D31.1

Formal Specification of a Generic Separation Kernel

<table>
<thead>
<tr>
<th>Project number:</th>
<th>318353</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project acronym:</td>
<td>EURO-MILS</td>
</tr>
<tr>
<td>Project title:</td>
<td>EURO-MILS: Secure European Virtualisation for Trustworthy Applications in Critical Domains</td>
</tr>
<tr>
<td>Start date of the project:</td>
<td>1st October, 2012</td>
</tr>
<tr>
<td>Duration:</td>
<td>36 months</td>
</tr>
<tr>
<td>Programme:</td>
<td>FP7/2007-2013</td>
</tr>
<tr>
<td>Deliverable type:</td>
<td>R</td>
</tr>
<tr>
<td>Deliverable reference number:</td>
<td>ICT-318353 / D31.1 / 0.0</td>
</tr>
<tr>
<td>Activity and Work package contributing to deliverable:</td>
<td>Activity 3 / WP 3.1</td>
</tr>
<tr>
<td>Due date:</td>
<td>September 2013 – M12</td>
</tr>
<tr>
<td>Actual submission date:</td>
<td>13th September, 2023</td>
</tr>
<tr>
<td>Responsible organisation:</td>
<td>Open University of The Netherlands</td>
</tr>
<tr>
<td>Editors:</td>
<td>Freek Verbeek, Julien Schmaltz</td>
</tr>
<tr>
<td>Dissemination level:</td>
<td>PU</td>
</tr>
<tr>
<td>Revision:</td>
<td>0.0 (r-2)</td>
</tr>
</tbody>
</table>

Abstract:

We introduce a theory of intransitive non-interference for separation kernels with control. We show that it can be instantiated for a simple API consisting of IPC and events.

Keywords: separation kernel with control, formal model, instantiation, IPC, events, Isabelle/HOL
Editors
Freek Verbeek, Julien Schmaltz (Open University of The Netherlands)

Contributors (ordered according to beneficiary numbers)
Sergey Tverdyshev, Oto Havle, Holger Blasum (SYSGO AG)
Bruno Langenstein, Werner Stephan (Deutsches Forschungszentrum für künstliche Intelligenz / DFKI GmbH)
Abderrahmane Feliachi, Yakoub Nemouchi, Burkhart Wolff (Université Paris Sud)
Freek Verbeek, Julien Schmaltz (Open University of The Netherlands)

Acknowledgment
The research leading to these results has received funding from the European Union’s Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 318353.
Executive Summary

Intransitive noninterference has been a widely studied topic in the last few decades. Several well-established methodologies apply interactive theorem proving to formulate a noninterference theorem over abstract academic models. In joint work with several industrial and academic partners throughout Europe, we are helping in the certification process of PikeOS, an industrial separation kernel developed at SYSGO. In this process, established theories could not be applied. We present a new generic model of separation kernels and a new theory of intransitive noninterference. The model is rich in detail, making it suitable for formal verification of realistic and industrial systems such as PikeOS. Using a refinement-based theorem proving approach, we ensure that proofs remain manageable.

This document corresponds to the deliverable D31.1 of the EURO-MILS Project http://www.euromils.eu.
## Contents

1. Introduction 2

2. Preliminaries 3
   2.1 Binders for the option type 3
   2.2 Theorems on lists 4

3. A generic model for separation kernels 5
   3.1 \(K\) (Kernel) 6
      3.1.1 Execution semantics 7
   3.2 \(SK\) (Separation Kernel) 8
      3.2.1 Security for non-interfering domains 9
      3.2.2 Security for indirectly interfering domains 11
   3.3 \(ISK\) (Interruptible Separation Kernel) 14
   3.4 \(CISK\) (Controlled Interruptible Separation Kernel) 17
      3.4.1 Execution semantics 19
      3.4.2 Formulations of security 19
      3.4.3 Proofs 20

4. Instantiation by a separation kernel with concrete actions 21
   4.1 Model of a separation kernel configuration 22
      4.1.1 Type definitions 22
      4.1.2 Configuration 22
   4.2 Formulation of a subject-subject communication policy and an information flow policy, and showing both can be derived from subject-object configuration data 23
      4.2.1 Specification 23
      4.2.2 Derivation 23
   4.3 Separation kernel state and atomic step function 24
      4.3.1 Interrupt points 24
      4.3.2 System state 25
      4.3.3 Atomic step 25
   4.4 Preconditions and invariants for the atomic step 27
      4.4.1 Atomic steps of \(SK_{IPC}\) preserve invariants 28
      4.4.2 Summary theorems on atomic step invariants 28
   4.5 The view-partitioning equivalence relation 29
      4.5.1 Elementary properties 30
   4.6 Atomic step locally respects the information flow policy 30
      4.6.1 Locally respects of atomic step functions 30
      4.6.2 Summary theorems on view-partitioning locally respects 31
   4.7 Weak step consistency 31
      4.7.1 Weak step consistency of auxiliary functions 31
      4.7.2 Weak step consistency of atomic step functions 32
      4.7.3 Summary theorems on view-partitioning weak step consistency 33
   4.8 Separation kernel model 33
      4.8.1 Initial state of separation kernel model 33
      4.8.2 Types for instantiation of the generic model 34
      4.8.3 Possible action sequences 35
      4.8.4 Control 35
      4.8.5 Discharging the proof obligations 36
4.9 Link implementation to CISK: the specific separation kernel is an interpretation of the generic model. ................................................................. 40

5 Related Work ............................................................................. 41

6 Conclusion .................................................................................. 42
   6.0.1 Acknowledgement. ................................................................. 42
1 Introduction

Separation kernels are at the heart of many modern security-critical systems [23]. With next generation technology in cars, aircrafts and medical devices becoming more and more interconnected, a platform that offers secure decomposition of embedded systems becomes crucial for safe and secure performance. PikeOS, a separation kernel developed at SYSGO, is an operating system providing such an environment [12, 2]. A consortium of several European partners from industry and academia works on the certification of PikeOS up to at least Common Criteria EAL5+, with "+" being applying formal methods compliant to EAL7. Our aim is to derive a precise model of PikeOS and a precise formulation of the PikeOS security policy.

A crucial security property of separation kernels is intransitive noninterference. This property is typically required for systems with multiple independent levels of security (MILS) such as PikeOS. It ensures that a given security policy over different subjects of the system is obeyed. Such a security policy dictates which subjects may flow information to which other subjects.

Intransitive noninterference has been an active research field for the last three decades. Several papers have been published on defining intransitive noninterference and on unwinding methodologies that enable the proof of intransitive noninterference from local proof obligations. However, in the certification process of PikeOS these existing methodologies could not be directly applied. Generally, the methodologies are based on highly abstract generic models of computation. The gap between such an abstract model and the reality of PikeOS is large, making application of the methodologies tedious and cumbersome.

This paper presents a new generic model for separation kernels called CISK (for: Controlled Interruptible Separation Kernel). This model is richer in details and contains several facets present in many separation kernels, such as interrupts, context switches between domains and a notion of control. Regarding the latter, this concerns the fact that the kernel exercises control over the executions as performed by the domains. The kernel can, e.g., decide to skip actions of the domains, or abort them halfway. We prove that any instantiation of the model provides intransitive noninterference. The model and proofs have been formalized in Isabelle/HOL [21] which are included in the subsequent sections of this document.

We have adopted Rushby’s definition of intransitive noninterference [24]. We first present an overview of our approach and then discuss the relation between our approach and existing methodologies in the next section.

Overview

Generally, there are two conflicting interests when using a generic model. On the one hand the model must be sufficiently abstract to ensure that theorems and proofs remain manageable. On the other hand, the model must be rich enough and must contain sufficient domain-knowledge to allow easy instantiation. Rushby’s model, for example, is on one end of the spectrum: it is basically a Mealy machine, which is a highly abstract notion of computation, consisting only of state, inputs and outputs [24]. The model and its proofs are manageable, but making a realistic instantiation is tedious and requires complicated proofs.

We aim at the other side of the spectrum by having a generic model that is rich in detail. As a result, instantiating the model with, e.g., a model of PikeOS can be done easily. To ensure maintainability of the theorems and proofs, we have applied a highly modularized theorem proving technique.

Figure 1 shows an overview. The initial module “Kernel” is close to a Mealy machine, but has several facets added, including interrupts, context switches and control. New modules are added in such a way that each new module basically inserts an adjective before “Kernel”. The use of modules allows us to prove, e.g., a separation theorem in module “Separation Kernel” and subsequently to reuse this theorem later on when details on control or interrupts are added.

The second module adds a notion of separation, yielding a module of a Separation Kernel (SK). A security policy is added that dictates which domains may flow information to each other. Local proof
In the third module calls to the kernel are no longer considered atomic, yielding an Interruptible Separation Kernel (ISK). In this model, one call to the kernel is represented by an action sequence. Consider, for example, an IPC call (for: Inter Process Communication). From the point of view of the programmer this is one kernel call. From the point of view of the kernel it is an action sequence consisting of three stages IPC_PREP, IPC_WAIT, and IPC_SEND. During the PREP stage, it is checked whether the IPC is allowed by the security policy. The WAIT stage is entered if a thread needs to wait for its communication partner. The SEND stage is data transmission. After each stage, an interrupt may occur that switches the current context. A consequence of allowing interruptible action sequences is that it is no longer the case that any execution, i.e., any combination of atomic kernel actions, is realistic. We formulate a definition of realistic execution and weaken the proof obligations of the model to apply only to realistic executions.

The final module provides an interpretation of control that allows atomic kernel actions to be aborted or delayed. Additional proof obligations are required to ensure that noninterference is still provided. This yields a Controlled Interruptible Separation Kernel (CISK). When sequences of kernel actions are aborted, error codes can be transmitted to other domains. Revisiting our IPC example, after the PREP stage the kernel can decide to abort the action. The IPC action sequence will not be continued and error codes may be sent out. At the WAIT stage, the kernel can delay the action sequence until the communication partner of the IPC call is ready to receive.

In Section 3 we introduce a theory of intransitive non-interference for separation kernels with control, based on [31]. We show that it can be instantiated for a simple API consisting of IPC and events (Section 4). The rest of this section gives some auxiliary theories used for Section 3.

## 2 Preliminaries

### 2.1 Binders for the option type

```isar
theory Option-Binders
imports Main
begin

The following functions are used as binders in the theorems that are proven. At all times, when a
result is None, the theorem becomes vacuously true. The expression \( m \rightarrow \alpha \) means “First compute \( m \), if it is None then return True, otherwise pass the result to \( \alpha \).” B2 is a short hand for sequentially doing two independent computations. The following syntax is associated to B2: “\( m_1||m_2 \rightarrow \alpha \)” represents “First compute \( m_1 \) and \( m_2 \), if one of them is None then return True, otherwise pass the result to \( \alpha \).”

```plaintext
definition B :: 'a option ⇒ ('a ⇒ bool) ⇒ bool (infixl → 65)
where B m α ≡ case m of None ⇒ True | (Some a) ⇒ α a

definition B2 :: 'a option ⇒ 'a option ⇒ ('a ⇒ 'a ⇒ bool) ⇒ bool
where B2 m1 m2 α ≡ m1 → (λ a . m2) ⇒ (λ b . α a b))
syntax B2 :: ['a option, 'a option, ('a ⇒ 'a ⇒ bool)] ⇒ bool ((- - -) [0, 0, 10] 10)
```

Some rewriting rules for the binders

```plaintext
lemma rewrite-B2-to-cases[simp]:
  shows B2 s t f = (case s of None ⇒ True | (Some s1) ⇒ (case t of None ⇒ True | (Some t1) ⇒ f s1 t1))
  (proof)
lemma rewrite-B-None[simp]:
  shows None ⇒ α = True
  (proof)
lemma rewrite-B-m-True[simp]:
  shows m ⇒ (λ a . True) = True
  (proof)
lemma rewrite-B2-cases:
  shows (case a of None ⇒ True | (Some s) ⇒ (case b of None ⇒ True | (Some t) ⇒ f s t))
  = (∀ s t . a = (Some s) ∧ b = (Some t) → f s t)
  (proof)

definition strict-equal :: 'a option ⇒ 'a ⇒ bool
where strict-equal m a ≡ case m of None ⇒ False | (Some a’) ⇒ a’ = a
end
```

2.2 Theorems on lists

```plaintext
theory List-Theorems
imports Main
begin

definition lastn :: nat ⇒ 'a list ⇒ 'a list
where lastn n x = drop ((length x) - n) x

definition is-sub-seq :: 'a ⇒ 'a ⇒ 'a list ⇒ bool
where is-sub-seq a b x ≡ ∃ n . Suc n < length x ∧ x!n = a ∧ x!(Suc n) = b

definition prefixes :: 'a list set ⇒ 'a list set
where prefixes s ≡ { x . ∃ n y . n > 0 ∧ y ∈ s ∧ take n y = x }
```

