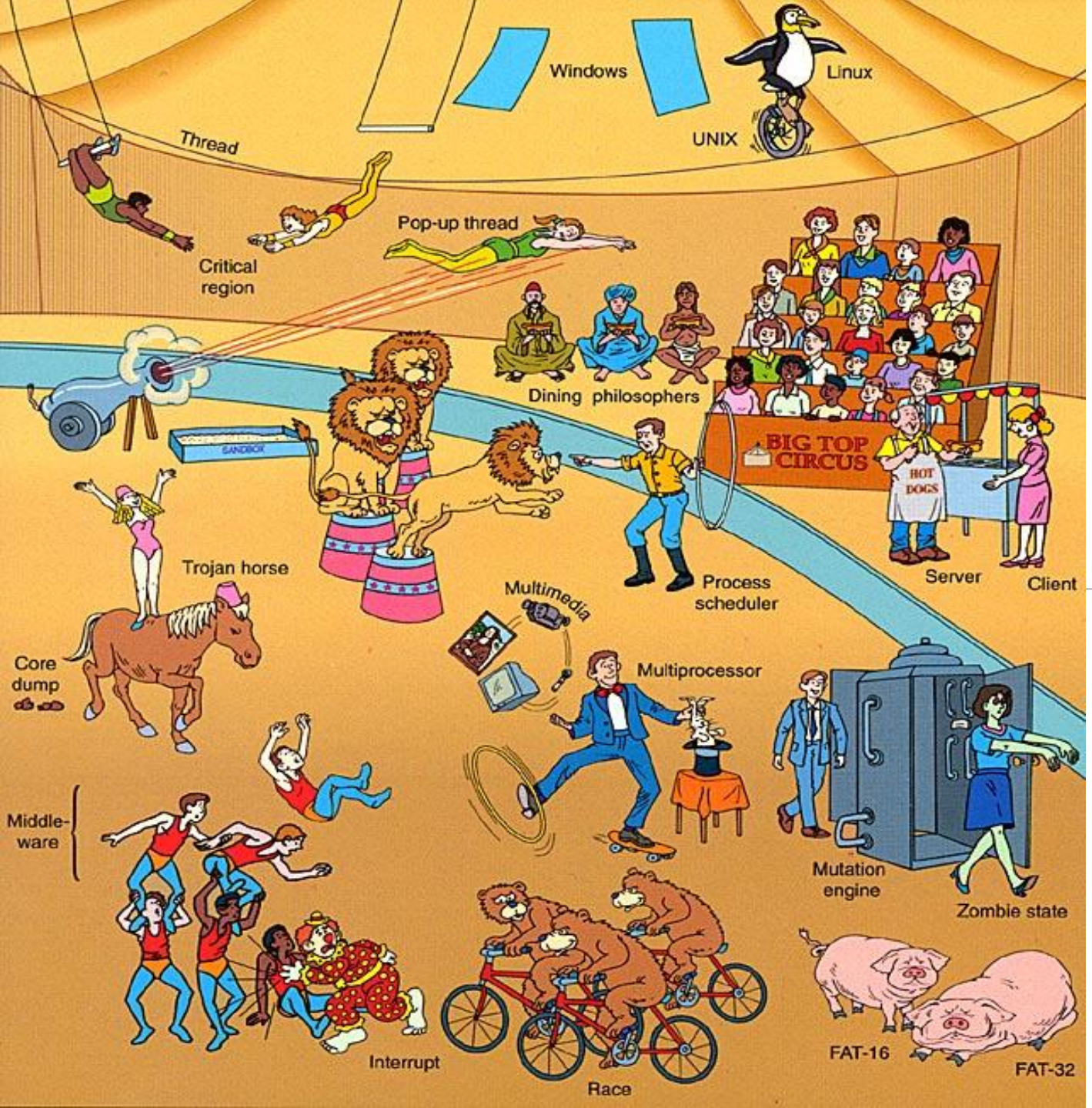
Computer Security
CS381

Operating System Security

Yuanyuan Zhang

Content

- Operating system
- Operating system security functions
  - Access control in general
  - Access control in OS
  - Isolation



Operating System

A Big Circus

OS Functionality

- Managing :
  - CPU
  - primary memory
  - external memory
  - I/O system
- Self-managing :
  - Robustness: the OS must function well
  - Security：preventing illegal operation and system invasion

