

CNT 4419: Secure Coding [Fall 2022]
Test IV

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. [3 points] What does it mean for a programming language to be type safe? [1 sentence]

2. [4 points] Describe the Curry-Howard Isomorphism, hitting all the main points discussed in class. [1-2 sentences]

3. [5 points] Describe the classic confused-deputy attack discussed in class. [1-3 sentences]

4. [8 points] [Short essay]
What are 4 of the “secure software design principles” we discussed in class?

5. [12 points] [Short essay]
Briefly describe the 4 attacks against the SimpleWebServer code discussed in class. What is the effect of each attack?

6. [8 points] [Short essay] Compare and contrast the Bell-LaPadula Model with the Biba Model.

7. [6 points] [1-3 sentences]

Describe the 3 standard authentication factors and provide 2 examples of each.

8. [3 points] Summarize ROP. [1-2 sentences]

9. [6 points] Describe how the stack gets manipulated during a function invocation, including explaining which code is responsible for each manipulation. [1-3 sentences]

10. [5 points] Describe how the stack gets manipulated during a function return, including explaining which code is responsible for each manipulation. [1-3 sentences]

11. [6 points] [Short essay] What are the common program-memory segments, and what sorts of data are stored in each of those segments?

12. [10 points] Prove or disprove: A property that's both safety and liveness must be trivial.

13. [10 points] Prove or disprove: The power set of natural numbers is countable.

14. [14 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 Test II 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.