

INSTITUT FÜR INFORMATIK

DER LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Lehr- und Forschungseinheit für theoretische Informatik



Bachelor-Thesis
in Computer Science

Noninterference in the take-grant model for the seL4 microkernel

Andrea Kuchar

Advisor: Dr Martin Hofmann, PD Dr Ulrich Schöpp
Submission Date: 07-27-2018

Declaration of authorship

I hereby declare that the thesis submitted is my own unaided work. All direct or indirect sources used are acknowledged as references.

Munich, the 07-27-2018

.....
Andrea Kuchar

Abstract

The thesis investigates the question if the specification of the seL4 access control system is strong enough to verify the Noninterference property on it. Using the specification of the extended Take-Grant-Protection Model [2] I show the Noninterference property [7] on each of it's system operations. As the specifications and proofs of the take-grant model are developed in the theorem proof assistant Isabelle/HOL I use the same to formalise my datatypes and functions.

List of Figures

1	Internal representation of application	4
2	Sample system architecture	5
3	take rule	6
4	grant rule	6
5	create rule	6
6	remove rule	7
7	CDT	7
8	Noninterference of Write 1	13
9	No confidentiality for Remove	14
10	Objects and Methods in the kernel	16
11	Noninterference for Create on Untyped Memory Objects	17
12	Noninterference for Create on object types \neq Untyped Memory Objects . .	18
13	Noninterference for Create on object types = AEP \vee SPage	19
14	Noninterference for Grant on an TCB, Synchronous IPC Endpoint, CNode, VSpace or Interrupt Controller object	20
15	Noninterference for Grant on an object \neq TCB, SEP, CNode, VSpace, IContr, SPage or AEP object	21
16	Noninterference for Grant on an Asynchronous IPC Endpoint object	22
17	Noninterference for Write on a TCB, Synchronous IPC Endpoint or Interrupt Handler object	23
18	Noninterference for Write on objects \neq TCB, SEP, IHandl, SPage and AEP	24
19	Noninterference for Write on an object = AEP executed from an entity \in Domain 2	25
20	Noninterference for Write on an object = AEP executed from an entity \in D1	26
21	Noninterference for Read on a TCB or Synchronous IPC Endpoint object . .	27
22	Noninterference for Read on objects \neq TCB, Asynchronous IPC Endpoint, Synchronous IPC Endpoint or Shared Page	28
23	Noninterference for Read on object types = Asynchronous IPC Endpoint executed from Domain 1	29
24	Noninterference for Read on object types = Asynchronous IPC Endpoint executed from Domain 2	30
25	Noninterference for Remove on object types = CNode, VSpace or IContr. The removed capability points to an entity in the same domain	31
26	Noninterference for Remove on object types = CNode, VSpace or IContr. The removed capability points to an entity outside the H domain	32
27	Noninterference for Remove on objects \neq CNode, VSpace and IContr. The removed capability points to an entity in the same domain	33
28	Noninterference for Remove on object types \neq CNode, VSpace or IContr. The removed capability points to an entity outside the H domain	34

Contents

Abstract	II
List of Figures	III
1 Introduction	1
1.1 Motivation	1
1.2 Aim of the thesis	1
1.3 Structure of the thesis	2
2 Requirements	3
2.1 The seL4 Microkernel	3
2.1.1 System Calls	3
2.1.2 Kernel Objects	3
2.1.3 Memory Allocation Model	5
2.2 The Take-Grant Model	6
2.2.1 The classical Model	6
2.2.2 Take-Grant specified for the seL4	6
2.3 Noninterference	7
3 Formalisation of the Take-Grant Model	9
3.1 Capabilities	9
3.2 System Operations	9
4 Formalisation of the Noninterference Model	12
5 Validation of Noninterference	13
6 Redesign of the take-grant-model	14
7 Validation with the new model	17
7.1 Create	17
7.1.1 Create on UMO	17
7.1.2 Create on all other object types inside a domain	18
7.1.3 Create on Asynchronous IPC Endpoint or Shared Page objects	19
7.2 Grant	19
7.2.1 Grant on TCB, SEP, CNode, VSpace or IContr objects	20
7.2.2 Grant on other objects inside a domain	21
7.2.3 Grant on Asynchronous IPC Endpoint or Shared Page objects	22
7.3 Write	23
7.3.1 Write on TCB, SEP or IHandl objects	23
7.3.2 Write on objects \neq TCB, SEP, IHandl, SPage and AEP	24
7.3.3 Write on AEP or SPage objects from Domain 2	25
7.3.4 Write on an AEP or SPage object from Domain 1	26
7.4 Read	27
7.4.1 Read on TCB or Synchronous IPC Endpoint objects	27
7.4.2 Read on other object types inside a domain	28
7.4.3 Read on AEP or SPage objects from Domain 1	29
7.4.4 Read on AEP or SPage objects from Domain 2	30
7.5 Remove	31
7.5.1 Remove on CNode, VSpace or Interrupt Controller objects	31
7.5.2 Remove on objects \neq CNode, VSpace and Interrupt Controller	33
7.6 Revoke	35

8 Conclusion	35
References	36

1 Introduction

1.1 Motivation

Nowadays our society becomes increasingly dependent on computer systems. In more and more areas small computers take over control. Whether it's our SmartTV, car or the control of the lights in our home. We are forced to confront ourselves with the topic how secure and reliable these systems are.

Especially if we entrust our lives to a computer this gets an essential meaning. From board-computers in planes or cars we want to expect that they are free from defects and unhackable. But this is not the reality. We know about cars whose board-computers can be taken over easily with a smartphone from the car next to it.

A key component in developing secure systems is the operating-system (OS) kernel of the system. The kernel has full access to hardware resources. One defect in the kernel can have the consequence that the security and reliability of the entire system can be lost.

The weakness of most previous kernels was their huge amount of code and mostly their monolithic design. This makes it impossible to review or verify the code. Monolithic designs have their weak point in the fact that not only fundamental functions as inter-process communication, scheduling or memory management are implemented in the kernel mode but also functions like driver for hardware or virtual filesystems are integrated in it. This makes the system more vulnerable for bugs. One crashed module can lead to a crash of the entire system.

The motivation behind microkernels is to reduce the possibility of bugs in the kernel code through reducing the code to an amount as minimal as possible and excluding functions from the kernel mode. With less code it becomes more feasible to guarantee the absence of defects within the kernel through formal verification.

Due to the fact that we feed our smartphones, tablets, board-computers, ... with growing amounts of sensitive informations like bank data, passwords, e-mails, chats, ... the significance of security in the area of embedded systems increases.

Through isolation of small subsystems, like it is done in microkernels, the security already can be raised to a higher level. With testing one can depict an huge amount of bugs. But as Dijkstra said "Testing can only show the presence, not the absence, of bugs." [8]

Like I already mentioned less lines of codes make it more feasible to verify it relating to its specification. The seL4 microkernel is the first microkernel whose correctness is formally verified. It's a high-assurance, high-performance microkernel, primarily developed, maintained and formally verified by NICTA (now Trustworthy Systems Group at Data61) for secure embedded systems. Its security model is based on the take-grant model, which was extended for being able to reason about kernel memory consumption of components.

1.2 Aim of the thesis

With this thesis I want to survey if the extended take-grant model is strong enough to show the noninterference property on it.

The security property of noninterference ensures that there is no unwanted information flow within a system. The take-grant model is an access control model. Therefore its duty is to "control" the access or the transfer of access on objects of a system. The noninterference property assured that there is no way information can flow to undesirable parties.

The thesis should investigate the different system operations of the model regarding the thereby occurring information flow.

With the collected information I want to answer two questions. First if the noninterference property can be verified with the existing model and second if the noninterference property is fulfilled.

1.3 Structure of the thesis

At the beginning I want to give an survey of the seL4 kernel, its set-up, the implementation of services and the memory management. For a better comprehension I then give a brief overview of the take-grant and the noninterference model. Chapter 3 focuses on the formalisation of the take-grant model an chapter 4 on the formalisation of the noninterference model.

From chapter 5 on I turn to the validation of the noninterference property. In chapter 7 the validation is subdivided into the different systemoperations. To show the property for the model I am going to extend the model in chapter 6.

Finally I'll take a short resume and give a prospect on the possibilities to enhance this topic.

2 Requirements

2.1 The seL4 Microkernel

The seL4 [6] is a small operation system kernel. It's based on the in the 1990s developed L4 microkernel and provides a minimal number of services to applications, such as abstractions for virtual address spaces, threads, inter process communication (IPC).

Each abstraction is implemented by a kernel object with methods dependent on the abstraction it supplies. The objects can be named and accessed by capabilities which are also stored in kernel objects called *CNodes*.

Each capability contains a target object and potentially several access rights. The access rights can be **Read**, **Write**, **Grant** and **Create**. By invoking a capability that points to the kernel object with an corresponding method name, applications can invoke system calls. As arguments these system calls can have data or other capabilities.

2.1.1 System Calls

Kernel provided system calls:

- **send()**: The system call argument is delivered to the target object and the application is allowed to continue. If the target is not able to receive and/or process the arguments immediately, the sending application will be blocked until the arguments can be delivered.
- **NBSend()**: Like **send()**. Exception: If the message is not deliverable it's silently dropped.
- **Call()**: Like **send()** but the application is blocked until the object provides a response, or the receiving application replies.
If the argument is delivered to an application via Endpoint the receiver needs the right to respond to the sender. So in this case an additional capability is added to the arguments.
- **Wait()**: If the target object is not ready **Wait()** is used by an application to block until the object is ready.
- **Reply()**: Used to respond to a **Call()**, using the capability generated by the **Call()** operation.
- **ReplyWait()**: As a combination of **Reply()** and **Wait()** it's efficient for the common case that replying to a request and waiting for the next can be performed in a single system call.

2.1.2 Kernel Objects

The kernel implements several objects to allocate the system operations [6].

- **CNodes**

The capabilities to invoke system calls are stored in *CNodes*. When created they get a fixed number of slots that can be empty or contain a capability. The kernel conducts a **Capability Derivation Tree** (CDT) to keep records about the created capabilities and their associations. This is required for the revoke operation.

They have the following operations:

- **Mint()**

creates a copy of an existing capability. The new capability is placed in a specified CNode slot and may have less rights than the parent capability. In the CDT the capability is placed as child of the original one.

- **Copy()**
is similar to the *Mint* operation. But the new capability has the same rights as the original one and in the CDT it's represented as a sibling of it.
- **Move()**
can maneuver a capability between two specified slots.
- **Mutate()**
moves the capability similar to *Move()* and is able to reduce it's rights like it's done in *Mint()* without an original copy remaining.
- **Rotate()**
moves two capabilities between three slots. Replaces two *Move()* operations.
- **Delete()**
can remove a capability from a specified slot.
- **Revoke()**
is used to remove a complete part of the CDT. From a defined capability on all children from the capability in the CDT are removed with *Delete()*.
- **Recycle()**
revokes all outstanding capabilities and reconfigures the object to its initial state. So the object can be reused in for another purpose.

• IPC Endpoints

Endpoints are used for the *interprocess communication* between threads. They can be divided into **synchronous (EP)** and **asynchronous (AEP)** endpoints. Threads in the seL4 kernel are grouped into security domains. Interprocess communication between different domains is only realised via AEPs. Generally capabilities to endpoints can be restricted to be read - or write - only.

• TCP

A thread of execution in seL4 is represented by a *thread control block*. It's always associated with a CSpace (provides the capabilities required to manipulate the kernel objects) and a VSpace (provides the virtual memory environment required to contain the code and data application).

The TCB object has the following methods:

`CopyRegisters()`, `ReadRegisters()`, `WriteRegisters()`, `SetPriority()`, `SetIPCBuffer()`, `SetSpace()`, `Configure()`, `Suspend()`, `Resume()`

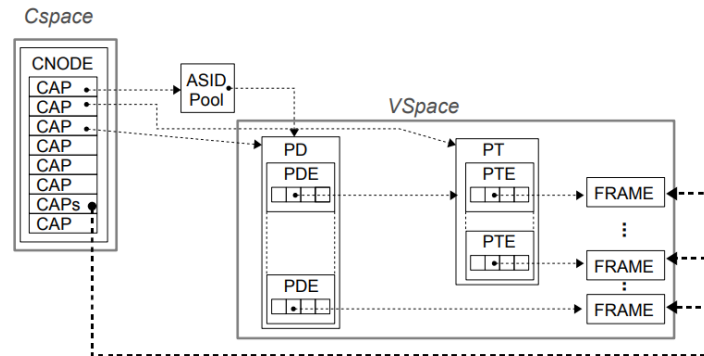


Figure 1: Internal representation of an application in seL4 [3]

• Virtual Memory

Objects in the *virtual address space* (VSpace) implement services for the management of virtual memory which largely directly correspond to those of the hardware:

Page Directory, Page Table, Page, ASID Control, ASID Pool

Figure 1 shows how they are connected.

- **Interrupt Objects**

Device driver applications require **Interrupt Objects** to be capable of receiving and acknowledging interrupts from hardware devices.

- **Untyped Memory**

Untyped memory objects (UMO) seclude a fixed-sized, size-aligned, continuous region of the physical memory. Each object can be divided into a group of smaller untyped memory objects. With **Retype()** a number of new kernel objects are created. It also returns capabilities to the new objects if it succeeds.

2.1.3 Memory Allocation Model

A special characteristic of the seL4 is that the memomry for kernel objects is not allocated dynamically. A goal was to isolate physical memory access between applllications and to control the amount of physical memory that applications can use.

To accomplish it applications get fixed sized memory reagonns they have to control by themselves.

Capabilities on Untyped Memory Objects (UMO) are needed to create new objects. So applications need the capabilities on UMOs to create new objects. After creation the objects have a fix amount of memory they can use.

At boot time the kernel pre-allocates all the memory required for the kernel to run. This includes the space for kernel code, data and kernel stack. The kernel then creates an *Initial User Thread* with associated CSpace and VSpace and hands over the remainig memory in form of capabilities on UMOs.

The Initial User Thread can create smaler sized UMOs out of an UMO or **retype** it into an other object type. The creator of new objects has full authority over the objects. This "full authority" depends on the object type.

Figure 2 shows a sample system architecture in which a resource manager running at user-level has the authority to the remaining untyped memory after boot strapping.

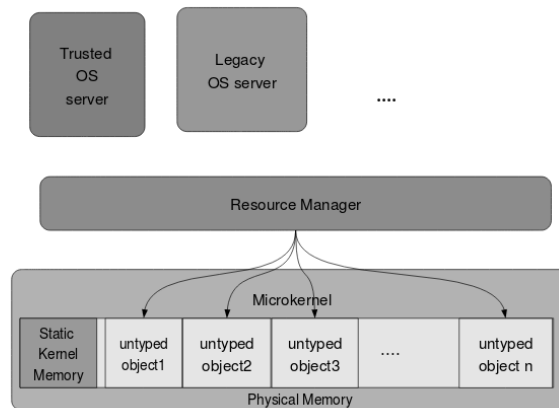


Figure 2: Sample System Configuration [2]

2.2 The Take-Grant Model

Protection or Access control models specify, analyse and implement security policies. The classical Take-Grant Model was primary introduced by Lipton and Snyder, 1977 in "A Linear Time Algorithm for Deciding Subject Security".

2.2.1 The classical Model

In the Take-Grant Model [2] subjects or objects are represented as nodes and authority as arcs in a directed graph that represents the system.

Rules for graph mutation represent the different system operations to modify the authority distribution. The most common rules in the classical model are *take*, *grant*, *create* and *remove*.

- **take rule:** Let S, X, Y be three distinct vertices in the protection graph with an arc, labelled with α , from X to Y and one labelled with γ from S to X , such that $t \in \gamma$.

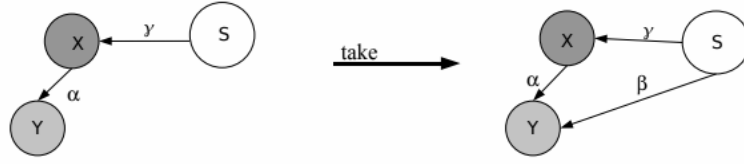


Figure 3: *Take* adds an edge from S to Y with the label $\beta \subseteq \alpha$. [2]

- **grant rule:** Let S, X, Y again be three distinct vertices in the graph with an arc, labelled with α , from S to Y and one labelled with γ from S to X , such that $g \in \gamma$.

