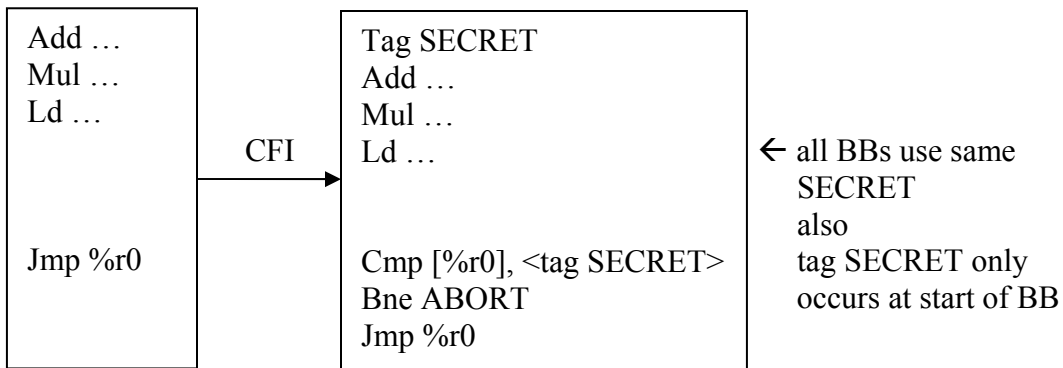


## CSE 509 Class Note 3/27

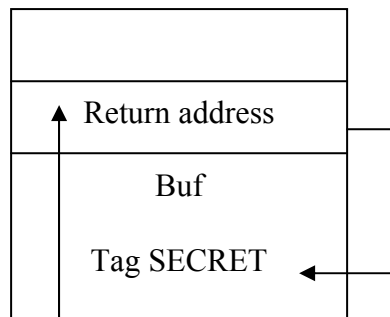
### Control Flow Integrity (CFI)

- Complete mediation for IRMs
- Key Idea : Ensure program always jumps to beginning of basic block.
- Basic block
  - o Sequence of instruction containing no branches except last instruction
    - Put checks in same Basic block as action being checked
- Ensuring the basic block property

### B.B.



- Why secret Tag parameters?
  - o Buffer overflow/code injection Stack

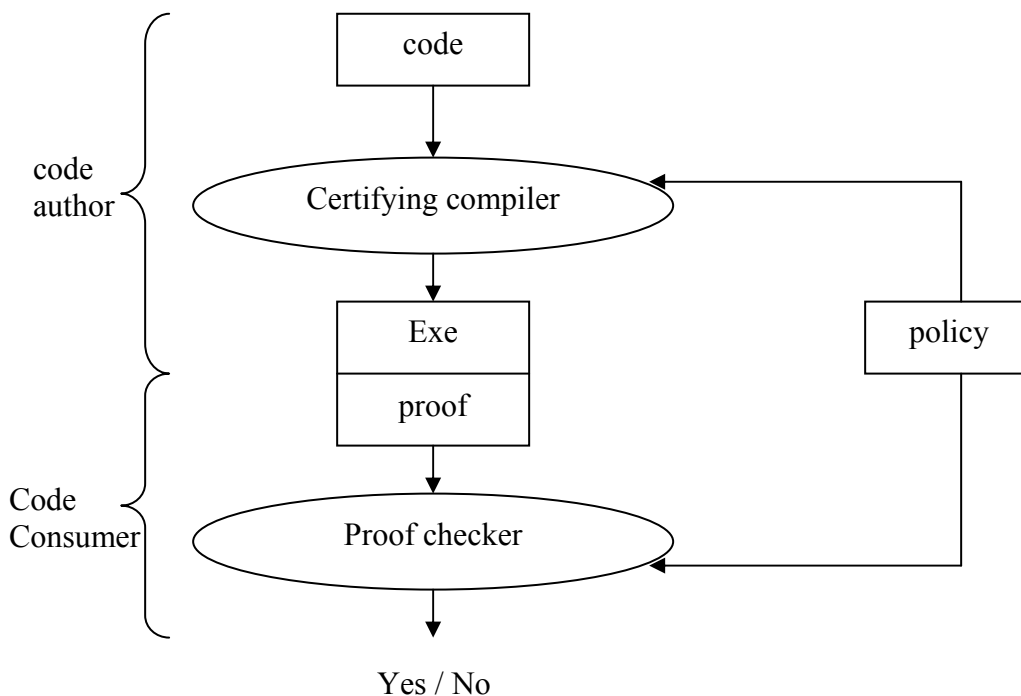


What if writable pages are non-executable?

