

# ECS 235B Module 35

## Security Policy and the Unwinding Theorem

# Security Policy

- Partitions systems into authorized, unauthorized states
- Authorized states have no forbidden interferences
- Hence a *security policy* is a set of noninterference assertions
  - See previous definition

# Alternative Development

- System  $X$  is a set of protection domains  $D = \{ d_1, \dots, d_n \}$
- When command  $c$  executed, it is executed in protection domain  $dom(c)$
- Give alternate versions of definitions shown previously

# Security Policy

- $D = \{ d_1, \dots, d_n \}$ ,  $d_i$  a protection domain
- $r: D \times D$  a reflexive relation
- Then  $r$  defines a security policy
- Intuition: defines how information can flow around a system
  - $d_i r d_j$  means info can flow from  $d_i$  to  $d_j$
  - $d_i r d_i$  as info can flow within a domain

# Projection Function

- $\pi'$  analogue of  $\pi$ , earlier
- Commands, subjects absorbed into protection domains
- $d \in D, c \in C, c_s \in C^*$
- $\pi'_d(v) = v$
- $\pi'_d(c_s c) = \pi'_d(c_s) c$  if  $dom(c)rd$
- $\pi'_d(c_s c) = \pi'_d(c_s)$  otherwise
- Intuition: if executing  $c$  interferes with  $d$ , then  $c$  is visible; otherwise, as if  $c$  never executed

# Noninterference-Secure

- System has set of protection domains  $D$
- System is *noninterference-secure with respect to policy  $r$*  if

$$P^*(c, T^*(c_s, \sigma_0)) = P^*(c, T^*(\pi'_d(c_s), \sigma_0))$$

- Intuition: if executing  $c_s$  causes the same transitions for subjects in domain  $d$  as does its projection with respect to domain  $d$ , then no information flows in violation of the policy

# Output-Consistency

- $c \in C, dom(c) \in D$
- $\sim_{dom(c)}$  equivalence relation on states of system  $X$
- $\sim_{dom(c)}$  *output-consistent* if

$$\sigma_a \sim_{dom(c)} \sigma_b \Rightarrow P(c, \sigma_a) = P(c, \sigma_b)$$

- Intuition: states are output-consistent if for subjects in  $dom(c)$ , projections of outputs for both states after  $c$  are the same

# Lemma

- Let  $T^*(c_s, \sigma_0) \sim^d T^*(\pi'_d(c_s), \sigma_0)$  for  $c \in C$
- If  $\sim^d$  output-consistent, then system is noninterference-secure with respect to policy  $r$



# Proof

- $d = \text{dom}(c)$  for  $c \in \mathcal{C}$
- By definition of output-consistent,

$$T^*(c_s, \sigma_0) \sim^d T^*(\pi'_d(c_s), \sigma_0)$$

implies

$$P^*(c, T^*(c_s, \sigma_0)) = P^*(c, T^*(\pi'_d(c_s), \sigma_0))$$

- This is definition of noninterference-secure with respect to policy  $r$

# Unwinding Theorem

- Links security of sequences of state transition commands to security of individual state transition commands
- Allows you to show a system design is multilevel-secure by showing it matches specs from which certain lemmata derived
  - Says *nothing* about security of system, because of implementation, operation, *etc.* issues

# Locally Respects

- $r$  is a policy
- System  $X$  *locally respects*  $r$  if  $dom(c)$  being noninterfering with  $d \in D$  implies  $\sigma_a \sim^d T(c, \sigma_a)$
- Intuition: when  $X$  locally respects  $r$ , applying  $c$  under policy  $r$  to system  $X$  has no effect on domain  $d$

# Transition-Consistent

- $r$  policy,  $d \in D$
- If  $\sigma_a \sim^d \sigma_b$  implies  $T(c, \sigma_a) \sim^d T(c, \sigma_b)$ , system  $X$  is *transition-consistent* under  $r$
- Intuition: command  $c$  does not affect equivalence of states under policy  $r$

