

Advanced Operating Systems and Virtualization (A.Y. 2020/2021)

Department of Computer, Control and Management Engineering "Antonio Ruberti" - Sapienza University of Rome

Teachers: Gabriele **Proietti Mattia**, Roberto **Beraldi**

Course Website: <https://gpm.name/teaching/2021-aosv>

Syllabus

1. **The x86 Boot Process**
 1. Step1: BIOS/UEFI
 1. Pre-Boot and Real Mode
 2. BIOS
 2. Step 2: Stage 1 Bootloader
 1. MBR
 2. x86 Protected Mode
 3. x86 Memory Addressing
 4. x86 Privileges and Protection
 5. Paging
 3. Step 3: Stage 2 Bootloader
 1. GRUB/UEFI
 2. Multi-core Support
2. **Step 4: Kernel Boot**
 1. Initial Life of the Linux Kernel
 2. `startup_32()`
 3. `start_kernel()`
 1. Bootmem and Memblock Allocators
 2. Paging Introduction
 3. Paging Initialization
 4. TLB
 5. Final operations and recap
3. **Memory Management**
 1. Memory Representation
 2. The Buddy System
 3. High Memory
 4. Memory Finalization
 5. Steady-state memory allocation
 1. Fast Allocations & Quicklists
 2. SLAB Allocator
 3. CPU Caches
 4. Large Allocations
 6. User & Kernel Space
4. **System Calls**
 1. Introduction
 2. Handler / Dispatcher
 3. Invoking Process
 1. User Space Invoking process

2. Kernel Wrapper Routines
 3. X86_64 Invoking Process
 4. vDSO
 5. Conclusions
- 5. Interrupts**
 1. Introduction
 2. IRQs and Inter-Processor Interrupts
 3. The IDT and the Activation Scheme
 4. Exception Handling
 1. Fixups and Page Fault Handler
 5. Interrupts Handling
 1. I/O Interrupts
 2. Inter-Processor Interrupts (IPIs)
 6. Software Interrupts (SoftIRQs) and Tasklets
 7. Work Queues
- 6. Time Management**
 1. Introduction
 2. Timekeeping Architecture
 1. Low-resolution Timers
 2. Generic Time Subsystem
 3. Watchdogs
- 7. Concurrency in the Kernel**
 1. Introduction
 2. Synchronization
 1. Per-CPU Variables
 2. Atomic operations
 3. Memory Barriers
 4. Spinlocks
 5. Seqlocks
 6. RCU
 7. Semaphores
- 8. Virtual File System**
 1. Introduction
 2. The Common File Model
 1. Operations
 3. Pathname Lookup
 4. Files
 5. The /proc filesystem
 6. The /sys filesystem
 7. Device Management
 1. Char Devices
 2. Block Devices
 3. Devices and VFS
 4. Classes
 5. Udev
- 9. Userspace Initialization**
 1. init
 2. runlevels/targets
 1. Systemd
 3. End of the boot process
- 10. Process Management**
 1. Process Control Block
 1. Accessing the PCB
 2. The fork()/exec() model

1. Kernel Threads
3. Out Of Memory (OOM) Killer
4. Process Starting
 1. The ELF Format
 2. Dynamic Linking
 3. Initial Steps of Programs' Life

11. Scheduling

1. Introduction
2. Priorities and Weights
3. Scheduler Core
 1. Wait Queues
 2. Scheduler Entry Point
 3. Scheduler Algorithms
4. Context Switch

12. Virtualization

1. Introduction
2. Software-based Virtualization
 1. VirtualBox
3. Paravirtualization
4. Hardware-assisted Virtualization
 1. Virtualization of Memory
5. Linux Containers
 1. cgroups
 2. namespaces
 3. Container Runtimes and Docker

13. Security

1. Introduction
2. User Authentication
3. Internet Security
4. Secure Operating Systems

14. Epilogue

1. Introduction
2. Linux History
3. Kernels

Labs/Hands-on

1. Git: an essential guide
2. Building the Kernel
3. ASM in C
4. Kernel Modules
5. Kernel Messaging & Debugging
6. Final project presentation and organization
7. Kernel Data Structures
8. Misc devices, ioctl and /proc filesystem
9. Function Hooking: Kprobes and ftrace
10. Rootkit Analysis