CNT 4419: Secure Coding [Fall 2022]
Test III

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. [10 points] Why does it matter whether a policy is a property, safety, or liveness? How might this information be useful? [1 paragraph]

2. [6 points] Describe the Curry-Howard Isomorphism, hitting all the main points discussed in class. [1-3 sentences]

3. [2 points] What is the classic defense against ransomware? [1 sentence]

4. [4 points]
What is polymorphic malware? Why might malware be polymorphic? [1-3 sentences]

5. [4 points]
What's the main idea of dialog fatigue? Provide a modern-day example of dialog fatigue that was discussed in class. [1-3 sentences]

6. [4 points]
Briefly describe two examples of path-traversal attacks discussed in class. [2 sentences]

7. [10 points] What are standard tradeoffs for improved software security? [1 paragraph]

8. [15 points] Prove: A property is both safety and liveness if and only if it is the trivial property.

9. [10 points] Prove or disprove: The set of real numbers is countable.

10. [10 points] Prove or disprove: The power set of natural numbers is countable.

11. [25 points] To keep things simple for this problem, assume that the only action of interest (i.e., the only security-relevant action) is `read(0)`.

When discussing the previous test in class, we defined a single property G such that G cannot be written as $G_S \cup G_L$, for any safety property G_S and liveness property G_L. Now define an infinite set I of properties such that every property in I cannot be written as $G_S \cup G_L$, for any safety property G_S and liveness property G_L. Is your infinite set I countable? Explain your answers.