April 10, 2026 Outline

Reading: *text*, §5.2.3–5.4, 6.1 **Due:** Homework #1, due April 10; Project selection, due April 17

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 $i \in T$; latter is an action of system
   (e) $(s,o,p) \in S \times O \times P$ satisfies the simple security condition relative to f iff:
      i. $p = \underline{e}$ or $p = \underline{a}$; or
      ii. $p = \underline{r}$ or $p = \underline{w}$ and $f_s(s) dom f_o(o))$
   (f) 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'; and
      ii. if $(s,o,x) \in b$ does not satisfy the simple security condition relative to f', then $(s,o,x) \notin b'$
   (g) Let $b(s : p_1,\ldots,p_n)$ be the set of all objects that s has $p_1,\ldots,p_n$ access to. Then state (b,m,f,h) satisfies the *-property iff for each $s \in S$ the following holds:
      i. $b(s : \underline{a}) \neq \varnothing \Rightarrow [\forall o \in b(s : \underline{a})[f_o(o) dom f_c(s)]]$;
      ii. $b(s : \underline{w}) \neq \varnothing \Rightarrow [\forall o \in b(s : \underline{w})[f_o(o) = f_c(s)]]$; and
      iii. $b(s : \underline{r}) \neq \varnothing \Rightarrow [\forall o \in b(s : \underline{r})[f_c(s) dom f_o(o)]]$.
   (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 $(r_i,d_i,(b',m',f',h'),(b,m,f,h))$:
      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 $(s,o,x) \notin b'$
   (i) State (b,m,f,h) satisfies the discretionary security property iff for each $(s,o,p) \in b$, then $p \in m[s,o]$.
   (j) Theorem: $\Sigma(R,D,W,z_0)$ satisfies the discretionary security property for any initial state z_0 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 discretionary security property; and
      ii. if $(s,o,x) \in b$ does not satisfy the discretionary security property, then $(s,o,x) \notin b'$
   (k) Theorem: $\Sigma(R,D,W,z_0)$ sis a secure system if the initial state z_0 is a secure state and W satisfies the conditions for the above three theorems
2. Using the Bell-LaPadula 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
4. System Z and the controversy
5. Integrity policy requirements