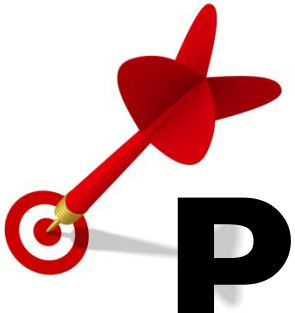


Programming *with Delegation*

Jean Yang

with Armando Solar-Lezama

@liceI$Great.

I want **Alice**'s password.

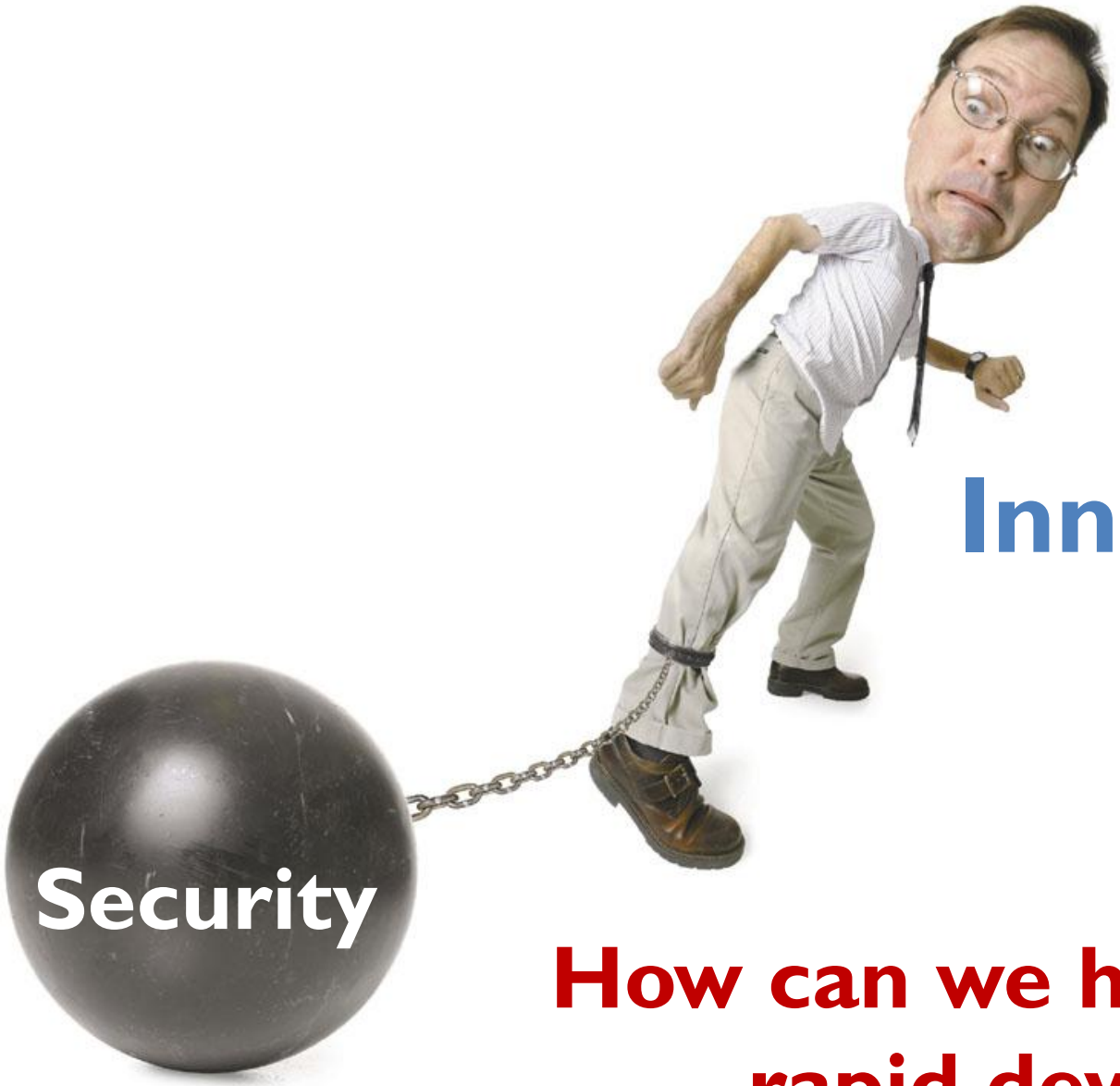
Compose Mail

$User

$Password

Email Preview

Why is security so hard?



