TECHNISCHE UNIVERSITÄT DRESDEN

Department of Computer Science, Institute for System Architecture, Operating Systems Group

Paper Reading Group:
HYDRA: The Kernel of a Multiprocessor Operating System

Marcus Völp

Context

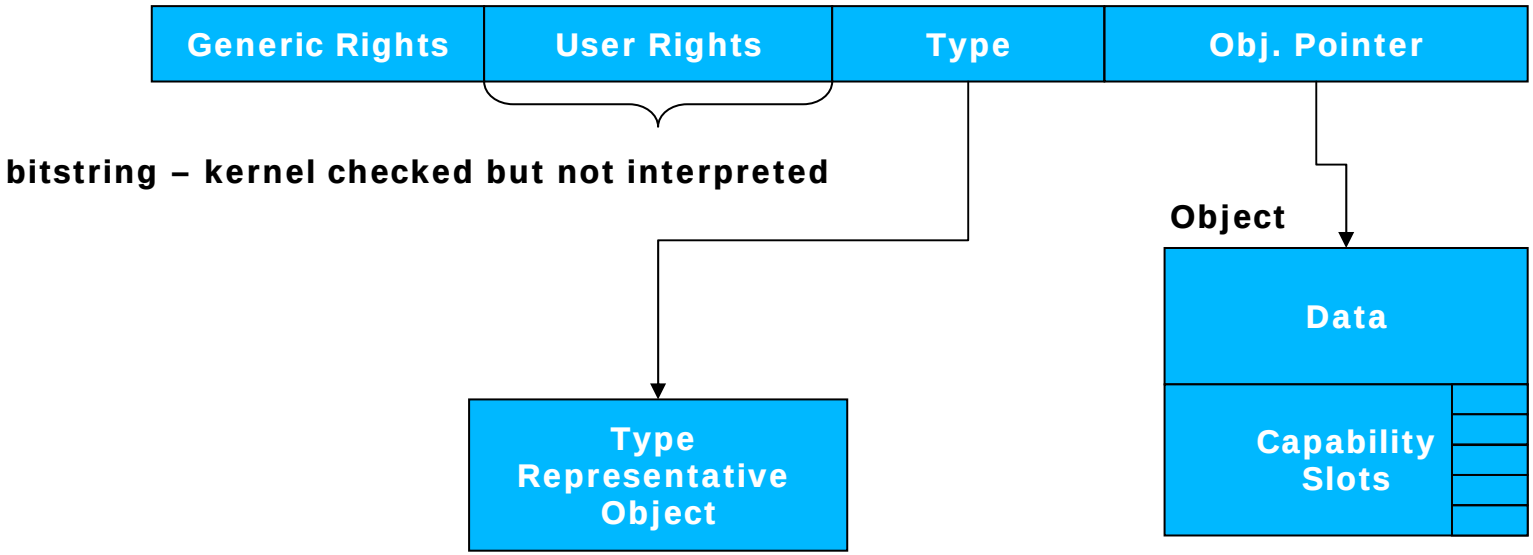
- Hydra (`74, `81):
  - (micro-)kernel for multiprocessor operating systems

- CMU: c.mmp Multiprocessor (`78)
  - 16 PDP11 minicomputers
  - 32MB shared memory (crossbar)
  - Local memory, devices
  - IPI factility
  - Global clock

- Paper:
  - protection mechanism in Hydra Kernel
  - take/grant capability model
  - protected procedure calls (intra process, similar to events)
  - semaphores, asynchronous IPC

