CNT 4419: Secure Coding [Fall 2023]
Test II

NAME: _____

Instructions:

1) This test is 7 pages in length.

2) You have 75 minutes to complete and turn in this test.

3) Short-answer and essay questions include guidelines for how much to write. Respond in complete English sentences. Responses will be graded as described on the syllabus. Respond at the level of detail discussed in class. Avoid using bullet points and enumerated lists.

4) This test is closed books, notes, papers, phones, smartwatches, laptops, friends, neighbors, etc.

5) Use the backs of pages in this test packet for scratch work. If you write more than a final answer in the area next to a question, circle your final answer.

1. [4 points] Buffers can be overflowed in which program segments? [1 sentence]

2. [Short essay] [6 points]
Explain the classic example of a confused-deputy attack, as discussed in class.

3. [Short essay] [6 points]
Explain the example path-traversal attack discussed in class, which is different from the attack referenced in Problem 2 above.

4. [One-page essay] [12 points]

Compare and contrast **computer security** with **healthcare**. Consider, for example, "defense in depth" and "attack evolution".

5. [21 points] Consider a simple, type-safe programming language L having two types, int and int list. The syntax for int-type expressions in L is the same as what we discussed in class; recall that int-type expressions may be added.

An int list in L is defined recursively as either nil (the empty list) or a pairing of (A) an int-type list head with (B) an int-list-type tail. For example, (5,(4,(3,nil))) is an expression of type int list that contains, in order, the values 5, 4, and 3. The overall list head is 5, and the overall list tail is (4,(3,nil)).

A list-type expression e may be decomposed into its head and tail using the syntax e.hd and e.tl. For the sake of simplicity, assume nil.hd returns 0, and nil.tl returns nil. An expression like (nil.hd,nil.tl) therefore also has type int list and evaluates to (0,nil).

a) Define L's syntax and semantics, using the conventions discussed in class.

b) Intuitively explain: Is the set of all possible int-list values in L countable? [1-2 sentences]

6. [6 points] Prove or disprove: The power set of binary numbers is countable. (For this problem you may assume that binary numbers do not have leading zeroes; for example, 01 never needs to be considered.)

7. [45 points]
For each of the following policies, prove whether it is a property, safety, and/or liveness. Assume the system of interest has some security-relevant action a.

a) $\{ \{t^1, t^2, ...\} \mid \forall i: a \notin t^i \}$

b) $\{ \{t^1, t^2, ...\} \mid \exists i: t^i = a;a;\ldots \}$

c) $\{ \{t^1, t^2, ...\} \mid \neg\exists i: t^i = a;a;\ldots \}$

d) $\{ \{t^1, t^2, ...\} \mid \forall i: t^i \text{ is infinite}\}$

e) { p | p is infinite}

f) $\emptyset$

g) $\{\emptyset\}$

h) $\{ \{t^1, t^2, ...\} \mid \forall i: a \notin t^i \} \cap \{ \{t^1, t^2, ...\} \mid \forall i: t^i \text{ is infinite}\}$

i) $\{ \{t^1, t^2, ...\} \mid \neg\exists i: t^i=a;a;\dots \} \cap \{ \{t^1, t^2, ...\} \mid \forall i: a \notin t^i \}$