```plaintext
lemma drop-one[simp]:
  shows drop (Suc 0) x = tl x (proof)
lemma length-ge-one:
  shows x ≠ [] ⇒ length x ≥ 1 (proof)
lemma take-but-one[simp]:
  shows x ≠ [] ⇒ lastn ((length x) - 1) x = tl x (proof)
lemma Suc-m-minus-n[simp]:
  shows m ≥ n ⇒ Suc m - n = Suc (m - n) (proof)
lemma lastn-one-less:
```
shows $n > 0 \land n \leq \text{length } x \land \text{last } n \ x = (a\#y) \rightarrow \text{last } n - 1 \ x = y \ (\text{proof})$

**lemma list-sub-implies-member:**
shows $\forall \ a \ . \ \text{set } (a\#x) \subseteq Z \rightarrow a \in Z \ (\text{proof})$

**lemma subset-smaller-list:**
shows $\forall \ a \ . \ \text{set } (a\#x) \subseteq Z \rightarrow \text{set } x \subseteq Z \ (\text{proof})$

**lemma second-elt-is-hd-tl:**
shows $\text{tl } x = (a \# x') \rightarrow a = x!1 \ (\text{proof})$

**lemma length-ge-2-implies-tl-not-empty:**
shows $\text{length } x \geq 2 \rightarrow \text{tl } x \neq [] \ (\text{proof})$

**lemma length-Lt-2-implies-tl-empty:**
shows $\text{length } x < 2 \rightarrow \text{tl } x = [] \ (\text{proof})$

**lemma first-second-is-sub-seq:**
shows $\text{length } x \geq 2 \Rightarrow \text{is-sub-seq } (\text{hd } x) (x!1) \ x$ 

**lemma hd-drop-is-nth:**
shows $\text{drop } n \ x = [] \rightarrow n < \text{length } x \ (\text{proof})$

**lemma def-of-hd:**
shows $y = a \# x \rightarrow \text{hd } y = a \ (\text{proof})$

**lemma def-of-tl:**
shows $y = a \# x \rightarrow \text{tl } y = x \ (\text{proof})$

**lemma drop-yields-results-implies-nbound:**
shows $\text{drop } n \ x \neq [] \rightarrow n < \text{length } x \ (\text{proof})$

**lemma consecutive-is-sub-seq:**
shows $a \# (b \# x) = \text{last } n \ y \Rightarrow \text{is-sub-seq } a \ b \ y \ (\text{proof})$

**lemma sub-seq-in-prefixes:**
assumes $\exists y \in \text{prefixes } X. \ \text{is-sub-seq } a \ a' \ y$
shows $\exists y \in X. \ \text{is-sub-seq } a \ a' \ y \ (\text{proof})$

**lemma set-tl-is-subset:**
shows $\text{set } (\text{tl } x) \subseteq \text{set } x \ (\text{proof})$

**lemma x-is-hd-snd-tl:**
shows $\text{length } x \geq 2 \rightarrow x = (\text{hd } x) \# x!1 \# \text{tl } (\text{tl } x) \ (\text{proof})$

**lemma tl-x-not-x:**
shows $x \neq [] \rightarrow \text{tl } x \neq x \ (\text{proof})$

**lemma tl-hd-x-not-tl-x:**
shows $x \neq [] \land \text{hd } x \neq [] \rightarrow \text{tl } (\text{hd } x) \# \text{tl } x \neq x \ (\text{proof})$

end

3 A generic model for separation kernels

theory $K$
imports List-Theorems Option-Binders
begin
This section defines a detailed generic model of separation kernels called CISK (Controlled Interruptible Separation Kernel). It contains a generic functional model of the behaviour of a separation kernel as a transition system, definitions of the security property and proofs that the functional model satisfies security properties. It is based on Rushby’s approach [25] for noninterference. For an explanation of the model, its structure and an overview of the proofs, we refer to the document entitled “A New Theory of Intransitive Noninterference for Separation Kernels with Control” [31].

The structure of the model is based on locales and refinement:

- locale “Kernel” defines a highly generic model for a kernel, with execution semantics. It defines a state transition system with some extensions to the one used in [25]. The transition system defined here stores the currently active domain in the state, and has transitions for explicit context switches and interrupts and provides a notion of control. As each operation of the system will be split into atomic actions in our model, only certain sequences of actions will correspond to a run on a real system. Therefore, the function \( \text{run} \), which applies an execution on a state and computes the resulting new state, is partial and defined for realistic traces only. Later, but not in this locale, we will define a predicate to distinguish realistic traces from other traces. Security properties are also not part of this locale, but will be introduced in the locales to be described next.

- locale “Separation_Kernel” extends “Kernel” with constraints concerning non-interference. The theorem is only sensible for realistic traces; for unrealistic traces it will hold vacuously.

- locale “Interruptible_Separation_Kernel” refines “Separation_Kernel” with interruptible action sequences. It defines function “realistic_trace” based on these action sequences. Therefore, we can formulate a total run function.

- locale “Controlled_Interruptible_Separation_Kernel” refines “Interruptible_Separation_Kernel” with abortable action sequences. It refines function “control” which now uses a generic predicate “aborting” and a generic function “set_error_code” to manage aborting of action sequences.

3.1 K (Kernel)

The model makes use of the following types:

- state_t A state contains information about the resources of the system, as well as which domain is currently active. We decided that a state does not need to include a program stack, as in this model the actions that are executed are modelled separately.

- dom_t A domain is an entity executing actions and making calls to the kernel. This type represents the names of all domains. Later on, we define security policies in terms of domains.

- action_t Actions of type ’action_t represent atomic instructions that are executed by the kernel. As kernel actions are assumed to be atomic, we assume that after each kernel action an interrupt point can occur.

- action_t_execution An execution of some domain is the code or the program that is executed by the domain. One call from a domain to the kernel will typically trigger a succession of one or more kernel actions. Therefore, an execution is represented as a list of sequences of kernel actions. Non-kernel actions are not taken into account.

- output_t Given the current state and an action an output can be computed deterministically.

- time_t Time is modelled using natural numbers. Each atomic kernel action can be executed within one time unit.
3.1.1 Execution semantics

Short-hand notations for using function control.

Abbreviation thread-empty :: 'action-t execution ⇒ bool

Where thread-empty exec ≡ exec = [] ∨ exec = [[]]

Wrappers for function kstep and kprecondition that deal with the case where the given action is None.

Definition step where step s oa ≡ case ao of None ⇒ s | (Some a) ⇒ kstep s a
Definition precondition :: 'state-t ⇒ 'action-t option ⇒ bool
Where precondition s a ≡ a → kprecondition s
Definition involved
Where involved ao ≡ case ao of None ⇒ {} | (Some a) ⇒ kinvolved a
Execution semantics are defined as follows: a run consists of consecutively running sequences of actions. These sequences are interruptable. Run first checks whether an interrupt occurs. When this happens, function cswitch may switch the context. Otherwise, function control is used to determine the next action \( a \), which also yields a new state \( s' \). Action \( a \) is executed by executing \((\text{step } s') \) \( a \). The current execution of the current domain is updated.

Note that run is a partial function, i.e., it computes results only when at all times the preconditions hold. Such runs are the realistic ones. For other runs, we do not need to – and cannot – prove security. All the theorems are formulated in such a way that they hold vacuously for unrealistic runs.

\[
\text{function} \quad \text{run} : \text{time-t} \Rightarrow \text{\textquotesingle \textit{state-t}} \Rightarrow (\text{\textquotesingle \textit{dom-t}} \Rightarrow \text{\textquotesingle \textit{action-t}} \Rightarrow \text{\textquotesingle \textit{exec-t}}) \Rightarrow \text{\textquotesingle \textit{state-t}} \Rightarrow \text{\textquotesingle \textit{exec-t}}
\]

\[
\text{where} \quad \text{run } 0 \text{ s execs} = s
\]

\[
\text{interrupt } (\text{Suc n}) \Rightarrow \text{run } \text{Suc n} \text{ Some s execs} = \text{run } n \text{ Some (cswitch (Suc n) s)} \text{ execs}
\]

\[
\text{\neg interrupt } (\text{Suc n}) \Rightarrow \text{\textquotesingle \textit{thread-empty}(execs (current s))} \Rightarrow \text{run } \text{Suc n} \text{ Some s execs} = \text{run } n \text{ Some s execs}
\]

\[
\text{\neg interrupt } (\text{Suc n}) \Rightarrow \text{\textquotesingle \textit{thread-empty}(execs (current s))} \Rightarrow \text{next-condition (next-state s execs) (next-action s execs)} \Rightarrow \text{run } \text{Suc n} \text{ Some s execs} = \text{None}
\]

\[
\text{\neg interrupt } (\text{Suc n}) \Rightarrow \text{\textquotesingle \textit{thread-empty}(execs (current s))} \Rightarrow \text{\textquotesingle \textit{precondition (next-state s execs) (next-action s execs)}} \Rightarrow \text{run } \text{Suc n} \text{ Some s execs} = \text{None}
\]

\[
\text{run } \text{Suc n} \text{ Some s execs} = \text{run } n \text{ Some (step (next-state s execs) (next-action s execs))) (next-execs s execs)}
\]

\[
\text{proof}
\]

\[
\text{termination} \quad \text{proof}
\]

end

3.2 SK (Separation Kernel)

theory SK
  imports K
begin

Locale Kernel is now refined to a generic model of a separation kernel. The security policy is represented using function \( ia \). Function \( vpeq \) is adopted from Rushby and is an equivalence relation representing whether two states are equivalent from the point of view of the given domain.

We assume constraints similar to Rushby, i.e., weak step consistency, locally respects, and output consistency. Additional assumptions are:

**Step Atomicity** Each atomic kernel step can be executed within one time slot. Therefore, the domain that is currently active does not change by executing one action.

**Time-based Interrupts** As interrupts occur according to a prefixed time-based schedule, the domain that is active after a call of switch depends on the currently active domain only (cswitch_consistency). Also, cswitch can only change which domain is currently active (cswitch_consistency).

**Control Consistency** States that are equivalent yield the same control. That is, the next action and the updated execution depend on the currently active domain only (next_action_consistent, next_execs_consistent), the state as updated by the control function remains in vpeq (next_state_consistent, locally_respects_next_state). Finally, function control cannot change which domain is active (current_next_state).

definition actions-in-execution: \( \text{\textquotesingle \textit{action-t}} \text{ execution} \Rightarrow \text{\textquotesingle \textit{action-t}} \text{ set} \)

where actions-in-execution exec \( \equiv \{ \ a . \ \exists \ aseq \in \text{set exec} . \ a \in \text{set aseq} \} \)
locale Separation-Kernel = Kernel kstep output-f s0 current cswitch interrupt kprecondition realistic-execution control kinvolved

for kstep :: 'state-t =⇒ 'action-t =⇒ 'state-t
and output-f :: 'state-t =⇒ 'action-t =⇒ 'output-t
and s0 :: 'state-t
and current :: 'state-t =⇒ 'dom-t — Returns the currently active domain
and cswitch :: 'time-t =⇒ 'state-t =⇒ 'state-t — Switches the current domain
and interrupt :: 'time-t =⇒ bool — Returns true if an interrupt occurs in the given state at the given time
and kprecondition :: 'state-t =⇒ 'action-t =⇒ bool — Returns true if an precondition holds that relates the current action to the state
and realistic-execution :: 'action-t-execution =⇒ bool — In this locale, this function is completely unconstrained.
and control :: 'state-t =⇒ 'dom-t — Switches the current domain
and kinvolved :: 'action-t =⇒ 'dom-t set
+
fixes ifp :: 'dom-t =⇒ 'dom-t =⇒ bool
and vpeq :: 'dom-t =⇒ 'state-t =⇒ bool
assumes vpeq-transitive: ∀ a b c. (vpeq u a b ∧ vpeq u b c) =⇒ vpeq u a c
and vpeq-symmetric: ∀ a b u. vpeq u a b =⇒ vpeq u b a
and vpeq-reflexive: ∀ a u. vpeq u a a
and ifp-reflexive: ∀ u . ifp u u
and weakly-step-consistent: ∀ s t u a . vpeq u s t ∧ vpeq (current s) s t ∧ kprecondition s a ∧ kprecondition t a ∧ current s = current t =⇒ vpeq u (kstep s a) (kstep t a)
and locally-respects: ∀ a s u. ¬ifp (current s) u ∧ kprecondition s a =⇒ vpeq u s (kstep s a)
and output-consistent: ∀ a s t . vpeq (current s) s t ∧ current s = current t =⇒ (output-f s a) = (output-f t a)
and step-atomicity: ∀ s a . current (kstep s a) = current s
and cswitch-independent-of-state: ∀ n s t . current s = current t =⇒ current (cswitch n s) = current (cswitch n t)
and cswitch-consistency: ∀ u s t n . vpeq u s t =⇒ vpeq u (cswitch n s) (cswitch n t)
and next-action-consistent: ∀ s t execs . vpeq (current s) s t ∧ (∀ d ∈ involved (next-action s execs) . vpeq d s t) ∧ current s = current t =⇒ next-action s execs = next-action t execs
and next-actions-consistent: ∀ s t execs . vpeq (current s) s t ∧ (∀ d ∈ involved (next-action s execs) . vpeq d s t) ∧ current s = current t =⇒ next-execs s execs (snd (control t (current s) (execs (current s)))) = fst (snd (control t (current s) (execs (current s))))
and next-state-consistent: ∀ s t u execs . vpeq (current s) s t ∧ vpeq u s t ∧ current s = current t =⇒ vpeq u (next-state s execs) (next-state t execs)
and current-next-state: ∀ s execs . current (next-state s execs) = current s
and locally-respects-next-state: ∀ s u execs. ¬ifp (current s) u =⇒ vpeq u s (next-state s execs)
and involved-ifp: ∀ s a . ∀ d ∈ involved (a) . kprecondition s (the a) =⇒ ifp d (current s)
and next-action-from-exec: ∀ s execs . next-action s execs = (λ a . a ∈ actions-in-execution (execs (current s)))
and next-exec-set: ∀ s execs u . actions-in-execution (next-execs s execs u) ⊆ actions-in-execution (execs u)

begin

Note that there are no proof obligations on function “interrupt”. Its typing enforces the assumptions that switching is based on time and not on state. This assumption is sufficient for these proofs, i.e., no further assumptions are required.

3.2.1 Security for non-interfering domains

We define security for domains that are completely non-interfering. That is, for all domains \(u\) and \(v\) such that \(v\) may not interfere in any way with domain \(u\), we prove that the behavior of domain \(u\) is independent of the actions performed by \(v\). In other words, the output of domain \(u\) in some run is at all times equivalent to the output of domain \(u\) when the actions of domain \(v\) are replaced by some other set actions.

A domain is unrelated to \(u\) if and only if the security policy dictates that there is no path from the domain to \(u\).
To formulate the new theorem to prove, we redefine purging: all domains that may not influence domain \( u \) are replaced by arbitrary action sequences.

**Definition**

**purge**

\( 'dom-t \Rightarrow 'action-t execution \) \( \Rightarrow 'dom-t \Rightarrow ( 'dom-t \Rightarrow 'action-t execution) \)

**Where**

\( \text{purge execs } u \equiv \lambda d . (\text{if unrelated } d u \text{ then} \\
(\text{SOME alpha . realistic-execution alpha} \\
\text{else execs } d) \)

A normal run from initial state \( s0 \) ending in state \( s_f \) is equivalent to a run purged for domain \( \text{currents}_f \).

**Definition**

**NI-unrelated**

\( \equiv \forall \text{execs } a n . \text{run } n (\text{Some } s0) \text{execs} \rightarrow \\
(\lambda s-f . \text{run } n (\text{Some } s0) (\text{purge execs } \text{current } s-f)) \rightarrow \\
(\lambda s-f2 . \text{output-f } s-f a = \text{output-f } s-f2 a \land \text{current } s-f = \text{current } s-f2) \)

The following properties are proven inductive over states \( s \) and \( t \):

1. Invariably, states \( s \) and \( t \) are equivalent for any domain \( v \) that may influence the purged domain \( u \). This is more general than proving that “\( \text{vpeq } u s t \)” is inductive. The reason we need to prove equivalence over all domains \( v \) is so that we can use weak step consistency.

2. Invariably, states \( s \) and \( t \) have the same active domain.

**Abbreviation**

**equivalent-states** :: 'state-t option \( \Rightarrow 'state-t option \Rightarrow 'dom-t \Rightarrow bool \)

**Where**

\( \equiv \forall \text{execs } ms mt m u . \text{equivalent-states } ms mt u \rightarrow \\
(\text{run } n \text{execs } || \\
\text{run } n \text{mt } (\text{purge execs } u) \rightarrow \\
(\lambda rs rt . \text{vpeq } u rs rt \land \text{current } rs = \text{current } rt)) \)

We formulate a version of predicate view_partitioned that is on one hand more general, but on the other hand easier to prove inductive over function run. Instead of reasoning over execs and (purge execs u), we reason over any two executions execs1 and execs2 for which the following relation holds:

**Definition**

**purged-relation** :: 'dom-t \( \Rightarrow ( 'dom-t \Rightarrow 'action-t execution) \) \( \Rightarrow ( 'dom-t \Rightarrow 'action-t execution) \Rightarrow bool \)

**Where**

\( \text{purged-relation } u \text{execs1 execs2 } \equiv \forall d . \text{ifp}^{**} d u \rightarrow \text{execs1 } d = \text{execs2 } d \)