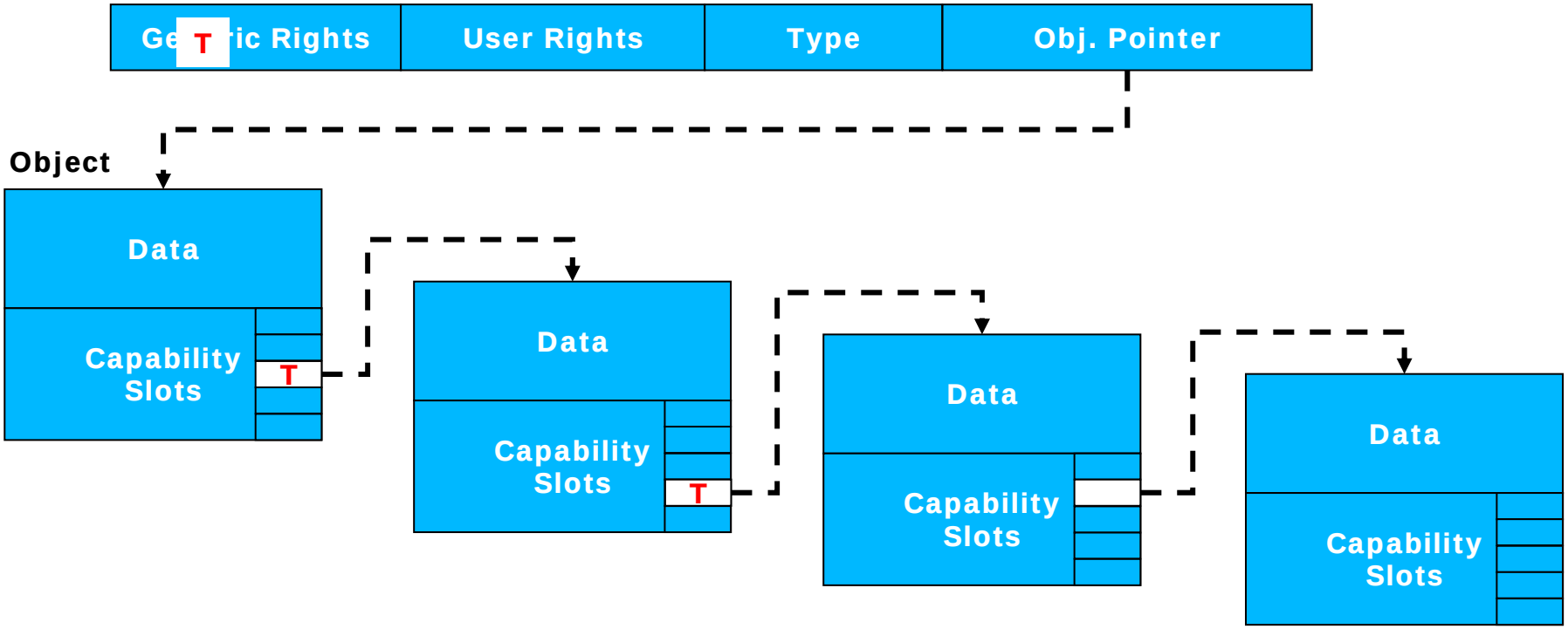
Hydra Capabilities

- User Defined / Kernel Enforced Capabilities



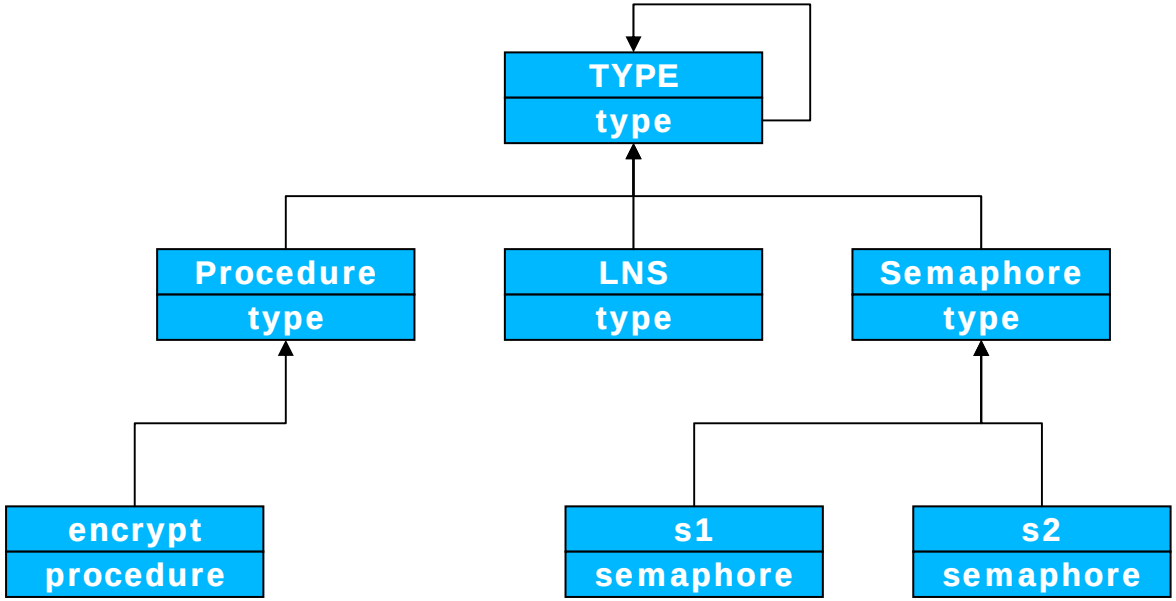
Hydra Capabilities

- Take(Walk) / Grant (in later paper) Protection Model
