Slicing Guarantees Information Flow Noninterference

Daniel Wasserrab

August 16, 2018

Abstract

In this contribution, we show how correctness proofs for intraprocedural and interprocedural slicing 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 Slicing guarantees IFC Noninterference

theory NonInterferenceIntra imports Slicing.Slice Slicing.CFGExit-uf 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 [8] accordingly in a new locale:

```plaintext
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-) ∧  
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-) ∧  
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 UseHigh: Use (-High-) = H
```
and \textit{UseLow}: \textit{Use} (-\textit{Low}-) = L  \\
and \textit{HighLowDistinct}: H \cap L = \{}  \\
and \textit{HighLowUNIV}: H \cup L = \text{UNIV}

begin

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

\textbf{lemma} \textit{Entry-path-High-path}:  \\
\hspace{1em} \textit{assumes} (-\textit{Entry-}) - as \rightarrow* n \textbf{ and} inner-node n  \\
\hspace{1em} \textit{obtains} a' as' \textbf{ where} as = a'\#as' \textbf{ and} (-\textit{High-}) - as' \rightarrow* n  \\
\hspace{1em} \textbf{and} kind a' = (\lambda s. \text{True})\sqrt  \\
(\textit{proof})

\textbf{lemma} \textit{Exit-path-Low-path}:  \\
\hspace{1em} \textit{assumes} n - as \rightarrow* (-\textit{Exit-}) \textbf{ and} inner-node n  \\
\hspace{1em} \textit{obtains} a' as' \textbf{ where} as = as'[\alpha'[a']] \textbf{ and} n - as' \rightarrow* (-\textit{Low-})  \\
\hspace{1em} \textbf{and} kind a' = (\lambda s. \text{True})\sqrt  \\
(\textit{proof})

\textbf{lemma} \textit{not-Low-High}: V /\notin L \implies V \in H  \\
(\textit{proof})

\textbf{lemma} \textit{not-High-Low}: V /\notin H \implies V \in L  \\
(\textit{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. \textit{Low equivalence} groups those states in an equivalence class using the relation \( \approx_L \):

\textbf{definition} \textit{lowEquivalence} :: 'state \Rightarrow 'state \Rightarrow bool (infixl \( \approx_L \) 50)  \\
\hspace{1em} \textbf{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.

\textbf{lemma} \textit{relevant-vars-Entry}:  \\
\hspace{1em} \textit{assumes} V \in rv S (-\textit{Entry-}) \textbf{ and} (-\textit{High-}) /\notin \text{backward-slice} S  \\
\hspace{1em} \textbf{shows} V \in L  \\
(\textit{proof})
lemma lowEquivalence-relevant-nodes-Entry:
assumes \( s \approx_L s' \) and \((-\text{High-}) \notin \text{backward-slice } S\)
shows \( \forall V \in \text{rv } S \ (-\text{Entry}). \ \text{state-val } s \ V = \text{state-val } s' \ V \)
\(\langle \text{proof} \rangle\)

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

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 \((-\text{Entry-}) - \text{as} \rightarrow^{\ast} (-\text{Exit-})\) 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 \((-\text{Entry-}) - \text{as} \rightarrow^{\ast} (-\text{Low-})\) and \(\text{preds } (\text{slice-kinds } S \ as) \ s\)
and \((-\text{Entry-}) - \text{as}' \rightarrow^{\ast} (-\text{Low-})\) and \(\text{preds } (\text{slice-kinds } S \ as') \ s'\)
shows \(\text{transfers } (\text{slice-kinds } S \ as) \ s \approx_L \text{transfers } (\text{slice-kinds } S \ as') \ s'\)
\(\langle \text{proof} \rangle\)

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

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 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 \((\lambda s. \text{True})\) 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).

\begin{proof}
\end{proof}

\section{Framework Graph Lifting for Noninterference}

\begin{verbatim}
theory LiftingIntra
  imports NonInterferenceIntra Slicing CDepInstantiations
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
\end{verbatim}
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 Lifting

3.1.1 The datatypes

\[
\text{datatype } '\text{node} \text{ LDCFG-node} = \begin{array}{l} \text{Node} \ '\text{node} \\ \text{NewEntry} \\ \text{NewExit} \end{array}
\]

\[
\text{type-synonym } ( \ '\text{edge} \ , \ '\text{node} \ , \ '\text{state} ) \text{ LDCFG-edge} = \begin{array}{l} \ '\text{node} \text{ LDCFG-node} \times ( \ '\text{state edge-kind} ) \times \ '\text{node} \text{ LDCFG-node} \end{array}
\]