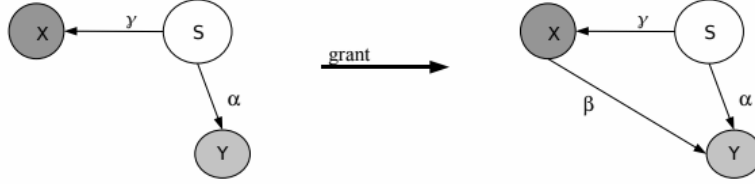


Figure 4: *Grant* adds an edge from X to Y with the label $\beta \subseteq \alpha$. [2]

- **create rule:** Let S be a vertex in the graph.

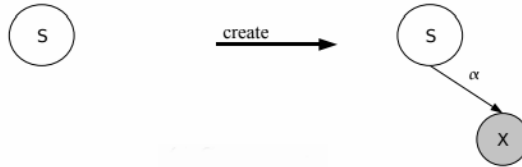


Figure 5: *Create* adds a new node X and an arc from S to X , labelled with α . [2]

- **remove rule:** Let S, X be vertices in the graph with an arc from S to X , labelled with α .

2.2.2 Take-Grant specified for the seL4

The Take-Grant Model specified in the paper "Noninterference for Operating System Kernels" [2] is a variant of the classical Take-Grant model.

From the modifications made the one on the *create rule* is the most important one. As I explained in chapter 2.1 authority in the kernel is implemented with capabilities. Adding

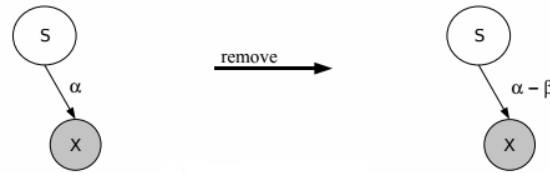


Figure 6: *Remove* deletes β labels from α or the arc itself if $\alpha - \beta = \{\}$. [2]

a new node to the protection graph in the model corresponds to the creation of a new object a capability pointing on it in the kernel. So the object executing the **create** operation needs a capability with **create** authority.

The *remove* rule was modified as it doesn't remove parts of labels anymore but the whole capability. That means the complete arc pointing on an object is removed.

To diminish authority a capability has to be removed and newly created with diminished authority.

With **retype** newly created capabilities are saved in a *Capability Derivation Tree* (CDT) as children of the UMO. A capability can be copied with the **mint** or **imitate** operation. A capability copied with **mint** is inserted in the CDT as Child of the original one. Those that are copied with **imitate** are siblings. Figure 7 shows a CDT where C1 and C2 are created from the UMO via **retype**. C3 and C4 are copied from C1 via **mint**. So they have the same or less authority as C1. C1' is copied from C1 via **imitate**. This operation transfers the same rights to the new capability. As a consequence the capability is inserted a sibling of C1.

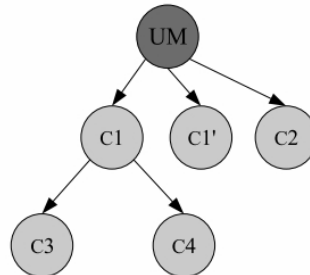


Figure 7: Example CDT with children and siblings [5]

To remove a set of capabilities the operation **revoke** was implemented.

With this operation **remove** is executed on every capability that is in the CDT below the target capability.

A speciality of the extended model is that objects and subjects are called *entities*.

The goal of the paper "Noninterference for Operating System Kernels" was to show that it is accomplishable to implement isolated subsystems using the mechanisms of the seL4 kernel. [2]

Isolated subsystems are implemented as a collection of *connected* entities. An entity that has *grant authority* on another one is connected with this entity. Authority can neither get in nor out of these isolated subsystems.

The exact specification of subsystems and entities follows in Chapter 3.

2.3 Noninterference

Noninterference is an enhancement of the information flow model, first published by Goguen and Meseguer in 1982 and updated in 1984. It ensures that objects and subject from different security levels don't interfere with those at other levels. In the model

variables are classified to be L (low security) or H (high security, private) variables. The goal is to prevent information from H variables from flowing to L variables.

I use the noninterference formulation of Geoffrey Smith [7]. It says "Program c satisfies noninterference if, for any memories μ and ν that agree on L variables, the memories produced by running c on μ and on ν also agree on L variables (provided that both runs terminate successfully)."

This means if in a program two states are equivalent on a low level domain they are still equivalent on this level after a program was executed.

Central to noninterference is the notion of a *policy* \rightsquigarrow . It specifies the allowed information flows between domains. $L \rightsquigarrow H$ if information is allowed to flow from domain L to domain H.

The model says two memories μ and ν that agree on L variables if they fulfill an equivalence relation $\mu \stackrel{L}{\sim} \nu$.

The exact formalisation of noninterference for the validation follows in chapter 4.

3 Formalisation of the Take-Grant Model

3.1 Capabilities

In the Take-Grant model for seL4 [2], where I got the formalisation from, the authors waived the usual differentiation between subjects and objects and called all kernel objects *entities*.

The entities memory address identifies them and is modeled as a natural number.

```
type_synonym entity_id = nat
```

With each capability a set of rights is associated. There are four access rights in the system model:

```
datatype rights = Read | Write | Grant | Create
```

- *Read* authorises the reading of information from another entity.
- *Write* authorises the writing of information to another entity.
- *Grant* authorises the passing of a capability to another entity.
- *Create* authorises the creation of new entities, which models the behavior of untyped memory objects.

A capability has two fields:

1. An identifier which names an target-entity
2. A set of rights which defines which system-operations the source-entity is authorised to perform on the target-entity.

```
record cap =   entity :: entity_id
              rights :: rights set
```

An entity has a set of capabilities:

```
record entity = caps :: cap set
```

The systems state includes two fields:

1. The *heap*, which stores the entities of the system like an array from address 0 up to and excluding *next_id*.
2. *next_id* contains slot for the next entity without overlapping with an existing one.

```
record state =   heap :: entity_id ⇒ entity
                next_id :: entity_id
```

3.2 System Operations

The data type `sysOps` defines the different system operations of the seL4.

```
datatype sysOps = SysNoOp entity_id
                | SysRead entity_id cap
                | SysWrite entity_id cap
                | SysCreate entity_id cap cap
                | SysGrant entity_id cap cap rights set
                | SysRemove entity_id cap cap
                | SysRevoke entity_id cap
```

The `entity_id` in each operation is the entity initiating the operation. The first named capability is the one that is being invoked. The second capability for `SysCreate` points to the target entity for the new capability. For `SysGrant` it's the passed capability and for `SysRemove` it's the one that has to be removed. The rights set in `SysGrant` necessary for the initiating entity to have the option only to transport a subset of the authority it offers to the receiver.

The `diminish` function applies this mask on the given access rights:

```
diminish :: "cap  $\Rightarrow$  rights set  $\Rightarrow$  cap" where
diminish c R  $\equiv$  c(rights := rights c  $\cap$  R)
```

`legal` defines on what terms any system operation is allowed.

```
legal :: "sysOPs  $\Rightarrow$  state  $\Rightarrow$  bool" where

    "legal (SysNoOp e) s = isEntityOf s e"
  | "legal (SysCreate e c1 c2) s = (isEntityOf s e  $\wedge$  c1, c2  $\subseteq$  caps_of s e  $\wedge$ 
    Grant  $\in$  rights c2  $\wedge$  Create  $\in$  rights c2)"
  | "legal (SysRead e c) s = (isEntityOf s e  $\wedge$  c  $\in$  caps_of s e  $\wedge$  Read
     $\in$  rights c)"
  | "legal (SysWrite e c) s = (isEntityOf s e  $\wedge$  c  $\in$  caps_of s e  $\wedge$  Write
     $\in$  rights c)"
  | "legal (SysGrant e c1 c2 r) s = (isEntityOf s e  $\wedge$  isEntityOf s (entity c1)
     $\wedge$  c1, c2  $\subseteq$  caps_of s e  $\wedge$  Grant  $\in$  rights c1)"
  | "legal (SysRemove e c1 c2) s = (isEntityOf s e  $\wedge$  c1  $\in$  caps_of s e)"
  | "legal (SysRevoke e c) s = isEntityOf s e  $\wedge$  c  $\in$  caps_of s e"
```

The function `isEntityOf` tests the existence of an `entity_id`, `caps_of` issues the set of all capabilities contained in the entity with the address `r` in state `s`.

The original executions of `SysRead` and `SysWrite` don't have an underlying function. For implying the noninterference property I have to include what happens if an entity reads or writes a value from another entity. For this purpose I defined a `readOperation` and a `writeOperation`.

The `step'` and `step` functions define the execution of a single system operation:

```
step' :: "sysOPs  $\Rightarrow$  state  $\Rightarrow$  state" where
    "step' (SysNoOp e) s = s"
  | "step' (SysRead e c) s = readOperation e c s"
  | "step' (SysWrite e c) s = writeOperation e c s"
  | "step' (SysCreat e c1 c2) s = createOperation e c1 c2 s"
  | "step' (SysGrant e c1 c2 R) s = grantOperation e c1 c2 R s"
  | "step' (SysRemove e c1 c2) s = removeOperation e c1 c2 s"
  | "step' (SysRevoke e c) s = revokeOperation e c s"
```

```
step :: "sysOps  $\Rightarrow$  state  $\Rightarrow$  state" where
step cmd s  $\equiv$  if legal cmd s then step' cmd s else s
```

The new defined functions `readOperation` and `writeOperation`:

```
readOperation :: "entity_id  $\Rightarrow$  cap  $\Rightarrow$  modify_state" where
"readOperation e c s  $\equiv$  s(| heap := (heap s)(e := (|caps = caps_of s e, eValue = value_of s (entity c)|)))"
```

```
writeOperation :: "entity_id  $\Rightarrow$  cap  $\Rightarrow$  modify_state" where
"writeOperation e c s  $\equiv$  s(| heap := (heap s)(entity c := (|caps = caps_of s (entity c), eValue = value_of s e|)|))"
```

The rest of the system operations stay as they are:

```
createOperation :: "entity_id  $\Rightarrow$  cap  $\Rightarrow$  cap  $\Rightarrow$  modify_state" where
createOperation e c1 c2 s  $\equiv$ 
    let nullEntity = (|cap = , eValue = NULL|) ;
        newCap = (|entity = next_id s, rights = all_rights|);
        newTarget = (|caps = newCap caps_of s (entity c2), eValue = NULL|)
    in s(heap := (heap s)(entity c2 := newTarget, next_id s := nullEntity), next_id := next_id s+1)"
```

```
grantOperation :: "entity_id  $\Rightarrow$  cap  $\Rightarrow$  cap  $\Rightarrow$  rights set  $\Rightarrow$  modify_state" where
"grantOperation e c1 c2 R s  $\equiv$ 
s(|heap := (heap s)(entity c1 := (|caps = diminish c2 R  $\cup$  caps_of s (entity c1), eValue = value_of s (entity c1)|)))"
```



```
removeOperation :: "entity_id  $\Rightarrow$  cap  $\Rightarrow$  cap  $\Rightarrow$  modify_state" where
"removeOperation c1 c2 s  $\equiv$  s( $\langle$ heap := (heap s)(entity c1 := ( $\langle$ caps = caps_of s (entity c1) - c2, eValue
= value_of s (entity c1) $\rangle$ ) $\rangle$ )"
```

4 Formalisation of the Noninterference Model

For the validation I have to formalise the noninterference property.

```
noninterference :: "bool" where
"noninterference  $\equiv \forall a l h s t s' t'. \text{reachable } s \wedge \text{reachable } t \wedge s \stackrel{l}{\sim} t \wedge (h \rightsquigarrow l \longrightarrow s \stackrel{h}{\sim} t) \wedge$ 
 $(s, s') \in \text{Step } a \wedge (t, t') \in \text{Step } a \longrightarrow s' \stackrel{l}{\sim} t'$ "
```

"a" names the system operation, "l" a low level domain, "h" a high level domain, from the states "s" and "t" the system operation is executed and "s'" and "t'" are the resulting states.

First I tried to validate confidentiality for the different system operations as they are defined in the take-grant-model. With this model it's impossible to decide whether a change of value has been recognized by another domain.

In the paper an entity only include a set of capabilities. For my purpose I need the option to access the content of the entities. This is because the rules for noninterference state that no information is allowed to flow from one domain to another. This includes the information stored in the kernel objects. Therefore I extended the original record `entity` by adding a *value* modelled by a natural number.

My entity type:

```
record entity =   caps :: cap set
                  eValue :: nat
```

To check noninterference I had to define a few functions.

1. The equivalence relation \sim :

$s \stackrel{d}{\sim} t$ means that for every entity *e* reachable from an entity in *d* the status of *e* in *s* and *t* has to be the same.

I named the function `aquiv_nonin`. It compares the value and capabilities of *e* and the entities of the subsystem *e* is located in for *s* and *t*.

```
aquiv_nonin :: "state  $\Rightarrow$  state  $\Rightarrow$  subSysT  $\Rightarrow$  bool" where
"aquiv_nonin s t d  $\equiv \{\forall e \in d. \text{value\_of } s \ e = \text{value\_of } t \ e \wedge \text{caps\_of } s \ e = \text{caps\_of } t \ e \wedge \text{subSys}$ 
 $s \ e = \text{subSys } t \ e\}$ "
```

2. A function to read the value of an entity:

```
value_of :: "state  $\Rightarrow$  entity_id  $\Rightarrow$  nat" where
"value_of s sref  $\equiv \text{eValue}(\text{heap } s \text{ sref})"$ 
```

3. The isolation with subsystems:

Subsystems are defined by entities that are `connected` with an entity *e* in a state *s*.

To identify subsystems I need a datatype for them:

```
type_synonym subSysT = "entity_id st"
```

Now I can define Subsystems with the function `subSys`:

```
subSys :: "state  $\Rightarrow$  entity_id  $\Rightarrow$  subSysT" where
"subSys s e  $\equiv \{\forall e_i. \text{in\_conc\_connected } s \ e \ e_i\}"$ 
```

`in_conc_connected s e ei` is true for entities *e* and *e_i* that are connected in state *s*.

e and *e_i* are connected in state *s* if a grant capability on *e_i* is part of `caps_of e` or if a grant capability on *e* is part of `caps_of ei`.

The function `caps_of ei` was defined in chapter 3.

5 Validation of Noninterference

After the formalisations in chapter 3 and 4 I tried to decide noninterference for the different system operations in the following way.

I took one Low-level-Subsystem and one High-level-Subsystem with entities in them and tested for different right-sets and different operations if the noninterference-property holds. The following first displays what I assume and then shows an example of this approach:

- H equates a High level domain that implements the subsystem 'H'
- L equates a Low level domain that implements the subsystem 'L'
- e_1 is an entity in H and e_2 is an entity in L

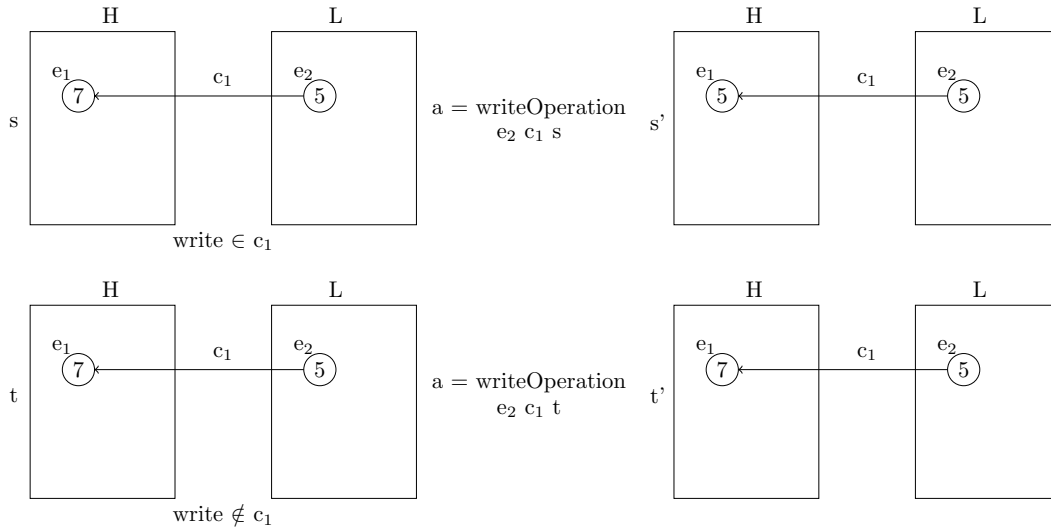


Figure 8: Noninterference of Write 1

To show noninterference I checked if the criterias for `aquiv_nonin s' t' L` are fulfilled after the execution of the `write` operation and the following preconditions.

