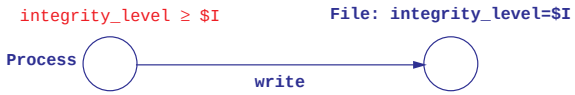
Biba Integrity Policy Constraint Graphs

Two constraints for Biba Integrity policy:

- ❏ only a process with higher or equal integrity level can write to a file



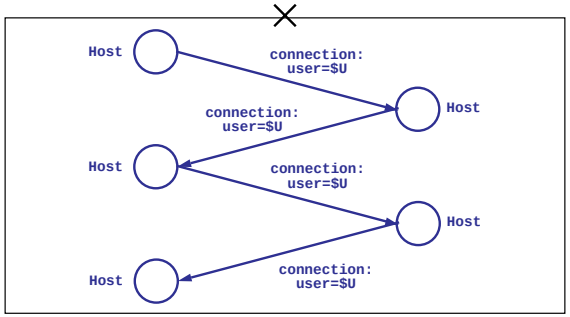
- ❏ only a process with lower or equal integrity level can read a file

Blue lines and predicates are part of the antecedent

Red lines and predicates are part of the consequent

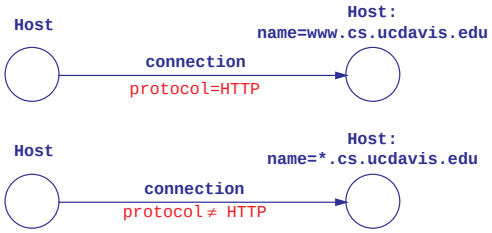
Negative Constraint Graph Example

If a user has a "chain" of logins 4 deep, then the policy is violated



Key: **antecedent is blue;** consequent is red

Contradicting Policy Example



Here the contradiction is because:

- ❏ the antecedent can apply at same time
- ❏ the consequents are opposing

The contradiction could be more subtle, i.e., if the second policy had consequent "transport_protocol=UDP", which implies "protocol ≠ HTTP", or only contradict part of the time

Specifying Polices Using Graphs

Graphs are well-studied visual formalisms with flexible semantics

- ❏ flexible semantics mean that a graph language designer has more options
- ❏ formality promotes reasoning and mechanical handling
- ❏ graphs are widely used and well-studied
  - known algorithms and properties can be used
- ❏ visual nature may facilitate the use of the language by humans
  - easier policy specification promotes broader specification of policy

Policy Specification in Miró

Miró is a visual policy language for expressing file system constraints

Miró project at Carnegie Mellon Univ. (Heydon, Tygar, Wing, *et al*)

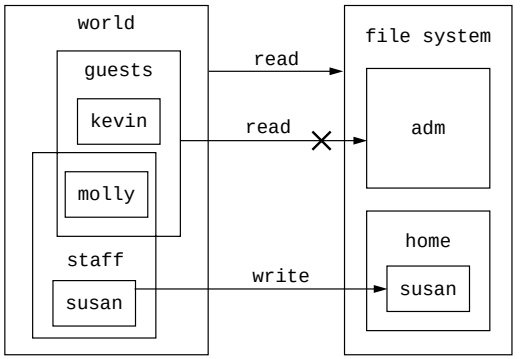
Miró has two languages

- ❏ instance language represents the state of the file system
- ❏ constraint language represent the file system constraints of a policy

Miró instance language is based on higraphs and state charts (David Harel)

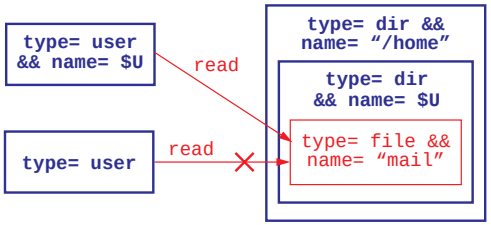
- ❏ boxes represent objects
- ❏ nesting of boxes are like Venn diagrams, indicating containment
- ❏ arrows represent access rights or lack thereof

Miró Instance Language Example



Miró Constraint Language Example

Constraint: Every user with a directory in "/home" should have a file named "mail" in that directory which is readable by that user and no others



Blue lines and text is the antecedent

Red lines and text is the consequent