The inductive version of view partitioning is redefined. Two states that are initially \( u \)-equivalent are \( u \)-equivalent after performing respectively a realistic run and a realistic purged run.

**Definition**

**view-partitioned**:bool

**Where**

\( \equiv \forall \text{execs } ms mt n u . \text{equivalent-states } ms mt u \rightarrow \\
(\text{run } n \text{ms execs } || \\
\text{run } n \text{mt } (\text{purge execs } u) \rightarrow \\
(\lambda rs rt . \text{vpeq } u rs rt \land \text{current } rs = \text{current } rt)) \)

A proof that when state \( t \) performs a step but state \( s \) not, the states remain equivalent for any domain \( v \) that may interfere with \( u \).

**Lemma**

**vpeq-s-nt**

**Assumes**

\( \text{prec-t : precondition } (\text{next-state } t \text{execs2 } ) (\text{next-action } t \text{execs2}) \)

**Assumes**

\( \text{not-ifp-curr-u : } \neg \text{ifp}^{**} (\text{current } t) u \)

**Assumes**

\( \text{vpeq-s-t} : \forall v . \text{ifp}^{**} v u \rightarrow \text{vpeq } v s t \)

**Shows**

\( (\forall v . \text{ifp}^{**} v u \rightarrow \text{vpeq } v s (\text{step } (\text{next-state } t \text{execs2 } ) (\text{next-action } t \text{execs2}))) ) \)
A proof that when state \( s \) performs a step but state \( t \) not, the states remain equivalent for any domain \( v \) that may interfere with \( u \).

**lemma** \( \text{vpeq-ns-t} \):

**assumes** \( \text{prec-s: precondition (next-state } s \text{ execs) (next-action } s \text{ execs)} \)

**assumes** \( \text{not-ifp-curr-u: } \neg \text{ ifp}^\text{**} (\text{current } s) \text{ u} \)

**assumes** \( \text{vpeq-s-t: } \forall v. \text{ ifp}^\text{**} v \text{ u } \rightarrow \text{vpeq } v \text{ s t} \)

**shows** \( \forall v. \text{ ifp}^\text{**} v \text{ u } \rightarrow \text{vpeq } v \text{ (step (next-state } s \text{ execs) (next-action } s \text{ execs)) } t \)

**proof**

A proof that when both states \( s \) and \( t \) perform a step, the states remain equivalent for any domain \( v \) that may interfere with \( u \). It assumes that the current domain *can* interact with \( u \) (the domain for which is purged).

**lemma** \( \text{vpeq-ns-nt-ifp-u} \):

**assumes** \( \text{vpeq-s-t: } \forall v. \text{ ifp}^\text{**} v \text{ u } \rightarrow \text{vpeq } v \text{ s t} \)

**shows** \( \text{current-s-t: current } s = \text{current } t' \)

**proof**

A proof that when both states \( s \) and \( t \) perform a step, the states remain equivalent for any domain \( v \) that may interfere with \( u \). It assumes that the current domain *cannot* interact with \( u \) (the domain for which is purged).

**lemma** \( \text{vpeq-ns-nt-not-ifp-u} \):

**assumes** \( \text{purged-a-a2: purged-relation } u \text{ execs execs2} \)

**assumes** \( \text{prec-s: precondition (next-state } s \text{ execs) (next-action } s \text{ execs)} \)

**assumes** \( \text{current-s-t: current } s = \text{current } t' \)

**shows** \( \neg \text{ifp}^\text{**} (\text{current } s) \text{ u } \rightarrow \text{vpeq } v \text{ s t'} \)

**proof**

A run with a purged list of actions appears identical to a run without purging, when starting from two states that appear identical.

**lemma** \( \text{unwinding-implies-view-partitioned-ind} \):

**shows** \( \text{view-partitioned-ind} \)

**proof**

From the previous lemma, we can prove that the system is view partitioned. The previous lemma was inductive, this lemma just instantiates the previous lemma replacing \( s \) and \( t \) by the initial state.

**lemma** \( \text{unwinding-implies-view-partitioned} \):

**shows** \( \text{view-partitioned} \)

**proof**

Domains that many not interfere with each other, do not interfere with each other.

**theorem** \( \text{unwinding-implies-NI-unrelated} \):

**shows** \( \text{NI-unrelated} \)

**proof**

### 3.2.2 Security for indirectly interfering domains

Consider the following security policy over three domains \( A, B \) and \( C \): \( A \rightsquigarrow B \rightsquigarrow C \), but \( A \not\rightsquigarrow C \). The semantics of this policy is that \( A \) may communicate with \( C \), but *only* via \( B \). No direct communication from \( A \) to \( C \) is allowed. We formalize these semantics as follows: without intermediate domain \( B \), domain \( A \) cannot flow information to \( C \). In other words, from the point of view of domain \( C \) the run
where domain $B$ is inactive must be equivalent to the run where domain $B$ is inactive and domain $A$ is replaced by an attacker. Domain $C$ must be independent of domain $A$, when domain $B$ is inactive.

The aim of this subsection is to formalize the semantics where $A$ can write to $C$ via $B$ only. We define to two ipurge functions. The first purges all domains $d$ that are intermediary for some other domain $v$. An intermediary for $u$ is defined as a domain $d$ for which there exists an information flow from some domain $v$ to $u$ via $d$, but no direct information flow from $v$ to $u$ is allowed.

**Definition** intermediary :: 'dom-t ⇒ 'dom-t ⇒ bool

where intermediary $d u ≡ \exists v . \text{ifp} = v d \land \text{ifp} d u \land \neg \text{ifp} v u \land d \neq u$

**Primrec** remove-gateway-communications :: 'dom-t ⇒ 'action-t execution ⇒ 'action-t execution

where remove-gateway-communications $u [] ≡ []$

| remove-gateway-communications $u (\text{aseq#exec}) = (\text{if } \exists a \in \text{aseq} . \exists v . \text{intermediary } v u \land v \in \text{involved} (\text{Some } a) \text{ then } [] \text{ else aseq}) \# (\text{remove-gateway-communications } u \text{ exec})$

**Definition** ipurge-l ::

('dom-t ⇒ 'action-t execution) ⇒ 'dom-t ⇒ ('dom-t ⇒ 'action-t execution) where

ipurge-l execs $u ≡ λ d . \text{if intermediary } d u \text{ then } []$

else if $d = u$ then

remove-gateway-communications $u (\text{execs } u)$

else execs $d$

The second ipurge removes both the intermediaries and the indirect sources. An indirect source for $u$ is defined as a domain that may indirectly flow information to $u$, but not directly.

**Abbreviation** ind-source :: 'dom-t ⇒ 'dom-t ⇒ bool

where ind-source $d u ≡ \text{ifp} = d u \land \neg \text{ifp} d u$

**Definition** ipurge-r ::

('dom-t ⇒ 'action-t execution) ⇒ 'dom-t ⇒ ('dom-t ⇒ 'action-t execution) where

ipurge-r execs $u ≡ λ d . \text{if intermediary } d u \text{ then } []$

else if ind-source $d u$ then

SOME alpha . realistic-execution alpha

else if $d = u$ then

remove-gateway-communications $u (\text{execs } u)$

else

execs $d$

For a system with an intransitive policy to be called secure for domain $u$ any indirect source may not flow information towards $u$ when the intermediaries are purged out. This definition of security allows the information flow $A \rightsquigarrow B \rightsquigarrow C$, but prohibits $A \rightsquigarrow C$.

**Definition** NI-indirect-sources :: bool

where NI-indirect-sources

$≡ \forall \text{ execs } a n . \text{run } n (\text{Some } s0) \text{ execs } →$

$(\lambda s-f . (\text{run } n (\text{Some } s0) (\text{ipurge-l execs } (\text{current } s-f)) \parallel$

$\text{run } n (\text{Some } s0) (\text{ipurge-r execs } (\text{current } s-f)) \rightarrow$

$(\lambda s-l s-r . \text{output-f } s-l a = \text{output-f } s-r a)))$

This definition concerns indirect sources only. It does not enforce that an unrelated domain may not flow information to $u$. This is expressed by “secure”.

This allows us to define security over intransitive policies.

**Definition** isecure :: bool

where isecure $≡ \text{NI-indirect-sources } \land \text{NI-unrelated}$

**Abbreviation** iequivalent-states :: 'state-t option ⇒ 'state-t option ⇒ 'dom-t ⇒ bool

where iequivalent-states $s t u ≡ s \parallel t → (\lambda s t . (\forall v . \text{ifp } v u \land \neg \text{intermediary } v u \rightarrow \text{vseq } v s t) \land \text{current } s =$ current $t)$
definition does-not-communicate-with-gateway
where does-not-communicate-with-gateway u execs \equiv \forall \; a . \; a \in \text{actions-in-execution} (execs u) \rightarrow (\forall \; v . \; \text{intermediary} v u \rightarrow v \notin \text{involved} (\text{Some} a))

definition iview-partitioned\::\::\text{bool}
where iview-partitioned
\equiv \forall \; \text{execs ms mt n u} . \; \text{iequivalent-states} \text{ ms mt u} \rightarrow
\left( \text{run n ms} (\text{ipurge-l execs u}) \mid \text{run n mt} (\text{ipurge-r execs u}) \right)
\leftarrow
(\lambda \; rs rt . \; \text{vpeq u rs rt} \land \text{current rs} = \text{current rt})

definition ipurged-relation\::\::\prime \; \text{dom-t} \Rightarrow \prime \; \text{dom-t} \Rightarrow \prime \; \text{action-t execution} \Rightarrow \prime \; \text{dom-t} \Rightarrow \prime \; \text{action-t execution} \Rightarrow \text{bool}
where ipurged-relation1 u execs1 execs2 \equiv \forall \; d . \; \text{ifp d u} \rightarrow \text{execs1 d = execs2 d} \land (\text{intermediary d u} \rightarrow \text{execs1 d} = [\text{false}])

Proof that if the current is not an intermediary for u, then all domains involved in the next action are vpeq.

lemma vpeq-involved-domains:
assumes ifp-curr: \text{ifp} (\text{current s}) u
\land \text{not-intermediary-curr} : \neg \text{intermediary} (\text{current s}) u
\land \text{no-gateway-comm} : \text{does-not-communicate-with-gateway} u \text{ execs}
\land \text{vpeq-s-t} : \forall \; v . \; \text{ifp} v u \land \neg \text{intermediary} v u \rightarrow \text{vpeq v s t'}
\land \text{prec-s} : \text{precondition} (\text{next-state s execs}) (\text{next-action s execs})
shows \forall \; d \in \text{involved} (\text{next-action s execs}) . \; \text{vpeq d s t'}

Proof that purging removes communications of the gateway to domain u.

lemma ipurge-l-removes-gateway-communications:
shows does-not-communicate-with-gateway u (ipurge-l execs u)

Proof of view partitioning. The lemma is structured exactly as lemma unwinding\_implies\_view\_partitioned\_ind and uses the same convention for naming.

lemma unwinding-implies-view-partitioned1:
shows iview-partitioned

Returns True iff and only if the two states have the same active domain, or if one of the states is None.

definition mcurrents \::\::\prime \; \text{state-t option} \Rightarrow \prime \; \text{state-t option} \Rightarrow \text{bool}
where mcurrents m1 m2 \equiv m1 \mid m2 \rightarrow (\lambda \; s t . \; \text{current s} = \text{current t})

Proof that switching/interrupts are purely time-based and happen independent of the actions done by the domains. As all theorems in this locale, it holds vacuously whenever one of the states is None, i.e., whenever at some point a precondition does not hold.

lemma current-independent-of-domain-actions:
assumes current-s-t: mcurrents s t
shows mcurrents (\text{run n s execs}) (\text{run n t execs2})

theorem unwinding-implies-NI-indirect-sources:
shows NI-indirect-sources

theorem unwinding-implies-isecure:
shows insecure (proof)
end
end

3.3 ISK (Interruptible Separation Kernel)

theory ISK
imports SK
begin

At this point, the precondition linking action to state is generic and highly unconstrained. We refine the previous locale by given generic functions “precondition” and “realistic_trace” a definition. This yields a total run function, instead of the partial one of locale Separation_Kernel.

This definition is based on a set of valid action sequences AS_set. Consider for example the following action sequence:

$$\gamma = [COPY_{\text{INIT}}, COPY_{\text{CHECK}}, COPY_{\text{COPY}}]$$

If action sequence $$\gamma$$ is a member of AS_set, this means that the attack surface contains an action COPY, which consists of three consecutive atomic kernel actions. Interrupts can occur anywhere between these atomic actions.

Given a set of valid action sequences such as $$\gamma$$, generic function precondition can be defined. It now consists of 1.) a generic invariant and 2.) more refined preconditions for the current action.

These preconditions need to be proven inductive only according to action sequences. Assume, e.g., that $$\gamma \in AS_{\text{set}}$$ and that $$d$$ is the currently active domain in state $$s$$. The following constraints are assumed and must therefore be proven for the instantiation:

- “AS_precondition s d COPY_INIT” since COPY_INIT is the start of an action sequence.
- “AS_precondition (step s COPY_INIT) d COPY_CHECK” since (COPY_INIT, COPY_CHECK) is a sub sequence.
- “AS_precondition (step s COPY_CHECK) d COPY_COPY” since (COPY_CHECK, COPY_COPY) is a sub sequence.

Additionally, the precondition for domain $$d$$ must be consistent when a context switch occurs, or when ever some other domain $$d'$$ performs an action.

Locale Interruptible_Separation_Kernel refines locale Separation_Kernel in two ways. First, there is a definition of realistic executions. A realistic trace consists of action sequences from AS_set.

Secondly, the generic control function has been refined by additional assumptions. It is now assumed that control conforms to one of four possibilities:

1. The execution of the currently active domain is empty and the control function returns no action.
2. The currently active domain is executing the action sequence at the head of the execution. It returns the next kernel action of this sequence and updates the execution accordingly.
3. The action sequence is delayed.
4. The action sequence that is at the head of the execution is skipped and the execution is updated accordingly.

As for the state update, this is still completely unconstrained and generic as long as it respects the generic invariant and the precondition.
locale Interruptible-Separation-Kernel = Separation-Kernel kstep output-f s0 current cswitch interrupt kprecondition realistic-execution control kinvolved ifp vpeq

for kstep :: 'state-t ⇒ 'action-t ⇒ 'state-t
and output-f :: 'state-t ⇒ 'action-t ⇒ 'output-t
and s0 :: 'state-t
and current :: 'state-t ⇒ 'dom-t — Returns the currently active domain
and cswitch :: 'time-t ⇒ 'state-t ⇒ 'state-t — Switches the current domain
and interrupt :: 'time-t ⇒ bool — Returns t iff an interrupt occurs in the given state at the given time
and kprecondition :: 'state-t ⇒ 'action-t ⇒ bool — Returns t if an precondition holds that relates the current action to the state
and realistic-execution :: 'action-t execution ⇒ bool — In this locale, this function is completely unconstrained.
and control :: 'state-t ⇒ 'dom-t ⇒ 'action-t execution ⇒ ('(action-t-option) × 'action-t execution × 'state-t)
and kinvolved :: 'action-t ⇒ 'dom-t set
and ifp :: 'dom-t ⇒ 'dom-t ⇒ bool
and vpeq :: 'dom-t ⇒ 'state-t ⇒ 'state-t ⇒ bool
+

fixes AS-set :: ('action-t list) set — Returns a set of valid action sequences, i.e., the attack surface
and invariant :: 'state-t ⇒ bool
and AS-precondition :: 'state-t ⇒ 'dom-t ⇒ 'action-t ⇒ bool
and aborting :: 'state-t ⇒ 'dom-t ⇒ 'action-t ⇒ bool
and waiting :: 'state-t ⇒ 'dom-t ⇒ 'action-t ⇒ bool
assumes empty-in-AS-set : [] ∈ AS-set
and invariant-s0 : invariant s0
and invariant-after-cswitch : ∀ s n . invariant s → invariant (cswitch n s)
and precondition-after-cswitch : ∀ s d n a . AS-precondition s d a → AS-precondition (cswitch n s) d a
and AS-prec-first-action : ∀ s d a . invariant s ∧ aseq ∈ AS-set ∧ aseq # [] → AS-precondition s d (hd aseq)
and AS-prec-after-step : ∀ s a a’ . (∃ aseq ∈ AS-set ∧ is-sub-seq a a’ aseq) ∧ invariant s ∧ AS-precondition s (current s) a ∧ ¬ aborting s (current s) a ∧ ¬ waiting s (current s) a → AS-precondition (kstep s a) (current s) a’a
and AS-prec-dom-independent : ∀ s d n a . invariant s ∨ ¬ AS-precondition s d a → AS-precondition (kstep s a) d a
and spec-of-invariant : ∀ s a . invariant s → invariant (kstep s a)
and kprecondition-def : kprecondition s a ≡ invariant s ∧ AS-precondition s (current s) a
and realistic-execution-def : realistic-execution aseq ≡ set aseq ⊆ AS-set
and control-spec : ∀ s d aseq . case control s d aseq of (a.aseqs,(s’)) ⇒ (thread-empty aseqs ∧ (a.aseqs’) = (None,[[]])) ∀ — Nothing happens
(aseqs # [] ∧ hd aseqs # [] ∧ ¬ aborting s’ d (the a) ∧ ¬ waiting s’ d (the a) ∧ (a.aseqs’) = (Some (hd (hd aseqs)),(tl (hd aseqs))#(tl aseqs))) ∀ — Execute the first action of the current action sequence
(aseqs # [] ∧ hd aseqs # [] ∧ waiting s’ d (the a) ∧ (a.aseqs’,s) = (Some (hd (hd aseqs)),a.aseqs,s)) ∀ — Nothing happens, waiting to execute the next action
(a.aseqs’) = (None,tl aseqs)
and next-action-after-cswitch : ∀ s n d aseqs . fst (control (cswitch n s) d aseqs) = fst (control s d aseqs)
and next-action-after-step : ∀ s d aseqs . current s ∨ ¬ +d → fst (control (next-state s execs d) d (execs d)) = None χ fst (control (next-state s execs d) d (execs d))
and next-action-after-step : ∀ s d aseqs . current s ∨ ¬ +d → fst (control (step s a) d aseqs) = fst (control s d aseqs)
and next-state-precondition : ∀ s d a . AS-precondition s d a → AS-precondition (next-state s execs) d a
and next-state-invariant : ∀ s d a . invariant s → invariant (next-state s execs)
and spec-of-waiting : ∀ s d a . waiting s (current s) a → kstep s a = s