The `write` operation in the extended model satisfies the noninterference property:

- $\text{value_of } s' e = \text{value_of } s e \wedge \text{caps_of } s' e = \text{caps_of } s e$ and $\text{subSys } s' e = \text{subSys } s e$ as the `write` operation on the entity, $c_1 \in e_2$ is pointing on, changes an entity $e_1 \in H$ and does not affect an entity $e \in L$.
- $\text{value_of } s e = \text{value_of } t e \wedge \text{caps_of } s e = \text{caps_of } t e$ and $\text{subSys } s e = \text{subSys } t e$ as one of the preconditions was $s \stackrel{L}{\sim} t$. I defined the equivalence relation with the function `aquiv_nonin s t L`, which is equal to the requirement.
- The `step` function first checks whether the execution of the system operation is legal, if not the new state t' equals the old state t .
 $\text{value_of } t e = \text{value_of } t' e \wedge \text{caps_of } t e = \text{caps_of } t' e$ and $\text{subSys } t e = \text{subSys } t' e$ as `write` is not part of c_1 . So $\text{legal}(\text{SysWrite } e_2 c_1) s = \text{false}$ what leads to $t=t'$.

In the following cases the proof looks allways the same. So I shortend it:

Preconditions:

- * $s \stackrel{L}{\sim} t \Rightarrow \text{aquiv_nonin } s t L$
- ** `writeOperation e2 c1` changes $e_1 \in H$ no $e \in L$
- *** $\text{legal}(\text{SysWrite } e_2 c_1) t = \text{false} \Rightarrow t=t'$

Proof of the noninterference property for Write 1:

$\forall e \in L.$

$$\begin{aligned}
 & (\text{value_of } s' e = \text{value_of } s e = \text{value_of } t e = \text{value_of } t' e \\
 & \wedge \text{caps_of } s' e = \text{caps_of } s e = \text{caps_of } t e = \text{caps_of } t' e \\
 & \wedge \text{subSys } s' e = \text{subSys } s e = \text{subSys } t e = \text{subSys } t' e) \\
 & \Rightarrow \text{aquiv_nonin } s' t' L \Rightarrow s' \stackrel{L}{\sim} t'
 \end{aligned}$$

With $s' \stackrel{L}{\sim} t'$ the noninterference property for `write` is fulfilled.

6 Redesign of the take-grant-model

This procedure worked until I came to the remove-operation. There I got the problem, that an entity in the given model is allowed to delete a capability and with that also an object in another domain without any restrictions:

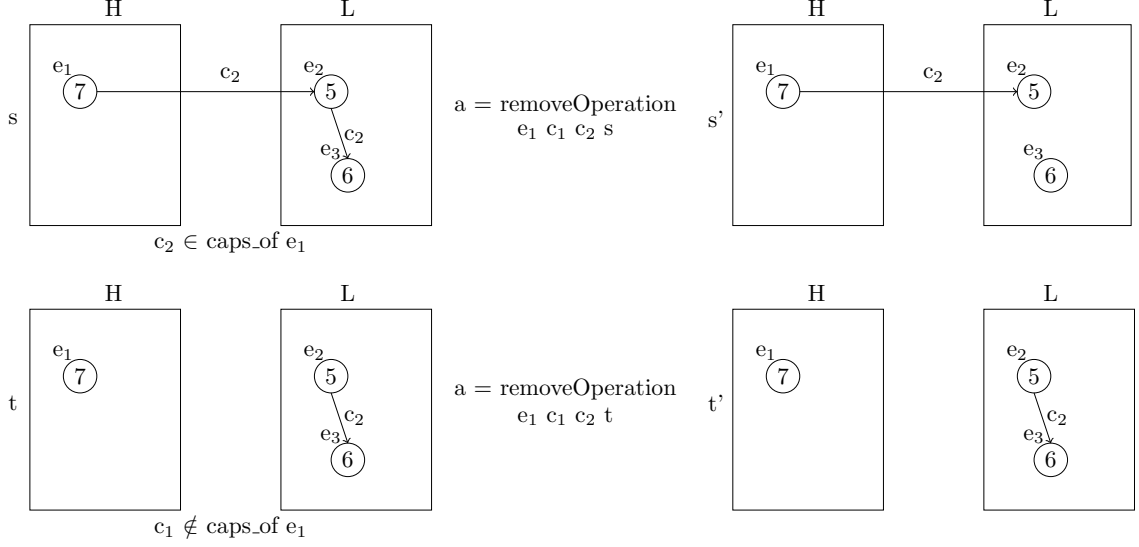


Figure 9: No confidentiality for Remove

In this example the L domain knows that the `removeOperation` was performed in the H domain as the capability `c2` was deleted. As a consequence the noninterference property is not achieved.

To research into this problem I decided to classify the entities by their types, corresponding to the kernel specification [6]:

- Untyped
- TCB
- Synchronous IPC Endpoint (SEP)
- Asynchronous IPC Endpoint (AEP)
- CNode
- VSpace
- Interrupt Controller
- Interrupt Handler
- Shared Pages (Pages (Frames) can be shared between domains. The corresponding capability has to be copied and then mapped in the VSpace of the other domain.)

The following table shows the different object types with the different operation executable on them and the corresponding take-grant system calls:

Capability Type	Concrete Kernel	protection model
Untyped	Retype Revoke	sequence of <i>SysCreate</i> <i>SysRevoke</i>
TCB	TreadControl Exchange Registers Yield	<i>SysNoOP</i> , <i>SysGrant</i> <i>SysWrite</i> or <i>SysRead</i> <i>SysNoOP</i>
Synchronous IPC (Endpoint)	Send IPC Wait IPC Grant IPC	<i>SysWrite</i> or <i>SysNoOP</i> <i>SysRead</i> <i>SysWrite</i> , <i>SysGrant</i> or <i>SysNoOP</i>
Asynchronous IPC (AsyncEndpoint)	Send Event Wait Event	<i>SysWrite</i> <i>SysRead</i>
CNode	imitate mint Remove Revoke Move Recycle	<i>SysGrant</i> <i>SysGrant</i> <i>SysRemove</i> <i>SysRevoke</i> <i>SysGrant</i> , <i>SysRemove</i> <i>SysRevoke</i> , sequence of <i>SysRemove</i>
VSpace	Install Mapping Remove Mapping Remap initialise	<i>SysGrant</i> <i>SysRemove</i> <i>SysRemove</i> , <i>SysGrant</i> <i>SysNoOP</i>
InterruptController	Register interrupt Unregister interrupt	<i>SysGrant</i> <i>SysRemove</i>
Interrupt Handler	Acknowledge interrupt	<i>SysWrite</i>

Table 1: Relationship: operation of concrete kernel \longleftrightarrow of protection model [5]

To discern the different object types I need to revise the entity record and the preconditions for the different system operations.

New datatype for the object types:

```

datatype   eType = Untyped
                | TCB
                | SEP
                | AEP
                | SPage
                | CNode
                | VSpace
                | IContr
                | IHandl

```

The final version of the **entity** record:

```

record   entity = caps :: cap set
                eValue :: nat
                eType :: eType

```

The revised version of the **legal** function:

legal :: "sysOPs \Rightarrow state \Rightarrow bool" where

```

    "legal (SysNoOp e) s" = isEntityOf s e"
  | "legal (SysCreate e c1 c2) s" = (isEntityOf s e  $\wedge$  c1, c2  $\subseteq$  caps_of s e  $\wedge$ 
    Grant  $\in$  rights c2  $\wedge$  Create  $\in$  rights c2)  $\wedge$ 
    eType (entity c1) = Untyped"
  | "legal (SysRead e c) s" = (isEntityOf s e  $\wedge$  c  $\in$  caps_of s e  $\wedge$  Read
     $\in$  rights c)  $\wedge$  eType (entity c) = TCB  $\vee$  SEP  $\vee$  AEP  $\vee$  SPage"
  | "legal (SysWrite e c) s" = (isEntityOf s e  $\wedge$  c  $\in$  caps_of s e  $\wedge$  Write
     $\in$  rights c)  $\wedge$  eType (entity c) = TCB  $\vee$  SEP  $\vee$  AEP
     $\vee$  IHandl  $\vee$  SPage"
  | "legal (SysGrant e c1 c2 r) s" = (isEntityOf s e  $\wedge$  isEntityOf s (entity c1)
     $\wedge$  c1, c2  $\subseteq$  caps_of s e  $\wedge$  Grant  $\in$  rights c1)  $\wedge$ 
    eType (entity c1) = TCB  $\vee$  SEP  $\vee$  CNode  $\vee$  VSpace  $\vee$ 
    IContr"
  | "legal (SysRemove e c1 c2) s" = (isEntityOf s e  $\wedge$  c1  $\in$  caps_of s e)  $\wedge$ 
    eType (entity c1) = CNode  $\vee$  VSpace  $\vee$  IContr"
  | "legal (SysRevoke e c) s" = isEntityOf s e  $\wedge$  c  $\in$  caps_of s e  $\wedge$ 
    eType (entity c) = Untyped  $\vee$  CNode"

```

As mentioned in chapter 3.2 (System Operations) the step function first proves if a system operation is "legal" in state *s*. If it is, the system operation is performed. Otherwise the new state *s'* is defined as

$s' = s$. This means that if a system operation is not legal nothing happens. For the validation I took a subsystem (SS1) of one Domain (D1) and another subsystem (SS2) of a second Domain (D2). In chapter 2.1.2 (Kernel Objects) I explained that the only communication between Domains goes through *Asynchronous Endpoints* and *Shared Pages*. Figure 10 pictures an example of how the objects and methods can be placed in the domains and how the connection to *Asynchronous Endpoints* and *Shared Pages* is implemented if the information is allowed to flow from Domain 1 to Domain 2: $D1 \leadsto D2$ but $D2 \not\leadsto D1$

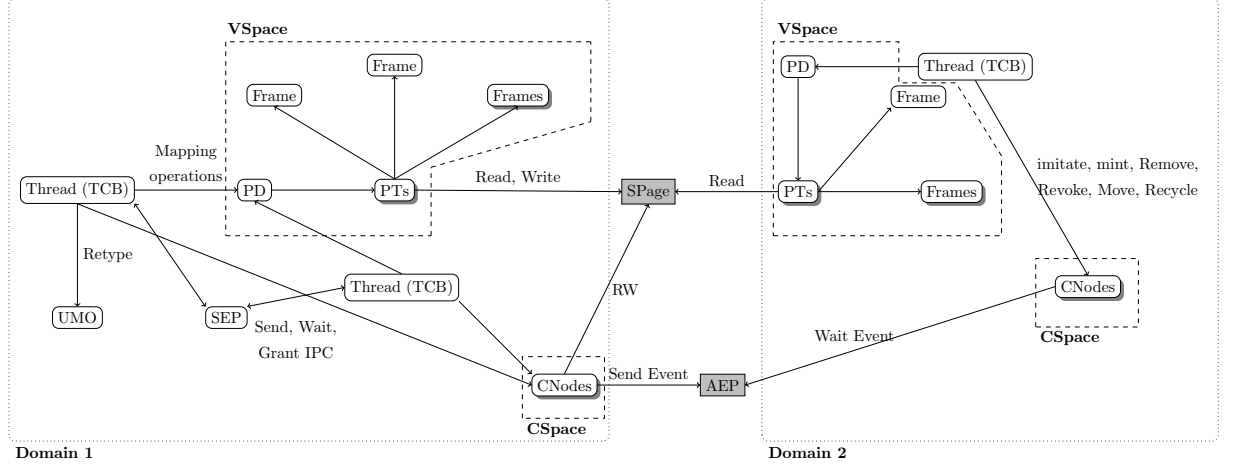


Figure 10: Objects and Methods in the kernel

7 Validation with the new model

I examine each operation of the protection model and distinguish therefore between the different object types.

For this I assume that Domain 1 equates a low level domain and Domain 2 a high level domain. So information is allowed to flow from Domain 1 to Domain 2 but not from Domain 2 to Domain 1.

$D1 \rightsquigarrow D2$ but $D2 \not\rightsquigarrow D1$

Further I assume that state s is equivalent to state t for Domain 1. What is represented by the function `equiv_nonin`

$$s \stackrel{D1}{\sim} t \equiv \text{equiv_nonin } s \ t \ D1$$

In this chapter I show that the criteria for the equivalence relation still holds in Domain 1, between s' and t' , after every type of operation.

7.1 Create

Create corresponds to the *Retype* operation on untyped memory objects (UMOs). Each Domain has a own and fixed section of memory. So the UMO for the `retype` is located in the same Domain as the implementing entity. Furthermore the created entity is placed in the same Domain as in the CDT it is a child of the UMO.

7.1.1 Create on UMO

The following picture shows how a create operation in a H domain changes or not changes the equivalence criteria in the L domain that is not allowed to get information from the primer one.

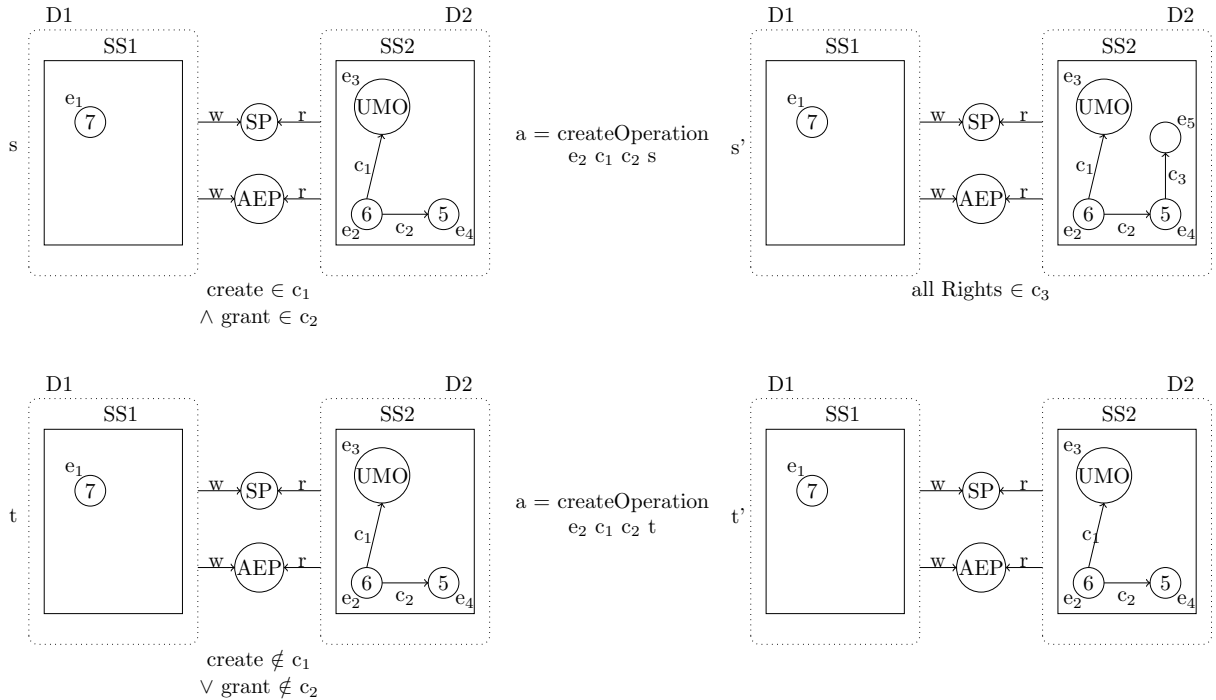


Figure 11: Noninterference for Create on Untyped Memory Objects

I have to show that if $s \stackrel{D1}{\sim} t$ and $(s, s') \in \text{Step } a$ and $(t, t') \in \text{Step } a$ then $s' \stackrel{D1}{\sim} t'$. $s \stackrel{D1}{\sim} t$ was defined in Chapter 5 as the boolean function `equiv_nonin s t D1`. The function is true if all entities $e \in D1$ have the same value in s and t (`value_of s e = value_of t e`), if they also have the same capabilities in s and t (`caps_of s e = caps_of t e`) and if D1 has the same entities in s and t (`subSys s e = subSys t e`).

