An Isabelle/HOL formalization of Strong Security

Sylvia Grewe, Alexander Lux, Heiko Mantel, Jens Sauer

August 16, 2018

Abstract

Research in information-flow security aims at developing methods to identify undesired information leaks within programs from private sources to public sinks. Noninterference captures this intuition. Strong security from [2] formalizes noninterference for concurrent systems.

We present an Isabelle/HOL formalization of strong security for arbitrary security lattices ([2] uses a two-element security lattice). The formalization includes compositionality proofs for strong security and a soundness proof for a security type system that checks strong security for programs in a simple while language with dynamic thread creation.

Our formalization of the security type system is abstract in the language for expressions and in the semantic side conditions for expressions. It can easily be instantiated with different syntactic approximations for these side conditions. The soundness proof of such an instantiation boils down to showing that these syntactic approximations imply the semantic side conditions.

Contents

1 Preliminary definitions 2
   1.1 Type synonyms ............................................. 2

2 Strong security 4
   2.1 Definition of strong security ............................. 4
   2.2 Proof technique for compositionality results .......... 6
   2.3 Proof of parallel compositionality ........................ 7

3 Example language and compositionality proofs 8
   3.1 Example language with dynamic thread creation ........ 8
   3.2 Proofs of atomic compositionality results .............. 9
   3.3 Proofs of non-atomic compositionality results .......... 11
4 Security type system

4.1 Abstract security type system with soundness proof . . . . . 12
4.2 Example language for Boolean and arithmetic expressions . . 13
4.3 Example interpretation of abstract security type system . . . 14

1 Preliminary definitions

1.1 Type synonyms

The formalization is parametric in different aspects. Notably, it is parametric in the security lattice it supports.

For better readability, we use the following type synonyms in our formalization:

theory Types
imports Main
begin

— type parameters:
— 'exp: expressions (arithmetic, boolean...)
— 'val: values
— 'id: identifier names
— 'com: commands
— 'd: domains

This is a collection of type synonyms. Note that not all of these type synonyms are used within Strong-Security - some are used in WHATandWHERE-Security.

— type for memory states - map ids to values
type-synonym ('id, 'val) State = 'id ⇒ 'val

— type for evaluation functions mapping expressions to a values depending on a state
type-synonym ('exp, 'id, 'val) Evalfunction = 'exp ⇒ ('id, 'val) State ⇒ 'val

— define configurations with threads as pair of commands and states
type-synonym ('id, 'val, 'com) TConfig = 'com × ('id, 'val) State

— define configurations with thread pools as pair of command lists (thread pool) and states
type-synonym ('id, 'val, 'com) TPCConfig = ('com list) × ('id, 'val) State

— type for program states (including the set of commands and a symbol for terminating - None)
type-synonym 'com ProgramState = 'com option
— type for configurations with program states
\texttt{type-synonym \texttt{('id, 'val, 'com)} PSConfig = 'com ProgramState \times (\texttt{'id, 'val}) State}

— type for labels with a list of spawned threads
\texttt{type-synonym \texttt{('com list)}}

— type for step relations from single commands to a program state, with a label
\texttt{type-synonym \texttt{('exp, 'id, 'val, 'com)} TLSteps = ((\texttt{'id, 'val, 'com}) TConfig \times (\texttt{'com Label})
\quad \times (\texttt{'id, 'val, 'com}) PSConfig) set}

— curried version of previously defined type
\texttt{type-synonym \texttt{('exp, 'id, 'val, 'com)} TLSteps-curry = 'com \Rightarrow (\texttt{'id, 'val}) State \Rightarrow (\texttt{'id, 'val}) State \Rightarrow bool}

— type for step relations from thread pools to thread pools
\texttt{type-synonym \texttt{('exp, 'id, 'val, 'com)} TPSteps = ((\texttt{'id, 'val, 'com}) TPConfig \times (\texttt{'id, 'val, 'com}) TPConfig) set}

— curried version of previously defined type
\texttt{type-synonym \texttt{('exp, 'id, 'val, 'com)} TPSteps-curry = \texttt{'com list} \Rightarrow (\texttt{'id, 'val}) State \Rightarrow (\texttt{'id, 'val}) State \Rightarrow bool}

— define type of step relations for single threads to thread pools
\texttt{type-synonym \texttt{('exp, 'id, 'val, 'com)} TSteps = ((\texttt{'id, 'val, 'com}) TConfig \times (\texttt{'id, 'val, 'com}) TPConfig) set}