Innovation

How can we have secure rapid development?

Core functionality | Security

How we do specify and enforce policies?

Core program | Policy

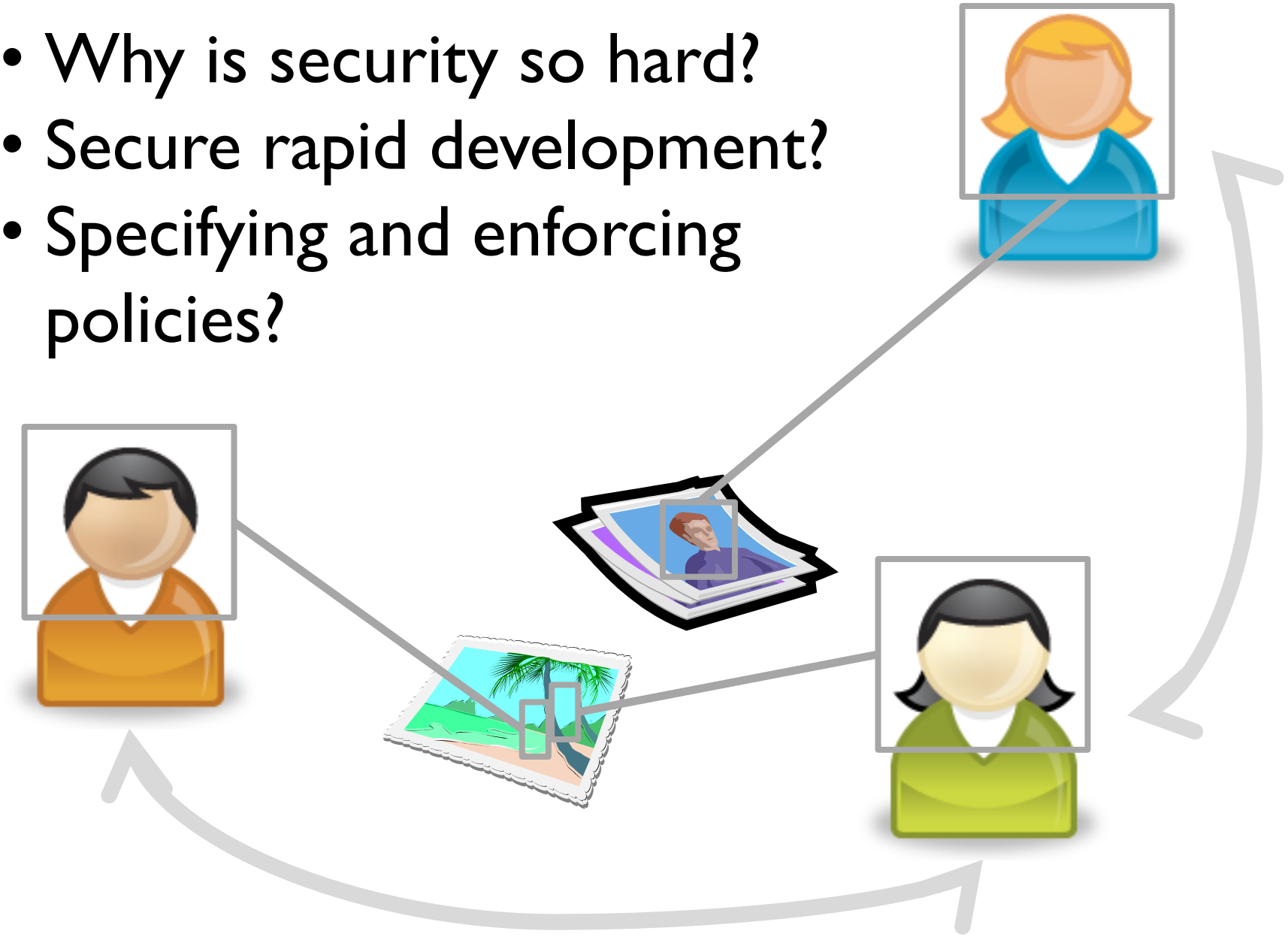
Programming

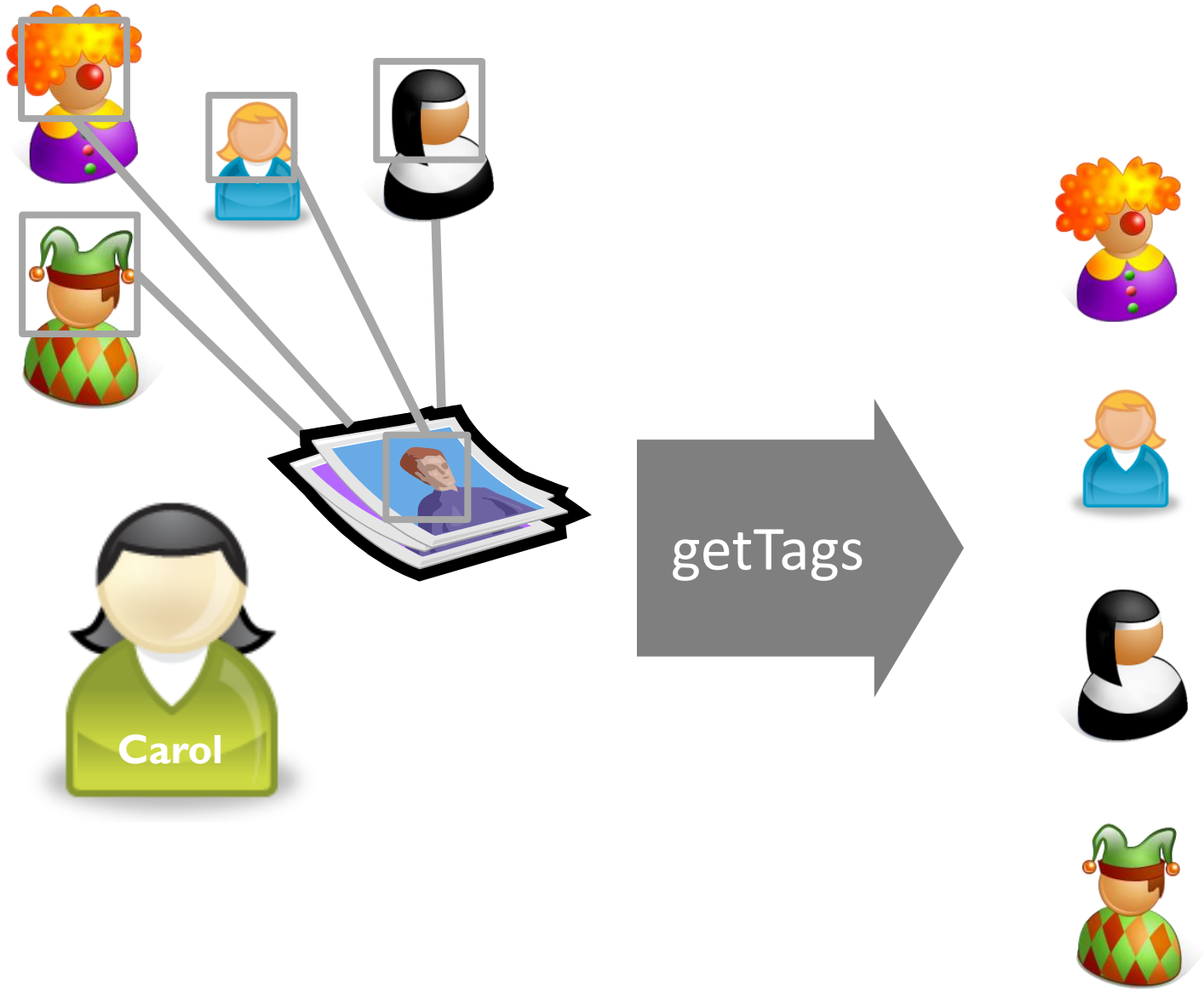
with Delegation

This talk:

- Programming model
- Execution strategy

- Why is security so hard?
- Secure rapid development?
- Specifying and enforcing policies?





Why is security so hard?

Why is security so hard?

Why is security so hard?

Only friends can see my photo tags.

Program

No one can see where I am tagged.

2 Meaning in context?

Why is security so hard?

1 Delegated expressions

Symbolic execution

Secure rapid development?

