

CNT 4419, Sec 001, Test 1, 75 minutes **NAME:** _____

Instructions: All the instructions that are on the syllabus. For example, 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. Use the same notations, definitions, and assumptions that we have been using in class. Respond at the level of detail discussed in class. This test is 6 pages.

1. [4 points] As discussed in class, what are four ways software may misplace trust? [1 sentence]

2. [6 points] Briefly describe phishing and types of phishing, as discussed in class. [2-4 sentences]

3. [6 points] Briefly explain why the termination property can be enforced completely and soundly but not precisely. [2-4 sentences]

4. [13 points] In class we discussed the classic example of a confused-deputy attack. Explain how the overarching vulnerability in this example could be considered as allowing violations of C, I, and A policies (per the CIA triad), following our discussion in class. [3-5 sentences]

5. [6 points] Explain the many-to-many relationship between policies and mechanisms and why it is useful. [2-4 sentences]

6. [5 points] Prove that the property $G = \{ t \mid \text{read}(0) \in t \}$ is not safety using the shortest possible counterexample.

7. [13 points] Let $P_1 = \{\emptyset, \{\varepsilon\}\}$ and $P_2 = \{p \mid p \notin P_1\}$.
Where would P_1 and P_2 belong, in our map of policies? In other words, for each of P_1 and P_2 , prove whether it is a property, safety, and/or liveness.

8. [14 points] Define the complement of a property having “good” trace set G to be the property having good trace set $G' = \{ t \mid t \notin G \}$.

- a) Prove or disprove that safety properties are closed under complement.
- b) Prove or disprove that liveness properties are closed under complement.

9. [33 points] Given properties G_1 and G_2 , define their concatenation $G_1;G_2$ as follows.

$$G_1;G_2 = \{ t_1;t_2 \mid t_1 \text{ is finite and } t_1 \in G_1 \text{ and } t_2 \in G_2 \}$$

a) Let $G_1 = \{ \epsilon, \text{read}(1) \}$ and $G_2 = \{ \epsilon, \text{read}(2), \text{read}(2);\text{write}(1) \}$. Then for each of the three properties G_1 , G_2 , and $G_1;G_2$, prove whether that property is safety, liveness, both, or neither.

b) Let $G_1 = \{ t \mid \forall a \in t: a = \text{read}(0) \}$ and $G_2 = \{ \epsilon \}$. Then for each of the three properties G_1 , G_2 , and $G_1;G_2$, prove whether that property is safety, liveness, both, or neither.

c) Let $G = \{ t \mid t \text{ is infinite} \}$. Then for each of the two properties G and $G;G$, prove whether that property is safety, liveness, both, or neither.

d) Can you draw any conclusions from Parts (a)-(c)? Explain briefly. [1-2 sentences]

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

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