CS5430 Homework 4: Mandatory Access Control

General Instructions. You may (but do not have to) collaborate with one other student on this assignment. If you do collaborate then both students should form a CMS group and submit their solution to that group. Both students are responsible for all of the answers.

Due: November 3, 2020 at 10:00am. No late assignments will be accepted.

Submit your solution using CMS. Typeset your solution to produce .pdf, as follows:

- Use 10 point or larger font.
- Put each problem into a separate file and submit it to the correct CMS submission box for that problem.
- Use at most 1 page per problem (unless stated otherwise).

Problem 1. To ensure that prerequisites are satisfied before a student enrolls in classes each semester, Corinth University decided to implement a mandatory access control scheme based on tags.

- Associated with each student S would be a tag T(S) that encodes information about what classes that student has taken.
- Associated with each course C would be a tag T(C) that encodes information about the prerequisites that must be satisfied prior to enrolling in C.

The plan had been to implement a reference monitor that ensures $T(C) \sqsubseteq T(S)$ holds before allowing a student S to enroll in a course C.

The set $\mathcal{T}$ of tags in this system were to be propositional logic formulas (i.e., Boolean expressions), where the propositional variables (i.e. variables) are names of courses. Here are examples of tags:

(*) (CS2800=true) $\wedge$ (CS2110=true)

(**) (CS2800=true) $\wedge$ ((CS2110=true) $\vee$ (CS2112=true))

The propositional variables in such formulas were to be interpreted as follows.

- In a formula being used as the tag associated with a student S, a propositional variable Cxxxx is true if and only if the associated student has already completed the named class. So, for example, tag (*) above would be associated with a student who has already completed CS2800 and CS2110. Tags associated with students are always conjunctions.

- In a formula being used as the tag associated with a course C, a propositional variable Cxxxx indicates that a course is part of the prerequisite. So, for example, tag (**) above might be associated with a course having as its prerequisite the completion of CS2800 as well as the completion of either CS2110 or CS2112.

Unfortunately, the company implementing this scheme went bankrupt before the work was completed. Corinth University has asked your advice in helping to understand what was to be done.

(a) T(C) and T(S) are propositional logic formulas. How can "T(C) $\sqsubseteq$ T(S)" be translated into a propositional logic formula that equals true if and only if a student S should be allowed to enroll in a course C.

(b) The set $\mathcal{T}$ of tags in this scheme are propositional logic formulas involving propositional variables Cxxxx, where Cxxxx is a course number listed in *Courses of Study* for Corinth University. In class, we discussed that having $\langle \mathcal{T}, \sqsubseteq \rangle$ be a poset facilitates the use of these tags for authorization. List the properties that must hold for $\langle \mathcal{T}, \sqsubseteq \rangle$ and explain/prove that each holds for the translation you suggested in (a).

(c) A student typically will enroll in multiple courses each semester. We therefore might define a join operator $\sqcup$ on tags. With this operator, for example, we could write

(***) (T(C1) $\sqcup$ T(C2) $\sqcup$ T(C3) $\sqcup$ T(C4)) $\sqsubseteq$ T(S)

to describe the situation when a student S is attempting to enroll in courses C1, C2, C3, and C4. Recall, we require that $\sqcup$ be defined in a way that satisfies:

forall tags T $\in \mathcal{T}$, T' $\in \mathcal{T}$: (T $\sqcup$ T') $\in \mathcal{T}$

That means T $\sqcup$ T' must translate into a formula of propositional logic. (i) Propose a translation of T $\sqcup$ T' into a propositional logic formula such that the translation of (***) equals true if and only if student S has satisfied the pre-requisites for all courses C1, C2, C3, and C4. (ii) Give the properties that must hold for T $\sqcup$ T'. (iii) Show that these properties hold for your translation of T $\sqcup$ T' into a propositional logic formula.

(d) **Extra Credit**. *[Submit to the appropriate separate CMS assignment*] Corinth University is interested in extending the above tag scheme to handle prerequisites that concern grades a student earns. The extended scheme should be able to support a prerequisite requirement like

(+) "Grade B or better in CS2110 and grade C+ or better in CS2800".

At Corinth University, students can receive one of the following grades in a course: F, D, D+, C-, C, C+, B-, B, B+, A-, A, A+. Prerequisites involving required grades must be specified using: "at least G" and/or "at most G" for a grade G.

Outline your proposed extensions to accommodate restrictions on grades. Schemes where the tags $\mathcal{T}$ still are propositional logic formulas will receive more credit than schemes where tags must be written using predicate logic. Your submission should explain: (i) What is the set $\mathcal{T}$ of

all possible tags, (ii) how to translate (+) into such a tag, (iii) what is the new definition of $\sqsubseteq$ (if a new definition is needed), (iv) what is the new definition of $\sqcup$ (if a new definition is needed).

Problem 2. [Up to 2 pages may be used.] The staff associated with a typical CS Department course at Cornell includes faculty, course support administrators, graduate teaching assistants, and undergraduate assistants. Students submit assignments --- either individually or in groups --- to CMS. CMS controls access to assignments, from submission to grading to regrades. In some classes, the different problems in an assignment are graded by different staff members; in other classes, a single staff member might be assigned to grade all of the problems in a subset of the submissions for a given assignment.

This enterprise seems well suited for role-based access control. Describe the design of such a role-based access control scheme for this application. At a minimum, your discussion should cover the following roles associated with a specific assignment *A*: *A*-faculty, *A*-grader, *A*-group (which identifies one or more students). However, feel free to discuss other roles, based on your understanding of how things work or ought to work.

- For each role discuss:
  - who is allowed to occupy the role
  - what privileges (if any) would be associated with that role.
  - what privileges (if any) would be inherited from other roles.
- List any constraints associated with a user's occupancy in roles. Give an English description or a Predicate Logic formulation using the terminology given in Figure 8.5 (page 189).