— define the same type as TSteps, but in a curried version (allowing syntax abbreviations)
\texttt{type-synonym \texttt{('exp, 'id, 'val, 'com)} TSteps-curry = \texttt{'com list} \Rightarrow (\texttt{'id, 'val}) State \Rightarrow (\texttt{'id, 'val}) State \Rightarrow bool}

— type for simple domain assignments; \texttt{'d} has to be an instance of order (partial order)
\texttt{type-synonym \texttt{('id, 'd) DomainAssignment = 'id} \Rightarrow 'd::order}

\texttt{type-synonym \texttt{'com Bisimulation-type = ((\texttt{'com list}) \times (\texttt{'com list}) set}}

— type for escape hatches
\texttt{type-synonym \texttt{('d, 'exp) Hatch = 'd} \times 'exp}

— type for sets of escape hatches
\texttt{type-synonym \texttt{('d, 'exp) Hatches = (('d, 'exp) Hatch) set}}

— type for local escape hatches
\texttt{type-synonym \texttt{('d, 'exp) lHatch = 'd} \times 'exp \times nat}
— type for sets of local escape hatches

**type-synonym**

\[ ('d, 'exp) lHatches = (('d, 'exp) lHatch) \text{ set} \]

end

2 Strong security

2.1 Definition of strong security

We define strong security such that it is parametric in a security lattice \( ('d) \). The definition of strong security by itself is language-independent, therefore the definition is parametric in a programming language \( ('com) \) in addition.

```plaintext
theory Strong-Security
imports Types
begin
locale Strong-Security =
fixes SR :: \( ('exp, 'id, 'val, 'com) \) TSteps
and DA :: \( ('id, 'd::order) \) DomainAssignment
begin

— define when two states are indistinguishable for an observer on domain \( d \)

**definition**

\( d\text{-equal} \) :: \( 'd::order \Rightarrow ('id, 'val) State \Rightarrow bool \)

where

\[ d\text{-equal} \ d \ m \ m' \equiv \forall \ x. \ ((DA \ x) \leq d \rightarrow (m \ x) = (m' \ x)) \]

**abbreviation**

\( d\text{-equal}' \) :: \( ('id, 'val) State \Rightarrow 'd::order \Rightarrow ('id, 'val) State \Rightarrow bool \)

( \( (-, -) \) )

where

\( m =_d m' \equiv d\text{-equal} \ d \ m \ m' \)

— transitivity of \( d\)-equality

**lemma**

\( d\text{-equal-trans} \):

\[ [ m =_d m'; m' =_d m'' ] \rightarrow m =_d m'' \]

⟨proof⟩

**abbreviation**

\( SR\text{abbr} \) :: \( ('exp, 'id, 'val, 'com) \) TSteps-curry

\( ((1 \cdot, \cdot, \cdot) \rightarrow (1 \cdot, \cdot, \cdot)) [0,0,0,0] \) 81⟩

where

\( \langle c, m \rangle \rightarrow \langle c', m' \rangle \equiv ((c, m), (c', m')) \in SR \)
— predicate for strong d-bisimulation

**definition** Strong-d-Bisimulation :: 'd ⇒ 'com Bisimulation-type ⇒ bool

**where**

Strong-d-Bisimulation d R ≡

\((\text{sym } R) \land
\begin{align*}
& (\forall (V,V') \in R. \text{length } V = \text{length } V') \land \\
& (\forall (V,V') \in R. \forall i \lt \text{length } V. \forall m1 m1' m2 W. \\
& \langle V!i,m1 \rangle \rightarrow \langle W,m2 \rangle \land m1 \stackrel{d}{=} m1' \\
& \rightarrow (\exists W' m2'. \langle V!i,m1' \rangle \rightarrow \langle W',m2' \rangle \land (W,W') \in R \land m2 \stackrel{d}{=} m2'))
\end{align*}
\)

— union of all strong d-bisimulations

**definition** USdB :: 'd ⇒ 'com Bisimulation-type

\((\approx_d) \equiv \bigcup \{r. \text{Strong-d-Bisimulation } d r\}\)

**abbreviation** relatedbyUSdB :: 'com list ⇒ 'd ⇒ 'com list ⇒ bool

\((\approx_d) \equiv \bigcup \{r. \text{Strong-d-Bisimulation } d r\}\)

