Technische Universität München
Fakultät für Informatik

Dr. K. N. Verma
verma@in.tum.de
Room: MI 02.07.041

Language Based Security

Winter Semester 2008

Exercise sheet 3. *12 Nov 2008*

Exercise 1:

The shellcode discussed in the lecture spawned a shell by calling execve. If the vulnerable program is setuid root, then this can give us a shell running with root permissions. However newer shells prevent effective user id (uid) and group id (gid) being different from the real uid and gid. This problem can be solved by changing real uid and gid to the effective uid and gid before the execve call. This can be done by the following code.

```
setreuid(geteuid(), -1);
setregid(getegid(), -1);
```

Modify the shellcode appropriately so that the example vulnerable program of the lecture spawns a root shell in case this vulnerable program is setuid root.