# Different branch（11）

6804-traps.c

9416-debug-monitors.c

9460-traps.c

18968-disassemble.c

19524-process\_64.c

21327-mpx.c

22972-xilinx\_hwicap.c

37814-spidev.c

48713-sock.c

51071-dmasound\_atari.c

51099-sb\_audio.c

# Different offset(arg)（186）

s-4775-signal.c

s-6787-signal.c

s-6799-sys\_oabi-compat.c

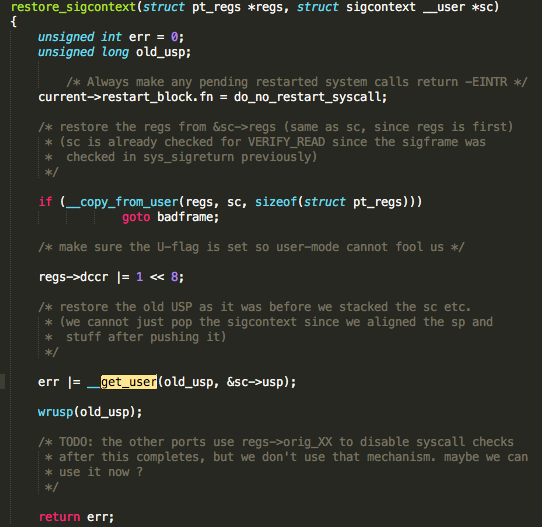
s-8932-vfpmodule.c

s-9446-signal.c

s-9447-signal32.C

s-9960-signal.c

s-10374-signal.c



s-10376-traps.c

s-10419-signal.c

s-11139-signal.c

s-11252-process.c

s-11257-signal.

s-11362-signal.

s-11707-signal.c

s-11715-unaligned.c

s-11750-init.c

s-12447-signal.c

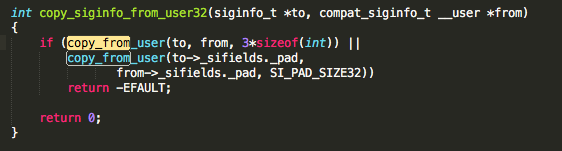
s-12903-backtrace.c

s-14293-termios.h

s-14468-ptrace.c

s-14487-signal.c

s-14488-signal32.c



s-14526-mips.c

s-14576-sysctl.c

s-14662-cp1emu.