**where**

\(V \approx_d V' \equiv (V,V') \in USdB d\)

— predicate to define when a program is strongly secure

**definition** Strongly-Secure :: 'com list ⇒ bool

\(\text{Strongly-Secure } V \equiv \bigcup \{d. V \approx_d V\}\)

— auxiliary lemma to obtain central strong d-Bisimulation property as Lemma in meta logic (allows instantiating all the variables manually if necessary)

**lemma** strongdB-aux: \(\forall V V' m1 m1' m2 W i. \big[ \text{Strong-d-Bisimulation } d R; \\
\forall i \lt \text{length } V; \forall V,V' \in R; \forall m1 \rightarrow \langle W,m2 \rangle; m1 \stackrel{d}{=} m1' \big] \\
\rightarrow (\exists W' m2'. \forall i. \forall m1' \rightarrow \langle W',m2' \rangle \land (W,W') \in R \land m2 \stackrel{d}{=} m2')\)

**lemma** trivialpair-in-USdB:

\(\llbracket \approx_d \rrbracket\)

**lemma** USdBsym:

\(\text{sym } (\approx_d)\)

**lemma** USdBlen:

\(V \approx_d V' \rightarrow \text{length } V = \text{length } V'\)

**lemma** USdB-Strong-d-Bisimulation:

\(\text{Strong-d-Bisimulation } d (\approx_d)\)
2.2 Proof technique for compositionality results

For proving compositionality results for strong security, we formalize the following “up-to technique” and prove it sound:

theory Up-To-Technique
imports Strong-Security
begin

case Strong-Security
begin

— define d-bisimulation 'up to' union of strong d-Bisimulations

definition d-Bisimulation-Up-To-USdB ::

\( \mathcal{D} \rightarrow \mathcal{C} \times \mathbb{B} \)

where

d-Bisimulation-Up-To-USdB \( d \mathcal{R} \)

\( \equiv (\text{sym } \mathcal{R}) \land (\forall (V, V') \in \mathcal{R}. \text{length } V = \text{length } V') \land \\
(\forall (V, V') \in \mathcal{R}. \forall i < \text{length } V. \forall m1 m1' W m2. \\
\langle V!i, m1 \rangle \rightarrow \langle W, m2 \rangle \land (m1 =_d m1') \\
\rightarrow (\exists W' m2'. \langle V'!i, m1' \rangle \rightarrow \langle W', m2' \rangle \\
\land (W, W') \in (\mathcal{R} \cup (\approx_d)) \land (m2 =_d m2')))

lemma UpTo-aux: \( \forall V V' m1 m1' m2 W \ i. [\ \text{d-Bisimulation-Up-To-USdB } d \mathcal{R}; \\
\ i < \text{length } V; (V, V') \in \mathcal{R}; \langle V!i, m1 \rangle \rightarrow \langle W, m2 \rangle; m1 =_d m1' ] \\
\rightarrow (\exists W' m2'. \langle V'!i, m1' \rangle \rightarrow \langle W', m2' \rangle \\
\land (W, W') \in (\mathcal{R} \cup (\approx_d)) \land (m2 =_d m2')) \\
\langle \text{proof} \rangle)

lemma RuUSdBeqlen:
[ d-Bisimulation-Up-To-USdB d \mathcal{R}; \\
\ (V, V') \in (\mathcal{R} \cup (\approx_d)) ] \\
\rightarrow \text{length } V = \text{length } V' \\
\langle \text{proof} \rangle)

lemma Up-To-Technique:

assumes upToR: d-Bisimulation-Up-To-USdB d \mathcal{R} \\
shows \( R \subseteq \approx_d \\
\langle \text{proof} \rangle)

end
2.3 Proof of parallel compositionality

We prove that strong security is preserved under composition of strongly
secure threads.

theory Parallel-Composition
imports Up-To-Technique
begin

context Strong-Security
begin

theorem parallel-composition:
  assumes eqlen: length V = length V'
  assumes partsrelated: ∀ i < length V. [V!i] ≈d [V'!i]
  shows V ≈d V'
⟨proof⟩

lemma parallel-decomposition:
  assumes related: V ≈d V'
