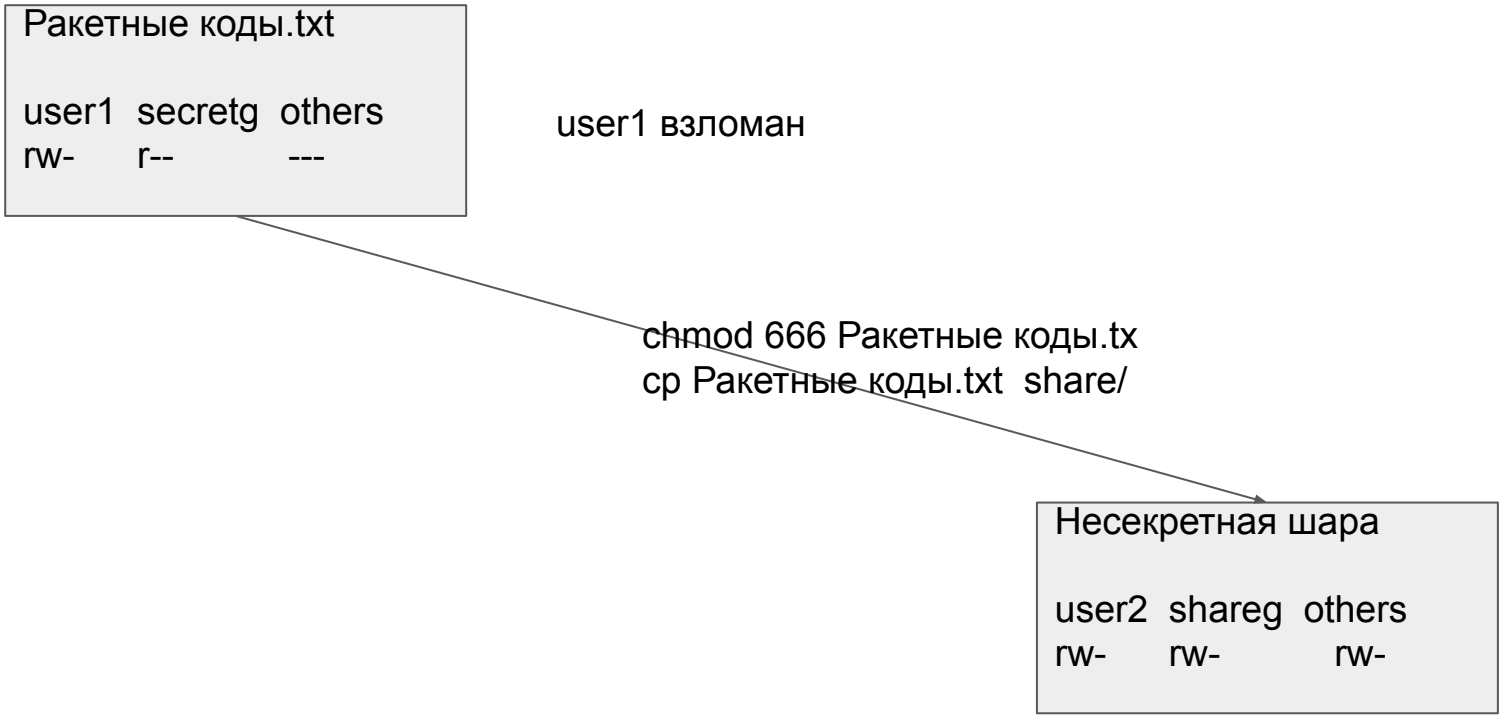
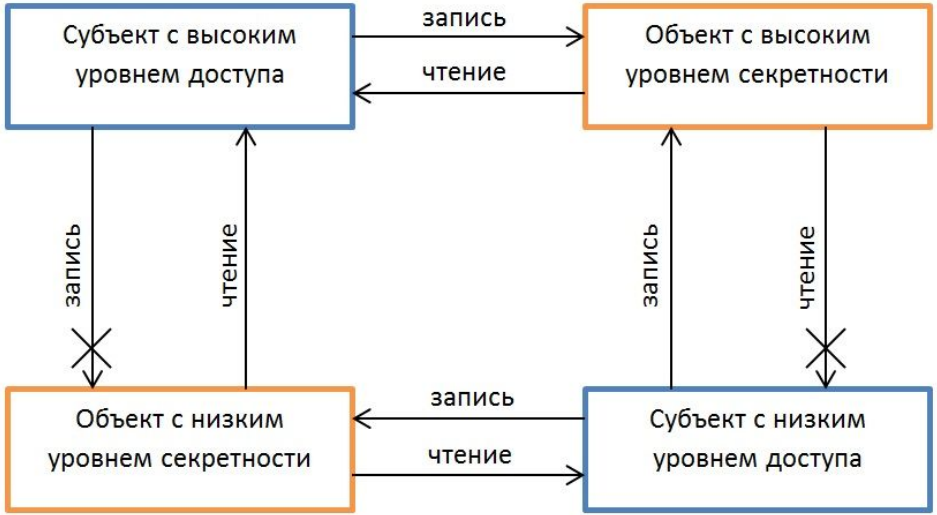
Программирование в Linux

