

Slicing Guarantees Information Flow Noninterference

Daniel Wasserrab

September 13, 2023

Abstract

In this contribution, we show how correctness proofs for intra- [8] and interprocedural slicing [9] can be used to prove that slicing is able to guarantee information flow noninterference. Moreover, we also illustrate how to lift the control flow graphs of the respective frameworks such that they fulfil the additional assumptions needed in the noninterference proofs. A detailed description of the intraprocedural proof and its interplay with the slicing framework can be found in [10].

1 Introduction

Information Flow Control (IFC) encompasses algorithms which determines if a given program leaks secret information to public entities. The major group are so called IFC type systems, where well-typed means that the respective program is secure. Several IFC type systems have been verified in proof assistants, e.g. see [1, 2, 5, 3, 7].

However, type systems have some drawbacks which can lead to false alarms. To overcome this problem, an IFC approach basing on slicing has been developed [4], which can significantly reduce the amount of false alarms. This contribution presents the first machine-checked proof that slicing is able to guarantee IFC noninterference. It bases on previously published machine-checked correctness proofs for slicing [8, 9]. Details for the intraprocedural case can be found in [10].

2 HRB Slicing guarantees IFC Noninterference

```
theory NonInterferenceInter  
  imports HRB-Slicing.FundamentalProperty  
begin
```

2.1 Assumptions of this Approach

Classical IFC noninterference, a special case of a noninterference definition using partial equivalence relations (per) [6], partitions the variables (i.e. locations) into security levels. Usually, only levels for secret or high, written H , and public or low, written L , variables are used. Basically, a program that is noninterferent has to fulfil one basic property: executing the program in two different initial states that may differ in the values of their H -variables yields two final states that again only differ in the values of their H -variables; thus the values of the H -variables did not influence those of the L -variables.

Every per-based approach makes certain assumptions: (i) all H -variables are defined at the beginning of the program, (ii) all L -variables are observed (or used in our terms) at the end and (iii) every variable is either H or L . This security label is fixed for a variable and can not be altered during a program run. Thus, we have to extend the prerequisites of the slicing framework in [9] accordingly in a new locale:

```

locale NonInterferenceInterGraph =
  SDG sourcenode targetnode kind valid-edge Entry
  get-proc get-return-edges procs Main Exit Def Use ParamDefs ParamUses
  for sourcenode :: 'edge  $\Rightarrow$  'node and targetnode :: 'edge  $\Rightarrow$  'node
  and kind :: 'edge  $\Rightarrow$  ('var,'val,'ret,'pname) edge-kind
  and valid-edge :: 'edge  $\Rightarrow$  bool
  and Entry :: 'node ('('Entry'-')) and get-proc :: 'node  $\Rightarrow$  'pname
  and get-return-edges :: 'edge  $\Rightarrow$  'edge set
  and procs :: ('pname  $\times$  'var list  $\times$  'var list) list and Main :: 'pname
  and Exit::'node ('('Exit'-'))
  and Def :: 'node  $\Rightarrow$  'var set and Use :: 'node  $\Rightarrow$  'var set
  and ParamDefs :: 'node  $\Rightarrow$  'var list and ParamUses :: 'node  $\Rightarrow$  'var set list +
  fixes H :: 'var set
  fixes L :: 'var set
  fixes High :: 'node ('('High'-'))
  fixes Low :: 'node ('('Low'-'))
  assumes Entry-edge-Exit-or-High:
   $\llbracket$ valid-edge a; sourcenode a = (-Entry-) $\rrbracket$ 
     $\implies$  targetnode a = (-Exit-)  $\vee$  targetnode a = (-High-)
  and High-target-Entry-edge:
   $\exists$  a. valid-edge a  $\wedge$  sourcenode a = (-Entry-)  $\wedge$  targetnode a = (-High-)  $\wedge$ 
    kind a = ( $\lambda$ s. True) $\surd$ 
  and Entry-predecessor-of-High:
   $\llbracket$ valid-edge a; targetnode a = (-High-) $\rrbracket \implies$  sourcenode a = (-Entry-)
  and Exit-edge-Entry-or-Low:  $\llbracket$ valid-edge a; targetnode a = (-Exit-) $\rrbracket$ 
     $\implies$  sourcenode a = (-Entry-)  $\vee$  sourcenode a = (-Low-)
  and Low-source-Exit-edge:
   $\exists$  a. valid-edge a  $\wedge$  sourcenode a = (-Low-)  $\wedge$  targetnode a = (-Exit-)  $\wedge$ 
    kind a = ( $\lambda$ s. True) $\surd$ 
  and Exit-successor-of-Low:
   $\llbracket$ valid-edge a; sourcenode a = (-Low-) $\rrbracket \implies$  targetnode a = (-Exit-)