s-14680-dsemul.c

s-15283-signal.c

s-15464-misaligned.c

s-15471-signal.c

s-15560-signal.c

s-15737-signal32.c

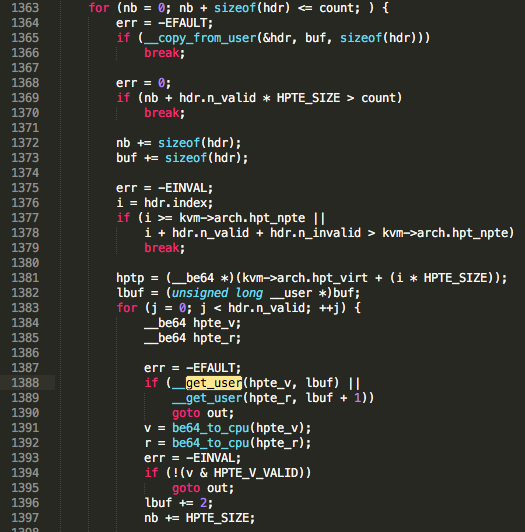
s-16980-align.c

s-17073-process.c

s-17078-ptrace.c

s-17105-syscalls.c

s-17150-book3s\_64\_mmu\_hv

head used for check

s-17850-hypfs\_sprp.c

18058-compat\_signal.c

18064-dis.c

18099-signal.c

18304-signal.c

19008-signal\_32.c

19009-signal\_64.c

19020-traps\_32.c

19532-ptrace\_32.c

19533-ptrace\_64.c

19540-signal32.c

19541-signal\_32.c

19542-signal\_64.c

19544-sigutil\_32.c

19545-sigutil\_64.c

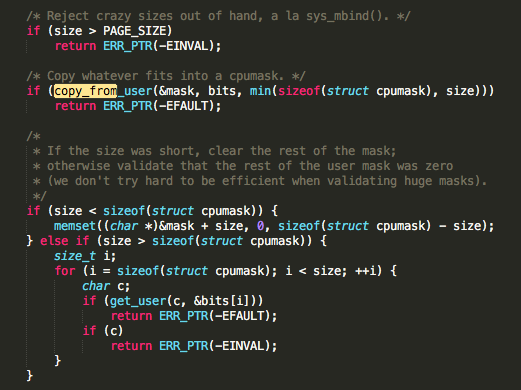
19581-unaligned\_64.c

19585-visemul.c

19669-math\_64.c

19913-compat\_signal.c

19917-hardwall.c



19958-unaligned.c

20319-signal.c

20541-ia32\_aout.c

20542-ia32\_signal.c

20836-uaccess\_64.h

21013-if.c

21016-perf\_event.c

21138-signal.c

21139-signal\_compat.c

21164-vm86\_32.c

21282-reg\_ld\_str.c

21579-signal.c

21776-ptrace.c

21778-signal.c

21870-compat\_ioctl.c

22509-zatm.c

22668-mtip32xx.c

22697-pg.c

22715-skd\_main.c

22835-ds1620.c

22836-dsp56k.c

22837-dtlk.c

22838-efirtc.c

22879-ipmi\_devintf.c

22896-3780i.c

22911-nwflash.c

22919-ppdev.c

22921-random.c

23748-adf\_ctl\_drv.c

24081-core-cdev.c

24300-amdgpu\_cs.c

24726-drm\_atomic.c

24733-drm\_crtc.c

24754-drm\_ioc32.c

24791-etnaviv\_gem\_submit.c

24824-exynos\_drm\_g2d.c

25058-mga\_ioc32.c

26140-r128\_state.c

26393-savage\_state.c

26455-drm.c

26522-vc4\_gem

26563-virtgpu\_ioctl.c

26891-dell-smm-hwmon.c

27247-ide-floppy\_ioctl.c

27268-ide-taskfile.c

27635-uverbs\_cmd.c

27636-uverbs\_main.c

27779-qib\_file\_ops.c

27878-evdev.c

28820-hypercalls.c

29094-dvb\_ca\_en50221.c

29543-media-device.c

29939-av7110\_hw.c

29969-zoran\_driver.c

31050-v4l2-ctrls.c

31420-card\_dev.c

31422-card\_utils.c

33502-bpqether.c

35326-bus.c

36652-keyboard.c

36748-zcrypt\_api.c

36759-zcrypt\_msgtype6.c

37187-gdth.c

37327-megaraid\_sas\_base.c

37348-mpt3sas\_ctl.c

37383-osst.c

37414-pmcraid.c

37562-st.c

37850-compat\_ion.c

37901-comedi\_compat32.c

40004-consolemap.c

40008-keyboard.c

40009-selection.c

40011-vt.c

40012-vt\_ioctl.c

40960-fbcmap.c

40962-fbmem.c

41240-sbuslib.c

41281-tmiofb.c

41935-binfmt\_aout.c ++

42149-compat.c

42151-compat\_ioctl.c

42249-exec.c

42820-super.c

43241-compat.c

43297-select.c

43300-splice.c

43760-termios-base.h

43761-termios.h

45294-pagemap.h

47789-compat.c

47790-compat\_mq.c

47824-syscall.c

47830-compat.c

47973-user.c

47981-ptrace.c

48025-signal.c

48082-trace.c //++

48243-kfifo.c

48461-mempolicy.c

48464-migrate.c

48594-ioctl.c

48608-resources.c

48691-sock.c

48697-sock.c

49032-arp\_tables.c

49035-ip\_tables.c

49166-ip6\_tables.c

49238-af\_irda.c

49739-af\_packet.c

49934-socket.c

49975-sysctl.c

50713-control\_compat.c

50718-hwdep\_compat.c

50738-pcm.c

50739-pcm\_compat.c

50746-pcm\_native.c

50749-rawmidi.c

50750-rawmidi\_compat.c

50765-seq\_oss\_rw.c

51073-dmasound\_paula.c ++

51078-midi\_synth.c

51108-sequencer.c

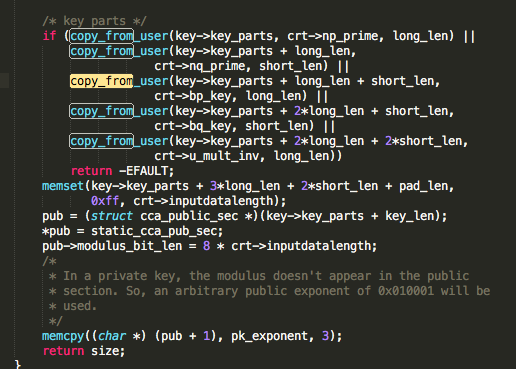
51313-emufx.c

52099-skl-topology.c

53888-vringh\_test.c

53914-kvm\_main.c

36750-zcrypt\_cca\_key.h



36757-zcrypt\_msgtype50.c //same

# incomplete or wrong identification（50）

s-4783-unwind.c

s-9493-sys\_regs.c

s-9693-ptrace.c

s-11694-perfmon.