begin

We can now formulate a total run function, since based on the new assumptions the case where the precondition does not hold, will never occur.

function run-total :: 'time-t ⇒ 'state-t ⇒ ('dom-t ⇒ 'action-t execution) ⇒ 'state-t
where run-total 0 s execs = s
interrupt (Suc n) = run-total (Suc n) s execs = run-total n (cswitch (Suc n) s) execs
¬interrupt (Suc n) = thread-empty(execs (current s)) =⇒ run-total (Suc n) s execs = run-total n s execs
The major part of the proofs in this locale consist of proving that function run_total is equivalent to function run, i.e., that the precondition does always hold. This assumes that the executions are realistic. This means that the execution of each domain contains action sequences that are from AS_set. This ensures, e.g., that a COPY_CHECK is always preceded by a COPY_INIT.

Lemma run_total_equals_run is proven by doing induction. It is however not inductive and can therefore not be proven directly: a realistic execution is not necessarily realistic after performing one action. We generalize to do induction. Predicate realistic_executions_ind is the inductive version of realistic_executions. All action sequences in the tail of the executions must be complete action sequences (i.e., they must be from AS_set). The first action sequence, however, is being executed and is therefore not necessarily an action sequence from AS_set, but it is the last part of some action sequence from AS_set.

We need to know that invariably, the precondition holds. As this precondition consists of 1.) a generic invariant and 2.) more refined preconditions for the current action, we have to know that these two are invariably true.

Proof that “execution is realistic” is inductive, i.e., assuming the current execution is realistic, the execution returned by the control mechanism is realistic.

The lemma that proves that the total run function is equivalent to the partial run function, i.e., that in this refinement the case of the run function where the precondition is False will never occur.

Theorem unwinding_implies_isecure gives security for all realistic executions. For unrealistic executions, it holds vacuously and therefore does not tell us anything. In order to prove security for this refinement (i.e., for function run_total), we have to prove that purging yields realistic runs.
lemma remove-gateway-comm-subset:
  shows set (remove-gateway-communications d exec) ⊆ set exec ∪ {[]} (proof)

lemma realistic-ipurge-l:
  shows ∀ execs d. realistic-executions execs ⟹ realistic-executions (ipurge-l execs d) (proof)

lemma realistic-ipurge-r:
  shows ∀ execs d. realistic-executions execs ⟹ realistic-executions (ipurge-r execs d) (proof)

We now have sufficient lemma’s to prove security for run_total. The definition of security is similar to that in Section 3.2. It now assumes that the executions are realistic and concerns function run_total instead of function run.

definition NI-unrelated-total::bool
where NI-unrelated-total
  ≡ ∀ execs a n. realistic-executions execs ⟹
      (let s-f = run-total n s0 execs in
        output-f s-f a = output-f (run-total n s0 (purge execs (current s-f))) a
      ∧ current s-f = current (run-total n s0 (purge execs (current s-f))))

definition NI-indirect-sources-total::bool
where NI-indirect-sources-total
  ≡ ∀ execs a n. realistic-executions execs ⟹
      (let s-f = run-total n s0 execs in
        output-f (run-total n s0 (ipurge-l execs (current s-f))) a =
        output-f (run-total n s0 (ipurge-r execs (current s-f))) a)

definition isecure-total::bool
where isecure-total ≡ NI-unrelated-total ∧ NI-indirect-sources-total

definition unwinding-implies-secure-total:
shows isecure-total (proof)

3.4 CISK (Controlled Interruptible Separation Kernel)

theory CISK
  imports ISK
begin

This section presents a generic model of a Controlled Interruptible Separation Kernel (CISK). It formulates security, i.e., intransitive noninterference. For a presentation of this model, see Section 2 of [31].

First, a locale is defined that defines all generic functions and all proof obligations (see Section 2.3 of [31]).

locale Controllable-Interruptible-Separation-Kernel = — CISK
  fixes kstep :: 'state-t ⇒ 'action-t ⇒ 'state-t — Executes one atomic kernel action
  and output-f :: 'state-t ⇒ 'action-t ⇒ 'output-t — Returns the observable behavior
  and s0 :: 'state-t — The initial state
  and current :: 'state-t ⇒ 'dom-t — Returns the currently active domain
and cswitch :: time-t ⇒ 'state-t ⇒ 'state-t — Performs a context switch
and interrupt :: time-t ⇒ bool — Returns true if an interrupt occurs in the given state at the given time
and kinvolved :: 'action-t ⇒ 'dom-t-set — Returns the set of domains that are involved in the given action
and ifp :: 'dom-t ⇒ 'dom-t ⇒ bool — The security policy,
and vpeq :: 'dom-t ⇒ 'state-t ⇒ 'state-t ⇒ bool — View partitioning equivalence
and AS-set :: ('action-t list) set — Returns a set of valid action sequences, i.e., the attack surface
and invariant :: 'state-t ⇒ bool — Returns an inductive state-invariant
and AS-precondition :: 'state-t ⇒ 'dom-t ⇒ 'action-t ⇒ bool — Returns the preconditions under which the given action can be executed.
and aborting :: 'state-t ⇒ 'dom-t ⇒ 'action-t ⇒ bool — Returns true if the action is aborted.
and waiting :: 'state-t ⇒ 'dom-t ⇒ 'action-t ⇒ bool — Returns true if execution of the given action is delayed.
and set-error-code :: 'state-t ⇒ 'action-t ⇒ 'state-t — Sets an error code when actions are aborted.

assumes vpeq-transitive: ∀ a b c. (vpeq u a b ∧ vpeq u b c) ⇒ vpeq u a c
and vpeq-symmetric: ∀ a b u. vpeq u a b → vpeq u b a
and vpeq-reflexive: ∀ a u. vpeq u a a
and ifp-reflexive: ∀ u. ifp u u
and weakly-step-consistent: ∀ s t u a. vpeq u s t ∧ vpeq (current s) s t ∧ invariant s ∧ AS-precondition s (current s) a ∧ invariant t ∧ AS-precondition t (current t) a ∧ current s = current t → vpeq u (kstep s a) (kstep t a)
and locally-respects: ∀ s a u. ¬ifp (current s) u ∧ invariant s ∧ AS-precondition s (current s) a → vpeq u s (kstep s a)
and output-consistent: ∀ a s t. vpeq (current s) s t ∧ current s = current t → (output-f s a) = (output-f t a)
and step-atomicity: ∀ s a u. vpeq u s a = current s
and cswitch-independent-of-state: ∀ n s t. current s = current t → (cswitch n s) = current (cswitch n t)
and cswitch-consistency: ∀ u s t n. vpeq u s t → vpeq u (cswitch n s) (cswitch n t)
and empty-in-AS-set: [] ∈ AS-set
and invariant-s0 invariant s0
and invariant-after-cswitch: ∀ s n s. invariant s → invariant (cswitch n s)
and precondition-after-cswitch: ∀ s d n a. AS-precondition s d a → AS-precondition (cswitch n s) d a
and AS-prec-first-action: ∀ s d aseq. invariant s ∧ aseq ∈ AS-set ∧ aseq ≠ [] → AS-precondition s d (hd aseq)
and AS-prec-after-step: ∀ s a a' . (∃ aseq ∈ AS-set . is-sub-seq a a' aseq) ∧ invariant s ∧ AS-precondition s (current s) a ∧ ¬aborting s (current s) a ∧ ¬waiting s (current s) a → AS-precondition (kstep s a) (current s) a'
and AS-prec-dom-independent: ∀ s d a a'. current s ≠ d ∧ AS-precondition s d a → AS-precondition (kstep s a') d a
and spec-of-invariant: ∀ s a. invariant s → invariant (kstep s a)
and aborting-switch-independent: ∀ n s a. aborting (cswitch n s) = aborting s
and aborting-error-update: ∀ s d a a'. current s ≠ d ∧ aborting s d a → aborting (set-error-code s a') d a
and aborting-after-step: ∀ s a d. current s ≠ d → aborting (kstep s a) d = aborting s d
and aborting-consistent: ∀ s t u. vpeq u s t → aborting s u = aborting t u
and waiting-switch-independent: ∀ n s. waiting (cswitch n s) = waiting s
and waiting-error-update: ∀ s d a a'. current s ≠ d ∧ waiting s d a → waiting (set-error-code s a') d a
and waiting-consistent: ∀ s t u a. vpeq (current s) s t ∧ (∀ d ∈ kinvolved a . vpeq d s t) ∧ vpeq u s t → waiting s u a = waiting t u a
and spec-of-waiting: ∀ s a. waiting s (current s) a → kstep s a = s
and set-error-consistent: ∀ s t u a. vpeq u s t → vpeq u (set-error-code s a) (set-error-code t a)
and set-error-locally-respects: ∀ s u a . ¬ifp (current s) u → vpeq u s (set-error-code s a)
and current-set-error-code: ∀ s a u. current s (set-error-code s a) = current s
and precondition-after-set-error-code: ∀ s d a a'. AS-precondition s d a ∧ aborting s (current s) a' → AS-precondition (set-error-code s a') d a
and invariant-after-set-error-code: ∀ s a . invariant s → invariant (set-error-code s a)
and involved-ifp: ∀ s a . ∀ d ∈ (kinvolved a) . AS-precondition s (current s) a → ifp d (current s)
3.4.1 Execution semantics

Control is based on generic functions aborting, waiting and set_error_code. Function aborting decides whether a certain action is aborting, given its domain and the state. If so, then function set_error_code will be used to update the state, possibly communicating to other domains that an action has been aborted. Function waiting can delay the execution of an action. This behavior is implemented in function CISK_control.

function CISK-control :: 'state-t ⇒ 'dom-t ⇒ 'action-t execution ⇒ ('action-t option × 'action-t execution × 'state-t)
where
| CISK-control s d [] = (None, [], s) — The thread is empty
| CISK-control s d ([]#[]) = (None, [], s) — The current action sequence has been finished and the thread has no next action sequences to execute

Function run defines the execution semantics. This function is presented in [31] by pseudo code (see Algorithm 1). Before defining the run function, we define accessor functions for the control mechanism. Functions next_action, next_execs and next_state correspond to “control.a”, “control.x” and “control.s” in [31].

abbreviation next-action::'state-t ⇒ ('dom-t ⇒ 'action-t execution) ⇒ 'action-t option
where
next-action ≡ Kernel.next-action current CISK-control

abbreviation next-execs::'state-t ⇒ ('dom-t ⇒ 'action-t execution) ⇒ ('dom-t ⇒ 'action-t execution)
where
next-execs ≡ Kernel.next-execs current CISK-control

abbreviation next-state::'state-t ⇒ ('dom-t ⇒ 'action-t execution) ⇒ 'state-t
where
next-state ≡ Kernel.next-state current CISK-control

A thread is empty iff either it has no further action sequences to execute, or when the current action sequence is finished and there are no further action sequences to execute.

abbreviation thread-empty::'action-t execution ⇒ bool
where
thread-empty exec ≡ exec = [] ∨ exec = [[]]

The following function defines the execution semantics of CISK, using function CISK_control.

function run :: time-t ⇒ 'state-t ⇒ ('dom-t ⇒ 'action-t execution) ⇒ 'state-t
where
| interrupt (Suc n) ⇒ run (Suc n) s execs = run n (cswitch (Suc n) s) execs
| ~interrupt (Suc n) ⇒ thread-empty(execs (current s)) ⇒ run (Suc n) s execs = run n s execs
| ~interrupt (Suc n) ⇒ ~thread-empty(execs (current s)) ⇒
  run (Suc n) s execs = (let control-a = next-action s execs;
  control-s = next-state s execs;
  control-x = next-execs s execs in
  case control-a of None ⇒ run n control-s control-x;
  Some a ⇒ run n (kstep control-s a) control-x)

(proof)
termination {proof}

3.4.2 Formulations of security

The definitions of security as presented in Section 2.2 of [31].
### 3.4.3 Proofs

The final theorem is unwinding_implies_isecure_CISK. This theorem shows that any interpretation of locale CISK is secure.

To prove this theorem, the refinement framework is used. CISK is a refinement of ISK, as the only difference is the control function. In ISK, this function is a generic function called `control`, in CISK it is interpreted in function `CISK_control`. It is proven that function `CISK_control` satisfies all the proof obligations concerning generic function `control`. In other words, `CISK_control` is proven to be an interpretation of control. Therefore, all theorems on `run_total` apply to the run function of CISK as well.

**lemma next-action-consistent:**

shows ∀ s t execs . vpeq (current s) s t ∧ (∀ d ∈ involved (next-action s execs) . vpeq d s t) ∧ current s = current t → next-action s execs = next-action t execs

(proof)

**lemma next-execs-consistent:**

shows ∀ s t execs . vpeq (current s) s t ∧ (∀ d ∈ involved (next-action s execs) . vpeq d s t) ∧ current s = current t → fst (snd (CISK-control s (current s) (execs (current s)))) = fst (snd (CISK-control t (current s) (execs (current s)))))

(proof)

**lemma next-state-consistent:**

shows ∀ s t u execs . vpeq (current s) s t ∧ vpeq u s t ∧ current s = current t → vpeq u (next-state s execs)

(proof)

**lemma current-next-state:**

shows ∀ s execs . current (next-state s execs) = current s

(proof)

**lemma locally-respects-next-state:**
D31.1 – Formal Specification of a Generic Separation Kernel

shows ∀ s u execs. ¬ifp (current s) u → vpeq u s (next-state s execs)

(proof)

lemma CISK-control-spec:
shows ∀ s d aseqs.
   case CISK-control s d aseqs of
      (a, aseqs′, s′) ⇒
      thread-empty aseqs ∧ (a, aseqs′) = (None, [] ) ∨
      aseqs ≠ [] ∧ hd aseqs ≠ [] ∧ ∼ aborting s′ d (the a) ∧ ∼ waiting s′ d (the a) ∧ (a, aseqs′) = (Some (hd (hd aseqs)), tl (hd aseqs)) # tl aseqs) ∨
      aseqs ≠ [] ∧ hd aseqs ≠ [] ∧ waiting s′ d (the a) ∧ (a, aseqs′, s′) = (Some (hd (hd aseqs)), aseqs, s) ∨ (a, aseqs′) = (None, tl aseqs)

(proof)

lemma next-action-after-cswitch:
shows ∀ s n d aseqs . fst (CISK-control (cswitch n s) d aseqs) = fst (CISK-control s d aseqs)

(proof)

lemma next-action-after-next-state:
shows ∀ s execs d . current s ≠ d → fst (CISK-control (next-state s execs) d (execs d)) = None ∨ fst (CISK-control (next-state s execs) d (execs d)) = fst (CISK-control s d (execs d))

(proof)

lemma next-action-after-step:
shows ∀ s a d aseqs . current s ≠ d → fst (CISK-control (step s a) d aseqs) = fst (CISK-control s d aseqs)

(proof)

lemma next-state-precondition:
shows ∀ s d a execs. AS-precondition s d a → AS-precondition (next-state s execs) d a

(proof)

lemma next-state-invariant:
shows ∀ s execs. invariant s → invariant (next-state s execs)

(proof)

lemma next-action-from-execs:
shows ∀ s execs . next-action s execs = (λ a . a ∈ actions-in-execution (execs (current s)))

(proof)

lemma next-execs-subset:
shows ∀ s execs u . actions-in-execution (next-execs s execs u) ⊆ actions-in-execution (execs u)

(proof)

theorem unwinding-implies-secure-CISK:
shows secure

(proof)

end
end

4 Instantiation by a separation kernel with concrete actions
In the previous section, no concrete actions for the step function were given. The foremost point we want to make by this instantiation is to show that we can instantiate the CISK model of the previous section with an implementation that, for the step function, as actions, provides events and interprocess communication (IPC). System call invocations that can be interrupted at certain interrupt points are split into several atomic steps. A communication interface of events and IPC is less “trivial” than it may seem at a first glance, for example the L4 microkernel API only provided IPC as communication primitive [16]. In particular, the concrete actions illustrate how an application of the CISK framework can be used to separate policy enforcement from other computations unrelated to policy enforcement.

Our separation kernel instantiation also has a notion of partitions. A partition is a logical unit that serves to encapsulate a group of CISK threads by, amongst others, enforcing a static per-partition access control policy to system resources. In the following instantiation, while the subjects of the step function are individual threads, the information flow policy ifp is defined at the granularity of partitions, which is realistic for many separation kernel implementations.

Lastly, as a limited manipulation of an access control policy is often needed, we also provide an invariant for having a dynamic access control policy whose maximal closure is bounded by the static per-partition access control policy. That the dynamic access control policy is a subset of a static access control policy is expressed by the invariant sp_subset. A use case for this is when you have statically configured access to files by subjects, but whether a file can be read/written also depends on whether the file has been dynamically opened or not. The instantiation provides infrastructure for such an invariant on the relation of a dynamic policy to a static policy, and shows how the invariant is maintained, without modeling any API for an open/close operation.

4.1 Model of a separation kernel configuration

4.1.1 Type definitions

The separation kernel partitions are considered to be the “subjects” of the information flow policy ifp. A file provider is a partition that, via a file API (read/write), provides files to other partitions. The configuration statically defines which partitions can act as a file provider and also the access rights (right/write) of other partitions to the files provided by the file provider. Some separation kernels include a management for address spaces (tasks), that may be hierachically structured. Such a task hierarchy is not part of this model.

