Slicing Guarantees Information Flow Noninterference

Daniel Wasserrab

September 19, 2015

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 fulfill 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 determine 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 Slicing guarantees IFC Noninterference

theory NonInterferenceIntra imports
..Slicing/StaticIntra/Slice
..Slicing/Basic/CFGExit-wf
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 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 can not be altered during a program run. Thus, we have to extend the prerequisites of the slicing framework in [8] accordingly in a new locale:

locale NonInterferenceIntraGraph =
BackwardSlice sourcenode targetnode kind valid-edge Entry Def Use state-val
backward-slice +
CFGExit-uf sourcenode targetnode kind valid-edge Entry Def Use state-val Exit
for sourcenode :: 'edge ⇒ 'node and targetnode :: 'edge ⇒ 'node
and kind :: 'edge ⇒ 'state edge-kind and valid-edge :: 'edge ⇒ bool
and Entry :: 'node ('(Entry')') and Def :: 'node ⇒ 'var set
and Use :: 'node ⇒ 'var set and state-val :: 'state ⇒ 'var ⇒ 'val
and backward-slice :: 'node set ⇒ 'node set
and Exit :: 'node ('(Exit')') +
fixes H :: 'var set
fixes L :: 'var set
fixes High :: 'node ('(High')')
fixes Low :: 'node ('(Low')')
assumes Entry-edge-Exit-or-High:
[valid-edge a; sourcenode a = (Entry-)]
⇒ targetnode a = (Exit) ∨ targetnode a = (High-)
and High-target-Entry-edge:
∃ a. valid-edge a ∧ sourcenode a = (Entry-) ∧ targetnode a = (High-) ∧
k kind a = (λs. True)_/
and Entry-predecessor-of-High:
[valid-edge a; targetnode a = (High-)]⇒ sourcenode a = (Entry-)
and Exit-edge-Entry-or-Low: [valid-edge a; targetnode a = (Exit-)]
⇒ sourcenode a = (Entry-) ∨ sourcenode a = (Low-)
and Low-source-Exit-edge:
∃ a. valid-edge a ∧ sourcenode a = (Low-) ∧ targetnode a = (Exit-) ∧
k kind a = (λs. True)_/
and Exit-successor-of-Low:
[valid-edge a; sourcenode a = (Low-)]⇒ targetnode a = (Exit-)
and Def[High]: Def (High-) = H
and Use[High]: Use (High-) = H
and UseLow: Use \((-\text{Low}\text{-})\) = \(L\)
and HighLowDistinct: \(H \cap L = \{\}\)
and HighLowUNIV: \(H \cup L = \text{UNIV}\)

begin

lemma Low-neq-Exit: assumes \(L \neq \{\}\) shows \((-\text{Low}\text{-}) \neq (-\text{Exit}\text{-})\)
(proof)

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

lemma Exit-path-Low-path:
assumes \(n \rightarrow^* (-\text{Exit}\text{-})\) and inner-node \(n\)
obtains \(a'\) as \(\text{where as} = \text{as}'\#a'\) and \(n \rightarrow^* (-\text{Low}\text{-})\)
and kind \(a' = (\lambda s. \text{True})\)
(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 :: 'state ⇒ 'state ⇒ bool (infixl \(\approx_L\) 50)
  where \(s \approx_L s' \equiv \forall V \in L. \text{state-val s V} = \text{state-val s'} V\)