Linux capabilities. Linux namespaces

Почему не подходят стандартные пользователи и группы?



Мандатный контроль доступа (SELinux, AstraLinux)



Модель Белла-Лападулы

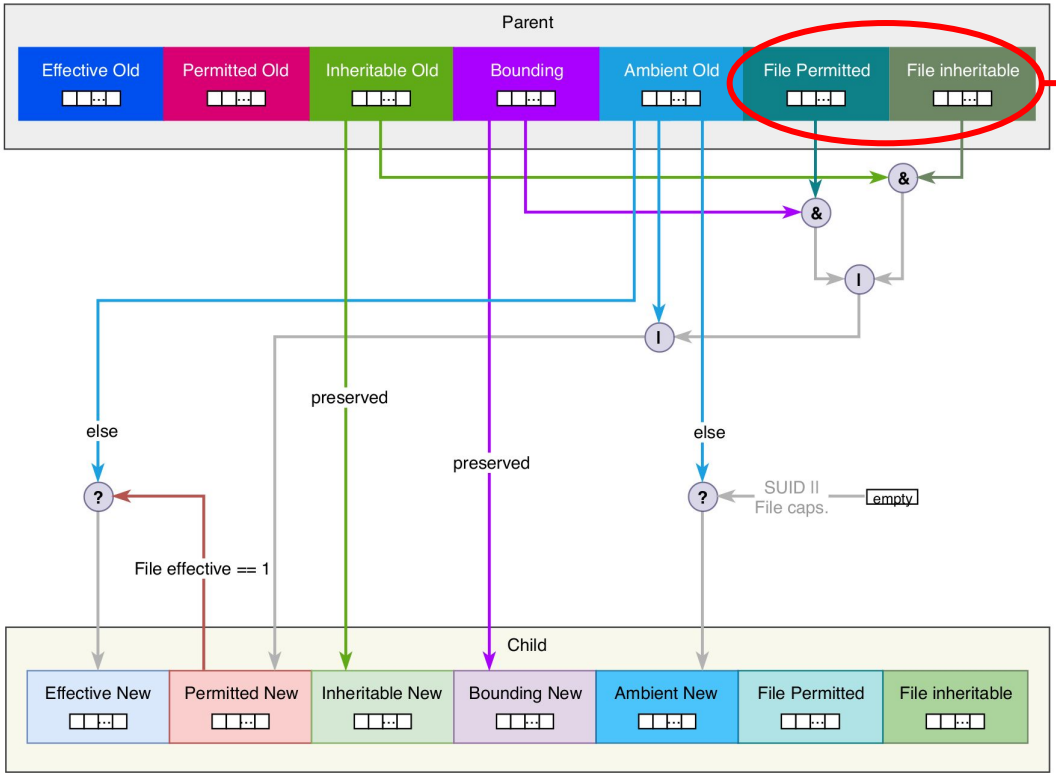
Сессия пользователя снабжена меткой:
Не секретно, ДСП, С, СС, ОВ

Объекты (файлы, процессы)
помечаются теми же метками

Linux capabilities

Linux capabilities

Нарежем root-права на 30+ частей и будем их раздавать исполнимым файлам и потокам/процессам



Нужна FS с поддержкой xattrs

Для потока

- Effective — какие используются в момент проверки доступа
- Permitted — какие можно выставить в Effective в процессе работы
- Inheritable — что передается сквозь exec к потомку
- Bounding — ограничение того, что может дать файл или что можно дописать в Inheritable
- Ambient (Linux 4.3) — а чего б еще такого прокинуть через exec, если исполняем непривилегированный файл

