Karol Ziarek 318749
Jakub Kieruczenko 318669

SKPS - Laboratorium 3

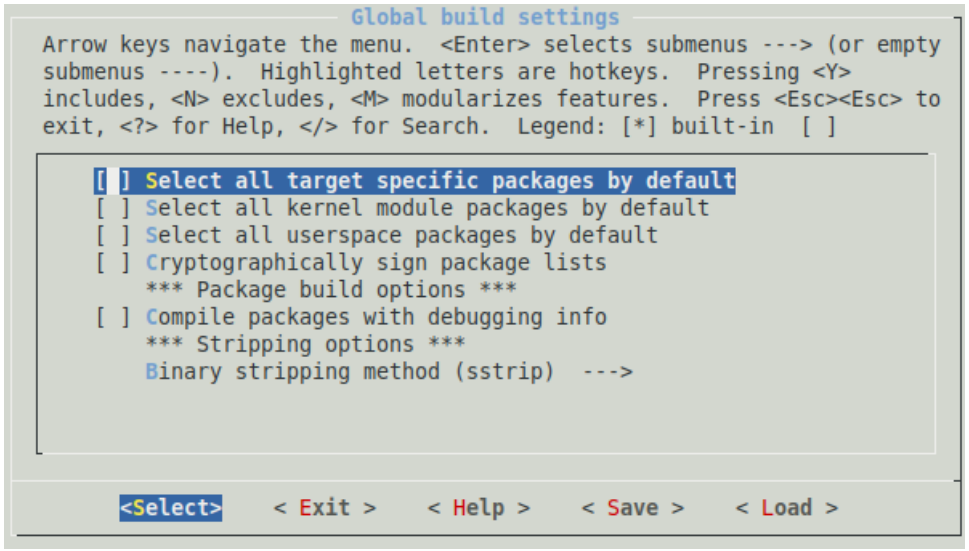
Zespół korzysta z karty SD - 105e

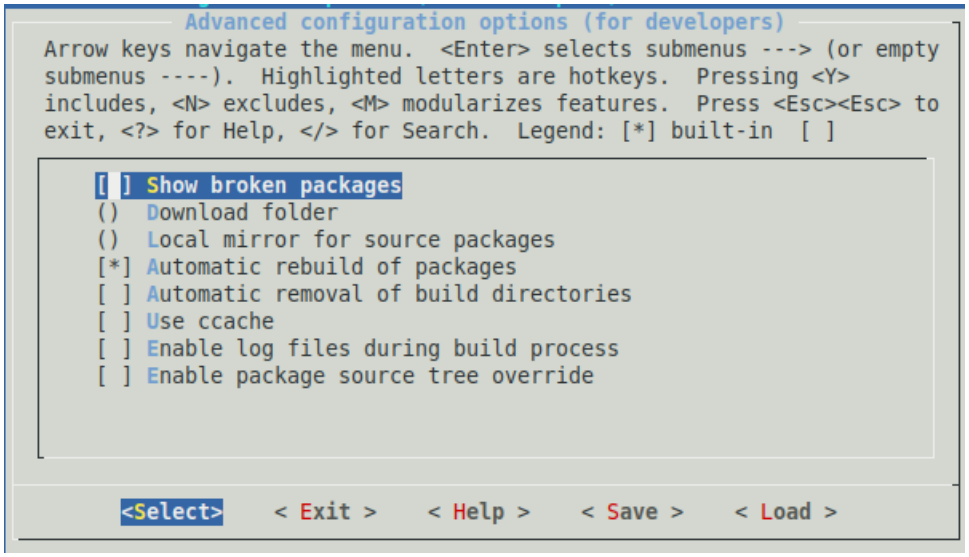
1. Pierwszy pakiet

1. Płytka została podłączona zgonie ze schematem z instrukcji
2. Prowadzący zweryfikował poprawność podłączenia
3. Wykorzystany jest OpenWRT zainstalowany na poprzednich zajęciach
4. Dopisano nameserver do konfiguracji resolvera