s-14720-gup.c

s-15671-uaccess.h

s-15759-memcpy.c

s-17986-uaccess.h

18160-gup.c

19021-traps\_64.c

19093-gup.c

19676-gup.c

19842-uaccess.h

20324-traps.c

20762-pmem.h

20834-uaccess.h

20835-uaccess\_32.h

21302-gup.c

21555-ptrace\_32.c

21556-ptrace\_64.c

21607-enlighten.c

22704-rbd.c

26126-qxl\_ioctl.c

26257-radeon\_kms.c

27631-umem\_odp.c

28479-divasmain.c

28819-core.c

29785-ivtv-yuv.c

30005-dm644x\_ccdc.c

31065-videobuf-dma-sg.c

35985-goldfish\_pipe.c

37017-bfad\_bsg.c

37128-esas2r\_ioctl.c

38412-conctl.c

38523-dir.c

40153-f\_hid.c

41936-binfmt\_elf.c

42717-namespace.c

43014-file.c

47863-uprobes.c

47869-futex.c

48189-dma-debug.c

48435-gup.c //get user pages

48438-hugetlb.c

48459-memory.c //pages

48508-userfaultfd.c

48509-util.c

49767-info.c

49781-page.c

50130-xfrm\_user.c

# Size control (7--4)

28856-smu.c //seperate --dr

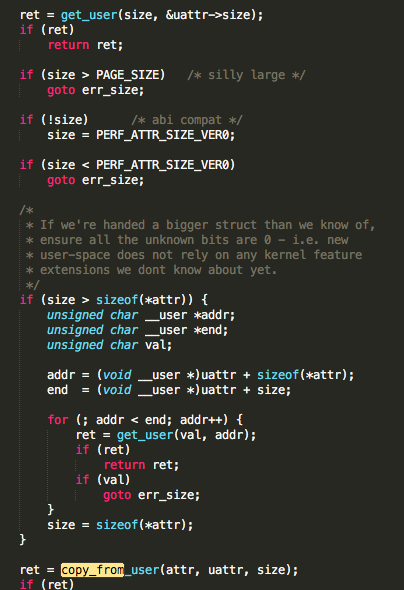


36825-openprom.c //seperate --dr

38524-file.c --dr

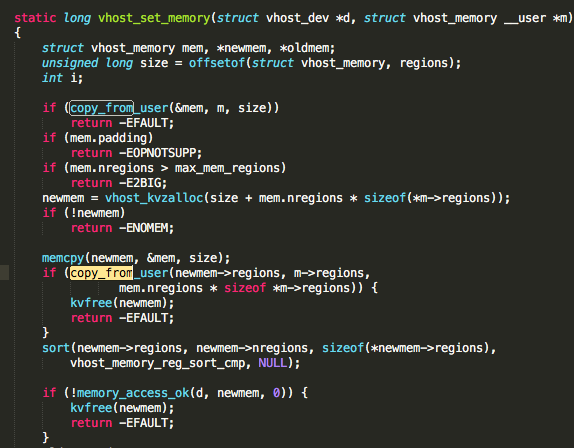
42378-fhandle.c

47859-core.c



48003-core.c //same

41608-gntdev.c --dr



# Type selection (2-1)

18138-interrupt.c

28503-mntfunc.c --dr

# Deep copy（23-15）

s-11799-sn\_hwperf.c

