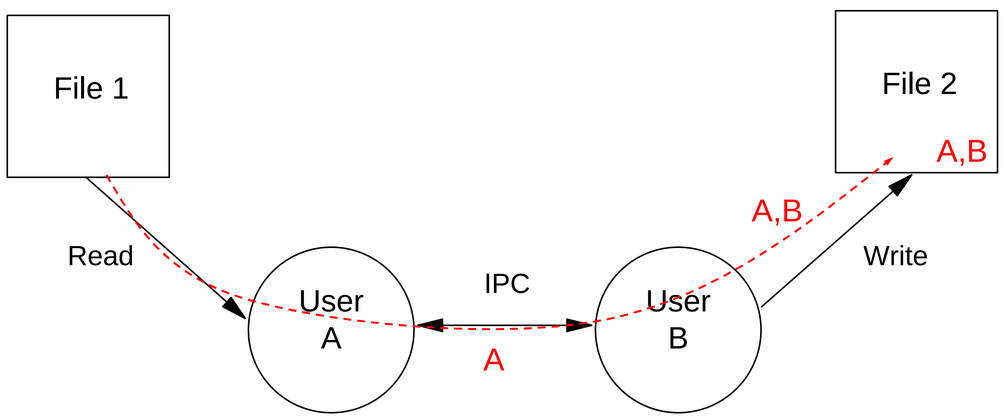
CERIAS

# Using Process Labels to obtain Forensic and Traceback Information

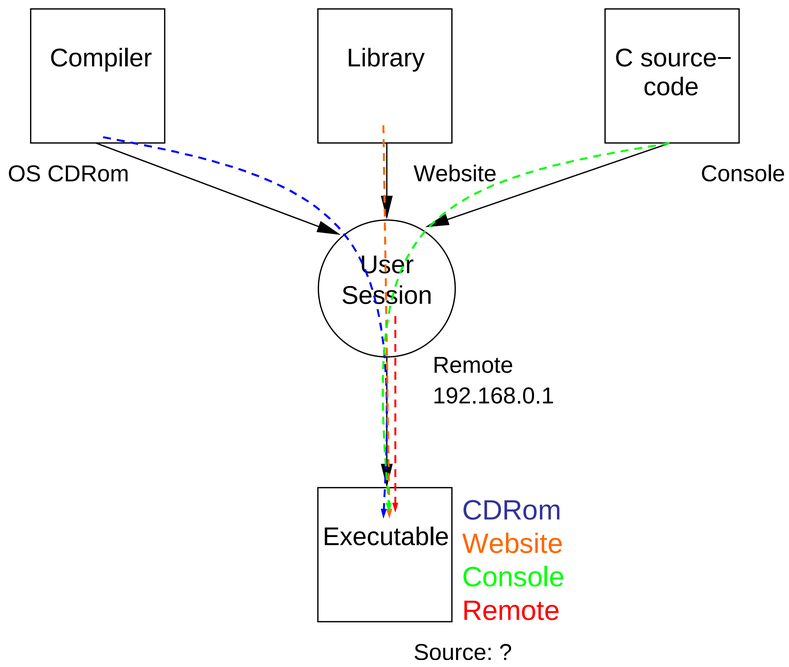
Florian Buchholz, P.I.: Prof. Eugene Spafford

Use labels to track information flow among principals.

## User information




## Location information




## Operations of the Model

- Addlabel(p, l)
- Create(p1,p2), Create(p, o)
- Open(p, o), open(o,p), open(p1, p2)
  - Read(o,p), read(p1,p2)
  - Write(p,o), write(p1,p2)
  - Close(p,o), close(o,p), close(p1.p2)
  - Destroy(p), destroy(o)

Update label sets of principals and objects as information is being exchanged.

## Properties of the Model

- If a label is bound at a principal p1 and there exists a potential information exchange path from p1 to principal p2, the label will be part of p2's set
- If a label is part of p2's label set and p2 is not in a principal that can generate labels, then information must have been exchanged between p2 and a principal that could have generated the label.