barkhausen institut

Microkernel Construction

Exercise 6: Capability Delegation and Revocation

Nils Asmussen

2026-06-18

Roadmap

- Proper UTCB layout
- Delegation during IPC
- More sophisticated application scenario
- Revoke system call

- Hands-on
  - Capability delegation
  - Capability revocation
  - Using `sys_revoke` in userspace

Get the Code

```shell
$ git clone https://github.com/Nils-TUD/MKC
$ git checkout exercise6
```

Shell

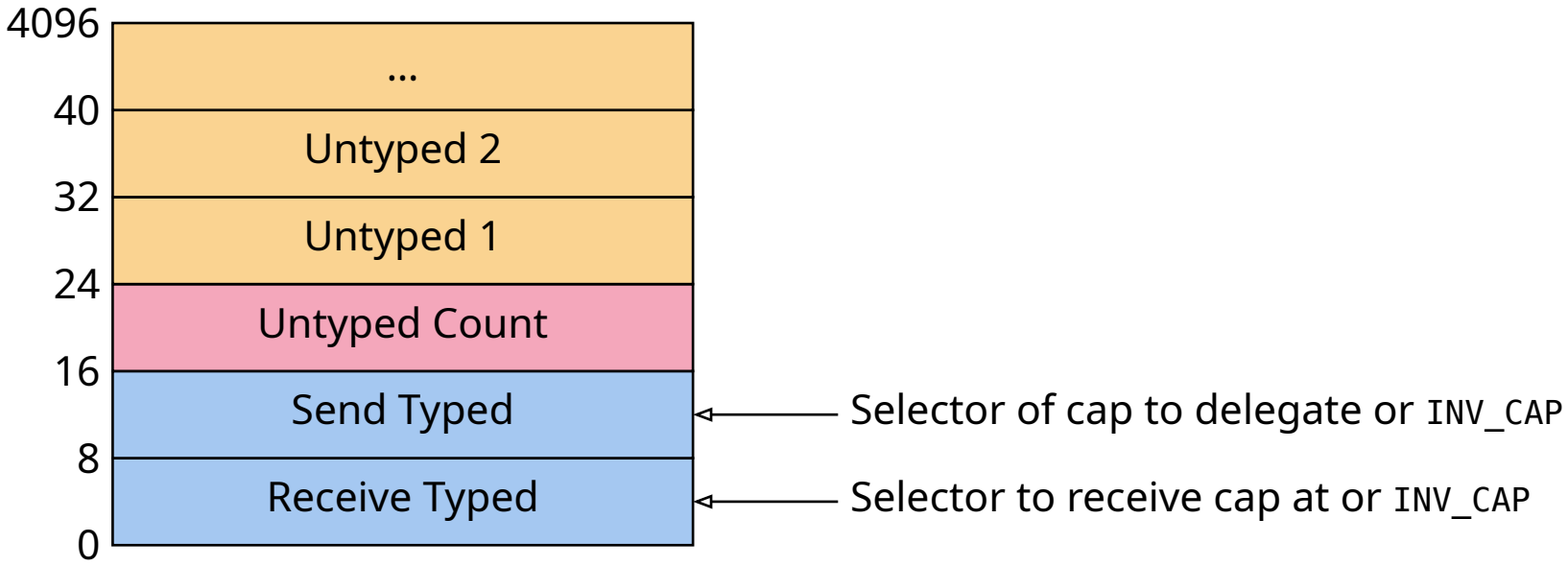
```shell
# build it
$ make
```

Shell

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

Shell

UTCB Layout


4096
...
40
Untyped 2
32
Untyped 1
24
Untyped Count
16
Send Typed
Selector of cap to delegate or INV_CAP
8
Receive Typed
Selector to receive cap at or INV_CAP
0

Delegation Infrastructure

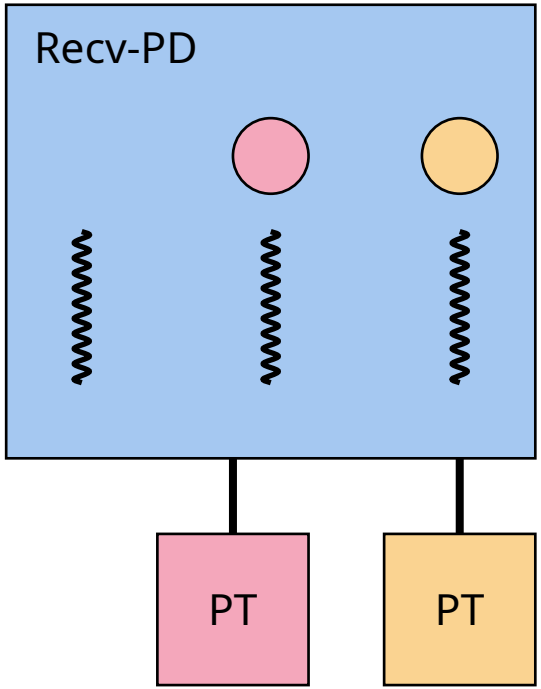
During IPC ...

```cpp
current->utcb->save(caller->utcb);
if (current->utcb->send_typed() != INV_CAP)
  delegate<false>();
```