```c
typedef partition-id-t
typedef thread-id-t

typedef page-t — physical address of a memory page
typedel filep-t — name of file provider

datatype obj-id-t =
    PAGE page-t
| FILEP filep-t

datatype mode-t =
    READ — The subject has right to read from the memory page, from the files served by a file provider.
| WRITE — The subject has right to write to the memory page, from the files served by a file provider.
| PROVIDE — The subject has right serve as the file provider. This mode is not used for memory pages or ports.
```

4.1.2 Configuration

The information flow policy is implicitly specified by the configuration. The configuration does not contain the communication rights between partitions (subjects). However, the rights can be derived from the configuration. For example, if two partitions \( p \) and \( p' \) can access a file \( f \), then \( p \) and \( p' \) can communicate. See below.
consts
configured-subj-obj :: partition-id-t ⇒ obj-id-t ⇒ mode-t ⇒ bool

Each user thread belongs to a partition. The relation is fixed at system startup. The configuration specifies how many threads a partition can create, but this limit is not part of the model.

c consts
partition :: thread-id-t ⇒ partition-id-t

end

4.2 Formulation of a subject-subject communication policy and an information flow policy, and showing both can be derived from subject-object configuration data

theory Step-policies
imports Step-configuration
begin

4.2.1 Specification

In order to use CISK, we need an information flow policy ifp relation. We also express a static subject-subject sp-spec-subj-subj and subject-object sp-spec-subj-obj access control policy for the implementation of the model. The following locale summarizes all properties we need.

locale policy-axioms =
  fixes sp-spec-subj-obj :: 'a ⇒ obj-id-t ⇒ mode-t ⇒ bool
  and sp-spec-subj-subj :: 'a ⇒ 'a ⇒ bool
  and ifp :: 'a ⇒ 'a ⇒ bool

assumes sp-spec-file-provider: ∀ p1 p2 f m1 m2.
  sp-spec-subj-obj p1 (FILEP f) m1 ∧
  sp-spec-subj-obj p2 (FILEP f) m2 → sp-spec-subj-subj p1 p2

and sp-spec-no-wronly-pages:
  ∀ p x. sp-spec-subj-obj p (PAGE x) WRITE → sp-spec-subj-obj p (PAGE x) READ

and ifp-reflexive:
  ∀ p. ifp p p

and ifp-compatible-with-sp-spec:
  ∀ a b. sp-spec-subj-subj a b → ifp a b ∧ ifp b a

and ifp-compatible-with-ipc:
  ∀ a b c x. (sp-spec-subj-subj a b
  ∧ sp-spec-subj-obj b (PAGE x) WRITE ∧ sp-spec-subj-obj c (PAGE x) READ)
  → ifp a c

begin end

4.2.2 Derivation

The configuration data only consists of a subject-object policy. We derive the subject-subject policy and the information flow policy from the configuration data and prove that properties we specified in Section 4.2.1 are satisfied.

locale abstract-policy-derivation =
  fixes configuration-subj-obj :: 'a ⇒ obj-id-t ⇒ mode-t ⇒ bool

begin
definition sp-spec-subj-obj \ a x m ≡
configuration-subj-obj \ a x m ∨ (\exists \ y . \ x = PAGE y ∧ m = READ ∧ configuration-subj-obj \ a x WRITE)

definition sp-spec-subj-subj \ a b ≡
(\exists \ f m1 m2 . sp-spec-subj-obj \ a (FILEP f) m1 ∧ sp-spec-subj-obj \ b (FILEP f) m2)

definition ifp \ a b ≡
sp-spec-subj-subj \ a b
∨ sp-spec-subj-subj \ b a
∨ (\exists \ c y . sp-spec-subj-subj \ a c ∧ sp-spec-subj-obj \ c \ (PAGE y) WRITE ∧ sp-spec-subj-obj \ b \ (PAGE y) READ)
∨ (a = b)

Show that the policies specified in Section 4.2.1 can be derived from the configuration and their definitions.

lemma correct:
shows policy-axioms sp-spec-subj-obj sp-spec-subj-subj ifp
{proof}
end

type-synonym sp-subj-subj-t = partition-id-t ⇒ partition-id-t ⇒ bool
type-synonym sp-subj-obj-t = partition-id-t ⇒ obj-id-t ⇒ mode-t ⇒ bool

interpretation Policy: abstract-policy-derivation configured-subj-obj{proof}
interpretation Policy-properties: policy-axioms Policy.sp-spec-subj-obj Policy.sp-spec-subj-subj Policy.ifp
{proof}

lemma example-how-to-use-properties-in-proofs:
shows ∀ \ p . Policy.ifp p p
{proof}
end

4.3 Separation kernel state and atomic step function

theory Step
  imports Step-policies
begin

4.3.1 Interrupt points

To model concurrency, each system call is split into several atomic steps, while allowing interrupts between the steps. The state of a thread is represented by an “interrupt point” (which corresponds to the value of the program counter saved by the system when a thread is interrupted).

datatype ipc-direction-t = SEND | RECV
datatype ipc-stage-t = PREP | WAIT | BUF page-t

datatype ev-consume-t = EV-CONSUME-ALL | EV-CONSUME-ONE
datatype ev-wait-stage-t = EV-PREP | EV-WAIT | EV-FINISH
datatype ev-signal-stage-t = EV-SIGNAL-PREP | EV-SIGNAL-FINISH
datatype int-point-t =
SK-IPC ipc-direction-t ipc-stage-t thread-id-t page-t — The thread is executing a sending / receiving IPC.
| SK-EV-WAIT ev-wait-stage-t ev-consume-t — The thread is waiting for an event.
| SK-EV-SIGNAL ev-signal-stage-t thread-id-t — The thread is sending an event.
| NONE — The thread is not executing any system call.
4.3.2 System state

typedec obj-t — value of an object

Each thread belongs to a partition. The relation is fixed (in this instantiation of a separation kernel).

consts

partition :: thread-id-t ⇒ partition-id-t

The state contains the dynamic policy (the communication rights in the current state of the system, for example).

record thread-t =

  ev-counter = nat — event counter

record state-t =

  sp-impl-subj-subj :: sp-subj-subj-t — current subject-subject policy
  sp-impl-subj-obj :: sp-subj-obj-t — current subject-object policy
  current :: thread-id-t — current thread
  obj :: obj-id-t ⇒ obj-t — values of all objects
  thread :: thread-id-t ⇒ thread-t — internal state of threads

Later (Section 4.4), the system invariant sp-subset will be used to ensure that the dynamic policies (sp_impl_...) are a subset of the corresponding static policies (sp_spec_...).

4.3.3 Atomic step

Helper functions

Set new value for an object.

definition set-object-value :: obj-id-t ⇒ obj-t ⇒ state-t ⇒ state-t where

  set-object-value obj-id val s =
  s ( fun-upd (obj s) obj-id val )

  Return a representation of the opposite direction of IPC communication.

definition opposite-ipc-direction :: ipc-direction-t ⇒ ipc-direction-t where

  opposite-ipc-direction dir ≡
  case dir of
    SEND ⇒ RECV
    RECV ⇒ SEND

  Add an access right from one partition to an object. In this model, not available from the API, but shows how dynamic changes of access rights could be implemented.

definition add-access-right :: partition-id-t ⇒ obj-id-t ⇒ mode-t ⇒ state-t ⇒ state-t where

  add-access-right part-id obj-id m s =
  s ( fun-sp-impl-subj-obj ⇒ λ q q' q''.
    (part-id = q ∧ obj-id = q' ∧ m = q'')
    ∨ sp-impl-subj-obj s q q'' )

  Add a communication right from one partition to another. In this model, not available from the API.

definition add-comm-right :: partition-id-t ⇒ partition-id-t ⇒ state-t ⇒ state-t where

  add-comm-right p p' s ≡
  s ( fun-sp-impl-subj-subj ⇒ λ q q' p = q ∧ p' = q' )

Model of IPC system call

We model IPC with the following simplifications:

1. The model contains the system calls for sending an IPC (SEND) and receiving an IPC (RECV), often implementations have a richer API (e.g. combining SEND and RECV in one invocation).

2. We model only a copying (“BUF”) mode, not a memory-mapping mode.

3. The model always copies one page per syscall.
**Definition**

\[ \text{ipc-precondition} :: \text{thread-id-t} \Rightarrow \text{ipc-direction-t} \Rightarrow \text{thread-id-t} \Rightarrow \text{page-t} \Rightarrow \text{state-t} \Rightarrow \text{bool} \]

where

\[ \text{ipc-precondition \ tid \ dir \ partner \ page \ s} \equiv \]

\[ \text{let sender} = \begin{cases} \text{case dir of} & \text{SEND} \Rightarrow \text{tid} / \text{divides.alt0} \\ \text{RECV} \Rightarrow \text{partner} \end{cases} \]

\[ \text{let receiver} = \begin{cases} \text{case dir of} & \text{SEND} \Rightarrow \text{partner} / \text{divides.alt0} \\ \text{RECV} \Rightarrow \text{tid} \end{cases} \]

\[ \text{let local-access-mode} = \begin{cases} \text{case dir of} & \text{SEND} \Rightarrow \text{READ} / \text{divides.alt0} \\ \text{RECV} \Rightarrow \text{WRITE} \end{cases} \]

\[ (\text{sp-impl-subj-subj s (partition sender)} (\text{partition receiver}) \text{ local-access-mode}) \]

\[ \text{atomic-step-ipc :: \text{thread-id-t} \Rightarrow \text{ipc-direction-t} \Rightarrow \text{ipc-stage-t} \Rightarrow \text{thread-id-t} \Rightarrow \text{page-t} \Rightarrow \text{state-t} \Rightarrow \text{state-t}} \]

where

\[ \text{atomic-step-ipc \ tid \ dir \ stage \ partner \ page \ s} \equiv \]

\[ \text{case stage of} \]

\[ \text{PREP} \Rightarrow \]

\[ s \]

\[ \text{WAIT} \Rightarrow \]

\[ s \]

\[ \text{BUF page}\' \Rightarrow \]

\[ \text{(case dir of} \]

\[ \text{SEND} \Rightarrow \]

\[ (\text{set-object-value (PAGE page') (obj s (PAGE page)) s}) \]

\[ \text{RECV} \Rightarrow s) \]

**Model of event syscalls**

**Definition**

\[ \text{ev-signal-precondition} :: \text{thread-id-t} \Rightarrow \text{thread-id-t} \Rightarrow \text{state-t} \Rightarrow \text{bool} \]

where

\[ \text{ev-signal-precondition \ tid \ partner \ s} \equiv \]

\[ (\text{sp-impl-subj-subj s (partition tid)} (\text{partition partner})) \]

**Definition**

\[ \text{atomic-step-ev-signal} :: \text{thread-id-t} \Rightarrow \text{thread-id-t} \Rightarrow \text{state-t} \Rightarrow \text{state-t} \]

where

\[ \text{atomic-step-ev-signal \ tid \ partner \ s} = \]

\[ s \text{ (} \text{thread} := \text{fun-upd} (\text{thread \ s}) \text{ partner} (\text{thread \ s partner} (\text{ev-counter} := \text{Suc (ev-counter (thread \ s partner)}))) \text{)} \]

**Definition**

\[ \text{atomic-step-ev-wait-one} :: \text{thread-id-t} \Rightarrow \text{state-t} \Rightarrow \text{state-t} \]

where

\[ \text{atomic-step-ev-wait-one \ tid \ s} = \]

\[ s \text{ (} \text{thread} := \text{fun-upd} (\text{thread \ s}) \text{ tid} (\text{thread \ s tid} (\text{ev-counter} := (\text{ev-counter (thread \ s tid)} - 1))) \text{)} \]

**Definition**

\[ \text{atomic-step-ev-wait-all} :: \text{thread-id-t} \Rightarrow \text{state-t} \Rightarrow \text{state-t} \]

where

\[ \text{atomic-step-ev-wait-all \ tid \ s} = \]

\[ s \text{ (} \text{thread} := \text{fun-upd} (\text{thread \ s}) \text{ tid} (\text{thread \ s tid} (\text{ev-counter} := 0))) \]

**Instantiation of CISK aborting and waiting**

In this instantiation of CISK, the **aborting** function is used to indicate security policy enforcement. An IPC call aborts in its **PREP** stage if the precondition for the calling thread does not hold. An event signal call aborts in its **EV-SIGNAL-PREP** stage if the precondition for the calling thread does not hold.

**Definition**

\[ \text{aborting} :: \text{state-t} \Rightarrow \text{thread-id-t} \Rightarrow \text{int-point-t} \Rightarrow \text{bool} \]