- Path: Cap:/3/4/2

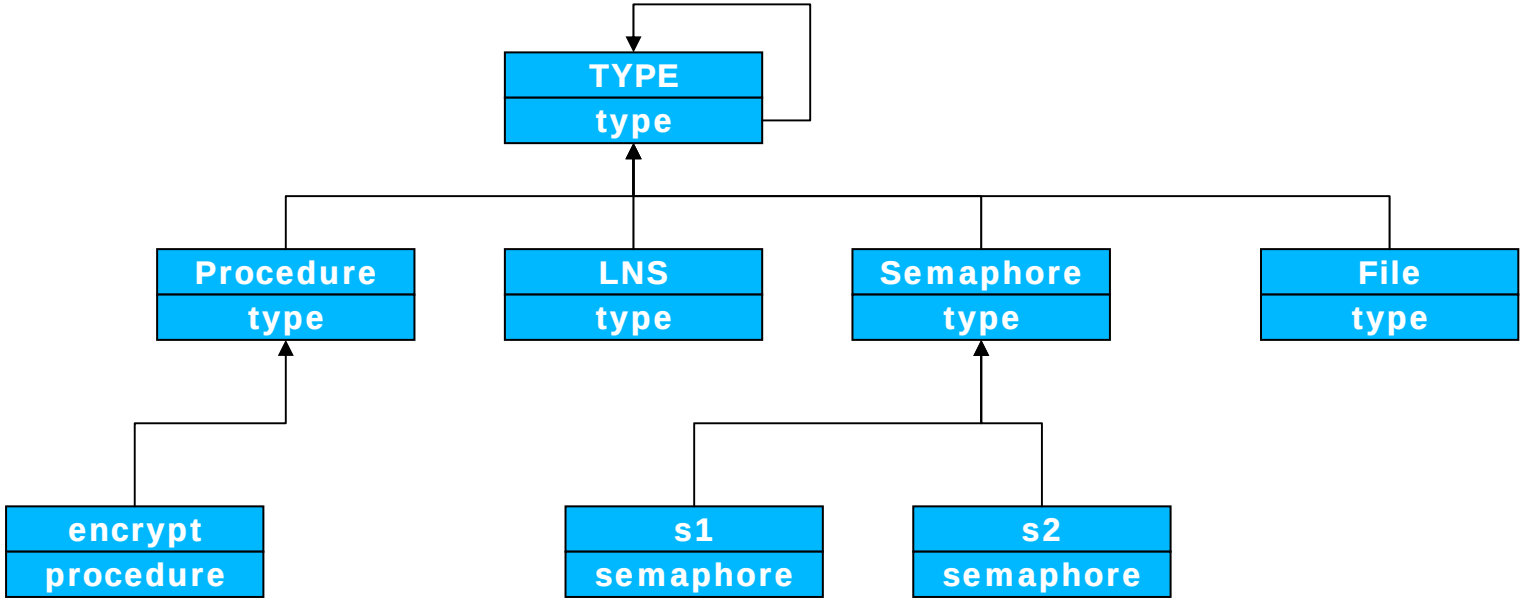


Walk != Indirection Capabilities

Extensible Types



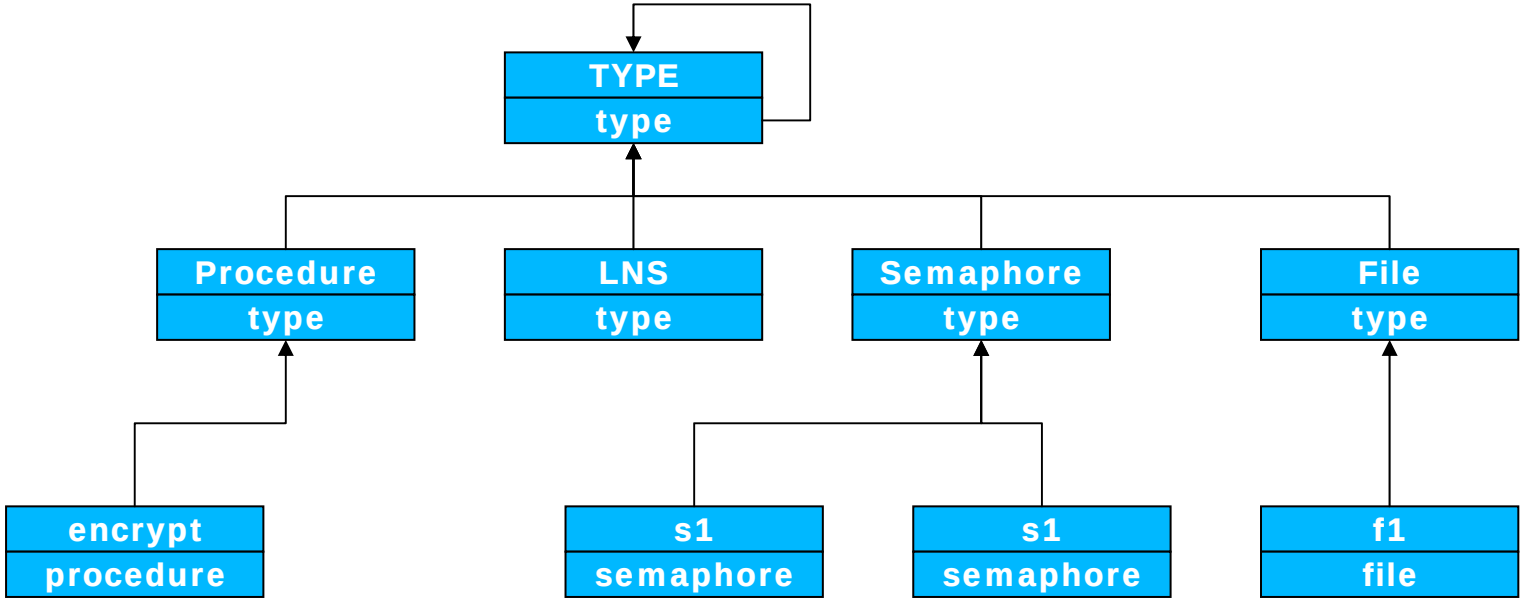
Extensible Types



Creating new Objects (e.g., Files)