OS Security Functions

- Access control
- Isolation

ACCESS CONTROL 访问控制

Access control in general

- Access control refers to exerting control over **who can interact with a resource**.
  - what you are allowed to do
  - focus is **policy**

- Goal: protect resources from unauthorized access

Multilevel Security Models

A model : Bell-LaPadula

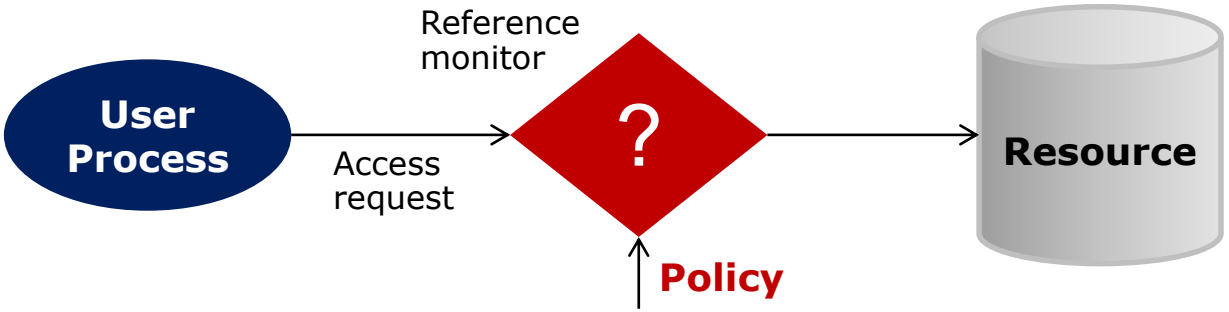
- **Bell–LaPadula (BLP) Model** is a state machine model used for enforcing access control in government and military applications
- a formal state transition model of computer security policy
- focuses on data confidentiality and controlled access to classified information, the entities in system are divided into subjects and objects
- Mandatory rules
  1. a subject at a given security level may not read an object at a higher security level (**no read-up**).
  2. a subject at a given security level must not write to any object at a lower security level (**no write-down**).
- discretionary
  - use of an access matrix to specify the access control
- Limitation: Only addresses confidentiality and control of writing

Further reading: Biba

- BLP: confidentiality
- Biba: integrity

Access control in OS

- Security assumption ：
  1. System knows about the identity of the user
  2. Resource is under the monitor of the system
  3. Monitor shall not be bypassed



