barkhausen institut

Microkernel Construction

Exercise 5: Capabilities

Nils Asmussen

2026-06-11

Roadmap

- Kernel objects and capability space
- Protection domains
- Capability lookup

- Hands-on
  - Capability space operations
  - Reimplementing `sys_create_ec`
  - Using capability in userspace

Get the Code

```shell
$ git clone https://github.com/Nils-TUD/MKC
$ git checkout exercise5
```

Shell

```shell
# build it
$ make
```

Shell

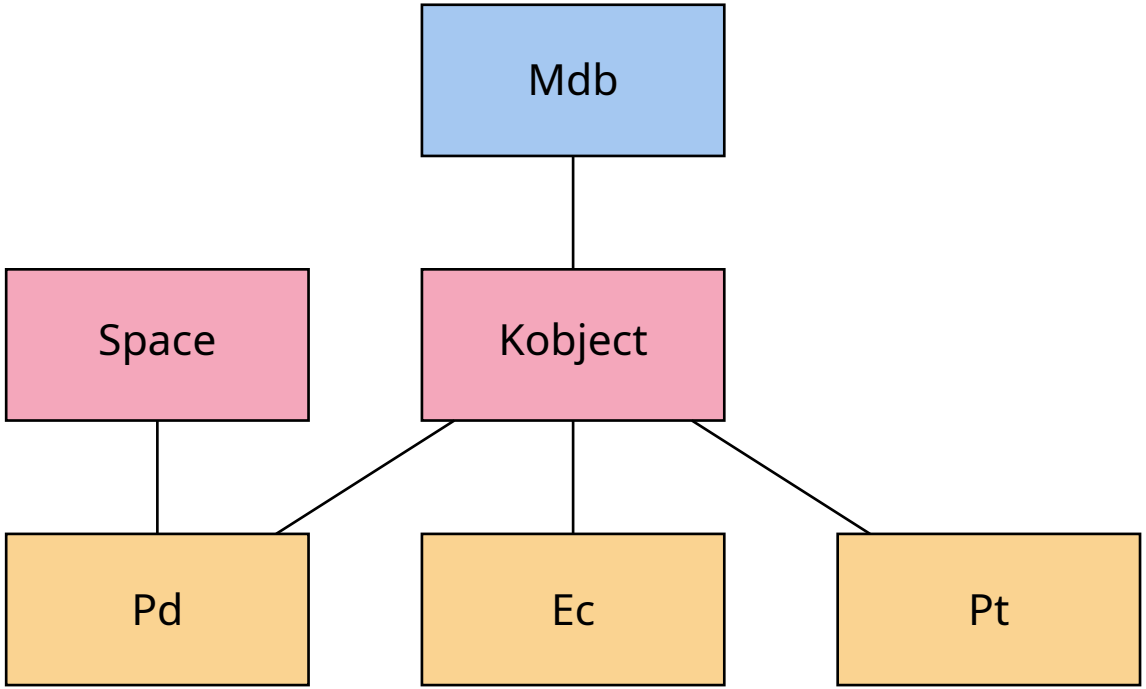
```shell
# run it
$ make run
```

Shell

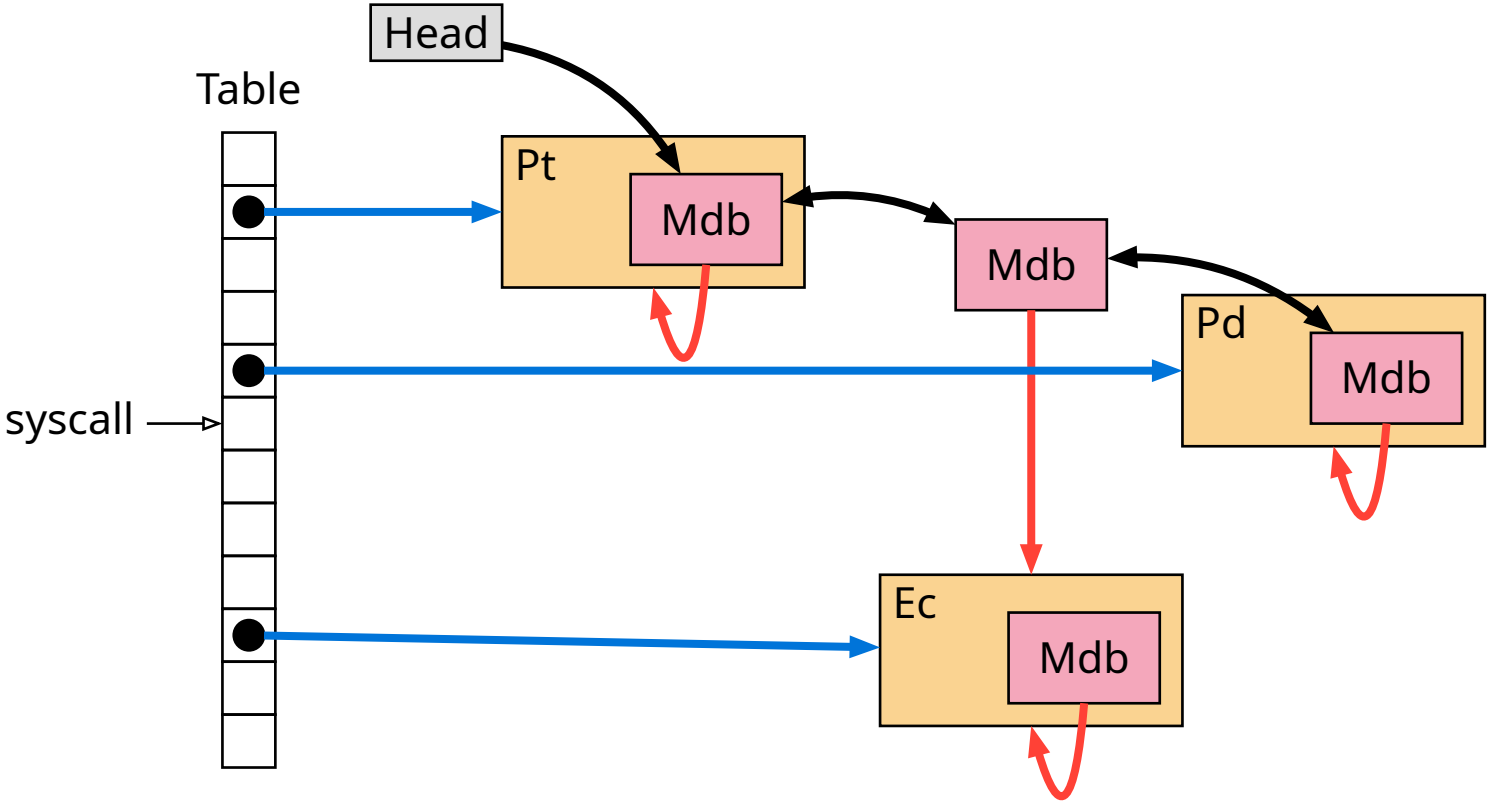
Capability Basics

- Introduced protection domains
  - No address space
  - Just object capabilities
- Mapping database
  - Doubly linked list instead of tree
  - Eagerly allocated 1-page table for quick access
- No delegate and revoke
  - So far: capabilities as a means to specify kernel objects
  - Next exercise: delegate and revoke

Kernel Objects



Capability Space



Task 1: Implement `{table,list}_insert`

1. Implement `Space::table_insert`
   - Look at `Capability`
   - Function should return false on invalid selectors

2. Implement `Space::list_insert`
   - Insert new node into doubly linked list
   - Note that there is a `head` element, initially `NULL`

Capabilities to Access Objects

- Got rid of:
  1. UTCB-address based specification of Ecs
  2. Searching for Ec on portal creation
  3. Portal id
  4. Linked list of portals
- New way:
  Table in `Space`, indexed by selector

Task 2: Rework Implementation of `sys_create_ec`

1. Lookup selector in capability space
   - You might get an invalid capability
   - You might get the wrong object type
   - Use `assert` for checks
2. Create a new Ec
   - Look at the changed constructors
3. Insert the created kernel object into your capability space
   - Use `Space::insert_root`

Task 3: Use Capabilities in Userspace

1. Create new Pd for receiver
   - All `sys_create_*` “allocate” an unused selector
   - … and return that selector
2. Create new local Ec in that Pd
   - The Ec will have no capabilities
   - Remember to use `local_ec_stack`
3. Create portal using the created local Ec
   - Remember the selector in `pt_sel`
   - Will be used in `sender`