# Errata Slip

## Proceedings of the 28th USENIX Security Symposium

For the paper “Detecting Missing-Check Bugs via Semantic- and Context-Aware Criticalness and Constraints Inferences” by Kangjie Lu, Aditya Pakki, and Qiushi Wu, University of Minnesota (Friday session, “Software Security,” pp. 1769–1786 of the Proceedings) the authors have provided the following corrections. In the original version, the entries in the “Filename” column in tables 4 and 5 have an extra character “g” prepended. The corrected tables are below.

| Subsystem | Filename | Line# | Impact | Category | Status | LP |
|---|---|---|---|---|---|---|
| net | vf.c | 511 | reliability | P | C | 2 |
| x86 | hv_init.c | 107 | DoS | S | A | 1 |
| x86 | tlb_uv.c | 2013 | DoS | S | S | 8 |
| char | hpet.c | 978 | reliability | S | S | 4 |
| firmware | driver.c | 711 | DoS | S | C | 1 |
| gpio | pio-exar.c | 150 | reliability | U | A | 2 |
| gpu | kfd_crat.c | 404 | DoS | U | S | 1 |
| gpu | i915_gpu_error.c | 230 | reliability | S | S | 2 |
| gpu | radeon_display.c | 679 | reliability | S | C | 2 |
| gpu | vkms_crtc.c | 227 | reliability | U | A | <1 |
| hid | hid-logitech-hidpp.c | 1954 | reliability | S | A | 3 |
| iio | max9611.c | 531 | DoS | U | S | 2 |
| iio | mxs-lradc-adc.c | 466 | DoS | U | A | 2 |
| iio | hmc5843_i2c.c | 62 | reliability | S | A | 4 |
| iio | hmc5843_spi.c | 62 | reliability | S | A | 4 |
| infiniband | cm.c | 1921 | DoS | S | C | 6 |
| infiniband | i40iw_cm.c | 3257 | DoS | S | A | 2 |
| infiniband | i40iw_cm.c | 3260 | DoS | S | A | 2 |
| input | pm8xxx-vibrator.c | 198 | DoS | P | S | 2 |
| isdn | hfcpci.c | 2034 | reliability | S | A | 10 |
| isdn | hfcsusb.c | 265 | DoS | S | A | 10 |
| isdn | mISDNinfineon.c | 716 | DoS | S | A | 9 |
| leds | leds-pca9532.c | 531 | crash /DoS | S | A | 2 |
| media | stv090x.c | 1449 | reliability | S | S | 10 |
| media | stv090x.c | 1452 | reliability | S | S | 10 |
| media | stv090x.c | 1456 | reliability | S | S | 10 |
| media | stv090x.c | 2229 | reliability | S | S | 5 |
| media | stv090x.c | 2607 | reliability | S | S | 10 |
| media | stv090x.c | 2913 | reliability | S | S | 10 |
| media | stv090x.c | 2957 | reliability | S | S | 10 |
| media | stv090x.c | 2975 | reliability | S | S | 10 |
| media | vpss.c | 520 | DoS | S | A | 6 |
| media | rcar-core.c | 267 | DoS | S | S | 1 |
| media | renesas-ceu.c | 1684 | DoS | S | S | 1 |
| media | rga.c | 894 | memory leak | S | A | 1 |
| media | rga.c | 896 | memory leak | S | A | 1 |
| media | rga.c | 910 | reliability | S | A | 1 |
| media | rga.c | 875 | reliability | S | A | 2 |
| media | rga.c | 915 | use-after-free | S | A | 1 |
| media | video-mux.c | 400 | DoS | U | A | 1 |
| media | video-mux.c | 402 | DoS | S | A | 1 |