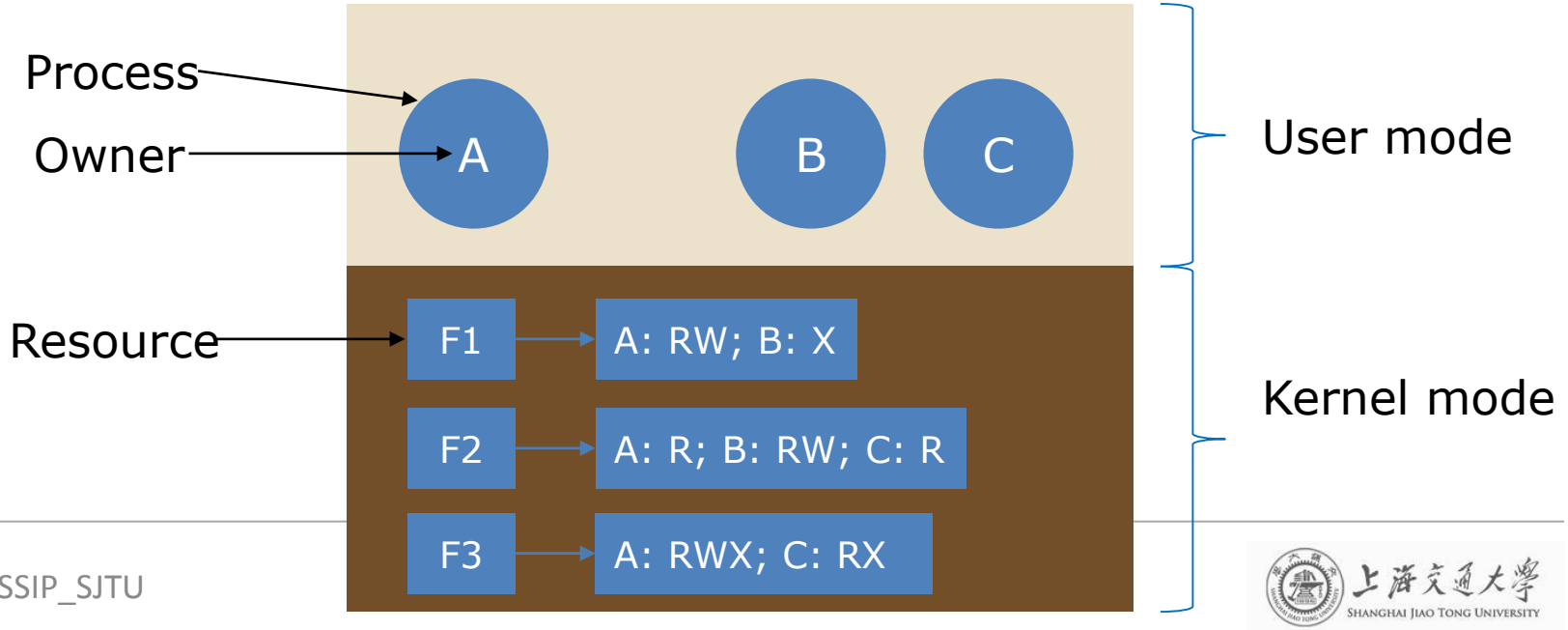
Access Control in OS

1. **Access Control List (ACL)**
2. **Capability**

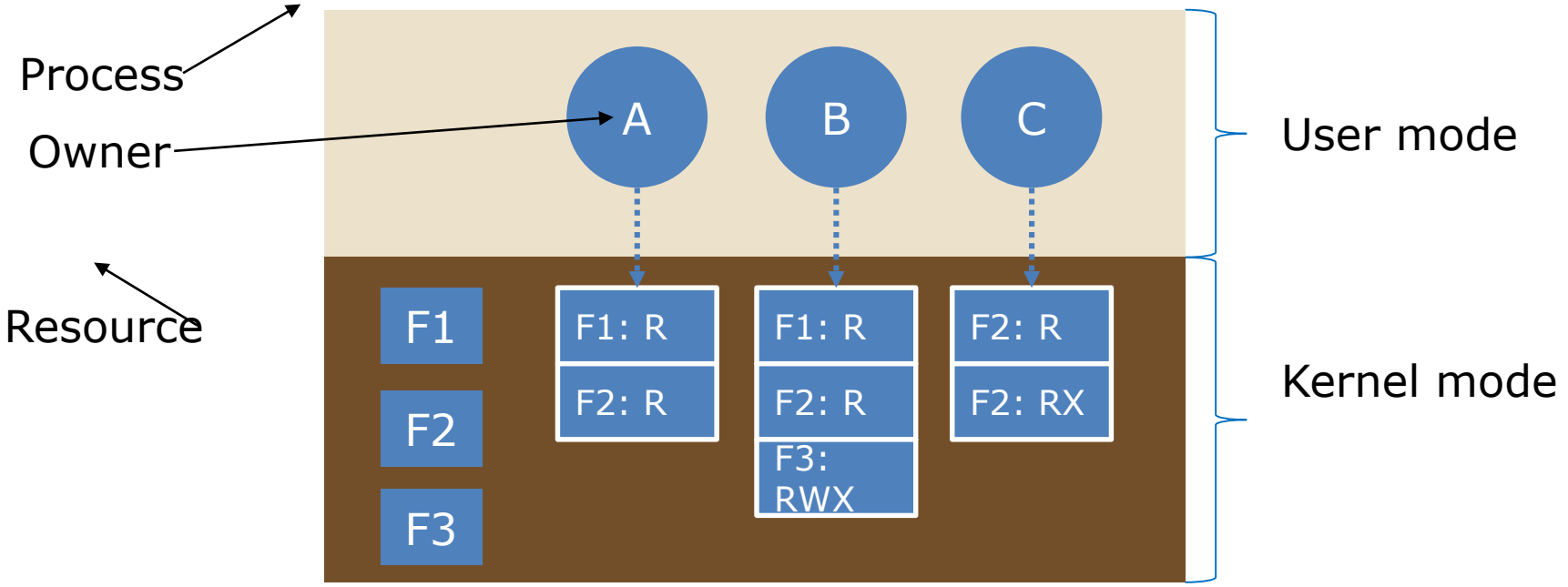
3. **DAC**
4. **MAC**

Access Control List (ACL)