  shows ∀ i < length V. [V!i] ≈d [V'!i]
⟨proof⟩

lemma USdB-comp-head-tail:
  assumes relatedhead: [c] ≈d [c']
  assumes relatedtail: V ≈d V'
  shows (c#V) ≈d (c'#V')
⟨proof⟩

lemma USdB-decomp-head-tail:
  assumes relatedlist: (c#V) ≈d (c'#V')
  shows [c] ≈d [c'] ∧ V ≈d V'
⟨proof⟩

end

end
3 Example language and compositionality proofs

3.1 Example language with dynamic thread creation

As in [2], we instantiate the language with a simple while language that supports dynamic thread creation via a fork command (Multi-threaded While Language with fork, MWLf). Note that the language is still parametric in the language used for Boolean and arithmetic expressions (‘exp).

theory MWLf
imports Types
begin

— SYNTAX

— Commands for the multi-threaded while language with fork (to instantiate ‘com)
datatype (‘exp, ‘id) MWLfCom
  = Skip (skip)
  | Assign ‘id ‘exp
     (:- [70,70] 70)
  | Seq (‘exp, ‘id) MWLfCom
     (‘exp, ‘id) MWLfCom
     (:: [61,60] 60)
  | If-Else ‘exp (‘exp, ‘id) MWLfCom
     (‘exp, ‘id) MWLfCom
     (if - then - else - fi [80,79,79] 70)
  | While-Do ‘exp (‘exp, ‘id) MWLfCom
     (while - do - od [80,79] 70)
  | Fork (‘exp, ‘id) MWLfCom
     ((‘exp, ‘id) MWLfCom) list
     (fork - [70,70] 70)

— SEMANTICS

locale MWLf-semantics =
  fixes E :: (‘exp, ‘id, ‘val) Evalfunction
  and BMap :: ‘val ⇒ bool
begin

— steps semantics, set of deterministic steps from single threads to either single
  threads or thread pools
inductive-set MWLfSteps-det :: (‘exp, ‘id, ‘val, (‘exp, ‘id) MWLfCom) TSteps
and MWLfSteps-det’ :: (‘exp, ‘id, ‘val, (‘exp, ‘id) MWLfCom) TSteps-curry
  (((1⟨-/-⟩) −→) (1⟨-/-⟩) [0,0,0,0] 81)
where
  ⟨c1,m1⟩ −→ ⟨c2,m2⟩ ≡ (((c1,m1),(c2,m2)) ∈ MWLfSteps-det |
skip: ⟨skip,m⟩ −→ ⟨[],m⟩ |
assign: \((E e m) = v \implies (x := e, m) \rightarrow ([I], m(x := v))\) |
seq1: \(c_1, m \rightarrow ([I], m') \implies c_1; c_2, m \rightarrow ([c_2], m')\) |
seq2: \(c_1, m \rightarrow (c_1', V, m') \implies (c_1; c_2, m') \rightarrow (c_1', c_2', V, m')\) |
iftrue: \(BMap (E b m) = True \implies (if b then c_1 else c_2 fi, m) \rightarrow ([c_1], m)\) |
ifferalse: \(BMap (E b m) = False \implies (if b then c_1 else c_2 fi, m) \rightarrow ([c_2], m)\) |
whiletrue: \(BMap (E b m) = True \implies (while b do c od, m) \rightarrow ([c; (while b do c od)], m)\) |
whilefalse: \(BMap (E b m) = False \implies (while b do c od, m) \rightarrow ([I], m)\) |
fork: \(fork c V, m \rightarrow c'@V, m\) |
skip: \(\langle skip, m \rangle \rightarrow (W, m')\) |
assign: \(\langle x := e, m \rangle \rightarrow (W, m')\) |
seq1: \(\langle c_1; c_2, m \rangle \rightarrow (W, m')\) |
seq2: \(\langle c_1', V, m' \rangle \rightarrow (c_1; c_2, m') \rightarrow (c_1', c_2', V, m')\) |
iftrue: \(BMap (E b m) = True \implies (if b then c_1 else c_2 fi, m) \rightarrow ([c_1], m)\) |
ifferalse: \(BMap (E b m) = False \implies (if b then c_1 else c_2 fi, m) \rightarrow ([c_2], m)\) |
whiletrue: \(BMap (E b m) = True \implies (while b do c od, m) \rightarrow ([c; (while b do c od)], m)\) |
whilefalse: \(BMap (E b m) = False \implies (while b do c od, m) \rightarrow ([I], m)\) |
fork: \(fork c V, m \rightarrow c'@V, m\) |
— non-deterministic, possibilistic system step (added for intuition, not used in the proofs)