5. Pobrano OpenWRT SDK i pakiet demonstracyjny
6. Do pliku feeds.conf.default dodano:

7. Po wywołaniu make menuconfig odznaczono opcje w sposób widoczny poniżej by przyspieszyć pracę w laboratorium

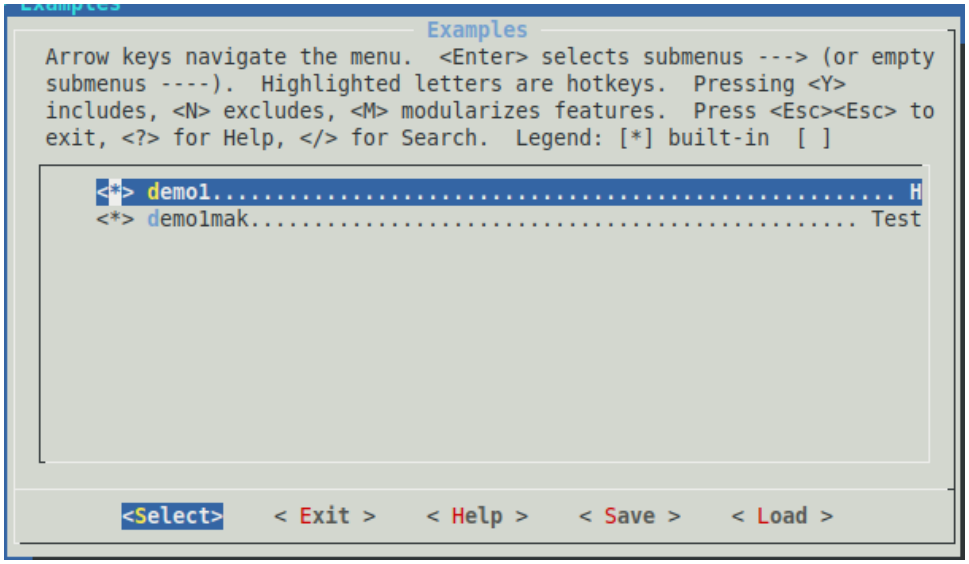




8. Zaktualizowano listy pakietów komendami:

./scripts/feeds update -a
./scripts/feeds install -p skps -a
./scripts/feeds install -p packages -a

9. W menu konfiguracyjnym zaznaczono pakiety demonstracyjne



10. Skompilowano pakiety demonstracyjne komendami

make package/demo1/compile

make package/demo1mak/compile

11. Pakiety zostały pobrane z użyciem serwera http Python
12. Zainstalowano pakiety z użyciem opkg
13. Pakiet działa prawidłowo.

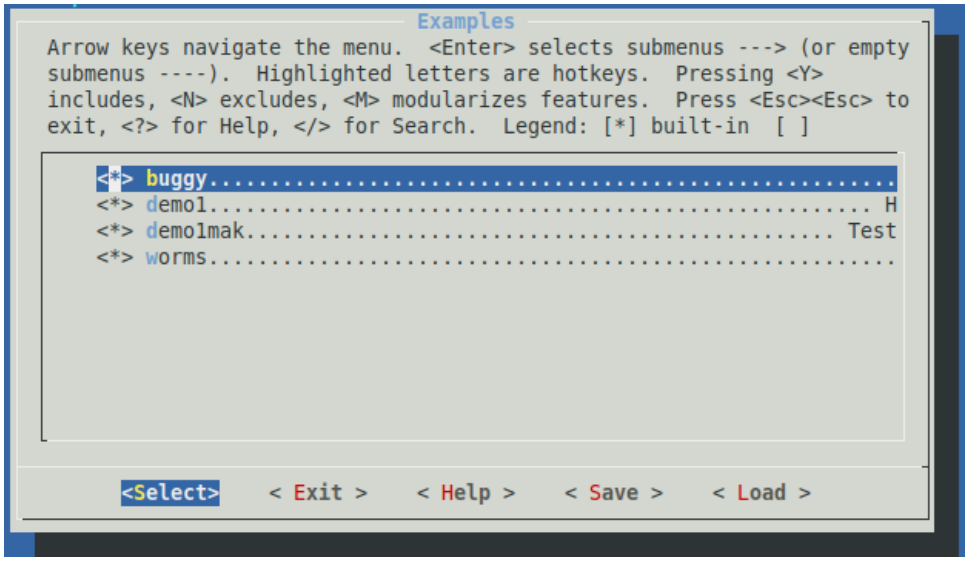
```
root@OpenWrt:/# wget http://192.168.9.117:8000/demo1mak_1_aarch64_cortex-a72.ipk
Downloading 'http://192.168.9.117:8000/demo1mak_1_aarch64_cortex-a72.ipk'
Connecting to 192.168.9.117:8000
Writing to 'demo1mak_1_aarch64_cortex-a72.ipk'
demo1mak_1_aarch64_c 100% |*****************************|  2023   0:00:00 ETA
Download completed (2023 bytes)
root@OpenWrt:/# wget http://192.168.9.117:8000/demo1_1.0-1_aarch64_cortex-a72.ip
k
Downloading 'http://192.168.9.117:8000/demo1_1.0-1_aarch64_cortex-a72.ipk'
Connecting to 192.168.9.117:8000
Writing to 'demo1_1.0-1_aarch64_cortex-a72.ipk'
demo1_1.0-1_aarch64_ 100% |*****************************|  2025   0:00:00 ETA
Download completed (2025 bytes)
root@OpenWrt:/# opkg install demo1
demo1_1.0-1_aarch64_cortex-a72.ipk  demo1mak_1_aarch64_cortex-a72.ipk
root@OpenWrt:/# opkg install demo1_1.0-1_aarch64_cortex-a72.ipk
Installing demo1 (1.0-1) to root...
Configuring demo1.
root@OpenWrt:/# demo1
dzien dobry
Komunikat z wątku A
Komunikat z wątku B
Komunikat z wątku B
Komunikat z wątku A
Komunikat z wątku B
^C
root@OpenWrt:/#
```

