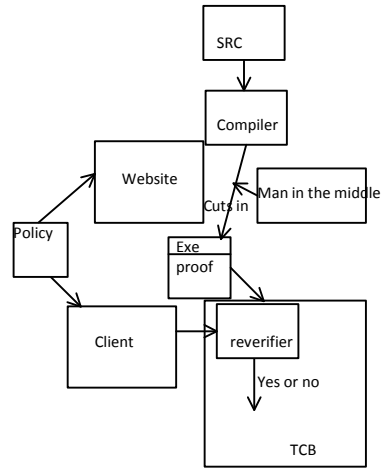
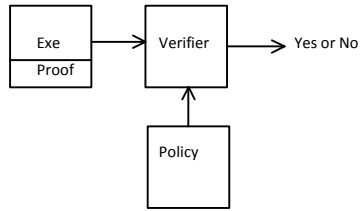
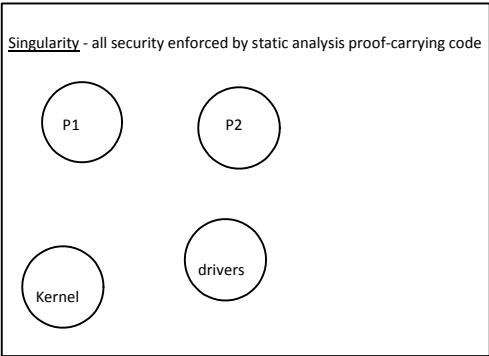
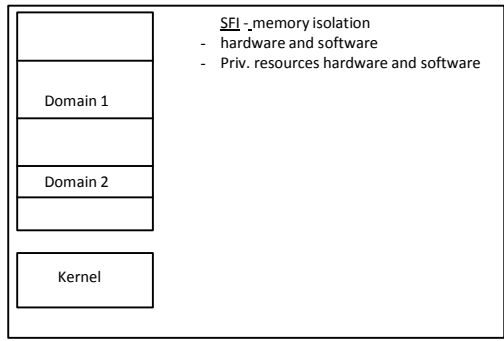
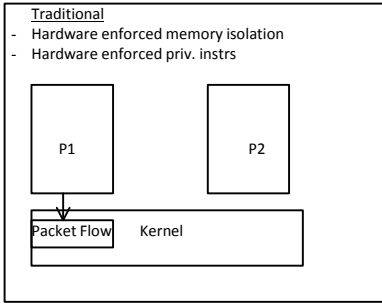


Future of OS Process Isolation?

Friday, April 03, 2009
12:51 PM



Proof Carrying Code

Verification Condition Generation

- o Pre condition is met
- o then we execute the program
- o then we want to verify that some post conditions is valid after the run

Defination - the weakest precondition of a statement S w.r.t. a predicate P is weakest statement P s.t. P, s, P

$$Wp(x=e, P) = P[e/x]$$

$$Wp(\text{if}(b)S_1 \text{ else } S_2, P) = b \rightarrow wp(S_1, P) \wedge \neg b \rightarrow wp(S_2, P)$$

$$Wp(S_1, S_2, P) = wp(wp(S_2, P), S_1)$$

