s, o]$; and
      ii. if $(s, o, x) \in b$ and $x \in m'[s, o]$, then $(s, o, x) \notin b'$
   h. 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
   a. Define ssc-preserving, *-property-preserving, ds-property-preserving
   b. Define relation $W(\omega)$
   c. Show conditions under which rules are ssc-preserving, *-property-preserving, ds-property-preserving
   d. Show when adding a state preserves those properties
   e. Example instantiation: get-read for Multics
3. Tranquility
   a. Strong tranquility
   b. Weak tranquility
4. System Z and the controversy