

Noninterference Model

Goguen and Meseguer

Noninterference Model

CS177 2011 1

Definition

One group of users using a certain set of commands is noninterfering with another group of users if what the first group does with those commands has no effect on what the second group of users can see

Noninterference Model

CS177 2011 2

State Machine

State machine M

- a set U of users
- a set S of states
- a set SC of state commands
- a set out of outputs

Function out: $S \times U \rightarrow \text{out}$

Function do: $S \times U \times SC \rightarrow S$

Constant S_0 , initial state

Noninterference Model

CS177 2011 3

Capability System

- a set U of users
- a set S of states
- a set SC of state commands
- a set out of outputs
- a set $CAPT$ of capability table values
- a set CC of capability commands
- Function out: $S \times CAPT \times U \rightarrow \text{out}$
- Function do: $S \times CAPT \times U \times SC \rightarrow S$
- Function cdo: $CAPT \times U \times CC \rightarrow CAPT$
- Constant S_0 , initial machine state
- Constant T_0 , initial capability table

Noninterference Model

CS177 2011 4

Notation

Ability - a subset of commands that define what a user can do, Ab

$CAPT: U \rightarrow Ab$

Alternatively, let

$C = SC \cup CC$

and consider

$csdo: S \times CAPT \times U \times C \rightarrow S \times CAPT$

Noninterference Model

CS177 2011 5

Notation

- Let W in $(U \times C)^*$

then

$[[W]] = csdo(T_0, S_0, W)$

$[[W]]u = out([[W]], U)$

Noninterference Model

CS177 2011 6

Let

G be a group of users $G \subseteq U$

A be an ability, $A \subseteq C$

$W \in (U \times C)^*$

Then denote

$PG(W)$ - subsequence of W obtained by eliminating tuples (U,C) with $U \in G$

$PA(W)$ -

$PG,A(W)$ -

Example

$G = \{u,v\}$ $A = \{c1,c2\}$

$PG,A((u',c1),(u,c3),(u,c2),(v',c1)) =$

$G :| G'$ G does not interfere with (or is noninterfering with) G'

iff

$\forall W \in (U \times C)^*$

$\forall g' \in G'$

$[[W]]_{g'} = [[PG(W)]]_{g'}$

$A :| G'$

iff

$\forall W \in (U \times C)^*$

$\forall g' \in G'$

$[[W]]_{g'} = [[PA(W)]]_{g'}$

$A,G :| G'$

iff

$\forall W \in (U \times C)^*$

$\forall g' \in G'$

$[[W]]_{g'} = [[PG,A(W)]]_{g'}$

Security Policy

A security policy is a set of noninterference assertions

Let:

seco be a security officer and
A be commands that change the capability
table

$A, -\{\text{seco}\} \vdash U$

To isolate a group of users G

Let $G' = -G$

then

$G \vdash G'$
 $G' \vdash G$

Multilevel Security

Let

$u[-\alpha, x] = \{u \in U \mid \text{level}(u) \leq x\}$
 $u[x, +\alpha] = \{u \in U \mid \text{level}(u) \geq x\}$

$\forall x > x'$

$u[x, +\alpha] \vdash u[-\alpha, x']$