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/StaticInter/FundamentalProperty
begin

1
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 fulfill 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 cannot 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 ⇒ 'node and targetnode :: 'edge ⇒ 'node
and kind :: 'edge ⇒ ('var,'val,'ret,'pname) edge-kind
and valid-edge :: 'edge ⇒ 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 set and ParamUses :: 'node ⇒ '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:
  \[\text{valid-edge a}; \text{sourcenode a} = (\text{-Entry-})\] \implies targetnode a = (\text{-Exit-}) ∨ targetnode a = (\text{-High-})
and High-target-Entry-edge:
  ∃ a. valid-edge a ∧ sourcenode a = (\text{-Entry-}) ∧ targetnode a = (\text{-High-}) ∧
  kind a = (\lambda s. True),\
and Entry-predecessor-of-High:
  \[\text{valid-edge a}; \text{targetnode a} = (\text{-High-})\] \implies sourcenode a = (\text{-Entry-})
and Exit-edge-Entry-or-Low: \[\text{valid-edge a}; \text{targetnode a} = (\text{-Exit-})\] \implies sourcenode a = (\text{-Entry-}) ∨ sourcenode a = (\text{-Low-})
and Low-source-Exit-edge:
  ∃ a. valid-edge a ∧ sourcenode a = (\text{-Low-}) ∧ targetnode a = (\text{-Exit-}) ∧
  kind a = (\lambda s. True),\
and Exit-successor-of-Low:
  \[\text{valid-edge a}; \text{sourcenode a} = (\text{-Low-})\] \implies targetnode a = (\text{-Exit-})
and DefHigh: Def (-High-) = H
and UseHigh: Use (-High-) = H
and UseLow: Use (-Low-) = L
and HighLowDistinct: H ∩ L = {} 
and HighLowUNIV: H ∪ L = UNIV

begin

lemma Low-neq-Exit: assumes L ≠ {} shows (-Low-) ≠ (-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-) →∗ n and inner-node n
obtains a' as' where as = a'#as' and (-High-) →∗ n
and kind a' = (λs. True) √
⟨proof⟩

lemma Exit-path-Low-path:
assumes n →∗ (-Exit-) and inner-node n
obtains a' as' where as = as'[a] and n →∗ (-Low-)
and kind a' = (λs. True) √
⟨proof⟩

lemma not-Low-High: V /∈ L ⇒ V ∈ H
⟨proof⟩

lemma not-High-Low: V /∈ H ⇒ V ∈ 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 $\approx_L$:

\[
\text{definition lowEquivalence :: } \left( \text{var} \rightarrow \text{val} \right) \text{ list } \Rightarrow \left( \text{var} \rightarrow \text{val} \right) \text{ list } \Rightarrow \text{bool} \\
\text{(infixl $\approx_L$ 50)}
\]

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 $V \in \text{rv } S \left( \text{CFG-node } (-\text{Entry}) \right)$ and $(-\text{High}) \notin \lfloor \text{HRB-slice } S \rfloor_{\text{CFG}}$

shows $V \in L$

(\textbf{proof})

**lemma lowEquivalence-relevant-nodes-Entry:**

assumes $s \approx_L s'$ and $(-\text{High}) \notin \lfloor \text{HRB-slice } S \rfloor_{\text{CFG}}$

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

(\textbf{proof})

2.3 The Correctness Proofs

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

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

**lemma slpa-rv-Low-Use-Low:**

assumes $\text{CFG-node } (-\text{Low}) \in S$

shows $\left[ \text{same-level-path-aux cs as; upd-cs cs cs as } = [] \right]; \left[ \text{same-level-path-aux cs as as'} \right]; \left[ \forall c \in \text{set cs. valid-edge c; m } \rightarrow* (-\text{Low}); m \rightarrow* (-\text{Low}); \forall i < \text{length cs. } \forall V \in \text{rv } S \left( \text{CFG-node } (\text{source-node } (\text{cs}!i)) \right) \right]; \text{fst } (s!\text{Suc } i) V = \text{fst } (s'!\text{Suc } i) V; \forall i < \text{Suc } (\text{length cs}). \text{snd } (s!i) = \text{snd } (s'?i); \forall V \in \text{rv } S \left( \text{CFG-node } m \right). \text{state-val } s V = \text{state-val } s' V; \text{preds } (\text{slice-kinds } S \text{ as } s); \text{preds } (\text{slice-kinds } S \text{ as' } s'); \text{length } s = \text{Suc } (\text{length cs}); \text{length } s' = \text{Suc } (\text{length cs}) \right] \Rightarrow \forall V \in \text{Use } (-\text{Low}). \text{state-val } (\text{transfers } (\text{slice-kinds } S \text{ as } s) \left( \text{transfers } (\text{slice-kinds } S \text{ as' } s') \right) V = \text{state-val } (\text{transfers } (\text{slice-kinds } S \text{ as' } s') V$

