Unix Fibers
AOSV Final Project

Andrea Mastropietro
1652886
Department of Computer, Control and Management Engineering
Sapienza University of Rome

Umberto Mazziotta
1647818
Department of Computer, Control and Management Engineering
Sapienza University of Rome

Specifications

The aim of the project is the implementation of Windows Fibers in Linux Kernel. Fibers are the Windows kernel-level implementation of User-Level Threads. The assignment consisted into implementing the facilities related to the conversion of a Thread into a Fiber, the creation of new Fibers and the possibility to switch from a Fiber to another. Each Fiber has a Fiber Local Storage (FLS) which can be accessed by that Fiber only. Each Fiber has its own information exposed in the proc FS under the folder related to the process the Fiber belongs to. Fibers are implemented in the project using a Kernel module. Such module registers and creates a char device, with which the user-space library communicates using IOCTLS.
The following section will cover the description of the implementation of the user-space library, the kernel module and the exposure to the prof FS. Finally, we will talk about the comparison between the user-space and the our kernel-space implementation

1 User-Space Library

The functions exposed to the user are `ConvertThreadToFiber`, `CreateFiber`, `SwitchToFiber` and four more functions employed to manage the FLS.
Besides `ConvertThreadToFiber` and `CreateFiber` all the functions are wrappers for IOCTLS calls to the char device.
`ConvertThreadToFiber` is endued with opening a descriptor to the device for the calling process. The function ensures that if a child of a process that has already called the function calls the `ConvertThreadToFiber` itself, it is given a different descriptor. The function then call the related IOCTL.
`CreateFiber` allocates the stack aligning it to the the dimension of a page. Since the kernel expects to find at the base of the stack the return address, we have to let stack pointer point 8 bytes below the top of the newly allocated stack.

2 Kernel-Space Code

The module uses a hashtable to keep track of the processes that are using Fibers. The hashtable size is chosen according to the default maximum number of possible process in the system. In such hashtable we store information regarding the PID of the process, two queues for Fiber (one for the active and one for the waiting ones) and the ID of the next Fiber to be allocated. The data structure has a lock that guarantees the safety of concurrent accesses to the entries of the table.

2.1 Fibers

Each Fiber is represented by a struct containing several fields, such as the fiber_id, the last thread the fiber run, the cpu and fpu states, the fls and all the fields that will be exposed in proc fs.
The `open` function checks if the current process is in the hashtable. If it is not present it is added to the hashtable and sets a pointer to the process in the private data field of the struct file. In this way any process can easily access the data structure representing itself without the need of scanning the hashtable.
The `release` function does nothing since all the cleanup work is done using a kprobe.

IOCTL According to the parameter passed to the `ioclt` function, we check if the buffer passed as argument is accessible. Then, the corresponding IOCTL is called.

- IOCTL_CONVERT: the function checks if we are already a Fiber; if true the convert fails, otherwise we allocate a new Fiber setting as entry point the current instruction pointer value.
- IOCTL_CREATE: it checks if the caller is a Fibers; if false it fails, otherwise we allocate a new Fibers and add it to the queue related to the waiting Fibers the the process hashtable.
- IOCTL_SWITCH: the function checks if the caller is a Fiber; if true we look for the Fiber we want to switch to in the waiting queue. We then scan the active queue. if the Fiber we want to switch to is active, the switch fails. If it is waiting and the calling Fiber is in the active queue, we copy the context of the cpu and fpu of *current* into the struct representing the calling Fiber and the contexts of the Fiber we want to switch to are moved into *current*. The two Fibers involved in the switching are swapped from one queue to the other.

2.2 FLS

2.3 Cleanup

2.4 proc