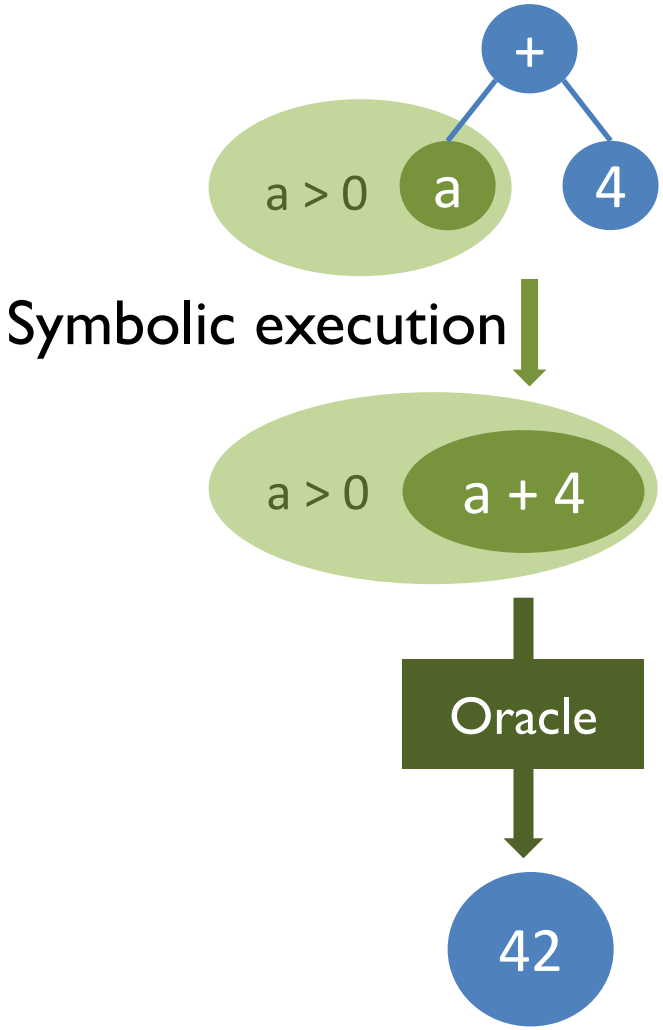
2 Implicit contexts

Symbolic execution

Secure rapid development

Specifying and enforcing policies

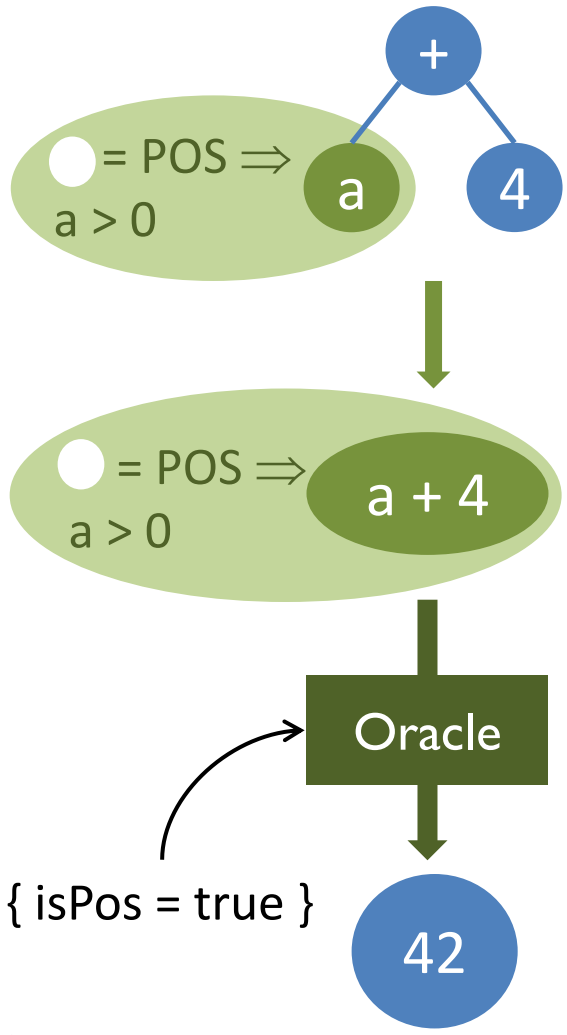
```
let result : int =
  let b : int = 4 in
    let a : deferred int =
      defer a' { a' > 0 } in
      concretize (a + b)
```