In the following section I check if `value_of s' e = value_of t' e`, `caps_of s' e = caps_of t' e` and `subSys s' e = subSys t' e` for all $e \in D1$ after the execution of `createOperation e2 c1 c2 s` respectively `createOperation e2 c1 c2 t`. If that's the case I can say that `equiv_nonin s' t' D1 = true`. From my definition of `equiv_nonin`

this leads to $s' \stackrel{D1}{\sim} t'$.

Preconditions:

- * $s \stackrel{D1}{\sim} t \equiv \text{equiv_nonin } s \ t \ D1$
- ** $\text{createOperation } e_2 \ c_1 \ c_2 \ s$ creates $e_3 \in D2$ and doesn't change or create any $e \in D1$
- *** $\text{legal } (\text{SysCreate } e_2 \ c_1 \ c_2) \ t = \text{false} \Rightarrow t' = t$

Proof of the noninterference property for create on UMO: $\forall e \in D1$.

$$\begin{aligned}
 & (\text{value_of } s' \ e \stackrel{**}{=} \text{value_of } s \ e \stackrel{*}{=} \text{value_of } t \ e \stackrel{***}{=} \text{value_of } t' \ e \\
 & \wedge \text{caps_of } s' \ e \stackrel{**}{=} \text{caps_of } s \ e \stackrel{*}{=} \text{caps_of } t \ e \stackrel{***}{=} \text{caps_of } t' \ e \\
 & \wedge \text{subSys } s' \ e \stackrel{**}{=} \text{subSys } s \ e \stackrel{*}{=} \text{subSys } t \ e \stackrel{***}{=} \text{subSys } t' \ e) \\
 & \Rightarrow \text{equiv_nonin } s' \ t' \ D1 \Rightarrow s' \stackrel{D1}{\sim} t'
 \end{aligned}$$

With $s' \stackrel{D1}{\sim} t'$ the noninterference property for create on an untyped memory object is fulfilled.

7.1.2 Create on all other object types inside a domain

If **create** is performed on another object type than an untyped memory object, the function step' ($\text{SysCreate } e \ c_1 \ c_2$)s does nothing. So the new state s' equates the old state s . The following figure shows the createOperation for every other object type inside a domain.

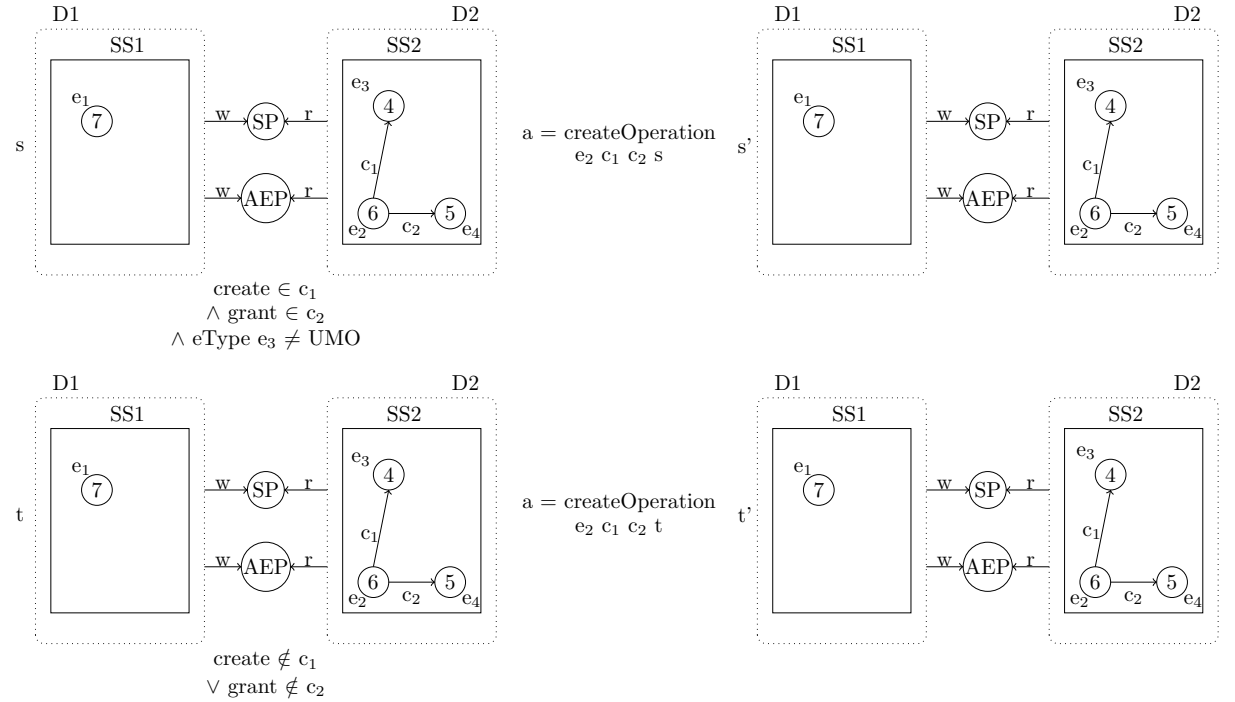


Figure 12: Noninterference for Create on object types \neq Untyped Memory Objects

Preconditions:

- * $s \stackrel{D1}{\sim} t \equiv \text{equiv_nonin } s \ t \ D1$
- ** $\text{legal } (\text{SysCreate } e_2 \ c_1 \ c_2) \ s = \text{false} \Rightarrow s' = s$
- *** $\text{legal } (\text{SysCreate } e_2 \ c_1 \ c_2) \ t = \text{false} \Rightarrow t' = t$

Proof of the noninterference property for create on other object types in a domain:

$\forall e \in D1$.

$$\begin{aligned}
 & (\text{value_of } s' \ e \stackrel{**}{=} \text{value_of } s \ e \stackrel{*}{=} \text{value_of } t \ e \stackrel{***}{=} \text{value_of } t' \ e \\
 & \wedge \text{caps_of } s' \ e \stackrel{**}{=} \text{caps_of } s \ e \stackrel{*}{=} \text{caps_of } t \ e \stackrel{***}{=} \text{caps_of } t' \ e \\
 & \wedge \text{subSys } s' \ e \stackrel{**}{=} \text{subSys } s \ e \stackrel{*}{=} \text{subSys } t \ e \stackrel{***}{=} \text{subSys } t' \ e) \\
 & \Rightarrow \text{equiv_nonin } s' \ t' \ D1 \Rightarrow s' \stackrel{D1}{\sim} t'
 \end{aligned}$$

With $s' \stackrel{D1}{\sim} t'$ the noninterference property for create on other object types in a domain is fulfilled.

7.1.3 Create on Asynchronous IPC Endpoint or Shared Page objects

Next I want to be sure that create has no impact on the entities in the L domain if it's executed on AEP or SPage objects.

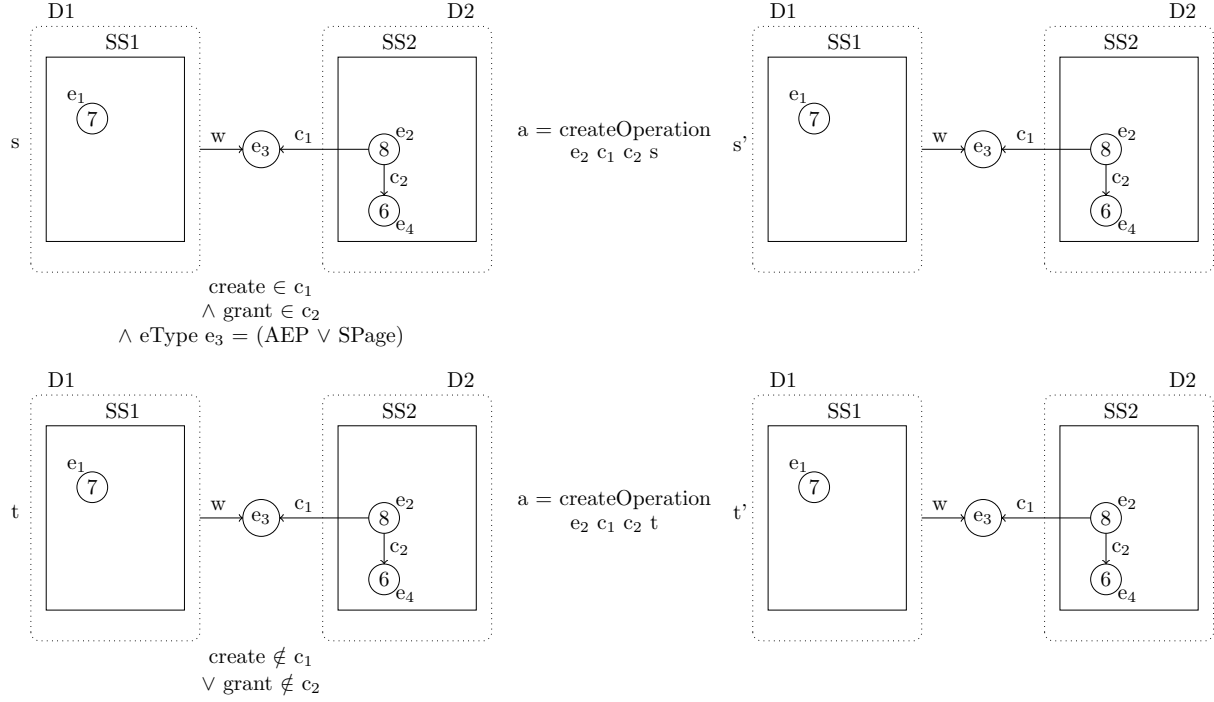


Figure 13: Noninterference for Create on object types = AEP \vee SPage

In this case the check if the execution is legal = false in both states. So in both states the step' function leads to the definition of the old state.

Preconditions:

* $s \stackrel{D1}{\sim} t \equiv \text{equiv_nonin } s \ t \ D1$
 ** $\text{legal } (\text{SysCreate } e_2 \ c_1 \ c_2) \ s = \text{false} \Rightarrow s' = s$
 *** $\text{legal } (\text{SysCreate } e_2 \ c_1 \ c_2) \ t = \text{false} \Rightarrow t' = t$

Proof of the noninterference property for create on Asynchronous IPC Endpoint or Shared Page objects:

$\forall e \in D1.$
 $(\text{value_of } s' \ e = \text{value_of } s \ e = \text{value_of } t \ e = \text{value_of } t' \ e)$
 $\wedge \text{caps_of } s' \ e = \text{caps_of } s \ e = \text{caps_of } t \ e = \text{caps_of } t' \ e$
 $\wedge \text{subSys } s' \ e = \text{subSys } s \ e = \text{subSys } t \ e = \text{subSys } t' \ e)$
 $\Rightarrow \text{equiv_nonin } s' \ t' \ D1 \Rightarrow s' \stackrel{D1}{\sim} t'$

With $s' \stackrel{D1}{\sim} t'$ the noninterference property for create on Asynchronous IPC Endpoint or Shared Page objects is fulfilled.

7.2 Grant

The **grant** operation can only be performed inside a domain on a TCB, Synchronous IPC, CNode, VSpace or Interrupt Controller object.

7.2.1 Grant on TCB, SEP, CNode, VSpace or IContr objects

Now I show that any grant operation inside a H domain on one of the named objects does not affect the values, capabilities or entities of an L domain.

Because every given object behaves the same way, I generalized $e_4 = \text{TCB} \vee \text{SIPC} \vee \text{CNode} \vee \text{VSpace} \vee \text{IContr}$.

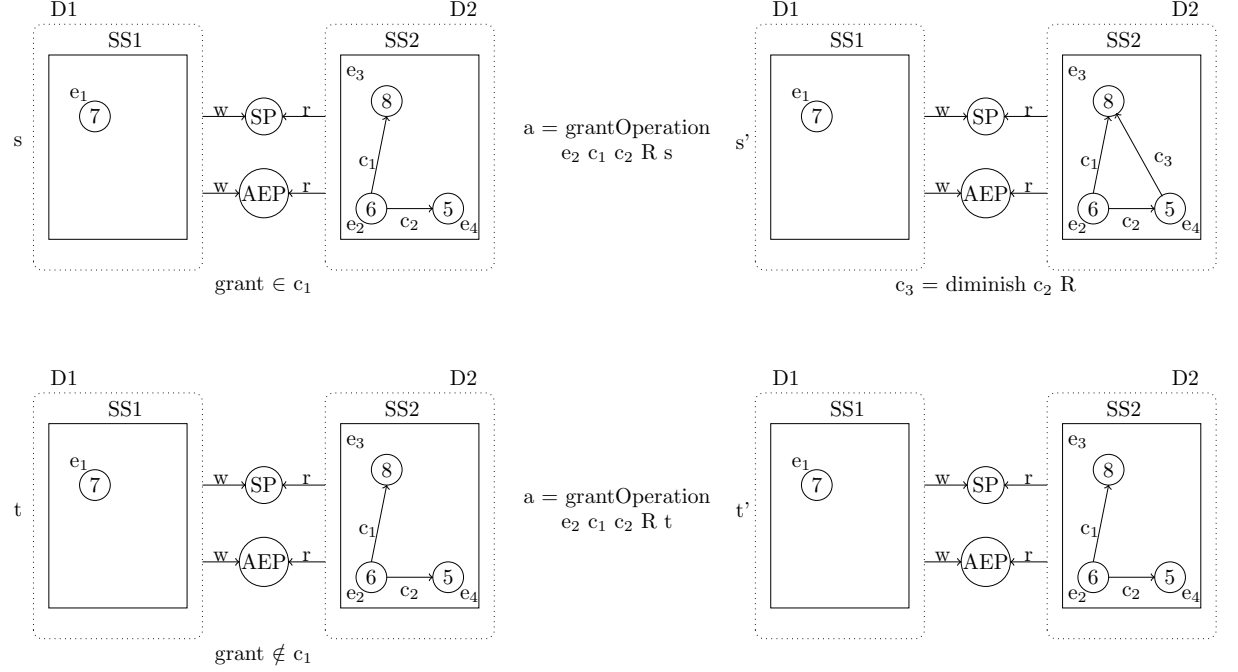


Figure 14: Noninterference for Grant on an TCB, Synchronous IPC Endpoint, CNode, VSpace or Interrupt Controller object

As it adds a capability to an entity inside the same domain as the target entity is, the **grant** operation has no impact on the entities of the other domain.

Preconditions:

- * $s \stackrel{D1}{\sim} t \equiv \text{equiv_nonin } s \ t \ D1$
- ** $\text{grantOperation } e_2 \ c_1 \ c_2 \ R \ s$ creates $c_3 \in D2$ and does not change or create any capability $\in D1$
- *** $\text{legal } (\text{SysGrant } e_2 \ c_1 \ c_2 \ R) \ t = \text{false} \Rightarrow t' = t$

Proof of the noninterference property for grant on TCB, Synchronous IPC Endpoint, CNode, VSpace and Interrupt Controller objects:

$$\begin{aligned}
 & \forall e \in D1. \\
 & \quad \text{value_of } s' \ e \stackrel{**}{=} \text{value_of } s \ e \stackrel{*}{=} \text{value_of } t \ e \stackrel{***}{=} \text{value_of } t' \ e \\
 & \quad \wedge \text{caps_of } s' \ e \stackrel{**}{=} \text{caps_of } s \ e \stackrel{*}{=} \text{caps_of } t \ e \stackrel{***}{=} \text{caps_of } t' \ e \\
 & \quad \wedge \text{subSys } s' \ e \stackrel{**}{=} \text{subSys } s \ e \stackrel{*}{=} \text{subSys } t \ e \stackrel{***}{=} \text{subSys } t' \ e \\
 & \Rightarrow \text{equiv_nonin } s' \ t' \ D1 \Rightarrow s' \stackrel{D1}{\sim} t'
 \end{aligned}$$

With $s' \stackrel{D1}{\sim} t'$ the noninterference property for grant on TCB, Synchronous IPC Endpoint, CNode, VSpace and Interrupt Controller objects is fulfilled.

7.2.2 Grant on other objects inside a domain

In this paragraph I check if an execution of the grant operation on another object than TCB, SEP, CNode, VSpace, Interrupt Controller or the object types that establish a communication interface between domains: AEP and SPage, alters the configuration of the other domain.