inductive-cases \(MWLfSteps-det-cases\):
\(\langle skip, m \rangle \rightarrow (W, m')\) |
\(\langle x := e, m \rangle \rightarrow (W, m')\) |
\(\langle c_1; c_2, m \rangle \rightarrow (W, m')\) |
\(\langle if b then c_1 else c_2 fi, m \rangle \rightarrow (c_1; c_2, m') \rightarrow (c_1', c_2', V, m')\) |
\(\langle while b do c od, m \rangle \rightarrow ([c; (while b do c od)], m)\) |
\(\langle while b do c od, m \rangle \rightarrow ([I], m)\) |
\(\langle while b do c od, m \rangle \rightarrow ([I], m)\) |
\(\langle fork c V, m \rangle \rightarrow (c', V, m)\) |

end

3.2 Proofs of atomic compositionality results

We prove for each atomic command of our example programming language (i.e. a command that is not composed out of other commands) that it is strongly secure if the expressions involved are indistinguishable for an observer on security level \(d\).

code theory \(Strongly-Secure-Skip-Assign\)
imports \(MWLf Parallel-Composition\)
begin
locale \(Strongly-Secure-Programs\) =

end
L? : MWLf-semantics E BMap
+ SS?: Strong-Security MWLfSteps-det DA
for E :: (exp, id, val) Evalfunction
and BMap :: val ⇒ bool
and DA :: (id, d::order) DomainAssignment
begin

abbreviation USdBname :: d ⇒ (exp, id) MWLfCom Bisimulation-type
(≈)
where ≈ d ≡ USdB d

abbreviation relatedbyUSdB :: (exp, id) MWLfCom list ⇒ d
⇒ (exp, id) MWLfCom list ⇒ bool
(infixr ≈ . 65)
where V ≈ d V′ ≡ (V, V′) ∈ USdB d

— define when two expressions are indistinguishable with respect to a domain d

definition d-indistinguishable :: d::order ⇒ exp ⇒ exp ⇒ bool
where
d-indistinguishable d e1 e2 ≡
∀ m m’. ((m = d m’) −→ ((E e1 m) = (E e2 m’)))

abbreviation d-indistinguishable' :: exp ⇒ d::order ⇒ exp ⇒ bool
( ( - ≡ - ) )
where
e1 ≡ d e2 ≡ d-indistinguishable d e1 e2

— symmetry of d-indistinguishable
lemma d-indistinguishable-sym:
e ≡ d e′ ⇒ e′ ≡ d e
⟨proof⟩

lemma d-indistinguishable-trans:
[ [ e ≡ d e’; e’ ≡ d e” ] ] ⇒ e ≡ d e”
⟨proof⟩

theorem Strongly-Secure-Skip:
[skip] ≈ d [skip]
⟨proof⟩

theorem Strongly-Secure-Assign:
assumes d-indistinguishable-exp: e ≡ DA x e’
shows [x := e] ≈ d [x := e’]
⟨proof⟩

end

end
3.3 Proofs of non-atomic compositionality results

We prove compositionality results for each non-atomic command of our example programming language (i.e., a command that is composed out of other commands): If the components are strongly secure and the expressions involved indistinguishable for an observer on security level $d$, then the composed command is also strongly secure.

theory Language-Composition
imports Strongly-Secure-Skip-Assign
begin

context Strongly-Secure-Programs
begin

theorem Compositionality-Seq:
assumes relatedpart1: $[c1] \approx_d [c1']$
assumes relatedpart2: $[c2] \approx_d [c2']$
shows $[c1;c2] \approx_d [c1';c2']$
⟨proof⟩

theorem Compositionality-Fork:
fixes $V::(\exp',\id')$ MWLjCom list
assumes relatedmain: $[c] \approx_d [c']$
assumes relatedthreads: $V \approx_d V'$
shows $[fork c V] \approx_d [fork c' V']$
⟨proof⟩

theorem Compositionality-If:
assumes dind-or-branchesrelated:
  $b \equiv_d b' \lor [c1] \approx_d [c2] \lor [c1'] \approx_d [c2']$
assumes branch1related: $[c1] \approx_d [c1']$
assumes branch2related: $[c2] \approx_d [c2']$
shows $[if b then c1 else c2 fi] \approx_d [if b' then c1' else c2' fi]$
