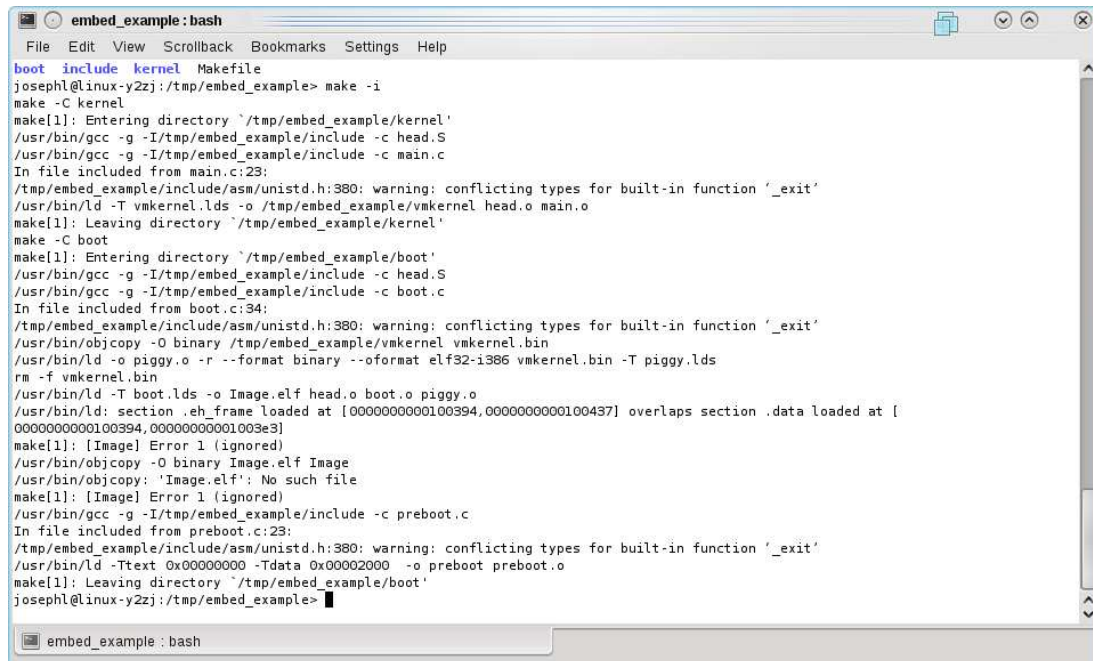


Linux kernel and driver programming homework assignment #1

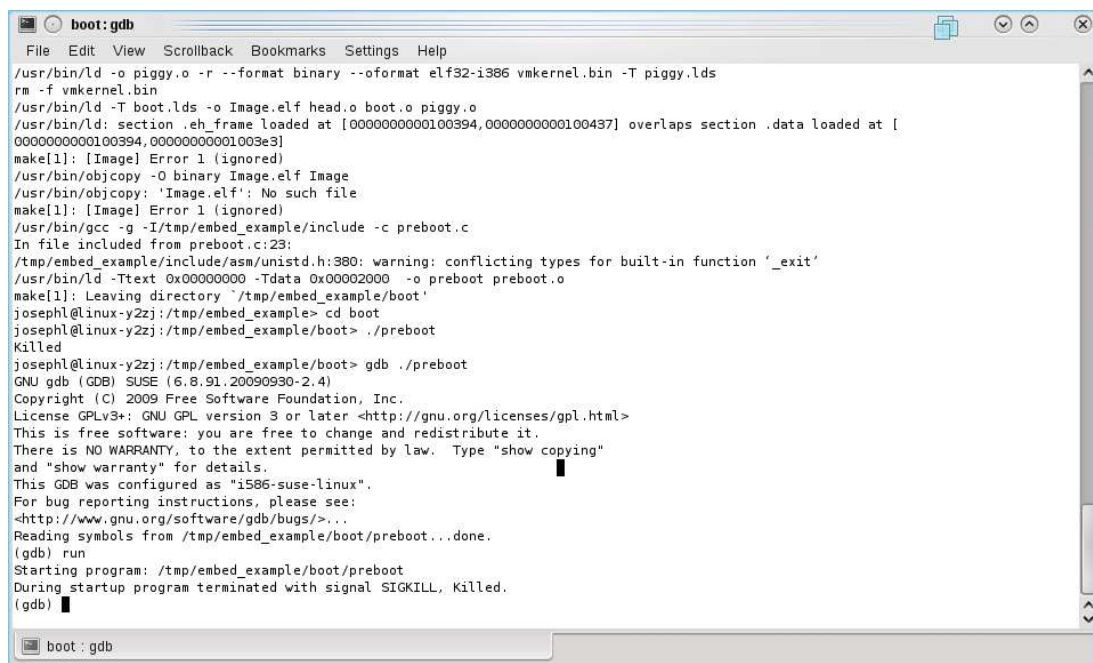
Deadline: 2010/07/06, Print your answer on A4 papers and submit during class.

