ECS 235B Module 49
Introduction to Information Flow

Basics

- Bell-LaPadula Model embodies information flow policy
  - Given compartments *A*, *B*, info can flow from *A* to *B* iff *B dom A*
- So does Biba Model
  - Given compartments *A*, *B*, info can flow from *A* to *B* iff *A dom B*
- Variables *x*, *y* assigned compartments $\underline{x}$, $\underline{y}$ as well as values
  - Confidentiality (Bel-LaPadula): if $\underline{x}$ = *A*, $\underline{y}$ = *B*, and *B dom A*, then *y* := *x* allowed but not *x* := *y*
  - Integrity (Biba): if $\underline{x}$ = *A*, $\underline{y}$ = *B*, and *A dom B*, then *x* := *y* allowed but not *y* := *x*
- For now, focus on confidentiality (Bell-LaPadula)
  - We'll get to integrity later

Entropy and Information Flow

- Idea: information flows from *x* to *y* as a result of a sequence of commands *c* if you can deduce information about *x* before *c* from the value in *y* after *c*
- Formally:
  - *s* time before execution of *c*, *t* time after
  - $H(x_s \mid y_t) < H(x_s \mid y_s)$
  - If no *y* at time *s*, then $H(x_s \mid y_t) < H(x_s)$

Example 1

- Command is $x := y + z$; where:
  - x does not exist initially (that is, has no value)
  - $0 \leq y \leq 7$, equal probability
  - $z = 1$ with probability 1/2, $z = 2$ or 3 with probability 1/4 each
- s state before command executed; t, after; so
  - $\mathrm{H}(y_s) = \mathrm{H}(y_t) = –8(1/8) \lg (1/8) = 3$
- You can show that $H(y_s \mid x_t) = (3/32) \lg 3 + 9/8 \approx 1.274 < 3 = H(y_s)$
  - Thus, information flows from y to x

Example 2

- Command is

  if x = 1 **then** y := 0 **else** y := 1;

  where x, y equally likely to be either 0 or 1
- $H(x_s) = 1$ as x can be either 0 or 1 with equal probability
- $H(x_s \mid y_t) = 0$ as if $y_t = 1$ then $x_s = 0$ and vice versa
  - Thus, $H(x_s \mid y_t) = 0 < 1 = H(x_s)$
- So information flowed from x to y

Implicit Flow of Information

- Information flows from *x* to *y* without an *explicit* assignment of the form *y* := *f*(*x*)
    - *f*(*x*) an arithmetic expression with variable *x*
- Example from previous slide:

if *x* = 1 **then** *y* := 0 **else** *y* := 1;

- So must look for implicit flows of information to analyze program

Notation

- $\underline{x}$ means class of *x*
  - In Bell-LaPadula based system, same as “label of security compartment to which *x* belongs”
- $\underline{x} \le \underline{y}$ means “information can flow from an element in class of *x* to an element in class of *y*
  - Or, “information with a label placing it in class $\underline{x}$ can flow into class $\underline{y}$”

Quiz

What is the intuition underlying the use of entropy in information flow?

1. As information flows from one variable to another, the uncertainty in the source's value decreases
2. As information flows from one variable to another, the uncertainty in the destination's value decreases
3. As information flows from one variable to another, the uncertainty in the source's value increases
4. As information flows from one variable to another, the uncertainty in the destination's value increases