January 24, 2024 Outline

Reading: *text*, §5.2.2–5.2.3
Assignments: Extra Credit #B, due January 30; Homework #2, due February 2; Project selection, due January 26

Module 17 (Reading: *text*, §5.2.2)

1. Bell-LaPadula Model: intuitive, now add category sets
   (a) Apply lattice
      i. Set of classes *SC* is a partially ordered set under relation *dom* with *glb* (greatest lower bound), *lub* (least upper bound) operators
      ii. Note: *dom* is reflexive, transitive, antisymmetric
      iii. Example: (A,C) *dom* (A',C') iff $A \leq A'$ and $C \subseteq C'$;
      $lub((A,C),(A',C')) = (max(A,A'), C \cup C')$; and
      $glb((A,C),(A',C')) = (min(A,A'), C \cap C')$
   (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
2. Maximum, current security level
3. Example: Trusted Solaris

Module 18 (Reading: *text*, §5.2.3)

4. 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) 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 $(s,o,x) \notin b'$