# CS5430 Homework 3: Information Flow

**General Instructions.** You are expected to work alone on this assignment.

**Due: December 1, 2023 11:59pm. No late assignments will be accepted.**

Submit your solution using CMS. Prepare your solution as .pdf, as follows:

- Use 10 point or larger font.
- Submit each problem (as a separate file) into the correct CMS submission box for that problem.

---

**Problem 1: Lattice of Labels.**

Your consulting company is implementing mandatory access control for its file system. Every employee has a rank and is certified as having expertise in one or more areas, as follows.

**Ranks**: consultant, srConsultant, director, vicePres, president
**Expertise areas**: hr, finance, opSys, middleware, compilers, networking.

Each file stores one or more documents Files and documents are assigned labels that list the minimum rank and expertise areas that a reader must have for read authorization.

(a) Describe a format for a label that can be associated with an employee or with a file.

(b) Give a definition for a partial order relation $\sqsubseteq$ on these labels such that

- An employee $E$ with label $L_E$ should be allowed to view the contents of a folder F with label $L_F$ if $L_F \sqsubseteq L_E$ holds.
- A folder with label $L_F$ should be allowed to store a document with label $L$ if $L \sqsubseteq L_F$ holds.

(c) Describe how to implement an operator $\sqcup$ on these labels. The goal is for label

$L_1 \sqcup L_2$

to be the appropriate label for the document that results when a document with label $L_1$ is stapled to the end of a document with label $L_2$.

**Problem 2: Type Checking a Program.**

Give a proof that the following program is type correct according to the type system described in the slides on Static Enforcement. Assume that $\Gamma(x) = L$, where $L \sqsubseteq H$ .

**if** *x*=0 **then** *x:*=1 **else skip fi**

**Problem 3: New type-checking rules.**

The type system described in the slides on Static Enforcement does not handle arrays and, in particular, assignment to arrays.

(a) Recall rule Assign for type checking an assignment statement involving an ordinary (unsubscripted variable).

$$\frac{\Gamma,ctx \vdash E:\lambda\,, \quad \lambda \sqcup ctx \sqsubseteq \Gamma(x)}{\Gamma,ctx \vdash x:=E}$$

What additional condition should be added as a hypothesis to the rule, in order to obtain a rule that can be used for subscripted variables.

$$\frac{\Gamma,ctx \vdash E:\lambda\,, \quad \lambda \sqcup ctx \sqsubseteq \Gamma(x)\,, \quad ?????}{\Gamma,ctx \vdash x[E'] := E}$$