IRIS LABS HARDWARE Assignment III

Platform: QEMU (Raspberry Pi Model 2B)
Objective: Familiarize yourself with low-level UART communication, privilege levels, and memory management using QEMU emulation.

Task 1: UART-Based Serial Output in EL1

Develop a bare-metal program that runs on the Raspberry Pi Model B using QEMU. Your program should:

- Operate entirely in **EL1 (privileged mode)**.
- Send the string **"Hello World"** to the serial monitor using the **UART0 peripheral** via memory-mapped I/O.
- Define and use a custom `printf()` function to output the message, without relying on any standard library UART APIs.

Note: Depending on the emulated model, the UART base address and relevant registers can be obtained from the BCM2835/BCM2836/BCM2837 datasheet.

Task 2: Restrict UART Access from EL0

Extend your setup to implement **exception level control** as follows:

- Switch from EL1 to **EL0 (user mode)** after system initialization.
- Ensure that **direct access to the UART peripheral is disallowed** from EL0.
- Attempts to call `printf()` from EL0 should result in a controlled failure or exception.
- Implement an appropriate **privileged mechanism (e.g., SVC/syscall)** to allow user-mode programs to request UART output indirectly.

Bonus Task: Virtual Memory and User Program Execution

For additional credit, extend the system to support:

- **Virtual memory** using the ARMv7/ARMv8 MMU.
- Creation of **page tables** that separate the kernel and user memory spaces.
- Execution of the "Hello World" output as a **user-mode program** residing in a separate memory region with appropriate access permissions.
- **Paging and translation table setup**, ensuring that MMIO regions like UART remain accessible only to the kernel.

Submission Guidelines

- Submit your code along with build and execution instructions.
- Include a brief README describing your approach, particularly for the exception handling and memory management components.
- Bonus points will be awarded for clean memory isolation and syscall handling mechanisms.

You'll be directly recruited into the team if you complete the bonus task and demonstrate a strong understanding!