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

lemma relevant-vars-Entry:
assumes \(V \in rv S\) \((-\text{Entry}\text{-})\) and \((-\text{High}\text{-}) \notin \text{backward-slice S}\)
shows \(V \in L\)
(proof)
lemma lowEquivalence-relevant-nodes-Entry:
assumes \( s \approx_L s' \) and \((-\text{High-}) \notin \text{backward-slice } S \)
shows \( \forall V \in \text{rv } S \, (-\text{Entry}) \cdot \text{state-val } s \, V = \text{state-val } s' \, V \)
(proof)

lemma rv-Low-Use-Low:
assumes \((-\text{Low-}) \in S \)
shows \[ n \rightarrow^{*} \text{(-Low-)}; \ n \rightarrow^{*} \text{(-Low-)}; \ 
\forall V \in \text{rv } S \cdot \text{n. state-val } s \, V = \text{state-val } s' \, V; \ 
\text{preds (slice-kinds } S \text{ as)} \, s; \ \text{preds (slice-kinds } S \text{ as}') \, s' \]
\( \Rightarrow \forall V \in \text{Use } (-\text{Low-)} \cdot \text{state-val } \left( \text{transfers (slice-kinds } S \text{ as)} \, s \right) \, V = \ 
\text{state-val } \left( \text{transfers (slice-kinds } S \text{ as}') \, s' \right) \, V \)
(proof)

2.3 The Correctness Proofs

In the following, we present two correctness proofs that slicing guarantees IFC noninterference. In both theorems, \((-\text{High-}) \notin \text{backward-slice } S \), where \((-\text{Low-}) \in S \), 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 nonInterference-path-to-Low:
assumes \( s \approx_L s' \) and \((-\text{High-}) \notin \text{backward-slice } S \) and \((-\text{Low-}) \in S \)
and \((-\text{Entry-}) \rightarrow^{*} \text{(-Low-)} \) and \text{preds (slice-kinds } S \text{ as)} \, s \)
and \((-\text{Entry-}) \rightarrow^{*} \text{(-Low-)} \) and \text{preds (slice-kinds } S \text{ as}') \, s' \)
shows \text{transfers (slice-kinds } S \text{ as)} \, s \approx_L \text{transfers (slice-kinds } S \text{ as}') \, s' \)
(proof)

theorem nonInterference-path:
assumes \( s \approx_L s' \) and \((-\text{High-}) \notin \text{backward-slice } S \) and \((-\text{Low-}) \in S \)
and \((-\text{Entry-}) \rightarrow^{*} \text{(-Exit-)} \) and \text{preds (slice-kinds } S \text{ as)} \, s \)
and \((-\text{Entry-}) \rightarrow^{*} \text{(-Exit-)} \) and \text{preds (slice-kinds } S \text{ as}') \, s' \)
shows \text{transfers (slice-kinds } S \text{ as)} \, s \approx_L \text{transfers (slice-kinds } S \text{ as}') \, s' \)
(proof)

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 NonInterferenceIntra =
The following theorem needs the explicit edge from \((-\text{High}-)\) to \(n\). An approach using a \textit{init} predicate for initial statements, being reachable from \((-\text{High}-)\) via a \((\lambda s. \text{True})\sqrt{\text{edge}}\), does not work as the same statement could be identified by several nodes, some initial, some not. E.g., in the program

\begin{verbatim}
while (True) Skip;;Skip
\end{verbatim}

two nodes identify this initial statement: the initial node and the node within the loop (because of loop unrolling).

\textbf{theorem} nonInterference:
\begin{enumerate}
\item \textbf{assumes} \(s_1 \approx_L s_2\) and \((-\text{High}-) \notin \text{backward-slice} S\) and \((-\text{Low}-) \in S\)
\item \textbf{and} \(\text{valid-edge}\) a and \(\text{sourcenode}\) a = \((-\text{High}-)\) and \(\text{targetnode}\) a = \(n\) and \(\text{kind}\) a = \((\lambda s. \text{True})\sqrt{\text{edge}}\)
\item \textbf{shows} \(s_1' \approx_L s_2'\)
\end{enumerate}

