

## Lecture 15 Outline

**Reading:** *text*, §8.2–8.2

1. Composing deterministic, noninterference-secure systems
2. Nondeducibility
  - a. Event system
  - b. Deducibly secure
  - c. Composing deducibly secure systems
3. Generalized noninterference
  - a. Assumptions and nondeducibility
  - b. Composing generalized noninterference systems
  - c. Feedback-free systems
4. Restrictiveness
  - a. State machine model
  - b. Composing restrictive systems

### Table of Notation

<i>notation</i>	<i>meaning</i>
$C$	set of commands $(s, z)$ , where $s$ executes operation $z$
$C^*$	set of sequences of commands
$\pi''$	generalized noninterference analogue to the purge function $\pi_{G,A}$
$\epsilon$	empty string
$c_s$	sequence of commands
$P(c, \sigma_i)$	output from command $c$ being executed in state $\sigma_i$
$P^*(c_s, \sigma_i)$	outputs when command sequence $c_s$ is executed in state $\sigma_i$
$proj(s, c_s, \sigma_i)$	set of outputs in $P^*(c_s, \sigma_i)$ that subject $s$ is authorized to see
$w$	sequence of elements of $C$ leading up to current state
$cando(w, s, z)$	true if $s$ can execute $z$ in current state
$pass(s, z)$	give $s$ right to execute $z$
$w_n$	$v_1, \dots, v_n$ where $v_i \in C^*$
$prev(w_n)$	$w_{n-1}$
$last(w_n)$	$v_n$
$\pi_L$	projection function deleting all <i>High</i> inputs from trace