2. Pakiety “worms” i “buggy”

1. W katalogu z pakietami demonstracyjnymi (demo1_owrt_pkg) zostały umieszczone katalogi worms i buggy w celu ułatwienia pracy
2. W katalogach worms i buggy znajdują się dopisane pliki Makefile (umieszczone w repozytorium) oraz pliki źródłowe w podkatalogach src
3. Zaktualizowano listy pakietów komendami:

./scripts/feeds update -a
./scripts/feeds install -p skps -a
./scripts/feeds install -p packages -a

4. W make menuconfig zaznaczono pakiety worms i buggy.



5. Skompilowano pakiety demonstracyjne komendami

make package/worms/compile

make package/buggy/compile

6. Pakiety zostały pobrane z użyciem serwera http Python
7. Zainstalowano pakiety z użyciem opkg

```
root@OpenWrt:/# wget http://192.168.9.117:8000/buggy_1.0-1_aarch64_cortex-a72.ip
k
Downloading 'http://192.168.9.117:8000/buggy_1.0-1_aarch64_cortex-a72.ipk'
Connecting to 192.168.9.117:8000
Writing to 'buggy_1.0-1_aarch64_cortex-a72.ipk'
buggy_1.0-1_aarch64_ 100% |*******************************|  2339   0:00:00 ETA
Download completed (2339 bytes)
root@OpenWrt:/# wget http://192.168.9.117:8000/worms_1.0-1_aarch64_cortex-a72.ip
k
Downloading 'http://192.168.9.117:8000/worms_1.0-1_aarch64_cortex-a72.ipk'
Connecting to 192.168.9.117:8000
Writing to 'worms_1.0-1_aarch64_cortex-a72.ipk'
worms_1.0-1_aarch64_ 100% |*******************************|  4014   0:00:00 ETA
Download completed (4014 bytes)
root@OpenWrt:/# opkg install buggy_1.0-1_aarch64_cortex-a72.ipk
Installing buggy (1.0-1) to root...
Configuring buggy.
root@OpenWrt:/# opkg install worms_1.0-1_aarch64_cortex-a72.ipk
Installing worms (1.0-1) to root...
Configuring worms.
root@OpenWrt:/#
```

8. Wynik działania Worms

```
root@OpenWrt:/# opkg install demo1
demo1_1.0-1_aarch64_cortex-a72.ipk  demo1mak_1_aarch64_cortex-a72.ipk
root@OpenWrt:/# opkg install demo1_1.0-1_aarch64_cortex-a72.ipk
Installing demo1 (1.0-1) to root...
  X
O
O
O
O
O
O
O
O
You hit a wall!
Your score is 14
root@OpenWrt:/#
```