	File 1	File 2	.....	File n
User 1	r	w	.....	-
User 2	w	w	.....	r
.....	.....	.....	.....	.....
User m	r	r	.....	w



Capability List (C-list)



DAC v.s. MAC

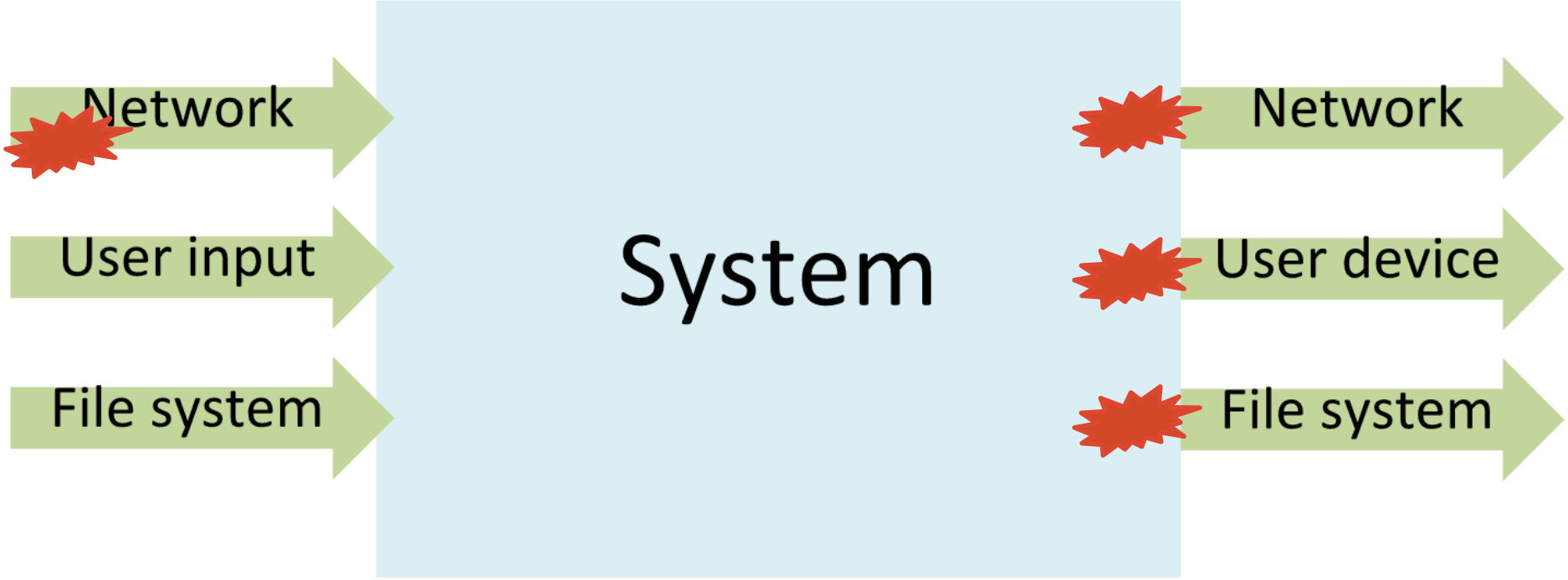
- Discretionary Access Control (DAC)
  - –自主访问控制
- Mandatory Access Control (MAC)
  - –强制访问控制