\textbf{⟨proof⟩}

\begin{enumerate}
\item \textbf{fixes} final :: \(\text{com} \Rightarrow \text{bool}\)
\item \textbf{assumes} final-edge-Low :: \([\text{final}\ c; n \triangleq c]\)
\item \(\implies \exists a. \text{valid-edge}\ a \land \text{sourcenode}\ a = n \land \text{targetnode}\ a = (-\text{Low}) \land \text{kind}\ a = \uparrow\text{id}\)
\begin{verbatim}
begin
\end{verbatim}

end

end

3 Framework Graph Lifting for Noninterference

\textbf{theory} LiftingIntra
\begin{verbatim}
imports NonInterferenceIntra ../Slicing/StaticIntra/CDepInstantiations
\end{verbatim}

\begin{verbatim}
begin
\end{verbatim}

In this section, we show how a valid CFG from the slicing framework in [8] can be lifted to fulfill all properties of the \textit{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,'state) LDCFG-edge =
'node LDCFG-node × ('state edge-kind) × 'node LDCFG-node

3.1.2 Lifting valid-edge

inductive lift-valid-edge :: ('edge ⇒ bool) ⇒ ('edge ⇒ 'node) ⇒ ('edge ⇒ 'node)
⇒
('edge ⇒ 'state edge-kind) ⇒ 'node ⇒ 'node ⇒ ('edge,'node,'state) LDCFG-edge
⇒
bool

for valid-edge::'edge ⇒ bool and src::'edge ⇒ 'node and trg::'edge ⇒ 'node
and knd::'edge ⇒ 'state 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⟩

3.1.3 Lifting Def and Use sets

inductive-set lift-Def-set :: ('node ⇒ 'var set) ⇒ 'node ⇒ '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 ⇒ (Node n, V) ∈ lift-Def-set Def E X H L

lift-Def-High:
V ∈ H ⇒ (Node E, V) ∈ lift-Def-set Def E X H L

Abbreviation lift-Def :: ('node ⇒ 'var set) ⇒ 'node ⇒ '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 ⇒ '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

lift-Use-node:
V ∈ Use n ⇒ (Node n, V) ∈ lift-Use-set Use E X H L

lift-Use-High:
V ∈ H ⇒ (Node E, V) ∈ lift-Use-set Use E X H L

lift-Use-Low:
V ∈ L ⇒ (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 }

3.2 The lifting lemmas

3.2.1 Lifting the basic locales

Abbreviation src :: ('edge,'node,'state) LDCFG-edge ⇒ 'node LDCFG-node

where src a ≡ fst a

Abbreviation trg :: ('edge,'node,'state) LDCFG-edge ⇒ 'node LDCFG-node

where trg a ≡ snd(snd a)

definition knd :: ('edge,'node,'state) LDCFG-edge ⇒ 'state edge-kind

where knd a ≡ fst(snd a)

Lemma lift-CFG:
assumes \( \text{af}: \text{CFGExit-wf} \) sourcenode targetnode kind valid-edge Entry Def Use state-val Exit

shows \( \text{CFG src trg} \)
\( (\text{lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit}) \) NewEntry
\( \langle \text{proof} \rangle \)

**lemma** lift-CFG-wf:
assumes \( \text{af}: \text{CFGExit-wf} \) sourcenode targetnode kind valid-edge Entry Def Use state-val Exit
shows \( \text{CFG-wf src trg knd} \)
\( (\text{lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit}) \) NewEntry NewExit
\( \langle \text{proof} \rangle \)

**lemma** lift-CFGExit:
assumes \( \text{af}: \text{CFGExit-wf} \) sourcenode targetnode kind valid-edge Entry Def Use state-val Exit
shows \( \text{CFGExit src trg knd} \)
\( (\text{lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit}) \) NewEntry NewExit
\( \langle \text{proof} \rangle \)

**lemma** lift-CFGExit-wf:
assumes \( \text{af}: \text{CFGExit-wf} \) sourcenode targetnode kind valid-edge Entry Def Use state-val Exit
shows \( \text{CFGExit-wf src trg knd} \)
\( (\text{lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit}) \) NewEntry NewExit
\( \langle \text{proof} \rangle \)