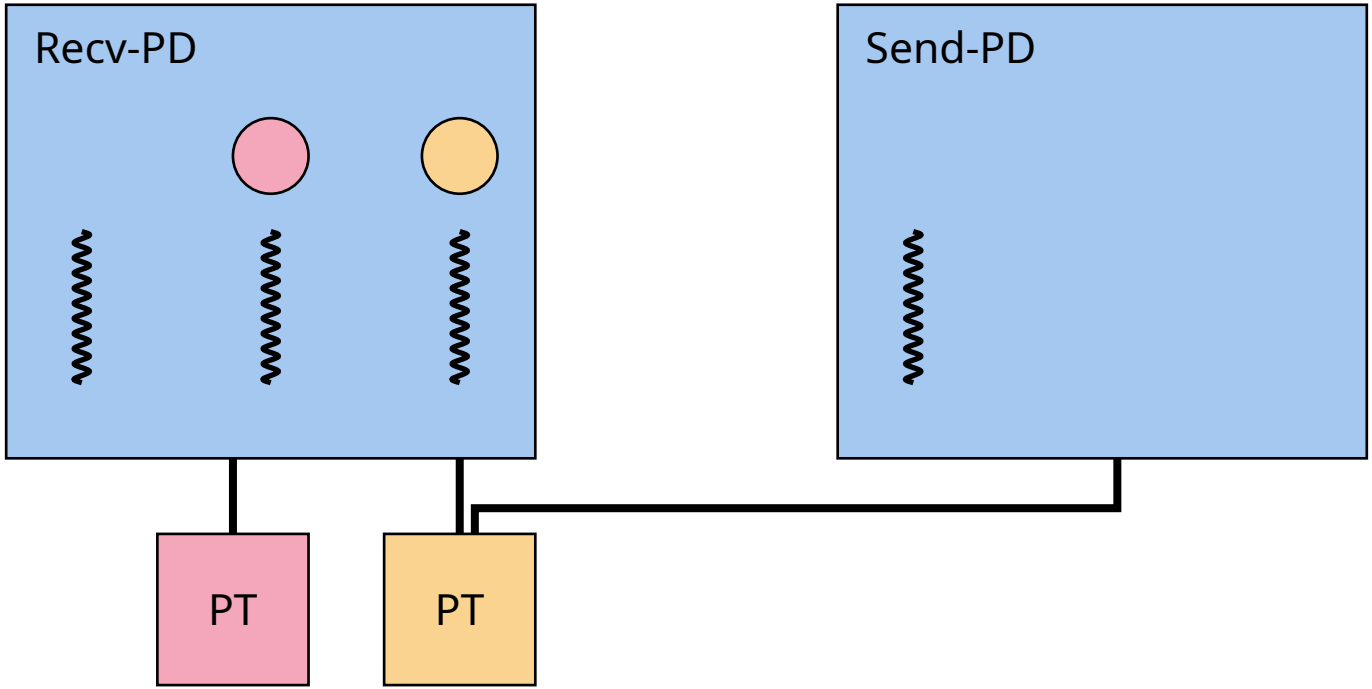
Ec::delegate

```cpp
template <bool C> void Ec::delegate() {
    Ec *ec = current->caller;
    Ec *src = C ? ec : current;
    Ec *dst = C ? current : ec;
    dst->pd->del_cap(src->pd, src->utcb->send_typed(), dst->utcb->recv_typed());
}
```

