IS2150/TEL2810 Introduction to Security

Homework 1

Total Points: 100

Due Date: Feb 13, 2013

1) Exercise on Propositional/Predicate logic & Induction **[20 Points]**

(a) Express the following sentences in propositional//first order logic. Be sure to define all propositional components (e.g., predicate function, constants, and variables).

i) Some mammals live in water.
ii) A person can activate roles R1 or R2 but not both.
iii) If Steelers does not reach Superbowl then I will not watch the Superbowl.
iv) A *directory* is older than the *directories* and the *files* that it contains.

2) Prove by using Induction the following **[10 Points]**

$$1^3 + 2^3 + 3^3 + \ldots + n^3 = \left[\frac{n(n+1)}{2}\right]^2$$

3) Exercise on Lattice **[** **[15 Points]**

Consider set of digits $D = \{1, 2, 3\}$. Let S be set of all numbers containing two digits from D; i.e., each element $a \in S$ can be written as $a = a_1a_2$ where $a_1, a_2 \in D$ (i.e., they are elements of D). For instance $a = a_1a_2 = 12$ is an element of S, as $a_1 = 1$ and $a_2 = 2$. Let relation $\lesssim$ be the "*dominance*" relation on S. For every $a, b \in S$ we say a is *dominated* by b (written as $a \lesssim b$) if and only if $a_1 \leq b_1$ and $a_2 \leq b_2$ (Here $\leq$ is the "*less than or equal to*" relation on natural numbers 1, 2, and 3, i.e., $1 \leq 2$, $2 \leq 3$, $1 \leq 1$, etc.)

Draw the *Hasse* diagram for the partial order generated.

4) Do the following **[20 Points]**

i) Exercise 1, and 4 from exercises 1.11 of the green book (note that the brown book may/will have a different exercise number)

ii) Exercises 1(a) and 2(c) (*note*: checking for *absence of right* is not allowed!!) from section 2.6

5) The proof of Theorem 3–1 states the following: Suppose two subjects s_1 and s_2 are created and the rights in $A[s_1, o_1]$ and $A[s_2, o_2]$ are tested. The same test for $A[s_1, o_1]$ and $A[s_1, o_2] = A[s_1, o_2] \cup A[s_2, o_2]$ will produce the same result. Justify this statement. Would it be true if one could test for the absence of rights as well as for the presence of rights? **[15 Points]**

6) Consider a Turing Machine with the following specification **[20 Points]**

1. Set of states: $\{k_0, k_1, k_2, k_3\}$
2. Tape symbols: $\{A, B, C\}$
3. Final (or halting) state is k_3
4. Transition Functions:

$\delta(k_1, B) = (k_1, A, R)$;

$\delta(k_1, A) = (k_2, B, R)$;

$\delta(k_2, C) = (k_3, A, L)$;

$\delta(k_3, B) = (k_1, A, L)$;

$\delta(k_0, A) = (k_1, B, R)$;

Assume your TM's initial configuration is as shown below.

1. Show the mapping of the elements of this TM to a protection system.
2. Show all possible transitions, indicating each new TM configuration reached (i.e., state, head position and the symbols in each cell) and its corresponding protection state (the entries in the Access Control Matrix).