At this homework assignment, we will port the `embed_example.zip`, which we used in the class to show you the skills of using `gcc` and `binutils` when developing an embedded platform, to Linux 2.6.3x (or later) kernel. I suggest you do this homework in OpenSUSE 11.2 in case if there is any difference in the kernel.



```
embed_example: bash
File Edit View Scrollback Bookmarks Settings Help
boot include kernel Makefile
josephl@linux-y2zj:/tmp/embed_example> make -i
make -C kernel
make[1]: Entering directory `/tmp/embed_example/kernel'
/usr/bin/gcc -g -I/tmp/embed_example/include -c head.S
/usr/bin/gcc -g -I/tmp/embed_example/include -c main.c
In file included from main.c:23:
/tmp/embed_example/include/asm/unistd.h:380: warning: conflicting types for built-in function '_exit'
/usr/bin/ld -T vmkernel.lds -o /tmp/embed_example/vmkernel head.o main.o
make[1]: Leaving directory `/tmp/embed_example/kernel'
make -C boot
make[1]: Entering directory `/tmp/embed_example/boot'
/usr/bin/gcc -g -I/tmp/embed_example/include -c head.S
/usr/bin/gcc -g -I/tmp/embed_example/include -c boot.c
In file included from boot.c:34:
/tmp/embed_example/include/asm/unistd.h:380: warning: conflicting types for built-in function '_exit'
/usr/bin/objcopy -O binary /tmp/embed_example/vmkernel vmkernel.bin
/usr/bin/ld -o piggy.o -r --format binary --oformat elf32-i386 vmkernel.bin -T piggy.lds
rm -f vmkernel.bin
/usr/bin/ld -T boot.lds -o Image.elf head.o boot.o piggy.o
/usr/bin/ld: section .eh_frame loaded at [0000000000100394,0000000000100437] overlaps section .data loaded at [
0000000000100394,00000000001003e3]
make[1]: [Image] Error 1 (ignored)
/usr/bin/objcopy -O binary Image.elf Image
/usr/bin/objcopy: 'Image.elf': No such file
make[1]: [Image] Error 1 (ignored)
/usr/bin/gcc -g -I/tmp/embed_example/include -c preboot.c
In file included from preboot.c:23:
/tmp/embed_example/include/asm/unistd.h:380: warning: conflicting types for built-in function '_exit'
/usr/bin/ld -Ttext 0x00000000 -Tdata 0x00002000 -o preboot preboot.o
make[1]: Leaving directory `/tmp/embed_example/boot'
josephl@linux-y2zj:/tmp/embed_example>
```

There are some warnings and errors in the screenshot above. We will investigate them one by one. First, try to execute the executable 'preboot'.



```
boot: gdb
File Edit View Scrollback Bookmarks Settings Help
/usr/bin/ld -o piggy.o -r --format binary --oformat elf32-i386 vmkernel.bin -T piggy.lds
rm -f vmkernel.bin
/usr/bin/ld -T boot.lds -o Image.elf head.o boot.o piggy.o
/usr/bin/ld: section .eh_frame loaded at [0000000000100394,0000000000100437] overlaps section .data loaded at [
0000000000100394,00000000001003e3]
make[1]: [Image] Error 1 (ignored)
/usr/bin/objcopy -O binary Image.elf Image
/usr/bin/objcopy: 'Image.elf': No such file
make[1]: [Image] Error 1 (ignored)
/usr/bin/gcc -g -I/tmp/embed_example/include -c preboot.c
In file included from preboot.c:23:
/tmp/embed_example/include/asm/unistd.h:380: warning: conflicting types for built-in function '_exit'
/usr/bin/ld -Ttext 0x00000000 -Tdata 0x00002000 -o preboot preboot.o
make[1]: Leaving directory `/tmp/embed_example/boot'
josephl@linux-y2zj:/tmp/embed_example> cd boot
josephl@linux-y2zj:/tmp/embed_example/boot> ./preboot
Killed
josephl@linux-y2zj:/tmp/embed_example/boot> gdb ./preboot
GNU gdb (GDB) SUSE (6.8.91.20090930-2.4)
Copyright (C) 2009 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "i586-suse-linux".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /tmp/embed_example/boot/preboot...done.
(gdb) run
Starting program: /tmp/embed_example/boot/preboot
During startup program terminated with signal SIGKILL, Killed.
(gdb)
```

