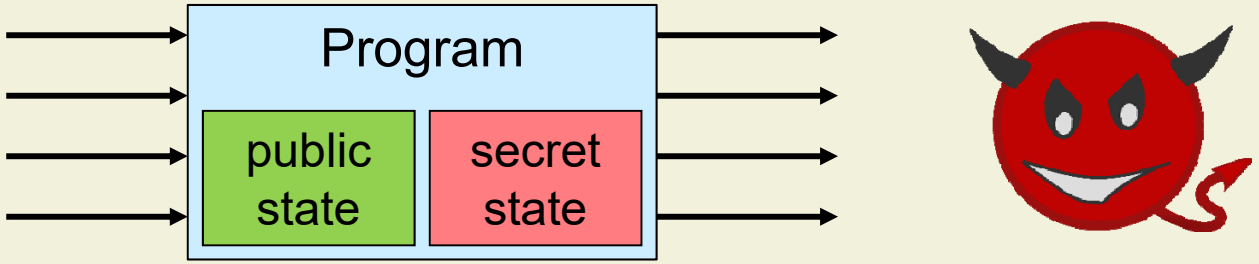
Modular Verification of Secure Information Flow

Peter Müller
ETH Zurich

Joint work with
Marco Eilers and Sam Hitz

Secure Information Flow

- Programs maintain secret state such as crypto keys



- High-level goal:
  Verify that attackers are not able to learn secrets by interacting with the implementation

Traditional Non-Interference

- Classify all variables as either high (secret) or low (public)
- Assume attacker can observe values of low variables
- A statement s is information-flow secure if:

$$\forall \sigma_1, \sigma_2 \bullet \sigma_1 \equiv_{low} \sigma_2 \wedge \langle s, \sigma_1 \rangle \rightarrow \sigma'_1 \wedge \langle s, \sigma_2 \rangle \rightarrow \sigma'_2 \Rightarrow \sigma'_1 \equiv_{low} \sigma'_2$$

Existing Work: Types and Static Analysis

- Strengths
  - Automation
  - Type systems are modular
- Weaknesses
  - Expressiveness
  - Precision

```
if( h )    { l := 7 }
else       { l := 3 + 4 }
```

```
if( h )    { foo( 7 ) }
else       { foo( 7 / x ) }
```

```
if( h )    { skip }
else       {
  while( true ) { skip }
}
```

Existing Work: Relational Hoare Logics

- Manipulate triples of the form

$$\{ P \}\ s \sim s' \{ Q \}$$

- Strengths
  - Very expressive
- Weaknesses
  - Poor automation
  - Requires dedicated tool support

Existing Work: Self-Composition

- Reduce non-interference to a safety property

```
while( l < 10 )
  invariant low( l )
{ l := l + 1 }
```

- Strengths
  - Supports off-the-shelf verifiers

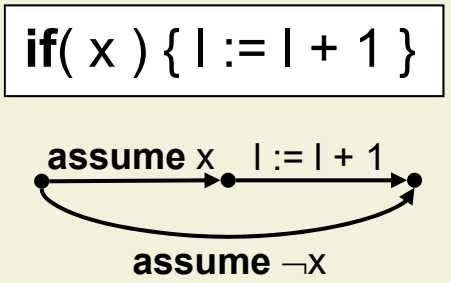
```
assume l == l'
while( l < 10 ) { l := l + 1 }
while( l' < 10 ) { l' := l' + 1 }
assert l == l'
```

- Weaknesses
  - Relational specifications
  - Separation of concerns
  - Non-modular