```

and *DefHigh*: $Def (-High-) = H$
and *UseHigh*: $Use (-High-) = H$
and *UseLow*: $Use (-Low-) = L$
and *HighLowDistinct*: $H \cap L = \{\}$
and *HighLowUNIV*: $H \cup L = UNIV$

begin

lemma *Low-neq-Exit*: **assumes** $L \neq \{\}$ **shows** $(-Low-) \neq (-Exit-)$
 ⟨*proof*⟩

lemma *valid-node-High* [*simp*]:*valid-node* $(-High-)$
 ⟨*proof*⟩

lemma *valid-node-Low* [*simp*]:*valid-node* $(-Low-)$
 ⟨*proof*⟩

lemma *get-proc-Low*:
 $get-proc (-Low-) = Main$
 ⟨*proof*⟩

lemma *get-proc-High*:
 $get-proc (-High-) = Main$
 ⟨*proof*⟩

lemma *Entry-path-High-path*:
assumes $(-Entry-) -as \rightarrow^* n$ **and** *inner-node* n
obtains $a' as'$ **where** $as = a' \# as'$ **and** $(-High-) -as' \rightarrow^* n$
and $kind\ a' = (\lambda s. True) \surd$
 ⟨*proof*⟩

lemma *Exit-path-Low-path*:
assumes $n -as \rightarrow^* (-Exit-)$ **and** *inner-node* n
obtains $a' as'$ **where** $as = as' @ [a']$ **and** $n -as' \rightarrow^* (-Low-)$
and $kind\ a' = (\lambda s. True) \surd$
 ⟨*proof*⟩

lemma *not-Low-High*: $V \notin L \implies V \in H$
 ⟨*proof*⟩

lemma *not-High-Low*: $V \notin H \implies V \in L$
 ⟨*proof*⟩

2.2 Low Equivalence

In classical noninterference, an external observer can only see public values, in our case the L -variables. If two states agree in the values of all L -variables, these states are indistinguishable for him. *Low equivalence* groups those states in an equivalence class using the relation \approx_L :

definition *lowEquivalence* :: ('var \rightarrow 'val) list \Rightarrow ('var \rightarrow 'val) list \Rightarrow bool
(infixl \approx_L 50)

where $s \approx_L s' \equiv \forall V \in L. \text{hd } s \ V = \text{hd } s' \ V$

The following lemmas connect low equivalent states with relevant variables as necessary in the correctness proof for slicing.

lemma *relevant-vars-Entry*:

assumes $V \in \text{rv } S$ (*CFG-node* (-Entry-)) **and** (-High-) $\notin \text{[HRB-slice } S\text{]}_{CFG}$

shows $V \in L$

<proof>

lemma *lowEquivalence-relevant-nodes-Entry*:

assumes $s \approx_L s'$ **and** (-High-) $\notin \text{[HRB-slice } S\text{]}_{CFG}$

shows $\forall V \in \text{rv } S$ (*CFG-node* (-Entry-)). $\text{hd } s \ V = \text{hd } s' \ V$

<proof>

2.3 The Correctness Proofs

In the following, we present two correctness proofs that slicing guarantees IFC noninterference. In both theorems, *CFG-node* (-High-) $\notin \text{HRB-slice } S$, where *CFG-node* (-Low-) $\in S$, makes sure that no high variable (which are all defined in (-High-)) can influence a low variable (which are all used in (-Low-)).