Для исполнимого файла

- Permitted — что будет разрешено выставлять процессу
- Inheritable — ограничение того, что можно наследовать процессу через exec
- Effective-bit — применить ли все Permitted сразу после exec ?

```
P'(ambient)     = (file is privileged) ? 0 : P(ambient)

P'(permitted)   = (P(inheritable) & F(inheritable)) |
                  (F(permitted) & P(bounding)) | P'(ambient)

P'(effective)   = F(effective) ? P'(permitted) : P'(ambient)

P'(inheritable) = P(inheritable)    [i.e., unchanged]

P'(bounding)    = P(bounding)       [i.e., unchanged]
```

см. man capabilities

Работа с linux capabilities

```
LIBCAP(3)                                Linux Programmer's Manual                                LIBCAP(3)

NAME
       cap_clear,  cap_clear_flag,  cap_compare,  cap_copy_ext,  cap_copy_int,  cap_free,  cap_from_name,  cap_from_text,  cap_get_fd,  cap_get_file,
       cap_get_flag, cap_get_pid, cap_get_proc, cap_set_fd, cap_set_file, cap_set_flag, cap_set_proc, cap_size, cap_to_name,  cap_to_text,  cap_get_pid,
       cap_dup - capability data object manipulation
```

```
GETCAP(8)                                System Manager's Manual                                GETCAP(8)

NAME
       getcap - examine file capabilities
```

```
SETCAP(8)                                System Manager's Manual                                SETCAP(8)

NAME
       setcap - set file capabilities

SYNOPSIS
       setcap [-q] [-n <rootid>] [-v] {capabilities|-|-r} filename [ ... capabilitiesN fileN ]
```

setcap cap_sys_rawio=+p test_fragmentation

Linux namespaces

UTS

Изоляция hostname и domainname

Mount

Изоляция дерева каталогов и точек монтирования

PID

Изоляция дерева процессов

User

Изоляция видимых пользователей и групп

IPC

Изоляция IPC-объектов (очереди, мьютексы, именованная память)