⟨proof⟩

theorem Compositionality-While:
assumes dind: $b \equiv_d b'$
assumes bodyrelated: $[c] \approx_d [c']$
shows $[while b do c od] \approx_d [while b' do c' od]$
⟨proof⟩

end

end
4 Security type system

4.1 Abstract security type system with soundness proof

We formalize an abstract version of the type system in [2] using locales [1]. Our formalization of the type system is abstract in the sense that the rules specify abstract semantic side conditions on the expressions within a command that satisfy for proving the soundness of the rules. That is, it can be instantiated with different syntactic approximations for these semantic side conditions in order to achieve a type system for a concrete language for Boolean and arithmetic expressions. Obtaining a soundness proof for such a concrete type system then boils down to proving that the concrete type system interprets the abstract type system.

We prove the soundness of the abstract type system by simply applying the compositionality results proven before.

theory Type-System
imports Language-Composition
begin
locale Type-System =
  SSP?: Strongly-Secure-Programs E BMap DA
for E :: ('exp, 'id, 'val) Evalfunction
and BMap :: 'val ⇒ bool
and DA :: ('id, 'd::order) DomainAssignment
+
fixes
AssignSideCondition :: 'id ⇒ 'exp ⇒ bool
and WhileSideCondition :: 'exp ⇒ bool
and IfSideCondition ::
  'exp ⇒ ('exp,'id) MWLfCom ⇒ ('exp,'id) MWLfCom ⇒ bool
assumes semAssignSC: AssignSideCondition x e =⇒ e ≡ DA x e
and semWhileSC: WhileSideCondition e =⇒ ∀ d. e ≡_d e
and semIfSC: IfSideCondition e c1 c2 =⇒ ∀ d. e ≡_d e ∨ [c1] ≈_d [c2]
begin
— Security typing rules for the language commands
inductive
ComSecTyping :: ('exp, 'id) MWLfCom ⇒ bool
(⌜⌜ C ⌝⌟)
and ComSecTypingL :: ('exp,'id) MWLfCom list ⇒ bool
(⌜⌜ V ⌝⌟)
where
skip: ⌜⌜ C ⌝⌟ skip |
Assign: ⌜⌜ AssignSideCondition x e ⌝⌟ =⇒ ⌜⌜ C x := e ⌝⌟ |
Fork: ⌜⌜ C c; ⌜⌜ V ⌝⌟ =⇒ ⌜⌜ C fork c V ⌝⌟ |
Seq: ⌜⌜ C c1; ⌜⌜ C c2 ⌝⌟ =⇒ ⌜⌜ C c1;c2 ⌝⌟ |
While: ⌜⌜ C c; ⌜⌜ WhileSideCondition b ⌝⌟
\[ \Rightarrow \vdash_C \text{while } b \text{ do } c \text{ od} \mid \\
\text{If: } [ \vdash_C c_1; \vdash_C c_2; \text{IfSideCondition } b \ c_1 \ c_2 ] \Rightarrow \vdash_C \text{if } b \ \text{then } c_1 \ \text{else } c_2 \ \text{fi} \mid \\
\text{Parallel: } [ \forall i < \text{length } V. \ \vdash_C V!i ] \Rightarrow \vdash_Y \ V \]

\textbf{inductive-cases parallel-cases:}
\[ \vdash_Y \ V \]

— soundness proof of abstract type system

\textbf{theorem} \textit{ComSecTyping-single-is-sound:}
\[ \vdash_C e \Rightarrow \text{Strongly-Secure } [e] \]
(\textit{proof})

\textbf{theorem} \textit{ComSecTyping-list-is-sound:}
\[ \vdash_Y \ V \Rightarrow \text{Strongly-Secure } V \]
(\textit{proof})

end

end

\section*{4.2 Example language for Boolean and arithmetic expressions}

As an example, we provide a simple example language for instantiating the parameter \texttt{'exp} for the language for Boolean and arithmetic expressions.

\textbf{theory} \textit{Expr}  \\
\textbf{imports} Types  \\
\textbf{begin}

— type parameters:  \\
— \texttt{'val}: numbers, boolean constants....  \\
— \texttt{'id}: identifier names

\textbf{type-synonym} \texttt{('val) operation} = \texttt{'val list \Rightarrow 'val}