| media | usbvision-core.c | 2301 | reliability | S | S | 9 |
| memstick | ms_block.c | 2141 | DoS | U | C | 5 |
| mfd | sm501.c | 1145 | DoS | S | A | 1 |
| mmc | mmc_spi.c | 821 | concurrency | U | A | 9 |
| net | mcp251x.c | 963 | reliability | S | S | 3 |
| net | lan9303-core.c | 1081 | system crash | S | S | 1 |
| net | lan9303-core.c | 1074 | system crash | S | S | <1 |
| net | pcnet_cs.c | 1424 | DoS | S | A | 8 |
| net | pcnet_cs.c | 290 | DoS | S | A | 8 |
| net | lio_main.c | 1194 | DoS | S | A | 2 |
| net | lio_vf_main.c | 1961 | DoS | S | S | 2 |
| net | lio_vf_main.c | 612 | DoS | S | S | 2 |
| net | lio_core.c | 1213 | DoS | S | A | 1 |
| net | lio_core.c | 1685 | DoS | S | A | 3 |
| net | nicvf_main.c | 2264 | DoS | S | A | 1 |
| net | fmvj18x_cs.c | 549 | DoS | S | A | 8 |
| net | fm10k_main.c | 42 | reliability | A | A | 2 |
| net | gen_rx.c | 721 | DoS | U | S | <1 |
| net | ocelot_board.c | 256 | DoS | U | C | 1 |
| net | qla3xxx.c | 3888 | system crash | U | A | 12 |
| net | qlge_main.c | 4682 | system crash | S | A | 2 |
| net | sh_eth.c | 3133 | reliability | U | A | 5 |
| net | ravb_main.c | 1996 | reliability | U | A | 3 |
| net | rocker_main.c | 2799 | DoS | S | A | 1 |
| net | dwmac-dwc-qos-eth.c | 487 | DoS | S | A | 2 |
| net | dwmac-sun8i.c | 1150 | system crash | S | A | 2 |
| net | fjes_main.c | 1254 | concurrency | U | S | 3 |
| net | fjes_main.c | 1255 | concurrency | S | S | 3 |
| net | netvsc_drv.c | 1377 | DoS | S | A | <1 |
| net | adf7242.c | 1269 | DoS | S | A | <1 |
| net | core.c | 645 | reliability | S | A | 2 |
| net | core.c | 646 | reliability | S | A | 2 |
| net | core.c | 653 | reliability | S | A | 2 |
| net | core.c | 662 | reliability | S | A | 1 |
| net | core.c | 689 | reliability | S | A | 2 |
| net | core.c | 714 | reliability | S | A | 2 |
| net | cfg80211.c | 5368 | DoS | S | A | 6 |
| net | cfg80211.c | 5384 | DoS | S | A | 6 |
| net | 3945-mac.c | 3405 | reliability | U | S | 7 |
| net | 4965-mac.c | 6241 | reliability | U | S | 7 |
| net | cmdevt.c | 342 | DoS | U | A | 7 |
| net | ray_cs.c | 395 | system crash | U | S | 8 |
| net | ray_cs.c | 409 | system crash | S | S | 8 |
| net | ray_cs.c | 423 | system crash | S | S | 8 |
| net | base.c | 471 | system crash | S | S | 4 |
| net | fw_common.c | 648 | DoS | S | A | 8 |
| net | fw.c | 600 | DoS | U | A | 8 |
| net | fw_common.c | 623 | DoS | U | A | 8 |
| net | fw.c | 744 | DoS | U | A | 8 |
| net | fw.c | 448 | DoS | U | A | 8 |
| net | fw.c | 562 | DoS | S | A | 8 |
| net | fw.c | 1623 | DoS | U | A | 8 |
| net | fw.c | 1759 | DoS | U | A | 8 |
| staging | fw.c | 745 | DoS | U | A | 8 |
| net | cmdevt.c | 342 | DoS | U | A | 8 |
