

# Flipped Classroom Exercise 1: Access Control Models

CS-E3130 Information Security, 12.09.2023

## 1. Access control concepts

Give an example (not a definition!) of each of the following concepts, explaining how it aids security:

1. Least-privilege principle
2. No-write-down
3. No-write-up

## 2. Parts of an access control system

Consider the Moodle system (named *MyCourses* at Aalto) containing the course material.

1. Identify the **Subjects** in the system.
2. Name at least two **Objects** in the system.
3. Suggest at least two **Permissions**.
4. Suggest two **Roles** that might be useful in MyCourses, and how they might be used.

## 3. The Bell-LaPadula model

Consider an EU computer system that uses a Bell-LaPadula to protect its data. EU classified information has the following labels, from most- to least-secret, which we denote with the bracketed letters:

- EU Top Secret (TS)
- EU Secret (S)
- EU Confidential (C)
- EU Restricted (R)

and implicitly,

- Unclassified (U)

The system contains the following users:

- Alice, clearance TS
- Bob, clearance R
- Carol, clearance U

and the following files, with the corresponding labels:

- Tender315-bids.xlsx (TS)
- timesheet.xlsx (R)
- logo.svg (U)

Answer the following questions:

1. To which files can each user write?
2. Write the protection state of the system in terms of an access control matrix.
3. What practical difficulties would you encounter, running the system above? *State your assumptions.*
4. Individual countries often have a similar system of labels for military information, with their own labels like TS, S, C, R, U. If the same system handled both national- and EU-classified information, would these labels be the same as the EU ones, or would you need to create a separate set of labels? Why? If so, what would the system's labels look like?