CS5432 Homework 3: Information Flow

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: April 30, 2021 at 11:59pm. 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.
- Start each problem on a separate page.

1. Using the type system developed in class, prove that the following program satisfies Relational Non-Interference (RNI). Use the label assignment $\Gamma = \{x : L, y : H, z : H\}$ and an initial context $ctx = L$.

   $x := 42; 
   \text{if } y > 0 
   \text{then } y := y - x 
   \text{else } z := x + 1 
   \text{fi}$
2. For each of the following programs and label assignments, determine whether or not the program satisfies (1) Termination Sensitive Non-Interference (TSNI), (2) Termination non-sensitive (aka Relational Non-Interference (RNI)).

a. \( \Gamma = \{ j : L, k : H \} \)
   \[
   \begin{align*}
   &k := 10; \\
   &\text{while } k > 0 \text{ do} \\
   &\quad j := j + 1; \\
   &\text{end}
   \end{align*}
   
   b. \( \Gamma = \{ m : L, n : L, p : H, q : H \} \)
   \[
   \begin{align*}
   &\text{if } n + m \neq -1 \\
   &\quad \text{then } m := 7 \\
   &\quad \text{else} \\
   &\quad\quad \text{if } p < 5 \\
   &\quad\quad\quad \text{then } q := p + 3 \\
   &\quad\quad\quad \text{else } n := 13 \\
   &\quad\quad \text{fi} \\
   &\text{fi}
   \end{align*}
   
   c. \( \Gamma = \{ i : L, j : H, k : H \} \)
   \[
   \begin{align*}
   &i := i + 10; \\
   &\text{if } i < 100 \\
   &\quad \text{then skip} \\
   &\quad \text{else} \\
   &\quad\quad \text{while } j \neq 0 \text{ do} \\
   &\quad\quad\quad k := k + j; \\
   &\quad\quad\quad j := j - 1 \\
   &\quad\quad \text{end} \\
   &\text{fi}
   \end{align*}
   
   d. \( \Gamma = \{ r : H, x : H, w : L \} \)
   \[
   \begin{align*}
   &\text{if } r \mod 2 = 0 \\
   &\quad \text{then } w := 0 \\
   &\quad \text{else} \\
   &\quad\quad x := (r + 1) \mod 2; \\
   &\quad\quad w := x \\
   &\text{fi}
   \end{align*}
   \]
3. We are given a programming language and type system (like was discussed in class) where all type-safe programs satisfy termination insensitive non-interference for the usual lattice involving L (public) and H (secret).

   a. You have been asked to endorse or reject a proposal to add a new built-in function, HRAND( ) to the programming language. Each time HRAND is called, it will return a value that has security label H and that is a random number. Thus, the history of past values it has returned tells nothing about future values it will return.

   b. You have been asked to endorse or reject a proposal to add a new built-in function, LRAND( ) to the programming language. Each time LRAND is called, it will return a value that has security label L and that is a random number. Thus, the history of past values it has returned tells nothing about future values it will return.