where

\[ \text{aborting \ s \ tid \ a} \equiv \text{case a of SK-IPC dir PREP partner page} \Rightarrow \]

\[ \text{~ipc-precondition \ tid \ dir \ partner \ page \ s} \]

\[ | \text{SK-EV-SIGNAL EV-SIGNAL-PREP partner} \Rightarrow \text{~ev-signal-precondition \ tid \ partner \ s} \]

\[ | \text{-} \Rightarrow \text{False} \]

The **waiting** function is used to indicate synchronization. An IPC call waits in its **WAIT** stage while the precondition for the partner thread does not hold. An **EV_WAIT** call waits until the event counter is not zero.

**Definition**

\[ \text{waiting} :: \text{state-t} \Rightarrow \text{thread-id-t} \Rightarrow \text{int-point-t} \Rightarrow \text{bool} \]
The atomic step function. In the definition of atomic-step the arguments to an interrupt point are not taken from the thread state – the argument given to atomic-step could have an arbitrary value. So, seen in isolation, atomic-step allows more transitions than actually occur in the separation kernel. However, the CISK framework (1) restricts the atomic step function by the waiting and aborting functions as well (2) the set of realistic traces as attack sequences rAS-set (Section 4.8). An additional condition is that (3) the dynamic policy used in aborting is a subset of the static policy. This is ensured by the invariant sp-subset.

definition atomic-step :: state-t ⇒ int-point-t ⇒ state-t where
atomic-step s ipt ≡
case ipt of
  SK-IPC dir stage partner page ⇒
    atomic-step-ipc (current s) dir stage partner page s
  SK-EV-WAIT EV-PREP consume ⇒ s
  SK-EV-WAIT EV-WAIT consume ⇒ s
  SK-EV-WAIT EV-FINISH consume ⇒
case consume of
  EV-CONSUME-ONE ⇒ atomic-step-ev-wait-one (current s) s
  EV-CONSUME-ALL ⇒ atomic-step-ev-wait-all (current s) s
  SK-EV-SIGNAL EV-SIGNAL-PREP partner ⇒ s
  SK-EV-SIGNAL EV-SIGNAL-FINISH partner ⇒
    atomic-step-ev-signal (current s) partner s
  NONE ⇒ s
end

4.4 Preconditions and invariants for the atomic step

theory Step-invariants
imports Step
begin

The dynamic/implementation policies have to be compatible with the static configuration.

definition sp-subset s ≡
(∀ p1 p2 . sp-impl-subj-subj s p1 p2 → Policy.sp-spec-subj-subj p1 p2)
∧ (∀ p1 p2 m . sp-impl-subj-obj s p1 p2 m → Policy.sp-spec-subj-obj p1 p2 m)

The following predicate expresses the precondition for the atomic step. The precondition depends on the type of the atomic action.

definition atomic-step-precondition :: state-t ⇒ thread-id-t ⇒ int-point-t ⇒ bool where
atomic-step-precondition s tid ipt ≡
case ipt of
  SK-IPC dir WAIT partner page ⇒
    — the thread managed it past PREP stage
    ipc-precondition tid dir partner page s
  SK-IPC dir (BUF page) partner page ⇒
    — both the calling thread and its communication partner managed it past PREP and WAIT stages
    ipc-precondition tid dir partner page s
∧ ipc-precondition partner (opposite-ipc-direction dir) tid page’ s
| SK-EV-SIGNAL EV-SIGNAL-FINISH partner ⇒
ev-signal-precondition tid partner s
| · ⇒
— No precondition for other interrupt points.
  True

The invariant to be preserved by the atomic step function. The invariant is independent from the type of the atomic action.

definition atomic-step-invariant ≔ state-t ⇒ bool where
  atomic-step-invariant s ≡
  sp-subset s

4.4.1 Atomic steps of SK_IPC preserve invariants

lemma set-object-value-invariant:
  shows atomic-step-invariant s = atomic-step-invariant (set-object-value ob va s)
{proof}

lemma set-thread-value-invariant:
  shows atomic-step-invariant s = atomic-step-invariant (s (/ thread := thrst []))
{proof}

lemma atomic-ipc-preserves-invariants:
  fixes s :: state-t
  and tid :: thread-id-t
  assumes atomic-step-invariant s
  shows atomic-step-invariant (atomic-step-ipc tid dir stage partner page s)
{proof}

lemma atomic-ev-wait-one-preserves-invariants:
  fixes s :: state-t
  and tid :: thread-id-t
  assumes atomic-step-invariant s
  shows atomic-step-invariant (atomic-step-ev-wait-one tid s)
{proof}

lemma atomic-ev-wait-all-preserves-invariants:
  fixes s :: state-t
  and tid :: thread-id-t
  assumes atomic-step-invariant s
  shows atomic-step-invariant (atomic-step-ev-wait-all tid s)
{proof}

lemma atomic-ev-signal-preserves-invariants:
  fixes s :: state-t
  and tid :: thread-id-t
  assumes atomic-step-invariant s
  shows atomic-step-invariant (atomic-step-ev-signal tid partner s)
{proof}

4.4.2 Summary theorems on atomic step invariants

Now we are ready to show that an atomic step from the current interrupt point in any thread preserves invariants.

theorem atomic-step-preserves-invariants:
  fixes s :: state-t
Finally, the invariants do not depend on the current thread. That is, the context switch preserves the invariants, and an atomic step that is not a context switch does not change the current thread.

**Theorem:** context-switch-preserves-invariants

**Proof:**

**Theorem:** atomic-step-does-not-change-current-thread

**Proof:**

---

### 4.5 The view-partitioning equivalence relation

**Theory:** Step-vpeq

**Imports:** Step, Step-invariants

**Definition:** vpeq-obj

**Definition:** vpeq-subj-subj

**Definition:** vpeq-subj-obj

**Definition:** vpeq-local

**Definition:** vpeq
4.5.1 Elementary properties

**lemma vpeq-rel:**

- shows vpeq-refl: vpeq u s s
- and vpeq-sym: vpeq u s t \iff\ vpeq u t s
- and vpeq-trans: [\text{trans}]: [\text{vpeq u s1 s2 \& vpeq u s2 s3}] \implies vpeq u s1 s3

(proof)

Auxiliary equivalence relation.

**lemma set-object-value-ign:**

- assumes eq-obs: Policy.sp-spec-subj-obj u x READ
- shows vpeq u s (set-object-value x y s)

(proof)

Context-switch and fetch operations are also consistent with vpeq and locally respect everything.

**theorem cswitch-consistency-and-respect:**

- fixes u: partition-id-t
- and s: state-t
- and new-current: thread-id-t
- assumes atomic-step-invariant s
- shows vpeq u s (s \{ current := new-current \})

(proof)

end

4.6 Atomic step locally respects the information flow policy

**theory Step-vpeq-locally-respects**

- imports Step Step-invariants Step-vpeq

begin

The notion of locally respects is common usage. We augment it by assuming that the \text{atomic-step-invariant} holds (see [31]).

4.6.1 Locally respects of atomic step functions

**lemma ipc-respects-policy:**

- assumes nos \sim Policy.ifp (partition tid) u
- and inv: atomic-step-invariant s
- and prec: atomic-step-precondition s tid (SK-IPC dir stage partner pag)
- and ipt-case: ipt = SK-IPC dir stage partner page
- shows vpeq u s (atomic-step-ipc tid dir stage partner page s)

(proof)

**lemma ev-signal-respects-policy:**

- assumes nos \sim Policy.ifp (partition tid) u
- and inv: atomic-step-invariant s
- and prec: atomic-step-precondition s tid (SK-EV-SIGNAL EV-SIGNAL-FINISH partner)
- and ipt-case: ipt = SK-EV-SIGNAL EV-SIGNAL-FINISH partner
- shows vpeq u s (atomic-step-ev-signal tid partner s)

(proof)

**lemma ev-wait-all-respects-policy:**

- assumes nos \sim Policy.ifp (partition tid) u
- and inv: atomic-step-invariant s
- and prec: atomic-step-precondition s tid ipt
and ipt-case: ipt = SK-EV-WAIT ev-wait-stage EV-CONSUME-ALL
shows vpeq u s (atomic-step-ev-wait-all tid s)
{proof}

lemma ev-wait-one-respects-policy:
  assumes nos ~ Policy.ifp (partition tid) u
  and inv: atomic-step-invariant s
  and prec: atomic-step-precondition s tid ipt
  and ipt-case: ipt = SK-EV-WAIT ev-wait-stage EV-CONSUME-ONE
  shows vpeq u s (atomic-step-ev-wait-one tid s)
  {proof}

4.6.2 Summary theorems on view-partitioning locally respects

Atomic step locally respects the information flow policy (ifp). The policy ifp is not necessarily the same as sp_spec_subj_subj.

theorem atomic-step-respects-policy:
  assumes nos ~ Policy.ifp (partition (current s)) u
  and inv: atomic-step-invariant s
  and prec: atomic-step-precondition s (current s) ipt
  shows vpeq u s (atomic-step ipt)
  {proof}

end

4.7 Weak step consistency

theory Step-vpeq-weakly-step-consistent
  imports Step Step-invariants Step-vpeq
begin

  The notion of weak step consistency is common usage. We augment it by assuming that the atomic-step-invariant holds (see [31]).

4.7.1 Weak step consistency of auxiliary functions

lemma ipc-precondition-weakly-step-consistent:
  assumes eq-tid: vpeq (partition tid) s1 s2
  and inv1: atomic-step-invariant s1
  and inv2: atomic-step-invariant s2
  shows ipc-precondition tid dir partner page s1 = ipc-precondition tid dir partner page s2
  {proof}

lemma ev-signal-precondition-weakly-step-consistent:
  assumes eq-tid: vpeq (partition tid) s1 s2
  and inv1: atomic-step-invariant s1
  and inv2: atomic-step-invariant s2
  shows ev-signal-precondition tid partner s1 = ev-signal-precondition tid partner s2
  {proof}

lemma set-object-value-consistent:
  assumes eq-obs: vpeq u s1 s2
  shows vpeq u (set-object-value x y s1) (set-object-value x y s2)
  {proof}
4.7.2 Weak step consistency of atomic step functions

**Lemma ipc-weakly-step-consistent:**

**Assumes**
- `eq-obs`: `vpeq u s1 s2`
- `eq-act`: `vpeq (partition tid) s1 s2`
- `inv1`: `atomic-step-invariant s1`
- `inv2`: `atomic-step-invariant s2`
- `prec1`: `atomic-step-precondition s1 tid ipt`
- `prec2`: `atomic-step-precondition s1 tid ipt`
- `ipt-case`: `ipt = SK-IPC dir stage partner page`

**Shows**
- `vpeq u (atomic-step-ipc tid dir stage partner page s1)`
- `vpeq u (atomic-step-ipc tid dir stage partner page s2)`

**Proof**

**Lemma ev-wait-one-weakly-step-consistent:**

**Assumes**
- `eq-obs`: `vpeq u s1 s2`
- `eq-act`: `vpeq (partition tid) s1 s2`
- `inv1`: `atomic-step-invariant s1`
- `inv2`: `atomic-step-invariant s2`
- `prec1`: `atomic-step-precondition s1 (current s1) ipt`
- `prec2`: `atomic-step-precondition s1 (current s1) ipt`

**Shows**
- `vpeq u (atomic-step-ev-wait-one tid s1)`
- `vpeq u (atomic-step-ev-wait-one tid s2)`

**Proof**

**Lemma ev-wait-all-weakly-step-consistent:**

**Assumes**
- `eq-obs`: `vpeq u s1 s2`
- `eq-act`: `vpeq (partition tid) s1 s2`
- `inv1`: `atomic-step-invariant s1`
- `inv2`: `atomic-step-invariant s2`
- `prec1`: `atomic-step-precondition s1 (current s1) ipt`
- `prec2`: `atomic-step-precondition s1 (current s1) ipt`

**Shows**
- `vpeq u (atomic-step-ev-wait-all tid s1)`
- `vpeq u (atomic-step-ev-wait-all tid s2)`

**Proof**

**Lemma ev-signal-weakly-step-consistent:**

**Assumes**
- `eq-obs`: `vpeq u s1 s2`
- `eq-act`: `vpeq (partition tid) s1 s2`
- `inv1`: `atomic-step-invariant s1`
- `inv2`: `atomic-step-invariant s2`
- `prec1`: `atomic-step-precondition s1 (current s1) ipt`
- `prec2`: `atomic-step-precondition s1 (current s1) ipt`

**Shows**
- `vpeq u (atomic-step-ev-signal tid partner s1)`
- `vpeq u (atomic-step-ev-signal tid partner s2)`

**Proof**

The use of `extend-f` is to provide infrastructure to support use in dynamic policies, currently not used.

**Definition**