| net | qlcnic_ethtool.c | 1050 | DoS | U | A | 8 |
| net | rsi_91x_mac80211.c | 199 | DoS | S | A | 5 |
| net | rsi_91x_mac80211.c | 208 | DoS | S | A | 5 |
| net | main.c | 347 | DoS | S | A | 6 |
| nfc | se.c | 345 | DoS | S | S | 4 |
| nvdimm | btt_devs.c | 200 | DoS | S | C | 3 |
| nvdimm | btt_devs.c | 217 | system crash | S | C | 3 |
| nvdimm | namespace_devs.c | 2250 | DoS | S | A | 2 |
| pci | pci-tegra.c | 1552 | buffer overflow | S | S | 1 |
| pci | pcie-rcar.c | 931 | buffer overflow | S | A | 5 |
| pci | pcie-xilinx.c | 343 | buffer overflow | S | C | 4 |
| pci | pci-epf-test.c | 571 | DoS | U | A | 2 |
| pinctrl | pinctrl-baytrail.c | 1711 | DoS | U | A | 3 |
| pinctrl | pinctrl-axp209.c | 366 | DoS | S | A | <1 |
| power | charger-manager.c | 2006 | DoS | U | A | 7 |
| rapidio | rio_cm.c | 2147 | DoS | S | A | 2 |
| scsi | cxgb4i.c | 619 | DoS | S | S | 8 |
| scsi | ql4_os.c | 3206 | DoS | S | A | 7 |
| scsi | ufs-hisi.c | 546 | DoS | U | A | <1 |
| spi | spi-s3c64xx.c | 294 | DoS | U | S | 5 |
| spi | spi-topcliff-pch.c | 1304 | DoS | S | A | 8 |
| spi | spi-topcliff-pch.c | 1307 | DoS | S | A | 8 |
| staging | audio_manager.c | 47 | system crash | P | A | 3 |
| staging | rtw_xmit.c | 1514 | DoS | S | A | 4 |
| staging | rtl_phydm.c | 182 | system crash | S | A | 1 |
| thunderbolt | property.c | 177 | DoS | S | A | 1 |
| thunderbolt | property.c | 550 | DoS | S | A | 1 |
| tty | main.c | 115 | DoS | S | A | 8 |
| tty | main.c | 135 | DoS | U | A | 8 |
| tty | 8250_lpss.c | 175 | DoS | U | C | 2 |
| tty | atmel_serial.c | 1285 | DoS | U | A | 5 |
| tty | mxs-auart.c | 1688 | DoS | S | S | 8 |
| usb | u132-hcd.c | 3203 | DoS | U | C | 11 |
| usb | alauda.c | 438 | DoS | U | S | 13 |
| usb | alauda.c | 439 | DoS | U | S | 13 |
| video | hgafb.c | 287 | DoS | S | A | 14 |
| video | imsttfb.c | 1517 | DoS | S | A | 13 |
| video | omapdss-boot-init.c | 113 | DoS | U | A | 3 |
| affs | file.c | 940 | DoS | S | C | 14 |
| btrfs | extent-tree.c | 7042 | reliability | S | A | 2 |
| ipv6 | ip6t_srh.c | 212 | DoS | S | A | 1 |
| ipv6 | ip6t_srh.c | 225 | DoS | S | A | 1 |
| ipv6 | ip6t_srh.c | 235 | DoS | S | A | 1 |
| openvswitch | datapath.c | 449 | DoS | U | A | 7 |
| smc | smc_ism.c | 290 | system crash | S | S | <1 |
| strparser | strparser.c | 552 | DoS | S | A | 2 |

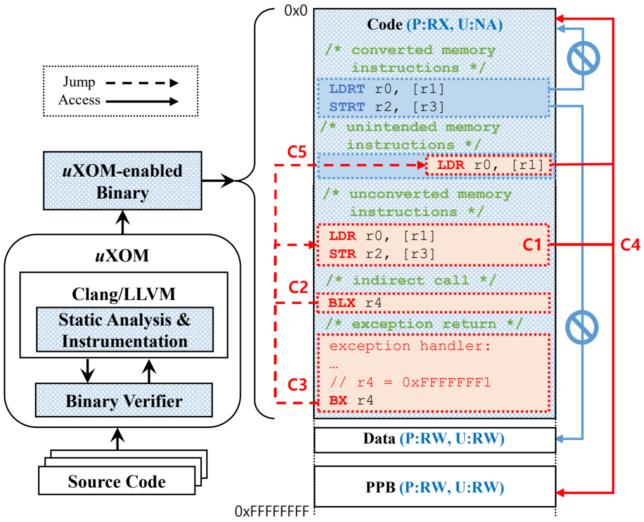
**Table 4:** List of new bugs (1-142) detected with CRIX. LP = Latent Period of bugs in years. Column `Category` specifies the category of peer-slice set used to identify the bugs. A, P, S, and U indicate categories `Source-Arg`, `Source-Param`, `Source-Ret`, and `Use-Param` respectively. The `S,C,A` in the `Status` field represent patch status - `Submitted`, `Confirmed`, `Applied` respectively.

