CS5430 Homework 6: Information Flow

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

Due: December 4, 2022 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.

Read pages 163 – 165 (introduction to section 8.1 "Multi-level Security") of Chapter 8 (Mandatory Access Control) to familiarize yourself with richer formulations of security labels.

You are consulting to a new Internet start-up company, `AppropriateTube`, whose value proposition is facilitating the creation and dissemination of age- and belief-appropriate videos for impressionable children. *Age* is measured in terms of integers (representing years since birth) and defines the minimum age of an appropriate viewer; *beliefs* are characterized by a set of the following terms, called *content-descriptors*:

```
Alcohol, Bambi, BarbieAndKen, Barney, Disrespect, Evolution,
Intelligent_Design, Sexuality, TeddyBears, VerbalAbuse, Violence.
```

(a) Describe a data structure to represent a label that can be associated with a video, with a file that is storing a video, or with a process that is accessing a file containing a video.

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

- A process with label L' should be allowed to view a video with label L if $L \sqsubseteq L'$ holds.
- A file with label L' should be allowed to store a video with label L if $L \sqsubseteq L'$ holds.

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

$$L_G \sqcup L_F$$

to be the appropriate label for the file that results when the video stored in a file F with label L_F is appended to the end of the video in file G with label L_G.

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 $\Gamma(y) = H$ and $\Gamma(x) = L$, where $L \sqsubseteq H$.

y := 0;
while $x \leq 5$ **do** $y := y + 1$ **end**

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) Using notation x → y to indicate that information flows from x to y during program execution, what information flow(s) are caused by executing the subscripted assignment

A[expr1] := expr2

(b) 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.

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