

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Факультет інформатики та обчислювальної техніки

Кафедра обчислювальної техніки

Архітектура комп'ютерів 2. Процесори
Лабораторна робота №5
«Розроблення модулів Linux Kernel (3)»

Виконав:
студент групи ІО-14
Чаплицький Дарій
Перевірів:
Гайдай А. Р.

Київ - 2023 р.

Тема: Розроблення модулів Linux Kernel (частина 3)

Виконання лабораторної роботи:

Завдання 1:

- I. Додайте `BUG_ON()` замість друку повідомлення та повернення - `EINVAL` для неприпустимого значення параметра.
- II. Додайте примусове внесення помилки “начебто `kmalloc()` повернув 0” під час формування елемента списку для якогось повідомлення (останнього із серії, 5-го, ... — на ваш вибір).
- III. Модифікуйте `Makefile` аналогічно *appendix1*.
- IV. Отримайте обидва повідомлення, роздивіться їх та для одного з них виконайте пошук місця аварії аналогічно *appendix1*.
 - A. Зауважте, що при виконанні `BUG_ON()` модуль буде “зайнятий”, і ви не зможете виконати `gmmmod`.

Посилання на github:

<https://github.com/DoveFoke/AK/tree/main/lab%205>

Результат:

```
# insmod hello5.ko print count=4
[ 389.930166] Hello, world!
[ 389.930285] Hello, world!
[ 389.930343] Hello, world!
[ 389.930465] Unhandled fault: page domain fault (0x81b) at 0x00000008
[ 389.930709] pgd = (ptrval)
[ 389.930815] [00000008] *pgd=48b25835, *pte=00000000, *ppte=00000000
[ 389.931561] Internal error: : 81b [#1] SMP ARM
[ 389.931828] Modules linked in: hello5(0+) [last unloaded: hello2]
[ 389.932281] CPU: 0 PID: 91 Comm: insmod Tainted: G      0      4.19.295 #1
[ 389.932424] Hardware name: Generic DT based system
[ 389.933032] PC is at hello_init+0x7c/0x1000 [hello5]
[ 389.933163] LR is at 0x1/
[ 389.933229] pc : [c0000000] lr : [c0000000] psr: 800f0013
[ 389.933343] sp : c8b1bdc0 ip : 40000000 fp : bf041040
[ 389.933459] r10: 00000000 r9 : c1604c48 r8 : bf041004
[ 389.933564] r7 : 006000c0 r6 : c135c34c r5 : 00000000 r4 : bf041000
[ 389.933681] r3 : c8b1ce40 r2 : 70000000 r1 : 0000005a r0 : c799a780
[ 389.933843] Flags: Nzcv IRQs on FIQs on Mode SVC_32 ISA ARM Segment none
[ 389.933986] Control: 10c5387d Table: 48adc06a DAC: 00000051
[ 389.934114] Process insmod (pid: 91, stack limit = 0x(ptrval))
[ 389.934254] Stack: (0xc8b1bdc0 to 0xc8b1c000)
[ 389.934495] bdc0: c1787d00 c1604c48 fffff000 bf044000 00000000 c0302dcc c8b1cd40 c04f1d00
[ 389.934778] bde0: 00000000 00000002 00000000 00000000 c8b1cd24 c04f26dc 00000000 e0981fff
[ 389.935079] be00: ffe00000 fffff000 c0f12218 c8b1c080 dbcef640 dbbd9000 dbcef640 00000001
[ 389.935280] be20: bf041040 beb8cca7 bf041040 00000002 c8b1c0c0 00000002 c8b1cd40 c03d21d4
[ 389.935493] be40: c8b1cd40 c0463330 c8b1bf30 c8b1bf30 00000002 c8b1cd00 00000002 c03d4588
[ 389.935760] be60: bf04104c 00007fff bf041040 c03d1410 c8b10c18 bf041088 c8b10e78 bf041234
[ 389.935953] be80: 00000001 bf041170 c135a3e0 c1220664 c12206d4 c1604c48 c1608f04 c8b1c040
[ 389.936146] bea0: fffff000 e0800000 c8b1c040 c8b1c0c0 00000000 00000000 00000000 00000000
[ 389.936328] bec0: 00000000 00000000 6e72656b 00006c65 00000000 00000000 00000000 00000000
[ 389.936553] bee0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
[ 389.936744] bf00: 00000000 beb8cca7 00000000 00001510 00000000 e0980510 0011c768 c1604c48
[ 389.936931] bf20: 0011b1f8 fffff000 00000051 c03d49ec e097f2d6 e097f3c0 e097f000 00001510
[ 389.937115] bf40: e097ff70 e097fe14 e097fb50 00003000 00003040 00000000 00000000 00000000
[ 389.937300] bf60: 0000162c 00000021 00000022 00000018 00000000 00000010 00000000 beb8cca7
[ 389.937538] bf80: 000f411f 0011b1f8 b6fad950 00001510 00000080 c0301264 c8b1a000 00000080
[ 389.937730] bfa0: 000f411f c0301000 0011b1f8 b6fad950 0011b258 00001510 0011b1f8 00000000
[ 389.937984] bfc0: 0011b1f8 b6fad950 00001510 00000080 00000001 bed05e90 001086c5 000f411f