21067-signal.c

21874-ioctl.c

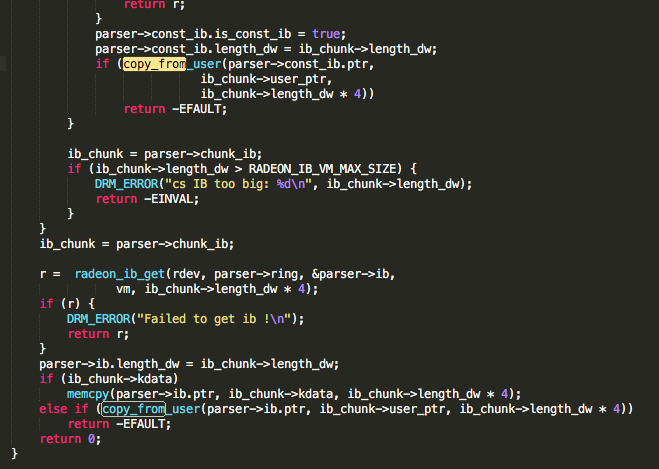
22611-DAC960.c --dr

22626-cciss.c --dr

22811-compat\_ioctl.c --dr

22814-frontend.c --dr

26237-radeon\_cs.c --dr

 //embedded

26253-radeon\_ioc32.c --dr

27193-i2c-dev.c --dr

27775-qib\_diag.c --dr

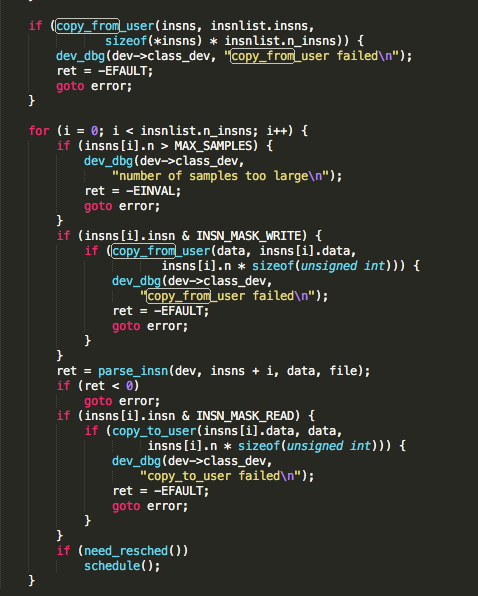


28396-act2000\_isa.c --dr

36823-jsflash.c --dr

37200-hpsa.c x2 --dr

37903-comedi\_fops.c //embeded --dr



38616-echo\_client.c --dr

40082-devio.c x2 --dr

41608-gntdev.c --dr

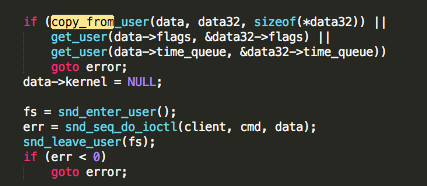
48032-sys.c

48581-ddp.c

51128-waveartist.c //only one element, direct access

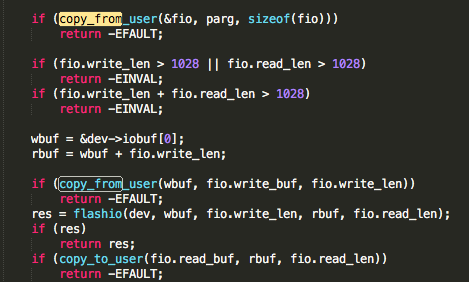
51492-hdsp.c //same

50775-seq\_compat.c



# deep copy & size control（11-9）

29736-ddbridge-core.c //with size control --dr



30086-ispccdc.c //with size control --dr

31617-block.c //with size control --dr

33645-ppp\_generic.c //with size control --dr

34095-ioctl.c //with size control --dr

34117-atmel.c //with size control --dr

35350-scsi.c //with size control --dr

40456-rio500.c x2 //with size control --dr

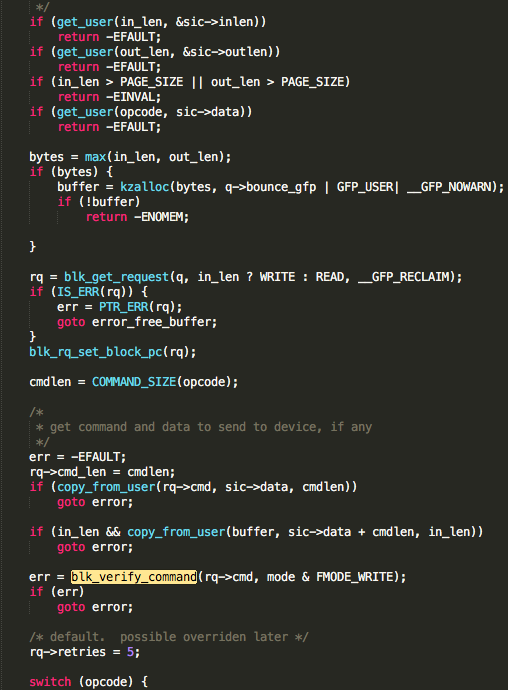
41375-fsl\_hypervisor.c //with size control --dr