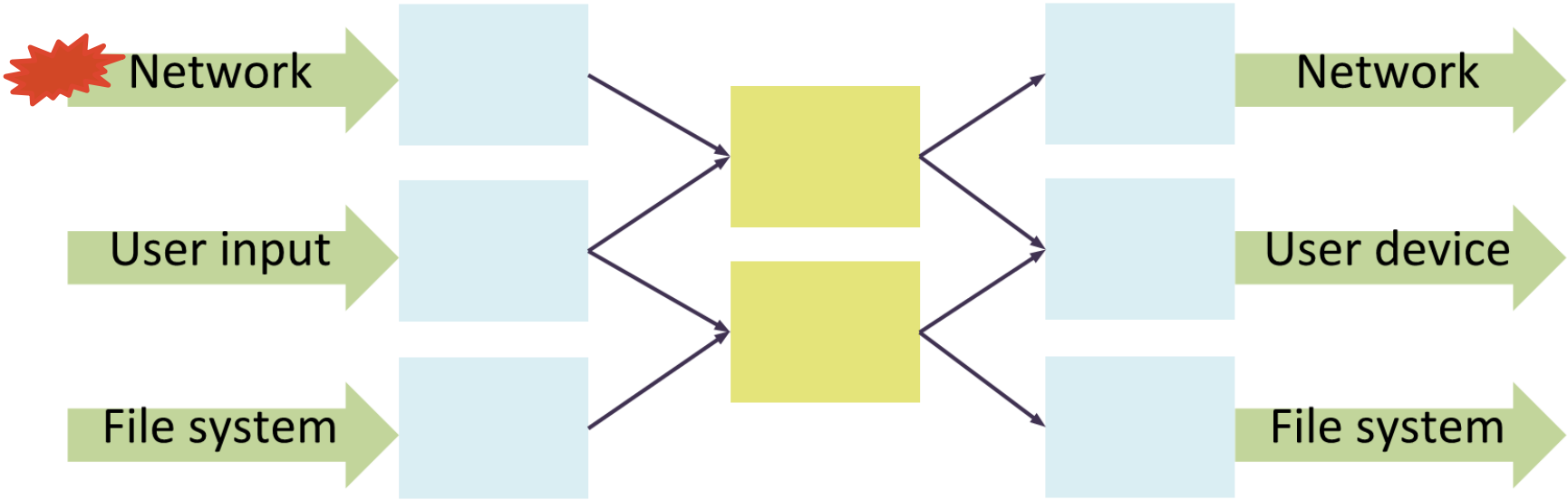
Further reading: SELinux


```
#ps -efZ | grep mail
system_u:system_r:sendmail_t    root      2661     1  0
12:30 ?        00:00:00 sendmail: accepting connections
system_u:system_r:sendmail_t    smmsp     2670     1  0
12:30 ?        00:00:00 sendmail: Queue runner@01:00:00 for /var/spool/clie
ntmqueue
```

ISOLATION 隔离


分隔思想
Compartmentalization/
Isolation


Network
User input
File system
System
Network
User device
File system


Network
User input
File system
Network
User device
File system

Methods of Isolation

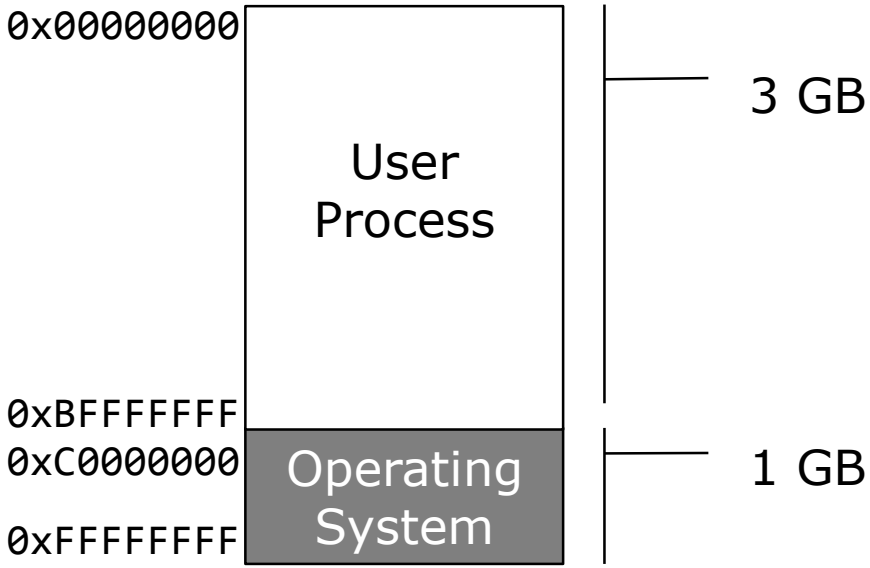
- **Physical**
  - Multiple printers, disks,...
- **Logical**
  - OS/environment provides isolation
- **Cryptographic**
  - Data and computation concealed cryptographically

