CNT 4419: Secure Coding [Fall 2022]
Test V

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] [Short essay] Explain, using an example, how an integer-overflow attack may proceed. As part of your example, show the vulnerable code.

2. [3 points] What is fuzz testing? [1 sentence]

3. [5 points] Describe what happens to memory during a function return. [1-2 sentences]

4. [10 points] Consider a property P specifying that no traces are valid, not even the empty trace. Prove that P is a safety property.

5. [6 points] [Short essay] Compare and contrast access-control lists and capability lists.

6. [6 points] [Short essay] Compare and contrast mandatory and discretionary access control.

7. [10 points] [Short essay] What does each layer of the TCP/IP model do? Include information about addresses.

8. Consider the following code. Assume a 16-bit architecture, that all needed #include directives are present, that each character is stored in 1 byte and each integer in 2 bytes, and that the get_input function returns a user-entered string allocated on the heap.

```
0       char z = 'z'
1       char q(char *t) {
2          printf(t);
3          return 'q';
4       }
5       char p(char *t) {
6          char x[64];
7          x[63] = 'y';
8          q(t);
9          return 'p';
10      }
11      int main(int argc, char *argv[])
12         p(get_input());
13         return 0;
14      }
```

a) Draw a representation of the program memory segments (including their contents when known) right before the printf is executed, at the level of detail shown in class. Assume the system uses integer stack canaries and uses an optimized layout of memory, as discussed in class, where printf is not given its own frame. [20 points]

b) Assuming the input is "abc%d%n", describe what happens when running the printf, at the level of detail discussed in class. [1-2 sentences] [10 points]

9. [20 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)`.

Define an uncountably infinite set U of properties such that every property in U can be written as $G_S \cup G_L$, for some safety property G_S and liveness property G_L. Explain your answer.