1) **Create new type representative: File**

Extensible Types

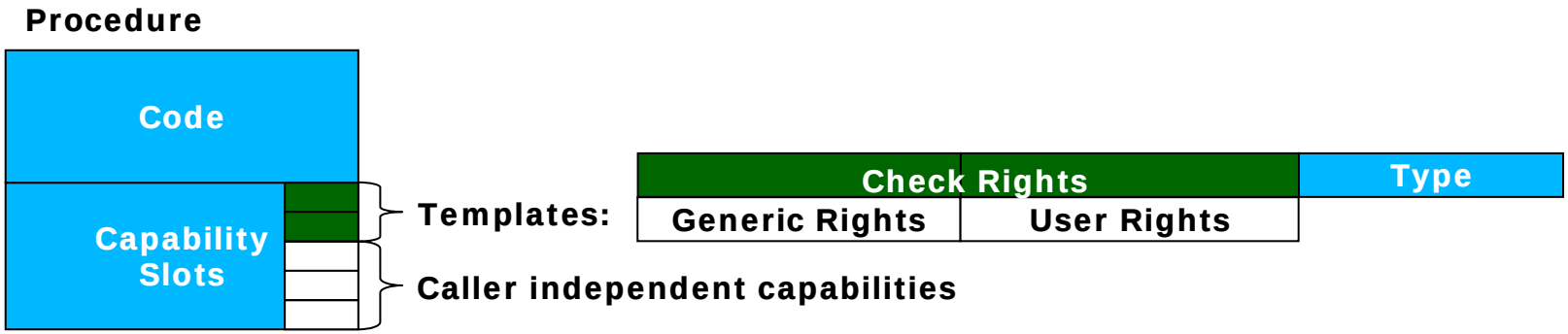


Creating new Objects (e.g., Files)

1) **Create new type representative: File**
2) **Create objects of new type: f1, ...**

Protected Procedure Calls

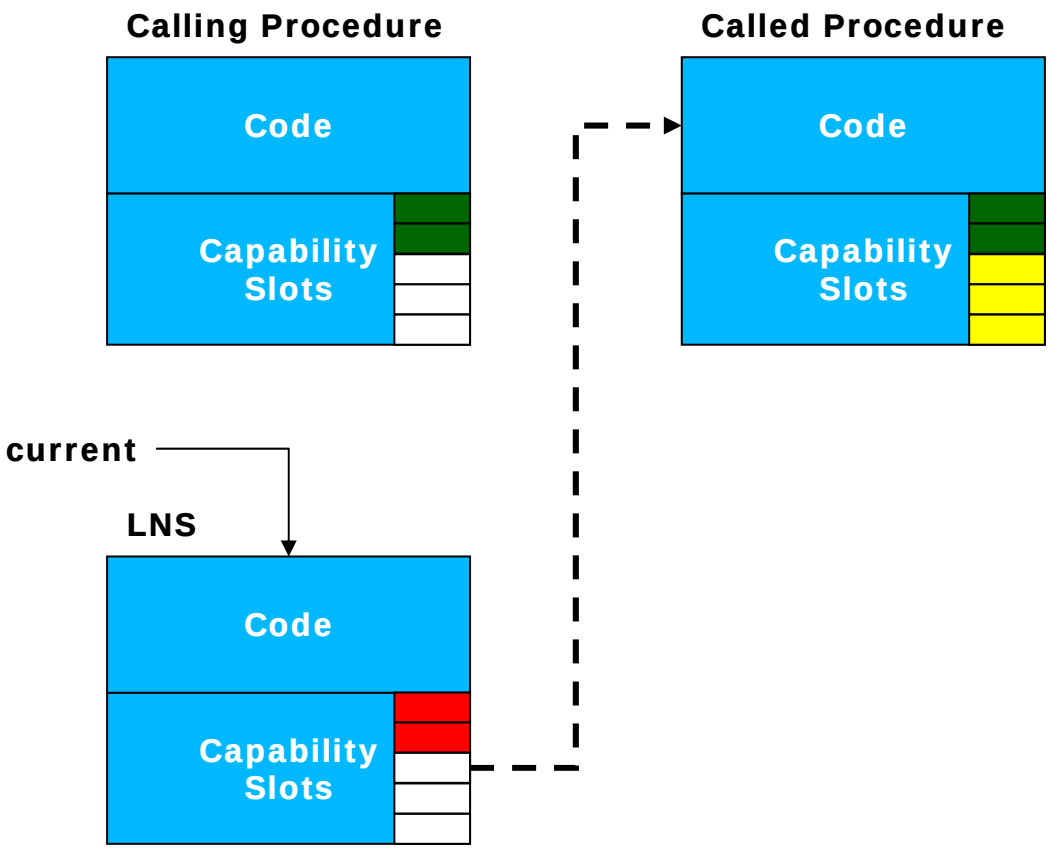
- Procedure
- Local Name Space (LNS)
- Templates



