Input sanitization

Component 1 → Component 2

validation

Taint tracking
for dealing with untrusted data

input
data
(for untrusted)

X

$Y_1 = f(X_1)$ ← taint

Y_2

$\vdots$

Y_N
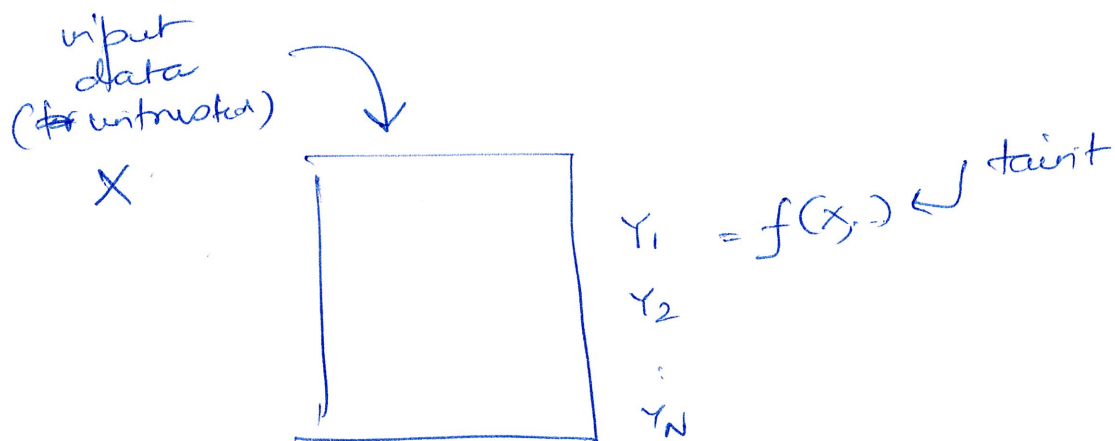
Data-based
taint tracking

System critical operation
on Y_i

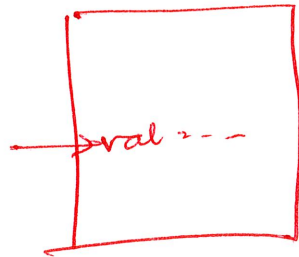Control-based
taint tracking

if $(Y_j == T)$

TB

else

FB

INSERT INTO Students (firstname) VALUES ('Elaine'

Robert'); DROP TABLE Students; --

Non re-entrant functions

foo(   )
{

    val = ---;

Interrupt
~~Exception~~ ⟶

    val2 = val + ... ;

}

Interrupt
~~Exception~~ handler
{

    val = -- ;

}

foo1 ( )
{

atomic

Shared
variable → val = ---

}

foo2( )
{

val = --

}

dst Acct. SetBal (dst Acct. getBal() + xfrAmt)

↓

dst Acct.
getBal()

20	
5	
5	
20	
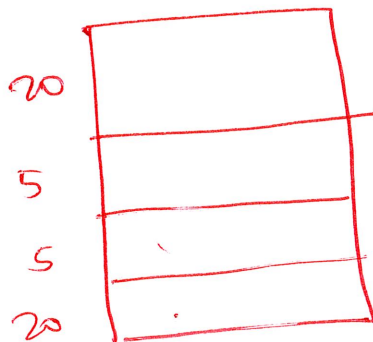
50 Assembly
instructions

CERT. SEI