9. Wynik działania Buggy

```
root@OpenWrt:/# bug1
Segmentation fault
root@OpenWrt:/# bug2
Segmentation fault
root@OpenWrt:/# bug3
s1=@ABCDEFGHIJKLMNOPQRSTUVW
s2=JKLMNOPQRSTUVW
root@OpenWrt:/#
```

3. Debugowanie zdalne

1. Zainstalowano gdb i gdbserver komendami:

opkg update

opkg install gdb

opkg install gdbserver

2. Na RPi uruchomiono gdbserver komendą:

gdbserver :9000 /usr/bin/bug3

3. Na hoście uruchomiono skrypt komendą:

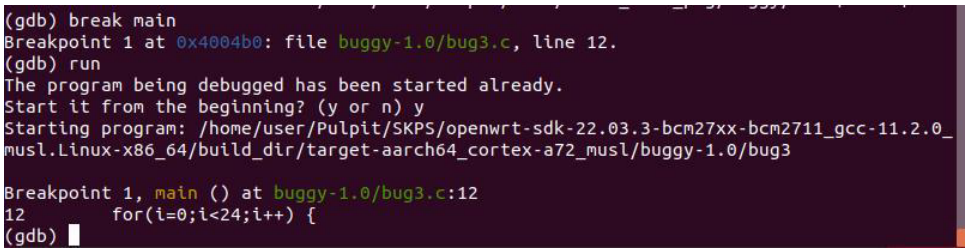
./scripts/remote-gdb 10.42.0.200:9000 ./build_dir/target-aarch64_cortex-a72_musl/buggy-1.0/bug3

4. Dodano podkatalog z kodami źródłowymi komendą:

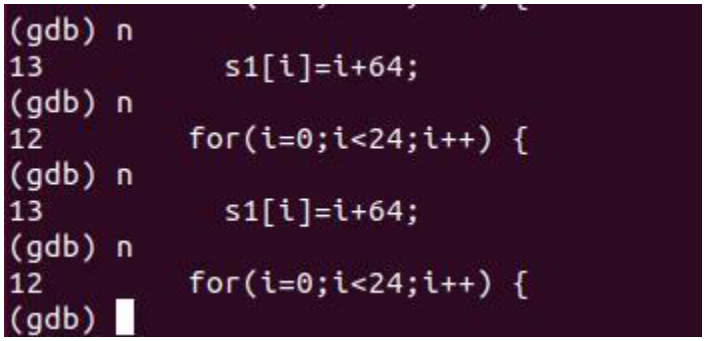
directory /home/user/Pulpit/SKPS/demo1_owrt_pkg/buggy/src

5. Doświadczenia z gdb:

5.1. Ustawienie breakpointu (break main)



5.2. Praca krokowa (next)



5.3. Podgląd wartości zmiennej (print i / display i)

```
(gdb) print i
$1 = 2
(gdb) display i
1: i = 2
(gdb) n
13          s1[i]=i+64;
1: i = 2
(gdb) n
12        for(i=0;i<24;i++) {
1: i = 3
(gdb) n
13          s1[i]=i+64;
1: i = 3
(gdb)
```

5.4. Podgląd stosu (x/40x $sp)

```
(gdb) x/40x $sp
0x7fffffd70:    0xffffd80       0x0000007f      0xf7f93190      0x0000007f
0x7fffffd80:    0x00000000      0x00000000      0x00000000      0x00000000
0x7fffffd90:    0xffffdb0       0x0000007f      0xf7ffdca8      0x0000007f
0x7fffffda0:    0xf7ffde50      0x0000007f      0xf7ffde50      0x0000007f
0x7fffffdb0:    0x00000001      0x00000000      0xffffff75      0x0000007f
0x7fffffdc0:    0x00000000      0x00000000      0xffffff83      0x0000007f
0x7fffffdd0:    0xffffff8b      0x0000007f      0xffffff96      0x0000007f
0x7fffffde0:    0xffffffa6      0x0000007f      0xffffffb6      0x0000007f
0x7fffffdf0:    0xffffffc1      0x0000007f      0xffffffe4      0x0000007f
0x7fffffe00:    0x00000000      0x00000000      0x00000021      0x00000000
(gdb)
```