Protected Procedure Calls

- Procedure
- Local Name Space (LNS)
- Templates

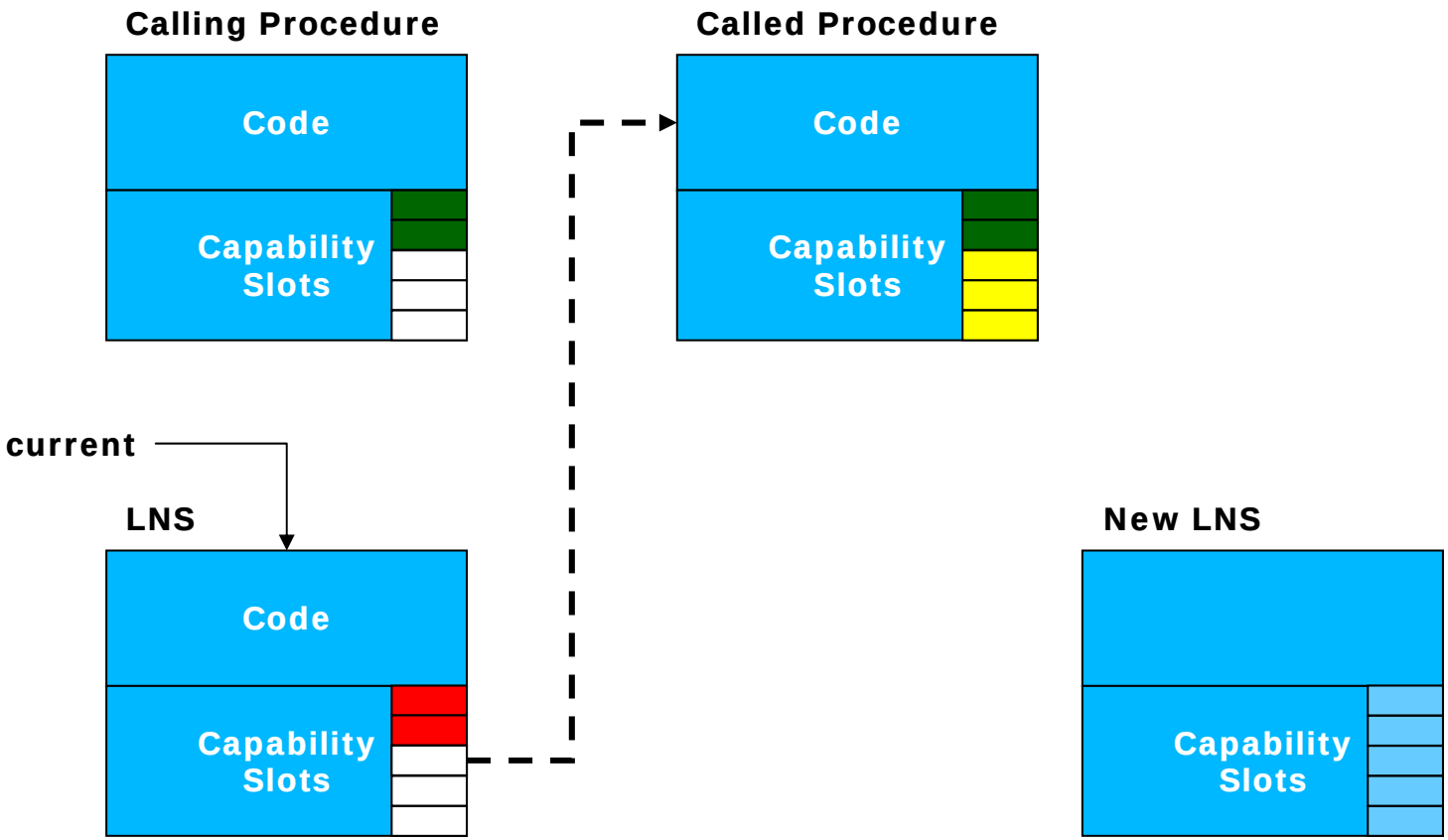
CALL (cap1, cap2)