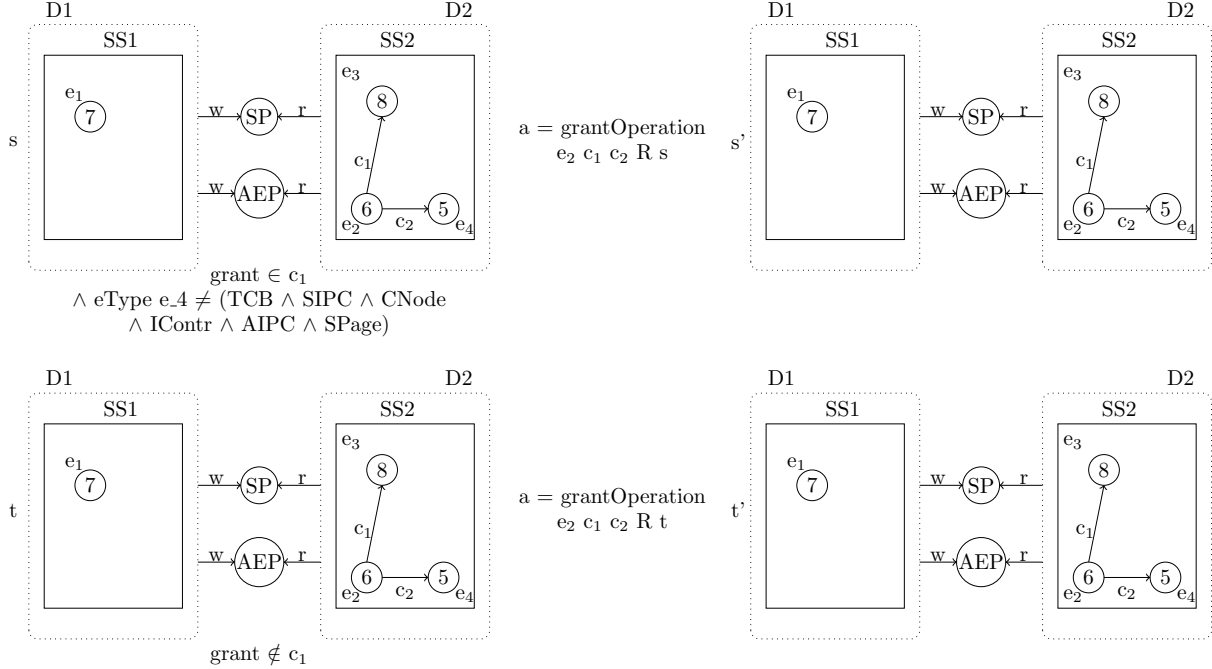


Figure 15: Noninterference for Grant on an object \neq TCB, SEP, CNode, VSpace, IContr, SPage or AEP object

Preconditions:

- * $s \stackrel{D1}{\sim} t \equiv \text{equiv_nonin } s \ t \ D1$
- ** $\text{legal } (\text{SysGrant } e_2 \ c_1 \ c_2) \ s = \text{false} \Rightarrow s' = s$
- *** $\text{legal } (\text{SysGrant } e_2 \ c_1 \ c_2 \ R) \ t = \text{false} \Rightarrow t' = t$

Proof of the noninterference property for grant on an object \neq TCB, SEP, CNode, VSpace, IContr, SPage or AEP:

$\forall e \in D1.$

$$\begin{aligned}
 & \text{value_of } s' \ e \stackrel{**}{=} \text{value_of } s \ e \stackrel{*}{=} \text{value_of } t \ e \stackrel{***}{=} \text{value_of } t' \ e \\
 & \wedge \text{caps_of } s' \ e \stackrel{**}{=} \text{caps_of } s \ e \stackrel{*}{=} \text{caps_of } t \ e \stackrel{***}{=} \text{caps_of } t' \ e \\
 & \wedge \text{subSys } s' \ e \stackrel{**}{=} \text{subSys } s \ e \stackrel{*}{=} \text{subSys } t \ e \stackrel{***}{=} \text{subSys } t' \ e \\
 & \Rightarrow \text{equiv_nonin } s' \ t' \ D1 \Rightarrow s' \stackrel{D1}{\sim} t'
 \end{aligned}$$

With $s' \stackrel{D1}{\sim} t'$ the noninterference property for grant on an object \neq TCB, SEP, CNode, VSpace, IContr, SPage or AEP is fulfilled.

7.2.3 Grant on Asynchronous IPC Endpoint or Shared Page objects

The next figure illustrates grant on the two object types connecting different domains. In both cases the operation is not legal. So the new state equates the old one.

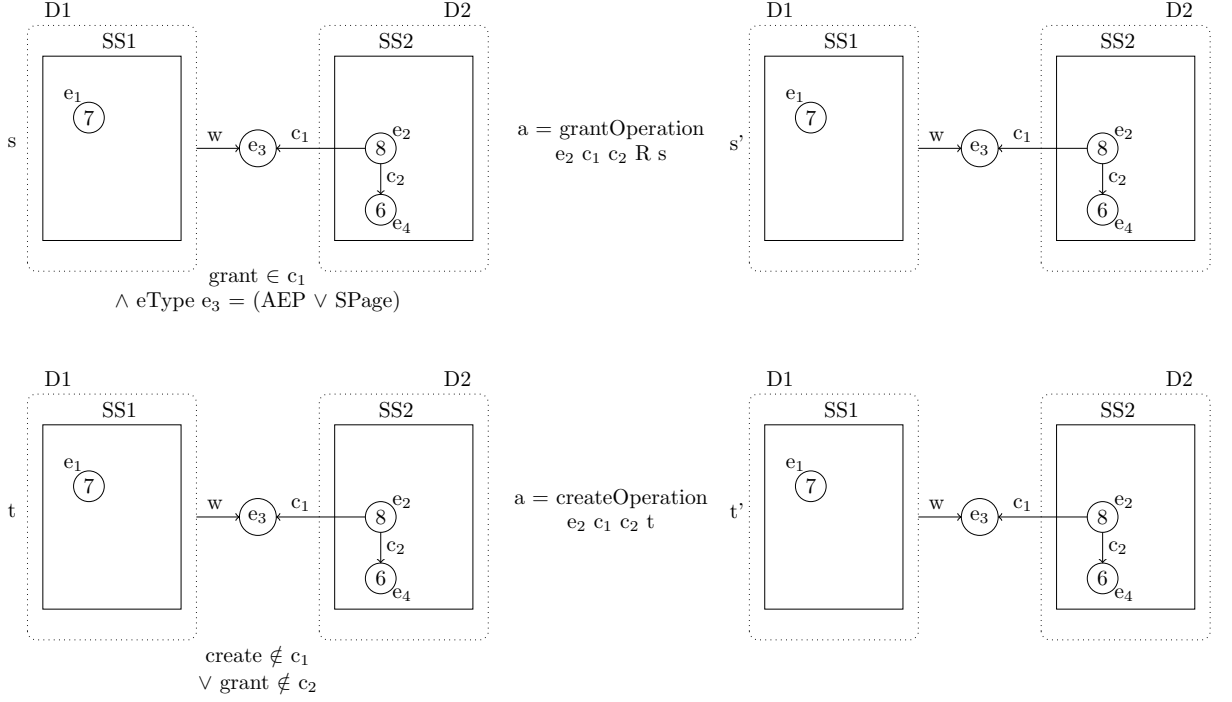


Figure 16: Noninterference for Grant on an Asynchronous IPC Endpoint object

Preconditions:

- * $s \stackrel{D1}{\sim} t \equiv \text{equiv_nonin } s \ t \ D1$
- ** $\text{legal } (\text{SysGrant } e_2 \ c_1 \ c_2) \ s = \text{false} \Rightarrow s' = s$
- *** $\text{legal } (\text{SysGrant } e_2 \ c_1 \ c_2) \ t = \text{false} \Rightarrow t' = t$

Proof of the noninterference property for grant on an object = SPAGE or AEP:

$\forall e \in D1.$

$$\begin{aligned}
 & \text{value_of } s' \ e \stackrel{**}{=} \text{value_of } s \ e \stackrel{*}{=} \text{value_of } t \ e \stackrel{***}{=} \text{value_of } t' \ e \\
 & \wedge \text{caps_of } s' \ e \stackrel{**}{=} \text{caps_of } s \ e \stackrel{*}{=} \text{caps_of } t \ e \stackrel{***}{=} \text{caps_of } t' \ e \\
 & \wedge \text{subSys } s' \ e \stackrel{**}{=} \text{subSys } s \ e \stackrel{*}{=} \text{subSys } t \ e \stackrel{***}{=} \text{subSys } t' \ e \\
 & \Rightarrow \text{equiv_nonin } s' \ t' \ D1 \Rightarrow s' \stackrel{D1}{\sim} t'
 \end{aligned}$$

With $s' \stackrel{D1}{\sim} t'$ the noninterference property for grant on an object = SPAGE or AEP is fulfilled.

7.3 Write

Write can be executed on TCB, SEP, AEP, SPage and Interrupt Handler objects.

7.3.1 Write on TCB, SEP or IHandl objects

I start with the **write** operation on all executable objects inside a domain. So in the next figure $e_3 = \text{TCB} \vee \text{SEP} \vee \text{IHandl}$.

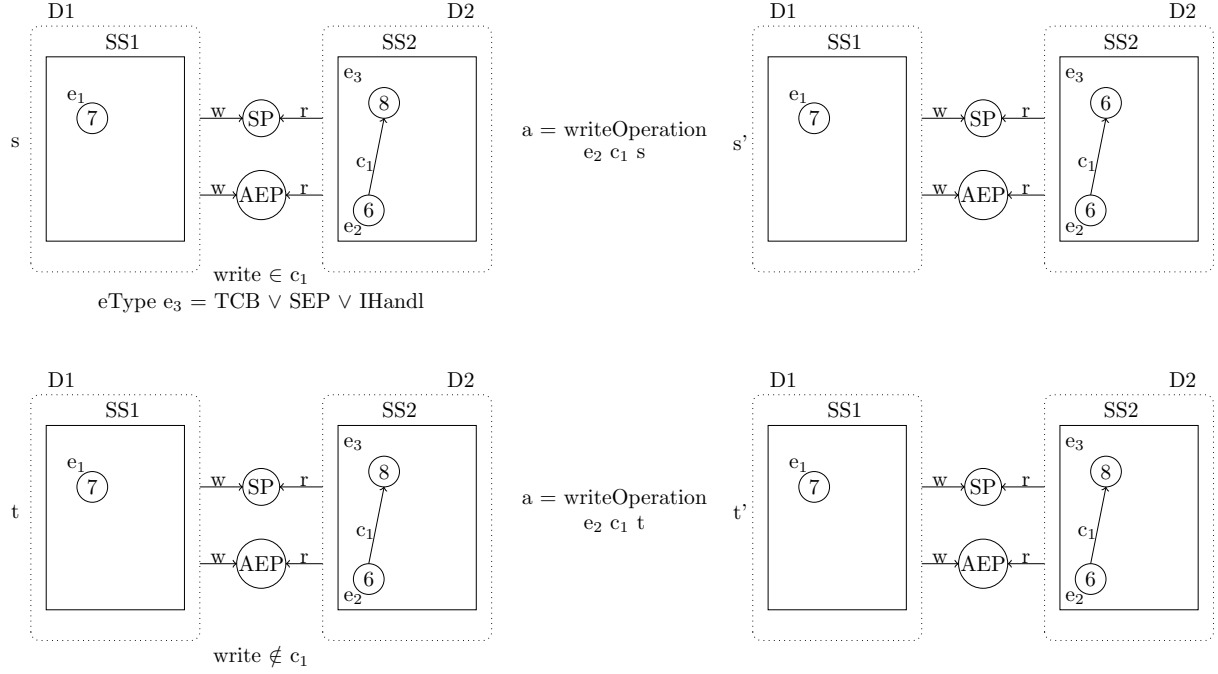


Figure 17: Noninterference for Write on a TCB, Synchronous IPC Endpoint or Interrupt Handler object

Preconditions:

- * $s \stackrel{D1}{\sim} t \equiv \text{equiv_nonin } s \ t \ D1$
- ** $\text{writeOperation } e_2 \ c_1 \ s$ only changes the value of an entity $\in D2$ nothing in D1
- *** $\text{legal } (\text{SysWrite } e_2 \ c_1) \ t = \text{false} \Rightarrow t' = t$

Proof of the noninterference property for write on TCB, SEP or IHandl objects:

$\forall e \in D1.$
 $\text{value_of } s' \ e \stackrel{**}{=} \text{value_of } s \ e \stackrel{*}{=} \text{value_of } t \ e \stackrel{***}{=} \text{value_of } t' \ e$
 $\wedge \text{caps_of } s' \ e \stackrel{**}{=} \text{caps_of } s \ e \stackrel{*}{=} \text{caps_of } t \ e \stackrel{***}{=} \text{caps_of } t' \ e$
 $\wedge \text{subSys } s' \ e \stackrel{**}{=} \text{subSys } s \ e \stackrel{*}{=} \text{subSys } t \ e \stackrel{***}{=} \text{subSys } t' \ e$
 $\Rightarrow \text{equiv_nonin } s' \ t' \ D1 \Rightarrow s' \stackrel{D1}{\sim} t'$

With $s' \stackrel{D1}{\sim} t'$ the noninterference property for write on TCB, SEP or IHandl objects is fulfilled.

7.3.2 Write on objects \neq TCB, SEP, IHandl, SPage and AEP

Like in 7.1 Create and 7.2 Grant there are other object types inside a domain, which are not executeable with the **write** operation. Those are CNodes, VSpaces, UMOs and Interrupt Controllers.

Write operation on these objects:

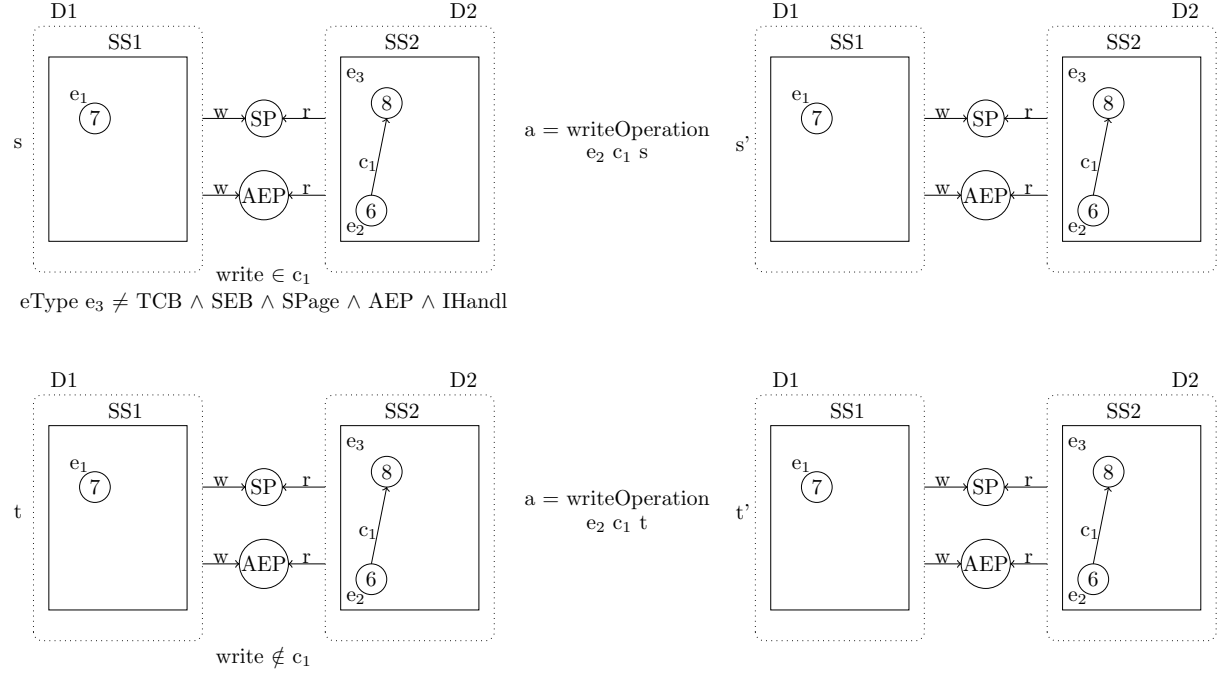


Figure 18: Noninterference for Write on objects \neq TCB, SEP, IHandl, SPage and AEP

Preconditions:

- * $s \stackrel{D1}{\sim} t \equiv \text{equiv_nonin } s \ t \ D1$
- ** $\text{legal } (\text{SysWrite } e_2 \ c_1) \ s = \text{false} \Rightarrow s' = s$
- *** $\text{legal } (\text{SysWrite } e_2 \ c_1) \ t = \text{false} \Rightarrow t' = t$

Proof of the noninterference property for write on objects \neq TCB, SEP, IHandl, SPage and AEP:

$$\begin{aligned}
 & \forall e \in D1. \\
 & \quad \text{value_of } s' \ e \stackrel{**}{=} \text{value_of } s \ e \stackrel{*}{=} \text{value_of } t \ e \stackrel{***}{=} \text{value_of } t' \ e \\
 & \quad \wedge \text{caps_of } s' \ e \stackrel{**}{=} \text{caps_of } s \ e \stackrel{*}{=} \text{caps_of } t \ e \stackrel{***}{=} \text{caps_of } t' \ e \\
 & \quad \wedge \text{subSys } s' \ e \stackrel{**}{=} \text{subSys } s \ e \stackrel{*}{=} \text{subSys } t \ e \stackrel{***}{=} \text{subSys } t' \ e \\
 & \Rightarrow \text{equiv_nonin } s' \ t' \ D1 \Rightarrow s' \stackrel{D1}{\sim} t'
 \end{aligned}$$

With $s' \stackrel{D1}{\sim} t'$ the noninterference property for **write** on objects \neq TCB, SEP, IHandl, SPage and AEP is fulfilled.

