HYDRA: The Kernel of a Multiprocessor Operating System

Matthew Roberts
Contribution and Related Work
HYDRA strives to…

- Provide an environment for effective utilization of the hardware resources (multiprocessor computer system)
- Facilitate the construction of these environments
Two views are commonly held:

an operating system defines an "abstract machine" by providing facilities, or resources, which are more convenient than those provided by the "bare" hardware.

an operating system allocates (hardware) resources in such a way as to most effectively utilize them.
HYDRA provides...

- Introduction of new facilities (system extension)
  - Objects
    - Creation of new types
    - Apply operations to this type
    - Sharing and protection

- Creation of a highly secure system
Capability-based system...

- Capabilities for memory addressing and protection derived through access rights
- Supports security policy by controlling propagation of access rights according to the policy
  - Poorly suited to providing policy flexibility
HYDRA makes the transition from...

- Capability-based

To

- Object-based with capabilities
  - Object is the unit of protection.
  - Capabilities are used to determine if access to an object is allowed.
  - Easier to protect if divided into objects
Object-based system...

- Everything is an object
  - Ex// procedures, LNS, processes, disks, files, directories, etc...
- Abstract objects are the fundamental units
- Extend by adding new types of resources
- Manipulate by adding procedures for resources
- (Name, Type, Representation)
Separating mechanism and policy...

- Control mechanisms are separate from security policy.
- Mechanisms should be included in the kernel, but policies should not.
- Kernel provides mechanisms to implement policies.
- Allows for experimentation
So…we have

An object-based model with capabilities

&

Separation of mechanism and policy

Allowing for …

Flexibility

&

Ease of Extension
3 Object types:

- The kernel provides an execution environment with the interrelationships of the following:
  - Procedure
  - Local Name Space (LNS)
  - Process
Procedure Object…

- Static entity
- Name, parameters, output, and capability
  - CODE and DATA
  + Protection Facilities
    - Required capabilities
      - Caller Independent – specified at creation time
      - Caller Dependent – specified at execution time
      • (actual parameters)
Local Name Space (LNS)...

- Dynamic set of capabilities that a running procedure may use at run-time
- Created at procedure call
- Destroyed at procedure return
Process...

- Smallest unit that can be scheduled for execution
- Stack of LNS’s representing cumulative state of a single sequential task.
- Unit exploited for parallel processing capabilities
Related Work…

- Capability-based Systems
- KeyKOS
  - Persistent, pure capability operating system
- EROS (Extremely Reliable Operating System)
  - Pure capability system with capabilities uniquely identifying an object and a set of access rights