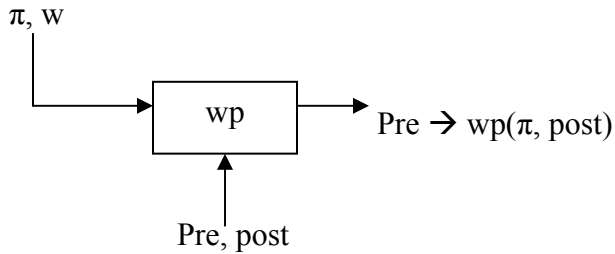


CSE 509 Class note 3/29

Proof carrying code

Pre \rightarrow wp(π , post)



Pre

S0
 Assert(P1)
 S1
 Assert(P2)
 S2
 Assert(P3)
 S3
 Post

Suppose

Pre \rightarrow wp(S0, P1) \wedge
 P1 \rightarrow wp(S1, P2) \wedge
 P2 \rightarrow wp(S2, P3) \wedge
 P3 \rightarrow wp(S3, post)

 Pre \rightarrow wp(S0;S1;S2;S3, post)

While(e) {
 Assert(p);
 S;
 }
 assert(post)

[P \wedge wp(s,e) \rightarrow P] \wedge
 [\neg e \rightarrow post] \wedge
 [e \rightarrow P] \wedge
 [P \wedge wp(s, \neg e) \rightarrow post]

L1 : \longleftarrow P \rightarrow P0
 assert(p)
 \longleftarrow P0 ...
 S1
 \longleftarrow P1 ...
 S2

 \longleftarrow P(n-1) ...
 Sn
 \longleftarrow Pn : x \neq \rightarrow post
 \wedge x=0 \rightarrow P
 bez x,L1
 \rightarrow post

	RPC	SFI	PCC
Domain crossing	2	X	X
Argument marshalling	2	1	X
Overhead			Proof overhead
Advantage			Cross domain calls = function calls

Costs of PCC

- programmer effort
- Theorem proving / checking
- Writing interface specs
- Runtime checks
- Exec size ?