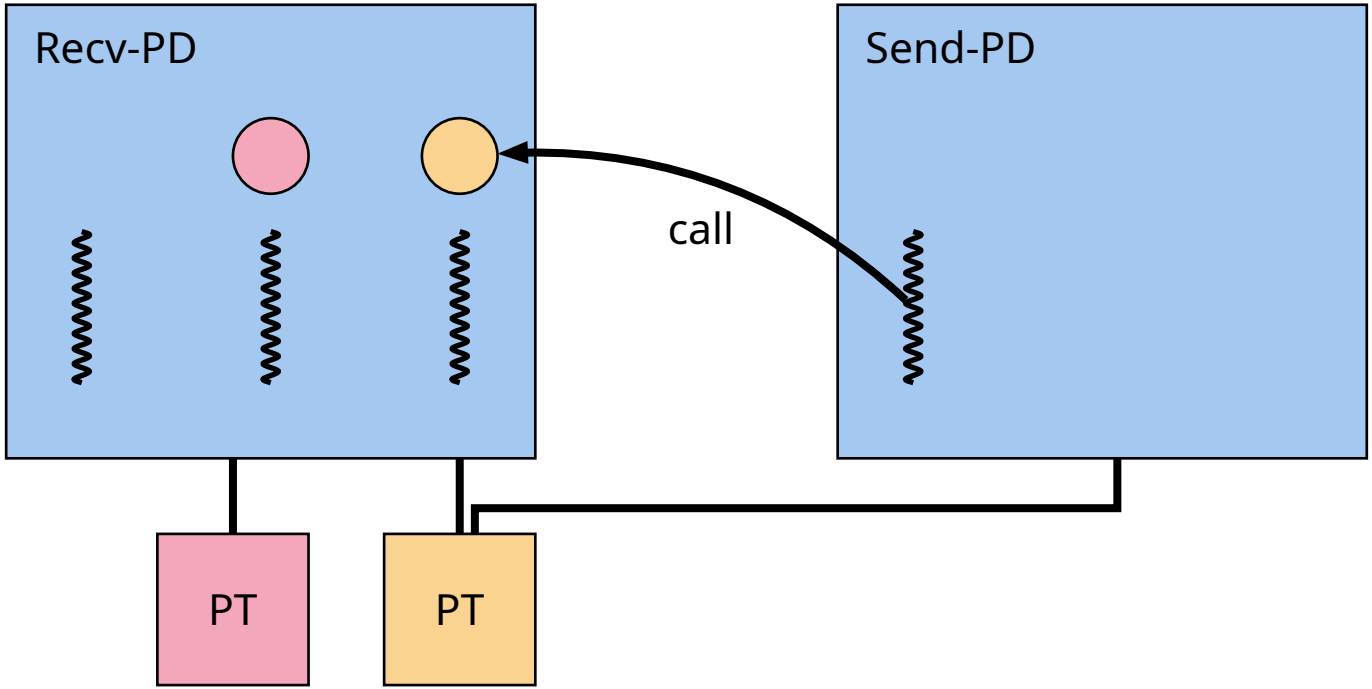
Userspace Scenario



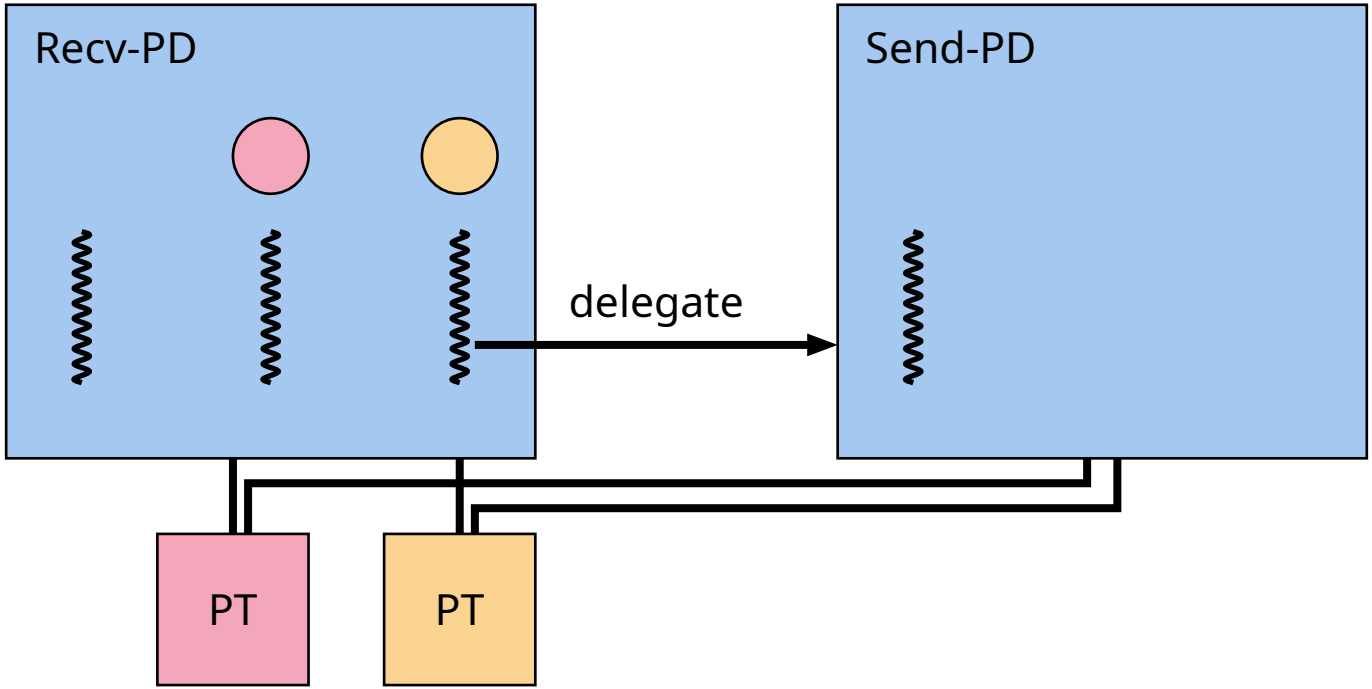
Userspace Scenario



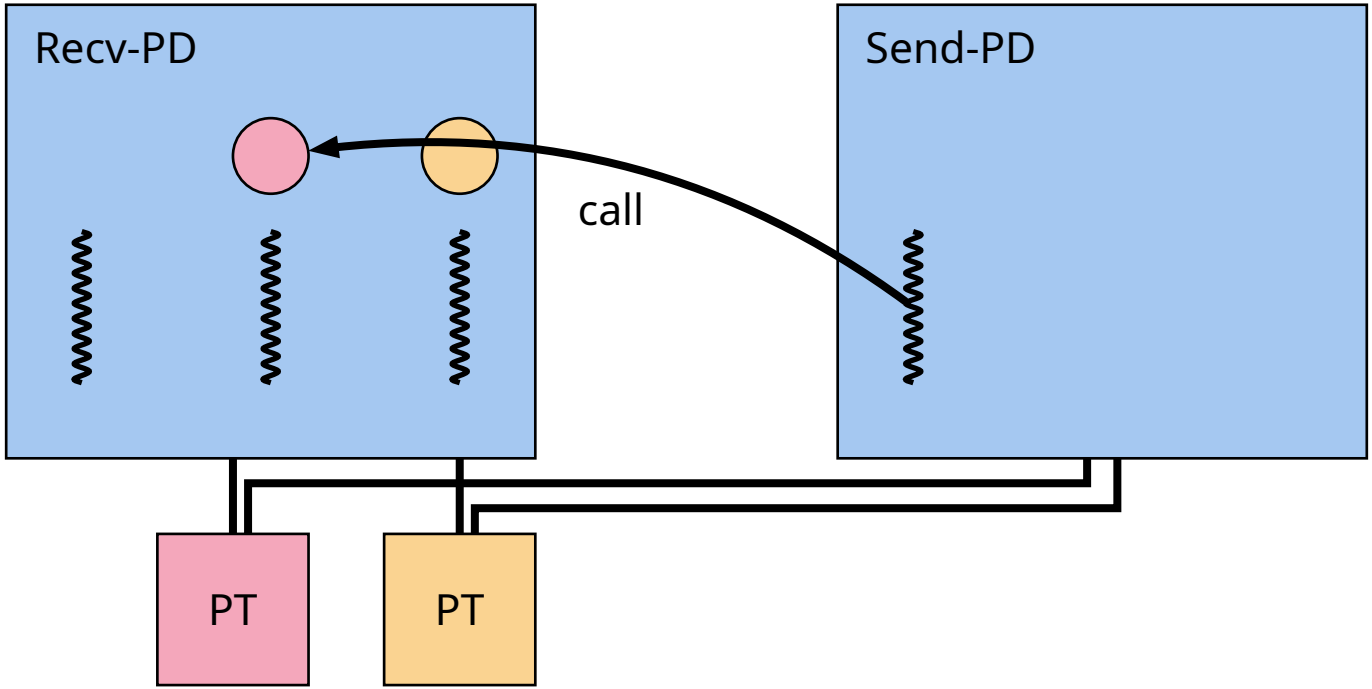
Userspace Scenario



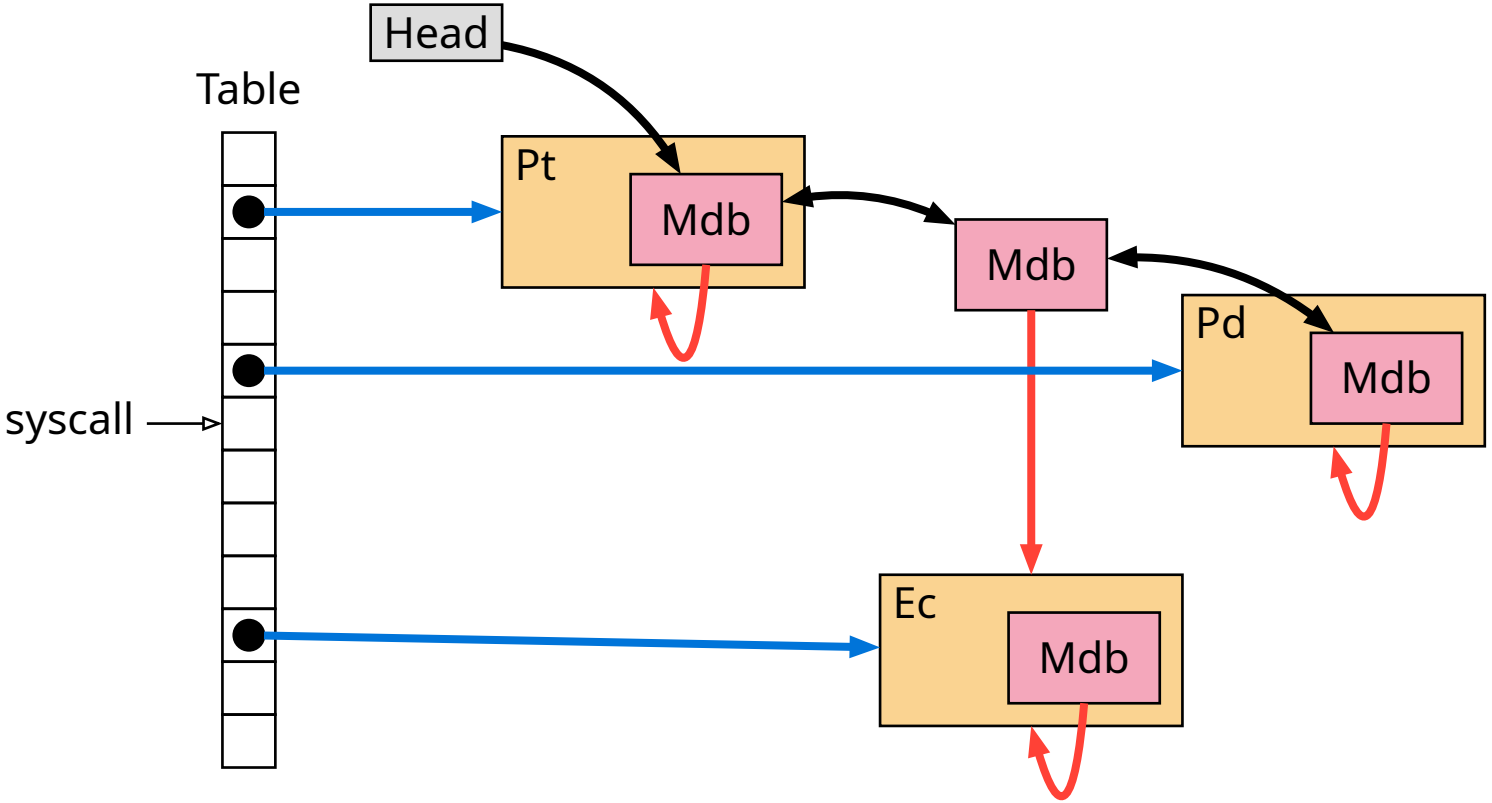
Userspace Scenario



Userspace Scenario



Capability Space



Task 1: Implement `Pd::del_cap`

- Find `Mdb` node
- Check if destination selector is unused
- Create new `Mdb` node
- Insert new node, update old node
- Remember delegation
  - Look at `Mdb::add_del`
- Check if userspace scenario works

Task 2: Implement `Pd::revoke_rec`

- Look at `Pd::revoke`
- Add recursive part in `Pd::revoke_rec`
- Remove from table and list
  - Look at `Space::table_remove`
  - And `Space::list_remove`
- Revoke children
  - Look at `Mdb::add_del`

- Use `sys_revoke` to test your implementation