### 3.2.2 Lifting wod-backward-slice

**lemma** lift-wod-backward-slice:
fixes valid-edge and sourcenode and targetnode and kind and Entry and Exit and Def and Use and H and L
defines \( \text{lve}: \text{lev} \equiv \text{lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit} \)
and \( \text{lDef}: \text{lDef} \equiv \text{lift-Def Def Entry Exit H L} \)
and \( \text{lUse}: \text{lUse} \equiv \text{lift-Use Use Entry Exit H L} \)
assumes \( \text{af}: \text{CFGExit-wf} \) sourcenode targetnode kind valid-edge Entry Def Use state-val Exit
and \( H \cap L = \{\} \) and \( H \cup L = \text{UNIV} \)
shows \( \text{NonInterferenceIntraGraph src trg knd lve NewEntry lDef lUse state-val} \)
\( (\text{CFG-wf.wod-backward-slice src trg lve lDef lUse}) \)
NewExit H L (Node Entry) (Node Exit)
\( \langle \text{proof} \rangle \)
3.2.3 Lifting PDG-BS with standard-control-dependence

**Lemma lift-Postdomination:**

- ** Assumes \( wf:CFGExit-wf\) sourcenode targetnode kind valid-edge Entry Def Use state-val Exit
- and \( pd:Postdomination\) sourcenode targetnode kind valid-edge Entry Exit
- and \( inner:CFGExit.inner-node\) sourcenode targetnode valid-edge Entry Exit nz
- Shows Postdomination src trg knd

\( (\text{lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit})\) NewEntry NewExit

⟨proof⟩

**Lemma lift-PDG-scd:**

- ** Assumes PDG sourcenode targetnode kind valid-edge Entry Def Use state-val Exit (Postdomination.standard-control-dependence sourcenode targetnode valid-edge Exit)
- and \( pd:Postdomination\) sourcenode targetnode kind valid-edge Entry Exit
- and \( inner:CFGExit.inner-node\) sourcenode targetnode valid-edge Entry Exit nz
- Shows PDG src trg knd

\( (\text{lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit})\) NewEntry (lift-Def Def Entry Exit H L) (lift-Use Use Entry Exit H L) state-val NewExit (Postdomination.standard-control-dependence src trg)

(⟨proof⟩)

**Lemma lift-PDG-standard-backward-slice:**

- ** Fixes valid-edge and sourcenode and targetnode and kind and Entry and Exit and Def and Use and H and L
- Defines lve:≤v ≡ (\text{lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit})
- and lDef:lDef ≡ (\text{lift-Def Def Entry Exit}) \ H \ L
- and lUse:lUse ≡ (\text{lift-Use Use Entry Exit}) \ H \ L
- Assumes PDG sourcenode targetnode kind valid-edge Entry Def Use state-val Exit (Postdomination.standard-control-dependence sourcenode targetnode valid-edge Exit)
- and \( inner:CFGExit.inner-node\) sourcenode targetnode valid-edge Entry Exit nz
- and \( H \cap L = \{} \ and \ H \cup L = \text{UNIV}
- Shows NonInterferenceIntraGraph src trg knd lve NewEntry lDef lUse state-val

\( (\text{PDG.PDG-BS src trg lve lDef lUse})\) (Postdomination.standard-control-dependence src trg lve NewExit)

\( \text{NewExit} \) \ H \ L \ (Node \ Entry) \ (Node \ Exit)

⟨proof⟩

3.2.4 Lifting PDG-BS with weak-control-dependence

**Lemma lift-StrongPostdomination:**

- ** Assumes \( wf:CFGExit-wf\) sourcenode targetnode kind valid-edge Entry Def Use
state-val Exit
and spd:StrongPostdomination sourcenode targetnode kind valid-edge Entry Exit
and inner:CFGEXIT.inner-node sourcenode targetnode valid-edge Entry Exit nx
shows StrongPostdomination src trg knd
(lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit) NewEntry NewExit
⟨proof⟩

