CNT 4419 Exam 5/7/25 (120 minutes) NAME: ____

Instructions: Same standard instructions as on the quizzes. As always, this exam is closed everything, including phones and other students. Do not talk to another student during the exam. Do not look at another student's answers during the exam. Do not ask a question during the exam that gives away any part of any answer. Respond at the level of detail discussed in class. Use the same notations and assumptions that we have been using in class. This exam is 9 pages in length.

1. [6 points] What are the primary addresses used in computer networking, common examples and sizes of those addresses in practice, and the OSI layer names and numbers at which each kind of address appears? Hit all the main points discussed in class. [Short essay]

2. [4 points] Continuing from the previous problem, what are the names, numbers, and primary functionalities of the other OSI layers, i.e., the layers not relevant for Problem 1? [Short essay]

3. [3 points] What is a vacuous truth? Provide and explain all the kinds of examples discussed in class. [2-3 sentences]

4. [4 points] Briefly describe “Deserialization of Untrusted Data” vulnerabilities and what application-level coders can do to mitigate them, hitting the main points discussed in class. [Short essay]

5. [5 points] What does authenticity mean in cryptography, which mechanisms are commonly used to provide authenticity, and under what assumptions do those mechanisms provide authenticity? Hit the main points discussed in class. [Short essay]

6. [8 points] Define SQL statements to create and populate two 2x2 tables (with none of their entries being null), then query an inner join and a right join of the two tables, and finally delete the tables. You do not have to use the join keyword for the inner join. Each join must produce a result with 1, 2, or 3 rows, and the right join must contain “where C is null” for some column-name C. Show the results of the queries.

7. [10 points]

Consider the following C code. Assume a 64-bit architecture, that all needed #include directives are present, that each character is stored in 1 byte and each integer in 4 bytes, that memory is laid out as in class (optimized to avoid a separate frame for printf), and that x is user supplied, is heap allocated, has a 512 max size, and cannot be overflowed.

```
float hi(char *x) {
   char y[512];
   printf(x);
   gets(y);
   return 2.718;
}
```

Assuming the system is using NX bits, ASLR, and StackGuard with 4-byte canaries, describe how a user could attack this program. Describe the attack at the level of detail we described attacks in class, including drawing memory when appropriate. [1-2 paragraphs]

8. Let’s define the complement of a property having “good” trace set G to be the property having good trace set G'={ t | t ∉ G }.

a) [5 points] Prove or disprove that safety properties are closed under complement.

b) [5 points] Prove or disprove that liveness properties are closed under complement.

c) [5 points] Prove or disprove that safety properties are closed under union.

d) [5 points] Prove or disprove that liveness properties are closed under union.

The next page is blank, in case you would like to continue your response there.

[This page provides optional additional space for Problem 8.]

9. [40 points, Essay] Assignment IV was due 3 days ago and reviewed many of this course's topics.

Now, identify and briefly summarize the readings for Assignment IV.

Then identify, from the longer list you were asked to study for the assignment, 5 different categories and their placements in the longer list. The 5 categories you identify must be in the top third of the longer list you were asked to study. For each of those 5 categories, also briefly summarize the category and the mitigating actions application-level coders can take, hitting all the relevant main points discussed in class.

Then identify and summarize a 6th category C such that C appears in multiple of the lists you were asked to study (in the bottom third of those lists), but C stands out because we did not discuss C in class. (Hint: C is unique; only one category on both lists should have stood out to you, when doing the assignment, as something we did not discuss at all in class.) Using the ideas we did discuss in class, and the course readings, also describe mitigating actions application-level coders can take for category C.

As always, partial credit is possible; even if you can't fully answer everything, answer what you can.

The next 2 pages are blank, in case you would like to continue your essay there.

[This page provides optional additional space for Problem 9.]

[This page provides optional additional space for Problem 9.]