7.3.3 Write on AEP or SPage objects from Domain 2

In Chapter 7 I defined the precondition $\Rightarrow D1 \leadsto D2$ but $D2 \not\leadsto D1$. That means the rights from Domain 2 on Asynchronous Endpoints and Shared Pages are restricted to **read**. If the write operation is called from Domain 2 it looks like it is illustrated in Figure 19. The policy prescribes that information is only allowed to flow from Domain 1 to Domain 2 but not from Domain 2 to Domain 1. As a consequence **write** can not be part of c_1 .

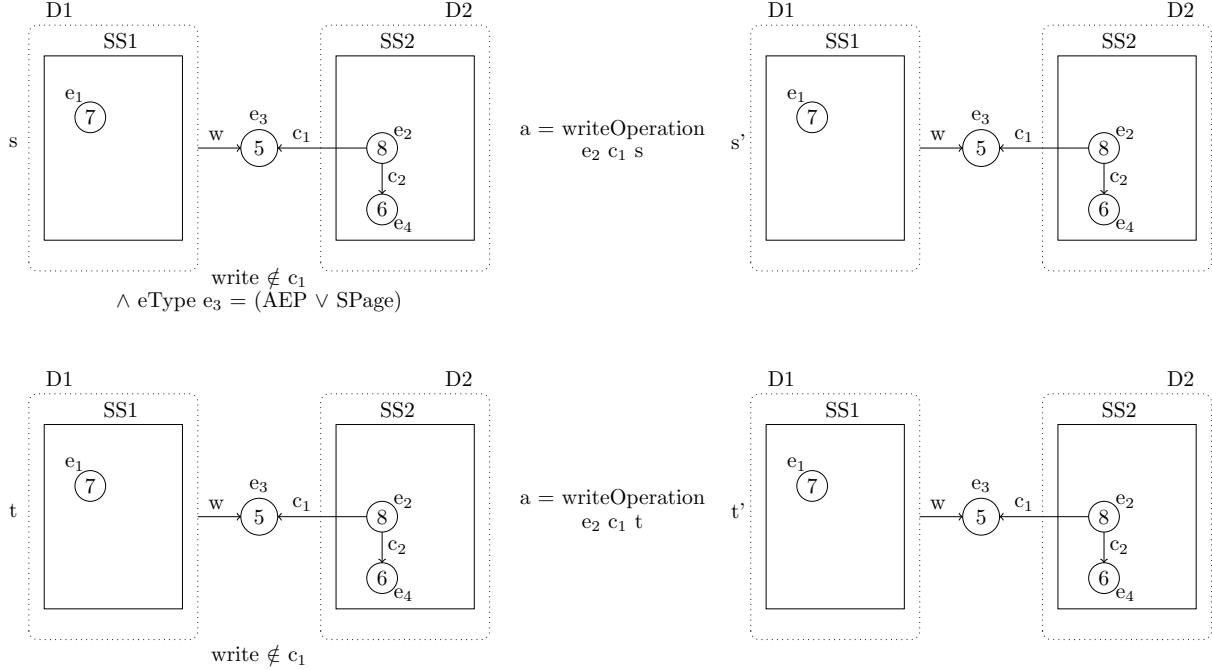


Figure 19: Noninterference for Write on an object = AEP executed from an entity \in Domain 2

Preconditions:

- * $s \stackrel{D1}{\sim} t \equiv \text{equiv_nonin } s \ t \ D1$
- ** $\text{legal } (\text{SysWrite } e_2 \ c_1) \ s = \text{false} \Rightarrow s' = s$
- *** $\text{legal } (\text{SysWrite } e_2 \ c_1) \ t = \text{false} \Rightarrow t' = t$

Proof of the noninterference property for write on AEP or SPage objects from Domain 2:

$\forall e \in D1.$

$$\begin{aligned}
 & \text{value_of } s' \ e \stackrel{**}{=} \text{value_of } s \ e \stackrel{*}{=} \text{value_of } t \ e \stackrel{***}{=} \text{value_of } t' \ e \\
 \wedge & \text{caps_of } s' \ e \stackrel{**}{=} \text{caps_of } s \ e \stackrel{*}{=} \text{caps_of } t \ e \stackrel{***}{=} \text{caps_of } t' \ e \\
 \wedge & \text{subSys } s' \ e \stackrel{**}{=} \text{subSys } s \ e \stackrel{*}{=} \text{subSys } t \ e \stackrel{***}{=} \text{subSys } t' \ e \\
 \Rightarrow & \text{equiv_nonin } s' \ t' \ D1 \Rightarrow s' \stackrel{D1}{\sim} t'
 \end{aligned}$$

With $s' \stackrel{D1}{\sim} t'$ the noninterference property for write on AEP or SPage objects from Domain 2 is fulfilled.

7.3.4 Write on an AEP or SPage object from Domain 1

Write on AEP objects can be executed from Domain 1. Figure 20 shows that this has no influence on the noninterference property.

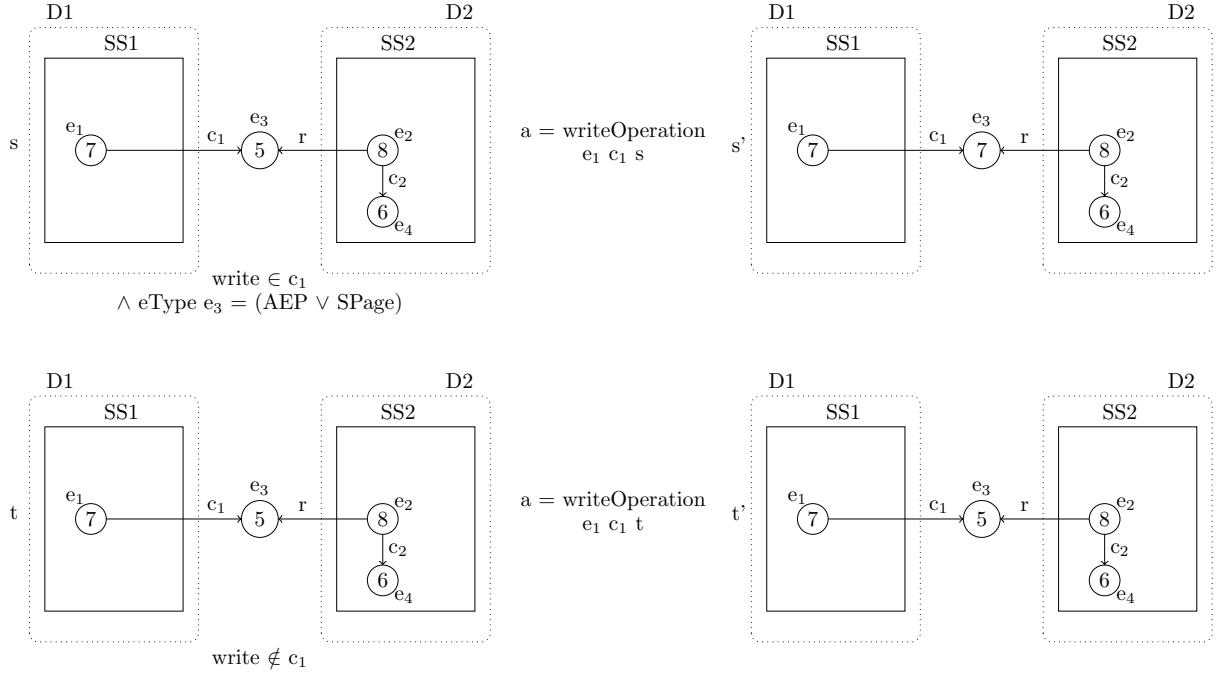


Figure 20: Noninterference for Write on an object = AEP executed from an entity $\in D1$

Preconditions:

- * $s \stackrel{D1}{\sim} t \equiv \text{equiv_nonin } s \ t \ D1$
- ** $\text{writeOperation } e_1 \ c_1 \ s$ changes the value $\in e_3 \notin D1$.
That means it has no impact on any entity $\in D1$
- *** $\text{legal } (\text{SysWrite } e_2 \ c_1) \ t = \text{false} \Rightarrow t' = t$

Proof of the noninterference property for write on AEP or SPage objects from Domain 1:

$\forall e \in D1.$

$$\begin{aligned}
 & \text{value_of } s' \ e \stackrel{**}{=} \text{value_of } s \ e \stackrel{*}{=} \text{value_of } t \ e \stackrel{***}{=} \text{value_of } t' \ e \\
 \wedge & \text{ caps_of } s' \ e \stackrel{**}{=} \text{caps_of } s \ e \stackrel{*}{=} \text{caps_of } t \ e \stackrel{***}{=} \text{caps_of } t' \ e \\
 \wedge & \text{ subSys } s' \ e \stackrel{**}{=} \text{subSys } s \ e \stackrel{*}{=} \text{subSys } t \ e \stackrel{***}{=} \text{subSys } t' \ e \\
 \Rightarrow & \text{equiv_nonin } s' \ t' \ D1 \Rightarrow s' \stackrel{D1}{\sim} t'
 \end{aligned}$$

With $s' \stackrel{D1}{\sim} t'$ the noninterference property for write on AEP or SPage objects from Domain 1 is fulfilled.

7.4 Read

Read is legal on TCB, Synchronous IPC Endpoint, Asynchronous IPC Endpoint and Shared Page objects. Like in chapter 7.3 I distinguish between objects with legal execution of **read** on objects inside a domain, illegal execution of **read** on objects inside a domain and both on objects outside a domain.

7.4.1 Read on TCB or Synchronous IPC Endpoint objects

TCB and SEP objects are the two object types that are executable with **read** from an endpoint in the same domain.

Figure 21 illustrates if the operation influences the L domain.

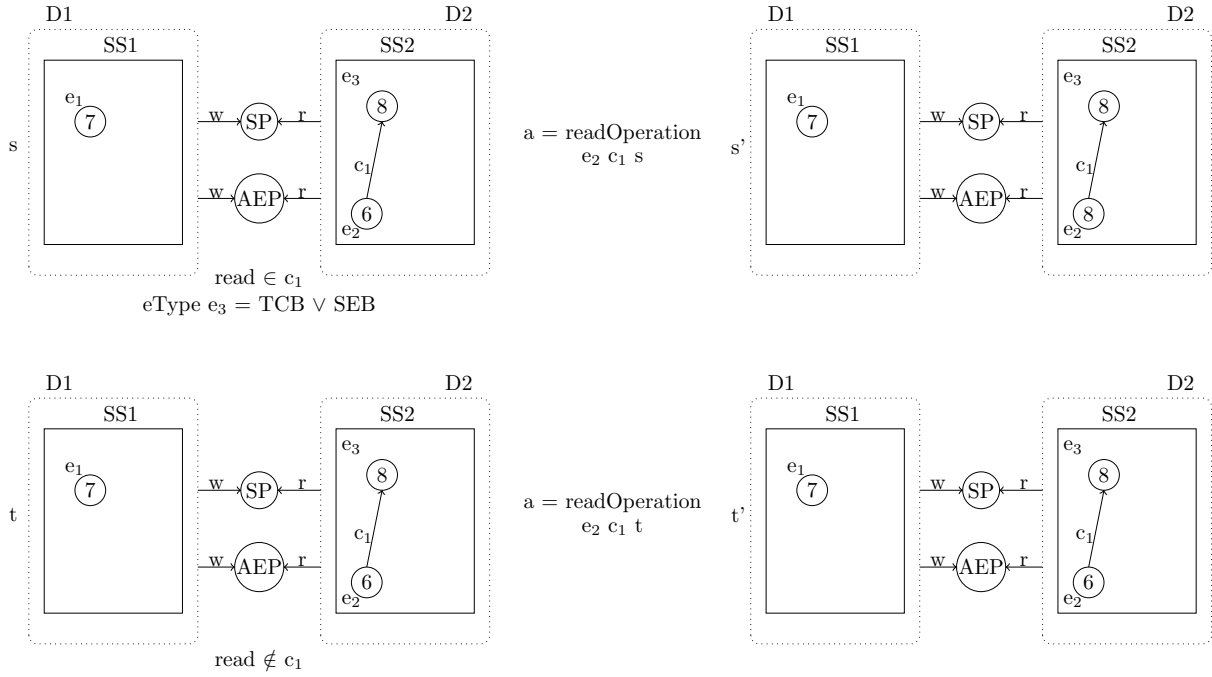


Figure 21: Noninterference for Read on a TCB or Synchronous IPC Endpoint object

Preconditions:

- * $s \stackrel{D1}{\sim} t \equiv \text{equiv_nonin } s \ t \ D1$
- ** $\text{readOperation } e_2 \ c_1 \ s$ only changes the value of an entity $\in D2$ nothing in $D1$
- *** $\text{legal } (\text{SysRead } e_2 \ c_1) \ t = \text{false} \Rightarrow t' = t$

Proof of the noninterference property for read on TCB or SEP objects:

$\forall e \in D1.$
 $\text{value_of } s' \ e \stackrel{**}{=} \text{value_of } s \ e \stackrel{*}{=} \text{value_of } t \ e \stackrel{***}{=} \text{value_of } t' \ e$
 $\wedge \text{caps_of } s' \ e \stackrel{**}{=} \text{caps_of } s \ e \stackrel{*}{=} \text{caps_of } t \ e \stackrel{***}{=} \text{caps_of } t' \ e$
 $\wedge \text{subSys } s' \ e \stackrel{**}{=} \text{subSys } s \ e \stackrel{*}{=} \text{subSys } t \ e \stackrel{***}{=} \text{subSys } t' \ e$
 $\Rightarrow \text{equiv_nonin } s' \ t' \ D1 \Rightarrow s' \stackrel{D1}{\sim} t'$

With $s' \stackrel{D1}{\sim} t'$ the noninterference property for read on TCB or SEP objects is fulfilled.

7.4.2 Read on other object types inside a domain

Figure 22 depicts the read operation on objects in the same domain on which `read` is not executable. It's similar to `write` in chapter 7.3.2.