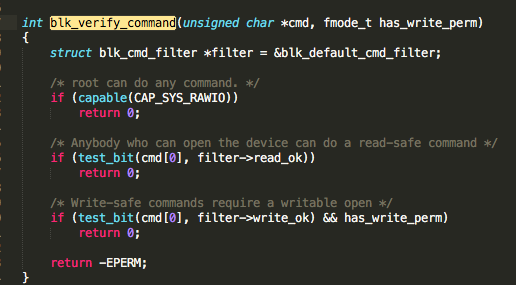
42899-ioctl.c //with size control

48776-ebtables.c //with size control

# type selection & size control（1-0）

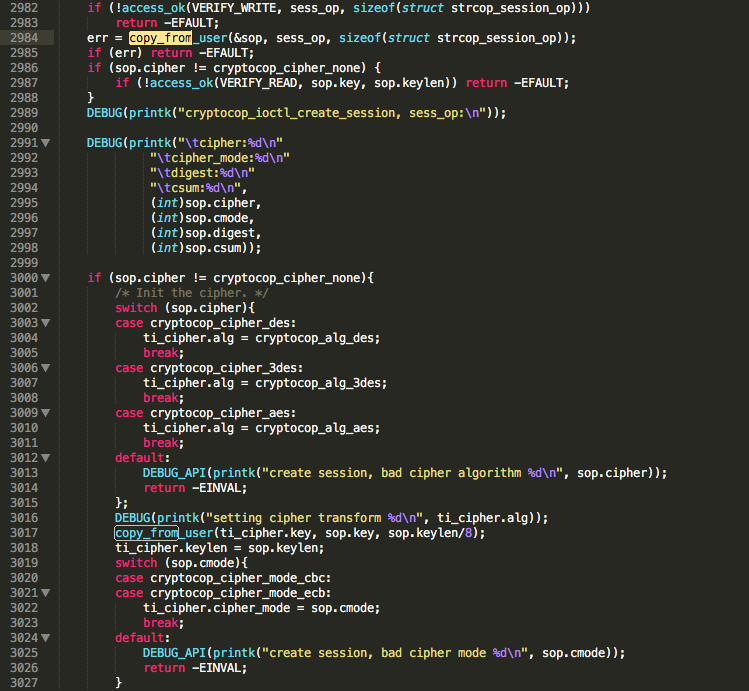
21914-scsi\_ioctl.c



 //with type selection

# Type selection & deep copy（5 -2）

s-10395-cryptocop.c



37324-megaraid\_mm.c --dr

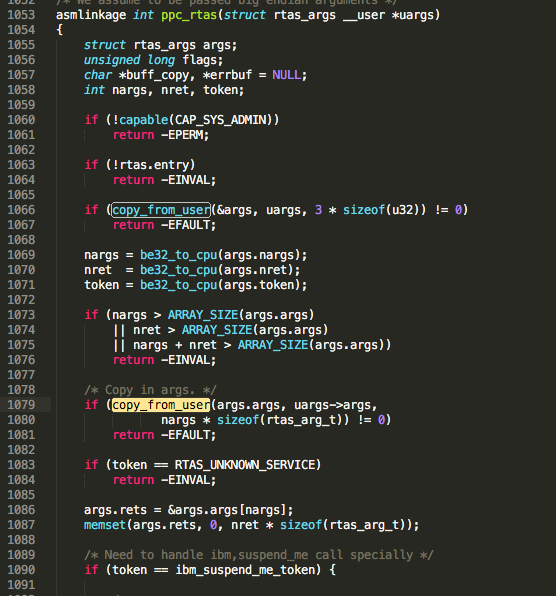
38850-file\_ops.c --dr

48738-br\_ioctl.c

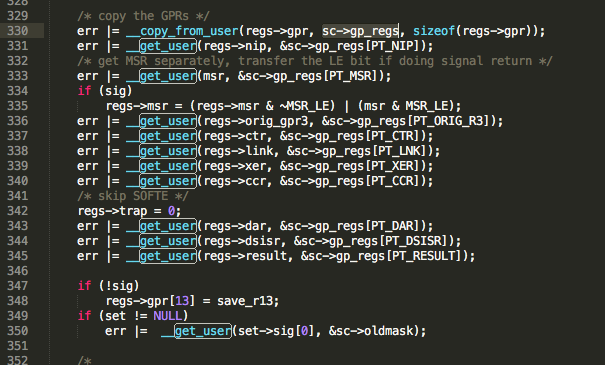
51043-wavefront\_synth.c

# whole>element（different offset）(7)

s-17084-rtas.c



s-17094-signal\_64.c



22830-applicom.c

26598-vmwgfx\_execbuf.c //differ elements

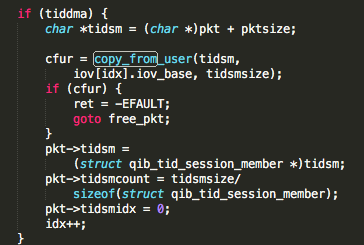
31037-uvc\_v4l2.c

31134-mptctl.c //differ elements