You see the program got SIGKILL signal immediately upon execution. It's not

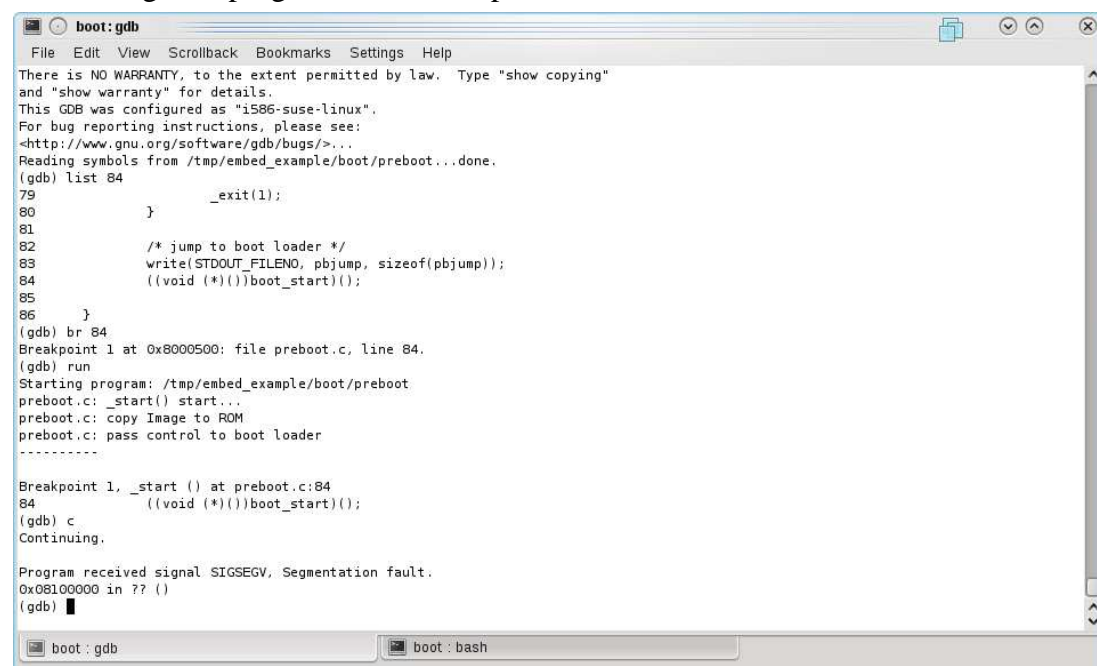
memory access error signal (SIGSEGV) we often see in user application. This error is probably that the memory area we defined is illegal now (.text at 0x00000000) and the ELF loader reject to load the binary.

(1) Adjust (shift) the memory layout of the example so that every program can run successfully. Please describe your modification and show me your adjusted memory layout in a table. (25 points)

After the adjustment, you should be able to run 'preboot', but it will fail to load Image.elf. In the first screenshot above, the linker complained that .eh_frame sections overlaps .data section. .eh_frame section is generated by gcc for every file it compiles. The purpose of the .eh_frame is to unwind call frames at exception handling (C++). We do not need .eh_frame here.

(2) Remove the .eh_frame section from all object file so that linker can link every program successfully. Please describe your modification (changes you've done to which file) (25 points)

At this stage, all program can be compiled. But ..



```
boot: gdb
File Edit View Scrollback Bookmarks Settings Help
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "i586-suse-linux".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /tmp/embed_example/boot/preboot...done.
(gdb) list 84
79         _exit(1);
80     }
81
82     /* jump to boot loader */
83     write(STDOUT_FILENO, pbjump, sizeof(pbjump));
84     ((void (*)(void))boot_start)();
85
86 }
(gdb) br 84
Breakpoint 1 at 0x8000500: file preboot.c, line 84.
(gdb) run
Starting program: /tmp/embed_example/boot/preboot
preboot.c: _start() start...
preboot.c: copy Image to ROM
preboot.c: pass control to boot loader
-----
Breakpoint 1, _start () at preboot.c:84
84     ((void (*)(void))boot_start)();
(gdb) c
Continuing.

Program received signal SIGSEGV, Segmentation fault.
0x08100000 in ?? ()
(gdb) █

boot: gdb
```

Since Linux 2.6, heap and stack are protected from being executed. Intel processor supports the 'NX bit' (no execution) in the page table. When a page is executed without NX bit while NX support is enabled, the processor raises the page fault exception. This prevents malicious program from feeding its own code to run in a careless designed program by exploiting techniques like buffer overrun.

(3) To run this example in OpenSUSE 11.2, NX support must be disabled. Please do a freetext search in the kernel source code to find out how to disable NX support in the Linux kernel. Describe your findings here. (25 points)

(4) The porting is almost completed. But there are still some warning messages during program compilation (check the warning message in the first screenshot above). Please consult gcc man page to find a gcc option that will fix these warning messages. (25 points)