Protected Procedure Calls

- Procedure
- Local Name Space (LNS)
- Templates

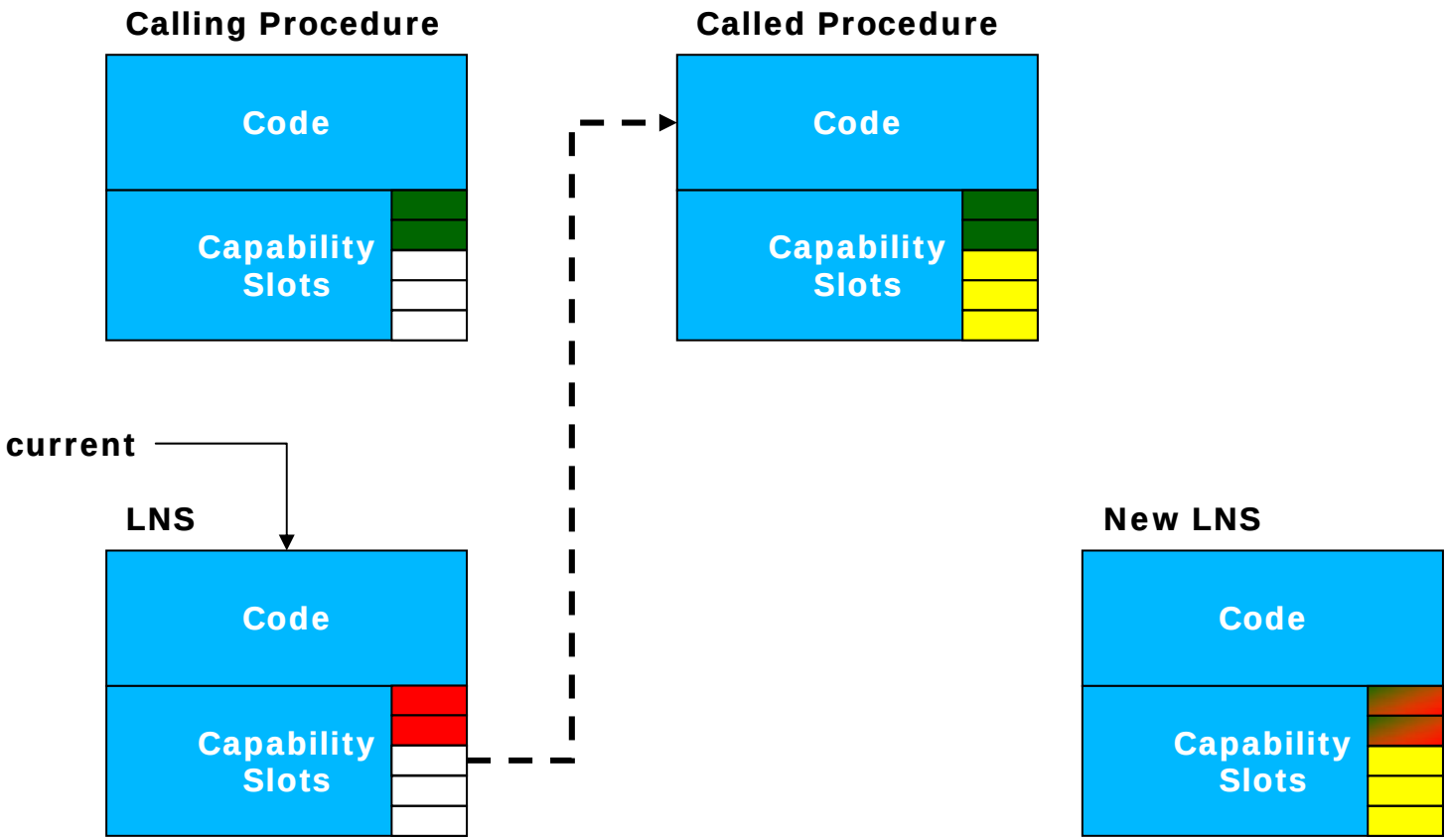
CALL (cap1, cap2)
1) Create new LNS



Protected Procedure Calls

- Procedure
- Local Name Space (LNS)
- Templates

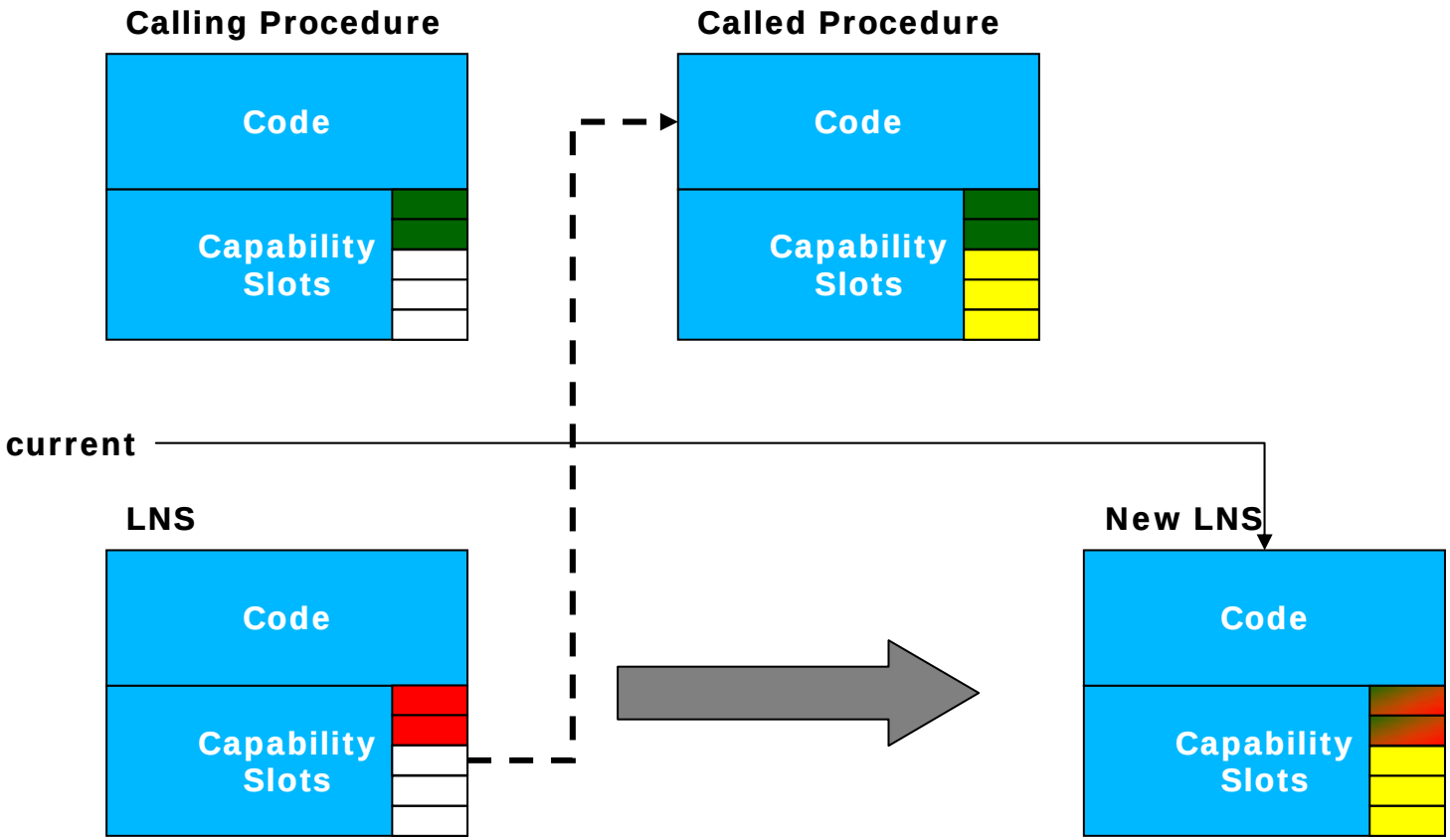
CALL (cap1, cap2)
1) Create new LNS
2) Transfer Parameter Caps