Isolation in OS

- Memory protection 逻辑上隔离存储器空间
- Privilege mode 设定不同层次的特权级别

Memory Protection

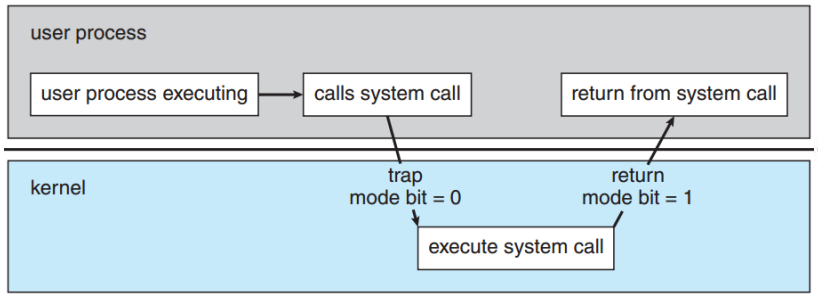
- Security Goal:
  - No interruption among multi processes and multi users
- Implementation:
  - Virtual address mapping
  - Executable space protection
    - W^X
    - DEP

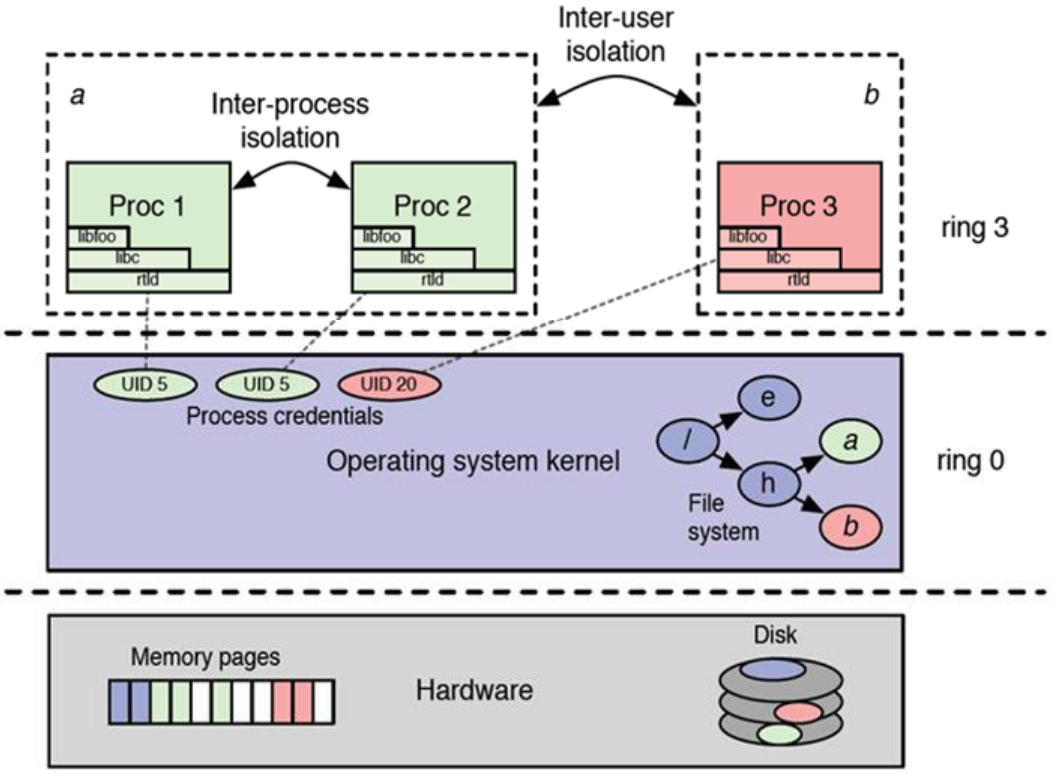


Linux System memory space

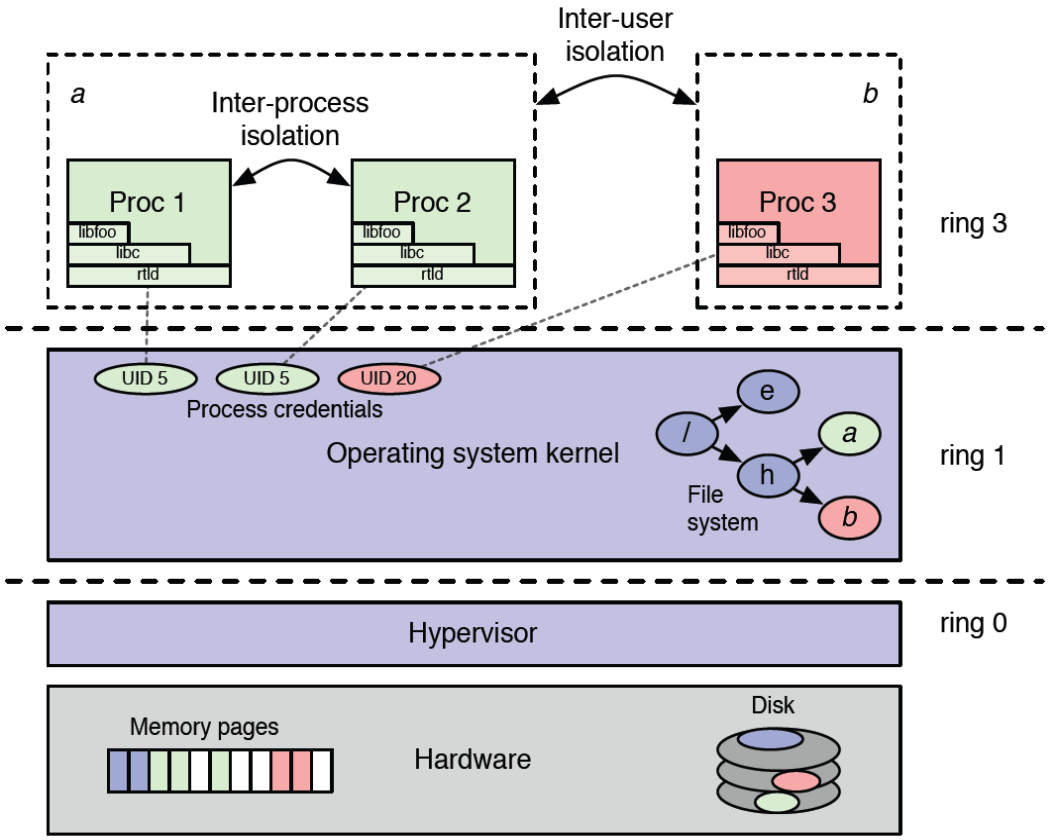
Privilege mode

