Provoking crashes with Linux Kernel Dump Test Module (LKDTM)

The lkdtm module provides an interface to disrupt (and usually crash) the kernel at predefined code locations to evaluate the reliability of the kernel's exception handling and to test crash dumps obtained using different dumping solutions. The module uses KPROBEs to instrument the trigger location, but can also trigger the kernel directly without KPROBE support via debugfs.

You can select the location of the trigger ("crash point name") and the type of action ("crash point type") either through module arguments when inserting the module, or through the debugfs interface.

Usage:

```
insmod lkdtm.ko [recur_count={>0}] cpoint_name=<> cpoint_type=<>
                [cpoint_count={>0}]
```

recur_count
: Recursion level for the stack overflow test. By default this is dynamically calculated based on kernel configuration, with the goal of being just large enough to exhaust the kernel stack. The value can be seen at */sys/module/lkdtm/parameters/recur_count*.

cpoint_name
: Where in the kernel to trigger the action. It can be one of INT_HARDWARE_ENTRY, INT_HW_IRQ_EN, INT_TASKLET_ENTRY, FS_DEVRW, MEM_SWAPOUT, TIMERADD, SCSI_QUEUE_RQ, or DIRECT.

cpoint_type
: Indicates the action to be taken on hitting the crash point. These are numerous, and best queried directly from debugfs. Some of the common ones are PANIC, BUG, EXCEPTION, LOOP, and OVERFLOW. See the contents of */sys/kernel/debug/provoke-crash/DIRECT* for a complete list.

cpoint_count
: Indicates the number of times the crash point is to be hit before triggering the action. The default is 10 (except for DIRECT, which always fires immediately).

You can also induce failures by mounting debugfs and writing the type to <debugfs>/provoke-crash/<crashpoint>. E.g.:

```
mount -t debugfs debugfs /sys/kernel/debug
echo EXCEPTION > /sys/kernel/debug/provoke-crash/INT_HARDWARE_ENTRY
```

The special file *DIRECT* will induce the action directly without KPROBE instrumentation. This mode is the only one available when the module is built for a kernel without KPROBEs support:

```
# Instead of having a BUG kill your shell, have it kill "cat":
cat <(echo WRITE_RO) >/sys/kernel/debug/provoke-crash/DIRECT
```