First, a theorem regarding (-Entry-) $-as \rightarrow^*$ (-Exit-) paths in the control flow graph (CFG), which agree to a complete program execution:

lemma *sipa-rv-Low-Use-Low*:

assumes *CFG-node* (-Low-) $\in S$

shows $\llbracket \text{same-level-path-aux } cs \ as; \text{upd-cs } cs \ as = \llbracket; \text{same-level-path-aux } cs \ as';$

$\forall c \in \text{set } cs. \text{valid-edge } c; m \ -as \rightarrow^* \ (-Low-); m \ -as' \rightarrow^* \ (-Low-);$

$\forall i < \text{length } cs. \forall V \in \text{rv } S$ (*CFG-node* (*ourcenode* ($cs!i$))).

$\text{fst } (s! \text{Suc } i) \ V = \text{fst } (s'! \text{Suc } i) \ V; \forall i < \text{Suc } (\text{length } cs). \text{snd } (s!i) = \text{snd } (s'!i);$

$\forall V \in \text{rv } S$ (*CFG-node* m). $\text{state-val } s \ V = \text{state-val } s' \ V;$

$\text{preds } (\text{slice-kinds } S \ as) \ s; \text{preds } (\text{slice-kinds } S \ as') \ s';$

$\text{length } s = \text{Suc } (\text{length } cs); \text{length } s' = \text{Suc } (\text{length } cs)\rrbracket$

$\implies \forall V \in \text{Use } (-Low-). \text{state-val } (\text{transfers}(\text{slice-kinds } S \ as) \ s) \ V =$

$\text{state-val } (\text{transfers}(\text{slice-kinds } S \ as') \ s') \ V$

<proof>

lemma *rv-Low-Use-Low*:

assumes $m -as \rightarrow_{\sqrt{*}} (-Low-)$ **and** $m -as' \rightarrow_{\sqrt{*}} (-Low-)$ **and** $get\text{-}proc\ m = Main$
and $\forall V \in rv\ S\ (CFG\text{-}node\ m). cf\ V = cf'\ V$
and $preds\ (slice\text{-}kinds\ S\ as)\ [(cf,undefined)]$
and $preds\ (slice\text{-}kinds\ S\ as')\ [(cf',undefined)]$
and $CFG\text{-}node\ (-Low-)\ \in\ S$
shows $\forall V \in Use\ (-Low-).$
 $state\text{-}val\ (transfers(slice\text{-}kinds\ S\ as)\ [(cf,undefined)])\ V =$
 $state\text{-}val\ (transfers(slice\text{-}kinds\ S\ as')\ [(cf',undefined)])\ V$
 $\langle proof \rangle$

lemma *nonInterference-path-to-Low*:

assumes $[cf] \approx_L [cf']$ **and** $(-High-) \notin [HRB\text{-}slice\ S]_{CFG}$
and $CFG\text{-}node\ (-Low-)\ \in\ S$
and $(-Entry-)\ -as \rightarrow_{\sqrt{*}} (-Low-)$ **and** $preds\ (kinds\ as)\ [(cf,undefined)]$
and $(-Entry-)\ -as' \rightarrow_{\sqrt{*}} (-Low-)$ **and** $preds\ (kinds\ as')\ [(cf',undefined)]$
shows $map\ fst\ (transfers\ (kinds\ as)\ [(cf,undefined)]) \approx_L$
 $map\ fst\ (transfers\ (kinds\ as')\ [(cf',undefined)])$
 $\langle proof \rangle$

theorem *nonInterference-path*:

assumes $[cf] \approx_L [cf']$ **and** $(-High-) \notin [HRB\text{-}slice\ S]_{CFG}$
and $CFG\text{-}node\ (-Low-)\ \in\ S$
and $(-Entry-)\ -as \rightarrow_{\sqrt{*}} (-Exit-)$ **and** $preds\ (kinds\ as)\ [(cf,undefined)]$
and $(-Entry-)\ -as' \rightarrow_{\sqrt{*}} (-Exit-)$ **and** $preds\ (kinds\ as')\ [(cf',undefined)]$
shows $map\ fst\ (transfers\ (kinds\ as)\ [(cf,undefined)]) \approx_L$
 $map\ fst\ (transfers\ (kinds\ as')\ [(cf',undefined)])$
 $\langle proof \rangle$

end

The second theorem assumes that we have a operational semantics, whose evaluations are written $\langle c, s \rangle \Rightarrow \langle c', s' \rangle$ and which conforms to the CFG. The correctness theorem then states that if no high variable influenced a low variable and the initial states were low equivalent, the resulting states are again low equivalent:

locale *NonInterferenceInter* =

NonInterferenceInterGraph *sourcenode targetnode kind valid-edge Entry*
 $get\text{-}proc\ get\text{-}return\text{-}edges\ procs\ Main\ Exit\ Def\ Use\ ParamDefs\ ParamUses$
 $H\ L\ High\ Low\ +$
SemanticsProperty *sourcenode targetnode kind valid-edge Entry get-proc*
 $get\text{-}return\text{-}edges\ procs\ Main\ Exit\ Def\ Use\ ParamDefs\ ParamUses\ sem\ identifies$
for *sourcenode* :: $'edge \Rightarrow 'node$ **and** *targetnode* :: $'edge \Rightarrow 'node$
and *kind* :: $'edge \Rightarrow ('var, 'val, 'ret, 'pname)\ edge\text{-}kind$
and *valid-edge* :: $'edge \Rightarrow bool$

```

and Entry :: 'node ('('Entry'-')) and get-proc :: 'node ⇒ 'pname
and get-return-edges :: 'edge ⇒ 'edge set
and procs :: ('pname × 'var list × 'var list) list and Main :: 'pname
and Exit::'node ('('Exit'-'))
and Def :: 'node ⇒ 'var set and Use :: 'node ⇒ 'var set
and ParamDefs :: 'node ⇒ 'var list and ParamUses :: 'node ⇒ 'var set list
and sem :: 'com ⇒ ('var → 'val) list ⇒ 'com ⇒ ('var → 'val) list ⇒ bool
  (((1⟨-,/-⟩) ⇒ / (1⟨-,/-⟩)) [0,0,0,0] 81)
and identifies :: 'node ⇒ 'com ⇒ bool (- ≜ - [51,0] 80)
and H :: 'var set and L :: 'var set
and High :: 'node ('('High'-')) and Low :: 'node ('('Low'-')) +
fixes final :: 'com ⇒ bool
assumes final-edge-Low: [final c; n ≜ c]
  ⇒ ∃ a. valid-edge a ∧ sourcenode a = n ∧ targetnode a = (-Low-) ∧ kind a =
  ↑id
begin

```

The following theorem needs the explicit edge from $(-High-)$ to n . An approach using a *init* predicate for initial statements, being reachable from $(-High-)$ via a $(\lambda s. True)_{\surd}$ edge, does not work as the same statement could be identified by several nodes, some initial, some not. E.g., in the program `while (True) Skip;;Skip` two nodes identify this initial statement: the initial node and the node within the loop (because of loop unrolling).

theorem *nonInterference*:

```

assumes [cf1] ≈L [cf2] and (-High-) ∉ [HRB-slice S]CFG
and CFG-node (-Low-) ∈ S
and valid-edge a and sourcenode a = (-High-) and targetnode a = n
and kind a = (λs. True)\surd and n ≜ c and final c'
and ⟨c,[cf1]⟩ ⇒ ⟨c',s1⟩ and ⟨c,[cf2]⟩ ⇒ ⟨c',s2⟩
shows s1 ≈L s2
⟨proof⟩

```

end

end

3 Framework Graph Lifting for Noninterference

theory *LiftingInter*

imports *NonInterferenceInter*

begin

In this section, we show how a valid CFG from the slicing framework in [8] can be lifted to fulfil all properties of the *NonInterferenceIntraGraph* locale. Basically, we redefine the hitherto existing *Entry* and *Exit* nodes as new *High* and *Low* nodes, and introduce two new nodes *NewEntry* and *NewExit*. Then, we have to lift all functions to operate on this new graph.