3.1.2 Lifting valid-edge

\[
\text{inductive } \text{lift-valid-edge} :: ( '\text{edge} \Rightarrow \text{bool} ) \Rightarrow ( '\text{edge} \Rightarrow '\text{node} ) \Rightarrow ( '\text{edge} \Rightarrow '\text{node} ) \Rightarrow ( '\text{edge} \Rightarrow \text{state edge-kind} ) \Rightarrow '\text{node} \Rightarrow '\text{node} \Rightarrow ( '\text{edge} , '\text{node} , \text{state} ) \text{ LDCFG-edge} \Rightarrow \text{bool}
\]

\[
\text{for } \text{valid-edge} :: '\text{edge} \Rightarrow \text{bool} \text{ and } \text{src} :: '\text{edge} \Rightarrow '\text{node} \text{ and } \text{trg} :: '\text{edge} \Rightarrow '\text{node} \text{ and } \text{knd} :: '\text{edge} \Rightarrow \text{state edge-kind} \text{ and } \text{E} :: '\text{node} \text{ and } \text{X} :: '\text{node}
\]

\[
\text{where } \text{lve-edge}:
\]

\[
[ \text{valid-edge } a; \text{src } a \neq E \lor \text{trg } a \neq X; \]
\[
\quad e = ( \text{Node } ( \text{src } a), \text{knd } a, \text{Node } ( \text{try } a) )]
\[
\Rightarrow \text{lift-valid-edge } \text{valid-edge } \text{src } \text{trg } \text{knd } E \ X \ e
\]

\[
| \text{lve-Entry-edge}:
\]

\[
\quad e = ( \text{NewEntry}, (\lambda s. \text{True})_\swarrow, \text{Node } E)
\]

\[
\Rightarrow \text{lift-valid-edge } \text{valid-edge } \text{src } \text{trg } \text{knd } E \ X \ e
\]

\[
| \text{lve-Exit-edge}:
\]

\[
\quad e = ( \text{Node } X, (\lambda s. \text{True})_\swarrow, \text{NewExit})
\]

\[
\Rightarrow \text{lift-valid-edge } \text{valid-edge } \text{src } \text{trg } \text{knd } E \ X \ e
\]

\[
| \text{lve-Entry-Exit-edge}:
\]

\[
\quad e = ( \text{NewEntry}, (\lambda s. \text{False})_\swarrow, \text{NewExit})
\]

\[
\Rightarrow \text{lift-valid-edge } \text{valid-edge } \text{src } \text{trg } \text{knd } E \ X \ e
\]

\[
\text{lemma } [\text{simp}]; \neg \text{lift-valid-edge } \text{valid-edge } \text{src } \text{trg } \text{knd } E \ X \ ( \text{Node } E, \text{et}, \text{Node } X)
\]

\[
\langle \text{proof} \rangle
\]

3.1.3 Lifting Def and Use sets

\[
\text{inductive-set } \text{lift-Def-set} :: ( '\text{node} \Rightarrow '\text{var set} ) \Rightarrow '\text{node} \Rightarrow '\text{node} \Rightarrow
\]
'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:
\[ V \in \text{Def } n \implies (\text{Node } n, V) \in \text{lift-Def-set } \text{Def } E \text{ } X \text{ } H \text{ } L \]

| lift-Def-High:
\[ V \in \text{H} \implies (\text{Node } E, V) \in \text{lift-Def-set } \text{Def } E \text{ } X \text{ } H \text{ } L \]

abbreviation lift-Def :: ('node ⇒ 'var set) ⇒ 'node ⇒ 'node ⇒ 'var set ⇒ 'var set ⇒ 'node LDCFG-node ⇒ 'var set
where lift-Def \text{Def } E \text{ } X \text{ } H \text{ } L \text{ } n \equiv \{ V. \ (n, V) \in \text{lift-Def-set } \text{Def } E \text{ } X \text{ } H \text{ } 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:
\[ V \in \text{Use } n \implies (\text{Node } n, V) \in \text{lift-Use-set } \text{Use } E \text{ } X \text{ } H \text{ } L \]

| lift-Use-High:
\[ V \in \text{H} \implies (\text{Node } E, V) \in \text{lift-Use-set } \text{Use } E \text{ } X \text{ } H \text{ } L \]

| lift-Use-Low:
\[ V \in \text{L} \implies (\text{Node } X, V) \in \text{lift-Use-set } \text{Use } E \text{ } X \text{ } H \text{ } L \]

abbreviation lift-Use :: ('node ⇒ 'var set) ⇒ 'node ⇒ 'node ⇒ 'var set ⇒ 'var set ⇒ 'node LDCFG-node ⇒ 'var set
where lift-Use \text{Use } E \text{ } X \text{ } H \text{ } L \text{ } n \equiv \{ V. \ (n, V) \in \text{lift-Use-set } \text{Use } E \text{ } X \text{ } H \text{ } 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 \( \text{wf:CFGExit-wf sourcenode targetnode kind valid-edge Entry Def Use state-val Exit} \)

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

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

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

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

3.2.2 Lifting \( \text{wod-backward-slice} \)

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

**Lemma** lift-Postdomination:

- **Assumes**
  - \textup{wf}: \text{CFGExit-wf} \text{ sourcenode targetnode kind valid-edge Entry Def Use state-val Exit}
  - \text{pd}: \text{Postdomination sourcenode targetnode kind valid-edge Entry Exit}
  - \text{inner}: \text{CFGExit.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 NewExit