Protected Procedure Calls

- Procedure
- Local Name Space (LNS)
- Templates

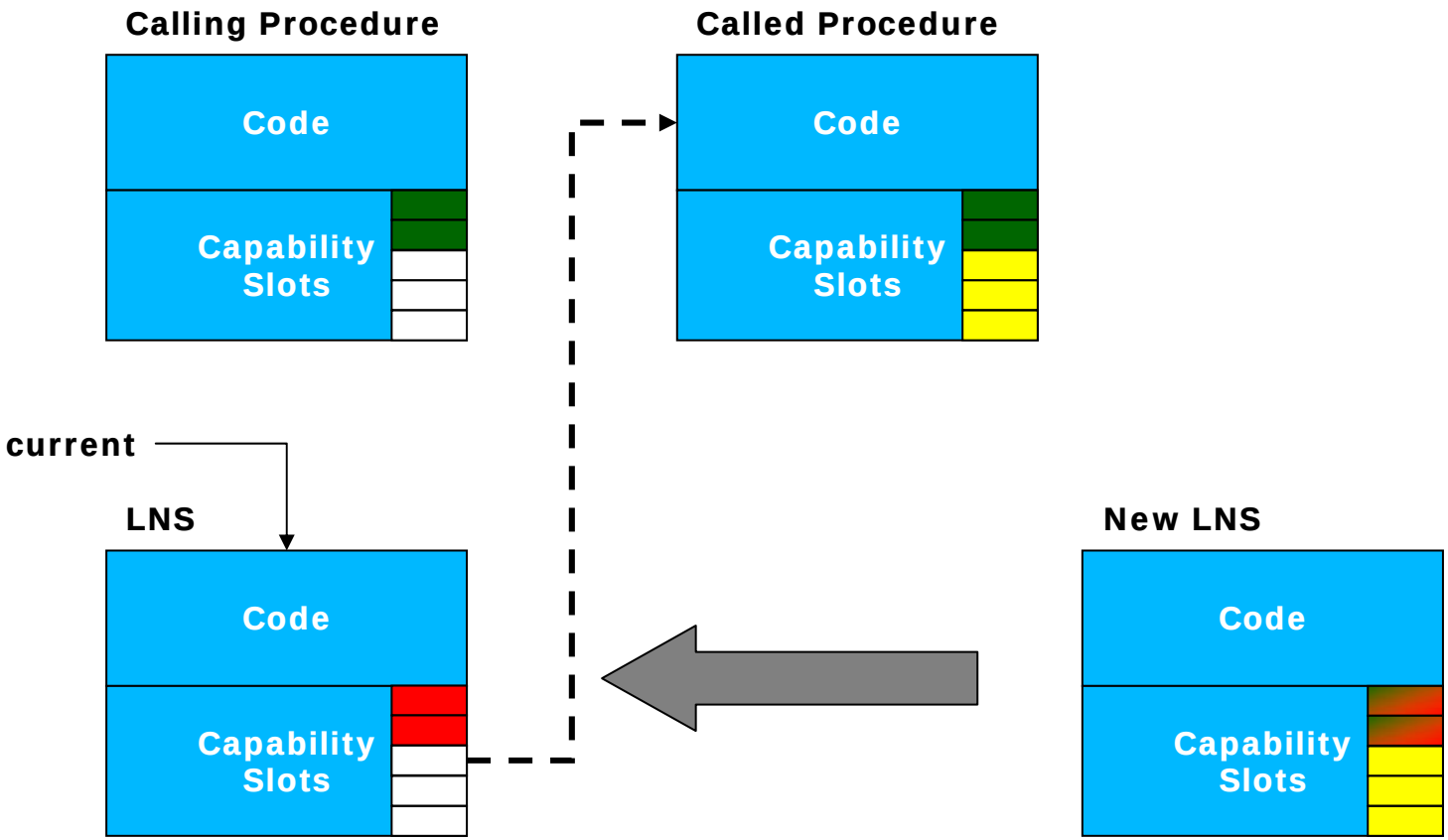
CALL (cap1, cap2)
1) Create new LNS
2) Transfer Parameter Caps
3) Transfer Control