3.1 Liftings

3.1.1 The datatypes

datatype *'node LDCFG-node* = *Node 'node*
| *NewEntry*
| *NewExit*

type-synonym (*'edge,'node,'var,'val,'ret,'pname*) *LDCFG-edge* =
'node LDCFG-node × ((*'var,'val,'ret,'pname*) *edge-kind*) × *'node LDCFG-node*

3.1.2 Lifting basic definitions using *'edge* and *'node*

inductive *lift-valid-edge* :: (*'edge* ⇒ *bool*) ⇒ (*'edge* ⇒ *'node*) ⇒ (*'edge* ⇒ *'node*)
⇒
(*'edge* ⇒ (*'var,'val,'ret,'pname*) *edge-kind*) ⇒ *'node* ⇒ *'node* ⇒
(*'edge,'node,'var,'val,'ret,'pname*) *LDCFG-edge* ⇒
bool
for *valid-edge*::*'edge* ⇒ *bool* **and** *src*::*'edge* ⇒ *'node* **and** *trg*::*'edge* ⇒ *'node*
and *knd*::*'edge* ⇒ (*'var,'val,'ret,'pname*) *edge-kind* **and** *E*::*'node* **and** *X*::*'node*

where *lve-edge*:

[[*valid-edge a*; *src a* ≠ *E* ∨ *trg a* ≠ *X*;
e = (*Node (src a),knd a,Node (trg a)*)]]
⇒ *lift-valid-edge valid-edge src trg knd E X e*

| *lve-Entry-edge*:

e = (*NewEntry,(λs. True)*√,*Node E*)
⇒ *lift-valid-edge valid-edge src trg knd E X e*

| *lve-Exit-edge*:

e = (*Node X,(λs. True)*√,*NewExit*)
⇒ *lift-valid-edge valid-edge src trg knd E X e*

| *lve-Entry-Exit-edge*:

e = (*NewEntry,(λs. False)*√,*NewExit*)
⇒ *lift-valid-edge valid-edge src trg knd E X e*

lemma [*simp*]:¬ *lift-valid-edge valid-edge src trg knd E X (Node E,et,Node X)*
{*proof*}

fun *lift-get-proc* :: (*'node* ⇒ *'pname*) ⇒ *'pname* ⇒ *'node LDCFG-node* ⇒ *'pname*
where *lift-get-proc get-proc Main (Node n)* = *get-proc n*
| *lift-get-proc get-proc Main NewEntry* = *Main*
| *lift-get-proc get-proc Main NewExit* = *Main*

inductive-set *lift-get-return-edges* :: ('edge \Rightarrow 'edge set) \Rightarrow ('edge \Rightarrow bool) \Rightarrow
('edge \Rightarrow 'node) \Rightarrow ('edge \Rightarrow 'node) \Rightarrow ('edge \Rightarrow ('var,'val,'ret,'pname) edge-kind)
 \Rightarrow ('edge,'node,'var,'val,'ret,'pname) LDCFG-edge
 \Rightarrow ('edge,'node,'var,'val,'ret,'pname) LDCFG-edge set
for *get-return-edges* :: 'edge \Rightarrow 'edge set **and** *valid-edge* :: 'edge \Rightarrow bool
and *src*::'edge \Rightarrow 'node **and** *trg*::'edge \Rightarrow 'node
and *knd*::'edge \Rightarrow ('var,'val,'ret,'pname) edge-kind
and *e*::('edge,'node,'var,'val,'ret,'pname) LDCFG-edge
where *lift-get-return-edgesI*:
 $\llbracket e = (\text{Node } (\text{src } a), \text{knd } a, \text{Node } (\text{trg } a)); \text{valid-edge } a; a' \in \text{get-return-edges } a;$
 $e' = (\text{Node } (\text{src } a'), \text{knd } a', \text{Node } (\text{trg } a')) \rrbracket$
 $\implies e' \in \text{lift-get-return-edges } \text{get-return-edges } \text{valid-edge } \text{src } \text{trg } \text{knd } e$

