CNT 4419: Secure Coding [Fall 2022]
Test I

NAME: _____

Instructions:

1) This test is 5 pages in length.

2) You have 40 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. Additionally, do not use bullet points in your responses.

4) This test is closed books, notes, papers, smartphones, 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. [5 points] As discussed in class, what does it mean for software to be secure? [1 sentence]

2. [5 points]
What does it mean for a programming language to be type safe? [1-2 sentences]

3. [5 points]
What are sound, complete, and precise mechanisms? [1-3 sentences]

4. [10 points] [1 paragraph]
Explain how a single mechanism may, depending on one's perspective, be considered either precise or imprecise. Hit all the main points discussed in class, including providing an example.

5. [45 points]
For each of the following policies, prove or disprove that the policy is a property.
$P_1 = \{\{t^1, t^2, \ldots\} \mid \forall i: \text{read}(0) \notin t^i\}$

$P_2 = \{\{t^1, t^2, \ldots\} \mid \forall i: \text{read}(0) \in t^i\}$

$P_3 = \{ \{t^1;\text{output}(k_1), t^2;\text{output}(k_2); \ldots\} \mid \{k_1,k_2,\ldots\} = K\}$, where K is the set of all 128-bit keys

$P_4 = \{ \{t^1;\text{output}(k_1), t^2;\text{output}(k_2); \ldots\} \mid \{k_1,k_2,\ldots\} \neq K\}$, where K is the set of all 128-bit keys

$P_5 = \{\{t^1, t^2, \ldots\} \mid \text{true } \}$

6. [5 points]
Contrast static mechanisms with dynamic mechanisms by stating the primary advantage and disadvantage of each, in general. [1-2 sentences]

7. [10 points]
In the instructor's opinion, what is the most challenging aspect of (i.e., biggest hurdle to) securing software? Hit all the main points discussed in class, and make an analogy with general software development. [2-5 sentences]

8. [5 points]
Explain what Type I errors are. Then explain what Type II errors are. Also provide synonyms for these terms. [2 sentences]

9. [10 points]
a) What is a predicate? [1 sentence]

b) How can a policy be defined as a predicate? [1-2 sentences]

c) How can a property be defined as a predicate? [1-2 sentences]