⟨proof⟩

**Lemma** lift-PDG-scd:

- **Assumes**
  - PDG: PDG sourcenode targetnode kind valid-edge Entry Def Use state-val Exit (Postdomination.standard-control-dependence sourcenode targetnode valid-edge Exit)
  - pd: Postdomination sourcenode targetnode kind valid-edge Entry Exit
  - 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
  - (Postdomination.standard-control-dependence src trg)
  - (lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit) NewExit)

⟨proof⟩

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

- **Fixes**
  - valid-edge and sourcenode and targetnode and kind and Entry and Exit
  - Def and Use and H and L

- **Defines**
  - lve: \equiv \text{lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit}
  - lDef: lDef \equiv \text{lift-Def Def Entry Exit H L}
  - lUse: lUse \equiv \text{lift-Use Use Entry Exit H L}

- **Assumes**
  - PDG: PDG sourcenode targetnode kind valid-edge Entry Def Use state-val Exit (Postdomination.standard-control-dependence sourcenode targetnode valid-edge Exit)
  - pd: Postdomination sourcenode targetnode kind valid-edge Entry Exit
  - inner: CFGExit.inner-node sourcenode targetnode valid-edge Entry Exit nx
  - H \cap L = \{\} \text{ and } H \cup L = \text{UNIV}

- **Shows**
  - NonInterferenceIntraGraph src trg knd lve NewEntry lDef lUse state-val (PDG.PDG-BS src trg lve lDef lUse
  - (Postdomination.standard-control-dependence src trg lve NewExit)) NewExit H L (Node Entry) (Node Exit)

⟨proof⟩

3.2.4 Lifting PDG-BS with weak-control-dependence

**Lemma** lift-StrongPostdomination:

- **Assumes**
  - \textup{wf}: \text{CFGExit-wf} \text{ 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:=lve ≡ lift-valid-edge valid-edge sourcenode targetnode kind Entry Exit
and lDef:=lDef ≡ lift-Def Def Entry Exit H L
and lUse:=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

definition theory NonInterferenceWhile imports
  Slicing.SemanticsWellFormed
  Slicing.SlicingStaticDependences
  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 ⇒ prog ⊢ n ↪ id → (-Exit-)
⟨proof⟩

4.2 Semantic Non-Interference for Weak Order Dependence

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

lemma WODNonInterference:
  NonInterferenceIntra src trg knd
   (lift-valid-edge (valid-edge prog) sourcenode targetnode kind
    (-Entry-) (-Exit-))
  NewEntry (lift-Def (Defs prog) (-Entry-) (-Exit-) H L)
  (lift-Use (Uses prog) (-Entry-) (-Exit-) H L) id
  (CFG-wf.wod-backward-slice src trg
   (lift-valid-edge (valid-edge prog) sourcenode targetnode kind
    (-Entry-) (-Exit-))
   (lift-Def (Defs prog) (-Entry-) (-Exit-) H L)
   (lift-Use (Uses prog) (-Entry-) (-Exit-) H L))
  reds (labels-LDCFG-nodes prog)
  NewExit H L (LDCFG-node.Node (-Entry-)) (LDCFG-node.Node (-Exit-)) final
⟨proof⟩

4.3 Semantic Non-Interference for Standard Control Dependence

lemma inner-node-exists: ∃ n. CFGExit.inner-node sourcenode targetnode
  (valid-edge prog) (-Entry-) (-Exit-) n
⟨proof⟩

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

lemma SCDNonInterference:
  NonInterferenceIntra src trg knd
   (lift-valid-edge (valid-edge prog) sourcenode targetnode 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 trg
   (lift-valid-edge (valid-edge prog) sourcenode targetnode kind
    (-Entry-) (-Exit-))

12
4.4 Semantic Non-Interference for Weak Control Dependence

lemmas WCDNonInterferenceGraph =
  lift-PDG-weak-backward-slice[OF WWeakControlDependence.PDG-wcd
  WhileStrongPostdomination-aux - HighLowDistinct HighLowUNIV]

lemma WCDNonInterference:
  NonInterferenceIntra src trg kind
  (lift-valid-edge (valid-edge prog) sourcenode targetnode 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 trg
   (lift-valid-edge (valid-edge prog) sourcenode targetnode kind
    (-Entry-) (-Exit-))
    (lift-Def (Defs prog) (-Entry-) (-Exit-) H L)
    (lift-Use (Uses prog) (-Entry-) (-Exit-) H L)
    (StrongPostdomination.weak-control-dependence src trg
     (lift-valid-edge (valid-edge prog) sourcenode targetnode kind
      (-Entry-) (-Exit-)) NewExit))
  reds (labels-LDCFG-nodes prog)
  NewExit H L (LDCFG-node.Node (-Entry-)) (LDCFG-node.Node (-Exit-)) final
  ⟨proof⟩
end

References


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