Protected Procedure Calls

- Procedure
- Local Name Space (LNS)
- Templates

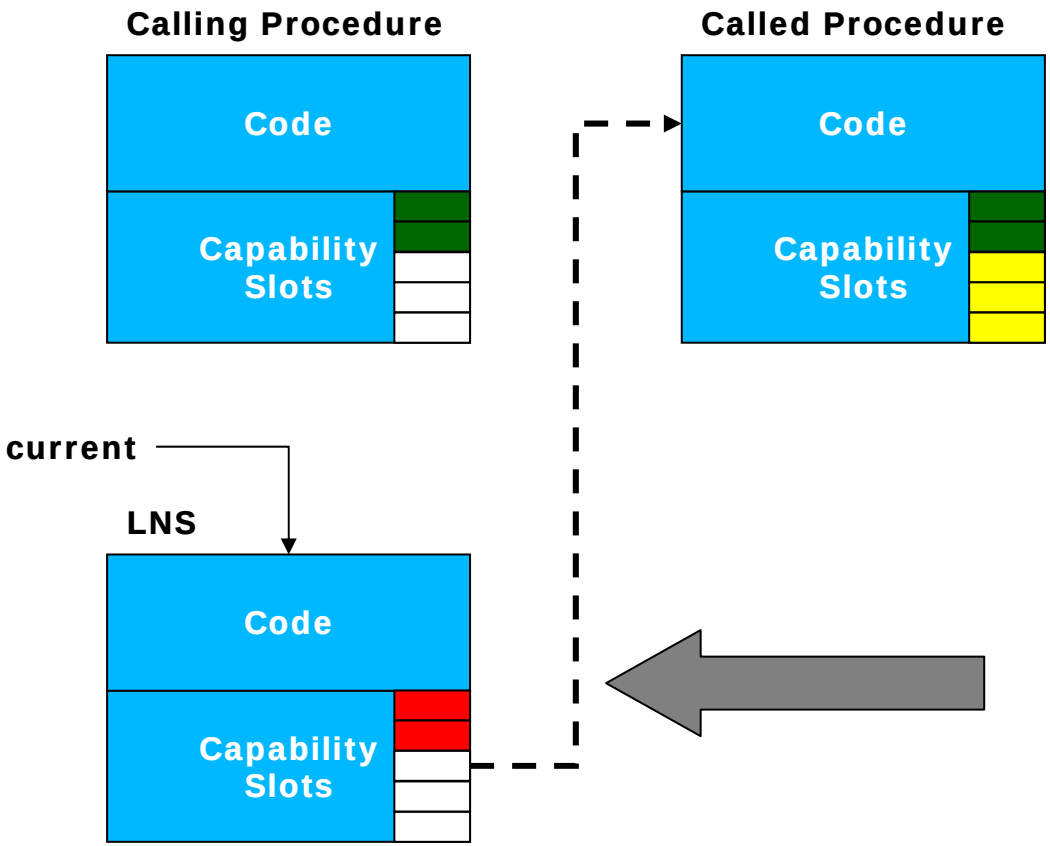
RETURN
1) Transfer Control to Caller



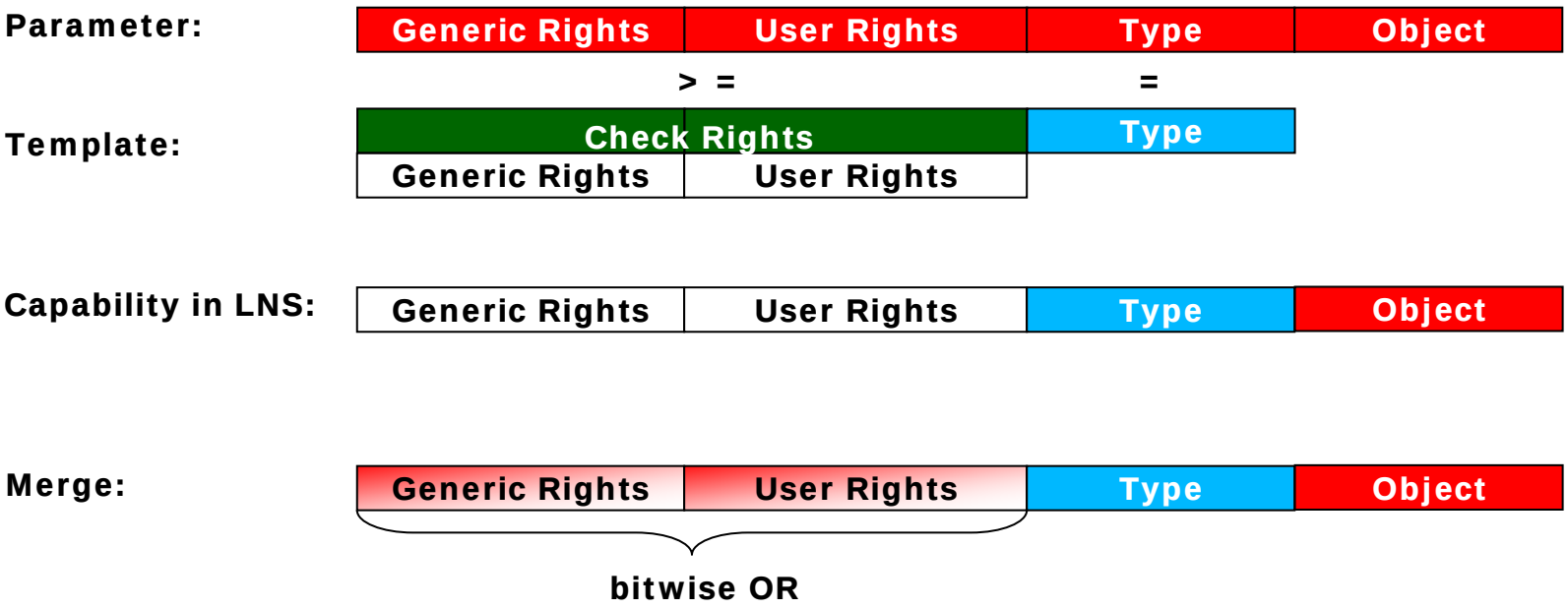
Protected Procedure Calls

- Procedure
- Local Name Space (LNS)
- Templates

RETURN
1) Transfer Control to Caller
2) Delete Callee LNS



Protected Procedure Call



Discussions

- Kernel enforced parameter check
  - Do we need to check call parameters (capabilities) in the caller context or is callee checking sufficient?

- Hierarchical layering
  - The authors argue against hierarchically layered systems.
    - Are hierarchies a bad thing?
    - Is hierarchical capability transfer (name servers) the right thing to do?