(\textbf{proof})
lemma rv-Low-Use-Low:
assumes \( m \leftarrow a \, \mapsto \, , \ast \, (\text{-Low-}) \) and \( m \leftarrow a' \, \mapsto \, , \ast \, (\text{-Low-}) \) and get-proc \( m = \text{Main} \)
and \( \forall \, V \in \, \text{rv} \,(\text{CFG-node} \, m) \). \( \text{cf} \, V = \text{cf}' \, V \)
and \( \text{preds} \,(\text{slice-kinds} \, \text{as}) \, [[\text{cf}, \text{undefined}]] \)
and \( \text{preds} \,(\text{slice-kinds} \, \text{as}') \, [[\text{cf}', \text{undefined}]] \)
and \( \text{CFG-node} \,(\text{-Low-}) \in \, S \)
shows \( \forall \, V \in \, \text{Use} \,(\text{-Low-}) \).
state-val \,(\text{transfers} \,(\text{slice-kinds} \, \text{as}) \, [[\text{cf}, \text{undefined}]] \, V =
state-val \,(\text{transfers} \,(\text{slice-kinds} \, \text{as}') \, [[\text{cf}', \text{undefined}]] \, V
⟨proofof⟩

lemma nonInterference-path-to-Low:
assumes \( \text{cf} \approx \text{L} \,(\text{cf}') \) and \( \text{-High-} \notin \text{HRB-slice} \, S \)
and \( \text{CFG-node} \,(\text{-Low-}) \in \, S \)
and \( \,(\text{-Entry-}) \leftarrow a \, \mapsto \, , \ast \, (\text{-Low-}) \) and \( \text{preds} \,(\text{kins} \, \text{as}) \, [[\text{cf}, \text{undefined}]] \)
and \( \,(\text{-Entry-}) \leftarrow a' \, \mapsto \, , \ast \, (\text{-Low-}) \) and \( \text{preds} \,(\text{kins} \, \text{as}') \, [[\text{cf}', \text{undefined}]] \)
shows \( \text{map} \, \text{fst} \,(\text{transfers} \,(\text{kins} \, \text{as}) \, [[\text{cf}, \text{undefined}]] \) \approx \text{L} 
\( \text{map} \, \text{fst} \,(\text{transfers} \,(\text{kins} \, \text{as}') \, [[\text{cf}', \text{undefined}]] 
⟨proofof⟩

theorem nonInterference-path:
assumes \( \text{cf} \approx \text{L} \,(\text{cf}') \) and \( \text{-High-} \notin \text{HRB-slice} \, S \)
and \( \text{CFG-node} \,(\text{-Low-}) \in \, S \)
and \( \,(\text{-Entry-}) \leftarrow a \, \mapsto \, , \ast \, (\text{-Exit-}) \) and \( \text{preds} \,(\text{kins} \, \text{as}) \, [[\text{cf}, \text{undefined}]] \)
and \( \,(\text{-Entry-}) \leftarrow a' \, \mapsto \, , \ast \, (\text{-Exit-}) \) and \( \text{preds} \,(\text{kins} \, \text{as}') \, [[\text{cf}', \text{undefined}]] \)
shows \( \text{map} \, \text{fst} \,(\text{transfers} \,(\text{kins} \, \text{as}) \, [[\text{cf}, \text{undefined}]] \approx \text{L} 
\( \text{map} \, \text{fst} \,(\text{transfers} \,(\text{kins} \, \text{as}') \, [[\text{cf}', \text{undefined}]] 
⟨proofof⟩

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

5
and Entry :: 'node ('Entry'-') and get-proc :: 'node ⇒ 'pname
and get-return-edges :: 'edge ⇒ 'edge set
and proc :: ('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
and identifies :: 'node ⇒ 'com ⇒ bool (\(\equiv\) - [51,0] 80)
and H :: 'var set and L :: 'var set
and High :: 'node ('High') and Low :: 'node ('Low')+
and final-edge-Low: [\[c; n \equiv c\]]
−⇒∃a. valid-edge a ∧ sourcenode a = n ∧ targetnode a = (Low) ∧ kind a = \(\uparrow id\)

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 (\(\lambda s. True\)) 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 \([cf_1] \equiv_L [cf_2]\) and (High) \notin |HRB-slice S| CFG
and CFG-node (Low) S
and valid-edge a and sourcenode a = (High) and targetnode a = n
and kind a = (\(\lambda s. True\)) and n \equiv c and final c'
and \(\langle c, [cf_1] \rangle \Rightarrow \langle c', s_1 \rangle\) and \(\langle c, [cf_2] \rangle \Rightarrow \langle c', s_2 \rangle\)
shows \(s_1 \equiv_L s_2\)
(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 NonInterferenceInterGraph
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
3.1.3 Lifting the Def and Use sets