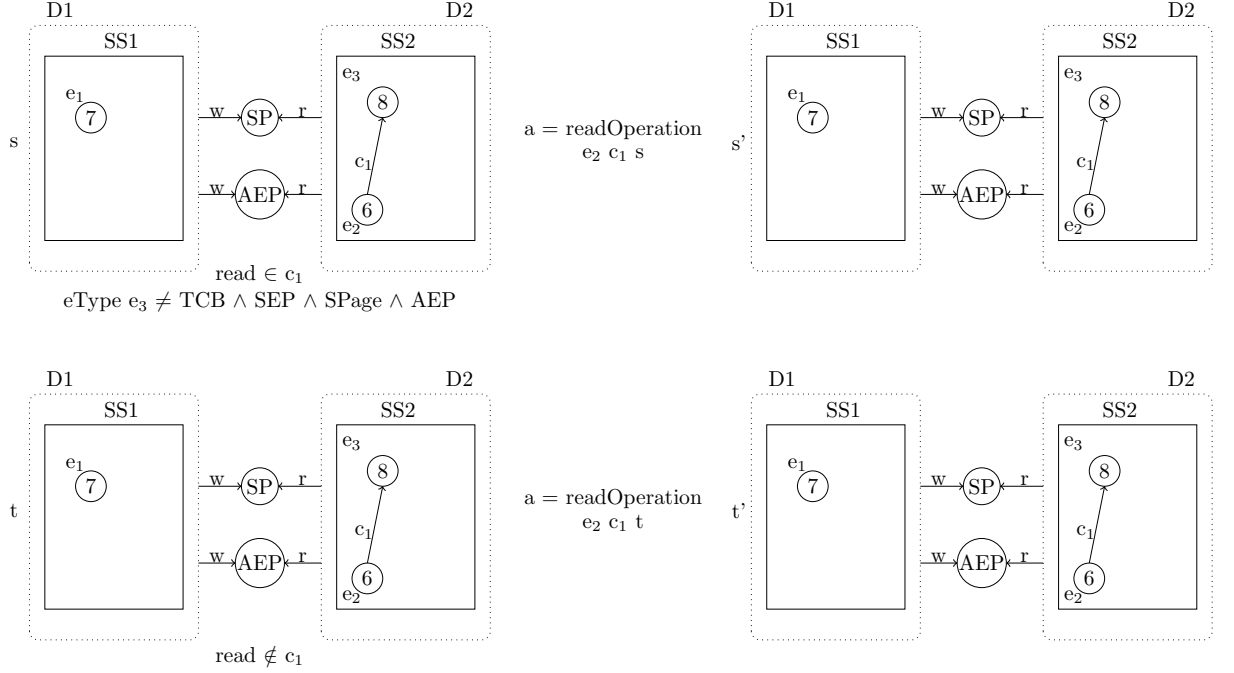


Figure 22: Noninterference for Read on objects \neq TCB, Asynchronous IPC Endpoint, Synchronous IPC Endpoint or Shared Page

Preconditions:

- * $s \stackrel{D1}{\sim} t \equiv \text{equiv_nonin } s \ t \ D1$
- ** $\text{legal } (\text{SysRead } e_2 \ c_1) \ s = \text{false} \Rightarrow s' = s$
- *** $\text{legal } (\text{SysRead } e_2 \ c_1) \ t = \text{false} \Rightarrow t' = t$

Proof of the noninterference property for read on objects \neq TCB, SEP, SPAGE and AEP:

$\forall e \in D1.$

$$\begin{aligned} & \text{value_of } s' \ e \stackrel{**}{=} \text{value_of } s \ e \stackrel{*}{=} \text{value_of } t \ e \stackrel{***}{=} \text{value_of } t' \ e \\ & \wedge \text{caps_of } s' \ e \stackrel{**}{=} \text{caps_of } s \ e \stackrel{*}{=} \text{caps_of } t \ e \stackrel{***}{=} \text{caps_of } t' \ e \\ & \wedge \text{subSys } s' \ e \stackrel{**}{=} \text{subSys } s \ e \stackrel{*}{=} \text{subSys } t \ e \stackrel{***}{=} \text{subSys } t' \ e \\ & \Rightarrow \text{equiv_nonin } s' \ t' \ D1 \Rightarrow s' \stackrel{D1}{\sim} t' \end{aligned}$$

With $s' \stackrel{D1}{\sim} t'$ the noninterference property for read on objects \neq TCB, SEP, SPAGE and AEP is fulfilled.

7.4.3 Read on AEP or SPage objects from Domain 1

Similar to chapter 7.3.3 **read** can only be executed from a H domain. That's the one to which information is allowed to flow. In my case it's Domain 2. No information is allowed to flow to Domain 1. So **read** is not legal if it is executed from Domain 1.

Figure 23 shows that this does not affect Domain 1.

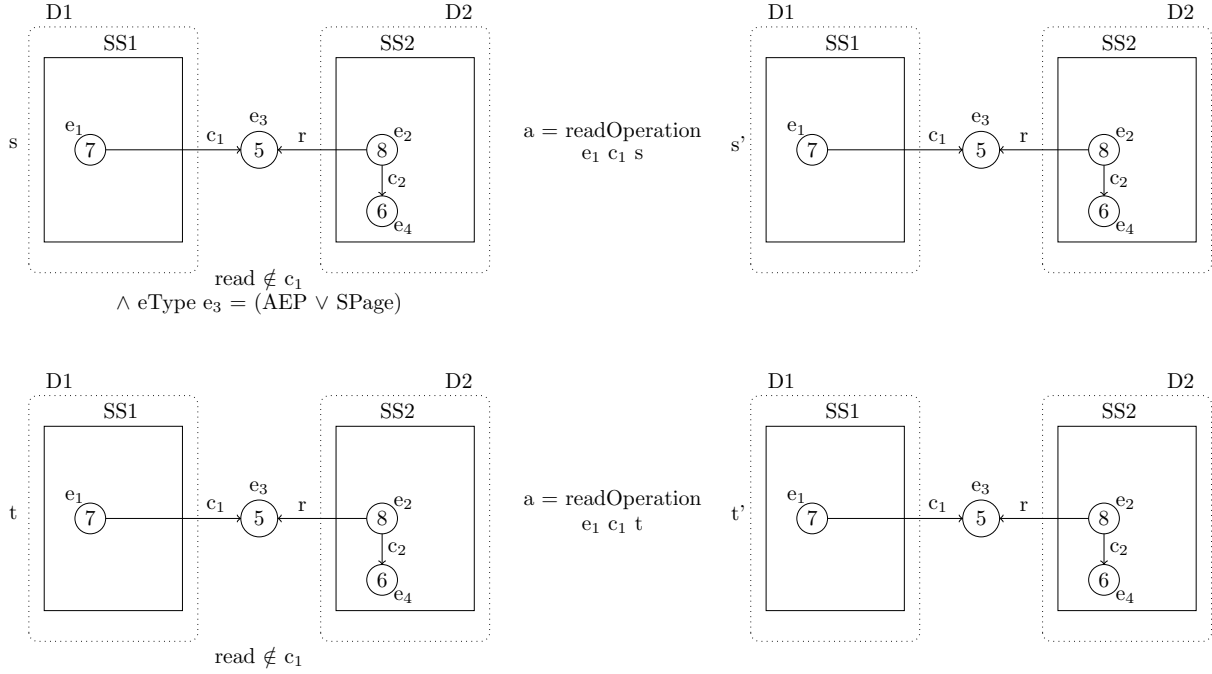


Figure 23: Noninterference for Read on object types = Asynchronous IPC Endpoint executed from Domain 1

Preconditions:

- * $s \stackrel{D1}{\sim} t \equiv \text{equiv_nonin } s \ t \ D1$
- ** $\text{legal } (\text{SysRead } e_1 \ c_1) \ s = \text{false} \Rightarrow s' = s$
- *** $\text{legal } (\text{SysRead } e_1 \ c_1) \ t = \text{false} \Rightarrow t' = t$

Proof of the noninterference property for read on AEP or SPage objects from Domain 1:

$\forall e \in D1.$
 $\text{value_of } s' \ e = \text{value_of } s \ e = \text{value_of } t \ e = \text{value_of } t' \ e$
 $\wedge \text{caps_of } s' \ e = \text{caps_of } s \ e = \text{caps_of } t \ e = \text{caps_of } t' \ e$
 $\wedge \text{subSys } s' \ e = \text{subSys } s \ e = \text{subSys } t \ e = \text{subSys } t' \ e$
 $\Rightarrow \text{equiv_nonin } s' \ t' \ D1 \Rightarrow s' \stackrel{D1}{\sim} t'$

With $s' \stackrel{D1}{\sim} t'$ the noninterference property for write on AEP or SPage objects from Domain 1 is fulfilled.

7.4.4 Read on AEP or SPage objects from Domain 2

Read can be executed from Domain 2. In Figure 24 I show the impact of this execution.

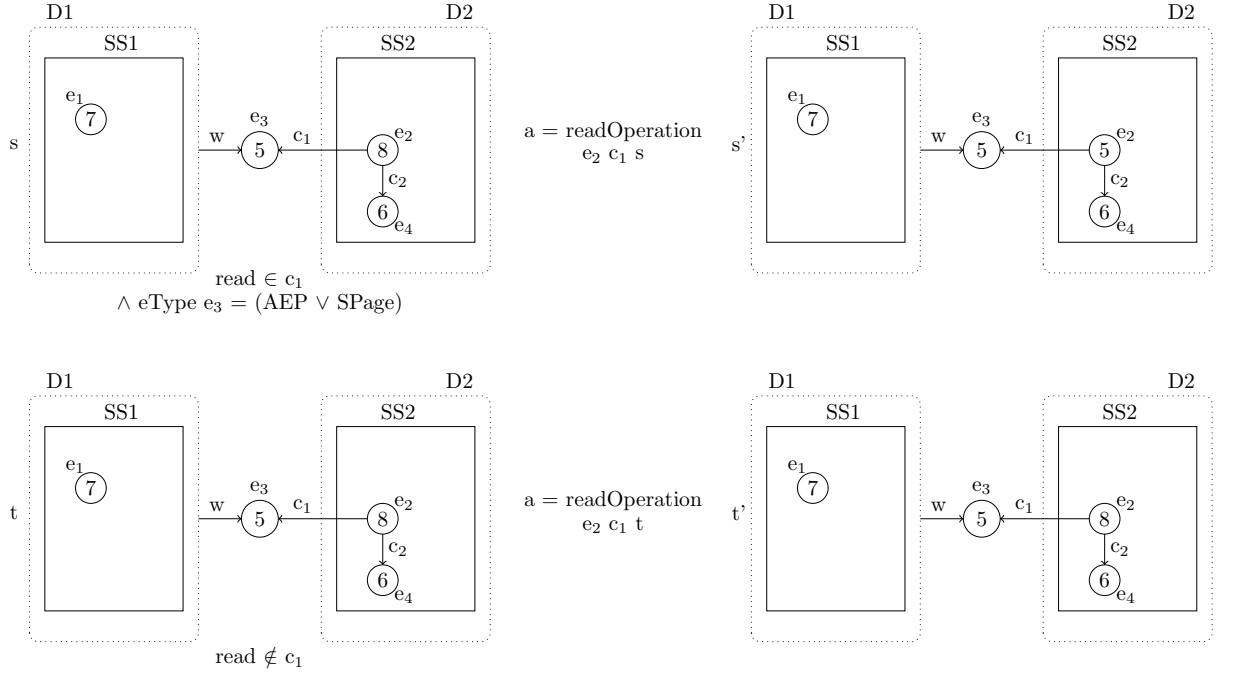


Figure 24: Noninterference for Read on object types = Asynchronous IPC Endpoint executed from Domain 2

Preconditions:

- * $s \stackrel{D1}{\sim} t \equiv \text{equiv_nonin } s \ t \ D1$
- ** $\text{readOperation}_{e_2 \ c_1 \ s}$ changes the value $\in e_3 \notin D1$.
That means it has no impact on any entity $\in D1$
- *** $\text{legal}(\text{SysRead}_{e_2 \ c_1}) \ t = \text{false} \Rightarrow t' = t$

Proof of the noninterference property for read on AEP or SPage objects from Domain 2:

$\forall e \in D1$.

$\text{value_of } s' \ e = \text{value_of } s \ e = \text{value_of } t \ e = \text{value_of } t' \ e$

$\wedge \text{caps_of } s' \ e = \text{caps_of } s \ e = \text{caps_of } t \ e = \text{caps_of } t' \ e$

$\wedge \text{subSys } s' \ e = \text{subSys } s \ e = \text{subSys } t \ e = \text{subSys } t' \ e$

$\Rightarrow \text{equiv_nonin } s' \ t' \ D1 \Rightarrow s' \stackrel{D1}{\sim} t'$

With $s' \stackrel{D1}{\sim} t'$ the noninterference property for write on AEP or SPage objects from Domain 1 is fulfilled.

7.5 Remove

Remove can be executed on CNode, VSpace or Interrupt Controller object types.

Like in the chapters before I distinguish between executing the operation inside and outside a domain. All legal object types are inside a domain. So I only have to differ between legal and not legal for the execution inside a domain.

7.5.1 Remove on CNode, VSpace or Interrupt Controller objects

Remove deletes a capability in an entity. This capability can point on an entity in the same domain or on an AEP or SPAGE object.

- Target object is in the same domain
If the removed capability points to an entity in the same domain and **remove** is legal for the executed entity, the operation is illustrated in figure 25.

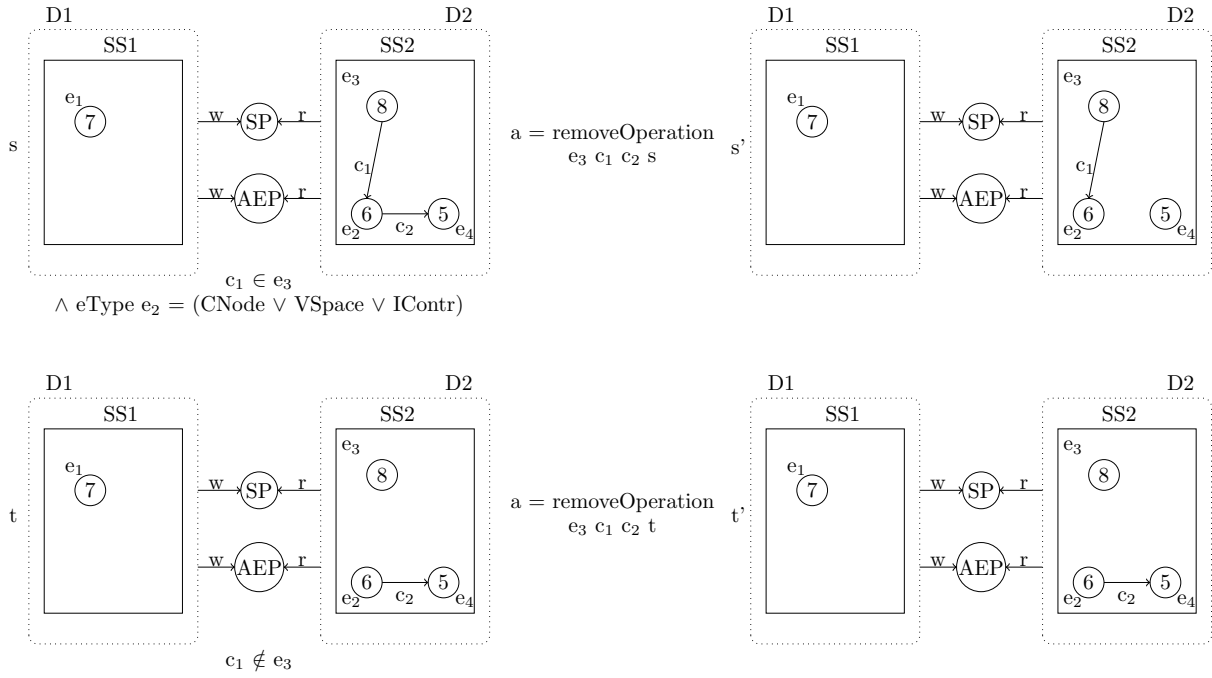


Figure 25: Noninterference for Remove on object types = CNode, VSpace or IContr.
The removed capability points to an entity in the same domain

Preconditions:

- * $s \stackrel{D1}{\sim} t \equiv \text{equiv_nonin } s\ t\ D1$
- ** $\text{removeOperation } e_2\ c_1\ c_2\ s$ removes a capability $\in e_2 \notin D1$ that points on an entity $\notin D1$.
That means it has no impact on any entity $\in D1$
- *** $\text{legal } (\text{SysRemove } e_2\ c_1\ c_2)\ t = \text{false} \Rightarrow t' = t$

Proof of the noninterference property for remove on CNode, VSpace or IContr objects where the removed capability points on an entity in the same domain:

$$\begin{aligned}
 & \forall e \in D1. \\
 & \quad \text{value_of } s' e \stackrel{**}{=} \text{value_of } s e \stackrel{*}{=} \text{value_of } t e \stackrel{***}{=} \text{value_of } t' e \\
 & \quad \wedge \text{caps_of } s' e \stackrel{**}{=} \text{caps_of } s e \stackrel{*}{=} \text{caps_of } t e \stackrel{***}{=} \text{caps_of } t' e \\
 & \quad \wedge \text{subSys } s' e \stackrel{**}{=} \text{subSys } s e \stackrel{*}{=} \text{subSys } t e \stackrel{***}{=} \text{subSys } t' e \\
 & \Rightarrow \text{equiv_nonin } s' t' D1 \Rightarrow s' \stackrel{D1}{\sim} t'
 \end{aligned}$$

With $s' \stackrel{D1}{\sim} t'$ the noninterference property for **remove** on CNode, VSpace or IContr objects where the removed capability points on an entity in the same domain is fulfilled.