5.5. Backtrace (bt)

```
(gdb) bt
#0  main () at buggy-1.0/bug3.c:13
(gdb)
```

5.6. Wykorzystanie watchpoint'ów (watch s1[10])

```
(gdb) watch s1[10]
Watchpoint 3: s1[10]
(gdb) c
Continuing.
Warning:
Could not insert hardware watchpoint 2.
Could not insert hardware breakpoints:
You may have requested too many hardware breakpoints/watchpoints.

Command aborted.
(gdb) info breakpoints
Num     Type           Disp Enb Address            What
1       breakpoint     keep y   0x00000000004004b0 in main at buggy-1.0/bug3.c:12
        breakpoint already hit 1 time
2       hw watchpoint  keep y                      s1[10]
3       watchpoint     keep y                      s1[10]
(gdb) delete breakpoints
Delete all breakpoints? (y or n) y
(gdb) info breakpoints
No breakpoints or watchpoints.
(gdb) watch s1[10]
Watchpoint 4: s1[10]
(gdb) c
Continuing.

Watchpoint 4: s1[10]

Old value = 97 'a'
New value = 74 'J'
main () at buggy-1.0/bug3.c:12
12        for(i=0;i<24;i++) {
1: i = 11
(gdb)
```

P

6. Znaleziony błąd bug1: brak alokacji tablicy table

```
(gdb) break main
Breakpoint 1 at 0x400460: file buggy-1.0/bug1.c, line 9.
(gdb) run
Starting program: /home/user/Pulpit/SKPS/openwrt-sdk-22.03.3-bcm27xx-bcm2711_gcc-11.2.
0_musl.Linux-x86_64/build_dir/target-aarch64_cortex-a72_musl/buggy-1.0/bug1

Breakpoint 1, main () at buggy-1.0/bug1.c:9
9         for(i=0;i<1000;i++) {
(gdb) step

Program received signal SIGSEGV, Segmentation fault.
0x000000000040046c in main () at buggy-1.0/bug1.c:9
9         for(i=0;i<1000;i++) {
(gdb) print table
$1 = (int *) 0x0
```

7. Znaleziony błąd bug2: dostęp poza tablicą

```
(gdb) break main
Breakpoint 1 at 0x400460: file buggy-1.0/bug2.c, line 7.
(gdb) run
Starting program: /home/user/Pulpit/SKPS/openwrt-sdk-22.03.3-bcm27xx-bcm2711_gcc-11.2.0_musl.
Linux-x86_64/build_dir/target-aarch64_cortex-a72_musl/buggy-1.0/bug2

Breakpoint 1, main () at buggy-1.0/bug2.c:7
7         for(i=0;i<1000000;i++) {
(gdb) watch i if i >= 999
Watchpoint 2: i
(gdb) continue
Continuing.

Watchpoint 2: i

Old value = 998
New value = 999
main () at buggy-1.0/bug2.c:7
7         for(i=0;i<1000000;i++) {
(gdb) display i
1: i = 999
(gdb) delete breakpoints
Delete all breakpoints? (y or n) y
(gdb) continue
Continuing.

Program received signal SIGSEGV, Segmentation fault.
main () at buggy-1.0/bug2.c:8
8           table[i]=i;
1: i = 1008
(gdb)
```

8. Znaleziony błąd bug3: nadpisanie ‘/0’ w stringu.

```
(gdb) break main
Breakpoint 1 at 0x4004b0: file buggy-1.0/bug3.c, line 12.
(gdb) run
Starting program: /home/user/Pulpit/SKPS/openwrt-sdk-22.03.3-bcm27xx-bcm2711_gcc-11.2.0_musl.Linux-x86_6
4/build_dir/target-aarch64_cortex-a72_musl/buggy-1.0/bug3

Breakpoint 1, main () at buggy-1.0/bug3.c:12
12      buggy-1.0/bug3.c: No such file or directory.
(gdb) watch i if i >= 9
Watchpoint 2: i
(gdb) display s1[9]
1: s1[9] = 0 '\000'
(gdb) c
Continuing.

Watchpoint 2: i

Old value = 8
New value = 9
main () at buggy-1.0/bug3.c:12
12      in buggy-1.0/bug3.c
1: s1[9] = 0 '\000'
(gdb) step
13      in buggy-1.0/bug3.c
1: s1[9] = 0 '\000'
(gdb) step

Watchpoint 2: i

Old value = 9
New value = 10
main () at buggy-1.0/bug3.c:12
12      in buggy-1.0/bug3.c
1: s1[9] = 73 'I'
```