| Subsystem | Filename | Line# | Impact | Category | Status | LP |
|---|---|---|---|---|---|---|
| security | inode.c | 339 | reliability | S | A | 5 |
| ceph | osdmap.c | 1900 | DoS | S | S | 7 |
| isa | sb8.c | 113 | reliability | U | A | 14 |
| pci | echoaudio.c | 1956 | DoS | U | A | 12 |
| soc | cs43130.c | 2324 | DoS | S | A | 1 |
| soc | rt5645.c | 3452 | system crash | U | A | <1 |
| soc | soc-pcm.c | 1236 | system crash | S | S | 4 |
| md | raid10.c | 3958 | system crash | S | A | 7 |
| md | raid5.c | 7399 | system crash | S | A | 7 |
| usb | usb_stream.c | 106 | DoS | S | A | 10 |
| usb | usb_stream.c | 107 | DoS | S | A | 10 |
| ata | sata_dwc_460ex.c | 1055 | DoS | U | S | 4 |
| block | nbd.c | 2117 | DoS | U | S | 2 |
| net | bcmmii.c | 217 | DoS | U | S | <1 |
| slimbus | com-ngd-ctrl.c | 1351 | reliability | U | A | <1 |
| ncsi | ncsi-netlink.c | 253 | reliability | U | A | 1 |
| ncsi | ncsi-netlink.c | 257 | DoS | U | A | 1 |
| openvswitch | conntrack.c | 2146 | DoS | U | S | 1 |
| openvswitch | datapath.c | 466 | DoS | U | A | 4 |
| openvswitch | datapath.c | 475 | DoS | U | A | 4 |
| openvswitch | datapath.c | 477 | reliability | U | A | 4 |
| tipc | group.c | 942 | DoS | U | A | <1 |
| tipc | group.c | 946 | system crash | U | A | <1 |
| tipc | socket.c | 3226 | DoS | U | A | 4 |
| tipc | socket.c | 3231 | reliability | U | A | 4 |
| extcon | extcon-axp288.c | 145 | reliability | S | A | 4 |
| thunderbolt | switch.c | 1325 | DoS | S | S | 2 |
| thunderbolt | xdomain.c | 540 | DoS | S | A | 1 |
| usb | usb251xb.c | 600 | DoS | U | A | 2 |
| tty | max310x.c | 1421 | DoS | U | A | 5 |
| tty | mvebu-uart.c | 791 | DoS | S | S | 1 |
| mtd | vf610_nfc.c | 856 | DoS | S | A | 3 |
| mfd | mc13xxx-i2c.c | 82 | DoS | U | S | 6 |
| pinctrl | berlin-bg4ct.c | 453 | DoS | U | S | 3 |
| pinctrl | pinctrl-as370.c | 334 | DoS | U | S | <1 |
| mfd | mc13xxx-spi.c | 160 | DoS | S | S | 6 |
| firmware | driver.c | 801 | DoS | S | A | 2 |
| net | tls.c | 227 | DoS | U | A | <1 |
| mmc | dw_mmc-exynos.c | 556 | DoS | U | S | 6 |
| mmc | dw_mmc-k3.c | 461 | DoS | S | S | 5 |
| mmc | dw_mmc-pltfm.c | 84 | DoS | S | S | 5 |
| pci | pci-host-generic.c | 85 | DoS | U | S | 3 |
| scsi | tc-dwc-g210-pltfrm.c | 63 | DoS | U | S | 3 |
| soc | sirf-audio-codec.c | 466 | system crash | S | A | 5 |
| slimbus | qcom-ngd-ctrl.c | 1333 | DoS | S | S | <1 |
| x86 | hpet.c | 79 | DoS | U | A | 11 |
| udf | super.c | 575 | system crash | S | S | 1 |
| nfc | llcp_sock.c | 726 | DoS | S | A | 7 |
| scsi | ufshcd.c | 1759 | DoS | S | S | <1 |
| thunderbolt | xdomain.c | 771 | DoS | S | A | 1 |
| scsi | ufshcd.c | 1786 | DoS | S | S | 1 |
| thunderbolt | icm.c | 475 | DoS | U | A | 1 |
| fmc | fmc-fakedev.c | 283 | DoS | S | S | 5 |
| usb | sierra_ms.c | 197 | system crash | S | A | 2 |