**inductive-set lift-get-return-edges :: ('edge ⇒ 'edge set) ⇒ ('edge ⇒ bool) ⇒
 ('edge ⇒ 'node) ⇒ ('edge ⇒ 'node) ⇒ ('edge ⇒ ('var,'val,'ret,'pname) edge-kind)
⇒ ('edge,'node,'var,'val,'ret,'pname) LDCFG-edge
⇒ ('edge,'node,'var,'val,'ret,'pname) LDCFG-edge set
for get-return-edges :: 'edge ⇒ 'edge set and valid-edge :: 'edge ⇒ bool
and src::'edge ⇒ 'node and trg::'edge ⇒ 'node
and kn::'edge ⇒ ('var,'val,'ret,'pname) edge-kind
and e::('edge,'node,'var,'val,'ret,'pname) LDCFG-edge
where lift-get-return-edgesI:
  \[e = (Node (src a),kn a,Node (try a)); valid-edge a; a' ∈ get-return-edges a; e' = (Node (src a'),kn a',Node (try a')])\]
  \[⇒ e' ∈ lift-get-return-edges get-return-edges valid-edge src trg kn e\]

**inductive-set lift-Def-set :: ('node ⇒ 'var set) ⇒ 'node ⇒
 'var set ⇒ 'var set ⇒ ('node LDCFG-node × 'var) set
for Def::('node ⇒ 'var set) and E::'node and X::'node
and H::'var set and L::'var set
where lift-Def-node:
  \[V ∈ Def n \implies (Node n,V) ∈ lift-Def-set Def E X H L\]
  \[| lift-Def-High:
  V ∈ H \implies (Node E,V) ∈ lift-Def-set Def E X H L\]
abbreviation lift-Def :: ('node ⇒ 'var set) ⇒ 'node ⇒
 'var set ⇒ 'var set ⇒ 'node LDCFG-node ⇒ 'var set
where lift-Def Def E X H L n ≡ \{V. (n,V) ∈ lift-Def-set Def E X H L\}

**inductive-set lift-Use-set :: ('node ⇒ 'var set) ⇒ 'node ⇒
 'var set ⇒ 'var set ⇒ ('node LDCFG-node × 'var) set
for Use::'node ⇒ 'var set and E::'node and X::'node
and H::'var set and L::'var set
where
  \[V ∈ Use n \implies (Node n,V) ∈ lift-Use-set Use E X H L\]
  \[| lift-Use-High:
  V ∈ H \implies (Node E,V) ∈ lift-Use-set Use E X H L\]
  \[| lift-Use-Low:
  V ∈ L \implies (Node X,V) ∈ lift-Use-set Use E X H L\]
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 LDCFG-node 
where src a ≡ fst a

abbreviation trg :: ('edge,'node,'var,'val,'ret,'pname) LDCFG-edge ⇒ 'node LDCFG-node 
where trg 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 af::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 trg 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 af::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 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 (lift-Def Def Entry Exit H L) (lift-Use Use Entry Exit H L)
(lift-ParamDefs ParamDefs) (lift-ParamUses ParamUses)
⟨proof⟩

lemma lift-CFGE Exit:
assumes wf:CFGEExit-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 CFGEExit src trg 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 NewExit
⟨proof⟩

lemma lift-CFGEExit-wf:
assumes wf:CFGEExit-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:CFGEExit.inner-node sourcenode targetnode valid-edge Entry Exit nx
shows Postdomination src trg 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 NewExit
⟨proof⟩

3.2.2 Lifting the SDG

lemma lift-Postdomination:
assumes wf:CFGEExit-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:CFGEExit.inner-node sourcenode targetnode valid-edge Entry Exit nx
shows Postdomination src trg 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 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 kind valid-edge Entry Exit nx
shows SDG src try kind
(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 ≡ lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit
and lget-proc:lget-proc ≡ lift-get-proc get-proc Main
and lget-return-edges:lget-return-edges ≡
lift-get-return-edges get-return-edges valid-edge sourcenode targetnode kind
and lDef:lDef ≡ lift-Def Def Entry Exit H L
and lUse:lUse ≡ lift-Use Use Entry Exit H L
and lParamDefs:lParamDefs ≡ lift-ParamDefs ParamDefs
and lParamUses:lParamUses ≡ 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 try kind lve NewEntry lget-proc
lget-return-edges procs Main NewExit lDef lUse lParamDefs lParamUses H L
(Node Entry) (Node Exit)
⟨proof⟩

end

References


