Assignment 1. RB Tree and Dynamic Probe in Linux Kernel (200 points)

Related Subjects

1. Linux kernel RB tree
2. Linux module and device driver
3. Kprobe
4. x86's TSC (Time stamp counter) to measure elapse time
5. Multi-threaded programs.

Project Assignment

Part 1: Accessing a kernel RB tree via device file interface

Linux kernel consists of several generic data structures. One of them is RB tree (red-black tree) which is a form of semi-balanced binary tree. To form a binary tree, each node in the tree contains up to two children. A node in a RB tree should consist of a value that is greater than that of all children in the "left" child branch, and less than that of all children in the "right" branch. Thus, it is possible to organize a red-black tree by performing a depth-first, left-to-right traversal. The implementation is provided in include/linux/rbtree.h and lib/rbtree.c.

In this assignment, you are requested to develop a Linux kernel module which initiates an empty RB tree in Linux kernel and allows the tree being accessed as a device file. We will name the tree as "rbt530". The objects of type *rb_object_t* can be added to or removed from the RB tree according to their "*key*" value

```
typedef struct rb_object {
        int key;
        int data ;
} rb_object_t;
```

The RB tree is implemented in kernel space as a device "rbt530_dev"and managed by a device driver "rbt530_drv". When the device driver is installed, the tree "rbt530" is created and a device "rbt530_dev" is added to Linux device file systems. The device driver should be implemented as a Linux kernel module and enable the following file operations:

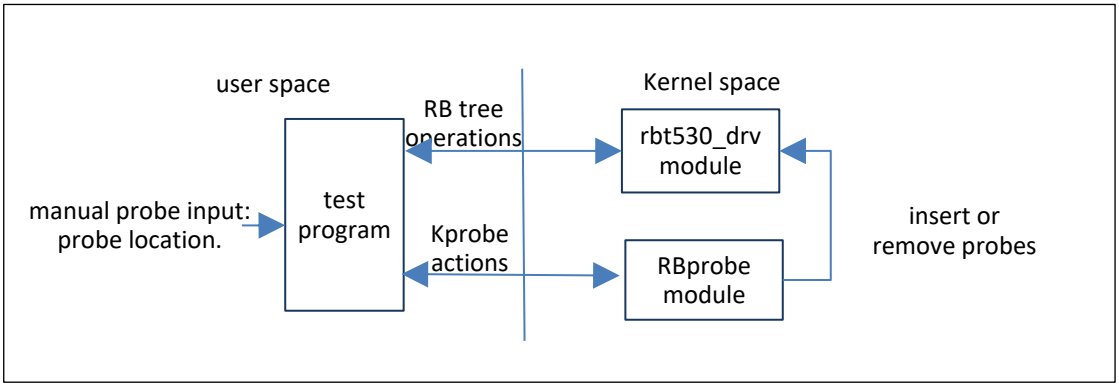
- *open:* to open a device (the device is "rbt530_dev").
- *write:* if the input object of *rb_object_t* has a non-zero data field*,* a node is created and added to the *rbt530*. If an object with the same key already exists in the tree, it should be replaced with the new one. If the data field is 0, any existing object with the input *key* is deleted from the table*.*
- *read:* to retrieve the first object (the object with the minimal "key") or last object (the object with the maximal "key") from the RB tree. If the RB tree is empty, -1 is returned and errno is set to EINVAL. After reading, the object is removed from the tree.
- *Ioctl:* The command "set_end" to set which object is to be read*.* If the argument is 0, read calls retrieve the first object in the tree. It if is 1, read calls get the last object. Otherwise, -1 is returned and errno is set to EINVAL.
- *release:* to close the descriptor of an opened device file.

To test your driver, a user program should be developed in which the main program creates 4 threads to populate (by calling write operation) the RB tree with a total of 40 objects and then invoke

read and write randomly. The threads are set with different real-time priorities and consecutive file operations are invoked after a random delay. After a total of 100 read and write operations are done, the threads should terminate and the main program dumps out all objects in the table. Note that the "*rbtree530*" and its associated objects should be deleted when the driver module is removed. So, the tree is empty at the first time your test program runs after the driver module is installed.

Part 2: Dynamic instrumentation in kernel modules

Linux has static and dynamic tracing facilities with which callback functions can be invoked when trace points (or probes) are hit. In this part of the assignment, you are required to develop a kernel module, named as "RBprobe", that uses kprobe API to add and remove dynamic probes in any kernel programs. With the module's device file interface, a user program can place a kprobe on a specific line of kernel code, access kernel information and variables. Integrated with part 1 of the assignment, you need to demonstrate the scenario depicted in the following diagram:



While exercising the RB tree *rbt530*, your test program reads in kprobe request information from console and then invokes *RBprobe* device file interface to register/unregister a kprobe at a given location of *rbt530_drv* module. When the kprobe is hit, the handler should retrieve few trace data items in a buffer such that they can be read out via RBprobe module interface. In the scenario, the user input request consists of the location (offset) of a source line of code on the execution path of read and write functions of *rbt530_drv*. The buffer is with a fixed size and holds one set of trace data, i.e. any old trace data will be overwritten when new trace data is generated. The trace data items to be collected by kprobe handler include: the address of the kprobe, the pid of the running process that hits the probe, time stamp (x86 TSC), and all *rb_object* objects traversed in the RB tree while performing the corresponding functions. Other than open and close file operations, the read and write operations of RBprobe device can be defined as:

- *write:* to register or unregister a kprobe. The location (offset) of the kprobe is passed in the buffer **buf* along with an integer flag. A kprobe is registered if the flag is 1, or unregistered if 0.
- *read:* to retrieve the trace data items collected in a probe hit and saved in the buffer. If the buffer is empty, -1 is returned and errno is set to EINVAL.

You can reuse the test program in part 1 for the scenario in part 2. For instance, besides the 4 threads that exercise the RB tree, an additional thread can be created to receive input from console, to set up kprobes in *rbt530_drv*, and to read out any collected data items. Using proper synchronizations,

you can control how the 4 threads invoke the operations to *rbt530* device file which can result in a hit at the kprobe point.

Due Date

TBD.

What to Turn in for Grading

- In your Github team repository, you should create a new branch, named "assignment1", where you can save all your work of the assignment, include source code, make and readme files. In your readme file, the instructions of running your programs should be included.
- Your committed code must be ready in your Github team repository before the due date and will be downloaded on the due date. For the submission committed after the due date, an email notification must be sent to the instructor and the TA. There will be 20 points penalty per day if the submission is late.
- Your team must work on the assignment without any help from other team, and is responsible to the submission committed in Github. No collaboration between teams is allowed, except the open discussion in the forum on Blackboard.
- Failure to follow these instructions may cause an annoyed and cranky TA or instructor to deduct points while grading your assignment.
- Here are few general rule for deductions:
    - No make file or compilation error -- 0 point for the part of the assignment.
    - Must have "–Wall" flag for compilation -- 5-point deduction for each warning.
    - 10-point deduction if no compilation or execution instruction in README file.
    - Source programs are not commented properly -- 10-20-point deduction.
- ASU Academic Integrity Policy (http://provost.asu.edu/academicintegrity), and FSE Honor Code (http://engineering.asu.edu/integrity) are strictly enforced and followed. A grade XE will be assigned to any cases of AIP violation.