3.1.3 Lifting the Def and Use sets

inductive-set *lift-Def-set* :: ('node \Rightarrow 'var set) \Rightarrow 'node \Rightarrow 'node \Rightarrow
'var set \Rightarrow 'var set \Rightarrow ('node LDCFG-node \times 'var) set
for *Def*::('node \Rightarrow 'var set) **and** *E*::'node **and** *X*::'node
and *H*::'var set **and** *L*::'var set

where *lift-Def-node*:

$V \in \text{Def } n \implies (\text{Node } n, V) \in \text{lift-Def-set } \text{Def } E X H L$

| *lift-Def-High*:

$V \in H \implies (\text{Node } E, V) \in \text{lift-Def-set } \text{Def } E X H L$

abbreviation *lift-Def* :: ('node \Rightarrow 'var set) \Rightarrow 'node \Rightarrow 'node \Rightarrow
'var set \Rightarrow 'var set \Rightarrow 'node LDCFG-node \Rightarrow 'var set
where *lift-Def* *Def* *E* *X* *H* *L* *n* $\equiv \{ V. (n, V) \in \text{lift-Def-set } \text{Def } E X H L \}$

inductive-set *lift-Use-set* :: ('node \Rightarrow 'var set) \Rightarrow 'node \Rightarrow 'node \Rightarrow
'var set \Rightarrow 'var set \Rightarrow ('node LDCFG-node \times 'var) set
for *Use*::'node \Rightarrow 'var set **and** *E*::'node **and** *X*::'node
and *H*::'var set **and** *L*::'var set

where

lift-Use-node:

$V \in \text{Use } n \implies (\text{Node } n, V) \in \text{lift-Use-set } \text{Use } E X H L$

| *lift-Use-High*:

$V \in H \implies (\text{Node } E, V) \in \text{lift-Use-set } \text{Use } E X H L$

| *lift-Use-Low*:

$V \in L \implies (\text{Node } X, V) \in \text{lift-Use-set } \text{Use } E X H L$

abbreviation *lift-Use* :: ('node ⇒ 'var set) ⇒ 'node ⇒ 'node ⇒
'var set ⇒ 'var set ⇒ 'node LDCFG-node ⇒ 'var set
where *lift-Use Use E X H L n* ≡ {V. (n,V) ∈ *lift-Use-set Use E X H L*}

fun *lift-ParamUses* :: ('node ⇒ 'var set list) ⇒ 'node LDCFG-node ⇒ 'var set list
where *lift-ParamUses ParamUses (Node n)* = *ParamUses n*
| *lift-ParamUses ParamUses NewEntry* = []
| *lift-ParamUses ParamUses NewExit* = []

fun *lift-ParamDefs* :: ('node ⇒ 'var list) ⇒ 'node LDCFG-node ⇒ 'var list
where *lift-ParamDefs ParamDefs (Node n)* = *ParamDefs n*
| *lift-ParamDefs ParamDefs NewEntry* = []
| *lift-ParamDefs ParamDefs NewExit* = []