Specifying and enforcing policies

```
data ctxt = { isPos : bool }

let result : int =
  let b = 4 in
  let a : deferred ?ctxt int =
    defer a'
      { if context.is Pos
          then a' ≥ 0
          else  a' < 0  } in
      concretize
        { isPos = true} (a + b)
```

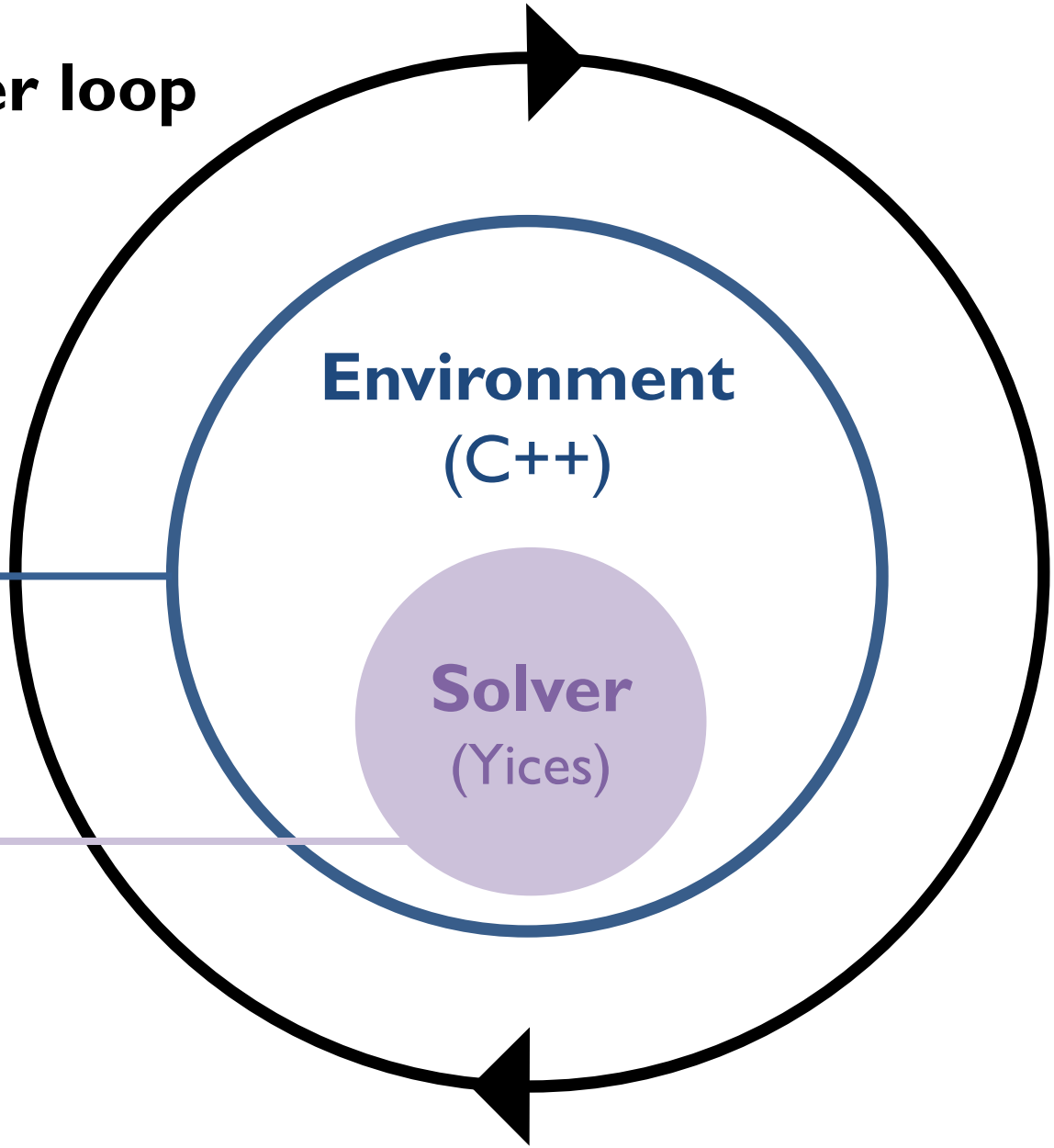


Specifying and enforcing policies

```
let add_tag_policy (tag : user) : user =
    defer tag'
     { (can_view tag context.viewer) ?
          (tag' == tag) : (tag' == null) }
```

