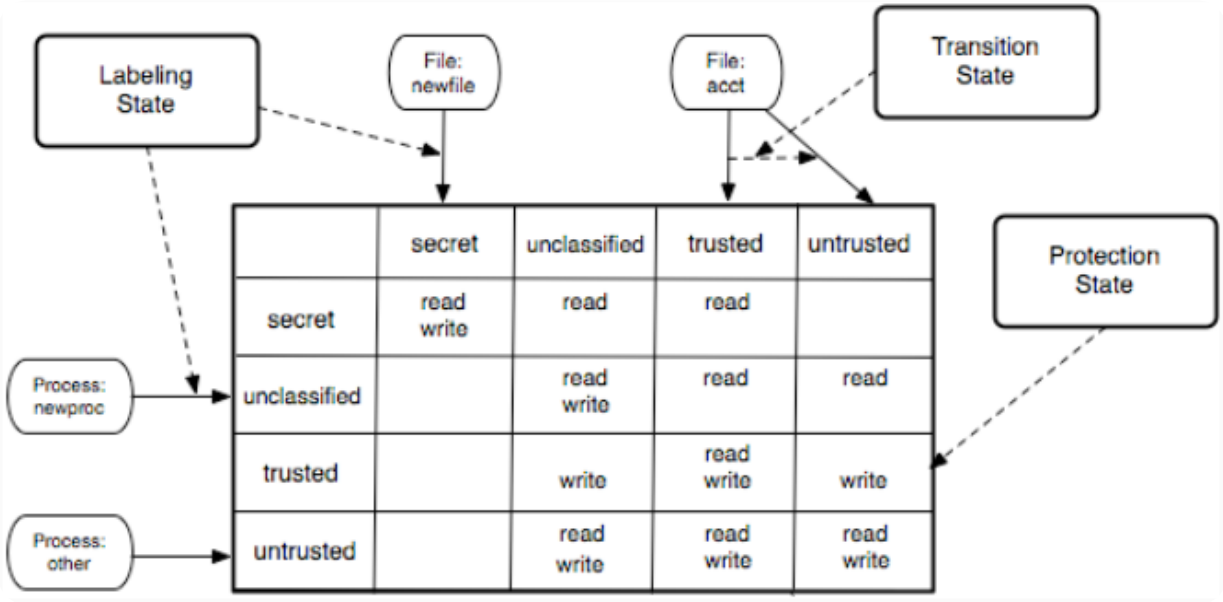
Mandatory Protection

#access_control/protection_system #access_control/protection_state

Mandatory Protection System

- mandatory protection system - protection system that can be modified only by trusted administration that consists of
  - **mandatory protection state** - protection state is defined in terms of a set of *labels* associated with subjects and objects
    - *label set* - defined by trusted administration
  - **labeling state** - assigns system subjects and objects to those labels in the mandatory protection state
  - **transition state** - determines the legal ways that subjects and objects may be relabeled
  - it is **immutable**
  - 

Mandatory Protection State

- can be represented as an *immutable table* of subject labels, object labels, and operations authorized for former upon latter
- example - mandatory protection system for an os
  - allow media player to communicate with browser and execute certain files
  - no network access
  - mandatory protection state for the media player

- plays only trusted input

Labeling State

- immutable rules mapping
  - *rows* - subjects to labels
  - *columns* - objects to labels
- example - labeling state for os
  - browser and media player have their own subject labels
  - label inputs from the network through the network connection
  - root and TCB program files have labels based on their trust
- example - labeling state for web application
  - content is untrusted
  - prevent integrity violation

Transition State

- immutable rules mapping
  - processes to conditions that change their *subject labels*
  - interprocess communication (?) to conditions that change their *object labels*
- example - transition state for os
  - change label of processes that receive untrusted input
  - change label of outputs of these processes
- example - transition state for programs
  - server, browser, and media player change labels of their internal objects (e.g. threads, variables)
  - sever, browser, and media players may be trusted to change their labels