3.2 The lifting lemmas

3.2.1 Lifting the CFG locales

abbreviation *src* :: ('edge,'node,'var,'val,'ret,'pname) LDCFG-edge ⇒ 'node LD-
CFG-node
where *src a* ≡ *fst a*

abbreviation *try* :: ('edge,'node,'var,'val,'ret,'pname) LDCFG-edge ⇒ 'node LD-
CFG-node
where *try a* ≡ *snd(snd a)*

abbreviation *knd* :: ('edge,'node,'var,'val,'ret,'pname) LDCFG-edge ⇒
('var,'val,'ret,'pname) edge-kind
where *knd a* ≡ *fst(snd a)*

lemma *lift-CFG*:

assumes *wf:CFGExit-wf sourcenode targetnode kind valid-edge Entry get-proc*
get-return-edges procs Main Exit Def Use ParamDefs ParamUses
and *pd:Postdomination sourcenode targetnode kind valid-edge Entry get-proc*
get-return-edges procs Main Exit
shows *CFG src try knd*
(*lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit*) *NewEntry*
(*lift-get-proc get-proc Main*)
(*lift-get-return-edges get-return-edges valid-edge sourcenode targetnode kind*)
procs Main
⟨*proof*⟩

lemma *lift-CFG-wf*:

assumes *wf:CFGExit-wf sourcenode targetnode kind valid-edge Entry get-proc*
get-return-edges procs Main Exit Def Use ParamDefs ParamUses
and *pd:Postdomination sourcenode targetnode kind valid-edge Entry get-proc*

get-return-edges procs Main Exit
shows *CFG-wf src trg kno*
(lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit) NewEntry
(lift-get-proc get-proc Main)
(lift-get-return-edges get-return-edges valid-edge sourcenode targetnode kind)
procs Main (lift-Def Def Entry Exit H L) (lift-Use Use Entry Exit H L)
(lift-ParamDefs ParamDefs) (lift-ParamUses ParamUses)
 <proof>

lemma *lift-CFGExit:*

assumes *wf:CFGExit-wf sourcenode targetnode kind valid-edge Entry get-proc*
get-return-edges procs Main Exit Def Use ParamDefs ParamUses
and *pd:Postdomination sourcenode targetnode kind valid-edge Entry get-proc*
get-return-edges procs Main Exit
shows *CFGExit src trg kno*
(lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit) NewEntry
(lift-get-proc get-proc Main)
(lift-get-return-edges get-return-edges valid-edge sourcenode targetnode kind)
procs Main NewExit
 <proof>

lemma *lift-CFGExit-wf:*

assumes *wf:CFGExit-wf sourcenode targetnode kind valid-edge Entry get-proc*
get-return-edges procs Main Exit Def Use ParamDefs ParamUses
and *pd:Postdomination sourcenode targetnode kind valid-edge Entry get-proc*
get-return-edges procs Main Exit
shows *CFGExit-wf src trg kno*
(lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit) NewEntry
(lift-get-proc get-proc Main)
(lift-get-return-edges get-return-edges valid-edge sourcenode targetnode kind)
procs Main NewExit (lift-Def Def Entry Exit H L) (lift-Use Use Entry Exit H L)
(lift-ParamDefs ParamDefs) (lift-ParamUses ParamUses)
 <proof>

3.2.2 Lifting the SDG

lemma *lift-Postdomination:*

assumes *wf:CFGExit-wf sourcenode targetnode kind valid-edge Entry get-proc*
get-return-edges procs Main Exit Def Use ParamDefs ParamUses
and *pd:Postdomination sourcenode targetnode kind valid-edge Entry get-proc*
get-return-edges procs Main Exit
and *inner:CFGExit.inner-node sourcenode targetnode valid-edge Entry Exit nx*
shows *Postdomination src trg kno*
(lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit) NewEntry
(lift-get-proc get-proc Main)
(lift-get-return-edges get-return-edges valid-edge sourcenode targetnode kind)
procs Main NewExit