Network

Изоляция сетевых интерфейсов (eth, wlan) и портов

Cgroup

Изоляция содержимого `/sys/fs/cgroup/`

```
dmis@dmis-MS-7A15:~$ ls -l /proc/$$/ns/
total 0
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:57 cgroup -> 'cgroup:[4026531835]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:57 ipc -> 'ipc:[4026531839]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:57 mnt -> 'mnt:[4026531840]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:57 net -> 'net:[4026531992]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:57 pid -> 'pid:[4026531836]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:57 pid_for_children -> 'pid:[4026531836]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:57 user -> 'user:[4026531837]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:57 uts -> 'uts:[4026531838]'
dmis@dmis-MS-7A15:~$
```

```
dmis@dmis-MS-7A15:~$ ls -l /proc/$$/ns
total 0
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:58 cgroup -> 'cgroup:[4026531835]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:58 ipc -> 'ipc:[4026531839]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:58 mnt -> 'mnt:[4026531840]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:58 net -> 'net:[4026531992]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:58 pid -> 'pid:[4026531836]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:58 pid_for_children -> 'pid:[4026531836]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:58 user -> 'user:[4026531837]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:58 uts -> 'uts:[4026531838]'
dmis@dmis-MS-7A15:~$
```

```
dmis@dmis-MS-7A15:~$ hostname
dmis-MS-7A15
dmis@dmis-MS-7A15:~$ ls -l /proc/$$/ns
total 0
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:58 cgroup -> 'cgroup:[4026531835]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:58 ipc -> 'ipc:[4026531839]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:58 mnt -> 'mnt:[4026531840]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:58 net -> 'net:[4026531992]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:58 pid -> 'pid:[4026531836]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:58 pid_for_children -> 'pid:[4026531836]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:58 user -> 'user:[4026531837]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 20:58 uts -> 'uts:[4026531838]'
dmis@dmis-MS-7A15:~$ hostname
dmis-MS-7A15
dmis@dmis-MS-7A15:~$ date
Bc 04 anp 2021 21:01:47 MSK
dmis@dmis-MS-7A15:~$ date
Bc 04 anp 2021 21:02:03 MSK
dmis@dmis-MS-7A15:~$ hostname
dmis-MS-7A15
dmis@dmis-MS-7A15:~$
```

```
dmis@dmis-MS-7A15:~$ sudo unshare -u bash
[sudo] password for dmis:
root@dmis-MS-7A15:/home/dmis# su dmis
dmis@dmis-MS-7A15:~$ hostname
dmis-MS-7A15
dmis@dmis-MS-7A15:~$ ls -l /proc/$$/ns
total 0
lrwxrwxrwx 1 dmis dmis 0 anp  4 21:00 cgroup -> 'cgroup:[4026531835]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 21:00 ipc -> 'ipc:[4026531839]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 21:00 mnt -> 'mnt:[4026531840]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 21:00 net -> 'net:[4026531992]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 21:00 pid -> 'pid:[4026531836]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 21:00 pid_for_children -> 'pid:[4026531836]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 21:00 user -> 'user:[4026531837]'
lrwxrwxrwx 1 dmis dmis 0 anp  4 21:00 uts -> 'uts:[4026533760]'
dmis@dmis-MS-7A15:~$ hostname new-namespace-hostname
hostname: you must be root to change the host name
dmis@dmis-MS-7A15:~$ sudo hostname new-namespace-hostname
dmis@dmis-MS-7A15:~$ hostname
new-namespace-hostname
dmis@dmis-MS-7A15:~$ date
Bc 04 anp 2021 21:01:45 MSK
dmis@dmis-MS-7A15:~$ hostname
new-namespace-hostname
dmis@dmis-MS-7A15:~$ date
Bc 04 anp 2021 21:02:00 MSK
dmis@dmis-MS-7A15:~$
```

```c
#define STACK_SIZE 4096

char child_stack[STACK_SIZE];

int child_cmd(void* arg) {
    system("hostname newname");
    system("hostname");
    return 0;
}

int main(int argc, char **argv)
{
    int clone_flags = SIGCHLD | CLONE_NEWUTS; // создать новое UTS пространство
    int cmd_pid = clone(child_cmd, child_stack + STACK_SIZE, clone_flags, NULL);

    if (cmd_pid < 0) {
        perror("clone");
        return EXIT_SUCCESS;
    }


    if (waitpid(cmd_pid, NULL, 0) == -1) {
        perror("waitpid");
        return EXIT_SUCCESS;
    }

    system("hostname");

    return 0;
}
```

```
dmis@dmis-MS-7A15:~$ ls LinuxEgs/
abuse_root      events        hello1             libexample.so  system_c
capabilities    files         hello_fs           libs_undef     weak_syms
coredumps       fokrs         hello_strip        links
create_hello.c  fuse_abuse.c  hello_world.c      link_script
ctors           hack          hello_world_entry.c  mappings
elf_parse       hello         lib_example.c      plugins_egs
dmis@dmis-MS-7A15:~$ sudo unshare -m /bin/bash
root@dmis-MS-7A15:/home/dmis# mount --bind  LinuxEgs /tmp/unshared/
root@dmis-MS-7A15:/home/dmis# ls /tmp/unshared/
abuse_root      events        hello1             libexample.so  system_c
capabilities    files         hello_fs           libs_undef     weak_syms
coredumps       fokrs         hello_strip        links
create_hello.c  fuse_abuse.c  hello_world.c      link_script
ctors           hack          hello_world_entry.c  mappings
elf_parse       hello         lib_example.c      plugins_egs
root@dmis-MS-7A15:/home/dmis# cd ..
root@dmis-MS-7A15:/home# cd ..
root@dmis-MS-7A15:/# umount -l /home/
root@dmis-MS-7A15:/# ls /home/
root@dmis-MS-7A15:/# mount --bind /tmp/unshared/ /home/
root@dmis-MS-7A15:/# ls /home/
abuse_root      events        hello1             libexample.so  system_c
capabilities    files         hello_fs           libs_undef     weak_syms
coredumps       fokrs         hello_strip        links
create_hello.c  fuse_abuse.c  hello_world.c      link_script
ctors           hack          hello_world_entry.c  mappings
elf_parse       hello         lib_example.c      plugins_egs
root@dmis-MS-7A15:/# exit
dmis@dmis-MS-7A15:~$ ls /home
dmis  lost+found
```

docker на минималках

unshare -m /bin/bash
mount --bind newroot newroot
cd newroot
mkdir put_old
pivot_root . put_old
cd /
umount -l put_old