Proof carrying code:

In native client:-

Programmer->Code->Compiler->Binary->Verifier->User

(Un-trusted) (Trusted)

- Verifier checks two properties:-
  - Read and write are safe
  - Jumps are same
- Compiler inserted checks to make verification easy

In proof carrying code

Programmer->Code->Compiler->Binary,proof->Verifier->user

Correction
Condition

- Verifier uses proof and binary to check if correction condition is valid
- Use correction condition (may be defined using induction)
- Code is already memory safe
- Compiler do not enter any checking code
- Proof is addition to binary
- Verification is simpler to code
- Verification is faster to perform
- No or little run-time checking
- Proof may be derived from source code

How to generate proofs? What does proof contains?

```java
int foo(int a)
{
    int b=a;
    if(b<0)
        b = -b
    return b;
}
```
Post condition: foo(x) >= 0  
Pre condition: none

How the program does it automatically?

Weakest precondition WP (s,p): It is the weakest predicate Q such that if Q is true before executing C, then P will be true afterwards.  
s-> is a program statement  
p-> post condition after executing the statement.

Example:
WP(x:=x+1, x==7)
   = x == 6  i.e. The precondition should be x==6 such that after executing x=x+1 the o/p is x=7

WP(x:=x+1, y==5)
   = y == 5

How do we set predicate (p)?
WP(x:=e,P)
   P[e/x]

WP(x:=x+1; x:=2x, x==8)
Put x=2,  
2x ==8 for predicate; then put x+1 in x  
2(x+1) = 8

So we conclude that WP(S1,S2,P) = WP(S1, WP(S2,P))
WP(if(e) then S1 else S2, P)
If(e is true => WP(S,P)) AND if(!e => WP(S2,P))

int foo(int a) {
   int b =a  
   if(b<=0)  
      b = -b; 
   return b; }

WP(b=a; if(b<0) hen b = -b else return b, b<0) =WP(b=a, b<0 => -b>=0) AND b>=0 => b>=0) = WP(a<0 => -a>=0)AND(a>=0 => a>=0)
Untrusted binary code (S) and there are same pre and post correction condition

\[
\begin{align*}
\{\text{PRE}\} &\quad \{\text{S}\} \quad \{\text{POST}\} \\
\downarrow &\\
\text{Verification condition generation} &\\
\downarrow &\\
\text{Pre }\Rightarrow WP(S,post) &\quad /\text{needs to be proven} \\
\downarrow &\\
\text{Theorem prover} &\quad (\text{On success}) \\
\downarrow &\\
\text{Proof} &\\
\text{At user end:-} \\
\bullet \quad \text{User takes the code and is aware of the verification codes.} \\
\{\text{Pre}\} &\quad \{\text{S}\} \quad \{\text{Post}\} \\
\downarrow &\\
\text{VC generator} &\\
\downarrow &\\
\text{VC} &\quad \text{Proof} \\
\downarrow &\\
\text{Verifier} &\\
\downarrow &\\
\text{Valid/Invalid}
\end{align*}
\]