Simple Loader in C

Contributors: Aditya Gupta & Abhishek Bansal

Individual Contribution

- Aditya: Loader & top-level Makefile
- Abhishek: Launcher & Sub-Makefiles & checks on elf file

Implementation

the steps for the implementation of the loader are as follows:

1. As given to us , we have too pointers ehdr and phdr. We have assigned the memory to them using malloc. Now edhr is of size - sizeof(Elf32_Ehdr) and for the phdr the size is (sizeof(ehdr → e_phentsize * ehdr → e_phnum))
2. As we have e_phnum number of program headers and each of that is of size e_phentsize. Now, we have a fd as the seek in which we have the starting pointer to the elf file . So , we can simply use read system call to point edhr to the starting of the elf file. Also , now we can use lseek system call to set the fd seek at the e_phoff position , where the program headers start from . Now read the fd again for phdr to make the phdr point at the first program header .
3. Now , we iterate through the program headers by simple array iteration . We want a program header with the p_type as PT_LOAD . Also the necessary condition is that the e_entry point lies inside the range of the program header virtual memory ,i.e it should be between phdr →v_addr to phdr →v_addr + phdr →p_memsz
4. Now ,after finding the suitable program header , we make a segment and store it inside the memory using the mmap function with suitable arguments . The first argument takes the starting address, the second takes the size ,the third and fourth are the PROT and MAP ,the fifth argument is fd (the seek) and the last argument is the offset .
5. after that we have typedefed ehdr→e_entry to _start functional pointer and called the _start and equated result to _start() .
6. we have also kept many checks on the elf file such as check of elf magic numbers, exit failure check , mapping check , etc .

Github Repository

Steps to run:

With-Bonus

1. Run top-level Makefile
2. Change directory to bin
3. Run ./launch with ./fib as parameter

Without-Bonus

1. Run makefile
2. Run ./loader with ./fib as parameter