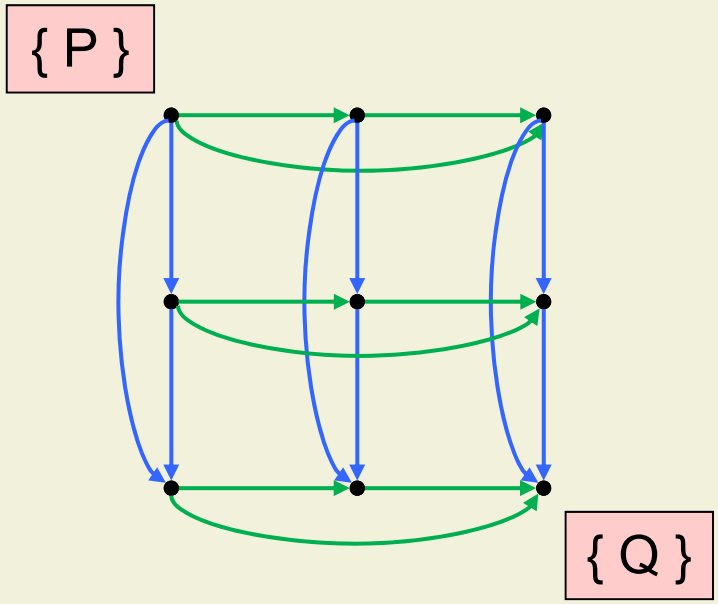
```
while( l < 10 ) {
  print( l )
  l := l + 1
}
```

Existing Work: Product Programs

- Execute two versions of the program interleaved rather than in sequence



- Strengths
  - Supports off-the-shelf verifiers
- Weaknesses
  - Relational specifications
  - Separation of concerns
  - Non-modular

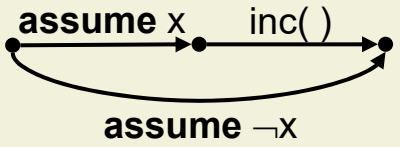


Relational Specifications

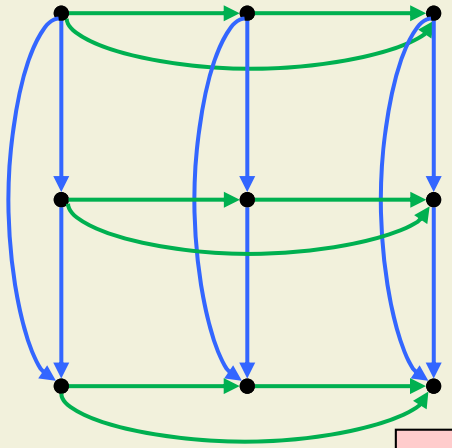
- Method specifications

```
inc( )
  requires low( g )
  ensures low( g )
{ g := g + 1 }
```

if(x) { inc( ) }



{ x = x' ∧ g = g' }



{ g = g' }

Our Product Programs

- Introduce boolean ghost variables p, p' to track which execution is active
- Make all operations conditional on p,p'
- p,p' are initially true

```
inc( )
{ g := g + 1 }
```

```
inc( p, p' ) {
  if( p ) { g := g + 1 }
  if( p' ) { g' := g' + 1 }
}
```

Our Product Programs: Definition

[[s]] (p, p’)

if(p) { s }
if(p’) { s’ }

[[**if**(b) { s_0 } **else** { s_1 }]] (p, p’)

p_0 := p ∧ b
p_0’ := p’ ∧ b’
p_1 := p ∧ ¬b
p_1’ := p’ ∧ ¬b’
[[s_0]] (p_0, p_0’)
[[s_1]] (p_1, p_1’)

[[**while**(b) **invariant** J { s }]] (p, p’)

while(p ∧ b ∨ p’ ∧ b’)
  invariant (p ⇒ J) ∧ (p’ ⇒ J’)
{
  p_0 := p ∧ b
  p_0’ := p’ ∧ b’
  [[s]] (p_0, p_0’)
}

Interpreting Relational Specifications

- Relational specifications apply only if both program executions proceed synchronously

```
if( x ) { inc( ) }
```

```
p0 := p ∧ x
p0' := p' ∧ x'
inc( p0, p0' )
```

```
inc( )
  requires low( g )
  ensures low( g )
{ g := g + 1 }
```

```
inc( p, p' )
  requires p∧p' ⇒ g=g'
  ensures p∧p' ⇒ g=g'
{
  if( p ) { g := g + 1 }
  if( p' ) { g' := g' + 1 }
}
```

Observable Output

```
print( x )
  requires low( x )
  requires lowEvent
```

```
while( y < 10 )
  invariant lowEvent
  invariant low( y )
{ print( 5 ); y := y + 1 }
```

```
print( p, p', x, x' )
  requires p∧p' ⇒ x=x'
  requires p=p'
```

```
while( p ∧ y<10 ∨ p' ∧ y'<10 )
  invariant p=p'
  invariant p∧p' ⇒ y=y'
{
  p0 := p ∧ y < 10
  p0' := p' ∧ y' < 10
  print( p0, p0', 5, 5 ); …
}
```