lemma lift-PDG-wcd:
assumes PDG:PDG sourcenode targetnode kind valid-edge Entry Def Use state-val Exit
(StrongPostdomination.weak-control-dependence sourcenode targetnode valid-edge Exit)
and spd:StrongPostdomination sourcenode targetnode kind valid-edge Entry Exit
and inner:CFGEXIT.inner-node sourcenode targetnode valid-edge Entry Exit nx
shows PDG src trg knd
(lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit) NewEntry
(lift-Def Def Entry Exit H L) (lift-Use Use Entry Exit H L) state-val NewExit
(StrongPostdomination.weak-control-dependence src trg
(lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit) NewExit)
⟨proof⟩

lemma lift-PDG-weak-backward-slice:
fixes valid-edge and sourcenode and targetnode and kind and Entry and Exit and Def and Use and H and L
defines lve:≡ lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit
and lDef:≡ lift-Def Def Entry Exit H L
and lUse:≡ lift-Use Use Entry Exit H L
assumes PDG:PDG sourcenode targetnode kind valid-edge Entry Def Use state-val Exit
(StrongPostdomination.weak-control-dependence sourcenode targetnode valid-edge Exit)
and spd:StrongPostdomination sourcenode targetnode kind valid-edge Entry Exit
and inner:CFGEXIT.inner-node sourcenode targetnode valid-edge Entry Exit nx
and H ∩ L = {} and H ∪ L = UNIV
shows NonInterferenceIntraGraph src trg knd lve NewEntry lDef lUse state-val
(PDG.PDG-BS src trg lve lDef lUse
(StrongPostdomination.weak-control-dependence src trg lve NewExit))
NewExit H L (Node Entry) (Node Exit)
⟨proof⟩

end
4 Information Flow for While

theory NonInterferenceWhile imports
  ../Slicing/While/SemanticsWellFormed
  ../Slicing/While/StaticControlDependences
  LiftingIntra
begin
 locale SecurityTypes =
  fixes H :: vname set
  fixes L :: vname set
  assumes HighLowDistinct: H ∩ L = {}
  and HighLowUNIV: H ∪ L = UNIV
begin

4.1 Lifting labels-nodes and Defining final
fun labels-LDCFG-nodes :: cmd ⇒ w-node LDCFG-node ⇒ cmd ⇒ bool
where labels-LDCFG-nodes prog (Node n) c = labels-nodes prog n c
| labels-LDCFG-nodes prog n c = False

lemmas WCFG-path-induct[consumes 1, case-names empty-path Cons-path]
  = CFG.path.induct[OF While-CFG-aux]

lemma lift-valid-node:
  assumes CFG.valid-node sourcenode targetnode (valid-edge prog) n
  shows CFG.valid-node src trg
  (lift-valid-edge (valid-edge prog) sourcenode targetnode kind (-Entry-) (-Exit-)) (Node n)
  ⟨proof⟩

lemma lifted-CFG-fund-prop:
  assumes labels-LDCFG-nodes prog n c and ⟨c,s⟩ -->* ⟨c',s'⟩
  shows ∃ n' as. CFG.path src trg
  (lift-valid-edge (valid-edge prog) sourcenode targetnode kind (-Entry-) (-Exit-)) n as n' ∧ transfers (CFG.kinds knd as) s = s' ∧
  preds (CFG.kinds knd as) s ∧ labels-LDCFG-nodes prog n' c'
  ⟨proof⟩

fun final :: cmd ⇒ bool
  where final Skip = True
  | final c = False
lemma final-edge:
    labels-nodes prog n Skip \implies prog \vdash n \uparrow \text{id} \rightarrow (\text{-Exit-})
    \langle \text{proof} \rangle

