CIS 6373: Foundations of Software Security [Fall 2019]
Test I

NAME: _____

Instructions:

1) This test is 7 pages in length.

2) You have 75 minutes to complete and turn in this test.

3) For essay problems, respond in complete English sentences. Responses will be graded as described on the syllabus. **Avoid bullet points in essays.**

4) This test is closed books, notes, papers, 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. [10 points, essay]
Compare and contrast the possible venues for publishing computer-security research, at the high level of detail discussed in class.

2. [5 points, essay]
Describe standard organizations/structures of research papers in the area of software security.

3. [10 points, essay]
Describe the CIA classification of policies and its limitations.

4. [15 points, essay]
Describe the different kinds of security automata we discussed in class, including their features, operational semantics, and benefits.

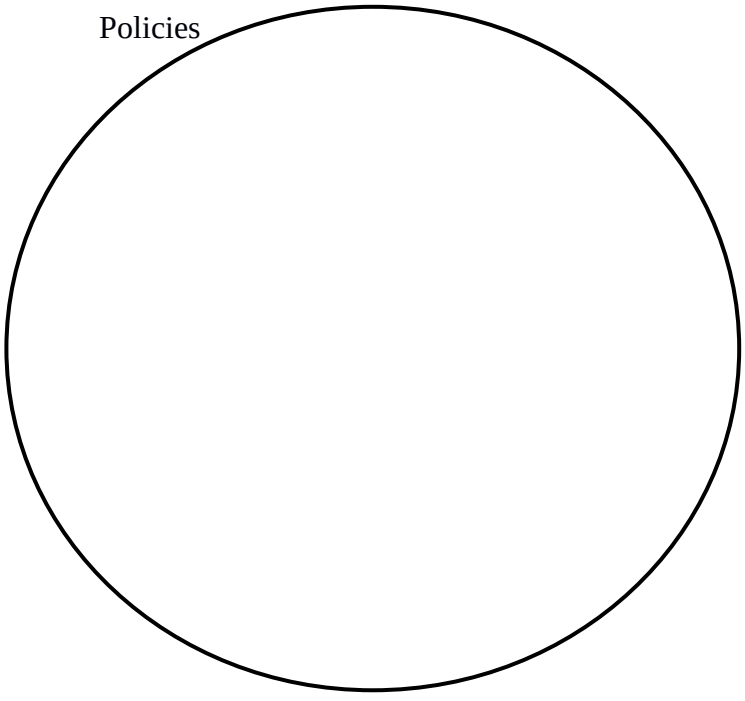
5. [15 points]
Draw a chart to show formal definitions of policy, property, safety, and liveness in qualitative and quantitative models.

6. [5 points, essay]
What are sound, complete, and precise mechanisms? How do these types of mechanisms relate to false positives and negatives?

7. [5 points, essay]
What are benefits, as discussed in class, of exchange-based executions?

8. [10 points, essay]
Why are many existing models of mechanisms limited to enforcing safety properties? What would be required to change in these models, to enable enforcement of nonsafety properties? How can mechanisms enforce nonsafety properties in practice?

9. [25 points]
a) Complete the diagram below by drawing the subsets of policies discussed in class (i.e., properties, safety, and liveness).



Parts (b) to (h) on the next page define policies P_b to P_h. Categorize each of these policies by adding a dot on the figure above to show where that policy exists, and label the dot with that policy's name. Also briefly explain each of your categorizations in 1-3 sentences.

For all programs p:
b) $p \in P_b$ iff $\forall$ traces $t \in p$, read(0) $\notin t$

c) $p \in P_c$ iff write(0);write(0);… $\in p$

d) $p \in P_d$ iff write(0);write(0);… $\notin p$

e) $p \in P_e$ iff $\forall p'$: $p' \subseteq p$

f) $p \in P_f$ iff $\forall p'$: $p \subseteq p'$

g) $p \in P_g$ iff true

h) $p \in P_h$ iff $p \in P_b$ and $p \in P_d$ and $p \in P_g$

i) Prove or disprove that P_c is a property. Hint: use the formal definition of "property".

j) Prove or disprove that P_d is a property. Hint: use the formal definition of "property".

k) Of the example policies P_b to P_h, which are the easiest to enforce (precisely) in practice and why? How would the enforcement mechanisms work? [1 paragraph]