Declassification

- Many programs intentionally leak some secret information

```
bool equals( a, b )
  ensures   low( a ) ∧ low( b ) ⇒
            low( result )
```

```
byte[ ] encypt( a, b )
  ensures   low( contents( result ) )
```

```
b := equals( passwd, input )
declassify( b )
if( b ) { … }
else  { print( error ) }
```

```
assume p∧p' ⇒ b=b'
```

Summary of Basic Technique

- Construct a new form of product program
- Support relational specifications
  - Modular verification
  - Separation of concerns
- Based on powerful program logic
  - Heap data structures, race-free concurrency
- Attacker can observe
  - Low output channels
  - Program crashes

Termination

- Attackers can observe termination

```
while( y ≠ 0 )
{ y := y - 1 }
```

- Specify for each loop a precise termination condition

```
while( y ≠ 0 )
  terminates 0 ≤ y
{ y := y - 1 }
```

- Verify for each loop that the two executions either both terminate or both run forever

Termination: Encoding

```
while( y ≠ 0 )
  terminates 0 ≤ y
  decreases rank
{ y := y – 1 }
```

```
if( p )   { t := ( 0 ≤ y ) }
if( p' )  { t' := ( 0 ≤ y' ) }
assert p ∧ ¬t  ⇔  p' ∧ ¬t'
while( p∧y ≠ 0  ∨  p'∧y' ≠ 0 )
{
  p0 := p ∧ y ≠ 0
  p0' := p' ∧ y' ≠ 0
  if( p0 ) { y := y – 1 }
  if( p0' ) { y' := y' – 1 }
  assert p0 ∧ t ⇒ rank decreased
  assert p0' ∧ t' ⇒ rank' decreased
}
assert (p ⇒ t) ∧ (p' ⇒ t')
```

Timing Channels

- Attackers can observe timing of certain events

```
if( h ) { … }
print( )
```

- Instrument program with ghost counters s,s' to track execution time in a suitable cost model

- Assertion

```
print( )
  requires lowEvent
  requires lowTime
```

requires $p \wedge p' \Rightarrow s = s'$

requires $p \wedge p' \Rightarrow |s - s'| \leq c$

Probabilistic Non-Interference

- Attackers can observe probabilities of certain events

```
if( h ) { … }          ||   acquire x
acquire x              ||   print( x.f )
x.f := x.f + 1         ||   release x
release x              ||
```

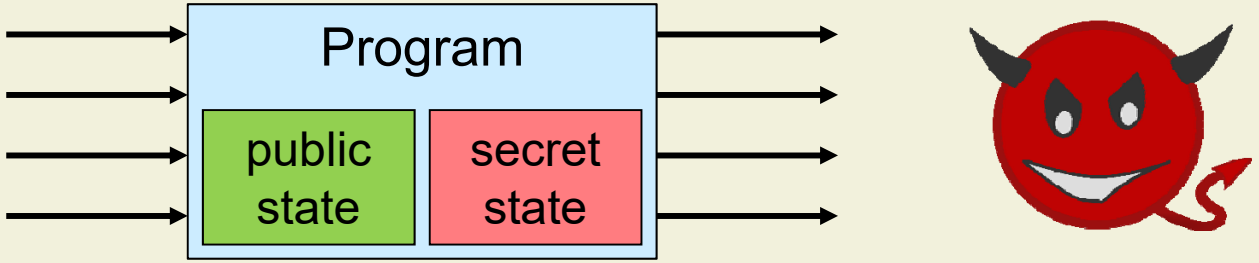
- Verify that timing is low before each thread interaction (fork, join, acquire, release, etc.)

```
acquire x
```

```
assert p = p'
if( p ∧ p' ) {
  assert s = s'
  assert x = x'
  …
}
```

Summary

- Modular verification of non-interference via product programs and relational specifications



- Secure for attackers that observe outputs, crashes, termination, timing, and probabilities

Next Steps

- Implementation
- Experiments
- Optimization, especially to avoid duplicate verification effort
- Soundness proof

- Declassification policies
- Generalization to other k-safety properties