→ Then tag parameters does not need to be secret

## Proof Carrying Code

- untrusted plugins to trusted system
- Goal : untrusted plugin obeys interface to trusted code
- Offline Reference Monitor
  - o Only need to check once
  - o Performance
- example policy
  - o untrusted function returns linked list of ints
  - o untrusted function doesn't modify memory
  - o untrusted function terminates in x stpes
  - o untrusted function preserves types of memory locations



## Proving things about code

Hoare Triple :  $\langle P ; S ; Q \rangle$

P : predicate, S: statement, Q : predicate

Means "If P is true before S executes, then Q will be true afterwards."

i.e.)  $\langle x=5 ; x=x+2 ; x=7 \rangle$

- Weakest precondition  
 $Wp(S,Q) = P$   
such that  $\langle P;S;Q \rangle$  and all  $P'$   
such that  $\langle P';S;Q \rangle \rightarrow P$

i.e.)  $wp(x=x+2 ; x=7) \equiv x=5$   
 $wp(x=x^2 ; x=9) \equiv (x=3 \text{ or } x=-3)$

$wp(x=e, Q) \equiv \lceil e/x \rceil * Q$   
 i.e.)  $wp(x=x+2, x=7) \equiv \lceil (x+2)/x \rceil (x=7)$   
 $\equiv x+2=7$   
 $\equiv x=5$   
 $wp(x=x^2, x=9) \equiv x^2=9$

$wp(S1;S2,Q) = wp(S1, wp(S2,Q))$

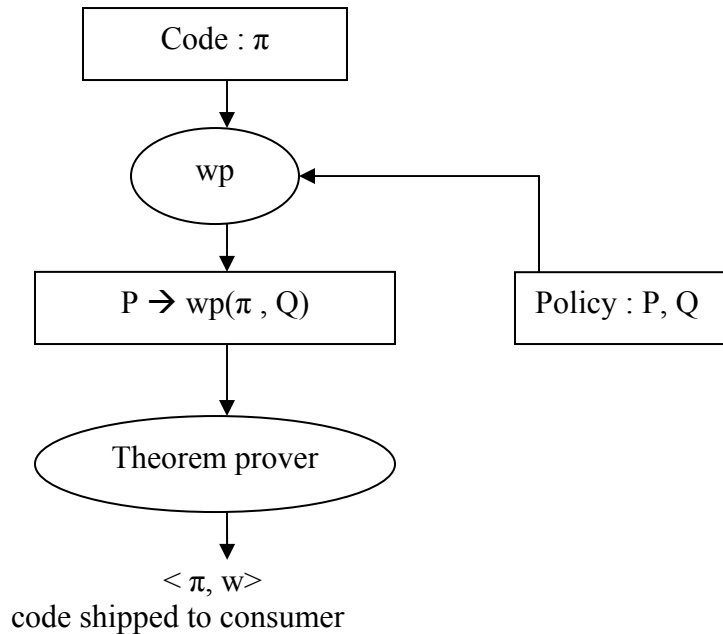
untrusted code :  $\pi$

trusted system always call  $\pi$  with precondition P and wants  $\pi$  to establish postcondition Q

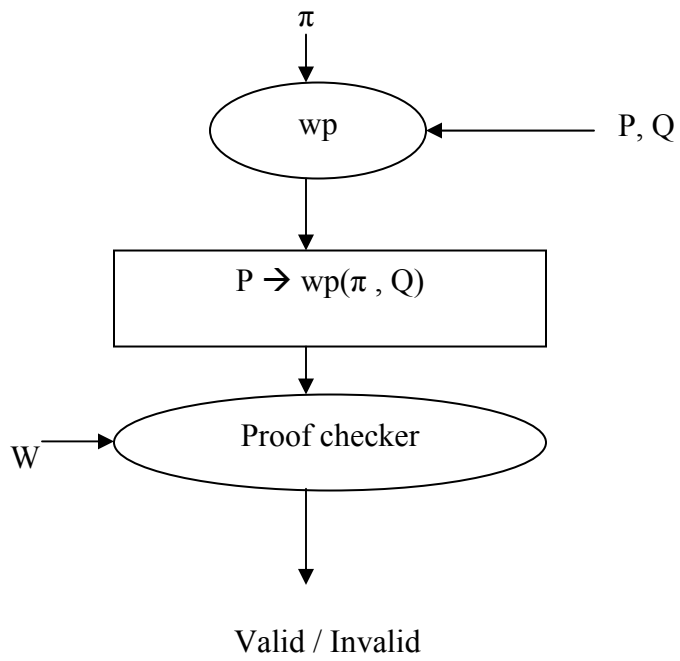
$P \rightarrow wp(\pi, Q)$

If this is true, code is OK.

- producer



- consumer



Tail (l :  $\tau$  list)  
Return l  $\rightarrow$  next ;

P = l :  $\tau$  list  
Q = ret :  $\tau$  list