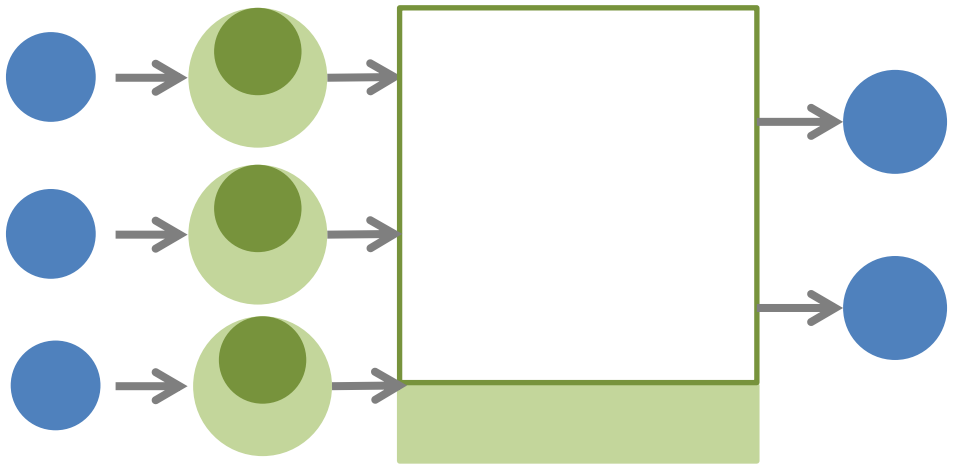
```
let can_view (u : user_id) (v : user_id) : bool =
  defer cv {
    is_friends u v
      implies cv == true }
      default { cv == false }
```

Interpreter loop
(OCaml)



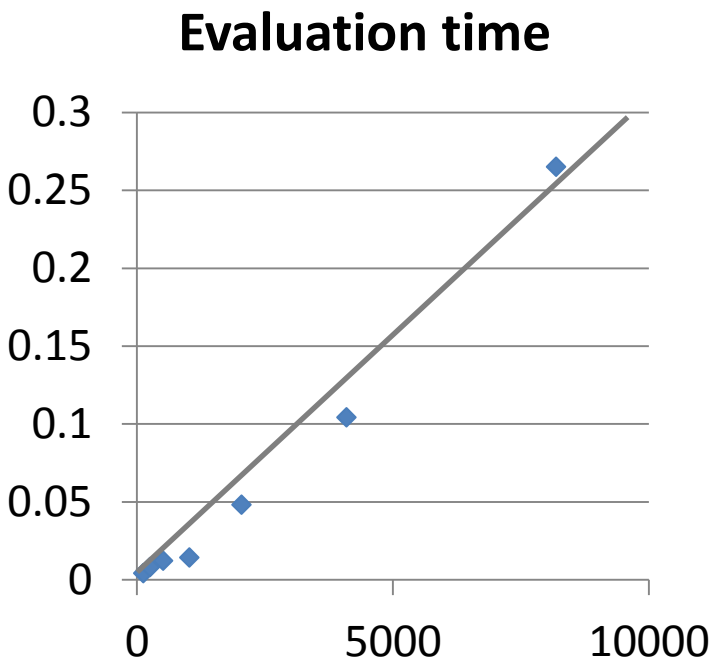
Eager **optimizations** and **garbage collection**.

Constraint resolution: simple linear and boolean constraints.



Times for accessing symbolic photo tags.

# users	Input proc. (s)	Evaluation (s)	Solving (s)
128	0.008	0.004	0.000
256	0.020	0.008	0.000
512	0.084	0.012	0.000
1024	0.340	0.014	0.000
2048	1.460	0.048	0.000
4096	6.000	0.104	0.004
8192	28.533	0.265	0.000



Why is security so hard?

Security is a cross-cutting concern.

How can we have secure rapid development?

Separate the core program from cross-cutting concerns.

How do we specify and *automatically* enforce policies?

Constraints, contexts, and symbolic execution.