Interprocedural Dataflow

context-insensitive

main:

1: x = 0

2: y = id(x)

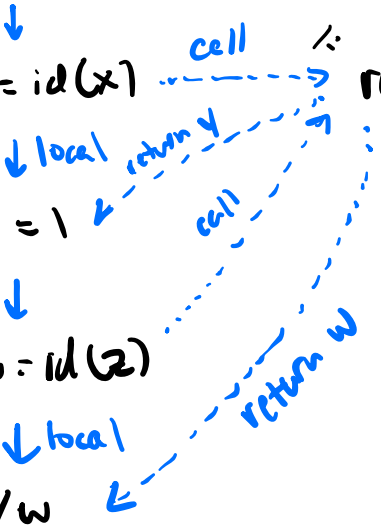
3: z = 1

4: w = id(z)

5: V w

id(a):

return a



$\{x \mapsto Z, z \mapsto NZ, y, w \mapsto T, \}$

$\sigma^{in}_{main-4} = \{x, y \mapsto Z, z \mapsto NZ\}$

$\sigma^{out-call}_{main-4} = \{a \mapsto NZ\}$

$\sigma^{in}_{main-2} = \{x \mapsto Z\}$

$\sigma^{out-call}_{main-2} = \{a \mapsto Z\}$

$\sigma^{out-local}_{main-2} = \{x \mapsto Z$

$\sigma^{out-ret-y}_{id-1} = \{y \mapsto Z\}$

$\sigma^{in}_{id-1} = \sigma^{out-call}_{main-2} \sqcup \sigma^{out-call}_{main-4}$

$= \{a \mapsto T\}$

$\sigma^{in}_{main-3} = \sigma^{out-local}_{main-2} \sqcup \sigma^{out-ret-y}_{id-1} = \{x \mapsto Z, y \mapsto Z\}$

$f(x = f(y^*), \sigma)_{local} =$

$\sigma \setminus \{x\}$

$f(x = f(y^*), \sigma)_{call} =$

$\{f.params[i] \mapsto \sigma[y_i]$

$f(return\ x, \sigma)_{return\ y} =$

$\{y \mapsto \sigma[x]\}$

Context-sensitive interprocedural analysis

$f(x = f(y^*), \sigma) =$

$\sigma^{start} = \{f.params[i] \mapsto \sigma[y_i]\}$

result = DATAFLOW(f, σ^{start})

state = $\bigsqcup_{i \in returns(f)}$ result[i][ret]

