Computer Security (COM-301)

Discretionary Access Control

Carmela Troncoso

SPRING Lab

carmela.troncoso@epfl.ch

Simon says

Simon is the owner of Color OS, a simple OS that has 4 files: `red`, `yellow`, `green`, and `blue`.

Simon says that a user Harry can read the file red, can write yellow, and can read and execute blue. What is the capability that Simon should give to Harry?

(a)
`red`: {(Harry, read, no write/execute)}
`yellow`: {(Harry, write, no read/execute)}
`blue`: {(Harry, read/execute, no write)}.

(b)
`red`: {(Harry, read)}
`yellow`: {(Harry, write)}
`blue`: {(Harry, read/execute)}.

(c)
Harry: {(`red`, read), (`yellow`, write), (green, -), (`blue`, read/execute)}

(d)
Harry: {(`red`, read), (`yellow`, write), (`blue`, read/execute)}

Confusion

Which of the following security violations is **NOT** caused by a confused deputy?

(a) A hacker gains access to a user's social network account by getting the user's browser to send the hacker this user's credential

(b) A virus infects an email client to send spam

(c) A journalist tricks a banker into revealing the bank statements of a famous singer

(d) A detective leaks information to a criminal using a covert channel

To ACL or not ACL

We are back in COVID times, and contact tracing is needed.

You are setting up a new Bar in Lausanne, and have one computer for people to give their phone numbers. To make it easy you let them register (create a row with their phone number) and then only add the date where they visit the bar.

Is ACL a good solution to manage access to the database?
(to avoid that users can influence the contact tracing process)

And if instead of one computer you have one computer per table but they are not connected to the internet?

Building a messenger

Alice writes a small application `msg` to allow other users to leave messages for her. The application works such that executing '`msg string`' writes `string` into `msgfile.txt`, as described by this pseudocode

```
program msg(string input)
        {
            file = open("msgfile.txt","a"); // open messages log with append rights
            write(input+'\n',file); // write input in messages log
            close(file); // close messages log
            exit;
        }
```

Alice shares this messenger with Bob, and creates a group `Alice+Bob` to manage permission. What is the correct (Linux) permission configuration for Alice and Bob to be able to converse securely. Securely for Alice means that she wants to be sure that the integrity of the conversation is preserved, and no one else can read her messages with Bob.

```
----------   Alice Alice+Bob msg
----------   Alice Alice+Bob msgfile
```

Building a messenger

Two propositions:

```
      -rwx--x---   Alice Alice+Bob msg
(1)   -rwx------   Alice Alice+Bob msgfile

      -rwx--x---   Alice Alice+Bob msg
(2)   -rwx-w----   Alice Alice+Bob msgfile
```

What is wrong with each proposition? Propose a solution.