April 8, 2026 Outline

Reading: *text*, §4, 5–5.2.1, 5.2.3 **Due:** Homework #1, due April 10; Project selection, due April 17

1. Policy , models, and mechanisms
2. Policy languages
3. 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
4. Review Bell-LaPadula Model: intuitive, security classifications only
   (a) Level, categories, define clearance and classification
   (b) Simple security condition (no reads up), *-property (no writes down), discretionary security property
   (c) Basic Security Theorem: if it is secure and transformations follow these rules, it will remain secure
5. Review Bell-LaPadula Model: intuitive, now add category sets
   (a) Apply lattice
   (b) Simple security condition (no reads up), *-property (no writes down), using the *dom* relation; discretionary security property
   (c) Basic Security Theorem: if it is secure and transformations follow these rules, it will remain secure
6. Maximum, current security level
7. 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