| staging | vchiq_2835_arm.c | 212 | DoS | S | C | 4 |
| thunderbolt | property.c | 581 | DoS | S | A | 3 |
| thunderbolt | property.c | 582 | buffer overflow | U | A | 1 |
| x86 | tlb_uv.c | 2144 | DoS | S | A | 2 |
| x86 | tlb_uv.c | 2147 | DoS | S | A | 4 |
| nfc | se.c | 329 | DoS | U | S | 1 |
| gpio | pio-aspeed.c | 1227 | DoS | S | A | 2 |
| soc | rt5663.c | 3472 | buffer overflow | S | C | 2 |
| soc | rt5663.c | 3513 | DoS | U | C | 1 |
| gpu | v3d_drv.c | 103 | system crash | S | A | 3 |
| net | mcr20a.c | 534 | system crash | S | A | 5 |
| net | mcr20a.c | 541 | reliability | S | S | 3 |
| net | mcr20a.c | 546 | reliability | S | S | 3 |
| media | tda18250.c | 705 | reliability | S | C | 2 |
| soc | cs35l34.c | 263 | reliability | S | S | 7 |
| dma | omap-dma.c | 1056 | system crash | A | S | 6 |
| firmware | edd.c | 279 | system crash | A | S | 4 |
| net | cfg80211.c | 2302 | system crash | A | S | 4 |
| rtc | rtc-ds1374.c | 449 | reliability | S | S | 2 |
| rtc | rtc-rx8010.c | 193 | system crash | S | S | 2 |
| mfd | tps65010.c | 431 | DoS | U | S | 2 |
| net | rx.c | 732 | DoS | U | C | <1 |
| net | rx.c | 733 | DoS | U | S | 3 |
| usb | realtek_cr.c | 815 | reliability | S | S | 5 |
| net | lag_conf.c | 307 | DoS | U | S | 6 |
| net | mesh.c | 799 | system crash | S | S | 2 |
| net | mesh.c | 800 | system crash | S | S | 2 |
| net | lag_conf.c | 307 | DoS | U | S | <1 |
| net | p2p.c | 1527 | concurrency | S | S | 6 |
| message | mptctl.c | 406 | concurrency | S | S | 10 |
| message | mptscsih.c | 1617 | concurrency | S | S | 10 |
| message | mptsas.c | 4803 | concurrency | S | S | 10 |
| misc | tifm_7xx1.c | 280 | concurrency | S | S | 4 |
| pci | pcie-designware-host.c | 309 | DoS | U | S | 1 |
| gpu | virtgpu_kms.c | 62 | DoS | U | S | 4 |
| gpu | virtgpu_vq.c | 48 | DoS | U | S | 6 |
| input | usbtouchscreen.c | 1076 | DoS | U | S | 8 |
| usb | iuu_phoenix.c | 369 | DoS | U | S | 12 |
| usb | iuu_phoenix.c | 177 | DoS | U | S | 12 |
| usb | iuu_phoenix.c | 729 | DoS | U | S | 12 |
| usb | iuu_phoenix.c | 389 | DoS | U | S | 12 |
| usb | iuu_phoenix.c | 253 | DoS | U | S | 12 |
| usb | kobil_sct.c | 248 | DoS | U | S | 4 |
| usb | kobil_sct.c | 339 | DoS | U | S | 4 |
| usb | kobil_sct.c | 354 | DoS | U | S | 4 |
| usb | kobil_sct.c | 284 | DoS | U | S | 3 |
| ncsi | ncsi-netlink.c | 250 | DoS | U | S | 3 |
| openvswitch | conntrack.c | 2131 | reliability | S | S | <1 |
| media | cx231xx-input.c | 91 | DoS | U | S | 4 |
| net | testmode.c | 242 | DoS | U | S | 8 |
| dma | fsl-edma-common.c | 540 | reliability | S | S | <1 |
| dma | coh901318_lli.c | 41 | reliability | S | S | 10 |
| mtd | generic.c | 69 | reliability | S | S | 3 |
| net | e1000_hw.c | 1046 | buffer overflow | S | S | 5 |
| mfd | vx855.c | 104 | reliability | S | S | 8 |