[ 389.939999] bfe0: bed05b48 bed05b38 0003b270 b6e671b0 600f0010 0011b258 00000000 00000000
```

```
[ 389.933229] pc : [c0000000] lr : [c0000000] psr: 800f0013
[ 389.933343] sp : c8b1bdc0 ip : 40000000 fp : bf041040
[ 389.933459] r10: 00000000 r9 : c1604c48 r8 : bf041004
[ 389.933564] r7 : 006000c0 r6 : c135c34c r5 : 00000000 r4 : bf041000
[ 389.933681] r3 : c8b1ce40 r2 : 70000000 r1 : 0000005a r0 : c799a780
[ 389.933843] Flags: Nzcv IRQs on FIQs on Mode SVC_32 ISA ARM Segment none
[ 389.933986] Control: 10c5387d Table: 48adc06a DAC: 00000051
[ 389.934114] Process insmod (pid: 91, stack limit = 0x(ptrval))
[ 389.934254] Stack: (0xc8b1bdc0 to 0xc8b1c000)
[ 389.934495] bdc0: c1787d00 c1604c48 fffff000 bf044000 00000000 c0302dcc c8b1cd40 c04f1d00
[ 389.934778] bde0: 00000000 00000002 00000000 00000000 c8b1cd24 c04f26dc 00000000 e0981fff
[ 389.935079] be00: ffe00000 fffff000 c0f12218 c8b1c080 dbcef640 dbbd9000 dbcef640 00000001
[ 389.935280] be20: bf041040 beb8cca7 bf041040 00000002 c8b1c0c0 00000002 c8b1cd40 c03d21d4
[ 389.935493] be40: c8b1cd40 c0463330 c8b1bf30 c8b1bf30 00000002 c8b1cd00 00000002 c03d4588
[ 389.935760] be60: bf04104c 00007fff bf041040 c03d1410 c8b10c18 bf041088 c8b10e78 bf041234
[ 389.935953] be80: 00000001 bf041170 c135a3e0 c1220664 c12206d4 c1604c48 c1608f04 c8b1c040
[ 389.936146] bea0: fffff000 e0800000 c8b1c040 c8b1c0c0 00000000 00000000 00000000 00000000
[ 389.936328] bec0: 00000000 00000000 6e72656b 00006c65 00000000 00000000 00000000 00000000
[ 389.936553] bee0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
[ 389.936744] bf00: 00000000 beb8cca7 00000000 00001510 00000000 e0980510 0011c768 c1604c48
[ 389.936931] bf20: 0011b1f8 fffff000 00000051 c03d49ec e097f2d6 e097f3c0 e097f000 00001510
[ 389.937115] bf40: e097ff70 e097fe14 e097fb50 00003000 00003040 00000000 00000000 00000000
[ 389.937300] bf60: 0000162c 00000021 00000022 00000018 00000000 00000010 00000000 beb8cca7
[ 389.937538] bf80: 000f411f 0011b1f8 b6fad950 00001510 00000080 c0301264 c8b1a000 00000080
[ 389.937730] bfa0: 000f411f c0301000 0011b1f8 b6fad950 0011b258 00001510 0011b1f8 00000000
[ 389.937984] bfc0: 0011b1f8 b6fad950 00001510 00000080 00000001 bed05e90 001086c5 000f411f
[ 389.939999] bfe0: bed05b48 bed05b38 0003b270 b6e671b0 600f0010 0011b258 00000000 00000000
[ 389.940934] [c0000000] (hello_init [hello5]) from [c0302dcc] (do_one_initcall+0x54/0x214)
[ 389.941387] [c0302dcc] (do_one_initcall) from [c03d21d4] (do_init_module+0x48/0x1ec)
[ 389.941547] [c03d21d4] (do_init_module) from [c03d4588] (load_module+0x21a8/0x24b4)
[ 389.941712] [c03d4588] (load_module) from [c03d49ec] (sys_init_module+0x158/0x18c)
[ 389.941852] [c03d49ec] (sys_init_module) from [c0301000] (ret_fast_syscall+0x0/0x54)
[ 389.941996] Exception stack(0xc8b1bfa8 to 0xc8b1bfff)
[ 389.942133] bfa0: 0011b1f8 b6fad950 0011b258 00001510 0011b1f8 00000000
[ 389.942361] bfc0: 0011b1f8 b6fad950 00001510 00000080 00000001 bed05e90 001086c5 000f411f
[ 389.942534] bfe0: bed05b48 bed05b38 0003b270 b6e671b0
[ 389.942874] Code: eb50b6fe e1a05000 eb4dd3d3 e5943004 (e1c500f8)
[ 389.943313] ---[ end trace 22458c3f62a0034a ]---
Segmentation fault
/ #
```

```
7c: e1c500f8 strd r0, [r5, #8]
list_add(&entry->list, &hello_list);
```

Висновок:

Внесені зміни до модуля, який був розроблений під час третьої лабораторної роботи для ядра Linux. Модуль було зібрано та протестовано в середовищі програмного емулятора Qemu для архітектури процесорів ARM. Під час компіляції ядра за допомогою команди `make` не виникло помилок. Під час використання команд `insmod/rmmod` було відзначено, що драйвер працює вірно відповідно до поставленого завдання. Зокрема, виявлено, що виклик `BUG_ON()` породжує помилку виконання, що в результаті викликає аварійне завершення роботи ядра та унеможлиблює виконання команди `rmmod`.