40796-vhost.c //differ elements

# doubles(10 -4)

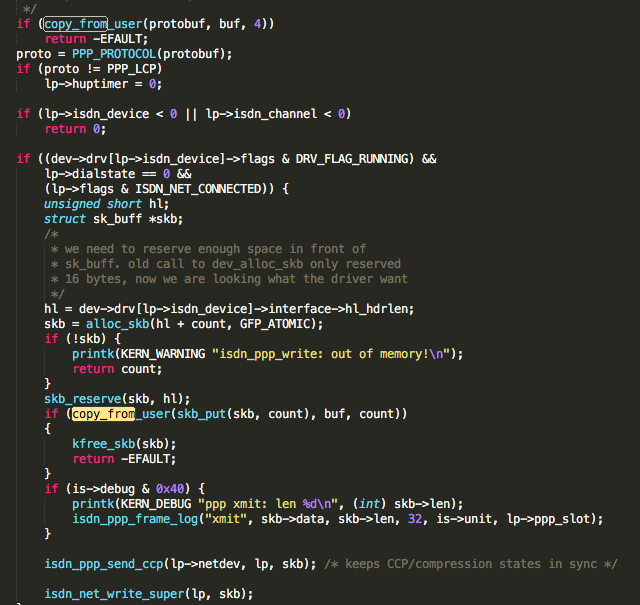
27807-qib\_user\_sdma.c --dr



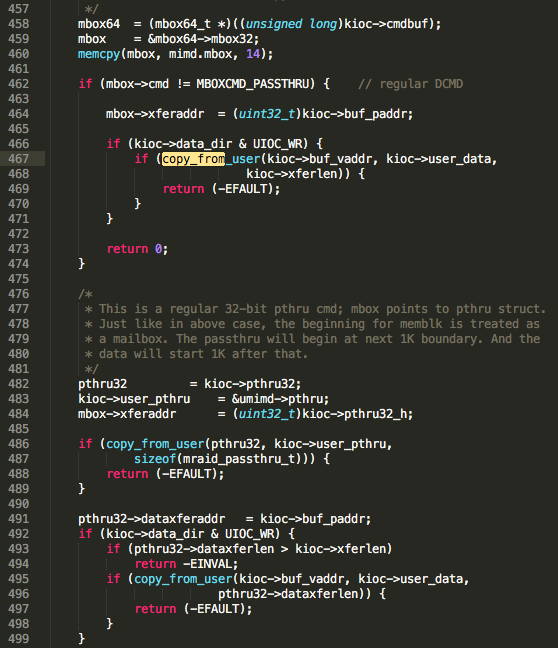
28478-divasi.c --dr



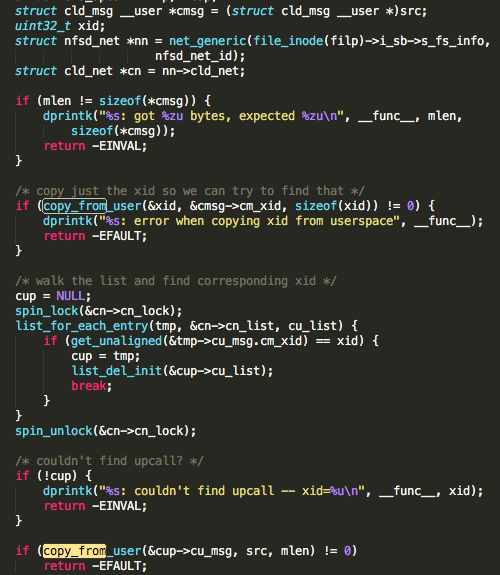
28673-isdn\_ppp.c --dr



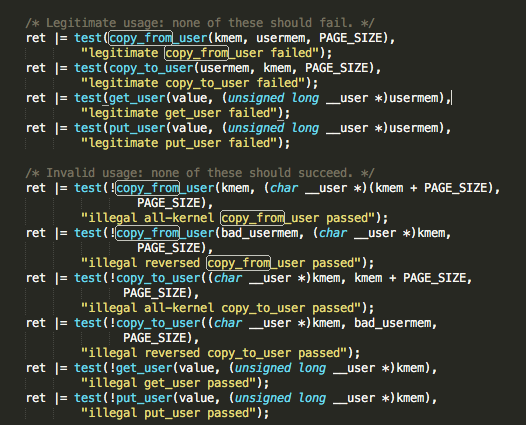
37324-megaraid\_mm.c --dr



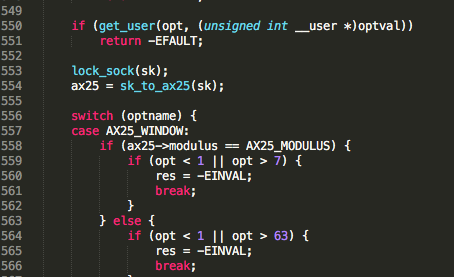
42853-nfs4recover.c

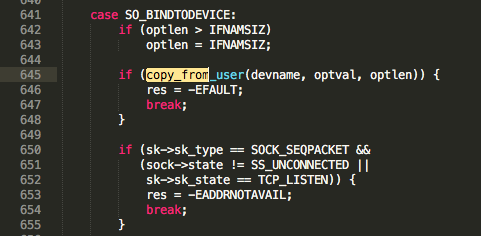
 //alias

48376-test\_user\_copy.c



48616-af\_ax25.c



//use in different cases

get some value outside switch, and the value only be used in the cases without another fetches.

48871-sock.c // same

49159-ipv6\_sockglue.c //same

49665-af\_netlink.c //same

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Output after stage 1: 421, driver related: 181, 43.0% | | | | | | | |
|  | False report: 329 | | | Analysis candidate: 92， driver related:64, 69.6% | | | | |
|  | Diff offset | Diff  Branch | Wrong identi | Size control | Type select | Deep copy | Other | Real |
| Deleted | 186+7 | 11 | 50 | 7+11+1 | 2+1+5 | 23+11+5 | 10 | 1 |
| Ouput2 | 33 | 41 | 1 | 7+3 | 8 | 2+1 | 5 | 3 |
| Result | 226 | 52 | 51 | 29 | 16 | 42 | 15 | 4 |
| Percent | 68.7% |  |  | 31.5% | 17.4% | 45.7% |  |  |
|  |  |  |  | 13 | 3 | 26 | 4 | 0 |
|  |  |  |  | 10 | 8 | 2 | 3 | 3 |
|  |  |  |  | 35.9% | 17.2% | 43.8% |  |  |
|  |  |  |  |  |  |  |  |  |

# ~~~~~~~~（1）

47815-auditsc