| mfd | ab3100-core.c | 926 | reliability | S | S | 8 |
| crypto | cryptd.c | 745 | reliability | S | S | 1 |
| hwmon | ad7418.c | 90 | buffer overflow | S | S | 3 |
| hwmon | lm92.c | 135 | buffer overflow | S | S | 3 |
| scsi | gdth.c | 5203 | buffer overflow | S | S | 4 |
| staging | mmal-vchiq.c | 1847 | DoS | U | S | 1 |
| fsi | fsi-core.c | 1250 | DoS | U | S | 2 |
| net | cxgb3_offload.c | 1268 | DoS | U | S | 7 |
| iio | mxs-lradc-adc.c | 470 | DoS | U | S | 1 |
| net | myri10ge.c | 2287 | reliability | S | S | 11 |
| gpu | si.c | 3614 | reliability | S | S | 6 |
| slimbus | qcom-ngd-ctrl.c | 1343 | DoS | U | S | <1 |
| net | e1000_hw.c | 141 | reliability | S | S | 10 |
| net | e1000_hw.c | 1043 | reliability | S | S | 10 |
| mtd | bcm63xxpart.c | 65 | buffer overflow | S | S | 3 |
| gpu | vc4_plane.c | 1011 | reliability | S | S | 1 |
| ext4 | super.c | 5866 | reliability | S | S | 8 |
| net | event.c | 105 | buffer overflow | S | S | 3 |
| net | pch_gbe_main.c | 1476 | DoS | U | S | 8 |
| net | isl_ioctl.c | 190 | reliability | S | S | 13 |
| gpu | ast_mode.c | 1201 | reliability | S | S | 7 |
| hid | wacom_sys.c | 2351 | reliability | S | S | 5 |
| media | ov9650.c | 609 | buffer overflow | S | S | <1 |
| soc | sti_uniperif.c | 292 | reliability | S | S | 2 |
| media | em28xx-cards.c | 3987 | reliability | S | S | 2 |
| usb | xhci-pci.c | 269 | reliability | S | S | 1 |
| net | nic_main.c | 1229 | crash | S | S | 3 |

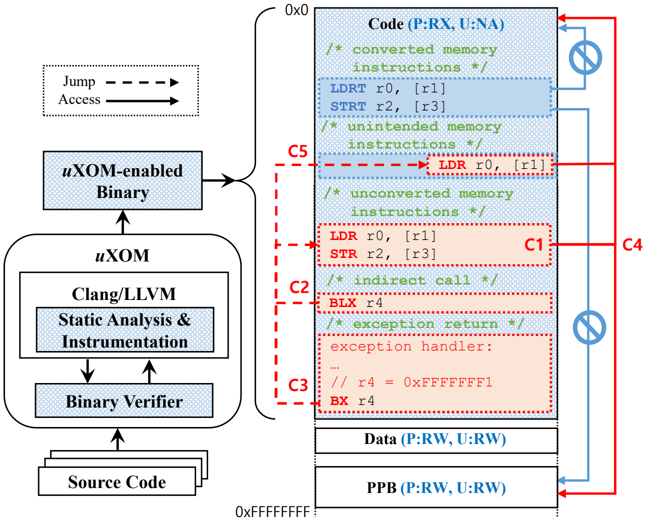
**Table 5:** Continued list of new bugs (143-278) detected with CRIX. LP = Latent Period of bugs in years. Column `Category` specifies the category of peer-slice set used to identify the bugs. A, P, S, and U indicate categories `Source-Arg, Source-Param, Source-Ret`, and `Use-Param` respectively. The `S,C,A` in the `Status` field represent patch status - `Submitted, Confirmed, Applied` respectively.

For the paper "uXOM: Efficient eXecute-Only Memory on ARM Cortex-M" by Donghyun Kwon, Jangseop Shin, Giyeol Kim, Byoungyoung Lee, Yeongpil Cho, Yunheung Paek (Wednesday session, "Hardware Security," pp. 231–247 of the Proceedings) the authors have provided the following correction. In the original version, the destination of the arrow in the figure is incorrect. The corrected figure is below.

**Original figure:**



**Corrected figure:**


Jump
Access
uXOM-enabled Binary
uXOM
Clang/LLVM
Static Analysis & Instrumentation
Binary Verifier
Source Code
0x0
0xFFFFFFFF
Code (P:RX, U:NA)
/* converted memory instructions */
LDRT r0, [r1]
STRT r2, [r3]
/* unintended memory instructions */
C5
LDR r0, [r1]
/* unconverted memory instructions */
LDR r0, [r1]
STR r2, [r3]
C1
C4
/* indirect call */
C2
BLX r4
/* exception return */
exception handler:
…
// r4 = 0xFFFFFFF1
C3
BX r4
Data (P:RW, U:RW)
PPB (P:RW, U:RW)