# Theorem

- $r$  policy,  $X$  system that is output consistent, transition consistent, and locally respects  $r$
- Then  $X$  noninterference-secure with respect to policy  $r$
- Significance: basis for analyzing systems claiming to enforce noninterference policy
  - Establish conditions of theorem for particular set of commands, states with respect to some policy, set of protection domains
  - Noninterference security with respect to  $r$  follows

# Proof

Must show  $\sigma_a \sim^d \sigma_b \Rightarrow T^*(c_s, \sigma_a) \sim^d T^*(\pi'_d(c_s), \sigma_b)$

- Induct on length of  $c_s$
- Basis: if  $c_s = v$ , then  $T^*(c_s, \sigma_a) = \sigma_a$  and  $\pi'_d(v) = v$ ; claim holds
- Hypothesis: for  $c_s = c_1 \dots c_n$ ,  $\sigma_a \sim^d \sigma_b \Rightarrow T^*(c_s, \sigma_a) \sim^d T^*(\pi'_d(c_s), \sigma_b)$

# Induction Step

- Consider  $c_s c_{n+1}$ . Assume  $\sigma_a \sim^d \sigma_b$  and look at  $T^*(\pi'_d(c_s c_{n+1}), \sigma_b)$
- 2 cases:
  - $dom(c_{n+1})rd$  holds
  - $dom(c_{n+1})rd$  does not hold

# $dom(c_{n+1})rd$ Holds

$$T^*(\pi'_d(c_s c_{n+1}), \sigma_b) = T^*(\pi'_d(c_s) c_{n+1}, \sigma_b) = T(c_{n+1}, T^*(\pi'_d(c_s), \sigma_b))$$

- By definition of  $T^*$  and  $\pi'_d$

$$\sigma_a \sim^d \sigma_b \Rightarrow T(c_{n+1}, \sigma_a) \sim^d T(c_{n+1}, \sigma_b)$$

- As  $X$  transition-consistent

$$T(c_{n+1}, T^*(c_s, \sigma_a)) \sim^d T(c_{n+1}, T^*(\pi'_d(c_s), \sigma_b))$$

- By transition-consistency and IH

$$T(c_{n+1}, T^*(c_s, \sigma_a)) \sim^d T^*(\pi'_d(c_s c_{n+1}), \sigma_b)$$

- By substitution from earlier equality

$$T^*(c_s c_{n+1}, \sigma_a) \sim^d T^*(\pi'_d(c_s c_{n+1}), \sigma_b)$$

- By definition of  $T^*$

proving hypothesis



# $dom(c_{n+1})rd$ Does Not Hold

$$T^*(\pi'_d(c_s c_{n+1}), \sigma_b) = T^*(\pi'_d(c_s), \sigma_b)$$

- By definition of  $\pi'_d$

$$T^*(c_s, \sigma_a) = T^*(\pi'_d(c_s c_{n+1}), \sigma_b)$$

- By above and IH

$$T(c_{n+1}, T^*(c_s, \sigma_a)) \sim^d T^*(c_s, \sigma_a)$$

- As  $X$  locally respects  $r$ ,  $\sigma \sim^d T(c_{n+1}, \sigma)$  for any  $\sigma$

$$T(c_{n+1}, T^*(c_s, \sigma_a)) \sim^d T^*(\pi'_d(c_s c_{n+1}), \sigma_b)$$

- Substituting back

proving hypothesis

# Finishing Proof

- Take  $\sigma_a = \sigma_b = \sigma_0$ , so from claim proved by induction,

$$T^*(c_s, \sigma_0) \sim^d T^*(\pi'_d(c_s), \sigma_0)$$

- By previous lemma, as  $X$  (and so  $\sim^d$ ) output consistent, then  $X$  is noninterference-secure with respect to policy  $r$

# Quiz

True or false:

A security policy may be considered a set of noninterference assertions