

## Outline for February 17, 2012

Reading: §8.2

---

1. Deterministic noninterference
  - a. Model of system
  - b. Example
  - c. Relationship of output to states
  - d. Projections and purge functions
2. Alternative definition of security policy
  - a. Output-consistent
  - b. Security policy
  - c. Alternate projection function
  - d. Noninterference-secure with respect to the policy  $r$
3. Unwinding Theorem
  - a. Locally respects
  - b. Transition-consistent
  - c. Unwinding theorem

### Table of Notation

<i>notation</i>	<i>meaning</i>
$S$	set of subjects $s$
$\Sigma$	set of states $\sigma$
$O$	set of outputs $o$
$Z$	set of commands $z$
$C$	set of state transition commands $(s, z)$ , where subject $s$ executes command $z$
$C^*$	set of possible sequences of commands $c_0, \dots, c_{n_i}$
$\nu$	empty sequence
$c_s$	sequence of commands
$T(c, \sigma_i)$	resulting state when command $c$ is executed in state $\sigma_i$
$T^*(c_s, \sigma_i)$	resulting state when command sequence $c_s$ is executed in state $\sigma_i$
$P(c, \sigma_i)$	output when command $c$ is executed in state $\sigma_i$
$P^*(c_s, \sigma_i)$	output 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
$\pi_{G,A}(c_s)$	subsequence of $c_s$ with all elements $(s, z)$ , $s \in G$ and $z \in A$ deleted
$dom(c)$	protection domain in which $c$ is executed
$\sim^{dom(c)}$	equivalence relation on system states
$\pi'_d(c_s)$	analogue to $\pi$ above, but with protection domain and subject included