\textbf{datatype} (dead \texttt{'id}, dead \texttt{'val}) \textit{Expr} =  \\
\texttt{Const \texttt{'val} |}  \\
\texttt{Var \texttt{'id} |}  \\
\texttt{Op \texttt{'val operation} ((\texttt{'id}, \texttt{'val}) \textit{Expr} \texttt{) list}}

— defining a simple recursive evaluation function on this datatype

\textbf{primrec} \textit{ExprEval} :: ((\texttt{'id}, \texttt{'val}) \textit{Expr}, \texttt{'id}, \texttt{'val}) \textit{Evalfunction}  \\
\textbf{and} \textit{ExprEvalL} :: ((\texttt{'id}, \texttt{'val}) \textit{Expr} \texttt{list} \Rightarrow (\texttt{'id}, \texttt{'val}) \textit{State} \Rightarrow \texttt{'val list}  \\
\textbf{where}  \\
\textit{ExprEval} (\texttt{Const } v) \ m = v |
ExprEval (Var x) m = (m x) |
ExprEval (Op f arglist) m = (f (ExprEvalL arglist m)) |

ExprEvalL [] m = [] |
ExprEvalL (e#V) m = (ExprEval e m)#(ExprEvalL V m)

end

4.3 Example interpretation of abstract security type system

Using the example instantiation of the language for Boolean and arithmetic expressions, we give an example instantiation of our abstract security type system, instantiating the parameter for domains 'd with a two-level security lattice.

theory Domain-example
imports Expr
begin

— When interpreting, we have to instantiate the type for domains. As an example, we take a type containing 'low' and 'high' as domains.

datatype Dom = low | high

instantiation Dom :: order
begin

definition less-eq-Dom-def: d1 ≤ d2 = (if d1 = d2 then True else (if d1 = low then True else False))

definition less-Dom-def: d1 < d2 = (if d1 = d2 then False else (if d1 = low then True else False))

instance ⟨proof⟩

end

end

theory Type-System-example
imports Type-System Expr Domain-example
begin

— When interpreting, we have to instantiate the type for domains.
— As an example, we take a type containing 'low' and 'high' as domains.
consts DA :: (′id,Dom) DomainAssignment
consts BMap :: ′val ⇒ bool

abbreviation d-indistinguishable :: (′id,′val) Expr ⇒ Dom
⇒ (′id,′val) Expr ⇒ bool
where
e1 ≡ d e2
≡ Strongly-Secure-Programs.d-indistinguishable ExprEval DA d e1 e2

abbreviation relatedbyUSD′ :: ((′id,′val) Expr, ′id) MWLfCom list
⇒ Dom ⇒ ((′id,′val) Expr, ′id) MWLfCom list ⇒ bool (infixr ≈ 65)
where V ≈ d V′ ≡ (V,V′) ∈ Strong-Security.USD (MWLf-semantics.MWLfSteps-det ExprEval BMap) DA d

— Security typing rules for expressions - will be part of a side condition
inductive
ExprSecTyping :: (′id, ′val) Expr ⇒ Dom set ⇒ bool
(⊢ E - : )
where
Consts: ⊢ E (Const v) : {d} |
Vars: ∀ i < length arglist. ⊢ E (Var x) : (dl!i)
⇒ ⊢ E (Op f arglist) : (∪ {d. (∃ i < length arglist. d = (dl!i))})

definition synAssignSC :: ′id ⇒ (′id, ′val) Expr ⇒ bool
where
synAssignSC x e ≡ ∃ D. (⊢ E e : D ∧ (∀ d ∈ D. (d ≤ DA x)))

definition synWhileSC :: (′id, ′val) Expr ⇒ bool
where
synWhileSC e ≡ ∃ D. (⊢ E e : D ∧ (∀ d ∈ D. ∀ d′. d ≤ d′))

definition synIfSC :: (′id, ′val) Expr ⇒ (((′id, ′val) Expr, ′id) MWLfCom ⇒ Dom ⇒ ((′id, ′val) Expr, ′id) MWLfCom ⇒ bool
where
synIfSC e c1 c2 ≡
∀ d. (∼ (e ≡_d e) → [c1] ≡_d [c2])

lemma ExprTypable-with-smallerD-implies-d-indistinguishable:
∥ ⊢ E e : D; ∀ d′ ∈ D′. d′ ≤ d ∥ → e ≡_d e
(proof)

interpretation Type-System-example: Type-System ExprEval BMap DA
synAssignSC synWhileSC synIfSC
(proof)

end
References