```
definition extend-f :: (partition-id-t ⇒ partition-id-t ⇒ bool) ⇒ (partition-id-t ⇒ partition-id-t ⇒ bool) ⇒ (partition-id-t ⇒ partition-id-t ⇒ bool) where
  extend-f f g = λ p1 p2 . f p1 p2 ∨ g p1 p2
```

**Definition**

```
definition extend-subj-subj :: (partition-id-t ⇒ partition-id-t ⇒ bool) ⇒ state-t ⇒ state-t where
```

---

**EURO-MILS D31.1**
extend-subj-subj \( f s \equiv s (/\text{divides.alt0} \text{sp-impl-subj-subj} = \text{extend-ff} (\text{sp-impl-subj-subj} s)) \)

**Lemma** extend-subj-subj-consistent:

- **Fixes** \( f :: \text{partition-id-t} \Rightarrow \text{partition-id-t} \Rightarrow \text{bool} \)
- **Assumes** \( \text{vpeq u s1 s2} \)
- **Shows** \( \text{vpeq u} (\text{extend-subj-subj} f s1) (\text{extend-subj-subj} f s2) \)

**Proof**

4.7.3 **Summary theorems on view-partitioning weak step consistency**

The atomic step is weakly step consistent with view partitioning. Here, the “weakness” is that we assume that the two states are vp-equivalent not only w.r.t. the observer domain \( u \), but also w.r.t. the caller domain \( \text{Step partition tid} \).

**Theorem** atomic-step-weakly-step-consistent:

- **Assumes** eq-obs: \( \text{vpeq u s1 s2} \)
- and eq-act: \( \text{vpeq} (\text{partition (current s1)}) s1 s2 \)
- and inv1: \( \text{atomic-step-invariant s1} \)
- and inv2: \( \text{atomic-step-invariant s2} \)
- and prec1: \( \text{atomic-step-precondition s1 (current s1)} ipt \)
- and prec2: \( \text{atomic-step-precondition s2 (current s2)} ipt \)
- and eq-curr: \( \text{current s1} = \text{current s2} \)
- **Shows** \( \text{vpeq u} (\text{atomic-step s1} ipt) (\text{atomic-step s2} ipt) \)

**Proof**

4.8 **Separation kernel model**

**Theory** Separation-kernel-model


**Begin**

First (Section 4.8.1) we instantiate the CISK generic model. Functions that instantiate a generic function of the CISK model are prefixed with an ‘r’, ‘r’ standing for ‘Rushby’;, as CISK is derived originally from a model by Rushby [31]. For example, ‘rifp’ is the instantiation of the generic ‘ifp’.

Later (Section 4.8.5) all CISK proof obligations are discharged, e.g., weak step consistency, output consistency, etc. These will be used in Section 4.9.

4.8.1 **Initial state of separation kernel model**

We assume that the initial state of threads and memory is given. The initial state of threads is arbitrary, but the threads are not executing the system call. The purpose of the following definitions is to obtain the initial state without potentially dangerous axioms. The only axioms we admit without proof are formulated using the “consts” syntax and thus safe.

**Consts**

- initial-current :: thread-id-t
- initial-obj :: obj-id-t \( \Rightarrow \) obj-t

**Definition** \( s0 :: \text{state-t where} \)

\( s0 \equiv (\{ /\text{sp-impl-subj-subj} = \text{Policy.sp-spec-subj-subj}, /\text{sp-impl-subj-obj} = \text{Policy.sp-spec-subj-obj} , \}

EURO-MILS D31.1 Page 33 of 44
current = initial-current,
obj = initial-obj.
thread = \lambda - . (| ev-counter = 0 |)

lemma initial-invariant:
shows atomic-step-invariant s0
(proof)

4.8.2 Types for instantiation of the generic model

To simplify formulations, we include the state invariant \textit{atomic-step-invariant} in the state data type. The initial state \(s0\) serves as witness that \textit{rstate-t} is non-empty.

typedef (overloaded) \textit{rstate-t} = \{ s . atomic-step-invariant s \}
(proof)

definition abs : state-t \Rightarrow \textit{rstate-t} (↑ -) where abs = Abs-rstate-t
definition rep : \textit{rstate-t} \Rightarrow state-t (↓ -) where rep = Rep-rstate-t

lemma rstate-invariant:
shows atomic-step-invariant (↓s)
(proof)

lemma rstate-down-up[simp]:
shows (↑↓s) = s
(proof)

lemma rstate-up-down[simp]:
assumes atomic-step-invariant s
shows (↓↑s) = s
(proof)

A CISK action is identified with an interrupt point.

type-synonym \textit{ract-int} = int-point-t
definition \textit{rcurrent} : \textit{rstate-t} \Rightarrow thread-id-t where
\textit{rcurrent} s a \equiv current (↓s)
definition \textit{rstep} : \textit{rstate-t} \Rightarrow \textit{ract-int} \Rightarrow \textit{rstate-t} where
\textit{rstep} s a \equiv ↑(atomic-step (↓s) a)

Each CISK domain is identified with a thread id.

type-synonym \textit{rdom-t} = thread-id-t

definition visible-obj-t = VALUE obj-t | EXCEPTION
type-synonym \textit{routput-t} = \textit{page-t} \Rightarrow \textit{visible-obj-t}
definition \textit{routput-f} : \textit{rstate-t} \Rightarrow \textit{ract-int} \Rightarrow \textit{routput-t} where
\textit{routput-f} s a p \equiv if sp-impl-subj-obj (↓s) (partition (rcurrent s)) (PAGE p) READ then
VALUE (obj (↓s) (PAGE p))
else
EXCEPTION

The precondition for the generic model. Note that \textit{atomic-step-invariant} is already part of the state.
D31.1 – Formal Specification of a Generic Separation Kernel

**Definition** rprecondition :: rstate-t ⇒ rdom-t ⇒ raction-t ⇒ bool where
rprecondition s d a ≡ atomic-step-precondition (↓s) d a

**Abbreviation** rinvariant
where rinvariant s ≡ True — The invariant is already in the state type.

Translate view-partitioning and interaction-allowed relations.

**Definition** rvpeq :: rdom-t ⇒ rstate-t ⇒ rstate-t ⇒ bool where
rvpeq u s1 s2 ≡ vpeq (partition u) (↓s1) (↓s2)

**Definition** rifp :: rdom-t ⇒ rdom-t ⇒ bool where
rifp u v = Policy.ifp (partition u) (partition v)

**Context Switches**

**Definition** rcswitch :: nat ⇒ rstate-t ⇒ rstate-t where
rcswitch n s ≡ ↑((↓s) (mod.alt0 current := (SOME t . True) (\s. True)))

**4.8.3 Possible action sequences**

An SK-IPC consists of three atomic actions PREP, WAIT and BUF with the same parameters.

**Definition** is-SK-IPC :: raction-t list ⇒ bool where
is-SK-IPC aseq ≡ ∃ dir partner page . aseq ≡ [SK-IPC dir PREP partner page, SK-IPC dir WAIT partner page, SK-IPC dir (BUF (SOME page′) . True)) partner page]

An SK-EV-WAIT consists of three atomic actions, one for each of the stages EV-PREP, EV-WAIT and EV-FINISH with the same parameters.

**Definition** is-SK-EV-WAIT :: raction-t list ⇒ bool where
is-SK-EV-WAIT aseq ≡ ∃ consume . aseq ≡ [SK-EV-WAIT EV-PREP consume , SK-EV-WAIT EV-WAIT consume , SK-EV-WAIT EV-FINISH consume ]

An SK-EV-SIGNAL consists of two atomic actions, one for each of the stages EV-SIGNAL-PREP and EV-SIGNAL-FINISH with the same parameters.

**Definition** is-SK-EV-SIGNAL :: raction-t list ⇒ bool where
is-SK-EV-SIGNAL aseq ≡ ∃ partner . aseq ≡ [SK-EV-SIGNAL EV-SIGNAL-PREP partner, SK-EV-SIGNAL EV-SIGNAL-FINISH partner]

The complete attack surface consists of IPC calls, events, and noops.

**Definition** rAS-set :: raction-t list set where
rAS-set ≡ { aseq . is-SK-IPC aseq ∨ is-SK-EV-WAIT aseq ∨ is-SK-EV-SIGNAL aseq } ∪ {[]}

**4.8.4 Control**

When are actions aborting, and when are actions waiting. We do not currently use the set-error-code function yet.

**Abbreviation** raborting
where raborting s ≡ aborting (↓s)

**Abbreviation** rwaiting
where rwaiting s ≡ waiting (↓s)

**Definition** rset-error-code :: rstate-t ⇒ raction-t ⇒ rstate-t where
rset-error-code s a ≡ s

Returns the set of threads that are involved in a certain action. For example, for an IPC call, the WAIT stage synchronizes with the partner. This partner is involved in that action.
**definition** \( rkinvolved :: \text{int-point-t} \Rightarrow \text{rdom-t set} \)

\[
\begin{align*}
\text{where } rkinvolved a & \equiv \\
\text{case } a \text{ of } \text{SK-IPC dir WAIT partner page} & \Rightarrow \{ \text{partner} \} \\
| \text{SK-EV-SIGNAL EV-SIGNAL-FINISH partner} & \Rightarrow \{ \text{partner} \} \\
| - & \Rightarrow \{ \}
\end{align*}
\]

**abbreviation** \( rimvolved :: \text{int-point-t option} \Rightarrow \text{rdom-t set} \)

\[
\begin{align*}
\text{where } rimvolved & \equiv \text{Kernel.involved } rkinvolved
\end{align*}
\]

4.8.5 Discharging the proof obligations

**lemma** \( \text{inst-vpeq-rel} \):

\[
\begin{align*}
\text{shows } \text{rvpeq-refl} \colon & \text{rvpeq } u \ s \ s \\
\text{and } \text{rvpeq-sym} \colon & \text{rvpeq } u \ s_1 \ s_2 \implies \text{rvpeq } u \ s_2 \ s_1 \\
\text{and } \text{rvpeq-trans} \colon & \left[ \left[ \text{rvpeq } u \ s_1 \ s_2; \text{rvpeq } u \ s_2 \ s_3 \right] \right] \implies \text{rvpeq } u \ s_1 \ s_3 \\
\langle \text{proof} \rangle
\end{align*}
\]

**lemma** \( \text{inst-ifp-refl} \):

\[
\begin{align*}
\text{shows } \forall u . \text{rifp } u \ u \\
\langle \text{proof} \rangle
\end{align*}
\]

**lemma** \( \text{inst-step-atomicity [simp]} \):

\[
\begin{align*}
\text{shows } \forall s \ a . \text{rcurrent } (\text{rstep } s \ a) = \text{rcurrent } s \\
\langle \text{proof} \rangle
\end{align*}
\]

**lemma** \( \text{inst-weakly-step-consistent} \):

\[
\begin{align*}
\text{assumes } \text{rvpeq } u \ s \ t \\
\text{and } \text{rvpeq } (\text{rcurrent } s) \ s \ t \\
\text{and } \text{rcurrent } s = \text{rcurrent } t \\
\text{and } \text{rprecondition } s \ (\text{rcurrent } s) \ a \\
\text{and } \text{rprecondition } t \ (\text{rcurrent } t) \ a \\
\text{shows } \text{rvpeq } u \ (\text{rstep } s \ a) \ (\text{rstep } t \ a) \\
\langle \text{proof} \rangle
\end{align*}
\]

**lemma** \( \text{inst-local-respect} \):

\[
\begin{align*}
\text{assumes } \neg \text{ifp} : & \neg \text{rifp } (\text{rcurrent } s) \ u \\
\text{and } \text{prec} : & \text{rprecondition } s \ (\text{rcurrent } s) \ a \\
\text{shows } \text{rvpeq } u \ s \ (\text{rstep } s \ a) \\
\langle \text{proof} \rangle
\end{align*}
\]

**lemma** \( \text{inst-output-consistency} \):

\[
\begin{align*}
\text{assumes } \text{rvpeq} : & \text{rvpeq } (\text{rcurrent } s) \ s \ t \\
\text{and } \text{current-eq} : & \text{rcurrent } s = \text{rcurrent } t \\
\text{shows } \text{routput-f } s \ a = \text{routput-f } t \ a \\
\langle \text{proof} \rangle
\end{align*}
\]

**lemma** \( \text{inst-cswitch-independent-of-state} \):

\[
\begin{align*}
\text{assumes } \text{rcurrent } s = \text{rcurrent } t \\
\text{shows } \text{rcurrent } (\text{rcswitch } n \ s) = \text{rcurrent } (\text{rcswitch } n \ t)
\end{align*}
\]
lemma inst-cswitch-consistency:
assumes rvpeq u s t
shows rvpeq u (rcswitch n s) (rcswitch n t)

For the PREP stage (the first stage of the IPC action sequence) the precondition is True.

lemma prec-first-IPC-action:
assumes is-SK-IPC aseq
shows rprecondition s d (hd aseq)

For the the first stage of the EV-WAIT action sequence the precondition is True.

lemma prec-first-EV-WAIT-action:
assumes is-SK-EV-WAIT aseq
shows rprecondition s d (hd aseq)

For the first stage of the EV-SIGNAL action sequence the precondition is True.

lemma prec-first-EV-SIGNAL-action:
assumes is-SK-EV-SIGNAL aseq
shows rprecondition s d (hd aseq)

When not waiting or aborting, the precondition is “1-step inductive”, that is at all times the precondition holds initially (for the first step of an action sequence) and after doing one step.

lemma prec-after-IPC-step:
assumes prec: rprecondition s (rcurrent s) (aseq ! n)
and n-bound: Suc n < length aseq
and IPC: is-SK-IPC aseq
and not-aborting: ¬raborting s (rcurrent s) (aseq ! n)
and not-waiting: ¬rwaiting s (rcurrent s) (aseq ! n)
shows rprecondition (rstep s (aseq ! n)) (rcurrent s) (aseq ! Suc n)

When not waiting or aborting, the precondition is 1-step inductive.

lemma prec-after-EV-WAIT-step:
assumes prec: rprecondition s (rcurrent s) (aseq ! n)
and n-bound: Suc n < length aseq
and IPC: is-SK-EV-WAIT aseq
and not-aborting: ¬raborting s (rcurrent s) (aseq ! n)
and not-waiting: ¬rwaiting s (rcurrent s) (aseq ! n)
shows rprecondition (rstep s (aseq ! n)) (rcurrent s) (aseq ! Suc n)

When not waiting or aborting, the precondition is 1-step inductive.

lemma prec-after-EV-SIGNAL-step:
assumes prec: rprecondition s (rcurrent s) (aseq ! n)
and n-bound: Suc n < length aseq
and SIGNAL: is-SK-EV-SIGNAL aseq
