CNT 4419, Fall 2026, Test 2, 75 minutes **NAME:**_____

Instructions: All the instructions in the syllabus. This test is closed everything, including phones, notes, AI, and other students. Do not talk to another student during the test. Do not look at another student's answers during the test. Do not ask a question during the test that gives away any part of any answer. If a response length is indicated, respond at that length and do not use bullet points or enumerated lists. Unless stated otherwise, use the same notations, definitions, and assumptions that we have been using in class. Respond at the level of detail discussed in class. Your proofs may repeat proofs discussed in class but should never establish a result merely by citing a theorem or proof discussed in class. This test is 5 pages.

1. [8 points] What is a CSPRING, and what are its features and characteristics? Hit all the main points discussed in class. [2-5 sentences]

2. [2 points] What is RCE? [1 sentence]

3. [4 points] Summarize one of the primary examples discussed in class, of quickly evolving an attack to circumvent a new defense. (Hint: Do not mention NX bits, StackGuard, ASLR, or CFI.) [1-2 sentences]

4. [4 points] Suppose a mechanism is measured to exhibit T_P true positives, T_N true negatives, F_P false positives, and F_N false negatives. The mechanism's *specificity* is defined as $T_N/(F_P+T_N)$. In the context of our in-class discussions, briefly summarize what specificity is measuring. [1 sentence]

5. [5 points] Summarize the story on Page 47 of the textbook, about a web application error. [1-3 sentences]

6. [20 points] For each of the following defenses, summarize the defense and how buffer-overflow attacks may still succeed, even with that defense. Hit all the main points discussed in class.
(a) NX bits [2-4 sentences]

(b) StackGuard [2-4 sentences]

(b) ASLR [2-4 sentences]

(c) CFI [2-4 sentences]

7. [25 points] As on Test 1, define the complement of policy P, written P^C, to be $\{p \mid p \notin P\}$.
(a) Prove or disprove the following. For all policies P, if P is a property then P^C is not a property.
(b) Prove or disprove the following. For all policies P, if P is not a property then P^C is a property.

8. [12 points] State as a theorem, and prove, the assertion from class, that Trivial is the only property that is both safety and liveness.

9. [20 points]
Consider the following code. Assume a 64-bit architecture, all needed `#include` directives are present, characters are 1 byte and integers 4 bytes, the `input` function returns a user-entered string allocated on the heap, and function arguments are always stored in reverse order (e.g., main's `argv` is stored at a higher address than `argc`) so successive varargs appear at successively higher addresses.

```
1     int f(char *t) {
2         printf(t);
3         return 0;
4     }
5     int y(char *s) {
6         int q;
7         f(s);
8         return 0;
9     }
10    int main(int argc, char *argv[])
11        y(input());
12        return 0;
13    }
```

a) Assume the system uses 64-bit stack canaries and an unoptimized memory layout, as discussed in class, where printf is given its own frame. Draw a representation of the program stack (including pointer values when known) right before the body of printf executes (i.e., right after the printf function-prologue finishes).

b) Assuming the input is "aaaaaaa%p%p%n" and addresses are always printed in 8 characters, describe what happens when running the printf, at the level of detail discussed in class. [1-2 sentences]