- **Rings**
- **Privileges in applications execution**





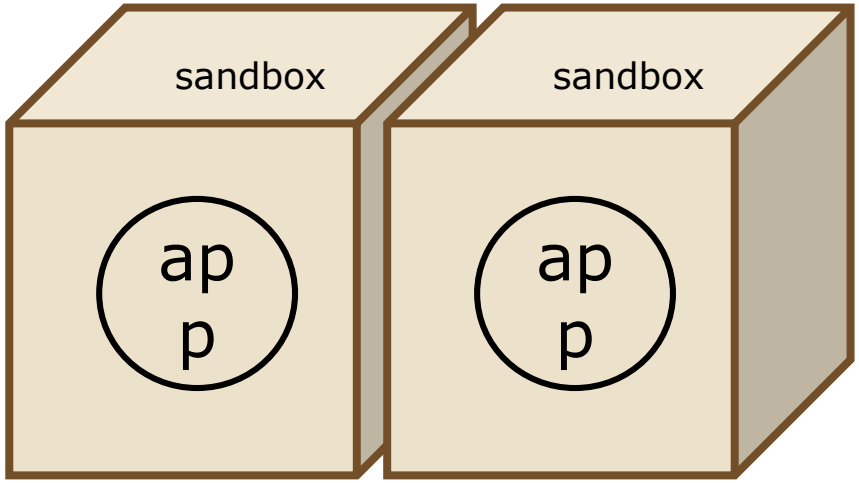
hardware rings & virtual machine



Sandbox

- a security mechanism for separating running programs. It is often used to execute untested code, or untrusted programs from unverified third-parties, suppliers, untrusted users and untrusted websites.

  - chroot
  - Virtual Machine
  - Google Native Client



例子：NaCl —— Google Native Client