and not-aborting: ¬raborting s (rcurrent s) (aseq ! n)
and not-waiting: ¬rwaiting s (rcurrent s) (aseq ! n)
shows rprecondition (rstep s (aseq ! n)) (rcurrent s) (aseq ! Suc n)
lemma on-set-object-value:
  shows sp-impl-subj-subj (set-object-value ob val s) = sp-impl-subj-subj s
  and sp-impl-subj-obj (set-object-value ob val s) = sp-impl-subj-obj s
{proof}

lemma prec-IPC-dom-independent:
assumes current s \neq d
  and atomic-step-invariant s
  and atomic-step-precondition s d a
shows atomic-step-precondition (atomic-step-ipc (current s) dir stage partner page s) d a
{proof}

lemma prec-ev-signal-dom-independent:
assumes current s \neq d
  and atomic-step-invariant s
  and atomic-step-precondition s d a
shows atomic-step-precondition (atomic-step-ev-signal (current s) partner s) d a
{proof}

lemma prec-ev-wait-one-dom-independent:
assumes current s \neq d
  and atomic-step-invariant s
  and atomic-step-precondition s d a
shows atomic-step-precondition (atomic-step-ev-wait-one (current s) s) d a
{proof}

lemma prec-ev-wait-all-dom-independent:
assumes current s \neq d
  and atomic-step-invariant s
  and atomic-step-precondition s d a
shows atomic-step-precondition (atomic-step-ev-wait-all (current s) s) d a
{proof}

lemma prec-dom-independent:
shows \forall s d a a'. rcurrent s \neq d \land rprecondition s d a --> rprecondition (rcswitch n s) d a
{proof}

lemma ipc-precondition-after-cswitch[simp]
shows ipc-precondition d dir partner page ((↓ s)([current := new-current]))
  = ipc-precondition d dir partner page (↓ s)
{proof}

lemma precondition-after-cswitch
shows \forall s d n a. rprecondition s d a --> rprecondition (rcswitch n s) d a
{proof}

lemma aborting-switch-independent:
shows \forall n s. raborting (rcswitch n s) = raborting s
{proof}
lemma waiting-switch-independent:
shows \forall n s. rwaiting (rcswitch n s) = rwaiting s
{proof}

lemma aborting-after-IPC-step:
assumes d1 \neq d2
shows aborting (atomic-step-ipc d1 dir stage partner page s) d2 a = aborting s d2 a
{proof}
lemma waiting-after-IPC-step:
assumes d1 ≠ d2
shows waiting (atomic-step-ipc d1 dir stage partner page s) d2 a = waiting s d2 a
(proof)

lemma raborting-consistent:
shows ∀ s t u. rvpeq u s t → raborting s u = raborting t u
(proof)

lemma aborting-dom-independent:
  assumes rcurrent s ≠ d
  shows raborting (rstep s a) d a' = raborting s d a'
(proof)

lemma ipc-precondition-of-partner-consistent:
assumes vpeq ∀ d ∈ rkinvolved (SK-IPC dir WAIT partner page) . rvpeq d s t
shows ipc-precondition partner dir' u page' (↓ s) = ipc-precondition partner dir' u page' ↓ t
(proof)

lemma ev-signal-precondition-of-partner-consistent:
assumes vpeq ∀ d ∈ rkinvolved (SK-EV-SIGNAL EV-SIGNAL-FINISH partner) . rvpeq d s t
shows ev-signal-precondition partner u (↓ s) = ev-signal-precondition partner u (↓ t)
(proof)

lemma waiting-consistent:
shows ∀ s t u a . rvpeq (rcurrent s) s t ∧ (∀ d ∈ rkinvolved a . rvpeq d s t)
∧ rvpeq u s t
→ rwaiting s u a = rwaiting t u a
(proof)

lemma ipc-precondition-ensures-ifp:
assumes ipc-precondition (current s) dir partner page s
and atomic-step-invariant s
shows rifp partner (current s)
(proof)

lemma ev-signal-precondition-ensures-ifp:
assumes ev-signal-precondition (current s) partner s
and atomic-step-invariant s
shows rifp partner (current s)
(proof)

lemma involved-ifp:
shows ∀ s a . ∀ d ∈ rkinvolved a . rprecondition s (rcurrent s) a → rifp d (rcurrent s)
(proof)

lemma spec-of-waiting-ev:
shows ∀ s a. rwaiting s (rcurrent s) (SK-EV-WAIT EV-FINISH EV-CONSUME-ALL)
→ rstep s a = s
(proof)

lemma spec-of-waiting-ev-w:
shows ∀ s a. rwaiting s (rcurrent s) (SK-EV-WAIT EV-WAIT EV-CONSUME-ALL)
→ rstep s (SK-EV-WAIT EV-WAIT EV-CONSUME-ALL) = s
lemma spec-of-waiting:
shows ∀ s a. rwaiting s (rcurrent s) a → rstep s a = s

4.9 Link implementation to CISK: the specific separation kernel is an interpretation of the generic model.

theory Link-separation-kernel-model-to-CISK
imports Separation-kernel-model
begin

We show that the separation kernel instantiation satisfies the specification of CISK.

theorem CISK-proof-obligations-satisfied:
shows Controllable-Interruptible-Separation-Kernel
rstep
output-f
↑s0
rcurrent
rcswitch
rkinvolved
rifp
rvpeq
rAS-set
rinvariant
rprecondition
raborting
rwaiting
rset-error-code

Now we can instantiate CISK with some initial state, interrupt function, etc.

interpretation Inst:
Controllable-Interruptible-Separation-Kernel
rstep — step function, without program stack
output-f — output function
↑s0 — initial state
rcurrent — returns the currently active domain
rcswitch — switches the currently active domain
(=) 42 — interrupt function (yet unspecified)
rkinvolved — returns a set of threads involved in the give action
rifp — information flow policy
rvpeq — view partitioning
rAS-set — the set of valid action sequences
rinvariant — the state invariant
rprecondition — the precondition for doing an action
raborting — condition under which an action is aborted
rwaiting — condition under which an action is delayed
rset-error-code — updates the state. Has no meaning in the current model.

The main theorem: the instantiation implements the information flow policy ifp.

theorem risecure:
Inst.isecure
5 Related Work

We consider various definitions of intransitive (I) noninterference (NI). This overview is by no means intended to be complete. We first prune the field by focusing on INI with as granularity the domains: if the security policy states the act “\(v \sim u\)”, this means domain \(v\) is permitted to flow any information it has at its disposal to \(u\). We do not consider language-based approaches to noninterference [26], which allow finer granularity mechanisms (i.e., flowing just a subset of the available information). Secondly, several formal verification efforts have been conducted concerning properties similar and related to INI such as no-exfiltration and no-infiltration [9]. Heitmeyer et al. prove these properties for a separation kernel in a Common Criteria certification process [11] (which kernel and which EAL is not clear). Martin et al. proved separation properties over the MASK kernel [18] and Shapiro and Weber verified correctness of the EROS confinement mechanism [28]. Klein provides an excellent overview of OS’s for which such properties have been verified [13]. Thirdly, INI definitions can be built upon either state-based automata, trace-based models, or process algebraic models [30]. We do not focus on the latter, as our approach is not based on process algebra.

Transitive NI was first introduced by Goguen and Meseguer in 1982 [7] and has been the topic of heavy research since. Goguen and Meseguer tried to extend their definition with an unless construct to allow such policies [8]. This construct, however, did not capture the notion of INI [17]. The first commonly accepted definition of INI is Rushby’s purging-based definition IP-secure [24]. IP-secure has been applied to, e.g., smartcards [27] and OS kernel extensions [7]. To the best of our knowledge, Rushby’s definition has not been applied in a certification context. Rushby’s definition has been subject to heavy scrutiny [22], [29] and a vast array of modifications have been proposed.

Roscoe and Goldsmith provide CSP-based definitions of NI for the transitive and the intransitive case, here dubbed as lazy and mixed independence. The latter one is more restrictive than Rushby’s IP-secure. Their critique on IP-secure, however, is not universally accepted [7]. Greve at al. provided the GWV framework developed in ACL2 [9]. Their definition is a non-inductive version of noninterference similar to Rushby’s step consistency. GWV has been used on various industrial systems. The exact relation between GWV and (I)P-secure, i.e., whether they are of equal strength, is still open. The second property, Declassification, means whether the definition allows assignments in the form of \(l := \text{declassify}(h)\) (where we use Sabelfelds [26] notation for high and low variables). Information flows from \(h\) to \(l\), but only after it has been declassified. In general, NI is coarser than declassification. It allows where downgrading can occur, but now what may be downgraded [17]. Mantel provides a definition of transitive NI where exceptions can be added to allow de-classification by adding intransitive exceptions to the security policy [17].

To deal with concurrency, definitions of NI have been proposed for Non-Deterministic automata. Von Oheimb defined noninfluence for such systems. His definition can be regarded as a “non-deterministic version” of IP-secure. Engelhardt et al. defined nTA-secure, the non-deterministic version of TA-secure. Finally, some notions of INI consider models that are in a sense richer than similar counterparts. Leslie extends Rushby’s notion of IP-secure for a model in which the security policy is Dynamic. Eggert et al. defined i-secure, an extension of IP-secure. Their model extends Rushby’s model (Mealy machines) with Local security policies. Murray et al. extends Von Oheimb definition of noninfluence to apply to a model that does not assume a static mapping of actions to domains. This makes it applicable to OS’s, as in such a setting such a mapping does not exist [20]. NI-OS has been applied to the seL4 separation kernel [20], [14].

Most definitions have an associated methodology. Various methodologies are based on unwinding [8]. This breaks down the proof of NI into smaller proof obligations (PO’s). These PO’s can be checked by some manual proof [24], [10], model checking [32] or dedicated algorithms [5]. The methodology of
Murray et al. is a combination of unwinding, automated deduction and manual proofs. Some definitions are undecidable and have no suitable unwinding.

We are aiming to provide a methodology for INI based on a model that is richer in detail than Mealy machines. This places our contribution next to other works that aim to extend IP-security [15], [4] in Figure 2. Similar to those approaches, we take IP-security as a starting point. We add kernel control mechanisms, interrupts and context switches. Ideally, we would simply prove IP-security over CISK. We argue that this is impossible and that a rephrasing is necessary.

Our ultimate goal — certification of PikeOS — is very similar to the work done on seL4 [20]–[19]. There are two reasons why their approach is not directly applicable to PikeOS. First, seL4 has been developed from scratch. A Haskell specification serves as the medium for the implementation as well as the system model for the kernel [6]. C code is derived from a high level specification. PikeOS, in contrast, is an established industrial OS. Secondly, interrupts are mostly disabled in seL4. Klein et al. sidestep dealing with the verification complexity of interrupts by using a mostly atomic API [14]. In contrast, we aim to fully address interrupts.

With respect to attempts to formal operating system verifications, notable works are also the Verisoft I project [1] where also a weak form of a separation property, namely fairness of execution was addressed [3].

6 Conclusion

We have introduced a generic theory of intransitive non-interference for separation kernels with control as a series of locales and extensible record definitions in order to achieve a modular organization. Moreover, we have shown that it can be instantiated for a simplistic API consisting of IPC and events.

In the ongoing EURO-MILS project, we will extend this generic theory in order make it sufficiently rich to be instantiated with a realistic functional model of PikeOS.

6.0.1 Acknowledgement.

This work corresponds to the formal deliverable D31.1 of the Euro-MILS project funded by the European Union’s Programme

\[ FP7/2007 \rightarrow 2013 \]

under grant agreement number ICT-318353.

References