$\sigma[x \mapsto state]$

$f(return\ x, \sigma) =$

$\sigma[ret \mapsto \sigma[x]]$

DATAFLOW

: Function * Domain

→ [Domain]

```
x = 0
y = id(x)
z = 1
w = id(z)
1/0
```

$\sigma^{start} = \{a \mapsto z\}$

result = $[\{a \mapsto 7, ret \mapsto z\}]$

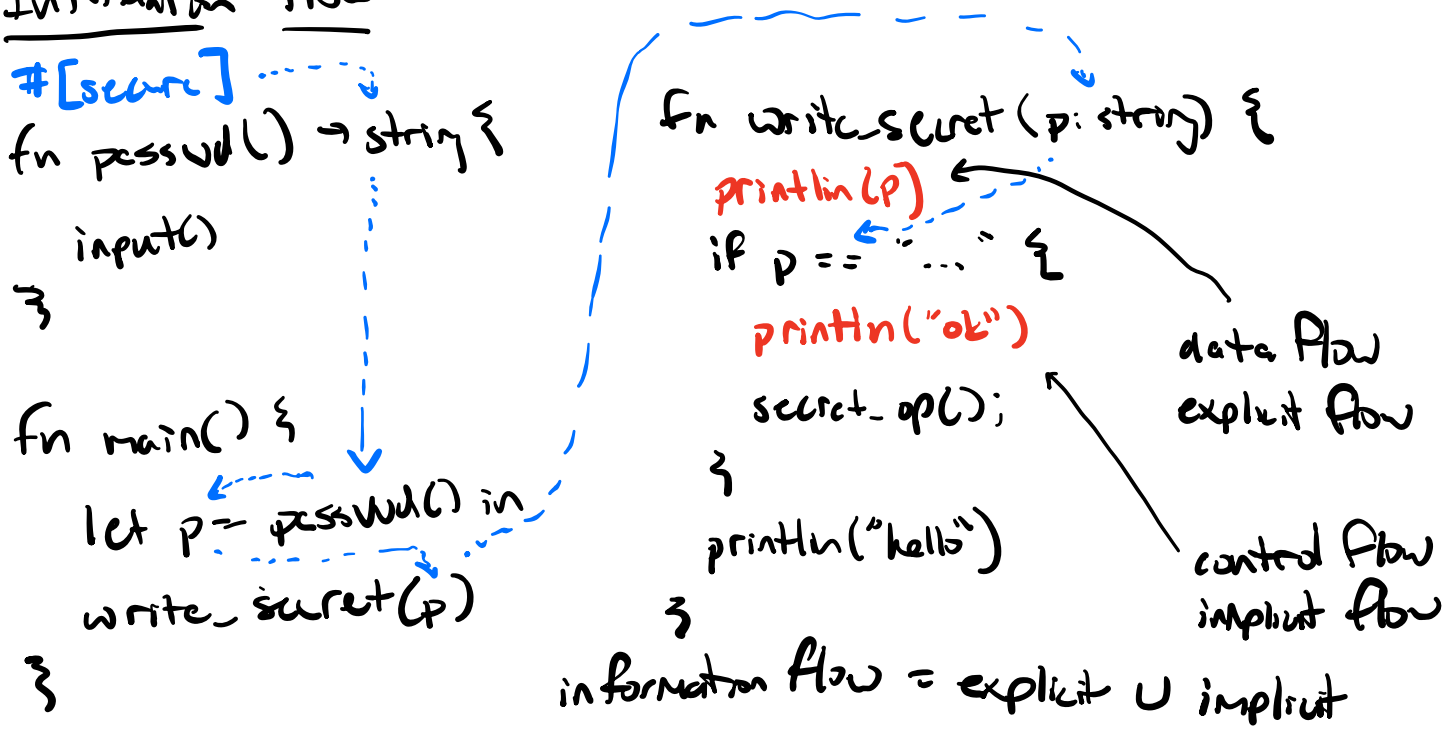
state = z

$\sigma[y \mapsto z]$

```
f(x : int)
  if ...
  ↙          ↘
return x    return 0
```

f(2)

Information flow



information flow = explicit ∪ implicit

Data flows

$\alpha = \{ \text{insecure}, \text{secure} \}$

$\text{insecure} \sqsubset \text{secure}$

$\sigma \in \{ \text{Var} \mapsto \alpha \}$

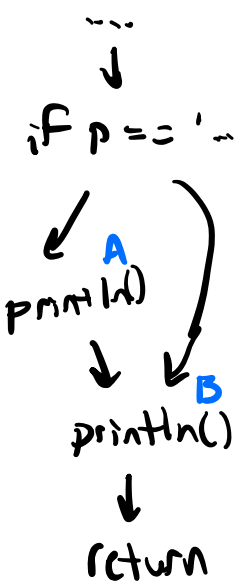
$f(x = c, \sigma) = \sigma[x \mapsto \text{insecure}]$

$f(x = f(y^{\alpha}), \sigma)$ if f marked secure

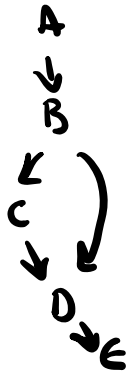
$= \sigma[x \mapsto \text{secure}]$

$f(x = y \oplus z, \sigma) = \sigma[x \mapsto \sigma[y] \sqcup \sigma[z]]$

$f(x = y, \sigma) = \sigma[x \mapsto \sigma[y]]$



Dominance



A dominates B if all paths from start to B go through A

Post-dominance:

A pdom B if all paths from exit

to B go through A

α is control-dependent on β if:

A) β does not pdom α

B) there exists a path from

to s.t. all C on the path

are pdom by (except ,)