<proof>

lemma *lift-SDG*:

assumes *SDG:SDG sourcenode targetnode kind valid-edge Entry get-proc
get-return-edges procs Main Exit Def Use ParamDefs ParamUses*
and *inner:CFGExit.inner-node sourcenode targetnode valid-edge Entry Exit nx*
shows *SDG src trg kno*
(lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit) NewEntry
(lift-get-proc get-proc Main)
(lift-get-return-edges get-return-edges valid-edge sourcenode targetnode kind)
procs Main NewExit (lift-Def Def Entry Exit H L) (lift-Use Use Entry Exit H L)
(lift-ParamDefs ParamDefs) (lift-ParamUses ParamUses)

<proof>

3.2.3 Low-deterministic security via the lifted graph

lemma *Lift-NonInterferenceGraph*:

fixes *valid-edge and sourcenode and targetnode and kind and Entry and Exit*
and *get-proc and get-return-edges and procs and Main*
and *Def and Use and ParamDefs and ParamUses and H and L*
defines *lve:lve \equiv lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit*
and *lget-proc:lget-proc \equiv lift-get-proc get-proc Main*
and *lget-return-edges:lget-return-edges \equiv*
lift-get-return-edges get-return-edges valid-edge sourcenode targetnode kind
and *lDef:lDef \equiv lift-Def Def Entry Exit H L*
and *lUse:lUse \equiv lift-Use Use Entry Exit H L*
and *lParamDefs:lParamDefs \equiv lift-ParamDefs ParamDefs*
and *lParamUses:lParamUses \equiv lift-ParamUses ParamUses*
assumes *SDG:SDG sourcenode targetnode kind valid-edge Entry get-proc
get-return-edges procs Main Exit Def Use ParamDefs ParamUses*
and *inner:CFGExit.inner-node sourcenode targetnode valid-edge Entry Exit nx*
and *H \cap L = {} and H \cup L = UNIV*
shows *NonInterferenceInterGraph src trg kno lve NewEntry lget-proc
lget-return-edges procs Main NewExit lDef lUse lParamDefs lParamUses H L*
(Node Entry) (Node Exit)

<proof>

end

References

- [1] G. Barthe and L. P. Nieto. Secure information flow for a concurrent language with scheduling. *Journal of Computer Security*, 15(6):647–689, 2007.
- [2] G. Barthe, D. Pichardie, and T. Rezk. A certified lightweight non-interference Java bytecode verifier. In *ESOP 2007*, volume 4421 of

LNCS, pages 125–140. Springer, 2007.

- [3] L. Beringer and M. Hofmann. Secure information flow and program logics. In *Archive of Formal Proofs*. <http://isa-afp.org/entries/SIFPL.shtml>, November 2008. Formal proof development.
- [4] C. Hammer and G. Snelting. Flow-sensitive, context-sensitive, and object-sensitive information flow control based on program dependence graphs. *International Journal of Information Security*, 8(6):399–422, 2009.
- [5] F. Kammüller. Formalizing non-interference for a simple bytecode language in Coq. *Formal Aspects of Computing*, 20(3):259–275, 2008.
- [6] A. Sabelfeld and D. Sands. A per model of secure information flow in sequential programs. *Higher Order Symbolic Computation*, 14(1):59–91, 2001.
- [7] G. Snelting and D. Wasserrab. A correctness proof for the Volpano/Smith security typing system. In G. Klein, T. Nipkow, and L. Paulson, editors, *Archive of Formal Proofs*. <http://isa-afp.org/entries/VolpanoSmith.shtml>, September 2008. Formal proof development.
- [8] D. Wasserrab. Towards certified slicing. In G. Klein, T. Nipkow, and L. Paulson, editors, *Archive of Formal Proofs*. <http://isa-afp.org/entries/Slicing.shtml>, September 2008. Formal proof development.
- [9] D. Wasserrab. Backing up slicing: Verifying the interprocedural two-phase Horwitz-Reps-Binkley slicer. In *Archive of Formal Proofs*. <http://isa-afp.org/entries/HRB-Slicing.shtml>, September 2009. Formal proof development.
- [10] D. Wasserrab, D. Lohner, and G. Snelting. On PDG-based noninterference and its modular proof. In *Proc. of PLAS '09*, pages 31–44. ACM, June 2009.