CNT 4419: Secure Coding [Fall 2019]
Test 2

NAME: ____

Instructions:

1) This test is 5 pages in length.

2) You have 40 minutes to complete and turn in this test.

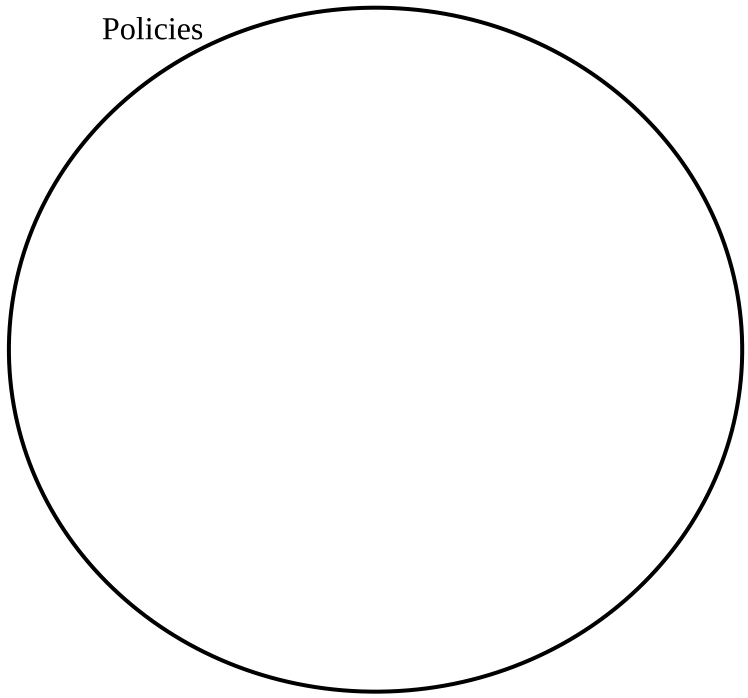
3) Short-answer and essay questions include guidelines for how much to write. Respond in complete English sentences. Responses will be graded as described on the syllabus.

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]
Explain why countability is relevant to software security. [2-4 sentences]

2. [60 points]
a) Complete the diagram below by drawing the subsets of policies discussed in class (i.e., properties, safety, and liveness).



Parts (b) to (h) define policies P_b to P_h. Categorize each of these policies by adding a dot on the figure above to show where that policy exists, and label the dot with that policy's name. Also briefly explain each of your categorizations in 1-3 sentences.

For all programs p:
b) $p \in P_b$ iff $\forall$ traces $t \in p$, $\text{read}(0) \notin t$

c) $p \in P_c$ iff $\text{write}(0);\text{write}(0);\ldots \in p$

d) $p \in P_d$ iff write(0);write(0);… $\notin p$

e) $p \in P_e$ iff $\forall p'$: $p' \subseteq p$

f) $p \in P_f$ iff $\forall p'$: $p \subseteq p'$

g) $p \in P_g$ iff $\top$

h) $p \in P_h$ iff $p \in P_b$ and $p \in P_d$ and $p \in P_g$

i) Prove or disprove that P_c is a property. Hint: use the formal definition of "property".

j) Prove or disprove that P_d is a property. Hint: use the formal definition of "property".

k) Of the example policies P_b to P_h, which are the easiest to enforce (precisely) in practice and why? How would the enforcement mechanisms work? [1 paragraph]

3. [30 points]

a) A triple of nats contains three values (i, j, k), where each of i, j, and k are natural numbers. Prove or disprove that the set of all triples of nats is countably infinite.

b) Let’s define a rint to be a value that’s either a positive real number or a negative integer. Prove or disprove that the set of rints is countably infinite.