- Target object = AEP or SPage object

If the removed capability points to an AEP or SPage object, it may be possible that information flows out of the H domain to the L domain. Figure 26 displays that no information flows to Domain 1.

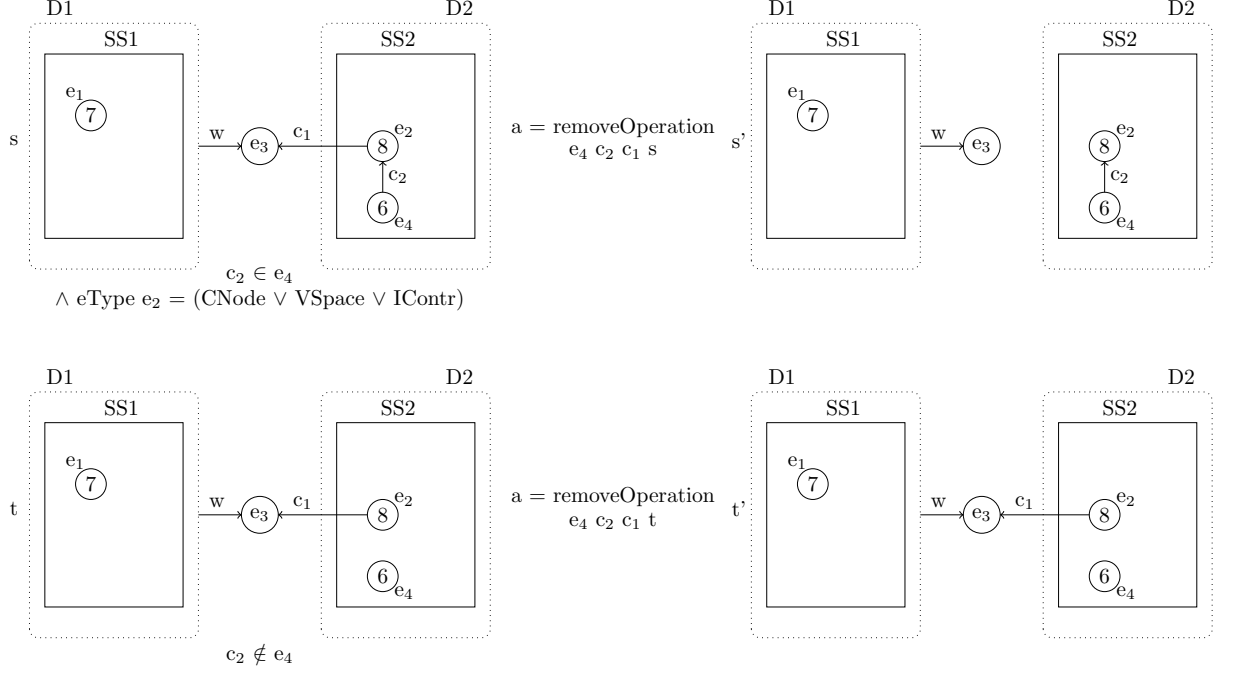


Figure 26: Noninterference for Remove on object types = CNode, VSpace or IContr.
The removed capability points to an entity outside the H domain

Preconditions:

- * $s \stackrel{D1}{\sim} t \equiv \text{equiv_nonin } s \ t \ D1$
- ** $\text{removeOperation } e_2 \ c_1 \ c_2 \ s$ removes a capability $\in e_2 \notin D1$ that points on an entity $\notin D1$. That means it has no impact on any entity $\in D1$
- *** $\text{legal } (\text{SysRemove } e_2 \ c_1 \ c_2) \ t = \text{false} \Rightarrow t' = t$

Proof of the noninterference property for remove on CNode, VSpace or IContr objects where the removed capability points on an entity in the same domain is fulfilled:

$\forall e \in D1.$

$$\begin{aligned}
 & \text{value_of } s' \ e \stackrel{**}{=} \text{value_of } s \ e \stackrel{*}{=} \text{value_of } t \ e \stackrel{***}{=} \text{value_of } t' \ e \\
 & \wedge \text{caps_of } s' \ e \stackrel{**}{=} \text{caps_of } s \ e \stackrel{*}{=} \text{caps_of } t \ e \stackrel{***}{=} \text{caps_of } t' \ e \\
 & \wedge \text{subSys } s' \ e \stackrel{**}{=} \text{subSys } s \ e \stackrel{*}{=} \text{subSys } t \ e \stackrel{***}{=} \text{subSys } t' \ e \\
 & \Rightarrow \text{equiv_nonin } s' \ t' \ D1 \Rightarrow s' \stackrel{D1}{\sim} t'
 \end{aligned}$$

With $s' \stackrel{D1}{\sim} t'$ the noninterference property for remove on CNode, VSpace or IContr objects where the removed capability points on an entity in the same domain is fulfilled.

7.5.2 Remove on objects \neq CNode, VSpace and Interrupt Controller

On all other object types the execution of **remove** is not legal. But for the sake of completeness I differ between a target object of the removed capability in the executing domain and one outside.

- Target object of the removed capability is in the same domain
The execution is not legal because the object the operation is executed on \neq CNode, VSpace and Interrupt Controller.

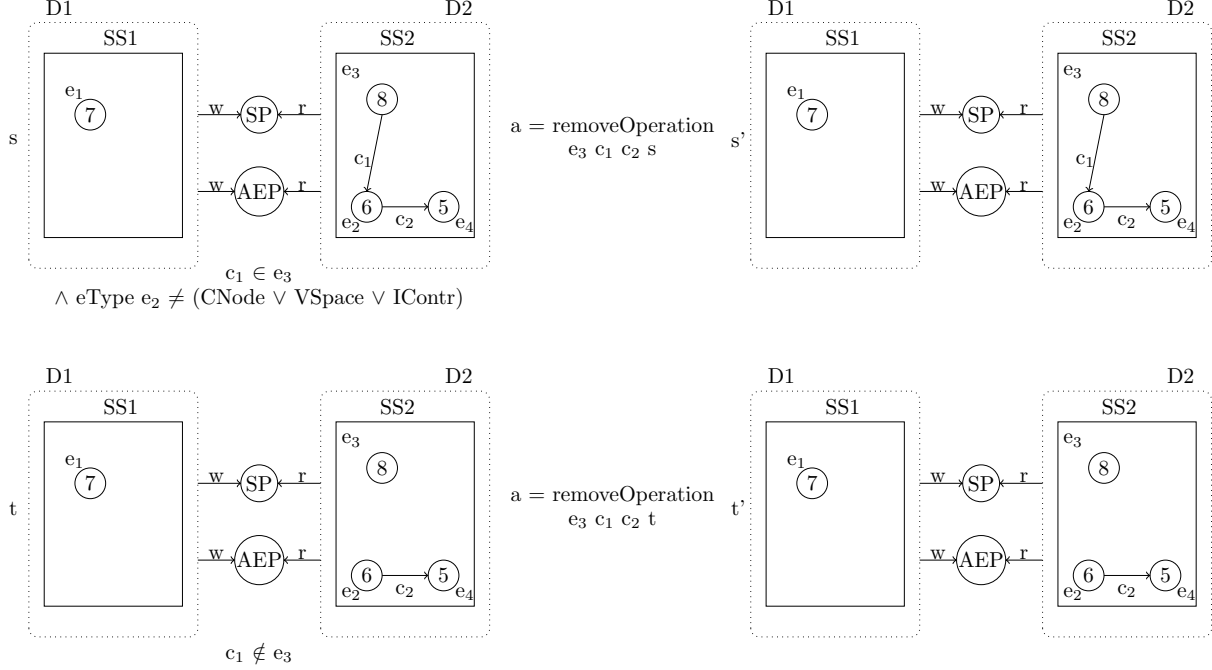


Figure 27: Noninterference for Remove on objects \neq CNode, VSpace and IContr. The removed capability points to an entity in the same domain

Preconditions:

- * $s \stackrel{D1}{\sim} t \equiv \text{equiv_nonin } s \ t \ D1$
- ** $\text{legal } (\text{SysRemove } e_2 \ c_1 \ c_2) \ s = \text{false} \Rightarrow s' = s$
- *** $\text{legal } (\text{SysRemove } e_2 \ c_1 \ c_2) \ t = \text{false} \Rightarrow t' = t$

Proof of the noninterference property for remove on objects \neq CNode, VSpace and IContr where the removed capability points on an entity in the same domain:

$\forall e \in D1.$

$$\begin{aligned}
 & \text{value_of } s' \ e = \text{value_of } s \ e = \text{value_of } t \ e = \text{value_of } t' \ e \\
 & \wedge \text{ caps_of } s' \ e = \text{caps_of } s \ e = \text{caps_of } t \ e = \text{caps_of } t' \ e \\
 & \wedge \text{ subSys } s' \ e = \text{subSys } s \ e = \text{subSys } t \ e = \text{subSys } t' \ e \\
 & \Rightarrow \text{equiv_nonin } s' \ t' \ D1 \Rightarrow s' \stackrel{D1}{\sim} t'
 \end{aligned}$$

With $s' \stackrel{D1}{\sim} t'$ the noninterference property for remove on objects \neq CNode, VSpace and IContr where the removed capability points on an entity in the same domain is fulfilled.

- Target object = AEP or SPage

If the removed capability points to an AEP or SPage object, also nothing happens to Domain 1 as the execution is not legal.

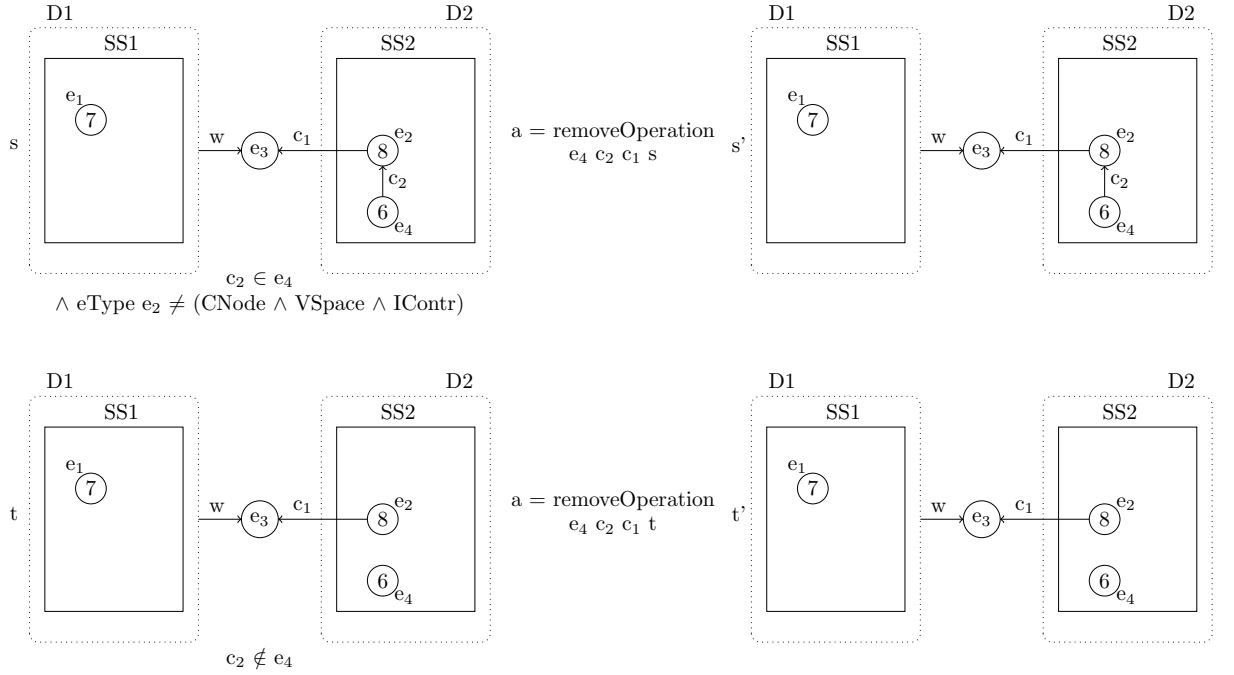


Figure 28: Noninterference for Remove on object types \neq CNode, VSpace or IContr.
The removed capability points to an entity outside the H domain

Preconditions:

- * $s \stackrel{D1}{\sim} t \equiv \text{equiv_nonin } s \ t \ D1$
- ** $\text{legal } (\text{SysRemove } e_2 \ c_1 \ c_2) \ s = \text{false} \Rightarrow s' = s$
- *** $\text{legal } (\text{SysRemove } e_2 \ c_1 \ c_2) \ t = \text{false} \Rightarrow t' = t$

Proof of the noninterference property for remove on objects \neq CNode, VSpace or IContr where the removed capability points on an object = AEP \vee SPage:

$$\begin{aligned}
 & \forall e \in D1. \\
 & \quad \text{value_of } s' \ e \stackrel{**}{=} \text{value_of } s \ e \stackrel{*}{=} \text{value_of } t \ e \stackrel{***}{=} \text{value_of } t' \ e \\
 & \quad \wedge \text{caps_of } s' \ e \stackrel{**}{=} \text{caps_of } s \ e \stackrel{*}{=} \text{caps_of } t \ e \stackrel{***}{=} \text{caps_of } t' \ e \\
 & \quad \wedge \text{subSys } s' \ e \stackrel{**}{=} \text{subSys } s \ e \stackrel{*}{=} \text{subSys } t \ e \stackrel{***}{=} \text{subSys } t' \ e \\
 & \Rightarrow \text{equiv_nonin } s' \ t' \ D1 \Rightarrow s' \stackrel{D1}{\sim} t'
 \end{aligned}$$

With $s' \stackrel{D1}{\sim} t'$ the noninterference property for remove on objects \neq CNode, VSpace or IContr where the removed capability points on an entity in the same domain is fulfilled.

7.6 Revoke

8 Conclusion

Summarized I tried to show the noninterference property on the take-grant model as it was specified by the team of NICTA in the paper Noninterference for Operating System Kernels. This trial failed so I had to extend the model by **read** and **write** operations, a value and objecttype for entities and a check if the object type is able to perform the particular system operation.

With this adaptations it was feasible to investigate if the system operations satisfy the noninterference property.

The conclusion of the thesis is that the original model is not appropriate to show noninterference on it. With the extended one it was possible and every system operation fulfills it.

As a next step the noninterference property should be specified and verified formal for the extended model. This can also be done with the theorem proof assistant Isabelle/HOL.

References

- [1] T. Murray, D. Matichuk, M. Brassil, P. Gammie and G. Klein:
Noninterference for Operating System Kernels.
International Conference on Certified Programs and Proofs, pp. 126142, Kyoto, Japan, December, 2012
- [2] D. Elkaduwe, G. Klein and K. Elphinstone:
Verified Protection Model of the seL4 Microkernel.
Technical Report NRL-1474, NICTA, October, 2007
- [3] J. Andronick T. Bourke P. Derrin D. Greenaway D. Elkaduwe, G. Klein and K. Elphinstone R. Kolanski D. Matichuk T. Sewell S. Winwood:
Abstract Formal Specification of the seL4/ARMv6 API.
Version 1.3
- [4] D. von Oheimb
Information flow control revisited: Noninfluence = Noninterference + Nonleakage.
In *9th ESORICS*, volume 3193 of *LNCS*, pages 225-243, 2004.
- [5] D. Elkaduwe:
A Principled Approach To Kernel Memory Management.
PhD Thesis, UNSW CSE, Sydney, Australia, March, 2010
- [6] M. Grosvenor and A. Walker:
seL4 Reference Manual.
Version 10.0.0
- [7] G. Smith:
Principles of Secure Information Flow Analysis.
Chapter 13 (pp. 291-307) of *Malware Detection*, Springer-Verlag, 2007
- [8] J.N. Buxton and B. Randell:
Software engineering techniques.
Report on a conference sponsored by the NATO science committee, Rome, Italy, 27th to 31st October 1969