4.2 Semantic Non-Interference for Weak Order Dependence

lemmas WODNonInterferenceGraph =
    lift-wod-backward-slice[\text{OF While-CFGExit-wf-aux} \text{HighLowDistinct} \text{HighLowUNIV}]

lemma WODNonInterference:
    \text{NonInterferenceIntra} \text{src} \text{try} \text{kind}
    (lift-valid-edge  \text{(valid-edge prog)} \text{sourcenode} \text{targetnode} \text{kind}
      \text{(-Entry-)} \text{(-Exit-)}))
    \text{NewEntry} (lift-Def  \text{(Defs prog)} \text{(-Entry-)} \text{(-Exit-)} \text{H L})
    (lift-Use (Uses prog) \text{(-Entry-)} \text{(-Exit-)} \text{H L} \text{id}
    \text{(CFG-wf,wod-backward-slice \text{src} \text{try})}
    (lift-valid-edge  \text{(valid-edge prog)} \text{sourcenode} \text{targetnode} \text{kind}
      \text{(-Entry-)} \text{(-Exit-)}))
    \text{(lift-Def} \text{(Defs prog)} \text{(-Entry-)} \text{(-Exit-)} \text{H L})
    (lift-Use (Uses prog) \text{(-Entry-)} \text{(-Exit-)} \text{H L})
    \text{reds} \text{(labels-LDCFG-nodes prog)}
    \text{NewExit} \text{H L} \text{(LDCFG-node.Node (-Entry-))} \text{(LDCFG-node.Node (-Exit-))} \text{final}
    \langle \text{proof} \rangle

4.3 Semantic Non-Interference for Standard Control Dependence

lemma inner-node-exists:\exists n. \text{CFGExit.inner-node} \text{sourcenode} \text{targetnode}
    \text{(valid-edge prog)} \text{(-Entry-)} \text{(-Exit-)} \text{n}
    \langle \text{proof} \rangle

lemmas SCDNonInterferenceGraph =
    lift-PDG-standard-backward-slice[\text{OF WStandardControlDependence.PDG-scd} \text{WhilePostdomination-aux - HighLowDistinct} \text{HighLowUNIV}]

lemma SCDNonInterference:
    \text{NonInterferenceIntra} \text{src} \text{try} \text{kind}
    (lift-valid-edge  \text{(valid-edge prog)} \text{sourcenode} \text{targetnode} \text{kind}
      \text{(-Entry-)} \text{(-Exit-)}))
    \text{NewEntry} (lift-Def \text{(Defs prog)} \text{(-Entry-)} \text{(-Exit-)} \text{H L})
    (lift-Use (Uses prog) \text{(-Entry-)} \text{(-Exit-)} \text{H L} \text{id}
    \text{(PDG.PDG-BS src try})
    (lift-valid-edge  \text{(valid-edge prog)} \text{sourcenode} \text{targetnode} \text{kind}
      \text{(-Entry-)} \text{(-Exit-)})
4.4 Semantic Non-Interference for Weak Control Dependence

lemmas WCDNonInterferenceGraph =
  lift-PDG-weak-backward-slice[\text{OF WeakControlDependence}.PDG-wcd
  WhileStrongPostdomination-aux - HighLowDistinct HighLowUNIV]

lemma WCDNonInterference:
  NonInterferenceIntra src try knd
  (lift-valid-edge (valid-edge prog) source node target node kind
   (-Entry-) (-Exit-))
  NewEntry (lift-Def (Defs prog) (-Entry-) (-Exit-) H L)
  (lift-Use (Uses prog) (-Entry-) (-Exit-) H L) id
  (PDG.PDG-BS src try
   (lift-valid-edge (valid-edge prog) source node target node kind
    (-Entry-) (-Exit-))
   (lift-Def (Defs prog) (-Entry-) (-Exit-) H L)
   (lift-Use (Uses prog) (-Entry-) (-Exit-) H L)
   (StrongPostdomination.weak-control-dependence src try
    (lift-valid-edge (valid-edge prog) source node target node kind
     (-Entry-) (-Exit-)) NewExit))
  reds (labels-LDCFG-nodes prog)
  NewExit H L (LDCFG-node.Node (-Entry-)) (LDCFG-node.Node (-Exit-)) final
  ⟨proof⟩
end

end

References


interference Java bytecode verifier. In *ESOP 2007*, volume 4421 of


