Cyber Security Past Paper

- Security (-2022), SecurityII (-2018)
- Reference
  - Credit: @Gyorgy Denes

## Access Control

For a directory D, the access control bits considered about **the list of filenames**. (different from a file F)

```
r for reading the names of the files contained

w to change the list of filenames in the directory
    create, delete, rename or move a file in it

The “sticky bit”  (10-th access control bit in *Berkeley Unix*)
    For D with access w, then a F inside can be removed/renamed only by the *owner* of F [or D].

x to access the contents or attributes of a file in it (directory traversal/search)
    dereference the inode of a known filename in it
```

set-user/group-ID

[Without] Process started by user U will have the same value U stored as the effective, real, and saved user ID and cannot change any of them.

[With] When a program file F with owner O is started by user U, the real user ID will be set to U, both the effective and the saved user ID of the process will be set to O.

- y2019p4q7 (a)
  - chmod
- y2012p4q8 (e)
  - dir, sticky bit

- y2021p4q6 (a)
    - file and dir
- y2020p4q7 (b)
    - setuid
- y2018p4q6
    - access-control matrix

## Buffer overflow

- y2022p4q6
- y2020p4q6 (a,c), y2018p4q7 (c)
    - countermeasures

## SQL injection

- y2021p4q7 (a)

## Malfunction

- y2023p4q7

## CSRF, XSS

- y2022p4q7
- y2019p4q6

## Password

Confidentiality, Integrity, Availability

- y2021p4q7 (b)
- y2012p4q8 (a)

    - salt

## Physical Security

- y2023p4q8