CNT 4419: Secure Coding [Fall 2022]
Test II

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. [3 points]   What does it mean for a programming language to be type safe? [1 sentence]

2. [3 points]   Contrast static mechanisms with dynamic mechanisms by stating the primary advantage and disadvantage of each, in general. [1-2 sentences]

3. [7 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]

4. [7 points]   Prove or disprove that the following policy is a property.
$P = \{ \{t^1;\text{output}(k_1), t^2;\text{output}(k_2); \ldots\} \mid \{k_1,k_2,\ldots\} \neq K\}$, where K is the set of all 128-bit keys

5. [25 points] Prove or disprove:
A property is both safety and liveness if and only if it is the trivial property.
Hint: "if and only if" is often notated $\Leftrightarrow$.

6. [15 points]   As discussed in class, explain why all access-control policies are safety properties. [1 paragraph]

7. [10 points]   As discussed in class, what is a general strategy for trying to enforce an arbitrary property in practice? [1-3 sentences]

8. [15 points]   As discussed in class, explain the CIA classification of policies, including its primary limitations. [1 paragraph]

9. [15 points]   Prove or disprove:
For all properties P, there exist safety property P_S and liveness property P_L such that $P = P_S \cup P_L$.