System Security Module: MCSSE-CYB-02
Constructor University Date: 2024-04-08
Dr. Jürgen Schönwälder **Due: 2024-04-15**

Problem Sheet #3

Problem 3.1: *POSIX discretionary access control* (1+1+1+1+1 = 5 points)

Some students use a Linux server to share files. The students have different interests, which is reflected in their group memberships.

user	group	groups
bob	bob	bob users painting electro
alice	alice	alice users painting photos
frank	frank	frank users electro
eve	eve	eve users photos

Frank created a directory to share electro beats with Bob. He did set the permissions as follows:

```
$ ls -ld beats
dr-xrws--- 2 frank electro 4096 Mar 29 17:30 beats
```

Answer the following questions:

a) Who can create files in the beats folder? For each user, explain why or why not.

b) What is the meaning of the `s` bit on the owning group permissions?

c) What is the corresponding POSIX ACL representation?

d) Frank wants to allow Eve to listen to the beats he is developing together with Bob. He executes the following shell command:

```
setfacl -m u:eve:r-x beats
```

What is the new POSIX ACL representation? Explain the new or modified elements.

e) New beats created by Bob have restrictive file permissions `-rw-r--r--` (since Bob uses a narrow `umask` of `0022` and Bob does not want to change his umask). Can POSIX ACLs be used to solve this problem? Which command needs to be executed and what is the resulting POSIX ACL representation?

Problem 3.2: *no Internet via seccomp-bpf (noinet)* (4+1 = 5 points)

Linux Secure Computing filters are inherited by `fork()`/`clone()` and `execve()` system calls. Hence, it is possible to write wrapper programs disallowing certain system calls before executing some other program.

a) Write a program `noinet` disallowing Internet communication by rejecting all `socket()` system calls that are not of type `AF_UNIX`. If an attempt to create a disallowed socket is made, fail the system call with an `EACCES` error. Here is how `noinet` would be used to execute `date` preventing any Internet access.

```
$ ./build/noinet date
Thu Apr 11 21:17:06 CEST 2024
```

b) Run five different command line programs that use the Internet under control of `noinet` and report how they react.