CNT 4419: Secure Coding [Fall 2019]
Test I

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.

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. [4 points]
As discussed in class, what does it mean for software to be secure? [1 sentence]

2. [12 points]
Why do we separate policies from mechanisms? What is the relationship between policies and mechanisms? [2-4 sentences]

3. [6 points]
Define sound, complete, and precise mechanisms. [1-3 sentences]

4. [6 points] [1-2 sentences]
Explain what Type I and Type II errors are. Also provide synonyms for these terms.

5. [16 points]
a) Formally define policies as we did in class.

b) Formally define properties as we did in class.

c) Formally define safety properties as we did in class.

d) The formal definition of policies discussed in class could be called a qualitative model, because the definition qualifies some programs as "good". Other models consider policies quantitatively; these models quantify how good programs are (e.g., on a scale of zero to one). Formally define policies in a quantitative model.

6. [6 points]
As we did in class, draw a diagram to show the high-level relationships between an untrusted program, a bi-directional dynamic mechanism, and a processing/executing system.

7. [10 points]
a) What is a predicate? [1 sentence]

b) How can a policy be defined as a predicate? [1-2 sentences]

c) How can a property be defined as a predicate? [1-2 sentences]

8. [20 points]
Describe the CIA classification of policies and its limitations. [1 paragraph]

9. [10 points]
Suppose that a thief obtains the password to unlock a victim's phone, steals the phone, and successfully uses the password on the stolen phone.
a) Explain how the phone's password checker may be considered to exhibit a false negative. [1-2 sentences]

b) Explain how the phone's password checker may be considered to exhibit a true negative. [1-2 sentences]

10. [10 points]
a) Define an example property, first using set-builder notation and then using a one-sentence English description. Prove that your example is indeed a property.

b) Define an example nonproperty policy, first using set-builder notation and then using a one-sentence English description. Prove that your example is not a property.